SEC eDGE™
Digital Security to the Edge

SECeDGE STUDIO™

USER GUIDE

May 7, 2024 | Version 1.2

1. TABLE OF CONTENTS

2. SECeDGE STUDIO™ OVERVIEW

SecEdge Studio is a development and test environment for SecEdge's chip-to-cloud security solution, available on Google Marketplace. SecEdge studio accelerates the integration and deployment of the SecEdge Service Platform, which provides device-level security, zero-trust networking, and secure data control and management.

With SecEdge Studio, IoT and Edge solution developers can deploy their solutions in a cloud environment, connect backend applications, and emulate edge devices. More than 80% of an IoT security solution's development and test can be done in a virtual environment by a single software engineer. Overall, security development and test time can be reduced from months to weeks.

IPsec Chip to Cloud Tunnels are automatically set up through SecEdge platform, enabling the configuration/policy/KMS and dashboard management.

This guide provides an overview of SecEdge Studio™ and its capabilities. Concepts and functionality are explained through a sample deployment and its various scenarios. The guide also describes the SecEdge Studio User Interface where the user can manage and configure MicroEdge™ and CloudEdge™ device groups, devices and their connectivity. Please see the SecEdge Studio Getting Started Guide for steps to set up the product.

2.1. BENEFITS

+ Decouple the cloud application team dependency from end device hardware availability.
+ Accelerates migration from sandbox environment to real edge device hardware.
+ Test end-to-end the solution with the security capabilities offered by MicroEdge, CloudEdge and ControlEdge.
+ Turnkey solution for secure connectivity enabling compliance with security industry standards and guidelines.

2.2. SECeDGE SERVICE PLATFORM

The SecEdge service platform includes MicroEdge™, CloudEdge™ and ControlEdge™. SecEdge Studio facilitates end-to-end testing, quickly, by decoupling hardware dependency and deploying VMs. After the end-to-end test using VMs is completed, the solution can be further customized using hardware.

MicroEdge™ is a middleware component which provides zero-touch security provisioning, secure end-to-end data in motion and at rest for Internet of Things and Operational

Technology embedded devices with Variscite SOM modules. Implementation examples include vending machines, automotive modules, IoT gateways, set-top boxes, smart locks, perimeter security, and smart city infrastructure. A single MicroEdge instance on a device enables multi-tunnel connectivity to different CloudEdge servers enabling more secure services and/or new monetization options for the owners of the IoT/Edge devices.

The MicroEdge software is installed on devices equipped with Linux OS.

CloudEdge™ is the cloud termination endpoint for MicroEdge device tunnels. Endpoint devices can be anchored to one or more peer endpoints on an external network, but residing on the same administrative span of control as the MicroEdge endpoint. This peer endpoint is referred to as the CloudEdge. All external network flows will be securely tunneled to CloudEdge where the flows can be subjected to additional security analysis before being routed to their ultimate destination.

Customers deploy one instance of CloudEdge in their backend to connect securely all IoT/Edge devices to their backend application server.

ControlEdge™ administers all edges (IoT devices equipped with MicroEdge and CloudEdge) within the SecEdge ecosystem. ControlEdge performs all the heavy lifting functions to set, configure and manage the security of the entire deployment. All of this connectivity and provisioning is managed by ControlEdge services which allow for the deployment of IPsec tunnels facilitating secure communications between instances.

ControlEdge is available as a SecEdge managed service and is accessed by customers via simple APIs.

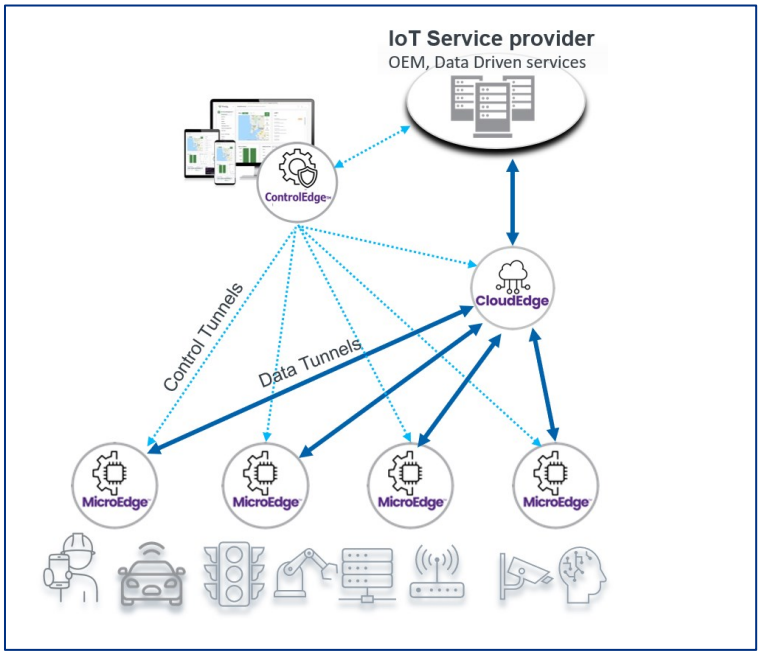

Figure 1 SecEdge Service Platform Architecture

2.3. SECeDGE STUDIO™ ARCHITECTURE

SecEdge Studio enables development and test end-to-end the SecEdge security solution in Google Cloud Platform (GCP) cloud environment without hardware. Shown in Figure 2, SecEdge Studio uses ControlEdge in GCP supported by SecEdge and deploys virtual machines (VMs) in the GCP customer's account.

ControlEdge in GCP

+ Orchestrates security services between MicroEdge (in VM1) and CloudEdge (in VM2).
+ User has full control to test end-to-end the various security features via SecEdge Studio dashboard.

VMs in Customer's GCP Account

+ VM1: Emulates Edge Device and its applications connectivity via an IPsec tunnel with MicroEdge.
+ One or more IPsec tunnel(s) can be implemented from the emulated device (in VM1) and tested easily (with one CloudEdge per tunnel).
+ VM2: CloudEdge receives encrypted data from the emulated device and delivers it to customer's backend application.

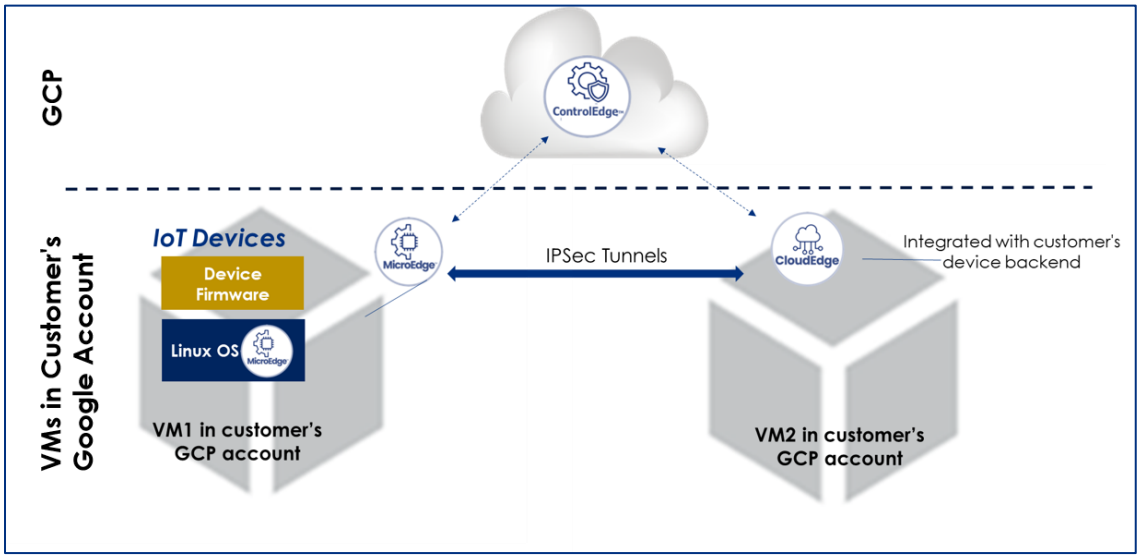

Figure 2 Architecture Overview

When customer uses the DEPLOY option in GCP, SecEdge Studio activates the CloudEdge and MicroEdge VMs and adds them to a default group. During activation the following credentials are used:

- Day0 Device, an IoT/Edge device which is known to SecEdge Studio but not authenticated yet.
- Day1 Device, an IoT/Edge device which is authenticated and verified by SecEdge Studio (ControlEdge).

During deployment the following processes take place:

1. Device setting:
   - OS and MicroEdge installation in MicroEdge VM.
   - OS and CloudEdge Installation in CloudEdge VM.
   - Day0 credentials pre-installed in both VMs.
2. When the MicroEdge and CloudEdge VMs are spawned, they register themselves with ControlEdge using Day0 credentials.
   - This step is automated for SecEdge Studio customers.
3. After MicroEdge and CloudEdge are successfully registered, they receive Day1 credentials and reconnect with ControlEdge as Day1 devices.
4. ControlEdge provisions the Day1 MicroEdge and CloudEdge with secure tunnel configurations so that the MicroEdge and CloudEdge establish a secure tunnel between them.

2.4. PREREQUISITES TO USE SECeDGE STUDIO™

The following are requirements to use the SecEdge Studio:

- Google account to access Google Cloud services.
- Login to Google Cloud Console, i.e. console.cloud.google.com.
- Familiarity with the following services in Google Cloud Console:
  - Compute Engine
  - VPC Network
  - Marketplace
- No hardware is required to use SecEdge Studio.

2.5. SAMPLE DEPLOYMENT

A sample deployment involving two service providers and various operational scenarios are used to explain capabilities of SecEdge Studio. The deployment is depicted in Figure 3:

+ **Alarm Management Systems** (**AMS**) wants to deploy and manage connected alarm devices in the building of its customers.
+ AMS also partners with 3rd party **Maintenance Co** (**MC**) whose staff services the alarm devices on site when needed.
+ **Maintenance Co** continuously monitors the alarm equipment remotely to ensure it operates normally.
+ Each alarm device is equipped with **MicroEdge**.
+ The devices communicate securely to **AMS Service** via **AMS_CloudEdge**.

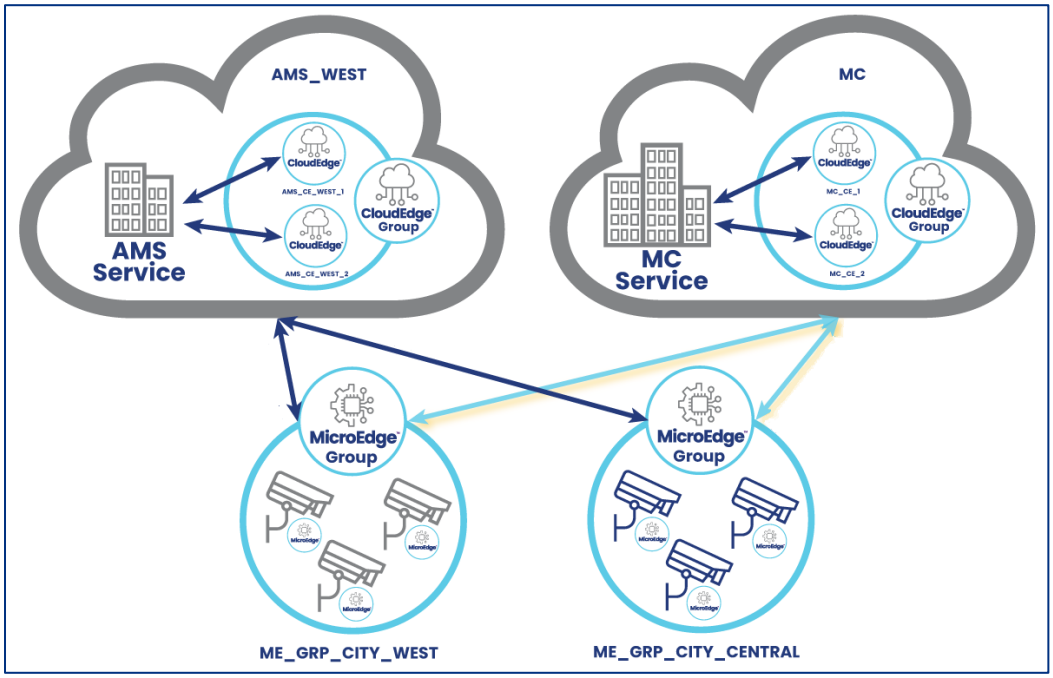

Figure 3 Sample Deployment

3. SECeDGE STUDIO™ USER INTERFACE

In the SecEdge Studio User Interface, the user can configure and manage groups of MicroEdge™ and CloudEdge™ devices, and their connectivity rules.

When the user logs in, the dashboard page shows the general status of the system, including total number of devices, devices down and alerts. Shown in Figure 4:

1. The graph in top left shows CloudEdges, MicroEdges and the connections between them for a particular CloudEdge group. The CloudEdge group can be selected from the dropdown.
2. The Key Stats section on the top right shows total number of CloudEdges, MicroEdges and number of devices that are down. Devices down are devices that have not connected back.

3. The Alerts table shows the different events happening to the CloudEdges and MicroEdges.
4. The pie chart on the bottom left shows the different types of MicroEdges. Figure 4 shows MicroEdge Host Type. If EmSPARK MicroEdge types were present, then they would be also shown in this pie chart.
5. The pie chart in the middle shows the status of MicroEdges connected to a particular CloudEdge. The CloudEdge can be selected from the dropdown. In the figure, the selected CloudEdge is not connected to any MicroEdge devices.
6. The pie chart to the right shows the connected and disconnected MicroEdges in a CloudEdge group. The CloudEdge group can be selected from the dropdown.

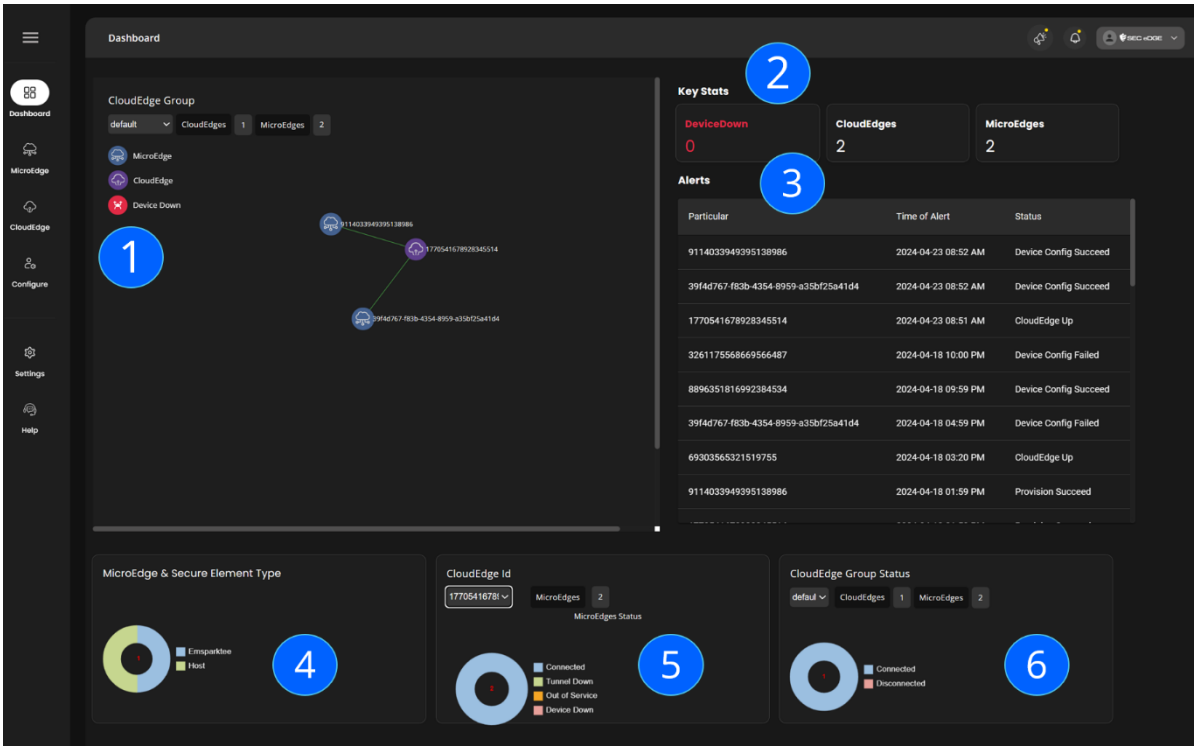

Figure 4 SecEdge Studio Dashboard

The left side options enable management of MicroEdge and CloudEdge groups, devices, profile configuration and user settings. The management and configuration options are explained in the following sections of this document.

4. MICROEDGE GROUP AND MICROEDGE™

A customer may have tens of thousands of devices on their deployment. MicroEdge groups enable management of large numbers of devices equipped with MicroEdge, or MicroEdges. Customer configures profiles to customize connection settings, including

reconnection time, tunnel provisioning, key and certificate rotation time and certificate expiry time.

MicroEdge groups allow customer to easily assign and manage the configuration profile of the deployed MicroEdges in the group. Customer uses the group to:

- Configure IPsec tunnels and their security profile for sets of devices to enable secure communication with CloudEdges.
- Manage the secure tunnels.
- Configure key rotation policies for sets of devices.

Characteristics:

- A MicroEdge always belongs to a MicroEdge Group.
- For a new customer, the system creates a default MicroEdge Group.
- When a MicroEdge is deployed, it is assigned to the default group.
- The default group configuration cannot be updated.
- Each Group has a basic configuration profile and a security profile.
- Customer can setup multiple configuration profiles and assign them to different groups.

Example:

AMS designates devices per groups based on device location

- AMS configured 5 MicroEdge groups in the city: North, West, South, East and Central.
- The devices communicate to the AMS service via AMS_CloudEdge.

Figure 5 depicts the MicroEdge West group and devices that belong to it.

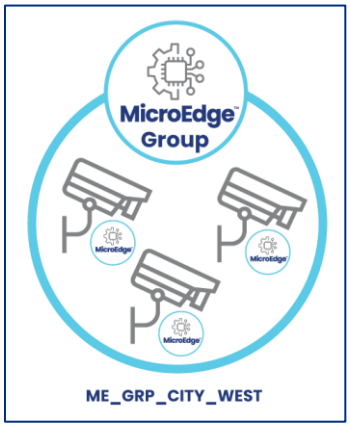

Figure 5 Example: MicroEdge Group

4.1. MICROEDGE GROUP OPERATIONS

The following operations are available to manage MicroEdge groups:

- Add MicroEdge Groups
- Add a MicroEdge device device(s) to Group
- View details of Group
- Edit properties of Group
- Delete Groups

4.1.1. ADD GROUPS

Create a MicroEdge group to assign a profile and security settings for a set of MicroEdge devices, or MicroEdges. Before creating the group, identify the basic profile of reconnection time and tunnel provisioning, described in 5.3 Basic Config Profiles. Also configure the security profile to setup the tunnel key rotation time, certificate rotation time and certificate expiry time, described in 5.4 Security Config Profiles. Then, assign MicroEdges to the group.

Example

AMS creates a MicroEdge group with custom configuration and security profile, depicted in Figure 6 and Figure 7.

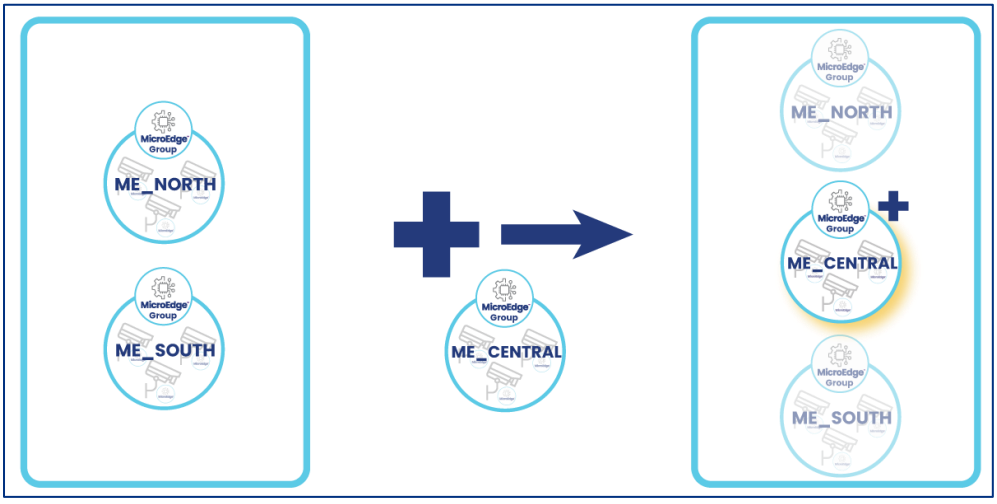

Figure 6 Example: Add ME_CENTRAL MicroEdge group

Steps

1. Select MicroEdge and MicroEdge Groups.
2. Click Add Group button.

3. Click Add button after input

   - Group Name, enter descriptive name.
   - Config Profile Name, select the profile that matches the periodic reconnect time interval and provisioning tunnels. Section 5.3 Basic Config Profiles describes the configuration settings.
   - Security Profile Name, select the profile that matches the key rotation time, certificate rotation time and certificate expiry time. Section 5.4 Security Config Profiles describes the configuration settings.

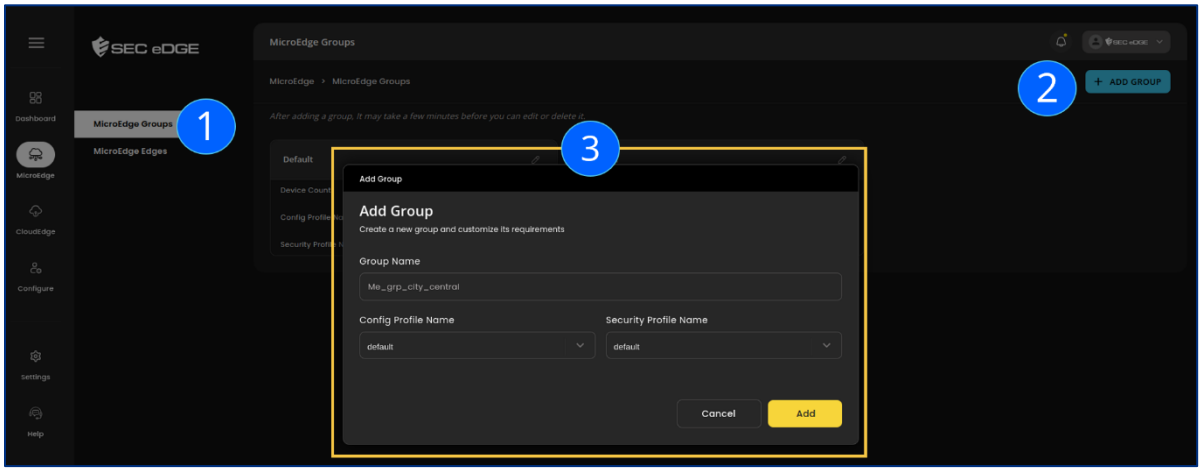

Figure 7 Add MicroEdge Group

4.1.2. ADD DEVICE TO GROUP

The MicroEdge device must be already created in the system. Adding the MicroEdge device to a group removes it from the group where it was previously assigned.

Example:

Add a MicroEdge device to a MicroEdge group, depicted in Figure 8 and Figure 9.

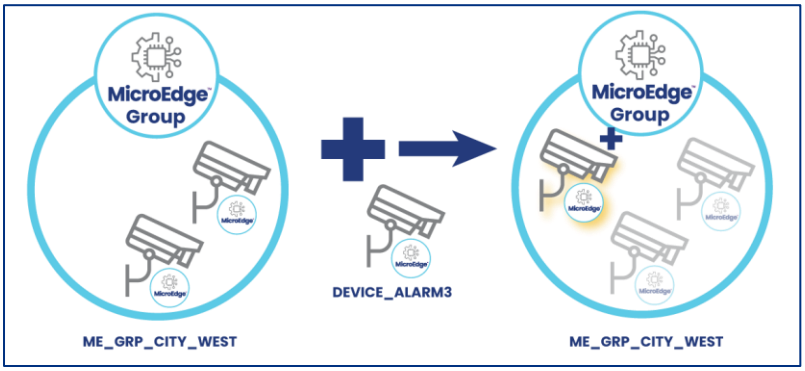

Figure 8 Example: Add DEVICE_ALARM3 to ME_GRP_CITY_WEST group

Steps:

1. Select MicroEdge and then Groups options on the left.
2. Select the group on the list and click on the Add Device button.
3. Input MicroEdge device data and then click on the Add button:
    - Device ID: device hardware id as listed in the MicroEdge Edges page.
    - Device Name: user defined name, as listed in the MicroEdge Edges page.

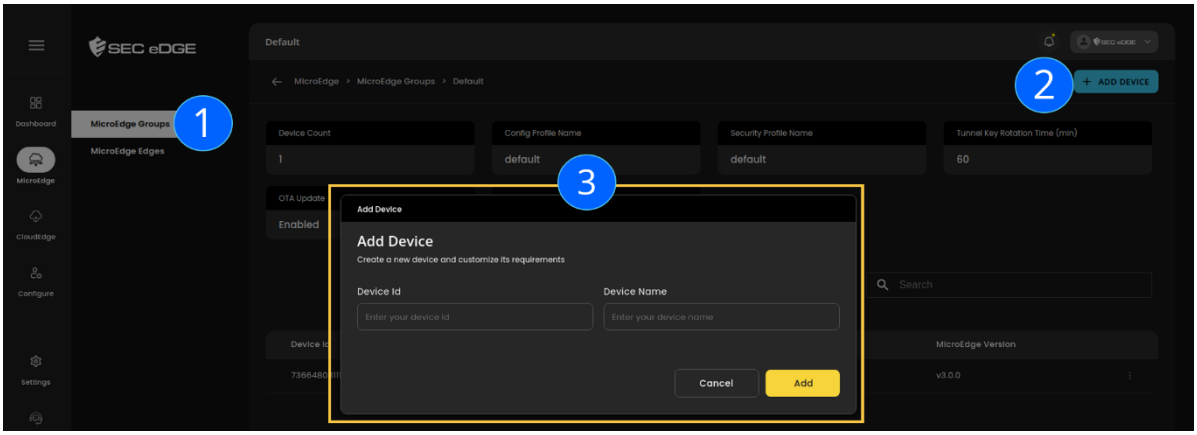

Figure 9 SecEdge User Interface Add MicroEdge Device

4.1.3. VIEW DETAILS OF GROUP

The details of a MicroEdge group show the group configuration and devices in the group:

+ Group detailed information: device count, configuration profile, security profile, tunnel key rotation time in min, OTA update enablement and secure tunnel enablement.
+ Group devices: device hardware, device name, secure element type, status, version and delete option.

Example

View details of a MicroEdge group, illustrated in Figure 10 and Figure 11.

Figure 10 Example: Select ME_GRP_CITY_WEST to view details about this group

Steps

1. Select MicroEdge and then Groups options on the left
2. Select the group on the list
3. View details of that Group

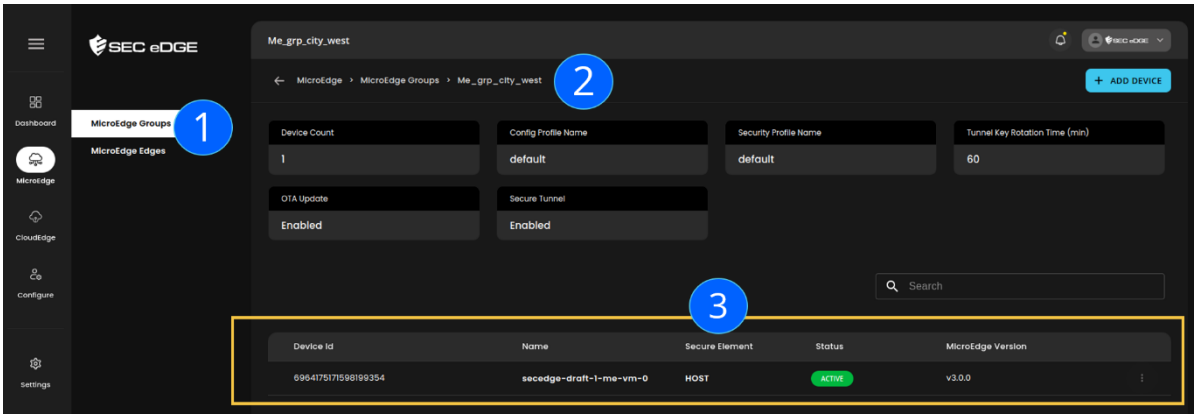

Figure 11 SecEdge User Interface View Group Details

4.1.4. EDIT PROPERTIES OF GROUP

The group profile configuration can be updated:

+ The basic profile of reconnection time and tunnel provisioning, described in 5.3 Basic Config Profiles.
+ The security profile to setup the tunnel key rotation time, certificate rotation time and certificate expiry time, described in 5.4 Security Config Profiles.
+ The group name.

Example:

Rename a MicroEdge Group, illustrated in Figure 12 and Figure 13

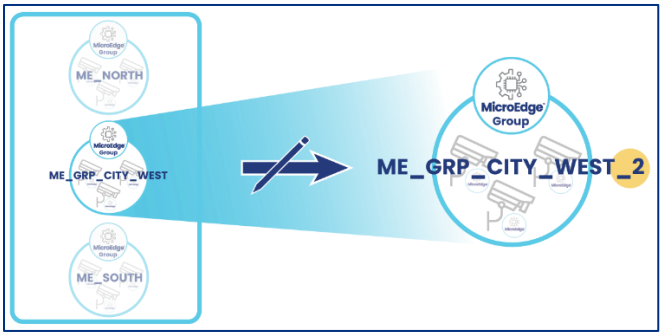

Figure 12 Example: Rename ME_GRP_CITY_WEST group to ME_GRP_CITY_WEST_2 group

Steps

1. Select MicroEdge and then Groups options on the left
2. Click Edit button (Pencil) of a Group
3. Change some fields on the Edit Group page and hit Save button

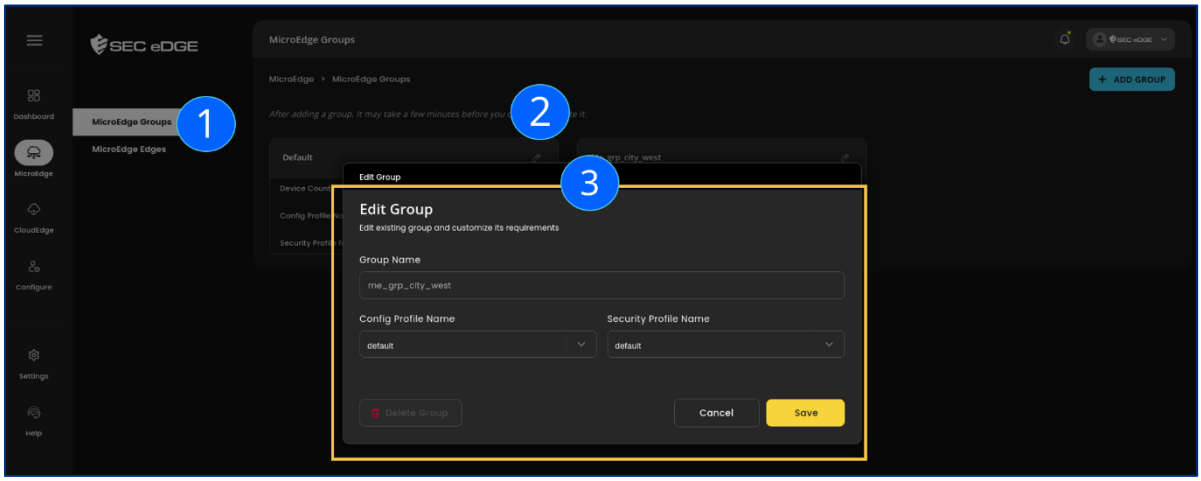

Figure 13 SecEdge User Interface Edit MicroEdge Group

4.1.5. DELETE GROUP

Considerations to delete MicroEdge groups:

- A MicroEdge group that has associated MicroEdges cannot be deleted.
- Before deleting a MicroEdge group, remove or reassign the devices from the group.
- To delete a group, follow the same steps to edit and click on the Delete Group button.

4.2. MICROEDGE OPERATIONS

Installation of the MicroEdge application on the device is described in the SecEdge Studio documentation for the specific hardware. On the SecEdge Studio User Interface, customer can request the execution of a specific operation for a MicroEdge:

- Create new MicroEdge
- Delete, reset or set Out Of Service a MicroEdge device
- View details of MicroEdge device

Note that the operation is executed on MicroEdge when it connects to the ControlEdge the next time. Until then, the MicroEdge continues functioning the same as previously the operation request.

4.2.1. CREATE A MICROEDGE™

Customer installs the MicroEdge application on a machine. The SecEdge Studio documentation for the specific hardware deployment instructs the steps. After the installation, customer adds the MicroEdge in the SecEdge Studio User Interface, as described in this section.

Creating a MicroEdge provisions the details of the MicroEdge in ControlEdge. This step is required before a MicroEdge can register itself with ControlEdge.

Example

Create a new alarm device that will be managed with the policies assigned to Group City West, illustrated in Figure 14 and Figure 15.

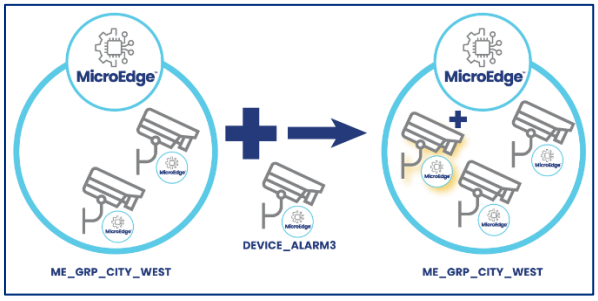

Figure 14 Example: Create new device DEVICE_ALARM3

Steps

1. Select MicroEdge and then Edge options on the left.
2. Click Add Device button
3. Input data and then click the Add button:
    - Device Id: string generated on the device during the MicroEdge installation and known by the MicroEdge application when it starts on the device. Considerations for Device ID are explained in the SecEdge Studio documentation for the specific hardware.
    - Device Name: human readable designation for the device on the user interface.
    - MicroEdge Group Name: select the group
    - Secure Element: two types are listed, HOST and EMSPARKTEE. HOST is the default type. EMPARKTEE requires customer to input the device public key uploading the public key in PEM encoding. After the MicroEdge is created the secure element value cannot be changed.

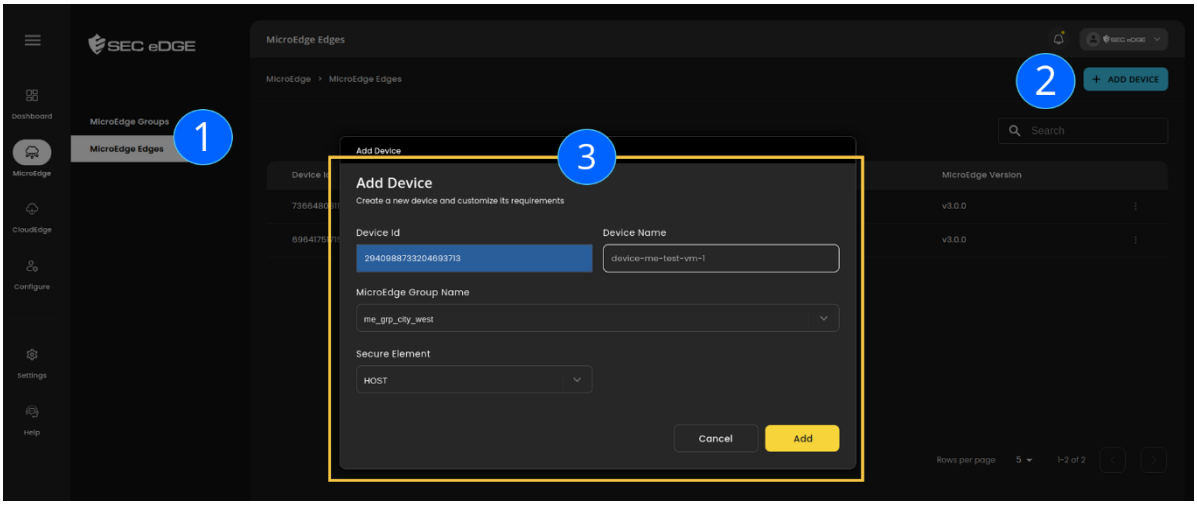

Figure 15 SecEdge User Interface Add MicroEdge Device

When deploying VMs using SecEdge Studio in the GCP customer's account Product details page, the MicroEdge is automatically created and registered with ControlEdge. The following data is assigned during deployment:

- Device Id, VM instance ID generated during the VM deployment
- Device Name, generated based on the GCP Deployment name and the number of deployed instances.
- Group Name, initially assigned to the Default group.
- Secure Element, type of secure element, default HOST.

4.2.2. VIEW DETAILS OF A MICROEDGE DEVICE

Customer has available detailed information about a MicroEdge:

- Current state
- Identity details
- Software and firmware details
- Tunnel information
- Various profile information

Example

View details about a device, illustrated in Figure 16, Figure 17, Figure 18 and Figure 19.

Figure 16 Example: Select DEVICE_ALARM3 to view details about this device

Steps

1. Select MicroEdge and then Edge options on the left.
2. Click on a selected device from the list of devices.
3. View the selected MicroEdge detail:
    - Basic Information, device id and device name, type of secure element, state, last connection time and MicroEdge version. The Device State can have the following values.

Device State	Description
REGISTERED	Device is registered with the cloud, but not connected yet.
ACTIVE	After the device connects with the cloud and can be served is moved to active state. For devices using EmSPARK, upon device key verification the device is moved to active state.
DEREGISTERED	State after the MicroEdge device has been deleted.
OOS	Device out-of-service.
DEREGISTER IN PROGRESS	State after the delete process has been initiated and before is it completed.
RESET IN PROGRESS	State after the reset process has been initiated and before is it completed.

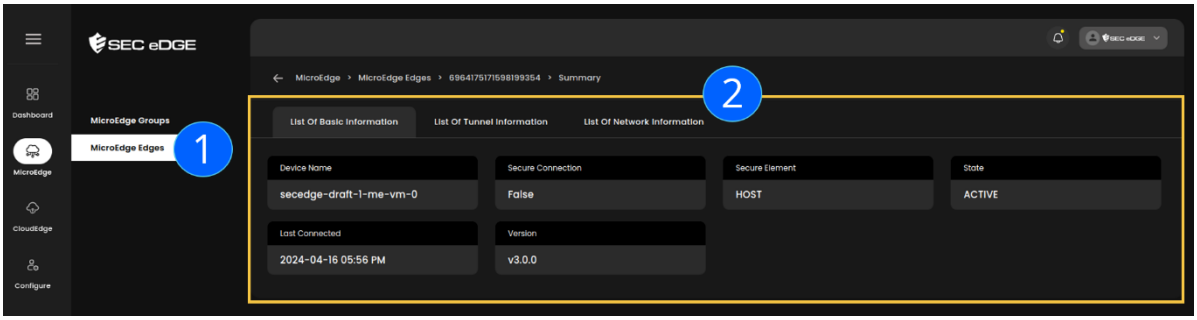

Figure 17 SecEdge User Interface View MicroEdge Detail

+ Tunnel Information. If secure connect feature is supported for the MicroEdge, click on Show More to see the Tunnel Profile details. Tunnel Status is the status of the IPsec tunnel reported by MicroEdge when MicroEdge last connected.

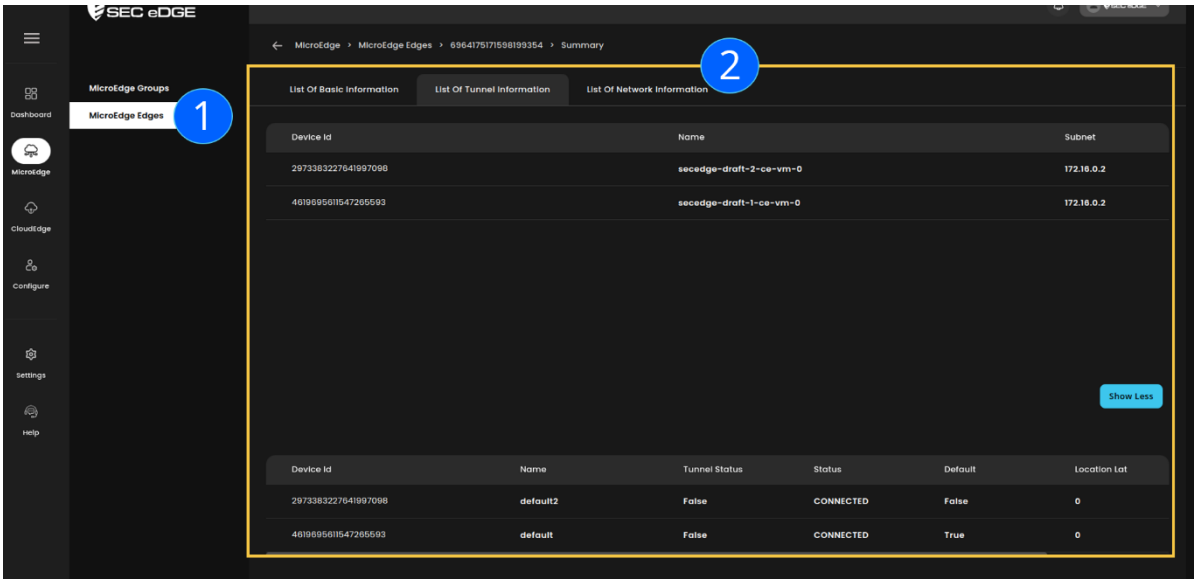

Figure 18 SecEdge User Interface MicroEdge List of Tunnel Information

- Network Information, WAN IP address, external IP address and external port.

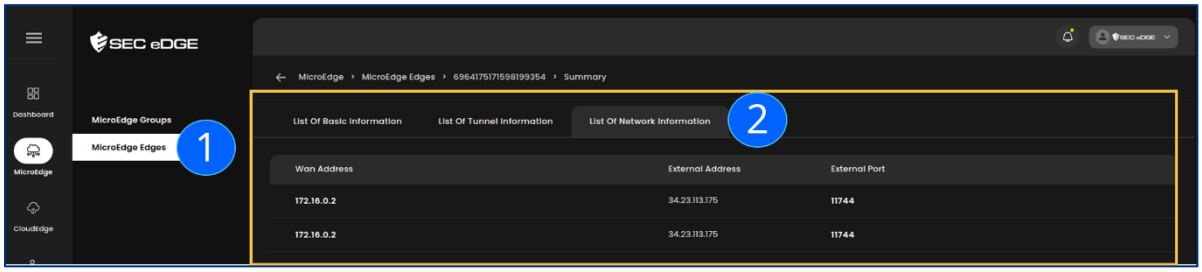

Figure 19 SecEdge User Interface MicroEdge List of Network Information

4.2.3. DELETE, RESET, SET OUT-OF-SERVICE, ROTATE CERTS A MICROEDGE DEVICE

On the list of MicroEdge devices, the three dots on the right side of the page permit selecting specific operations for a selected MicroEdge.

+ **Delete a MicroEdge device**

  The Delete option removes the device information from the system. After clicking DELETE, the page lists the device in DEREGISTERINPROG status. The next time the device connects, the device receives the deregistration command and the Day1 certificate is deleted from the device. The device sends a response back so it can be marked as deleted.

Deregistering a MicroEdge renders it unusable. A deregistered MicroEdge is not able to connect to ControlEdge (Day0/Day1) anymore until the MicroEdge is re-provisioned by the user using one of the provisioning APIs.

Note that the MicroEdge is deleted only when it connects the next time. Until that time, the MicroEdge functions work as usual. After the MicroEdge device is deleted, it is removed from the list of Edges.

Example

Delete a MicroEdge device from the device list, illustrated in Figure 20 and Figure 21.

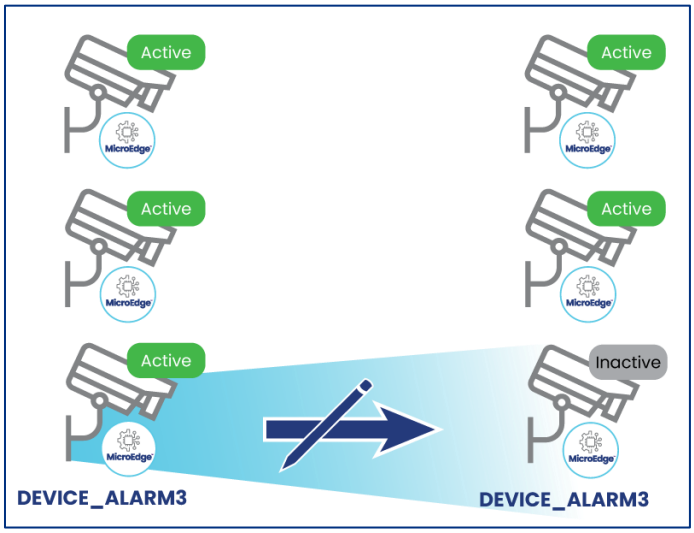

Figure 20 Example: Reset DEVICE_ALARM3

Steps

1. Select MicroEdge and then Edge options on the left.
2. Highlight a device, click on the three dots on the right side and select Delete.

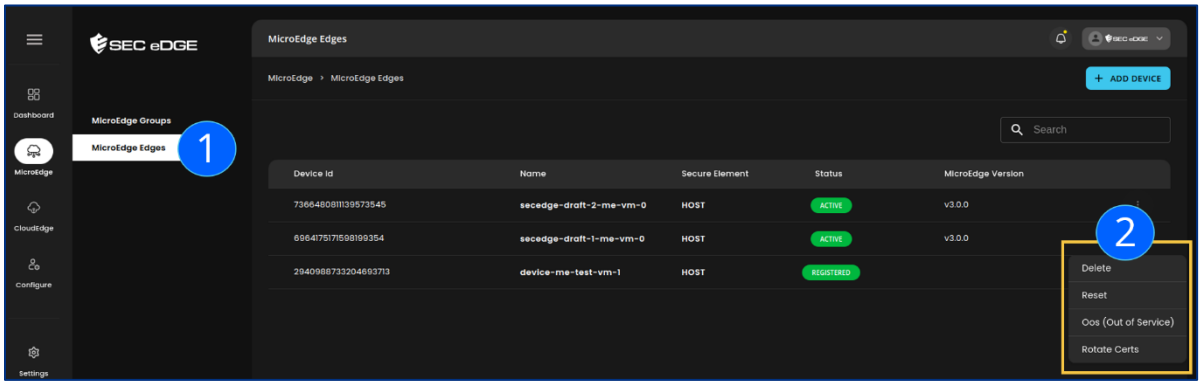

Figure 21 SecEdge User Interface Delete MicroEdge Device

+ **Reset a MicroEdge device**

  The Reset option moves the device back to Day0 state and issues tunnel configuration. After clicking on Reset, the page lists the device in RESET_IN_PROG status. The next time the device connects, the Day1 details are deleted from the device and the devices goes to Day0 state. The activation using Day0 and Day1 flow occurs. When the activation completes, the device sends a message so it can be moved to ACTIVE status again.

+ **Set Out Of Service a MicroEdge device**

  The Out of Service option temporarily deactivates the MicroEdge. After clicking on the Oos (Out of Service) option, the page lists the device in OOS state. The next time the device connects, the tunnels on the device are stopped. To reactivate the MicroEdge, select the ACTIVATE option on the right side which becomes available when the device is in OOS.

+ **Rotate Certs**

  The Security Config Profile allows to set the MicroEdge device certificate rotation time. In addition, the Rotate Certs option rotates the certificate the next time the MicroEdge device reconnects.

  The certificate rotation time configuration does not apply to CloudEdge devices.

5. CLOUDEDGE GROUP AND CLOUDEDGE™

A CloudEdge Group is a logical grouping of CloudEdge devices, i.e. a group of CloudEdges providing access to the same or similar servers. A CloudEdge is the cloud termination endpoint for MicroEdge device tunnels. A CloudEdge can anchor tens of thousands of MicroEdges. A MicroEdge device can be anchored to one or more peer CloudEdge devices. ControlEdge administers all devices equipped with MicroEdge and CloudEdge.

Characteristics

+ CloudEdge groups can be used to provide high availability. A MicroEdge can connect to any CloudEdge in a group. Thus, if one CloudEdge becomes unavailable, ControlEdge can configure the MicroEdges to connect to other available CloudEdges in the same group.

+ CloudEdge groups can be created and used for load balancing. When there is a large number of MicroEdges connected to the same backend and balancing the load across the network is required, Customer can add CloudEdges that reside on the same administrative span of control as the MicroEdge endpoint.

- Customer can add new CloudEdges. ControlEdge supports addition and registration of new CloudEdge to allow increased secure tunnel anchoring capacity.
- A newly created CloudEdge is automatically associated with the default CloudEdge Group.
- CloudEdge Groups are used for defining multi-tunnel profiles.
- Whenever a new MicroEdge is configured to establish a tunnel with a CloudEdge, the ControlEdge pushes the corresponding tunnel configuration to the CloudEdge which was selected to anchor the tunnel for this MicroEdge.
- In case of multiple tunnels, ControlEdge will push tunnel configuration to each CloudEdge with which the MicroEdge will be establishing the tunnel.

5.1. CLOUDEDGE GROUP OPERATIONS

The following operations are available to manage CloudEdge groups:

- Add and Delete Groups
- Add CloudEdge device(s) to a group
- Remove a CloudEdge from a group
- View details of Group
- Edit properties of Group
- Edit a route
- Delete a route

5.1.1. CREATE A CLOUDEDGE GROUP

When creating a new group, the customer configures routes and assigns a security profile that applies to the CloudEdges in the group.

Example

AMS creates a CloudEdge group with custom routing and security profile, illustrated in Figure 22 and Figure 23.

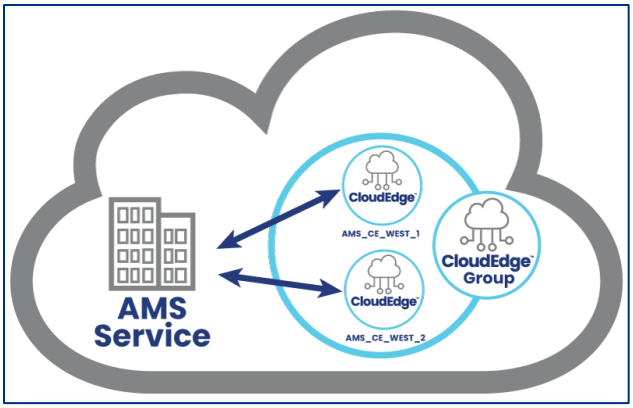

Figure 22 Example: Add new AMS_CE_GRP CloudEdge Group

Steps

1. Select CloudEdge and then Groups options on the left.
2. Click Add Group button
3. Click Add button after input below information
    - Group Name
    - Route list
        - Destination: subnet of the MicroEdge device.
        - Metric: integer to designate the preference of the route in the list. 0 is the highest priority. metric comes into effect only when multiple routes are present in a CloudEdge group.
    - Security Profile Name, the profile to setup the tunnel key rotation time described in 5.4 Security Config Profiles. Note that certificate rotation time in the security profile applies only to MicroEdge devices.

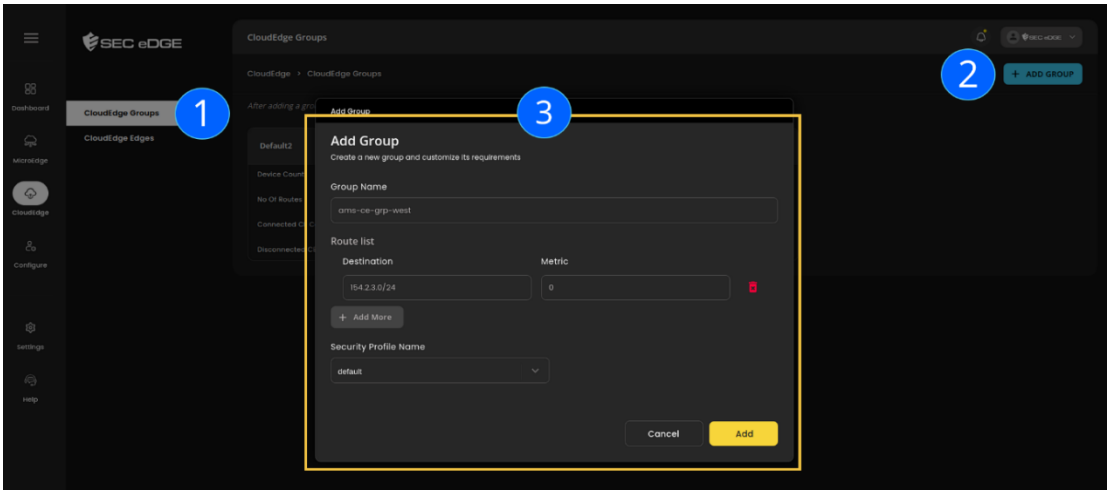

Figure 23 SecEdge User Interface Add CloudEdge Group

5.1.2. ADD A CLOUDEDGE™ TO GROUP

New CloudEdges can be added to a group to increase capacity or redundancy. The CloudEdge device must be already created in the system. Adding the CloudEdge to the group removes it from the group where it was previously assigned.

Example

AMS Service adds a CloudEdge to the CE_West group so that it uses the group's defined routes and security profile, Figure 24 and Figure 25.

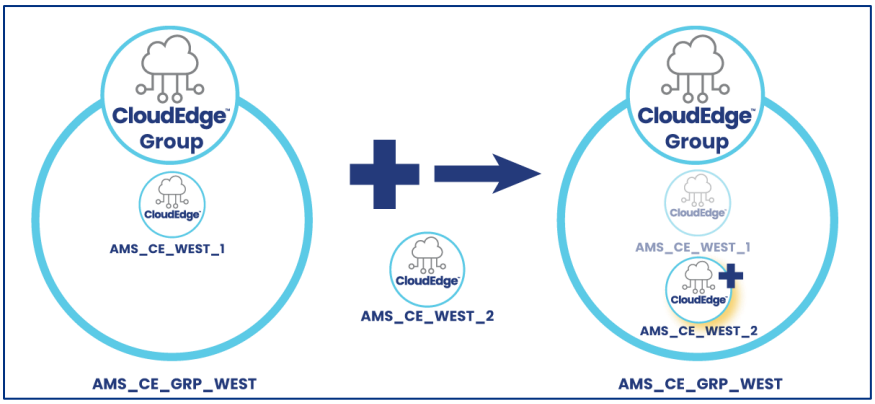

Figure 24 Example: Add AMS_CE_WEST_2 to AMS_CE_GRP_WEST group

Steps

1. Select CloudEdge and then Groups options on the left
2. Select the group on the list and click on the Add Device button.
3. Input device data and then click on the Add button
   - CloudEdge Id: device hardware id as listed in the CloudEdge Edges page
   - CloudEdge Name: user defined name, as listed in the CloudEdge Edges page.

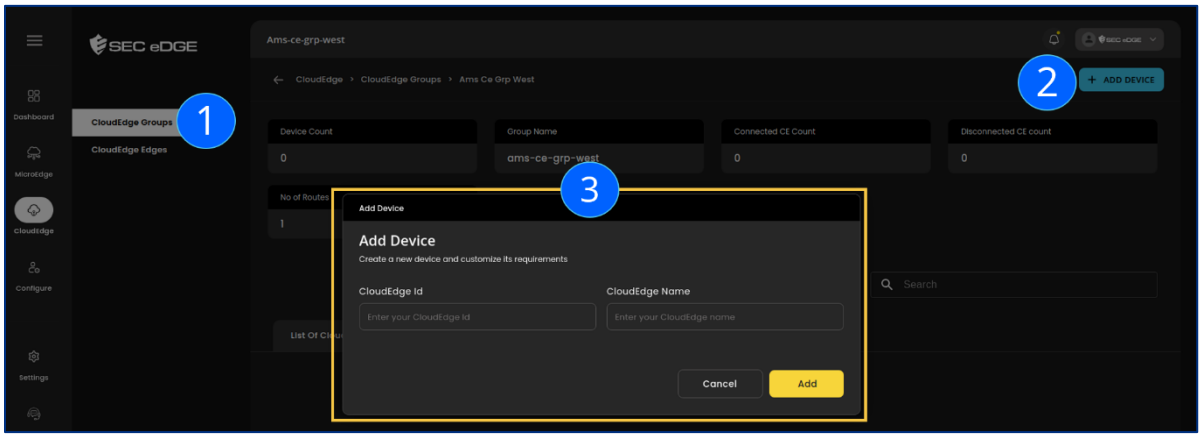

Figure 25 SecEdge User Interface Add CloudEdge Device

5.1.3. VIEW DETAILS OF CLOUDEDGE GROUP

Selecting a CloudEdge group, the detail page shows the device count, totals per connection status, and lists of CloudEdge devices and routes in the group. On this page, CloudEdge devices can be added or removed, and routes can be added or removed.

Example

AMS needs to know the totals of devices, their status and routes in the AMS CE West group, Figure 26 and Figure 27.

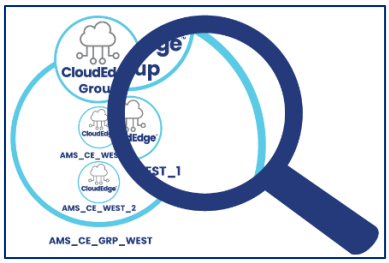

Figure 26 Example: Select AMS_CE_GRP_WEST to view details about this group

Steps

1. Select CloudEdge and then Groups options on the left.
2. Select a group on the list to view the details:
   - Total CloudEdges in the group.
   - Group Name.
   - Count of connected CloudEdges.
   - Count of disconnected CloudEdges.
   - List of CloudEdges with detail.
   - List of routes added to the group.

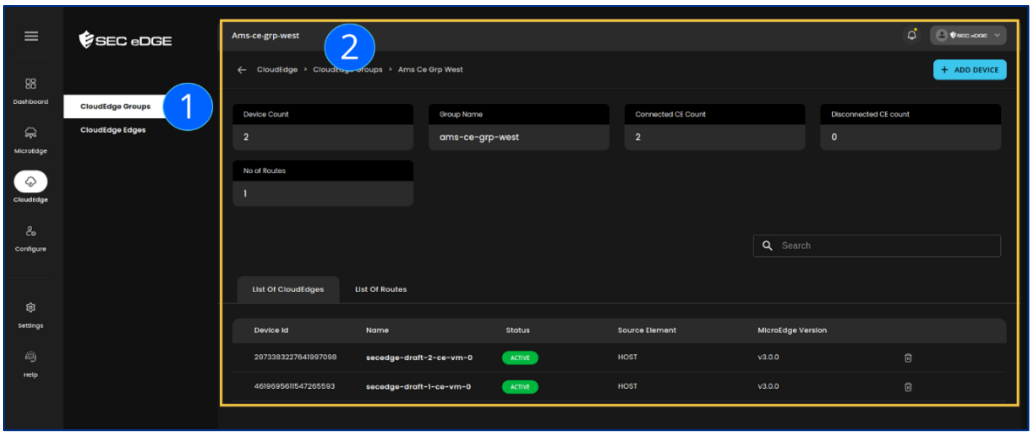

Figure 27 SecEdge User Interface View CloudEdge Group Detail

5.1.4. ADD OR DELETE A ROUTE

Routes are used in multi tunnel scenarios. Routes should be configured to appropriately route specific traffic originating from MicroEdges to the designated server(s) which are accessible only though the CloudEdge.

Example:

AMS adds routes to the CloudEdge group to redirect the traffic of specific data, such as video feed, Figure 28, Figure 29 and Figure 30.

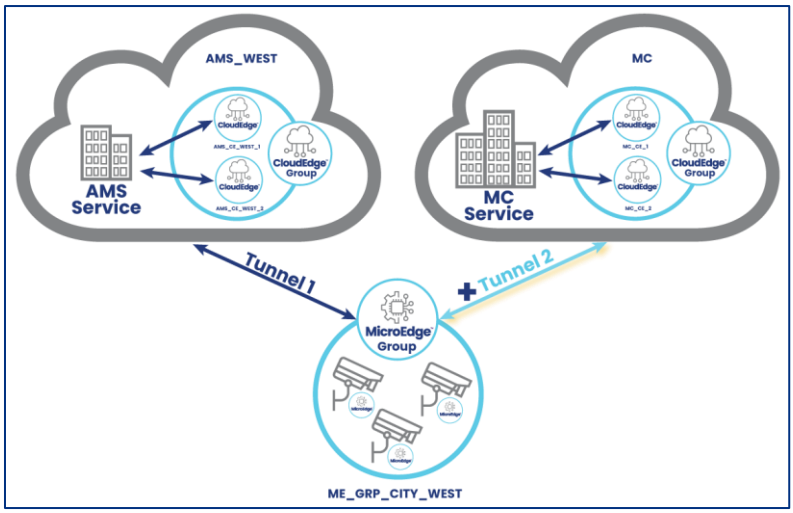

Figure 28 Example: AMS adds MC Service Route for AMS_CE_GRP_WEST group

Steps:

1. Select CloudEdge and then Groups options on the left.
2. Select a group on the list to view the details page.
3. Select the List of Routes tab.
4. Click on the Add Route button.
5. Enter Route information:
   - Destination, select true or false.
   - Metric, integer to designate the preference of the route in the list.

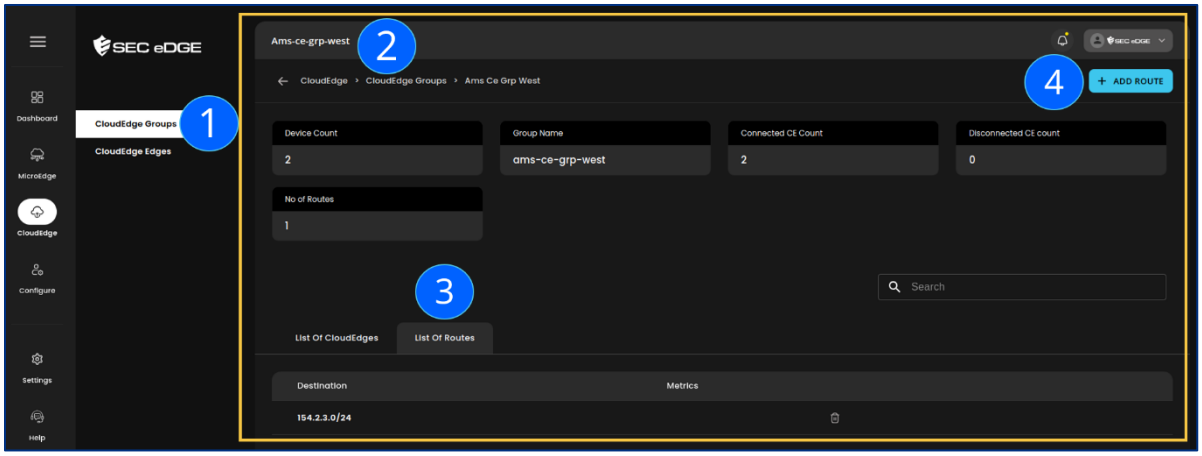

Figure 29 SecEdge User Interface List Routes

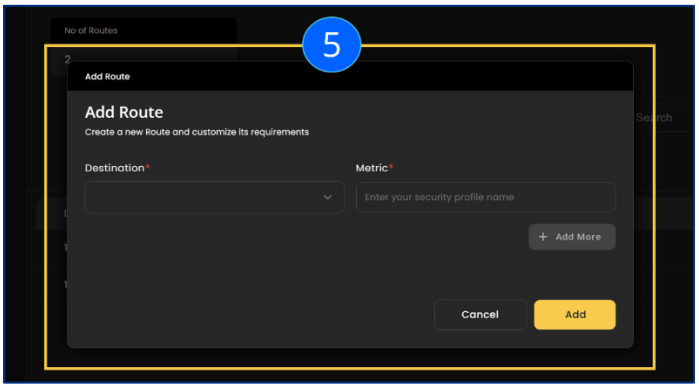

Figure 30 SecEdge User Interface Add Route

5.1.5. EDIT A CLOUDEDGE GROUP

Example:

The configuration of a group can be updated, Figure 31 and Figure 32.

Steps

1. Select CloudEdge and then Groups options on the left.
2. Click Edit button (Pencil) of a Group.
3. Change some fields on the Edit Group page and hit Save button.
    - Group name.
    - Route list, Figure 32:
        - Destination IP address in CIDR subnet notation.
        - Metric.
    - Security profile.

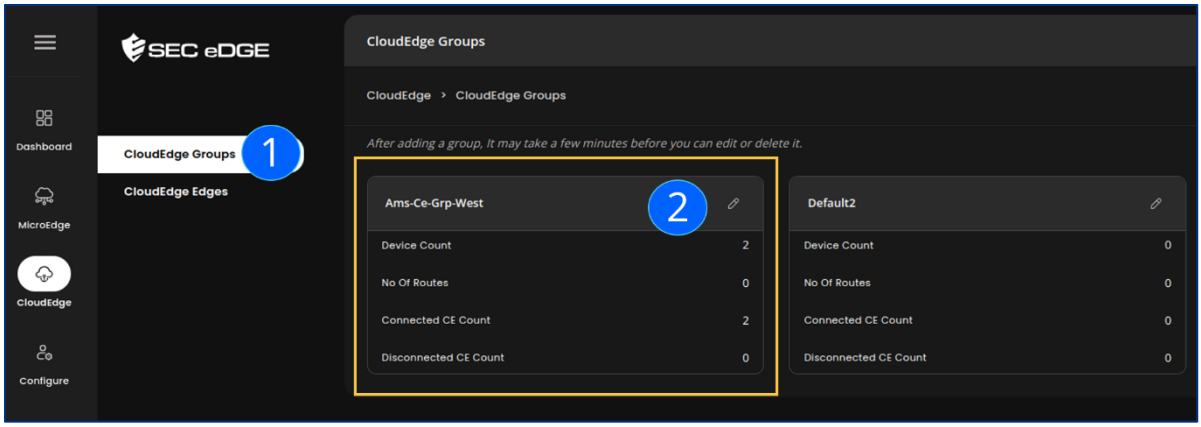

Figure 31 SecEdge User Interface List CloudEdge Groups

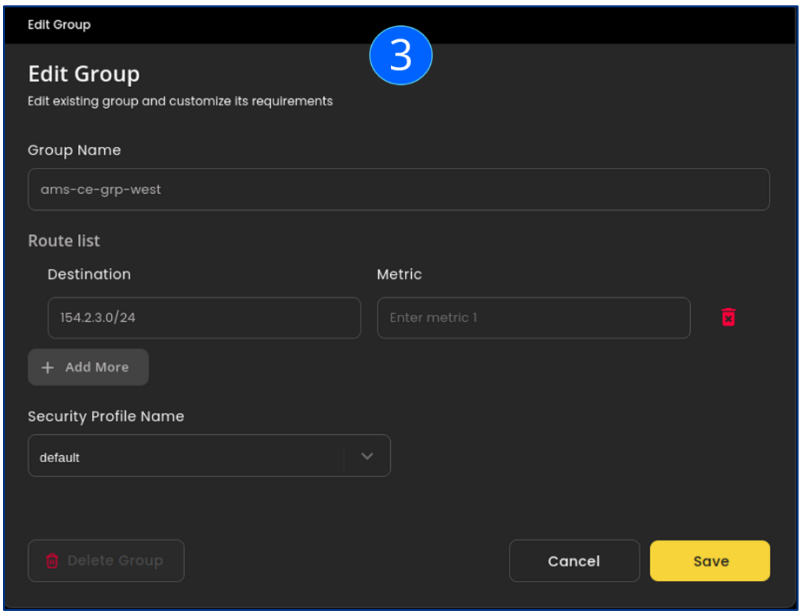

Figure 32 SecEdge User Interface Edit CloudEdge Group

5.1.6. DELETE A GROUP

The edit page has an option to delete the CloudEdge Group.

Considerations to delete CloudEdge groups:

- To delete a group, follow the same steps to edit and click on the Delete Group button.
- If there are CloudEdges associated with this group, then the delete operation fails.
- If any of the existing tunnel profiles are using this CloudEdge Group, then the delete operation fails.

5.2. CLOUDEDGE OPERATIONS

The following operations are available to manage CloudEdge devices:

- Create a CloudEdge
- Edit a CloudEdge
- View details of a CloudEdge
- Delete, reset or set Out Of Service a CloudEdge device

5.2.1. CREATE A CLOUDEDGE™

Customer installs the CloudEdge application on a machine. The SecEdge Studio documentation for the specific hardware deployment instructs the steps. After the machine is deployed, customer adds the CloudEdge in the SecEdge Studio User Interface, as described below.

Example

AMS adds a new CloudEdge to its operations and assigns it to a group, Figure 33 and Figure 34.

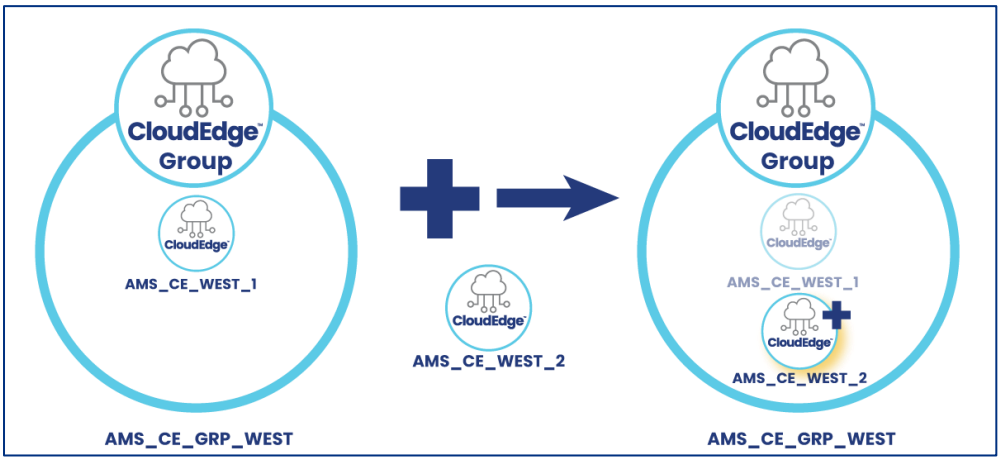

Figure 33 Example: Create AMS_CE_WEST_2 CloudEdge

Steps:

1. Select CloudEdge and then Edge options on the left.
2. Click Add Device button
3. Input data and then click the Add button:
    - Device Id: a unique ID configured on the device and known by the CloudEdge binary when it starts on the device.

- Device Name: human readable designation for the device on the user interface.
- CloudEdge Group Name: select the group
- Subnet

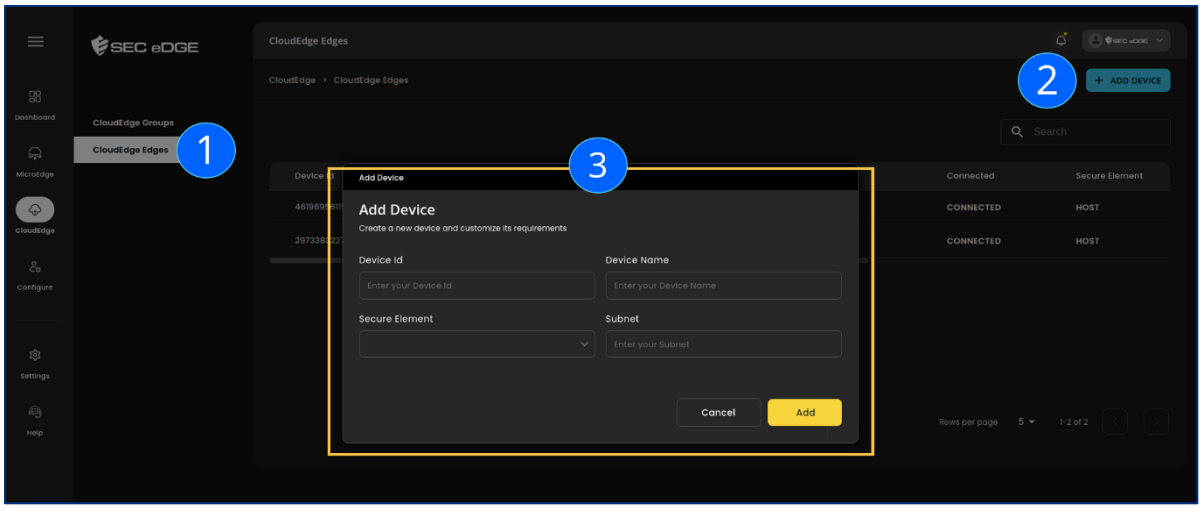

Figure 34 SecEdge User Interface Add CloudEdge Device

When deploying VMs using SecEdge Studio in the GCP customer's account Product details page, the CloudEdge is automatically created and registered with ControlEdge. The following data is assigned during deployment:

+ Device Id, VM instance ID generated during the VM deployment
+ Device Name, generated based on the GCP Deployment name and the number of deployed instances.
+ Secure Element, type HOST.
+ Subnet

5.2.2. VIEW DETAILS OF A CLOUDEDGE™

Example:

AMS views a CloudEdge basic information including device connectivity state and network information, Figure 35 and Figure 36.

Figure 35 Example: View AMS_CE_WEST_2 information

Steps

1. Select CloudEdge and then Edges options on the left.
2. Select a device from the list to view the details:
   - Basic information including name, connectivity and CloudEdge version.
   - Network details such as WAN address, external address, external port and subnets.

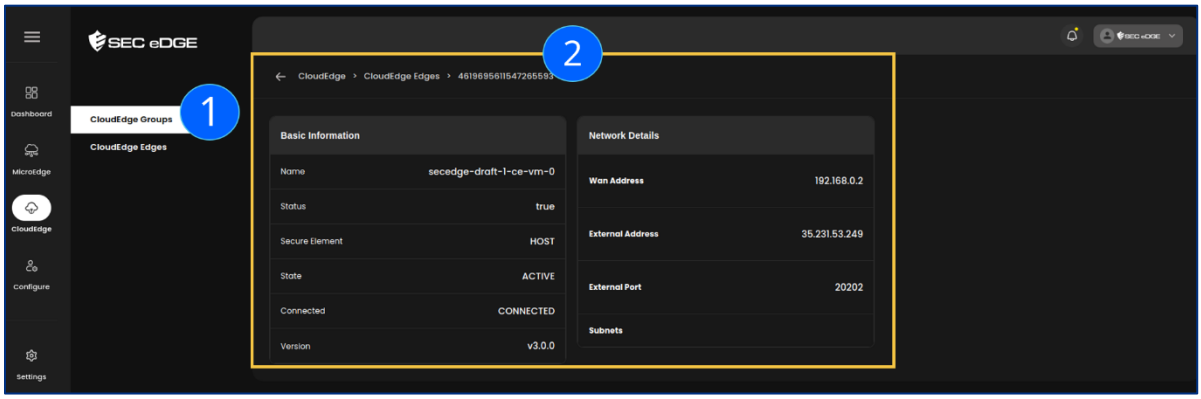

Figure 36 SecEdge User Interface View CloudEdge Device Detail

5.2.3. CONFIGURE PROFILES

Profiles enable configuring the policies that an IPsec tunnel between a MicroEdge and a CloudEdge use. Customer configures the profiles. After the profiles are configured, customer assigns them to MicroEdge groups and CloudEdge groups for deployment on the devices that belong to the assigned groups.

The following are types of profiles to configure and manage:

+ Basic configuration
+ Security configuration

+ Secure Element
+ Tunnel profiles

For each configuration type, SecEdge Studio has preconfigured a Default profile that is assigned to the MicroEdge Default group and CloudEdge Default group when the first customer's deployment occurs.

5.3. BASIC CONFIG PROFILES

The basic profile configures the device reconnection time and tunnel provisioning:

+ Reconnect Time: To optimize resource utilization on IoT devices, MicroEdge does not keep persistent connection with ControlEdge. After secure tunnels are established, MicroEdge disconnects from ControlEdge. This configuration is the interval after which MicroEdge should reconnect to ControlEdge for next instructions.
+ Provision Tunnel: True or False. This configuration specifies the cloud whether the MicroEdge device needs the IPsec tunnel feature or not.
    - If Provision Tunnel is false, then the IPsec tunnel is not created for all the MicroEdges using this profile.
    - If Provision Tunnel is true, then the IPsec tunnel is created for all the MicroEdges using this profile.

5.3.1. ADD A BASIC CONFIGURATION PROFILE

Steps

1. Select Configure and then Basic Config Profiles options on the left.
2. Click on Add Profile button.
3. Click on the Add button after entering the profile information:
    - Profile name
    - Reconnect Time, in seconds
    - Provision tunnel, True or False

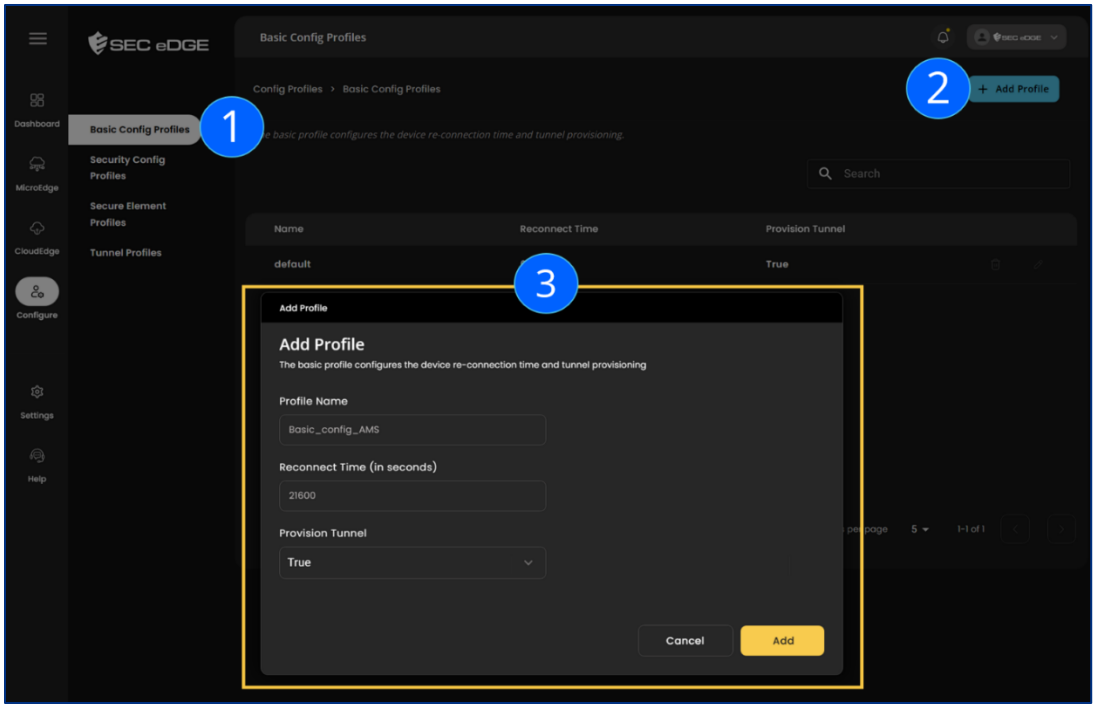

Figure 37 SecEdge User Interface Add a Basic Configuration Profile

5.3.2. EDIT A BASIC CONFIGURATION PROFILE

Steps

1. Select Configure and then Basic Config Profiles options on the left.
2. Click on the pencil icon on the right side to edit, Figure 38.
    - Modification of the Default profile settings is not permitted.
    - All values of the customer created profiles can be updated.

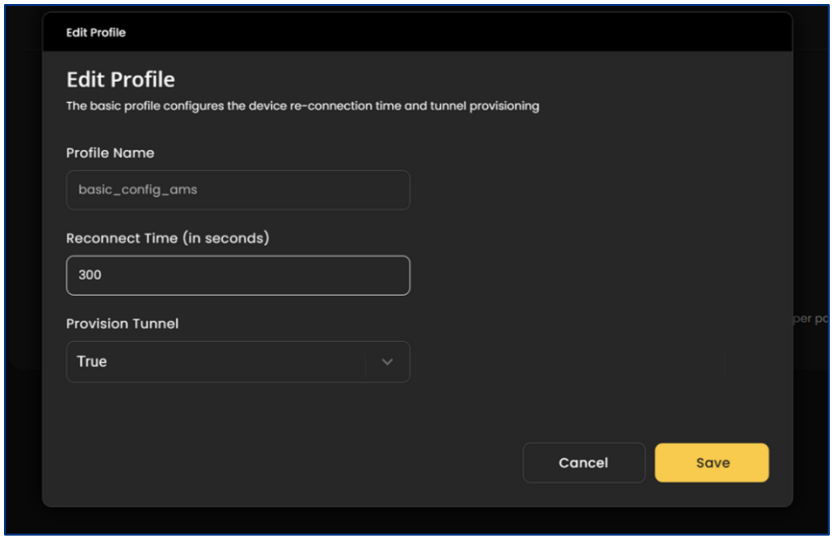

Figure 38 SecEdge User Interface Edit a Basic Configuration Profile

5.3.3. DELETE A BASIC CONFIGURATION PROFILE

Steps

1. Select Configure and then Basic Config Profiles options on the left.
2. Click on the three dots on the right side and select Delete, Figure 39.
    - Not permitted if the profile is assigned to a MicroEdge or a CloudEdge group.
    - Not permitted for preconfigured Default profiles.

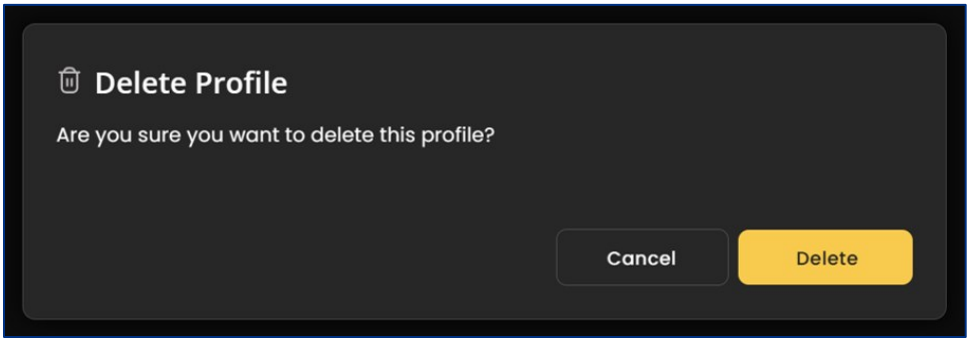

Figure 39 SecEdge User Interface Delete a Basic Configuration Profile

5.4. SECURITY CONFIG PROFILES

The connections are secured with keys and certificates. The security profile is used to associate tunnel-key-rotation time and Day1-certficate-rotation time for a MicroEdge:

+ Tunnel Key Rotation Time: IPSec tunnel keys between MicroEdge and CloudEdge will be rotated after this interval.
+ Certificate Expiry Time: The certificate for the TLS connection between MicroEdge and ControlEdge will be rotated after this interval.
+ For additional security of the data path, the ControlEdge takes care of periodically rotating the tunnel keys for each MicroEdge.
+ The new keys are then synchronized with the CloudEdge so that MicroEdge is able to communicate over IPsec tunnel using the new keys.
+ In case of multiple channels, the tunnel key rotation is done independently for each tunnel.
+ The default profile is not editable.

5.4.1. ADD A SECURITY CONFIGURATION PROFILE

Steps:

1. Select Configure and then Security Config Profiles options on the left.
2. Click on Add Profile button.
3. Click on the Add button after entering the profile information, Figure 40:
    - Profile name
    - Tunnel Key Rotation Time, in minutes, only applies to MicroEdge devices
    - Certificate Rotation Time, in minutes, only applies to MicroEdge devices
    - Certificate Expiry Time, in days

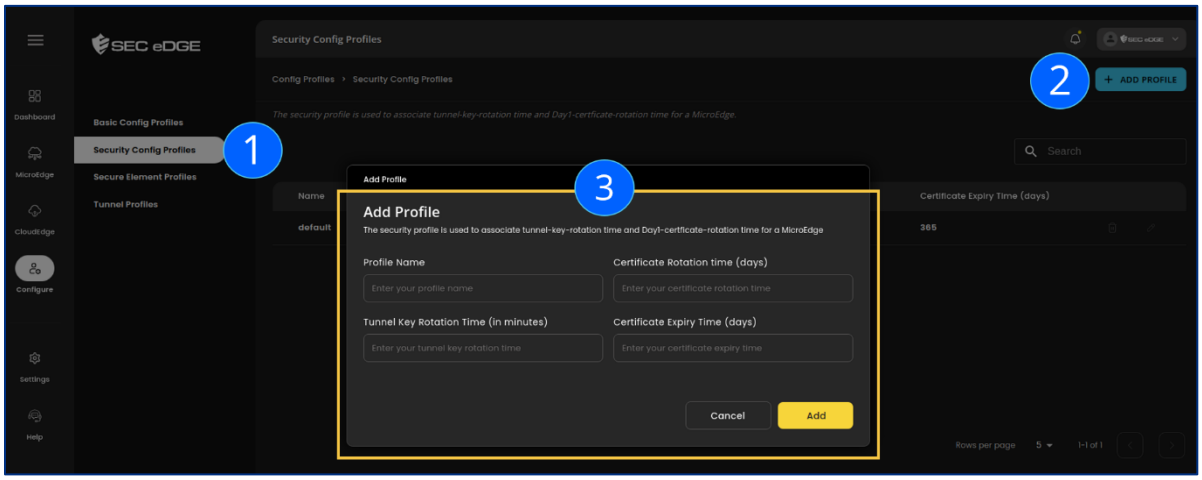

Figure 40 SecEdge User Interface Add a Security Configuration Profile

5.4.2. EDIT A SECURITY CONFIGURATION PROFILE

Steps:

1. Select Configure and then Security Config Profiles options on the left.
2. Select Configure and then Basic Config Profiles options on the left.
3. Click on the three dots on the right side and select Edit, Figure 41.
    - Modification of the Default profile settings is not permitted.
    - All values of the customer created profiles can be updated.

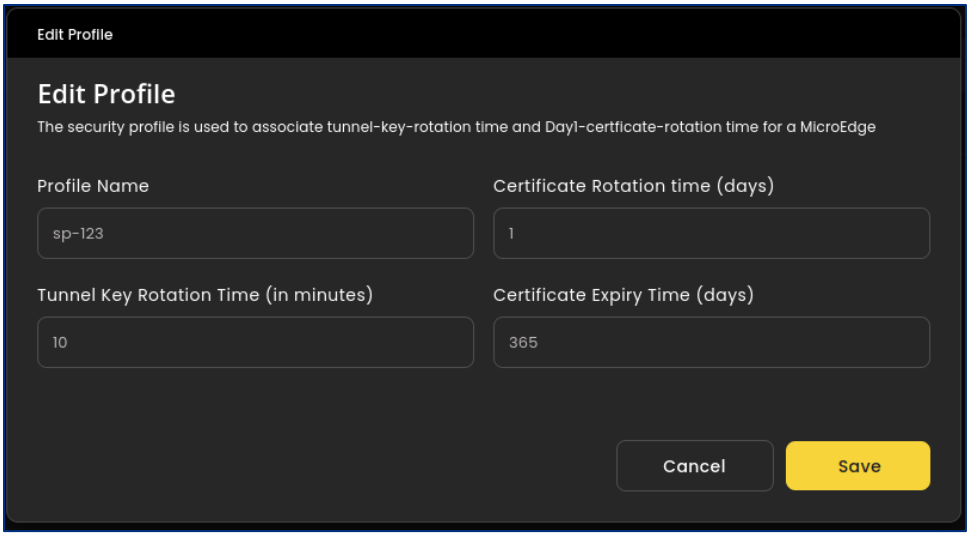

Figure 41 SecEdge User Interface Edit a Security Configuration Profile

5.4.3. DELETE A SECURITY CONFIGURATION PROFILE

Steps:

1. Select Configure and then Security Config Profiles options on the left.
2. Click on the three dots on the right side and select Delete, Figure 42
    - Not permitted if the profile is assigned to MicroEdge or CloudEdge group.
    - Not permitted for preconfigured Default profiles.

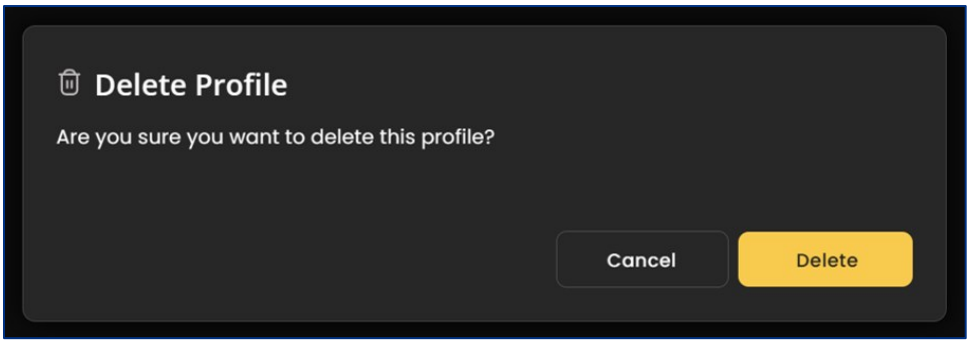

Figure 42 SecEdge User Interface Delete a Security Configuration Profile

5.5. SECURE ELEMENT PROFILES

Secure Element

+ Hardware root of trust or software emulation to identify and authenticate device.
+ Skip silicon validation: Whether HW root of trust support proof of silicon.

Operations:

- Add Secure Element profile
- Update a profile
- Delete a profile

5.5.1. ADD A SECURE ELEMENT PROFILE

Creates a new secure element configuration for the Secure Element (SE). The SecEdge Studio documentation for the specific machine where the SE is installed describes the steps to provision the various functions on the chip.

Steps, Figure 43**:**

1. Select Configure and then Secure Element Profiles options on the left.
2. Click on Add Profile button.
3. Click on the Add button after entering the profile information:
    - Profile name
    - Skip Silicon Validation, true or false

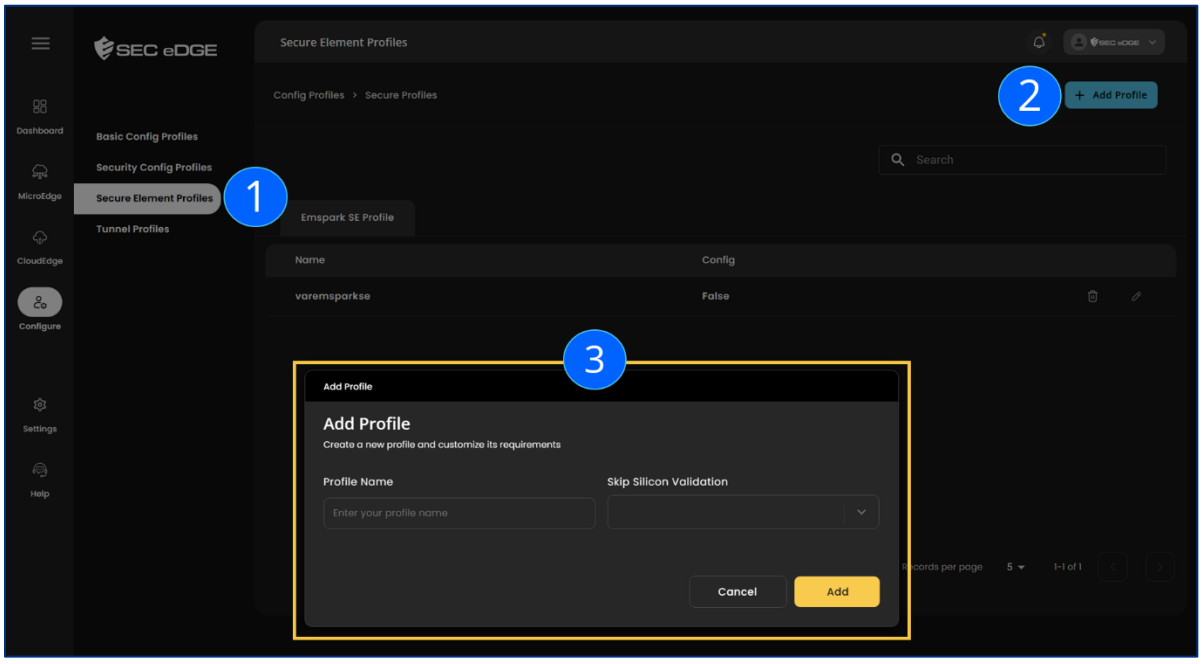

Figure 43 SecEdge User Interface Add a Secure Element Profile

5.5.2. EDIT A SECURE ELEMENT PROFILE

- Not permitted for preconfigured Default profiles.
- Updates the parameters of an existing secure element config.

5.5.3. DELETE A SECURE ELEMENT PROFILE

+ Not permitted if the profile is assigned to MicroEdge or CloudEdge group.
+ Not permitted for preconfigured Default profiles.

Steps:

1. Select CloudEdge and then Secure Element Profile options on the left.
2. Highlight a device, click on the three dots on the right side and select Delete, Figure 44.

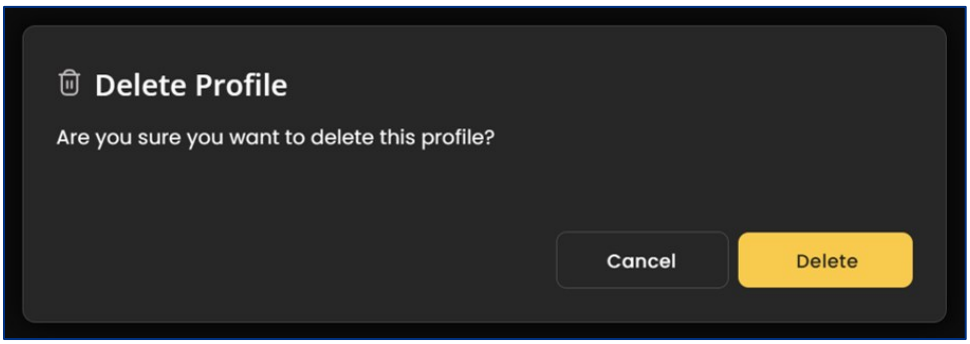

Figure 44 SecEdge User Interface Delete a Secure Element Profile

5.6. TUNNEL PROFILES

Tunnel configuration of MicroEdge. If a tunnel profile has multiple CloudEdge Groups and a MicroEdge is assigned to this profile then multiple tunnels will be set up for this MicroEdge.

5.6.1. ADD A TUNNEL PROFILE

Steps, Figure 45**:**

1. Select Configure and then Tunnel Profiles options on the left.
2. Click on Add Profile button.
3. Click on the Add button after entering the profile information:
   - Profile name
   - CloudEdge Group Name, select.
   - Default Group, select.

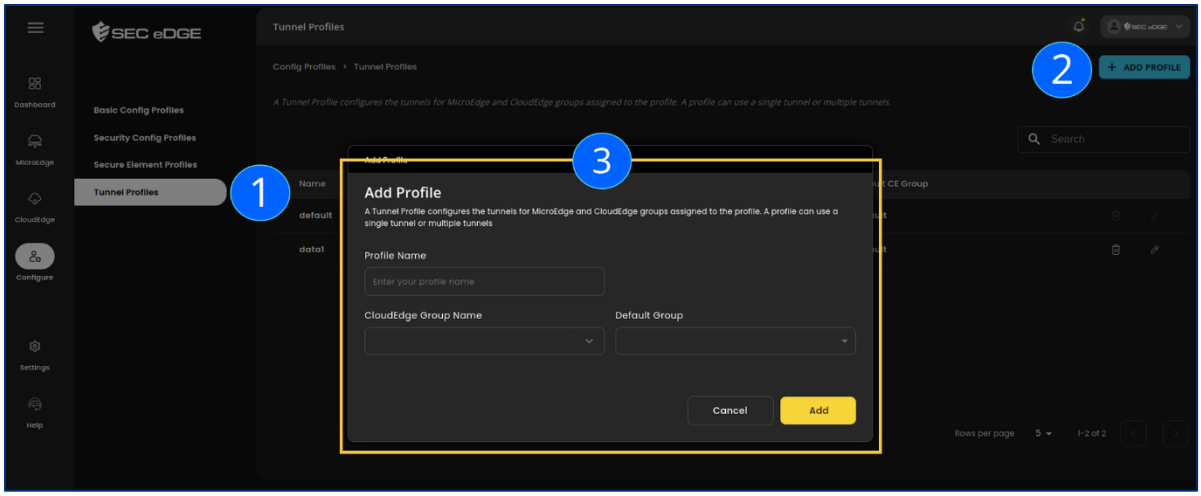

Figure 45 SecEdge User Interface Add a Tunnel Profile

5.6.2. UPDATE A TUNNEL PROFILE

+ Not permitted for preconfigured Default profiles.
+ Updates the parameters of an existing tunnel profile.
+ provision tunnel: what is the behavior? send it to the device?

Steps:

1. Select Configure and then Tunnel Profiles options on the left.
2. Click on the pencil icon on the right side.
3. Click on the Save button after updating the profile information, Figure 46.

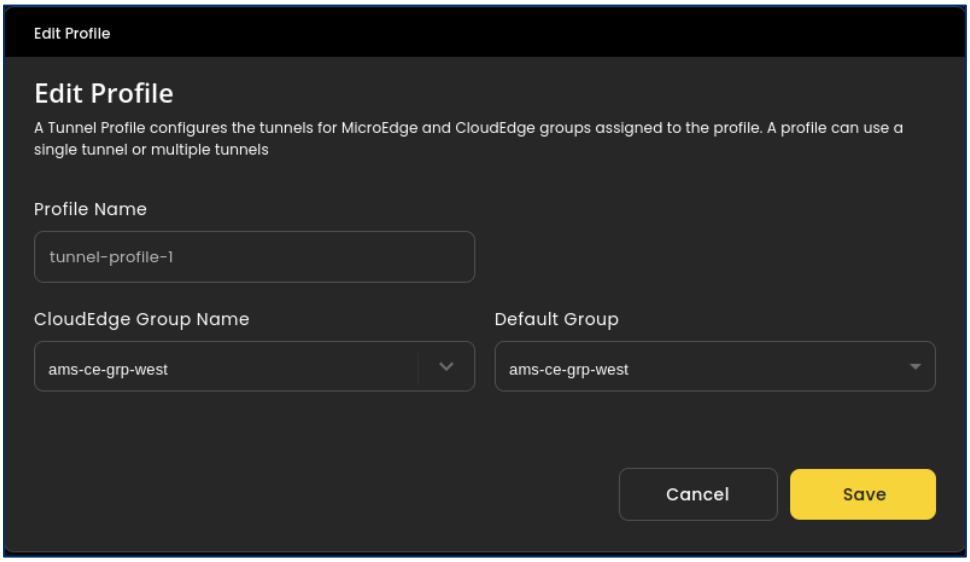

Figure 46 SecEdge User Interface Update a Tunnel Profile

5.6.3. DELETE A TUNNEL PROFILE

- Not permitted if the profile is assigned to MicroEdge or CloudEdge group.
- Not permitted for preconfigured Default profiles.

Steps:

1. Select Configure and then Tunnel Profiles options on the left.
2. Click on the basket icon on the right side.
3. Confirm operation, Figure 47:

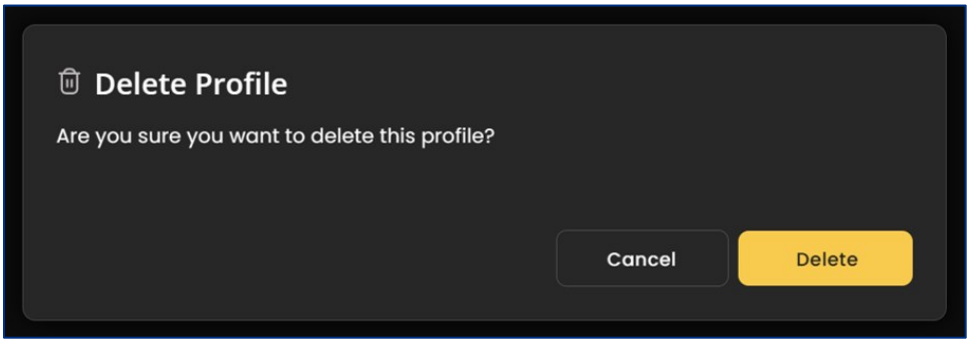

Figure 47 SecEdge User Interface Delete a Tunnel Profile

5.7. TUNNEL PROFILES – MULTI-TUNNEL OPTION

Customer can configure multiple tunnels to route certain traffic to different destinations.

Example:

AMS's alarm devices have configured tunnels to communicate from the building of AMS's customers with AMS Service to fulfill usual operations. The devices also have configured tunnels to MC Service whose staff monitors the alarm equipment and does maintainance on site, when needed, Figure 48.

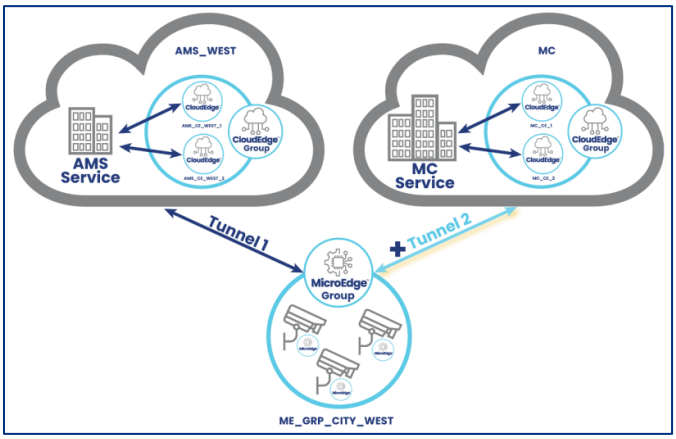

Figure 48 Example: Tunnel #2 added to communicate with MC Service (Maintenance Company)

- Create multi-tunnel profile (link to two or more CloudEdge Groups), Figure 49.

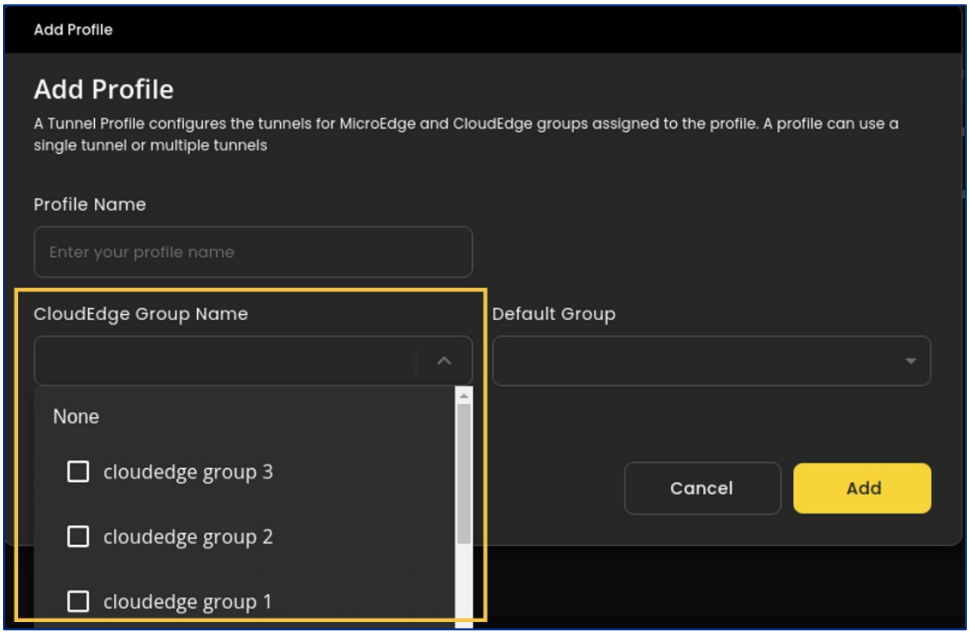

Figure 49 SecEdge User Interface Add a Multi-Tunnel Profile

- Assign that profile to MicroEdge (by device configuration)
- Restart MicroEdge so that ControlEdge can re-setup tunnels

6. SETTINGS

The SecEdge User Interface permits user and enterprise management functions:

+ User information
+ Enterprise profile
+ User management
+ Role management

6.1. ADMIN PROFILES

Users can update their password, Figure 50.

Steps:

+ Select Settings and Admin Profile on the left.
+ Click on the Change Password button.

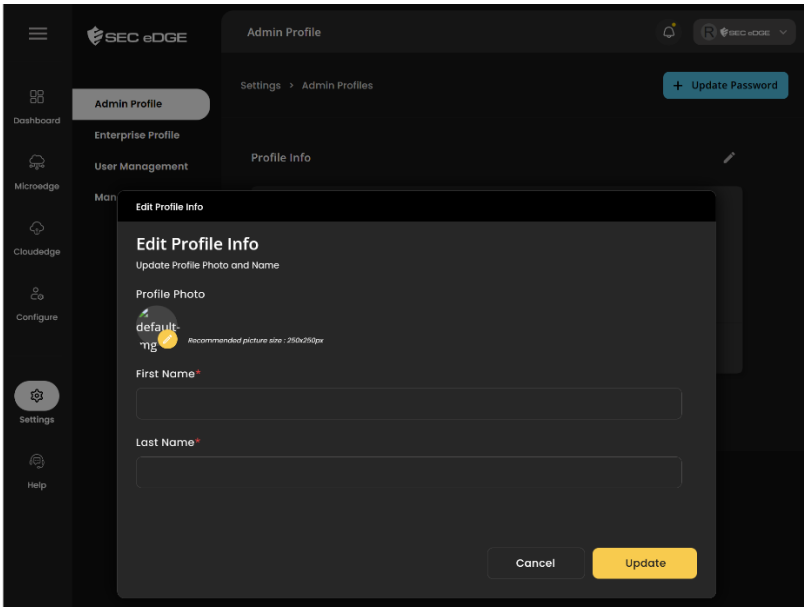

Figure 50 SecEdge User Interface Administrate Enterprise Profiles

6.2. ENTERPRISE PROFILE

A SecEdge Studio admin user can configure and update enterprise information, Figure 51.

Steps:

+ Select Settings and Enterprise Profile on the left.
+ Click on the pencil icon to edit profile.

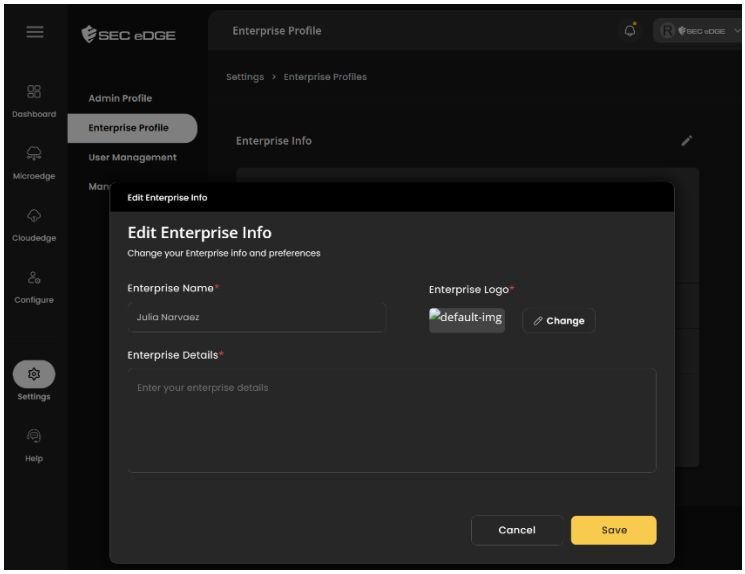

Figure 51 SecEdge User Interface Edit Enterprise Information

6.3. USER MANAGEMENT

A SecEdge Studio admin user can manage other users.

Steps:

+ Select Settings and User Management on the left.
+ To add a user, click on the Add User button Figure 52.
+ To update a user's information, click on the pencil icon of the corresponding user in the list, Figure 53.

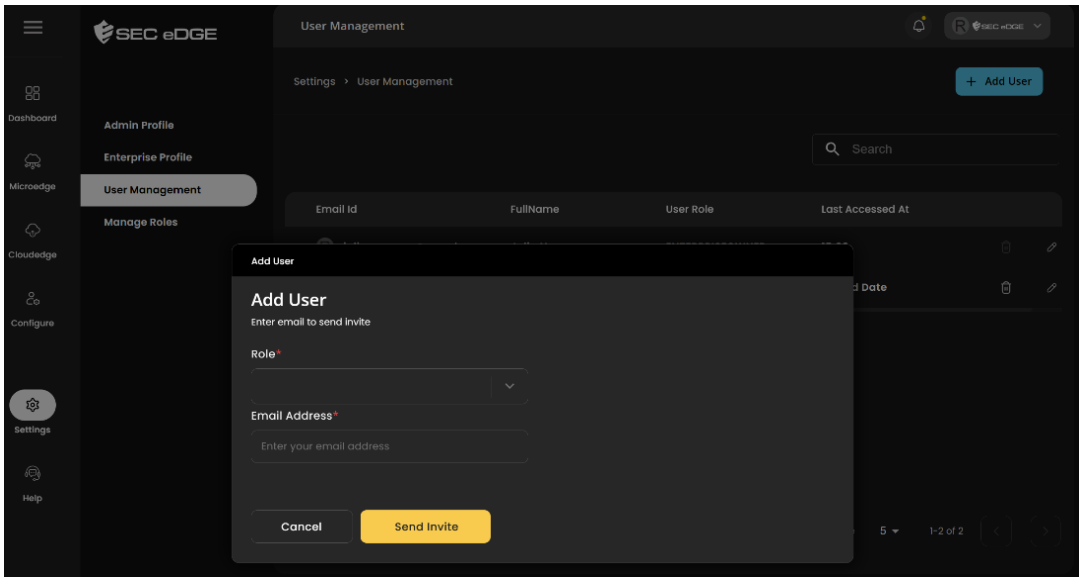

Figure 52 SecEdge User Interface Add User

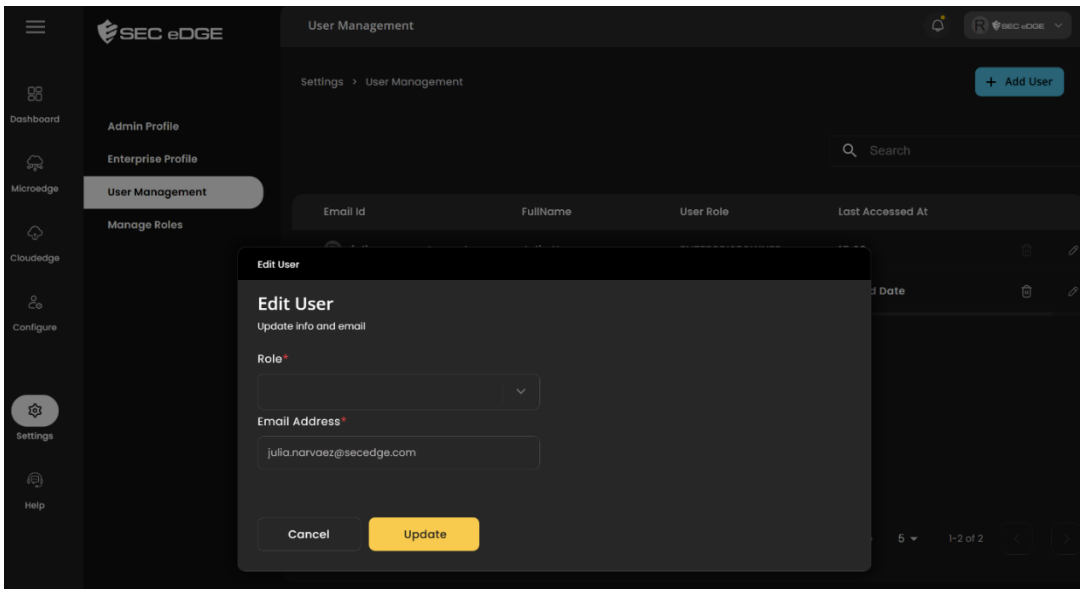

Figure 53 SecEdge User Interface Edit User

6.4. MANAGE ROLES

Configure roles and associate permissions.

Steps:

+ Select Settings and Manage Roles on the left.
+ View list of roles on the page, Figure 54.

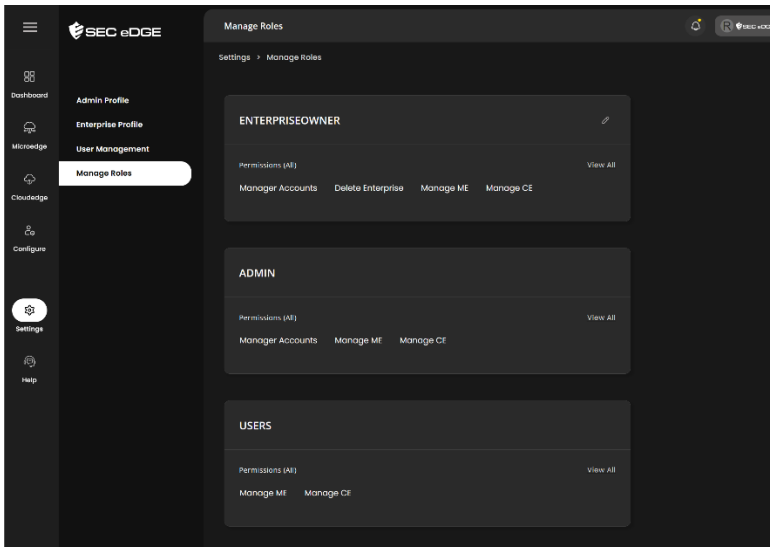

Figure 54 SecEdge User Interface Manage Roles

+ Click on View All for a specific role for list.
+ Click on the pencil icon to add a new role, Figure 55.

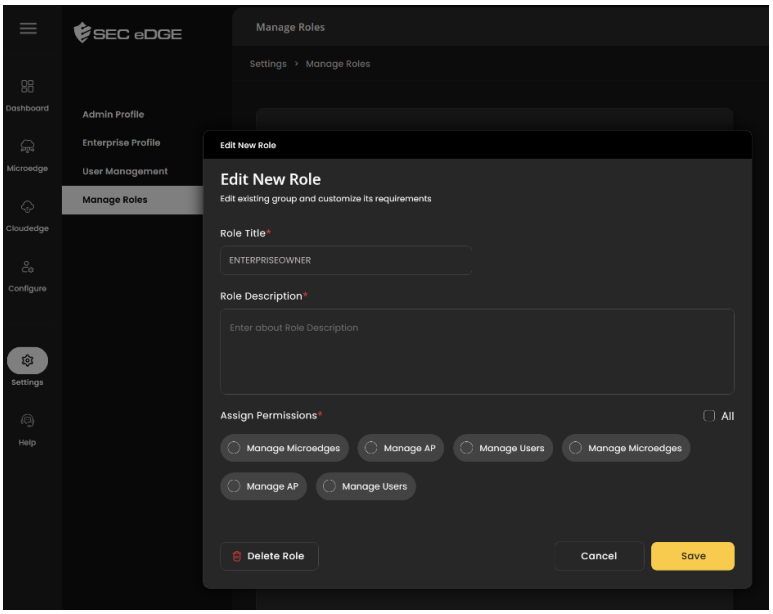

Figure 55 SecEdge User Interface Edit New Role

6.5. CERTIFICATES INFO

Customer generates Day0 certificates used for registration of MicroEdge hardware devices and additional files required to enable activation of MicroEdge devices. Customer designs the approach to generate the Day0 certificates, which may be common for groups of MicroEdge devices. The system generates certificate packages that contain the Day0 certificate and additional files required for device communication.

Certificates can be generated or deleted, as illustrated in Figure 56. Certificate packages can be downloaded only one time, which is on the generation step. In the Certificates Info list, the Common Name corresponds to the Common Name attribute in the Day0 certificate and Key Type is the type of key that customer selected to sign the certificate.

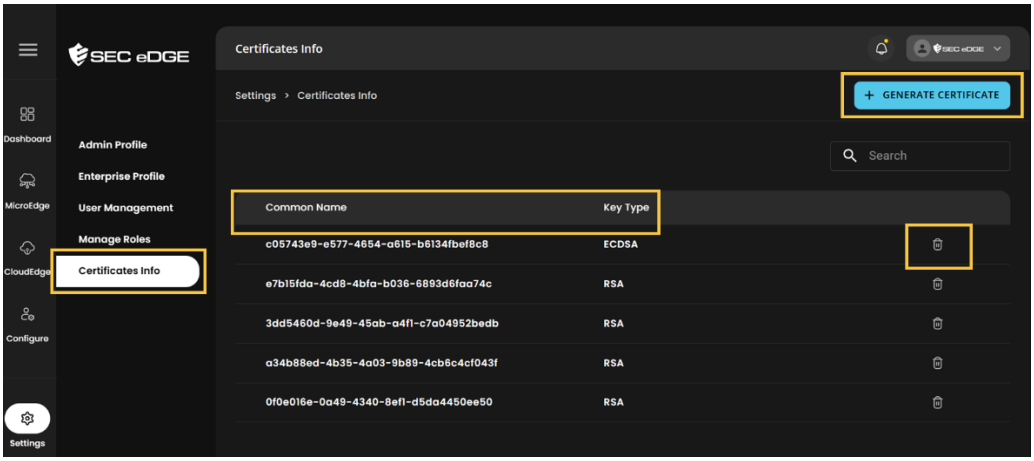

Figure 56 Day0 Certificate Information

6.5.1. GENERATING A DAY0 CERTIFICATE PACKAGE

Steps ,Figure 57 :

1. Select Settings and Certificate Info on the left.
2. To generate a Day0 certificate, click on the Generate Certificate button.
3. Select the certificate type: RSA or ECDSA and click on the Generate button.

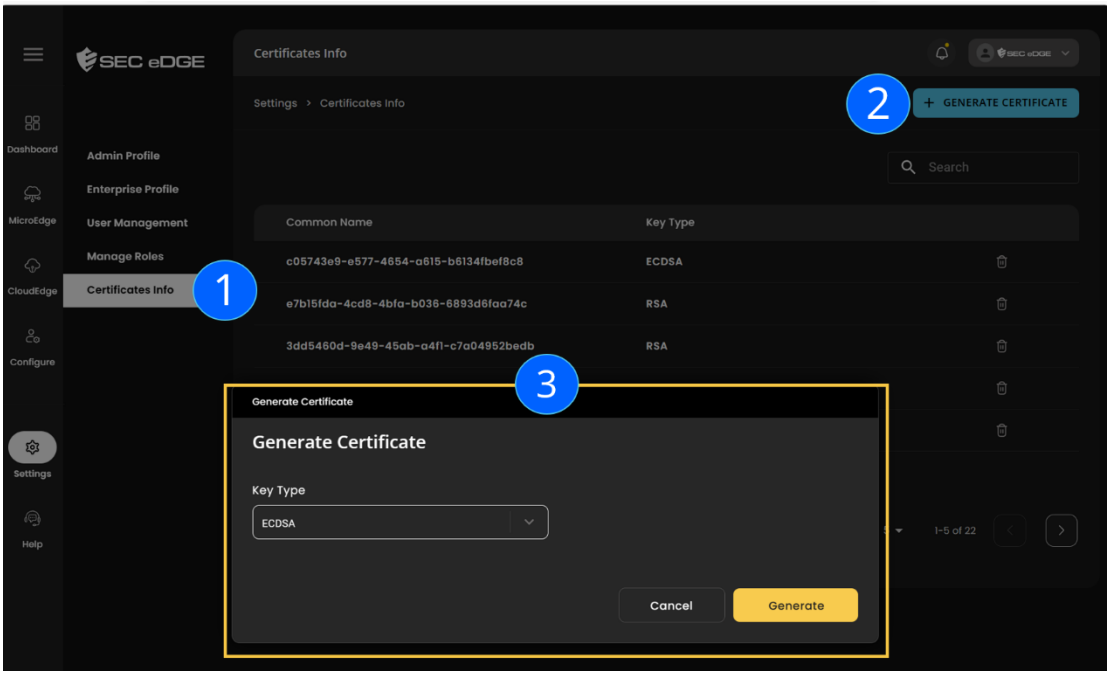

Figure 57 Day0 Certificate Generation

4. The system asks for confirmation and shows the "Certificates Can't Be Downloaded Again" warning, Figure 58, generates the certificate package and shows the download dialog box.

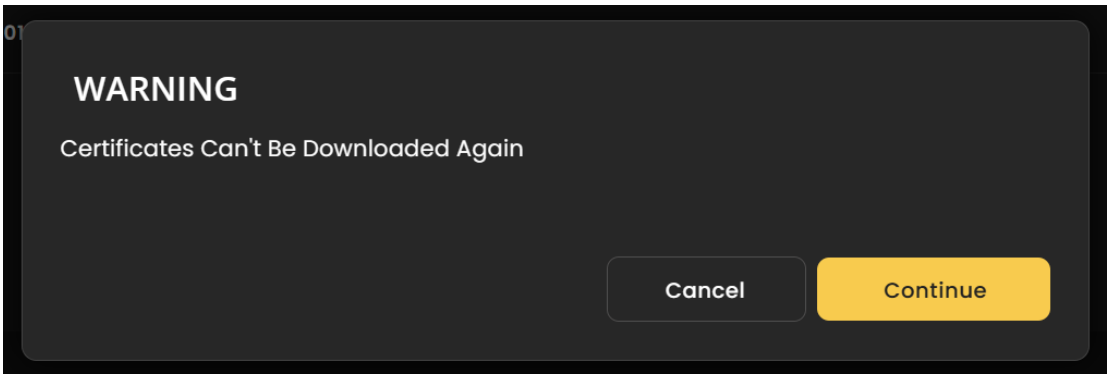

Figure 58 Certificate Package Download

The certificate package is a tarball named as <Day0 certificate common name>.tar. It contains several files used to provision MicroEdge on the device, including:

+ net-edge.cert, Day0 x509 certificate file.
+ net-edge.key, Day0 Private key file.
+ endpoint, file containing the day0 URI of the MQTT broker to use.

6.5.2. DELETING A DAY0 CERTIFICATE

To delete a Day0 certificate click on the basket icon of the corresponding certificate. Deleting the certificate in the list invalidates the Day0 Certificate in the system and prevents activation of devices using it.

RESOURCES

- SecEdge Studio Tutorial, available on the SecEdge website.
- SecEdge Studio Getting Started Guide, available on the SecEdge website.
- SecEdge Studio documentation for specific device hardware, available upon request.