Edge Software Configurator

Get Started Guide

March 2023

Document Number: 773406-1.1

Contents

Figures

Tables

Revision History

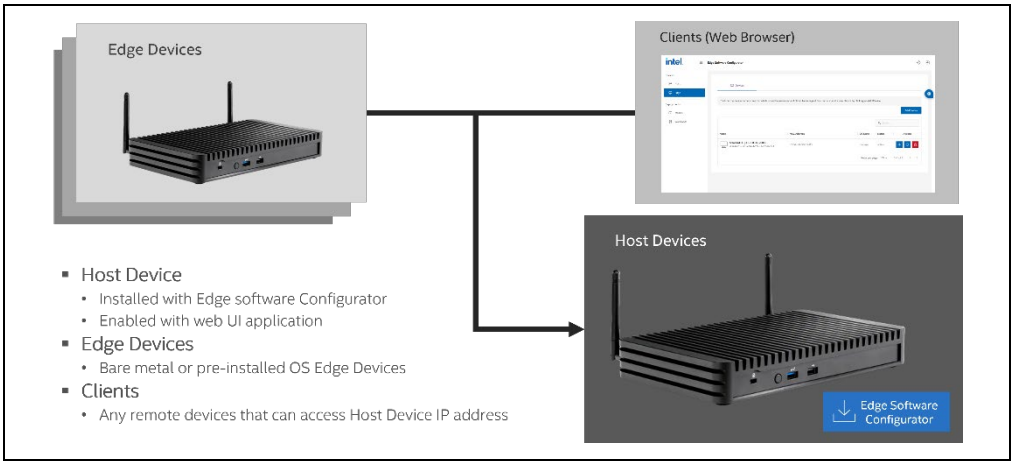
Date	Revision	Description
March 2023	1.1	• Updated release for software release version 6.1. • Updated with the latest figures.
December 2022	1.0	• Initial release for software release version 6.0.

§

1.0 How It Works

Edge Software Configurator (ESC) is a web-based graphical interface software toolkit that helps users to scale and enable software solutions on the Intel-based platform. It is also used to configure, deploy and manage workloads on the edge devices.

Figure 1. High-level Overview



The Edge Software Configurator will be installed on the host device, which will be enabled with a graphical user interface that can be accessed remotely via its IP address. Edge devices are the devices connected to the ESC server. The main component for this software framework is based on ansible. The ansible component allows the user to deploy the playbook configuration file on the specific devices. On top of the ansible framework, the backend and frontend server enables the background services management and graphical user interface respectively.

Edge Software Configurator provides a simple graphical user interface for:

- Host device configuration and management -This feature allows the user to install specific deployments or workloads on the host device itself where the Edge Software Configurator is being installed.
- Edge devices configuration and management - This feature allows the user to onboard remote edge devices and install specific deployments or workloads remotely without the need to run commands manually on specific edge devices.
- Asset management -This feature allows the user to manage the created assets through the deployed workloads.
- Deployment configuration and management. This feature allows the user to configure their own deployments that can be used to be deployed on specific edge devices.

Refer to the System Setup section for installation instructions and Tutorials to get started on using the Edge Software Configurator.

1.1 Terminology

Table 1. Terminology

Term	Description
ESC	Edge Software Configurator
ID	Identifier
Intel® SEO	Intel® Smart Edge Open
ISO	Optical Disc Image
KVM	Kernel-based Virtual Machine
OS	Operating System
USB	Universal Serial Bus
UUID	Universal Unique Identifier
VM	Virtual Machine

2.0 System Setup

Note: This system setup is intended for on-premises use cases. You should also configure the firewall on the device.

Note: Linux* bridge network will be configured automatically during the installation.

2.1 Hardware Setup

To get started with the complete features, both host and edge devices will be required including additional peripherals. However, users may skip some of the hardware required depending on their specific use cases.

2.1.1 Hardware Required

The table below lists the hardware required that will be used in this get started guide.

Table 2. Hardware Required

Hardware	Quantity	Description
Host device	1	Intel® Xeon®/ 11th Gen Intel® Core™ and above • At least 16GB memory (without Intel SEO) • At least 32GB memory (with Intel SEO) • At least 480GB storage
Edge device	1	Intel 11th Generation and above • At least 8GB memory
USB drive	1	Storage device used to create bootable ISO device • At least 8GB storage
Network switch/router	1	To provide network connectivity to devices • At least 2 LAN port that can be used
Other peripherals	1-2	Monitor, mouse, keyboard, LAN cable that will be used to connect with host and edge devices

Note: Older generation devices can still be used but may not be covered within the verified list of devices.

2.1.2 Device Setup

1. Connect the host device and edge devices to the same network. This can be done by connecting the device to the router/switch through their Ethernet ports.

Note: The default setup will use the default network routing IP address as server name or URL. Refer to README.md in the release package for the installation option if you need to customize the server URL via the custom domain name.

2. Connect the devices to other peripherals such as monitor, mouse and keyboard whenever necessary.

2.2 Software Setup

By downloading this get started guide, you should already have the released software package.

2.2.1 Software Required

Below is the software required for this get started guide

Table 3. Software Required

Software	Link	Description
Edge Software Configurator	Included in this software packages	Software package for Edge Software Configurator
Ubuntu* 22.04.01 Desktop LTS	Current: https://releases.ubuntu.com/22.04/ Alternative: https://old-releases.ubuntu.com/releases/22.04/	Linux* Ubuntu* 22.04 Desktop ISO installer that will be used on the host device and edge devices
clonezilla-live-20220620-jammy-amd64.iso	Current: https://jaist.dl.sourceforge.net/project/clonezilla/clonezilla_live_alternative/20220620-jammy/clonezilla-live-20220620-jammy-amd64.iso	Clonezilla* ISO image that will be downloaded automatically during the creation of configurator live image. Users **do not require** to download this file manually.
Rufus	https://rufus.ie/en/	Software to create bootable ISO device

2.2.2 Preparation

To avoid any unknown issues, please ensure that the host device is freshly installed with Ubuntu* 22.04. If you are running the setup behind a proxy network, please ensure the proxy configuration is configured properly in the `/etc/environment` file.

Note: This software will deploy multiple docker containers as part of the ESC services. Hence, Docker* will be part of the main requirements for this software to be up and running. You can either pre-install your system with Docker* or use the setup script in the Installation section to automatically install Docker* on your system. You

should secure your host configurations and Docker* daemon configurations properly on your system as part of the setup.

2.2.3 Installation

Assuming Ubuntu* 22.04 is already installed on the host device, below are the steps required to install the Edge Software Configurator on the host device.

3. Unzip or extract the release package of `<package_name>.zip` on the host device. In this example, it will be extracted in the home directory of the current user account.

Figure 2. Extracted Release Package

```
backend  CHANGELOG.md  frontend  licenses  README.DEV.md  README.md  setup  setup.sh
```

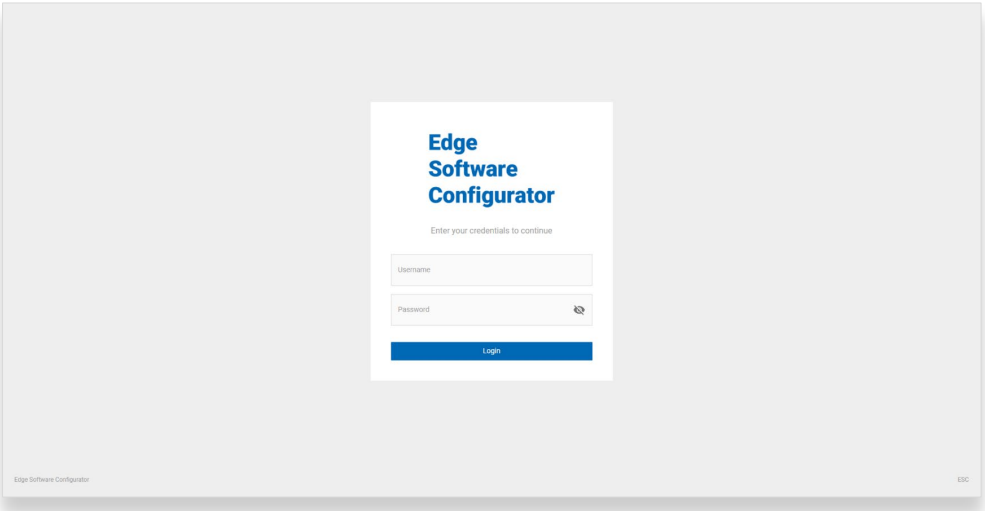
4. From the extracted package, run the command below to start the installation. The user will be prompted to enter the username and password that will be used to log in to the graphical user interface later.

Note: The default setup for SSL certificates configuration is valid for 365 days. All services will stop working when this SSL certificates are expired. Refer to README.md file of the release package for the available installation options to override the default setting.

```
sudo -E ./setup.sh -i
```

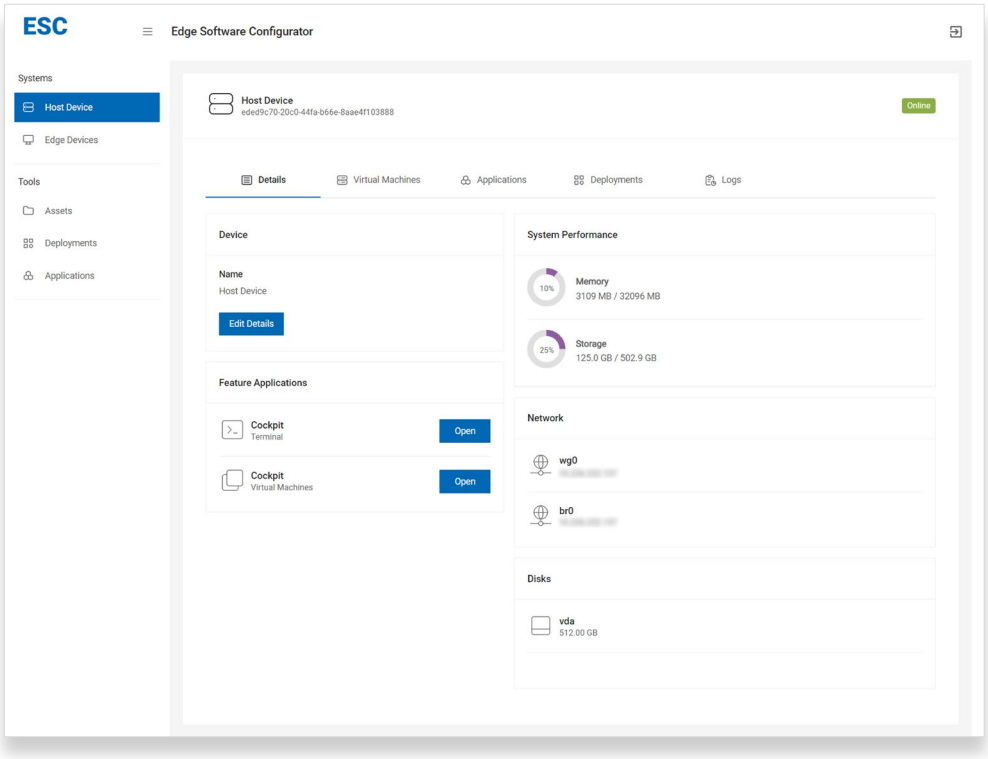
5. After the installation is completed, you can access the graphical user interface of Edge Software Configurator by accessing the URL of the host device IP address.

Figure 3. Edge Software Configurator Login



6. After logging in using the earlier credentials entered during installation, you should be able to see host device details as shown below.

Figure 4. Host Device Details



7. Now, you should be able to proceed with the remaining Tutorials and Use Cases depending on your requirements.

2.2.4 Uninstallation

Note: This step is only needed when you need to remove the software from your host device. Skip this step if it is not needed.

Note: All data created by this software will be automatically removed. Keep a backup if needed.

Below are the steps required to uninstall the Edge Software Configurator from the host device.

1. From the extracted package, run the command below to start the uninstallation.

```
sudo -E ./setup.sh -u
```

```
Verifying installation
Uninstalling
Verifying application
Application is running. Stopping
Removing service esc_backend_ansible
Removing service esc_backend_core
Removing service esc_backend_db
Removing service esc_backend_nginx
Removing service esc_backend_redis
Removing service esc_frontend_ui
Removing network esc_network_overlay
Removing core directories
Removing build directories
Docker secret 'app_key' found. Removing
Docker secret 'app_pwd_key' found. Removing
Docker secret 'app_ansible_key' found. Removing
Docker secret 'app_db_key' found. Removing
Docker secret 'app_redis_key' found. Removing
Docker secret 'app_jwt_pri_key.pem' found. Removing
Docker secret 'app_jwt_pub_key.pem' found. Removing
Docker secret 'server.key' found. Removing
Docker secret 'server.crt' found. Removing
Docker secret 'server-ca.crt' found. Removing
Docker image 'esc.frontend.ui' found. Removing
Docker image 'esc.backend.core' found. Removing
Docker image 'esc.backend.ansible' found. Removing
Docker image 'esc.backend.task' found. Removing
Removing application directories
Uninstallation completed
```

2. If any errors appear during the uninstallation, retry the command above until uninstallation is completed.

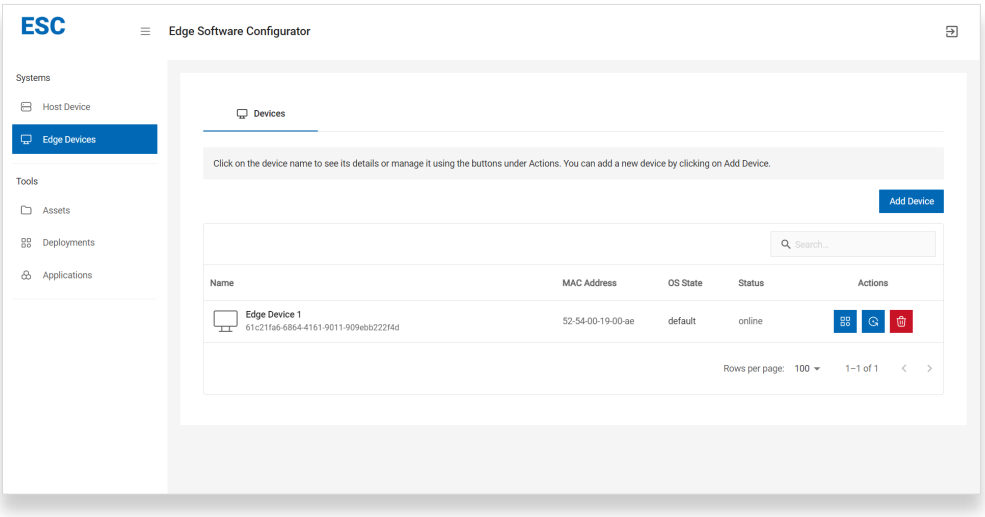
§

3.0 Tutorials

3.1 Devices

Systems consist of the host device and edge devices. You may onboard edge devices to manage them through ESC. Edge devices that have been onboarded will be listed in the **Edge Devices** tab under **Systems**. You may view their details and add different deployments to these devices to carry out different tasks.

Figure 5. View Edge Devices



3.1.1 Onboarding

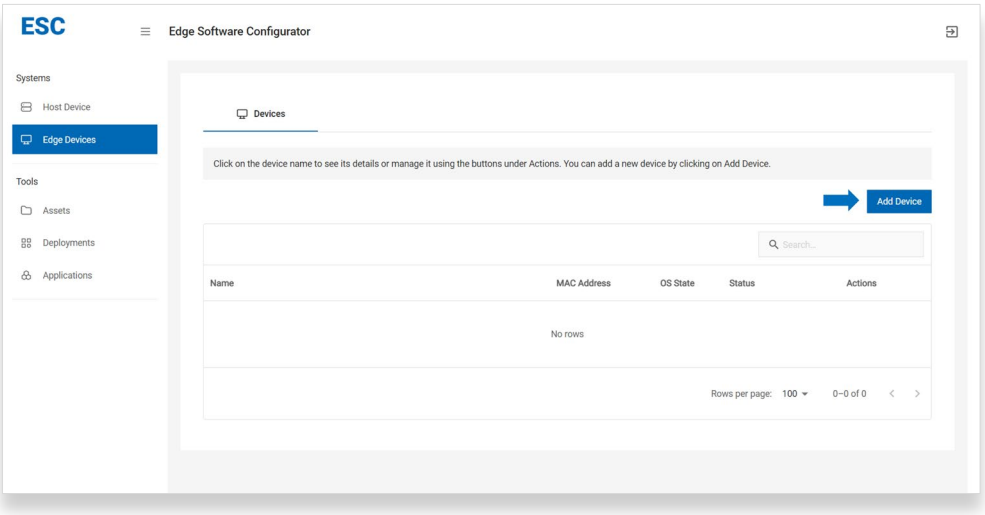
Both bare metal and pre-installed OS devices can be onboarded and managed by ESC.

Note: The device's UUID (product ID) will be used as a unique identifier in the database. Thus, each device that will be onboarded must have a unique UUID. Otherwise, onboarding the device will fail since it is detected as the same device.

Note: Devices with an empty UUID will fail to onboard. Please ensure the devices have a valid configuration.

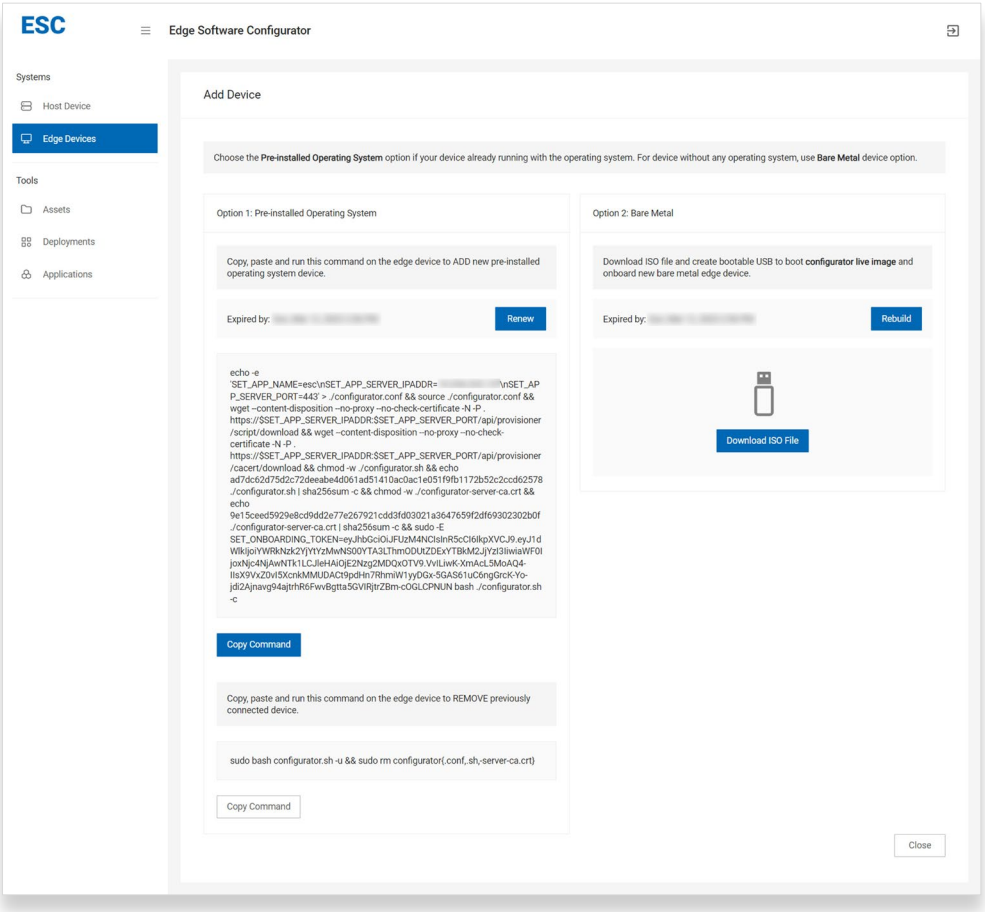
1. To onboard new edge devices, click on the **Add Device** button.

Figure 6. Add Device



2. You may onboard devices with a pre-installed OS or onboard them as bare metal devices.

Figure 7. Onboard Devices

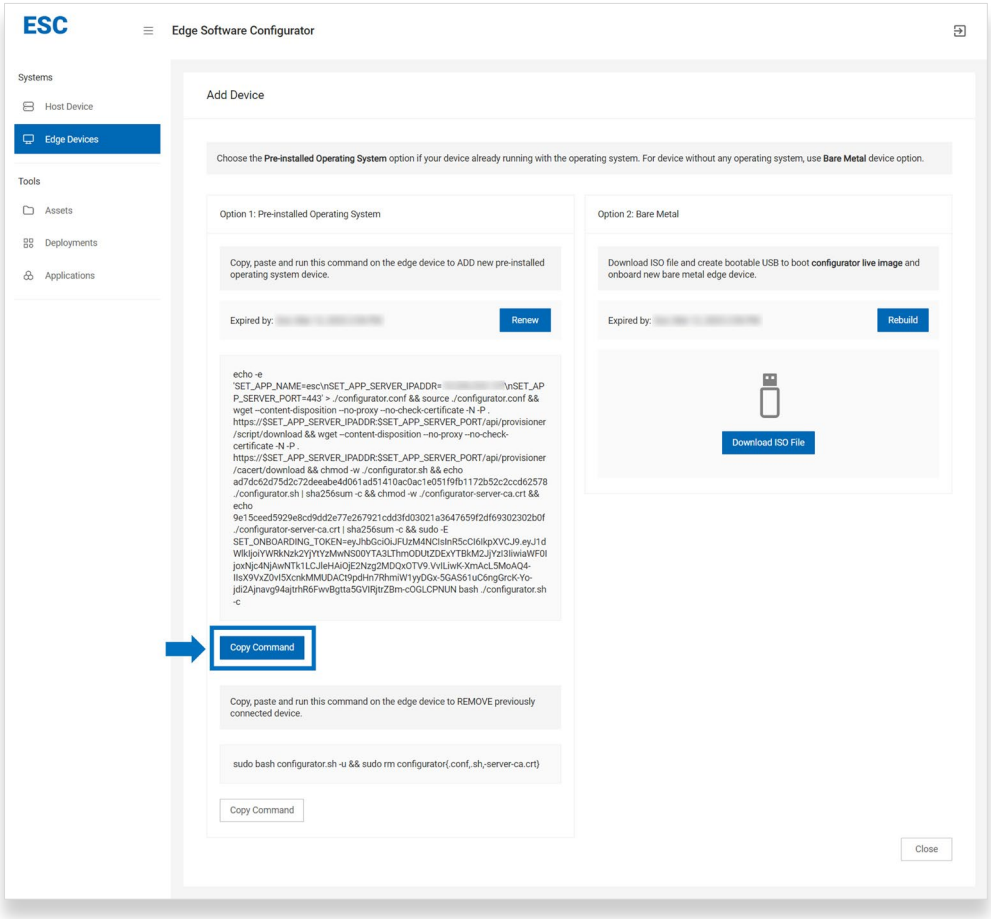


3.1.1.1 Pre-installed Operating System

To onboard devices with pre-installed OS:

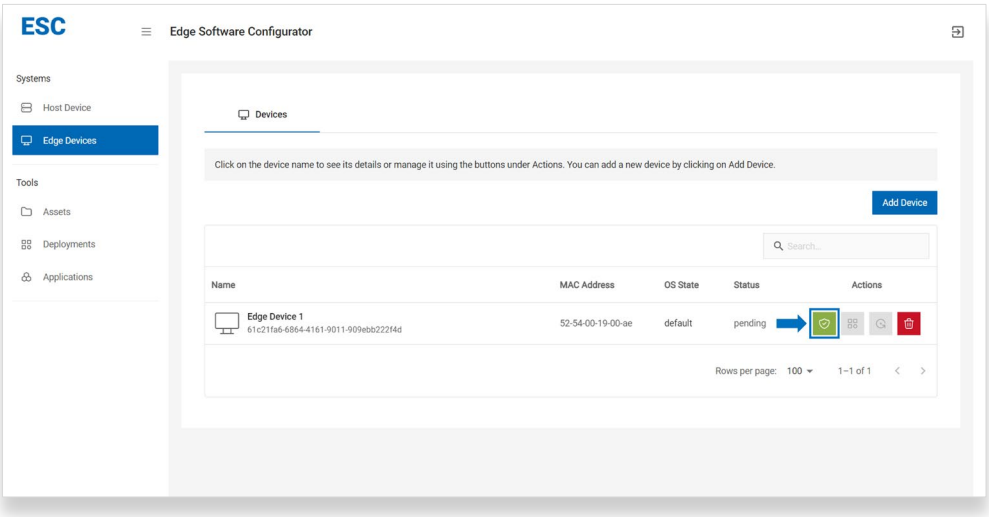
1. Copy the command via the **Copy Command** button.

Figure 8. Copy Command



2. Paste and run the command in the terminal of the device to be onboarded.
3. When the script has finished running, you will be prompted to authorize the device on the web UI.
4. Navigate to the **Edge** tab under **Devices** and authorize the device.

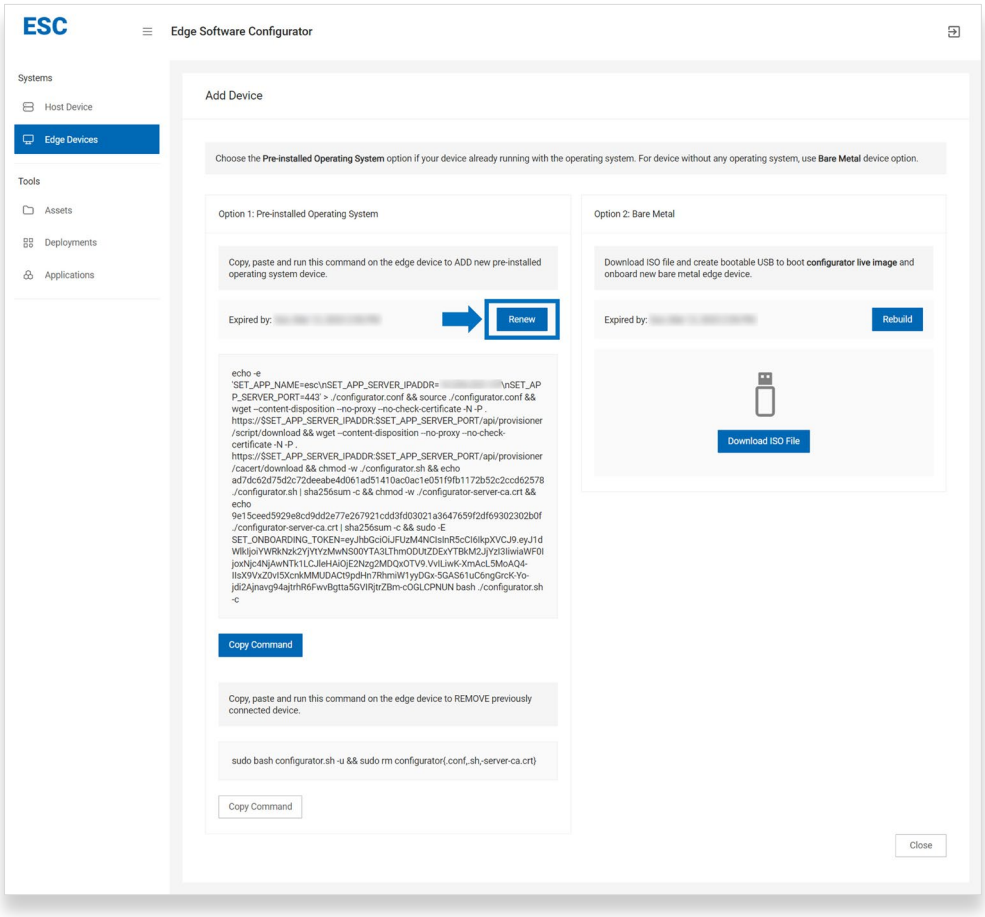
Figure 9. Authorize the Device



5. If onboarding is successful, the device should be online within a moment.

Note: The onboarding token has a time expiration. The onboarding will fail if the token has expired. You may renew the onboarding token by the **Renew** button or by logging out.

Figure 10. Renew Token

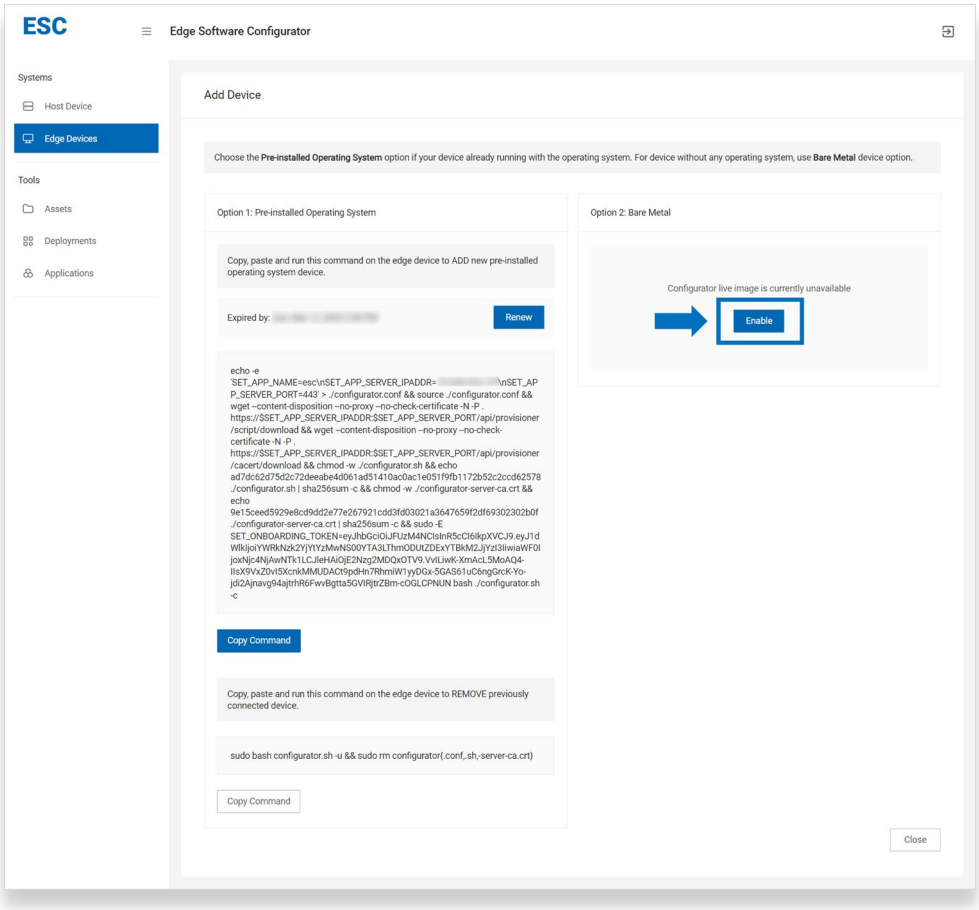


3.1.1.2 Bare Metal

To onboard bare metal devices, follow the steps below.

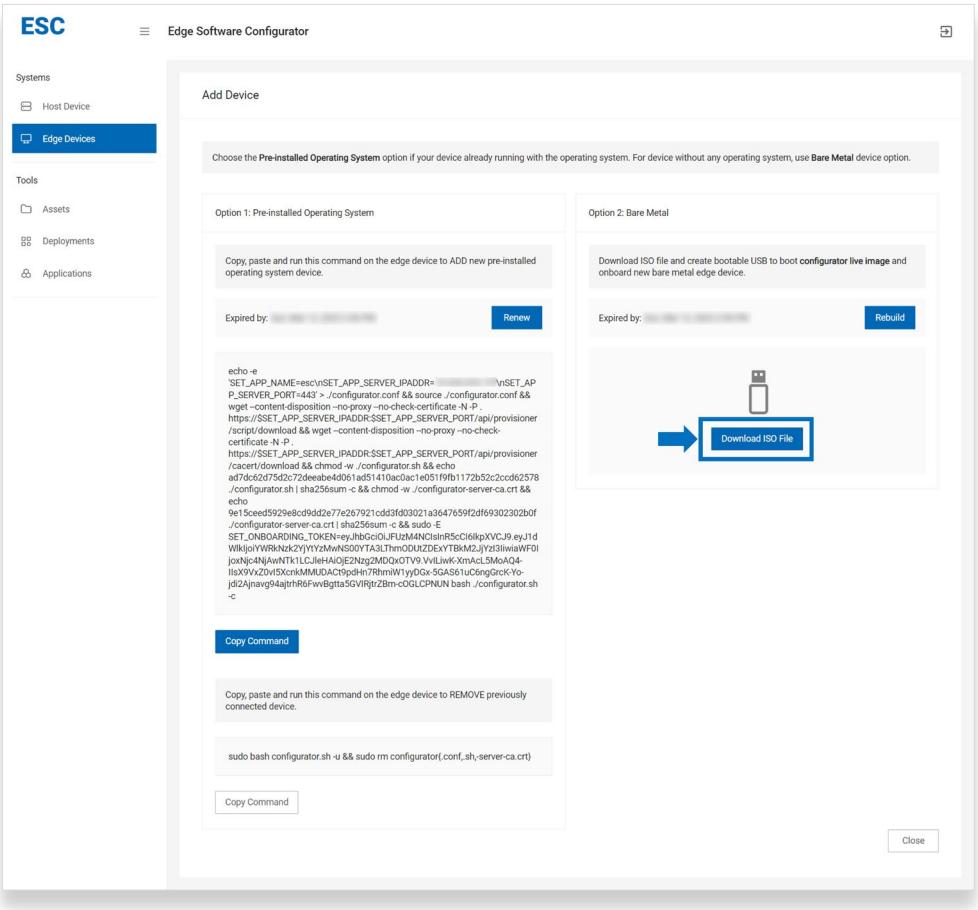
1. To enable bare metal device onboarding, you will have to enable the function on the web UI by clicking the **Enable** button. This will start the process to build the configurator live image.

Figure 11. Enable Bare Metal Device Onboarding



2. Once the configurator live image has been created, you may download it from the UI.

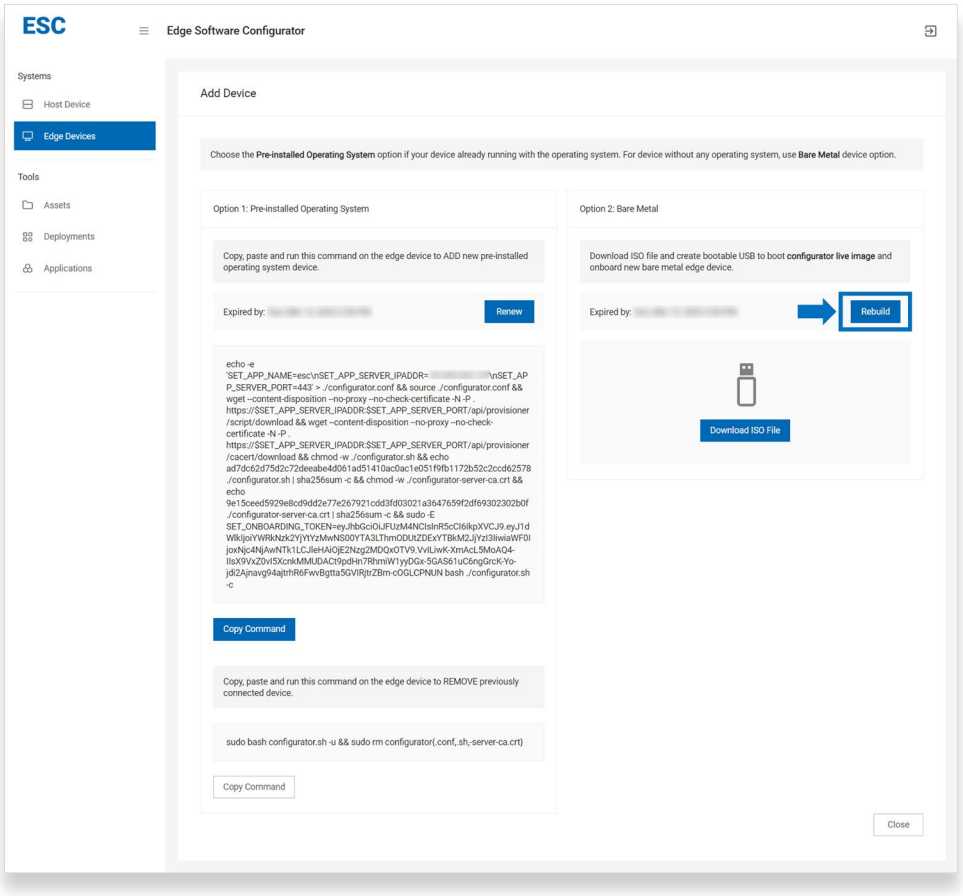
Figure 12. Download Live Image



3. Create a bootable USB using the live image. You can do this via Rufus*.
4. Boot the bare metal device to be onboarded using the newly created bootable USB.
5. Navigate to the **Edge** tab under **Devices**, and authorize the device.
6. The device should become online in a moment if the onboarding is successful.

Note: The configurator live image has a time expiration. The onboarding will fail if the image has expired. You may renew the image by clicking the **Rebuild** button.

Figure 13. Rebuild and Renew Image



3.1.2 Re-onboarding

This section is required if you are trying to re-onboard the same device between two different Operating system states. The two operating system states are as below:

1. Default operating system – The operating system that is directly booted from the physical hard drive.
2. Live operating system - The operating system booted from the bootable device which is referring to configurator live OS in this current scope

Note: Device re-onboarding is disabled by default to prevent unauthorized device onboarding request to appear on the server.

3.1.2.1 Pre-installed OS to Bare Metal

This scenario happens when the user has already onboarded a device with pre-installed OS and is trying to save its disk image by booting up the device with a configurator live image. Before booting up the device with the bootable USB which

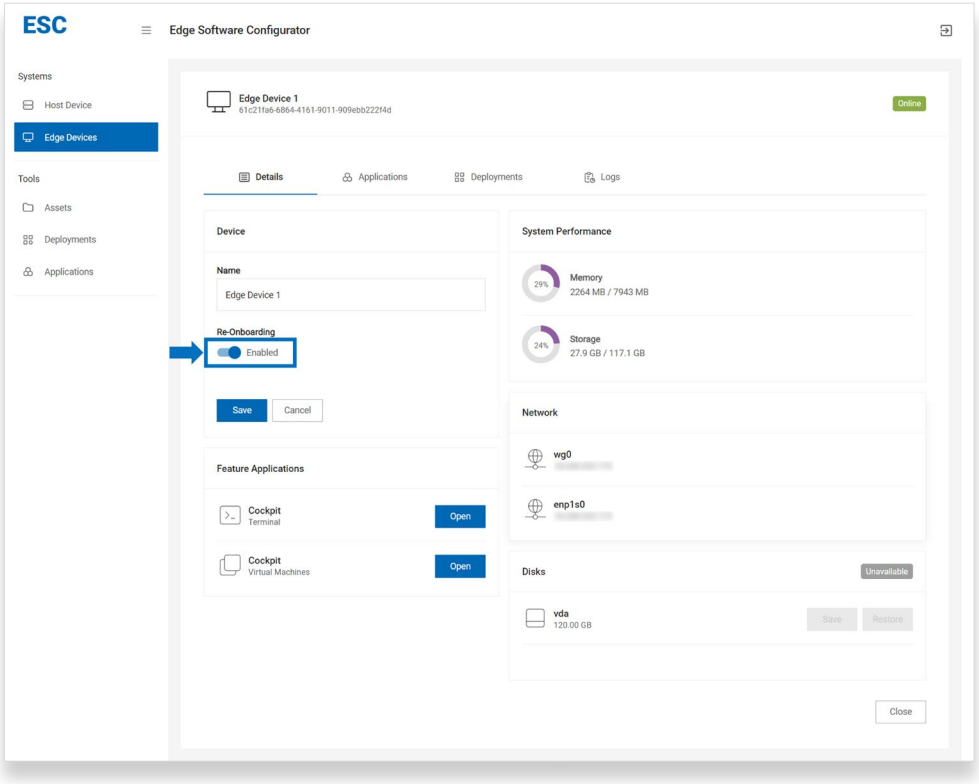
has been loaded with a configurator live image, you will need to enable device re-onboard.

Note: Proceed with the steps below if you are currently booted up with the default or pre-installed OS only. Refer to the Pre-installed Operating System section to onboard the device (if it is not) before proceeding with the steps below.

1. Go to **Edge** under the Devices tab, and click on the specific device name to see the device details.

2. From the device **Details** page, click on **Edit Details** button to enable device Re-onboarding and click the **Save** button.

Figure 14. Enable Device Re-onboarding from Pre-installed OS State



3. Proceed to boot up the device with a bootable USB and continue to authorize the device to complete the onboarding process.

3.1.2.2 Bare Metal to Pre-installed OS

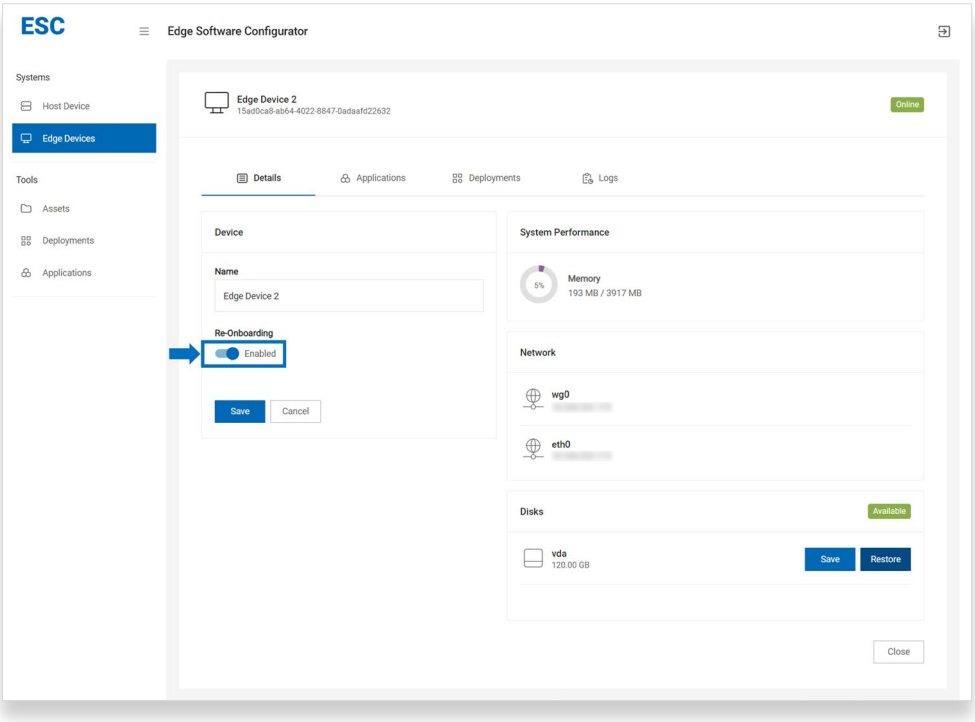
This scenario happens when the user has already onboarded a bare metal device and has restored the disk image. Before booting up the device with the restore disk image, you will need to enable device re-onboarding.

Note: Proceed with the steps below if you are currently booted with the configurator live image only. Refer to Bare Metal section before proceeding with the steps below.

1. Go to the Edge Devices tab, and click on the specific device name to see the device details.

2. From the device **Details** page, click the **Edit Details** button to enable device Re-onboarding, and click the **Save** button.

Figure 15. Enable Device Re-onboarding from Bare Metal State



3. Proceed to boot up the device with the restored disk image.

Note: If the restore disk image has not run the onboarding script yet, go to Pre-installed Operating System section to onboard the device.

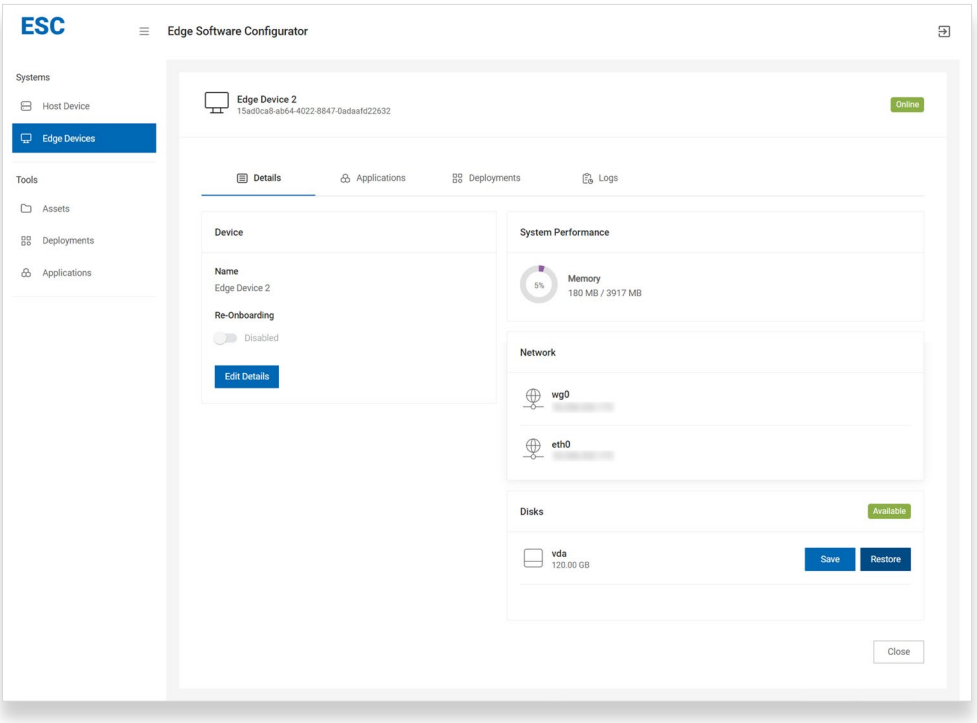
4. Authorize the device to complete the onboarding process.

Note: After the device is successfully re-onboarded, the user is recommended to disable the re-onboarding option if it is not required anymore. Only enable the option when it is needed.

3.1.3 Device Details

If the devices have been onboarded successfully, you should be able to observe their details by clicking their name. It will show the device name and the re-onboarding button, which can be edited by the **Edit Details** button. The memory status of the device as well as the disk information will be shown.

Figure 16. View Device Memory Status and Disk Information



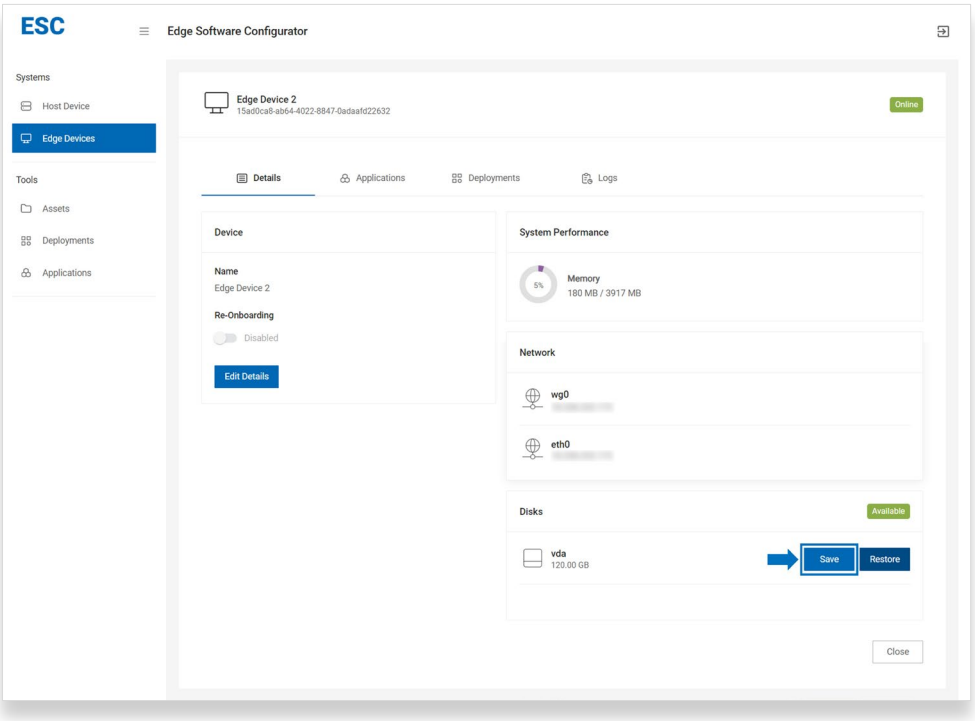
Note: Pre-installed OS devices will not have the Save and Restore disk option enabled.

3.1.3.1 Save Disk Image

Note: This section is only applicable when the user is currently booted up with the configurator live image. Go to the Bare Metal section to enable this feature.

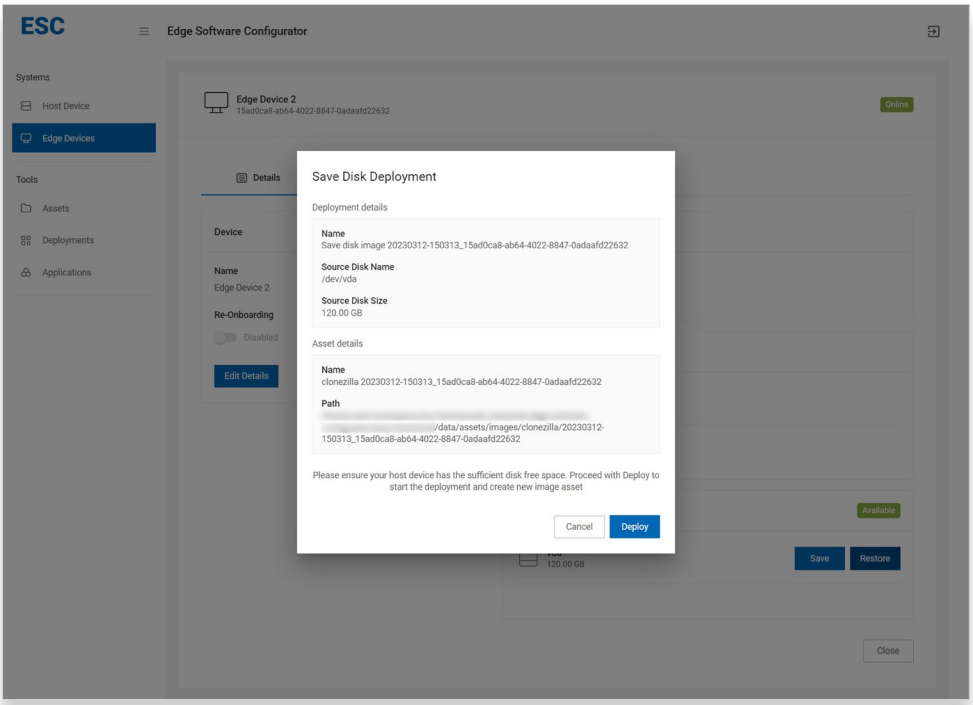
1. Go to **Edge Devices** tab under **Systems**, and click on the specific device name to see the device details .
2. Click on the **Save** button of the specific device disk to proceed with the new disk image asset creation.

Figure 17. Save the Specific Device Disk



3. Review the two instances that will be created as part of this deployment. Save disk deployment instance will be created to execute this process and a new image asset will be created as part of this save process.

Figure 18. Save Disk Deployment

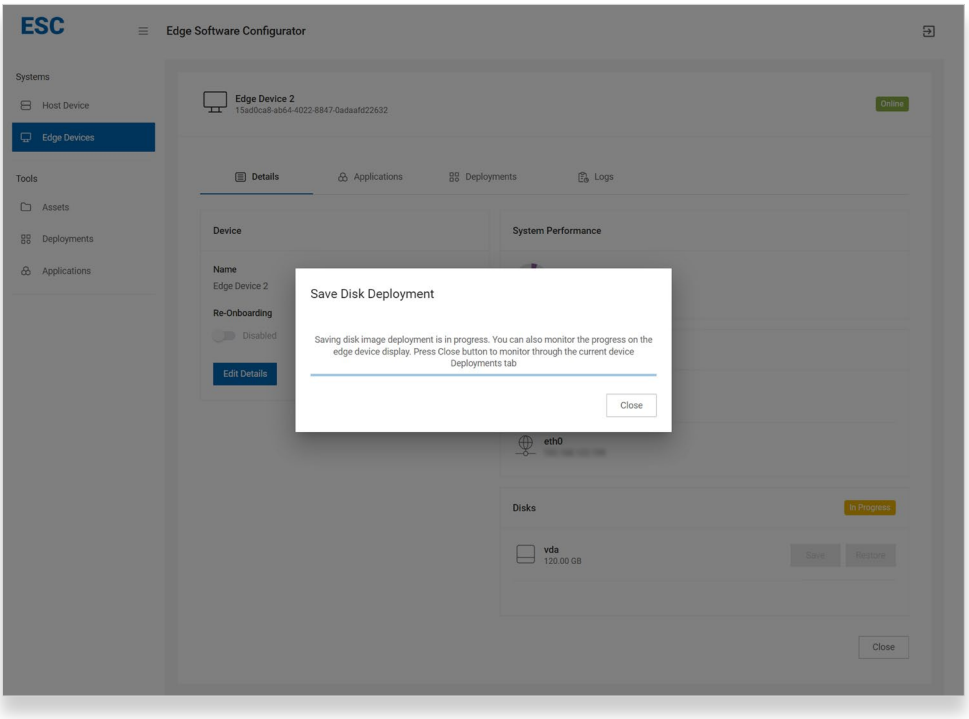


Note: Make sure you have sufficient disk storage on the host device before proceeding with the save disk image option. Insufficient disk storage will cause your host device to malfunction.

4. Click the Deploy button to save the disk image. You should be able to monitor the progress on the device display as well.

5. You can close the progress menu and monitor from the **Device** deployment tab if needed.

Figure 19. Disk Deployment Progress Status

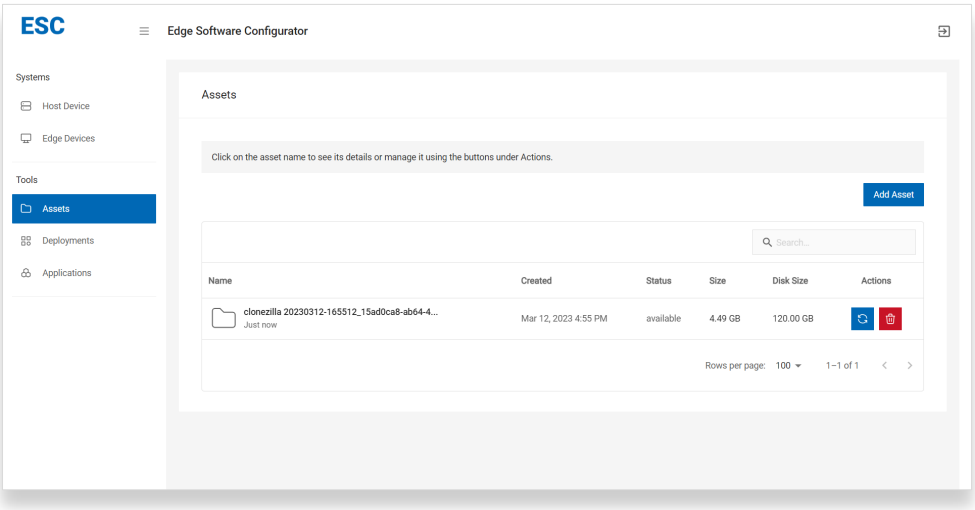


Note: Re-onboarding option should be enabled before proceeding with the next steps. Refer to this Re-onboarding section if it is not yet enabled.

8. Once the deployment is completed, you can proceed to boot back to your previously installed OS state.

9. Go to **Assets** under the **Tools** tab to check the save disk image asset created from the previous deployment. The image should be in the Available state if it is saved successfully.

Figure 20. Save Disk Image Asset

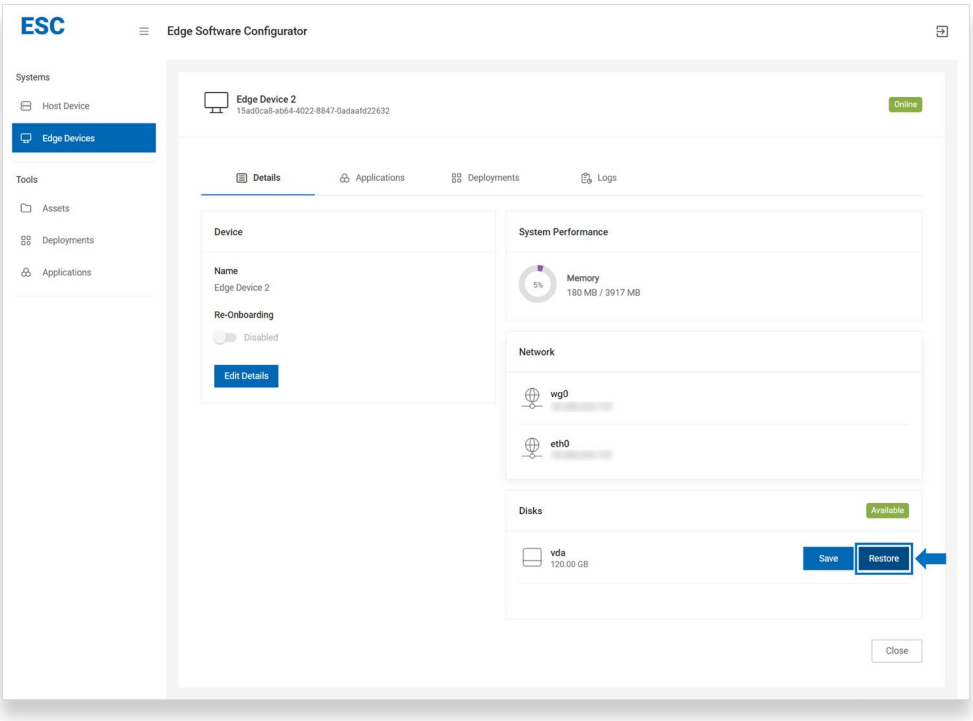


3.1.3.2 Restore Disk Images

Note: This section is only applicable when the user is booted with a configurator live image. Go to the Bare Metal section to enable this feature.

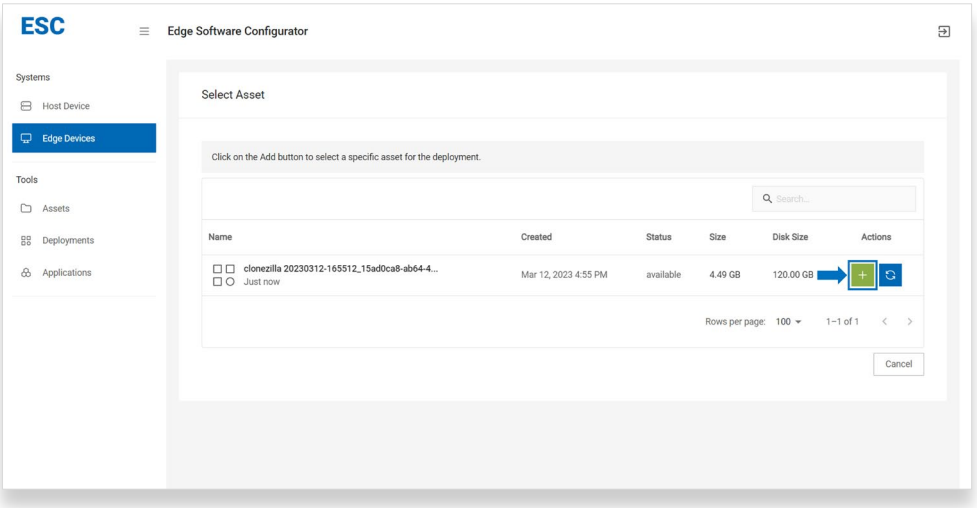
1. Go to **Edge Devices** under the **Systems** tab and click the specific device name to see the device details.
2. Click the **Restore** button for the specific device disk to proceed with the new disk image asset restoration.

Figure 21. Restore Disk Image Asset



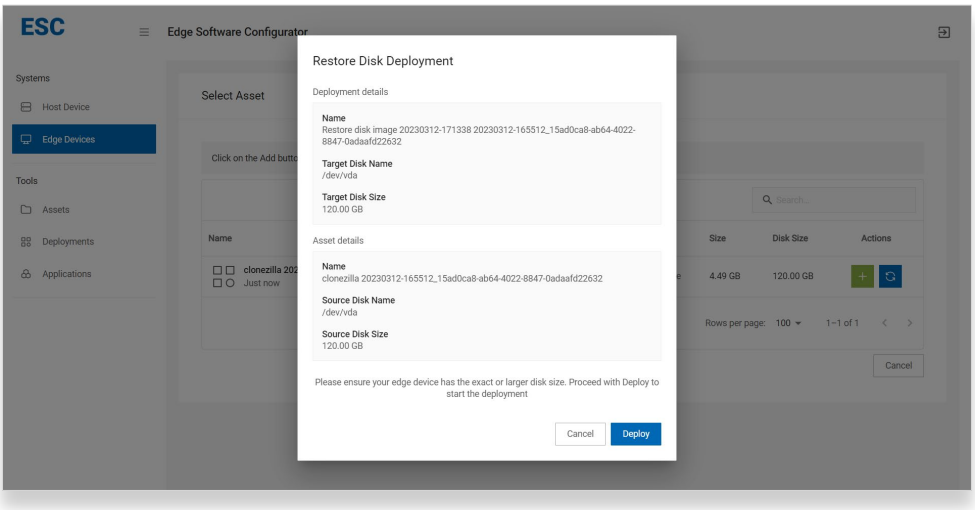
3. Select image asset.

Figure 22. Select Image Asset



4. Review the source disk and target disk detail instances.

Figure 23. Review Disk Details

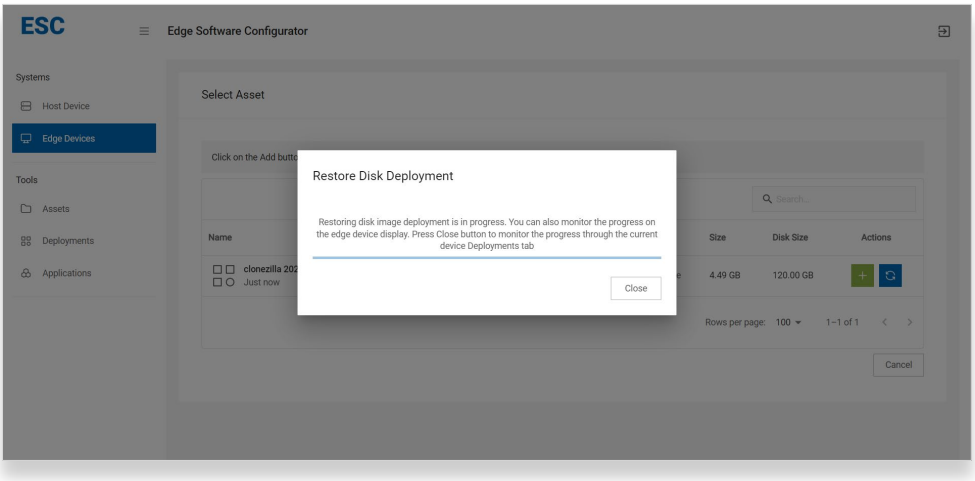


Note: Make sure you have sufficient disk storage on the edge device before restoring the disk image. Your edge device should have the exact size or larger than the current asset source disk size.

5. Click the **Deploy** button to restore the disk image. You should be able to monitor the progress on the device display as well.

6. You can close the progress menu and monitor from the **Device** deployment tab if needed.

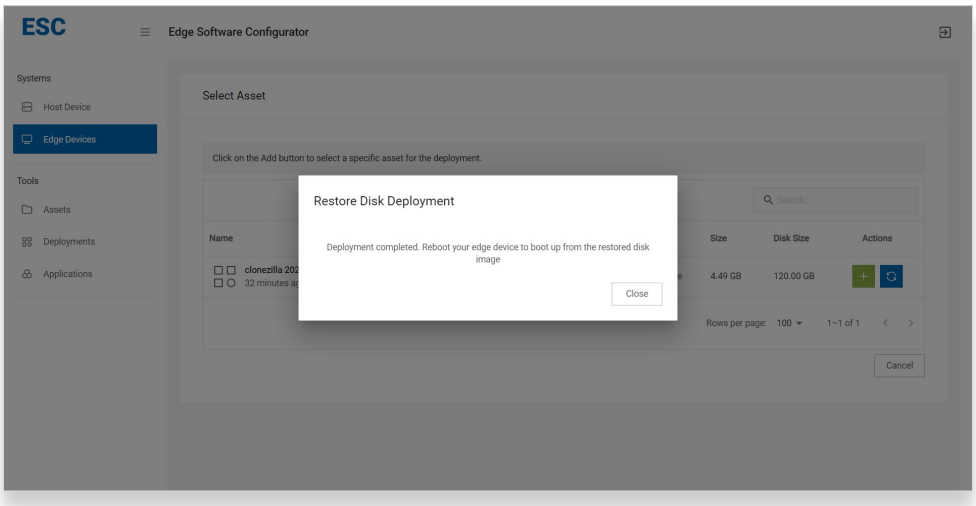
Figure 24. Restore Disk Deployment



Note: Re-onboarding option should be enabled before proceeding with the next steps. Refer to this Re-onboarding section if it not yet enabled.

6. Once the deployment is completed, you can proceed to restart and boot up from the restored disk.

Figure 25. Reboot Edge Device



3.1.4 Virtual Machines

Virtual machines or virtual hosts are the feature that help users to set up an isolated/virtualized computer system. This can help the user to run multiple applications together, monolithic applications, isolation between applications, and for legacy apps running on older operating systems.

Note: Make sure you have sufficient RAM and disk storage before proceeding with the virtual machine installation. A template to set up the virtual machine is provided. If

you do not have the sufficient hardware requirement to set up the virtual machine, it is recommended to adjust the requirement in the template based on your workload requirement.

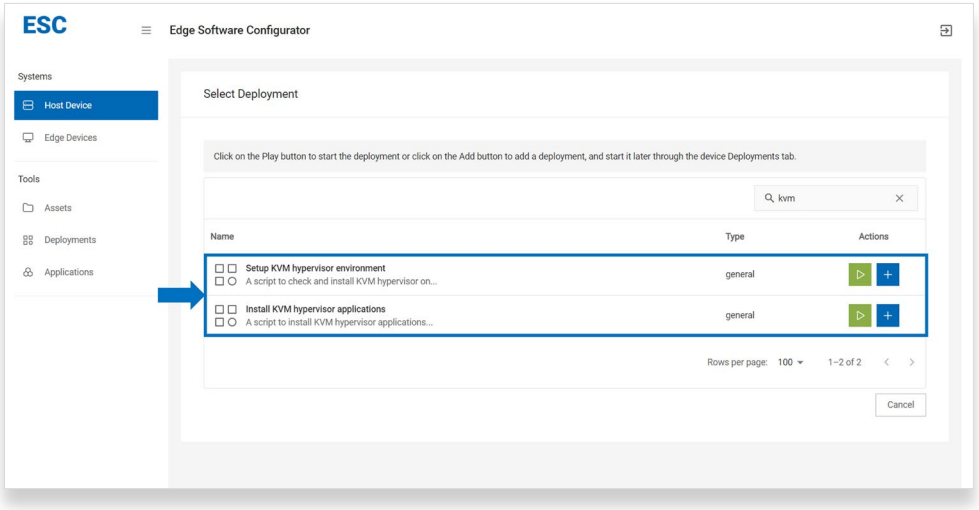
3.1.4.1 Set up KVM Environment

To install the virtual machine in the Host device, the KVM hypervisor environment and applications are required to be installed in the Host device. Refer to the Deployment section to add a deployment in the Host device.

Below are the steps required to proceed with this feature.

1. Go to **Systems** tab and click on the **Host Device** to enter the device **Deployments** list tab
2. Click the **Add Deployment** button. You can filter out the KVM only deployment task by searching for KVM on the search section.

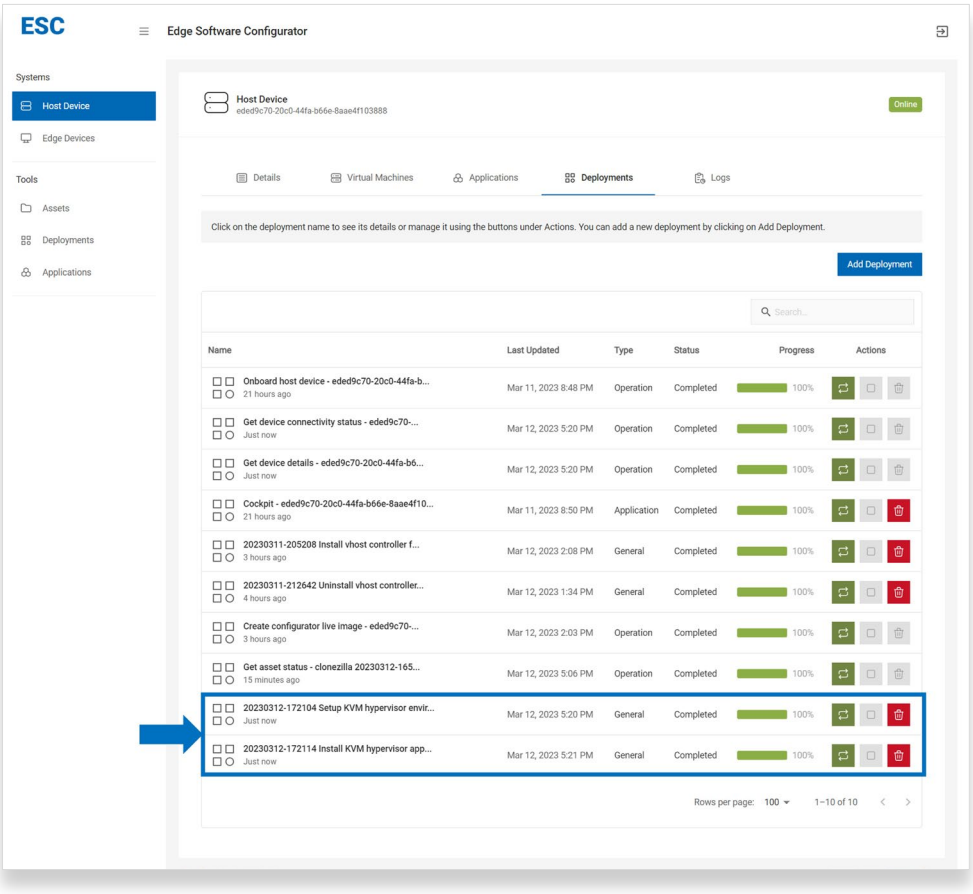
Figure 26. Install/ Set up KVM Hypervisor Environment



Note: Executing in the wrong order will lead to a KVM hypervisor setup failure.

3. Add the tasks and execute in the following order:
    a. Set up the KVM hypervisor environment.
    b. Install KVM hypervisor application deployment.
4. The KVM hypervisor is set up successfully after both deployments have been executed successfully.

Figure 27. Successful KVM Setup



3.1.4.2 Install Virtual Machine in Host Device

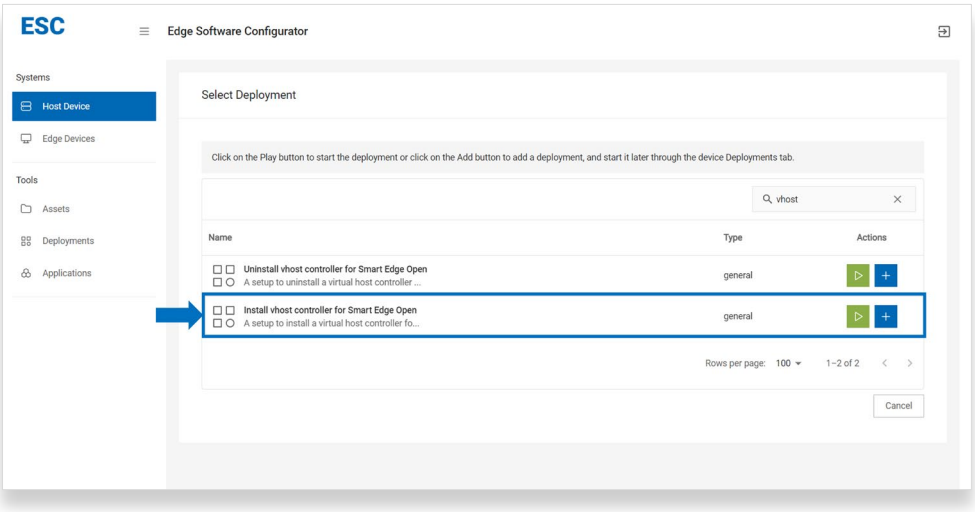
A sample virtual machine deployment is provided. The sample is for setting up a virtual machine and for the Intel® Smart Edge Open Enablement.

Note: Uninstall Virtual Machine in Host Device is a **required** step if your host device already installed or enabled with a virtual machine.

The steps below are required to proceed with this feature.

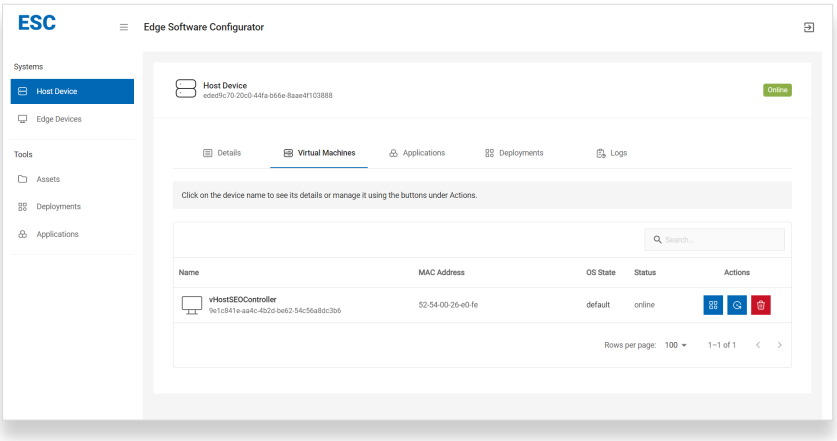
1. Add **Install vhost controller for Intel® Smart Edge Open** deployment in the Host device.

Figure 28. Install vhost Controller for Intel® Smart Edge Open



2. Run the deployment and wait for the deployment to complete.
3. Once the deployment is complete, navigate to the Virtual Machines to view, authorize, manage, and add deployment in the Virtual Machines tab.

Figure 29. Navigate to Virtual Machines



3.1.4.3 Accessing Virtual Machine in the Host Device via Virsh Console

The virtual machine for Intel® Smart Edge Open Enablement is assigned with the same IP address subnet with the host device via Linux* bridge br0. To retrieve the IP address or access the virtual machine directly, you can proceed with steps below.

1. From the host device terminal, run the command below to access the virtual machine console.

```
virsh console vHostSEOController
```

Note: The default username is **user.** The default password is the same web UI password that you used to configure during the setup. You should change the default password and create a new user account as required.

2. Log in and execute the required commands.

```
[redacted]:~$ virsh console vHostSEOController
Connected to domain vHostSEOController
Escape character is ^]

ubuntu login: user
Password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-132-generic x86_64)
```

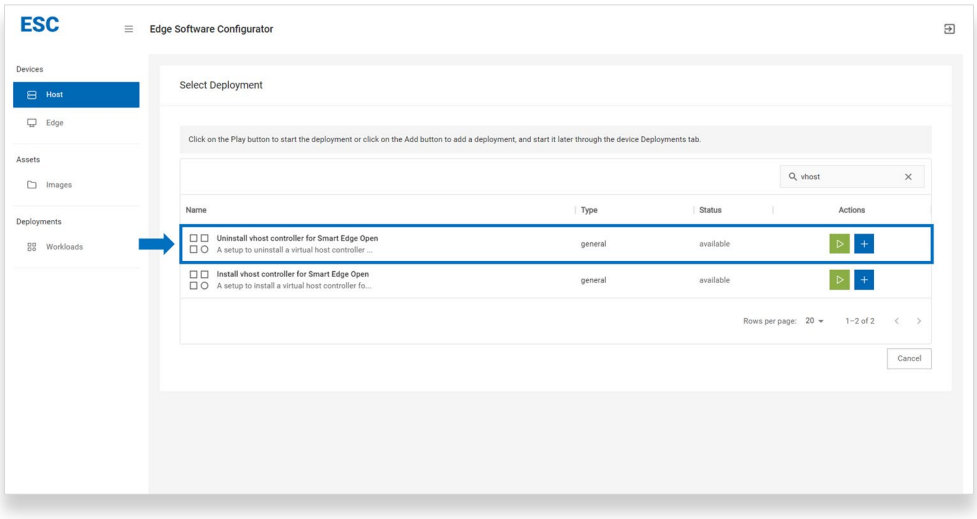
3.1.4.4 Uninstall Virtual Machine in the Host Device

The virtual machine can be uninstalled using the sample uninstall deployment.

Below are the steps required to proceed with the uninstallation.

3. Add the **Uninstall vhost controller for Intel® Smart Edge Open** deployment in the Host device.

Figure 30. Uninstall vhost Controller for Intel® Smart Edge Open



4. Run the deployment and wait for the deployment to complete.

5. Once the deployment is complete, navigate to the **Virtual Machines** tab to verify that the virtual machine is removed.

3.1.5 Device Deployment

Deployment consists of a series of playbook files to carry out a series of tasks. This section is applicable for both the host device and edge devices depending on your current device view.

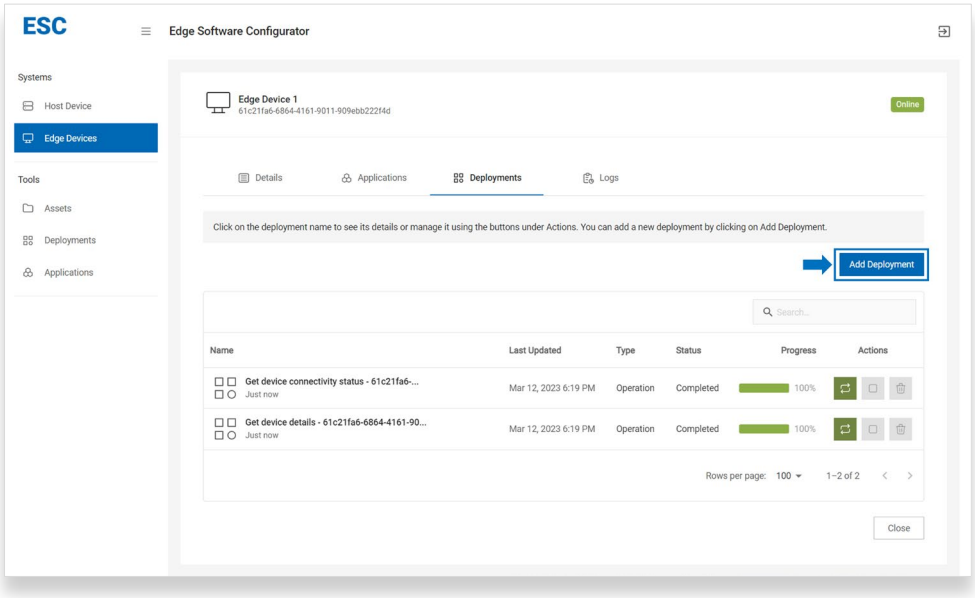
Note: Currently, only single workload deployment is allowed to be deployed at once on each device.

3.1.5.1 Add New Deployment

This section guides the user to edit the deployment before starting the execution.

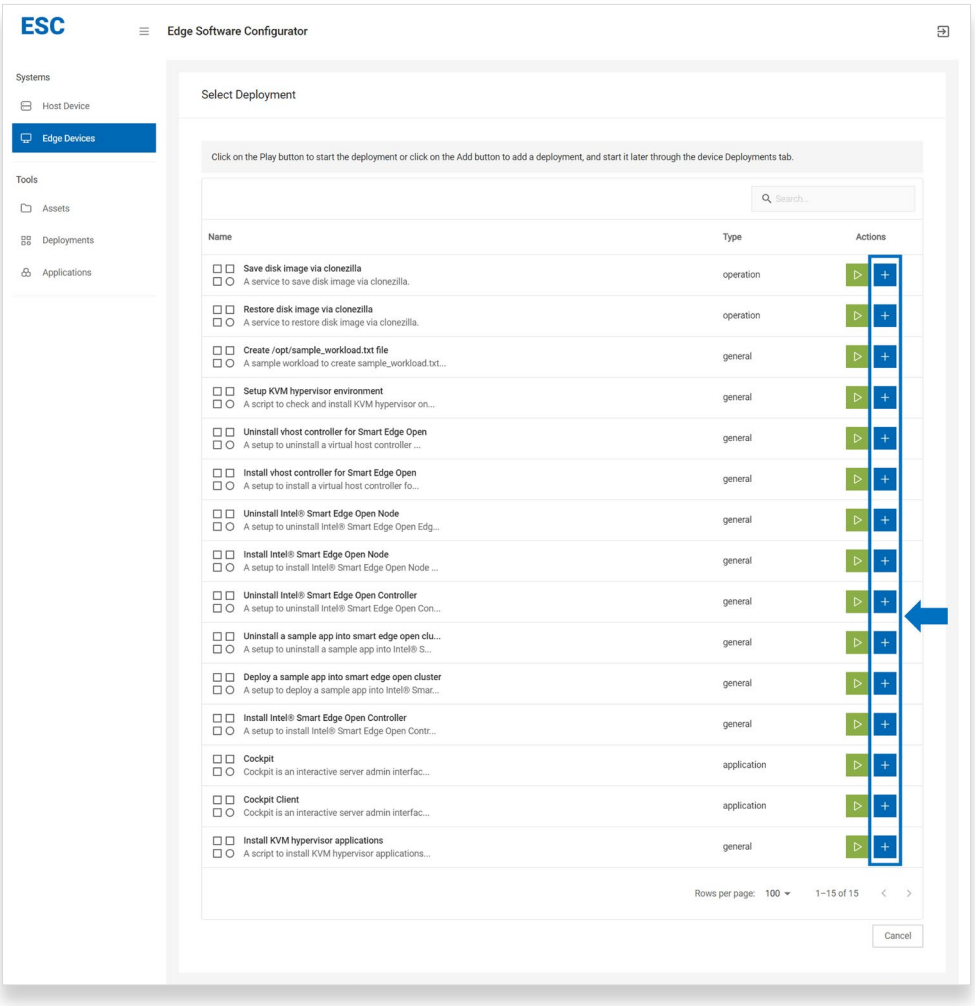
1. Click **Add Deployment** from the device deployment tab.

Figure 31. Add Deployment



2. Click the **Add** button from the Action column.

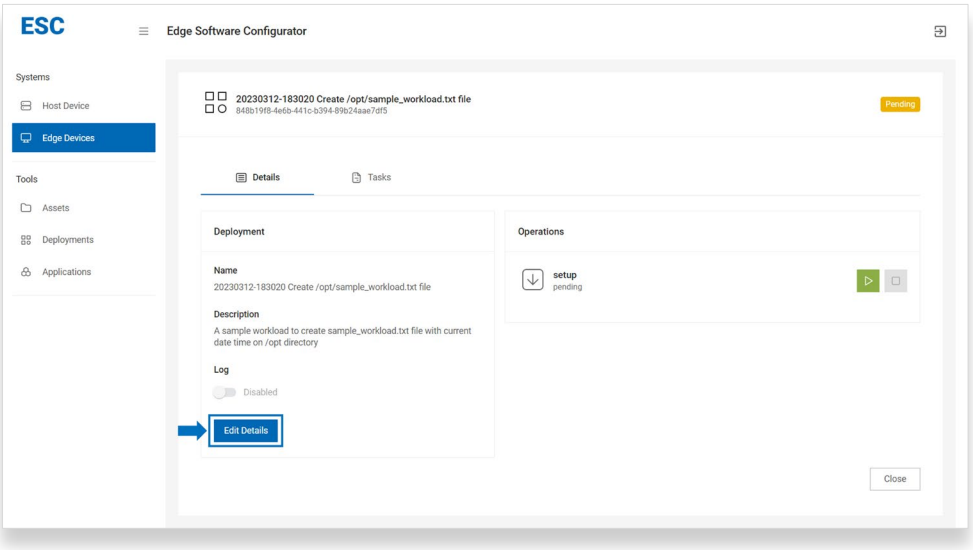
Figure 32. Add the Selected Deployment



3. From the Deployment tab, click on the name of the intended deployment.

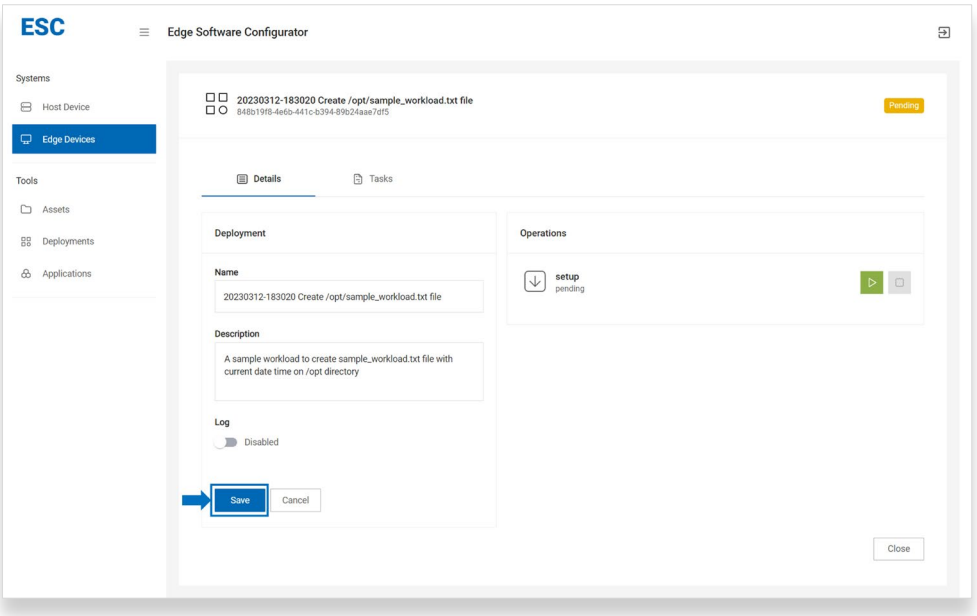
4. From deployment details, click the **Edit Details** button to edit the deployment details, and click Save to save the modifications. The editable details include the name and description of the deployment, and the option to enable Logging.

Figure 33. Edit Deployment Details



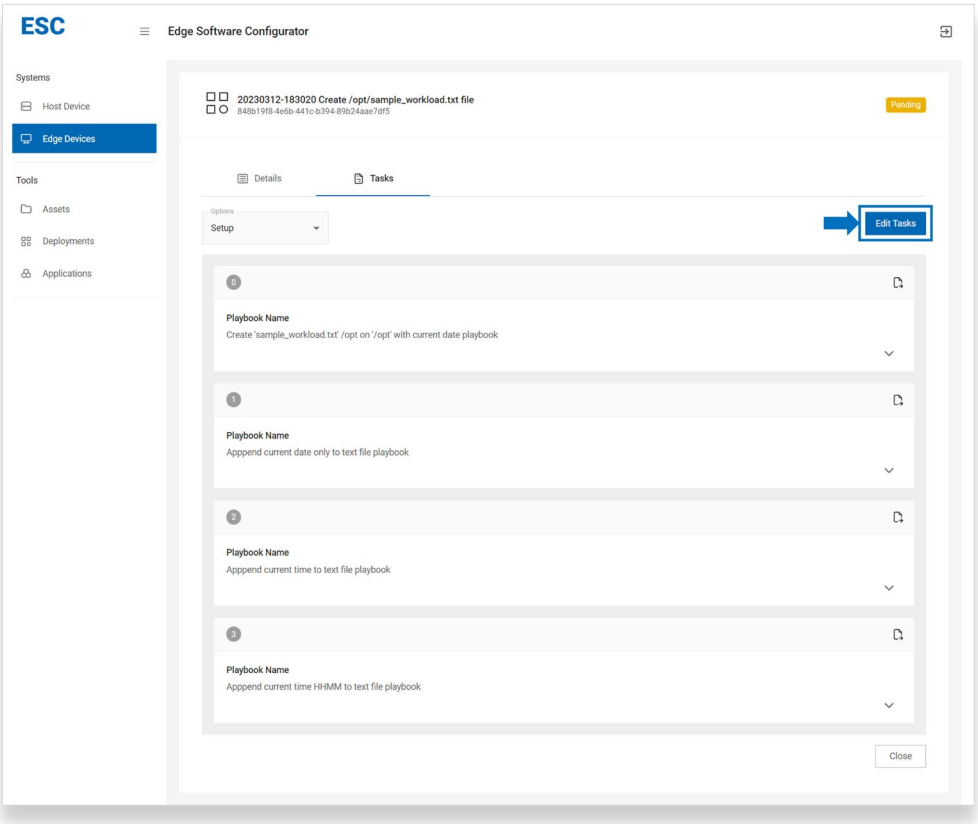
5. Once the required modifications are done, click **Save** to apply the changes.

Figure 34. Save Deployment Changes



6. From device **Deployment Tasks** tab, click **Edit Tasks** to edit the task order or the contents of the playbook files.

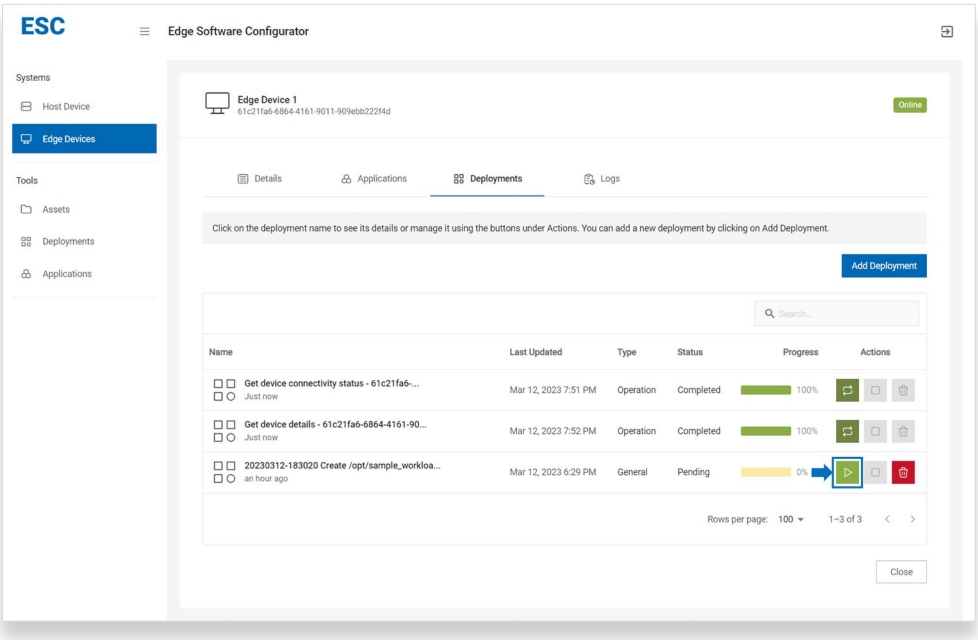
Figure 35. Edit Deployment Tasks



7. Save the changes and close the tab to return to the Device Deployments tab.

8. Click the **Start** button from the Action column to start the execution.

Figure 36. Start the Deployment



9. After the deployment has started, you can monitor the progress from the current Device Deployment tab.

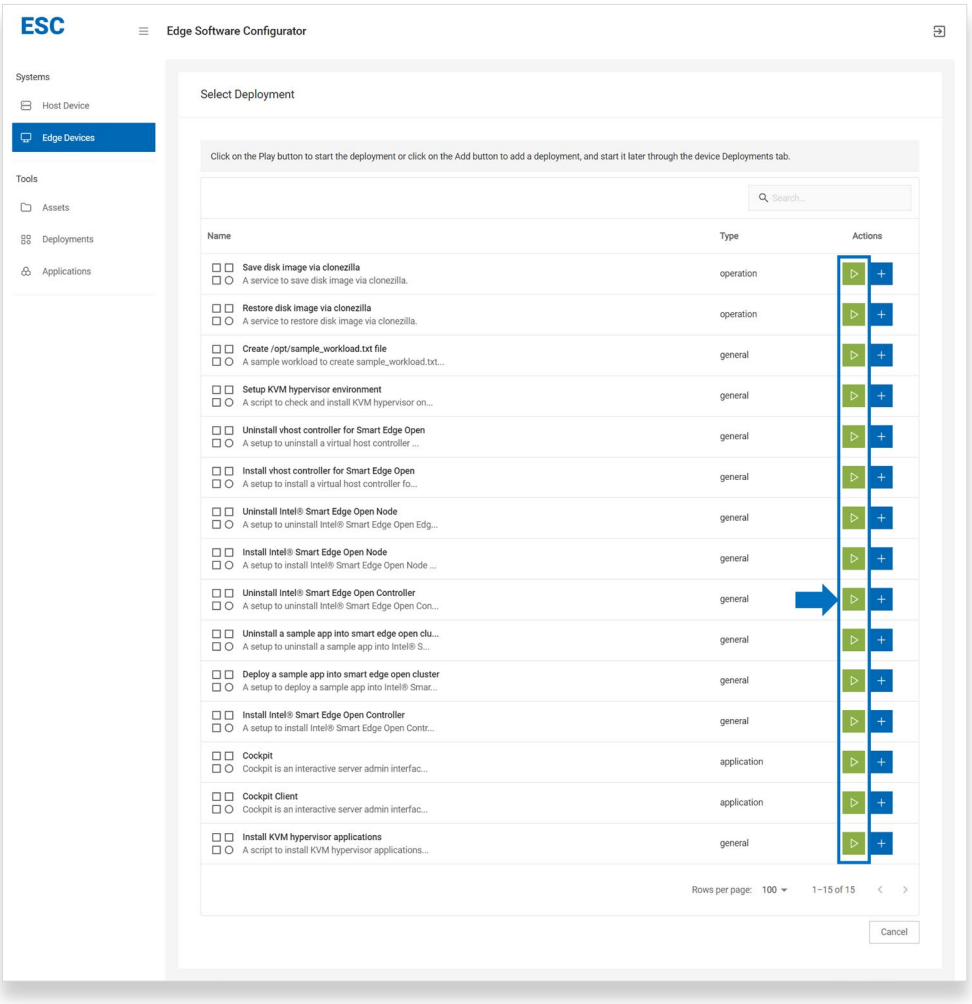
3.1.5.2 Start New Deployment

This section guides users to execute deployments directly without any modifications.

Below are the steps required to proceed with this feature.

1. Click **Add Deployment** from the device deployment tab.
2. Click the Start button from the Action column to start the execution.

Figure 37. Start the Selected Deployment Execution



3. After the deployment has started, you can monitor the progress from the current Device Deployment tab.

3.1.6 Logs

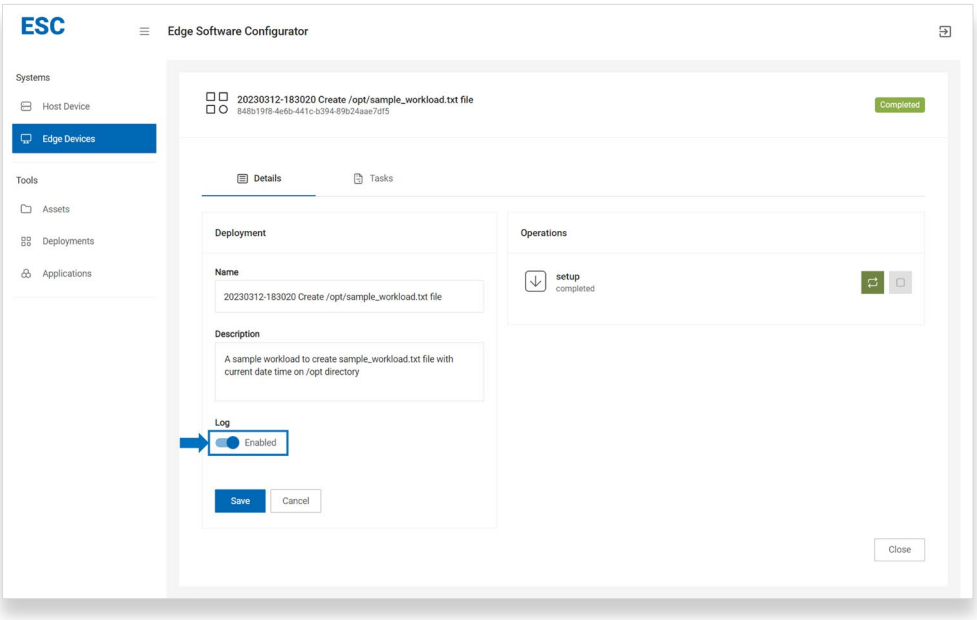
This section guides users to view specific deployment logs if enabled.

Note: All deployments logs are disabled by default. Do not enable it if it is not needed as it would create lengthy logs if the deployment was automatically executed. The user should manage and delete the log manually if it is not required anymore.

Below are the steps required to proceed with this feature.

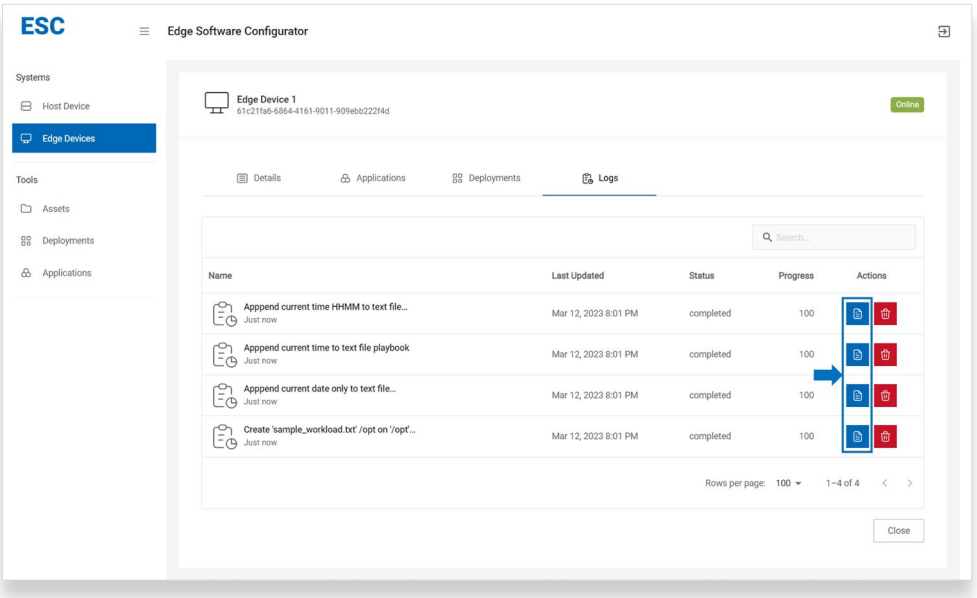
1. Go to the specific deployment details.
2. Click **Edit Details** to toggle the Log as Enable and click Save.

Figure 38. Enable Deployment Log



3. Start or restart the deployment to enable the log output.
4. After the deployment has completed or failed, go to the Device Logs tab to see the log details.

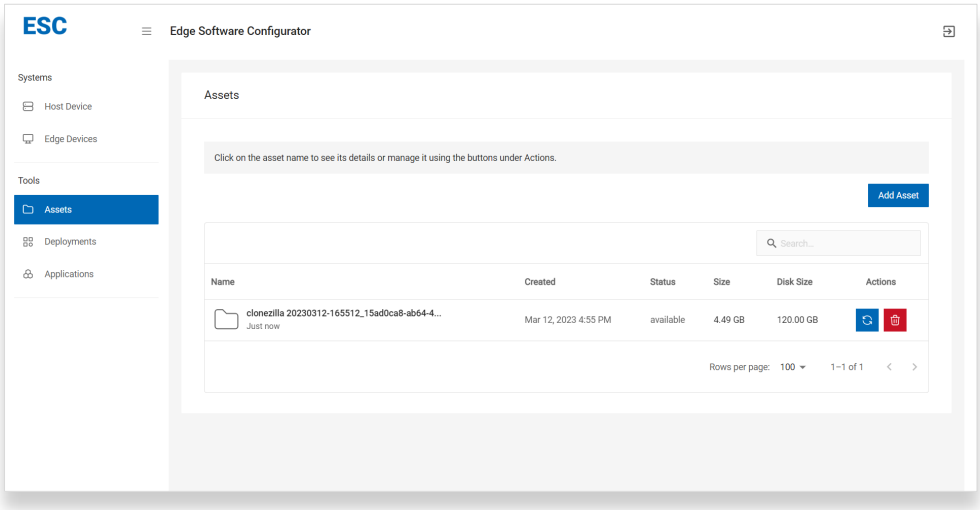
Figure 39. View Deployment Log Details



3.2 Assets

An asset consists of images saved using the live OS. The images can be restored to other devices once saved.

Figure 40. View Assets

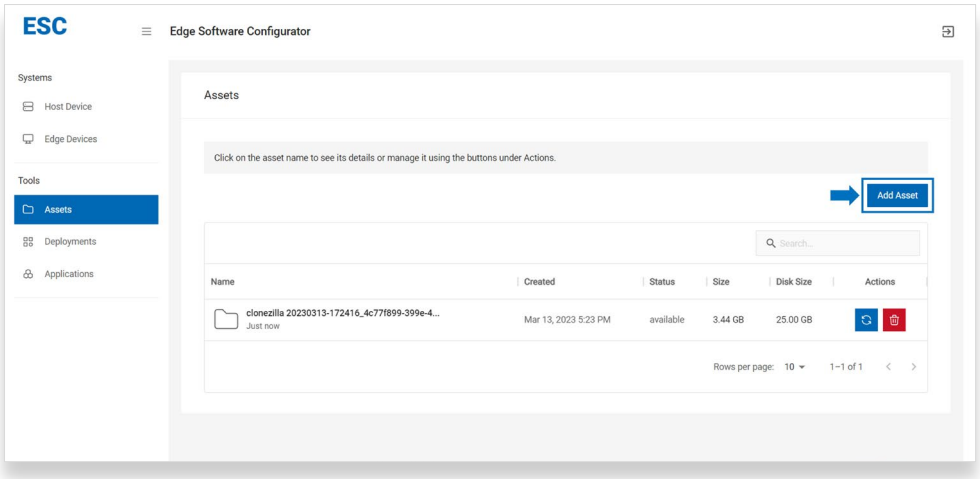


3.2.1 Create New Asset

Note: Currently, if an asset is an image, it will automatically be created when users trigger the save disk image deployment. Alternatively, user also can import any existing Clonezilla* saved disk image folder as a new instance.

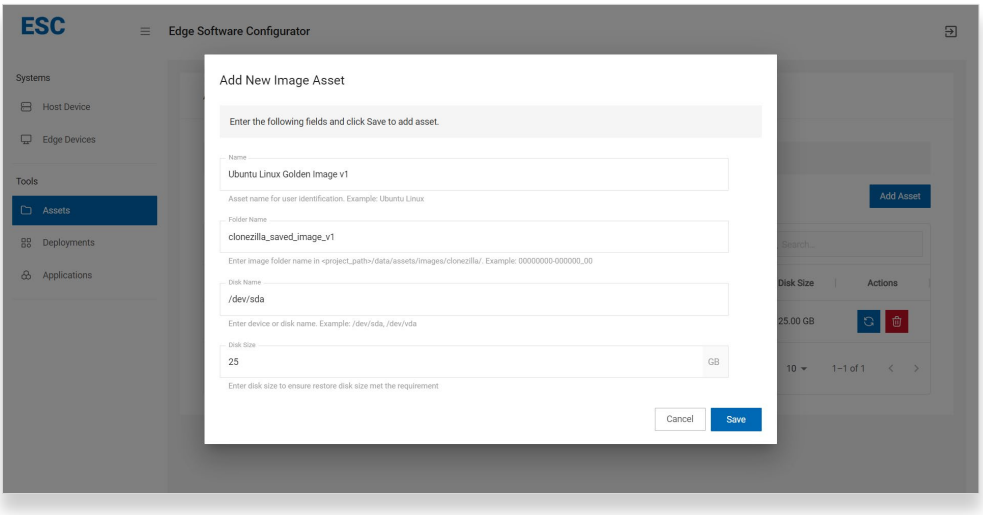
1. Go to **Assets** under the **Tools** tab, and click the **Add Asset** button.

Figure 41. Add Asset



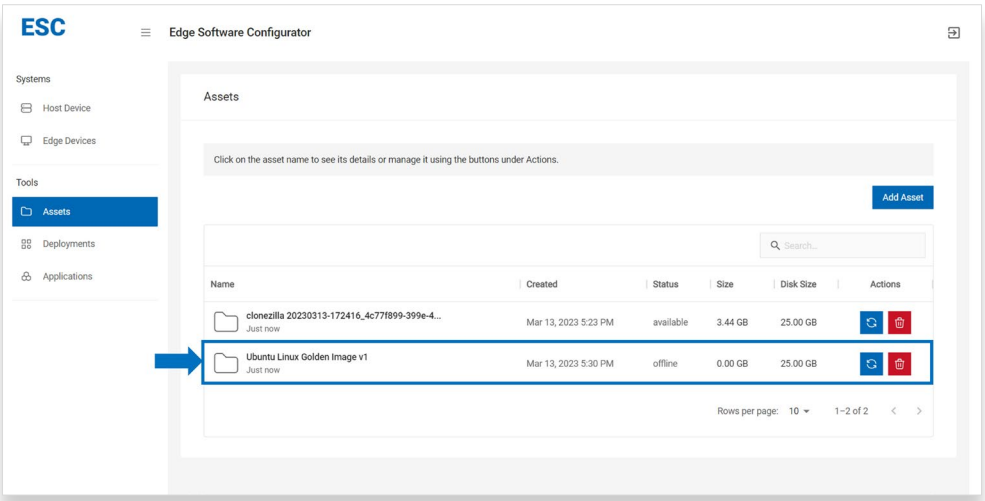
2. Enter the name, folder name, disk name and disk size of the asset into the corresponding input fields. Click **Save** when you are ready.

Figure 42. Enter Asset Details



3. The new asset will now be listed under the **Tools Assets** tab.

Figure 43. Asset Created



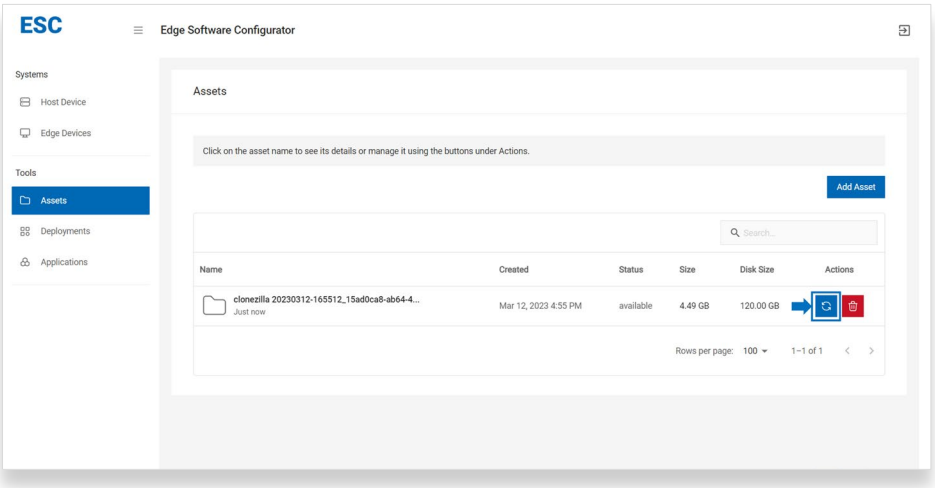
4. By default, newly created asset status will be offline. Refer to section Status to update the latest status.

3.2.2 Status

Note: The status will be checked remotely via the ansible playbook deployment from the host device to any connected edge device. Thus, it will take a few seconds for this deployment service to complete.

1. Go to **Assets** under the **Tools** tab, and click the Update Status icon from the Actions column.

Figure 44. Update Asset Status



2. Verify the latest status depending on your current image state.

    i. Creating: The asset is being created by the save image process.

    ii. Available: The asset has been created and can be restored to other devices.

    iii. Unavailable: The asset is not ready or is unusable.

3.2.3 Delete Asset

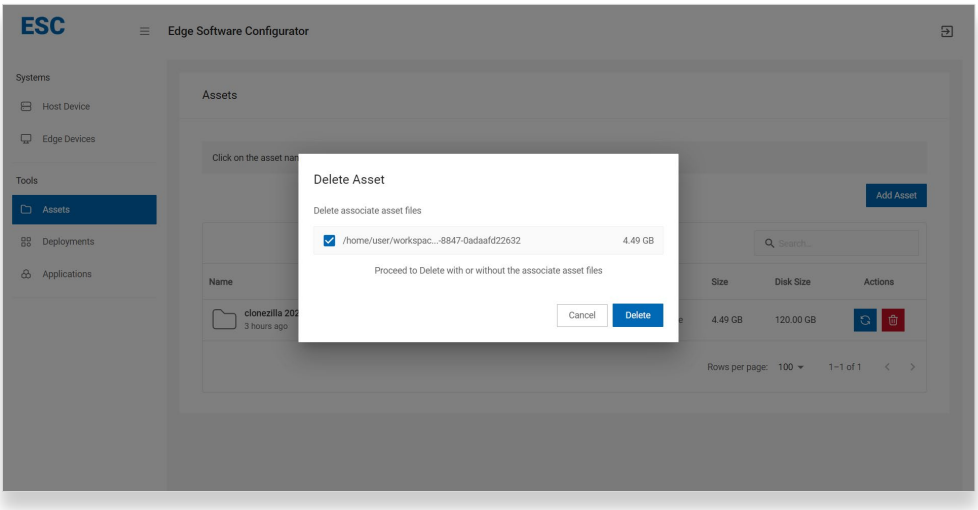
Note: Assets that are in the image type are created with associate files. Thus, when deleting the asset instance, you are required to check the associated files as well to avoid full disk storage. Otherwise, you can delete them manually via the shown path on the host system.

1. Check the current asset status as shown in the Status section before proceeding with the Delete action.

2. Go to Images under the Assets tab, and click the Update Status icon from the Actions column.

3. Check the associate file if the files exist, and click delete to proceed.

Figure 45. Delete Asset

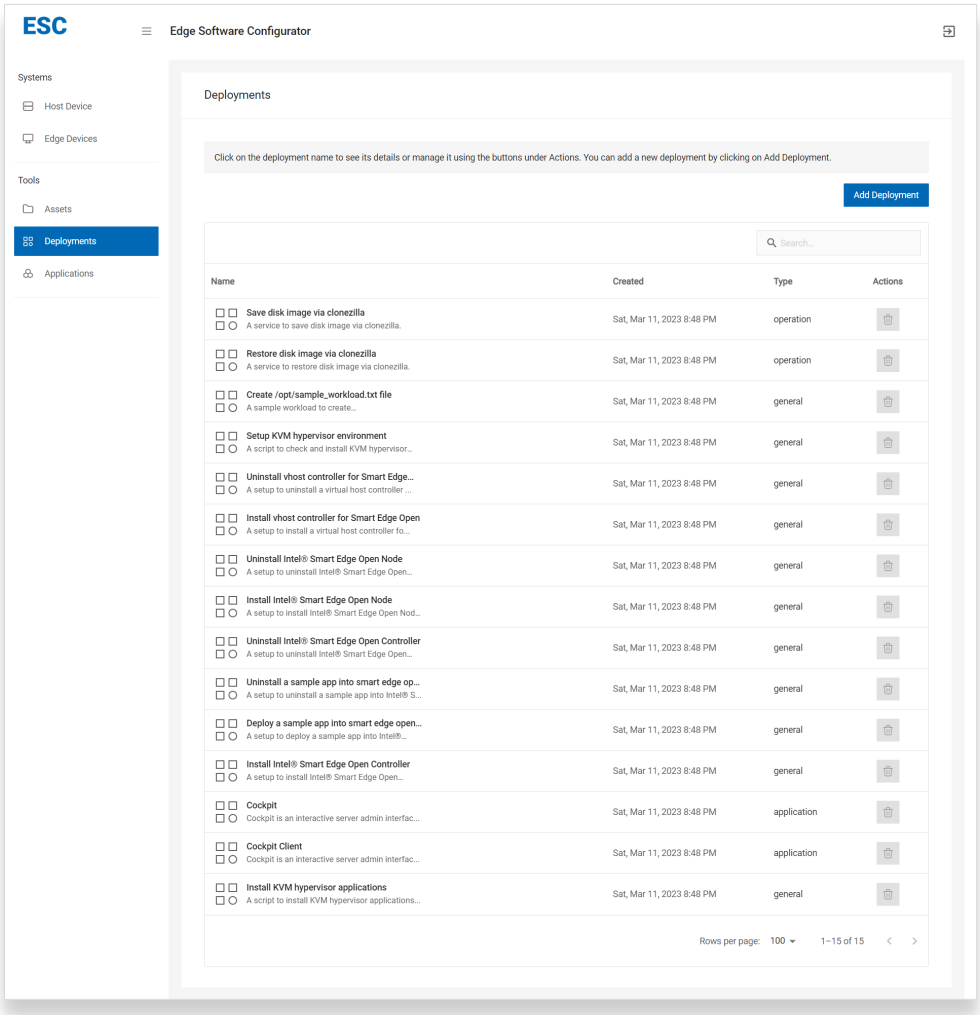


3.3 Deployments

Deployment consists of a series of playbook files to carry out a series of tasks. All available deployments are listed under the **Tools Deployments** tab.

Note: The default deployments cannot be deleted (only edited).

Figure 46. View Workloads

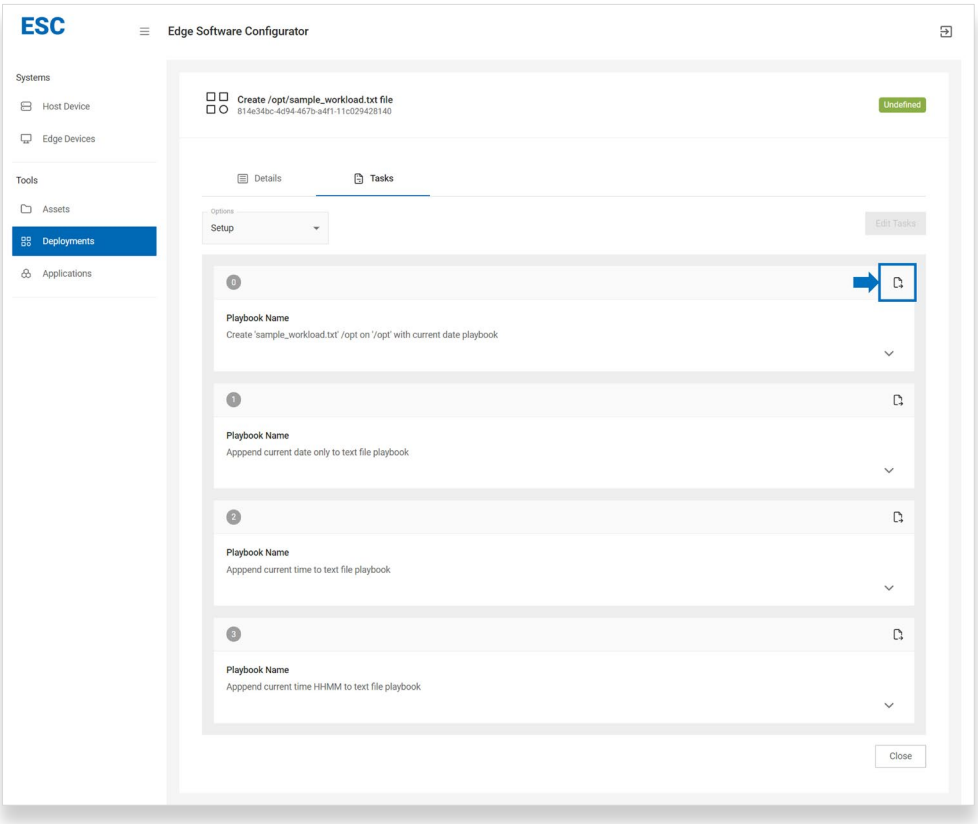


3.3.1 Export Playbook File

By default, all deployment playbook files can be exported as YAML files.

1. Click the name of the intended deployment.
2. Go to **Tasks** tab or click on the **View All** button under Tasks.
3. Click the button on the top right of the playbook to download the YAML file.

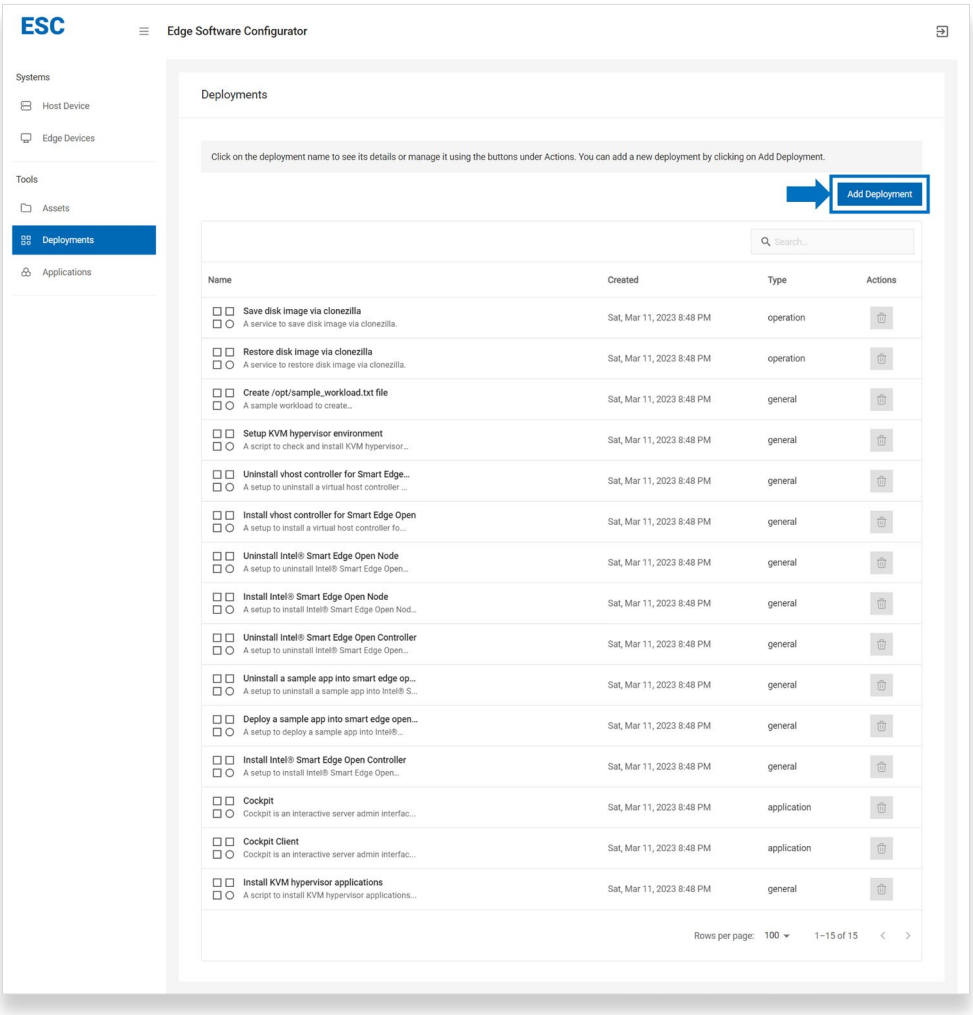
Figure 47. Export Playbook File



3.3.2 Create New Deployment

1. Navigate to the **Tools Deployments** tab, and click **Add Deployment**.

Figure 48. Add Deployment



2. Enter the name and description of the deployment into the corresponding input fields. Click **Next** when you are ready.

3. Upload the playbook files that need to be executed. The playbook files should be in YAML format. Click **Next** when you are ready.

4. Review the deployment details and the playbook files. Click **Finish** when you are ready. The new deployment will now be listed under the **Tools Deployment** tab.

4.0 Use Cases

4.1 Golden Image Deployment

ESC provides the utility to save a golden image and to deploy a golden image to multiple devices in quick succession.

4.1.1 Requirements

- Basic understanding of the functions of ESC

4.1.2 Steps

Below are the steps required to proceed with this feature.

1. Onboard the device with the golden image by following Bare Metal onboarding.
2. Save the image by following Save Disk Image.
3. Onboard the target device by following Bare Metal onboarding.
4. Restore the image to the target devices by following Restore Disk Image.

4.2 Intel® Smart Edge Open Enablement

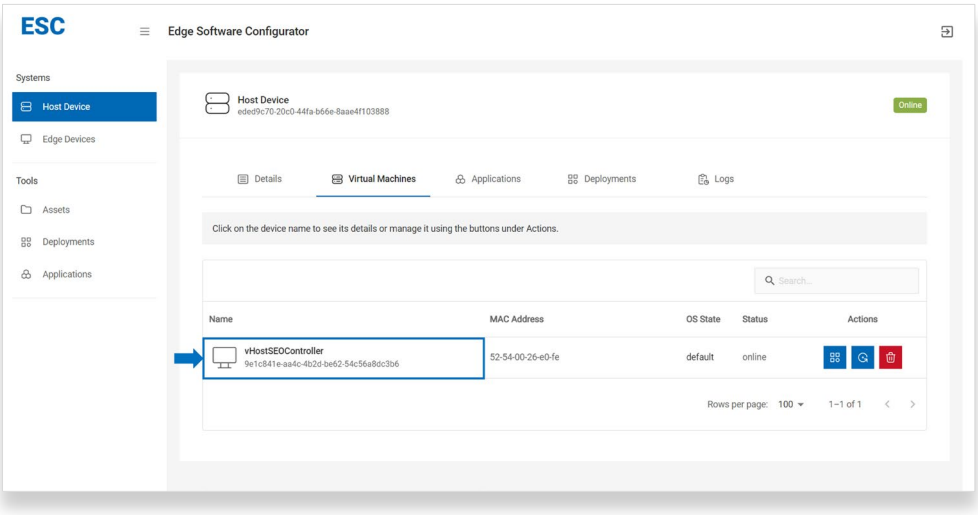
4.2.1 Install Intel® Smart Edge Open Controller Node

This section guides users to install Intel® Smart Edge Open Controller node in the virtual machine setup on ESC host device.

Below are the steps required to proceed with this feature.

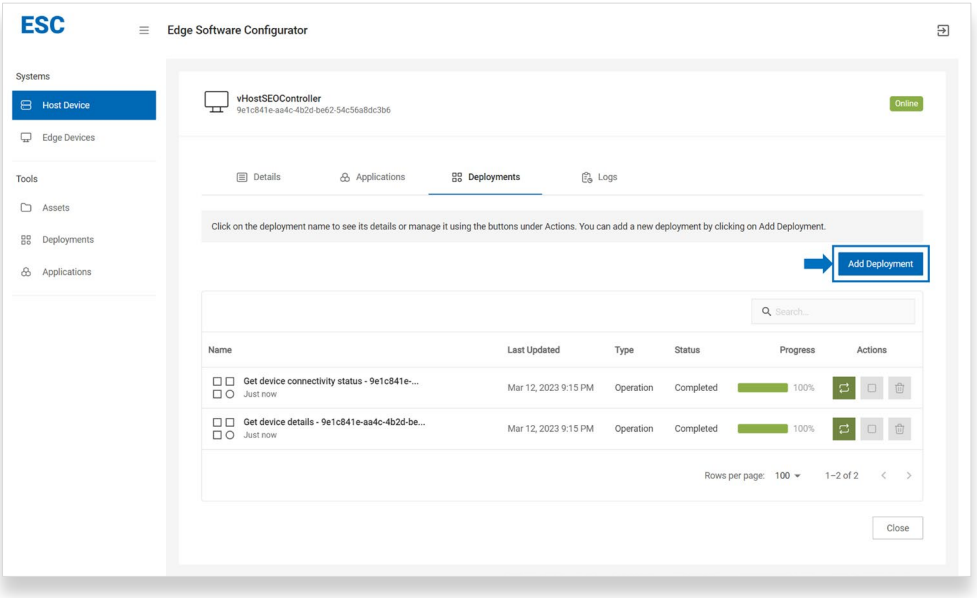
1. Create and navigate to the Virtual Machines tab by following the Virtual Machines section. Click the virtual machine device name to access the device details.

Figure 49. Go to Virtual Machine



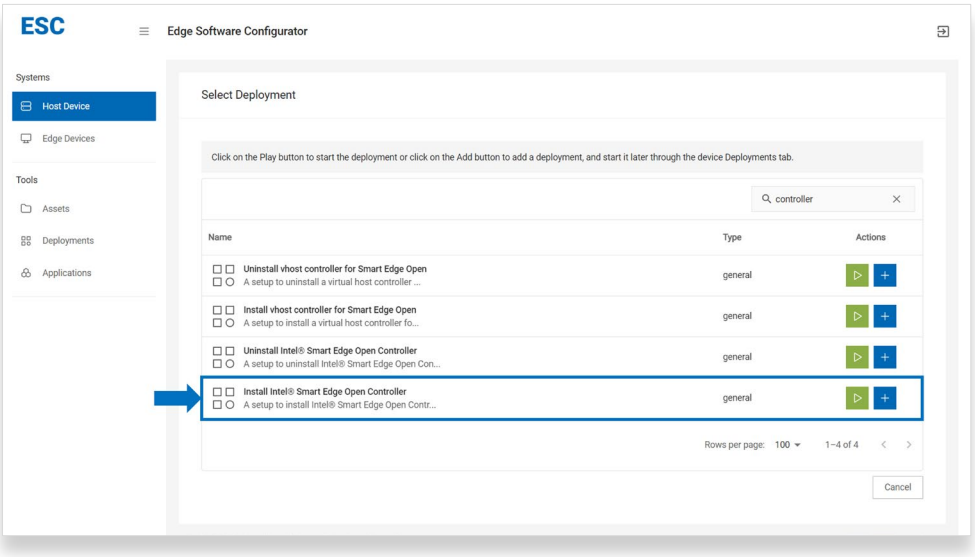
2. Navigate to virtual machine device's **Deployments** tab, and click **Add Deployment**.

Figure 50. Add Deployment



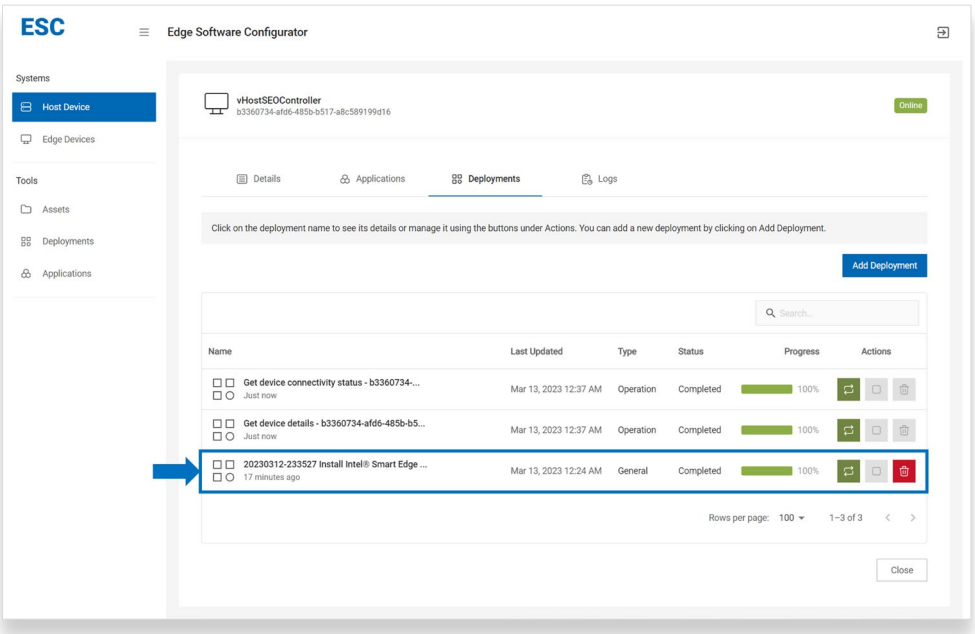
3. Add **Install Intel® Smart Edge Open Controller** deployment on the specific virtual machine device. Refer to the Deployment section if you are not sure on how to add a deployment.

Figure 51. Install Intel® Smart Edge Open Controller



4. The Intel® Smart Edge Open Controller Node is successfully set up when the deployment runs successfully.

Figure 52. Successful Setup



Note: If the virtual machine device is offline after the deployment installation has been completed or failed, refer to section Onboarded Virtual Machine Is Offline for further troubleshooting.

5. To access the Intel® Smart Edge Open Controller Node, refer to the Accessing Virtual Machine in Host Device via Virsh Console section.

Note: Command in virtual machine terminal should run with sudo.

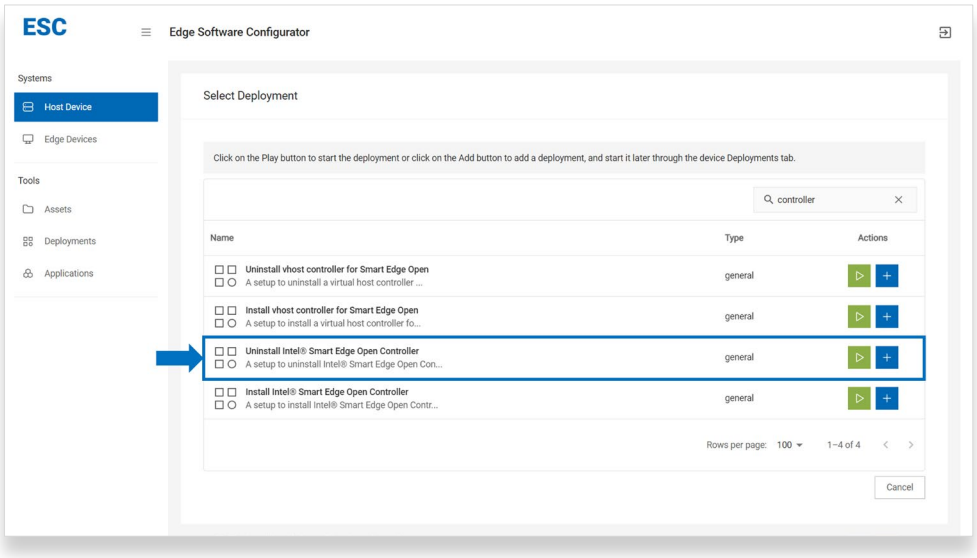
4.2.2 Uninstall Intel® Smart Edge Open Controller Node

This section guides users to uninstall the Intel® Smart Edge Open Controller node in the virtual machine setup on ESC host device.

Below are the steps required to proceed with this feature.

1. Add Uninstall Intel® Smart Edge Open Controller Node deployment. Refer to the Deployment section if you are not sure on how to add a deployment.

Figure 53. Add Uninstall Intel® Smart Edge Open Controller Node deployment



2. The Intel® Smart Edge Open Controller Node is successfully uninstalled when the deployment runs successfully.

5.0 Troubleshooting

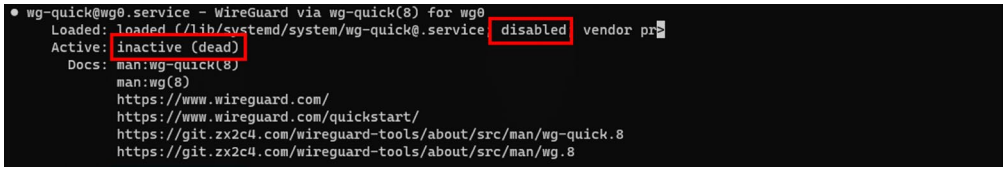
5.1 General

Below are the general troubleshooting guides.

5.1.1 Onboarded Virtual Machine is Offline

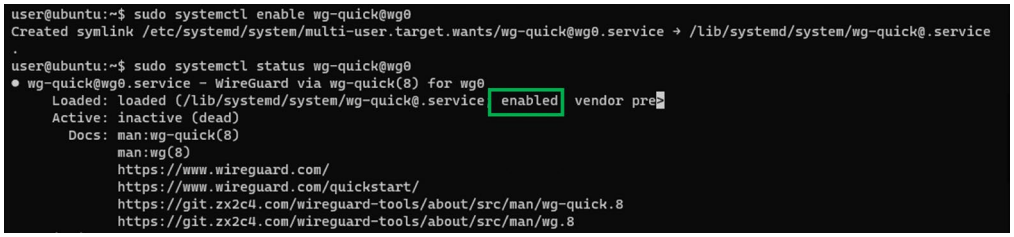
1. Access the virtual host by following the Accessing Virtual Host in Host Device via Virsh Console section.
2. Verify the current WireGuard* service status through the command below.

```
sudo systemctl status wg-quick@wg0
```



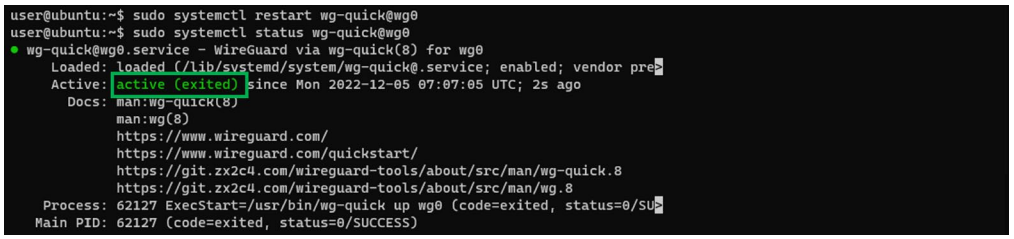
3. If WireGuard* service is disabled, enable it back through the command below.

```
sudo systemctl enable wg-quick@wg0
```



4. If the WireGuard* service is inactive, restart through via the command below.

```
sudo systemctl restart wg-quick@wg0
```



§