TECHNICAL DOCUMENT

OnBoard™ IoT Security User Manual

Building the trusted foundation for a connected world

Version	V3.4.0
Date	2026-09-10



Version: v3.4.0 (Latest)

Welcome to OnBoard™ IoT Security

Overview

OnBoard™ IoT Security (OBIS) is an authorization-based security platform designed to address the fundamental challenge of scaling secure device provisioning globally while retaining OEM control over cryptographic trust. It is built to protect the integrity, confidentiality, and authorized use of product digital assets. OBIS is delivered as a cloud platform with flexible deployment options to meet different data residency and operational requirements. It is not a PKI service or a factory security system—it is a security control plane that governs how product digital assets may be used across the device manufacturing lifecycle.

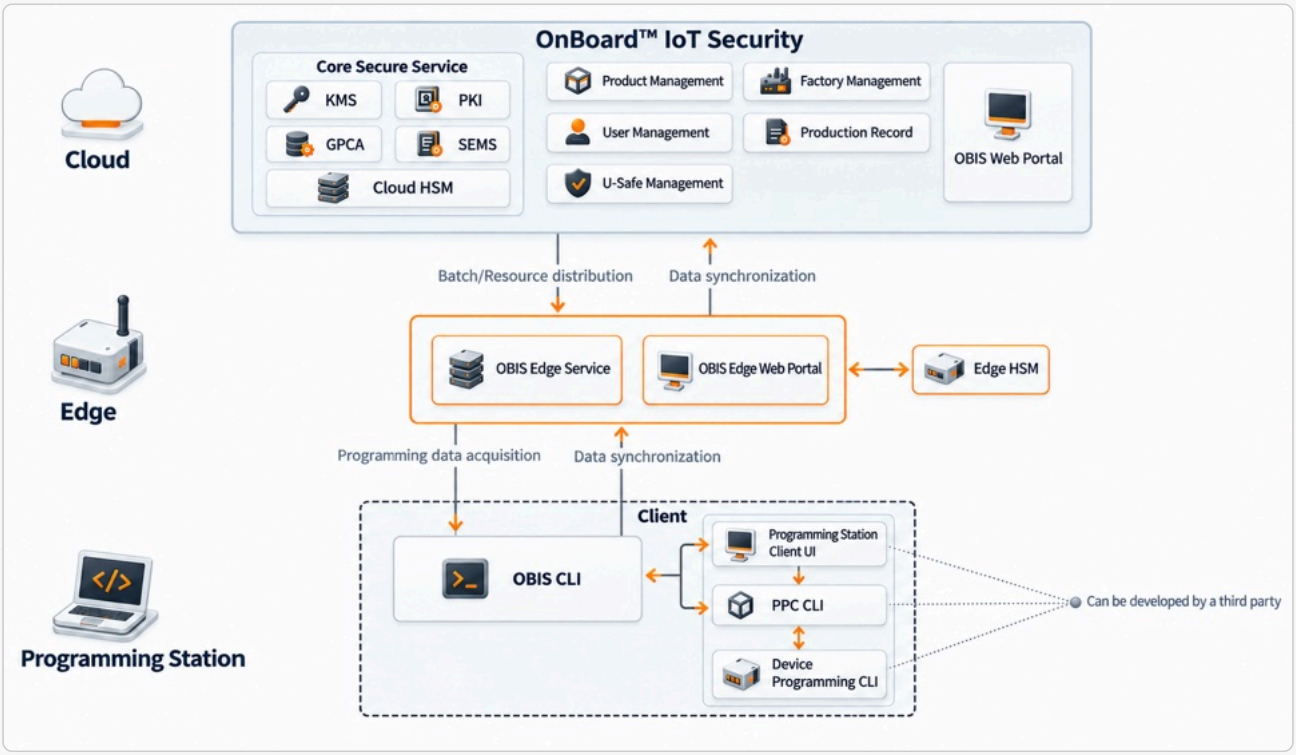
Built on an **authorization-based model** with **centralized control and distributed execution**, OBIS enables OEMs to govern all product digital assets and every security-critical operation across any number of factories and partners, without ever exposing sensitive material.

This architecture enables OEMs to:

- onboard new factories
- switch production partners or silicon suppliers
- scale across regions

All while maintaining centralized control and monitoring. Rather than requiring factories to be trustworthy, OBIS makes trust unnecessary by design.

Product architecture



OBIS consists of three main components: Cloud, Edge, and Programming Station:

Components	Description

Cloud	OnBoard™ IoT Security includes:
	• Core Secure Service, which is responsible for providing fundamental security services and management functions, including:
	  ◦ Key Management System (KMS)
	  ◦ Public Key Infrastructure (PKI)
	  ◦ Cloud Hardware Security Module (HSM)
	  ◦ GlobalPlatform Certificate Authority (GPCA)
	  ◦ Secure Element Management System (SEMS)
	• Product Management
	• Factory Management
	• Production Record
	• User Management
	• U-Safe Management
	• OBIS Web Portal: Users can perform product-related operations and management through the website, such as product management, factory management, user management, key management, and certificate management.

Edge	• OBIS Edge Service: Provides on-site production management capabilities for factories. • OBIS Edge Web Portal: Factory managers can manage on-site operations for factories visually through the website. • Edge HSM: A hardware security device used on production line servers.
Programming Station	OBIS CLI (Command Line Interface), Programming Station Client UI, PPC (Programming Process Control) CLI, and Device Programming CLI are provided by the Client, which are used for executing device programming.

Core features

- **Collaborative Digital Asset Management**

  Configures and manages digital assets with the "Product" as the central unit, OBIS supports multi-role collaboration such as OEM and ODM. Role-based access control ensures the security of digital assets. Through product configuration and task management, OBIS enables full-process collaboration from modeling to pre-mass production. The main functionalities include:

  - Product modeling: Define and maintain basic product information and parameters.
  - Team collaboration: Invite multiple participants, including cross-tenant members, to collaboratively manage products.
  - Resource management: Unified management of resources such as chip parameters, matter configurations, firmware, certificates, and keys.
  - Production programming management: Standardize each production programming task through version control and batch management.

- **Secure Provisioning**

  Provides an end-to-end secure programming process from Cloud configuration to Edge execution, covering key writing, certificate generation, device programming, secure boot, secure debugging, and other critical steps, ensuring that each device's parameters and data are trustworthy and secure during the production phase.

- **Device Lifecycle Management**

  Supports continuous management of programmed devices, offering capabilities such as device status monitoring and secure firmware updates, enabling full lifecycle visibility, controllability, and traceability from production to deployment.

- **Security Infrastructure**

  Provides standard KMS and PKI services, along with GP CA certificate management for GlobalPlatform SCP11c and SEMS configuration asset management for Secure Elements. By integrating with Cloud HSM, it establishes a unified cryptographic security infrastructure and supports the deployment of distributed security services at the Edge (factory side), ensuring end-to-end security for OBIS.

OBIS Positioning and System Boundary

OBIS provides OEMs with a centralized control plane for product digital assets and authorization management—positioned between upstream silicon manufacturing and downstream device lifecycle management.

- **Upstream: Trust Artifact Ingestion**

  OBIS can receive trust artifacts generated during semiconductor manufacturing, such as hardware Root of Trust materials or initial device secrets injected by chip vendors. These artifacts are incorporated into the OEM's product security model and managed consistently alongside other product digital assets within OBIS.

- **Manufacturing: Production Batch Execution**

  OBIS issues explicit Production Batches to OEM-owned or partner-operated factories, defining what may be produced, where, when, and at what scale.

- **Downstream: Trust Artifact Handoff**

  OBIS collects all production outcomes—including per-device security artifacts and immutable production records—and hands them off to OEM-managed or OEM-authorized device management platforms, enabling secure device onboarding and supporting downstream lifecycle operations.

  OBIS is not a factory execution system, a device management platform, or a replacement for MES—it is a centralized product digital asset management and authorization-driven security governance layer—enabling OEMs to coordinate security across all manufacturing partners through a single control plane.

Role classification and permission description

Supports role-based permission management. The current roles are divided into three categories: OBIS roles, product roles, and factory roles. The following six tables describe each role and the corresponding operational permissions.

OBIS roles

OBIS roles are predefined by the system to meet common permission requirements. The following roles can accommodate most usage scenarios, and users can configure one or more roles as needed. For special permission control requirements, please contact Snowball to create corresponding custom roles.

Roles	Description
System Manager	This role has permissions for all roles.
Product Manager	This role has permissions to view and operate the Product Management functional pages.
Resource Manager	This role has permissions to view and operate the KMS and PKI functional pages.
SE Resource Manager	This role has permissions to view and operate the GPCA and SEMS functional pages.
Factory Manager	This role has permissions to view and operate the Factory Management functional pages.
Normal User	This role has permissions to view all functional pages.

The following table summarizes the access and operational permissions of each OBIS role across different functions.

Functions	Permissions	System Manager	Product Manager	Factory Manager	Resource Manager	SE Resource Manager	Normal User
Product	Page Access	✓	✓				✓
	Page Operations	✓	✓				

Functions	Permissions	System Manager	Product Manager	Factory Manager	Resource Manager	SE Resource Manager	Normal User
Factory	Page Access	✓		✓			✓
	Page Operations	✓		✓			
Records	Page Access	✓	✓	✓	✓	✓	✓
KMS	Page Access	✓			✓		✓
	Page Operations	✓			✓		
PKI	Page Access	✓			✓		✓
	Page Operations	✓			✓		
GPCA	Page Access	✓					
	Page Operations	✓				✓	
SEMS	Page Access	✓				✓	
	Page Operations	✓				✓	

Functions	Permissions	System Manager	Product Manager	Factory Manager	Resource Manager	SE Resource Manager	Normal User
Account	Page Access	✓				✓	
	Page Operations	✓					
Group	Page Access	✓	✓				
	Page Operations	✓	✓				

Product roles

Product roles are designed to control access and operational permissions of product resources. Users can configure one or more roles as needed.

Roles	Description
Product Owner	This role defaults to the product creator, with full operational permissions for the product.
Product Manager	This role has full access to all product operations.
Resource Manager	This role has permissions to view the product and manage its resources.
Version Manager	This role has permissions to view the product and manage its versions.
Batch Manager	This role has permissions to view the product and manage its batches.

Roles	Description
Member	Default user role, with permission to view the product.

The following table summarizes the operational permissions of each role for the Product function.

Functions	Operations	Product Owner	Product Manager	Resource Manager	Version Manager	Batch Manager	Member
Product	Configure a product	✓	✓	✓			
	Check products	✓	✓	✓	✓	✓	✓
	Manage products	✓	✓				
	Create a version	✓	✓		✓		
	Check versions	✓	✓	✓	✓	✓	✓
	Manage versions	✓	✓		✓		
	Create a batch	✓	✓			✓	
	Check batches	✓	✓	✓	✓	✓	✓
	Check programmed devices	✓	✓	✓	✓	✓	✓
	Check logs	✓	✓	✓	✓	✓	✓

Functions	Operations	Product Owner	Product Manager	Resource Manager	Version Manager	Batch Manager	Member
	Manage members	✓	✓				

Factory roles

Factory roles are designed to manage and handle factory-related business, and can be configured (local factory & cloud factory by users as needed.

Role	Description
Factory Admin	This role defaults to the factory creator, with full operational permissions for the factory on both Cloud and Edge.
Factory Manager	This role has full access to all factory operations on both Cloud and Edge.

The following table summarizes the operational permissions of the Factory Admin and Factory Manager on both Cloud and Edge.

Components	Functions	Factory Type	Operations	Factory Admin	Factory Manager
Cloud	Factory	Local factory & Cloud factory	Create a factory	✓	✓
		Local factory & Cloud factory	Configure and manage factories	✓	✓
		Local factory & Cloud factory	Configure and manage programming stations	✓	✓
		Cloud factory	Manage batches and assign programming stations	✓	✓

Components	Functions	Factory Type	Operations	Factory Admin	Factory Manager
		Local factory & Cloud factory	Check factories	✓	✓
Edge	Factory	Local factory	Manage factories	✓	✓
	Station	Local factory	Configure and manage programming stations	✓	✓
	Batch	Local factory	Manage batches and assign programming stations	✓	✓

Version: v3.4.0 (Latest)

Register and sign in to OnBoard™ IoT Security

Welcome to Snowball OnBoard™ IoT Security (OBIS)! This article will guide you to quickly complete the OBIS account registration and sign-in, so that you can start using the OBIS functions immediately. Please follow the steps below:

Step one: Register an OBIS account

Please contact us with the following information, and we will assist you in completing your OBIS account registration:

- Company Name
- Name
- Email

After you submit the information, we will contact you as soon as possible to complete the registration process.

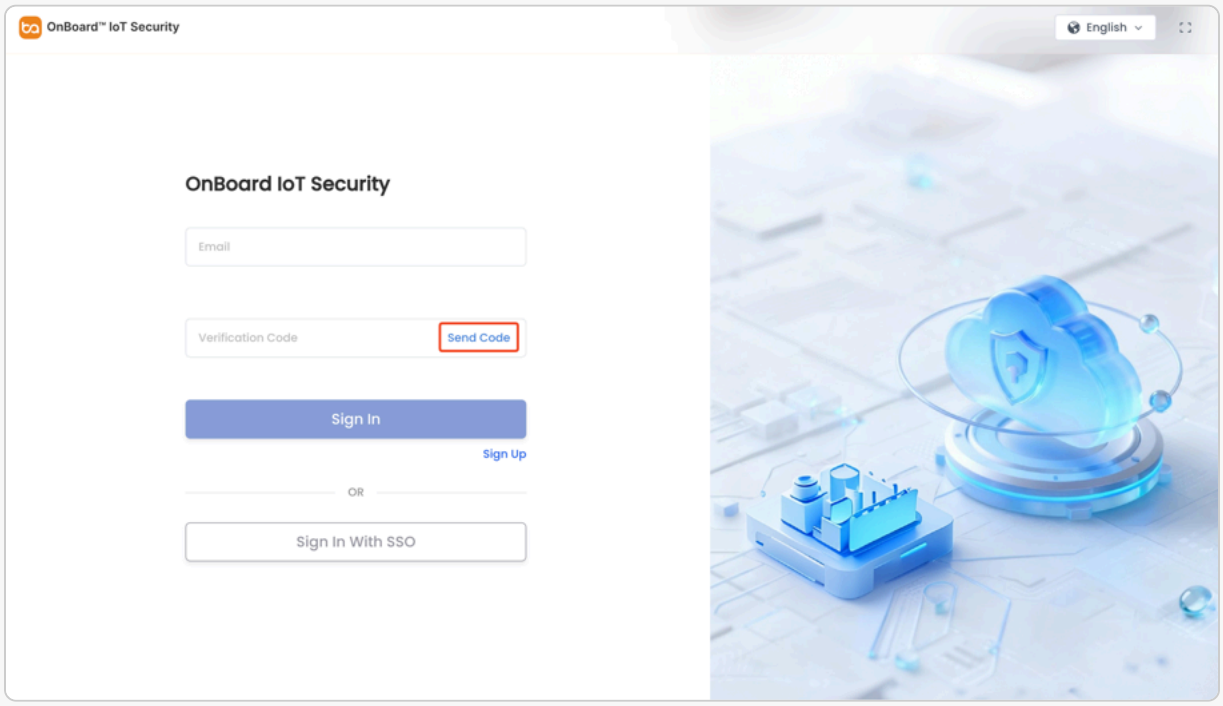
Step two: Sign in to OBIS

After the account is registered, you can sign in using either a verification code or the SSO (Single Sign-On) method:

Method one: Verification code

> **TIP**
>
> You can contact Snowball to enable the enterprise **Self-Registration** feature, allowing users to sign up accounts on the OBIS sign-in page using their company email and sign in with a verification code. OBIS will automatically assign default role permissions to them.

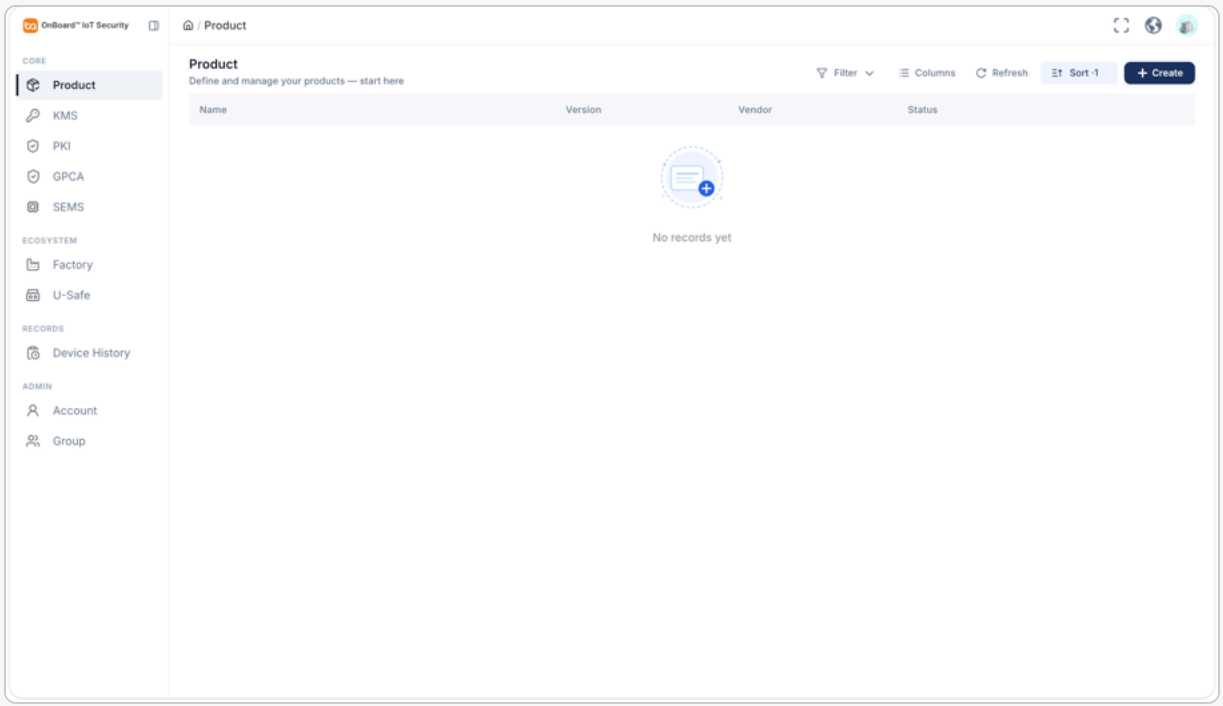
1. On the OBIS sign-in page, enter the email you provided when registering for the OBIS account, and then click **Send Code**.



2. Sign in to your email, check the verification email from OBIS which contains a six-digit verification code.

3. On the OBIS sign-in page, enter the six-digit verification code you received in your email, and then click **Sign In**.

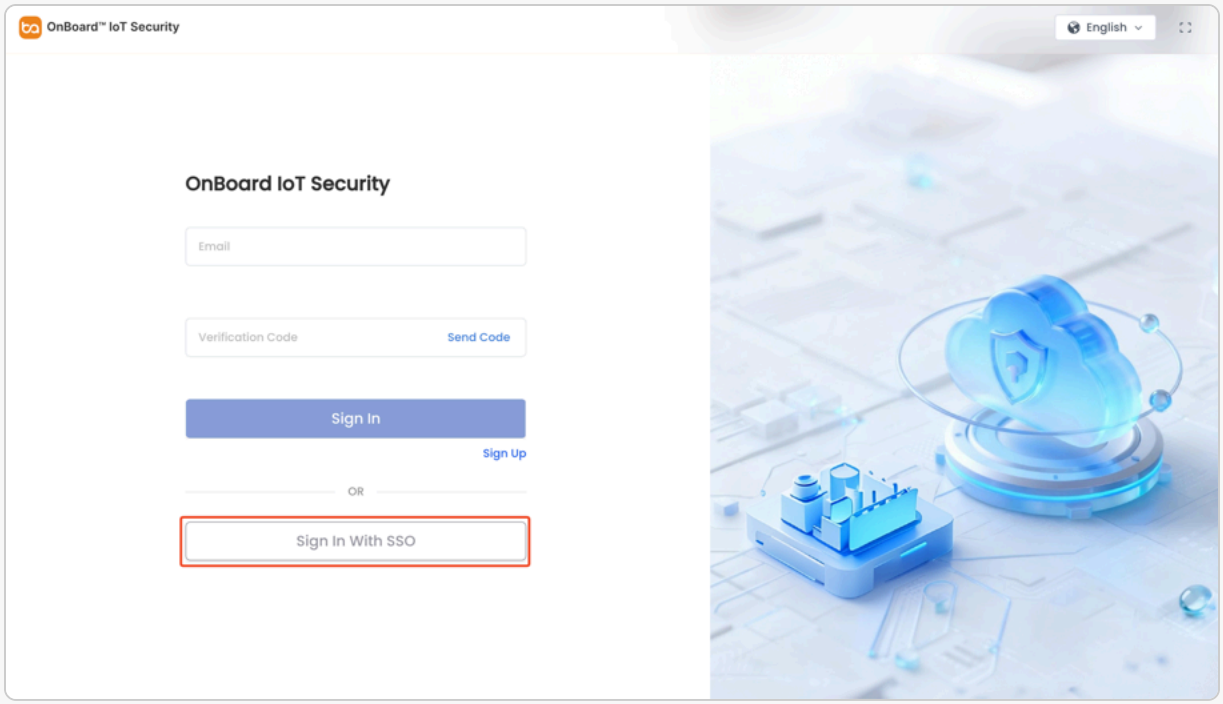
4. After a successful sign-in, the page will navigate to the OBIS home page.



Method two: SSO

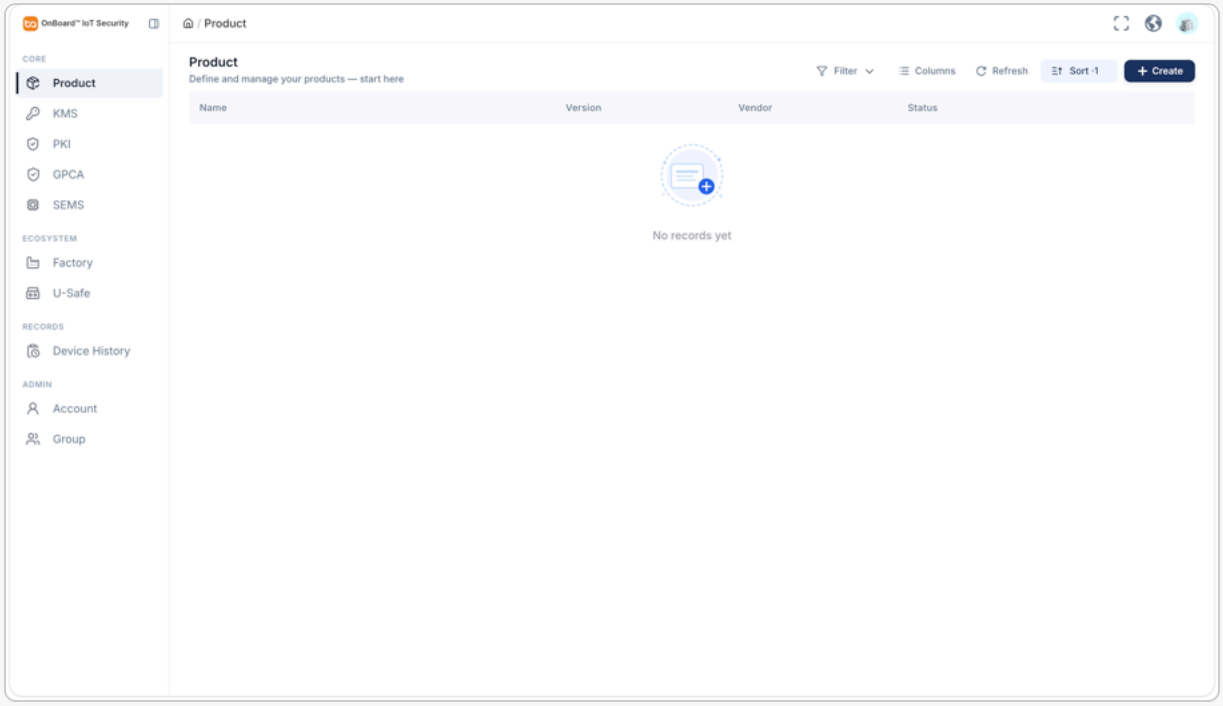
> **TIP**
>
> You can contact Snowball to enable the **Sign In with SSO** feature, allowing users to sign in with their company email through the Enterprise Identity Provider (IdP). OBIS will automatically create an account for them and assign default role permissions. For more information, refer to Configure Sign in with SSO.

1. On the OBIS sign-in page, select **Sign In With SSO**.



2. Enter your company email and then click **Next**, the page will navigate to the enterprise IdP authentication page.

3. After successful authentication, the page will navigate to the OBIS home page.


OnBoard™ IoT Security
/ Product
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
Product
Define and manage your products — start here
Filter
Columns
Refresh
Sort · 1
+ Create
Name
Version
Vendor
Status
No records yet

Version: v3.4.0 (Latest)

Product creation and device programming

Welcome to OnBoard™ IoT Security (OBIS)! This article provides a quick-start guide for the following steps:

- Creating and configuring a product
- Creating a version and batch
- Assigning a programming station to the batch and completing device programming

By following these steps, you'll quickly get started with OBIS and complete the entire process—from product creation to device programming.

Prerequisites

Before starting product creation and device programming, ensure that the following conditions are met:

- Your account has the permissions to complete the process—from product creation to device programming in OBIS.
- Contact Snowball to obtain the HSM U-Safe and Identity U-Safe.
- You have completed the creation and configuration of the factory. For detailed instructions, refer to the following steps:

- Creating a factory
- Configuring a factory (local factory & cloud factory)
- Configuring a programming station (local factory & cloud factory)

Operational diagram

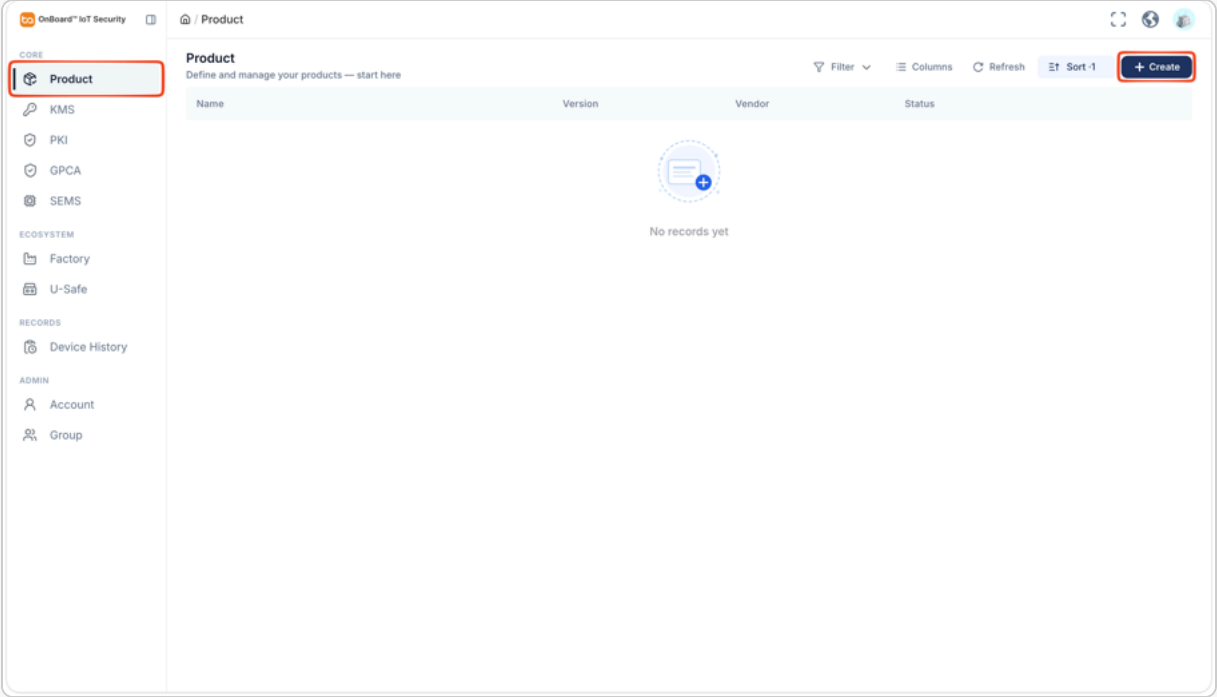


Step one: Create and configure a product

Refer to the steps below to create and configure your product in OBIS:

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then click **Create**.

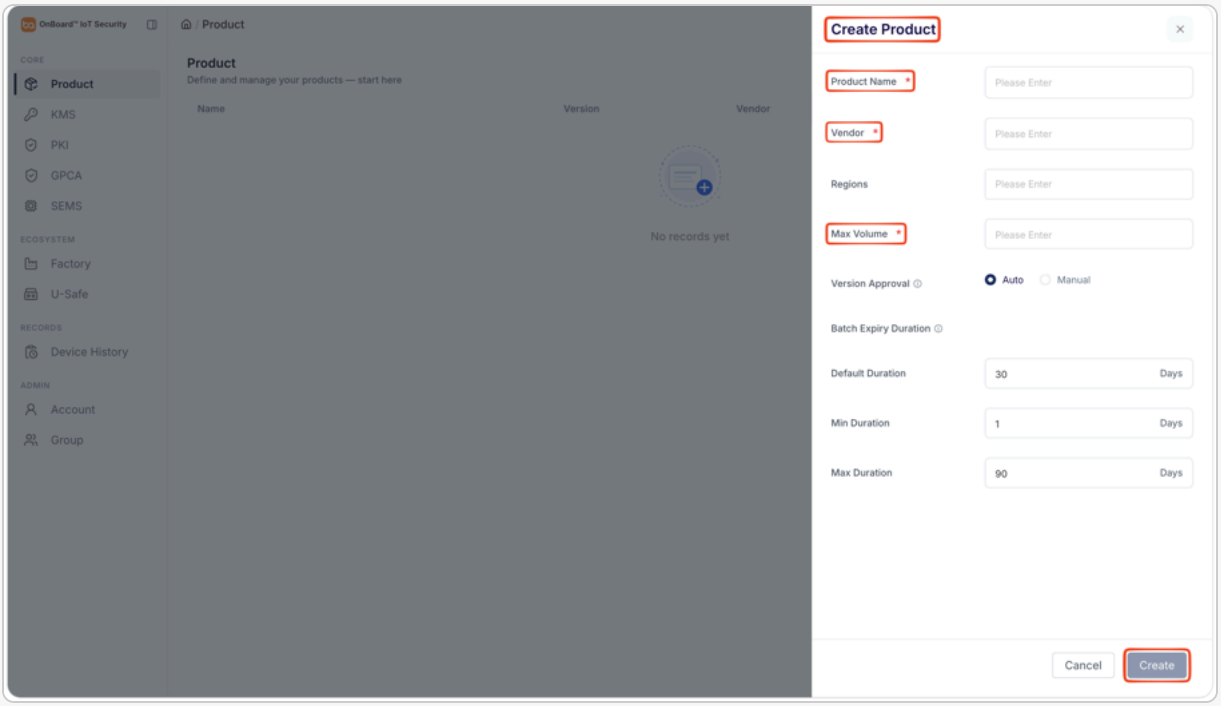


3. On the **Create Product** panel, enter the required basic information:

    - **Product Name**
    - **Vendor**
    - **Max.Volume**

    Then, click **Create**. After your product is created, the page will navigate to the product page.

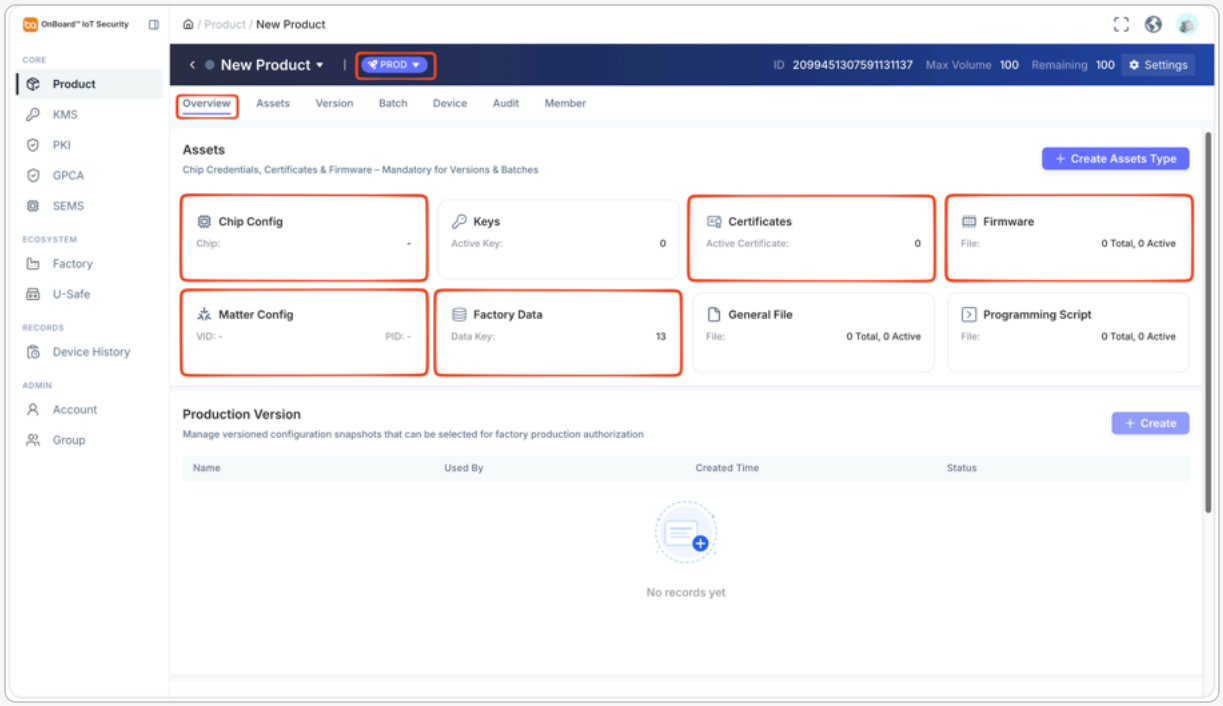
> **NOTE**
>
> For more information, refer to the description of product basic information.



4. Select either the **TEST** or **PROD** environment on the product page, select the **Overview** tab, locate the **Assets** section. Then, select and configure the required assets:

    - **Chip Config**
    - **Certificates**
    - **Firmware**
    - **Matter Config**
    - **Factory Data**

> **TIP**
>
> The configurations of the **Assets** section will be used for version and batch creation. For more information, refer to the steps for configuring a product.



Chip Config | Certificates | Firmware | Matter Config | Factory Data

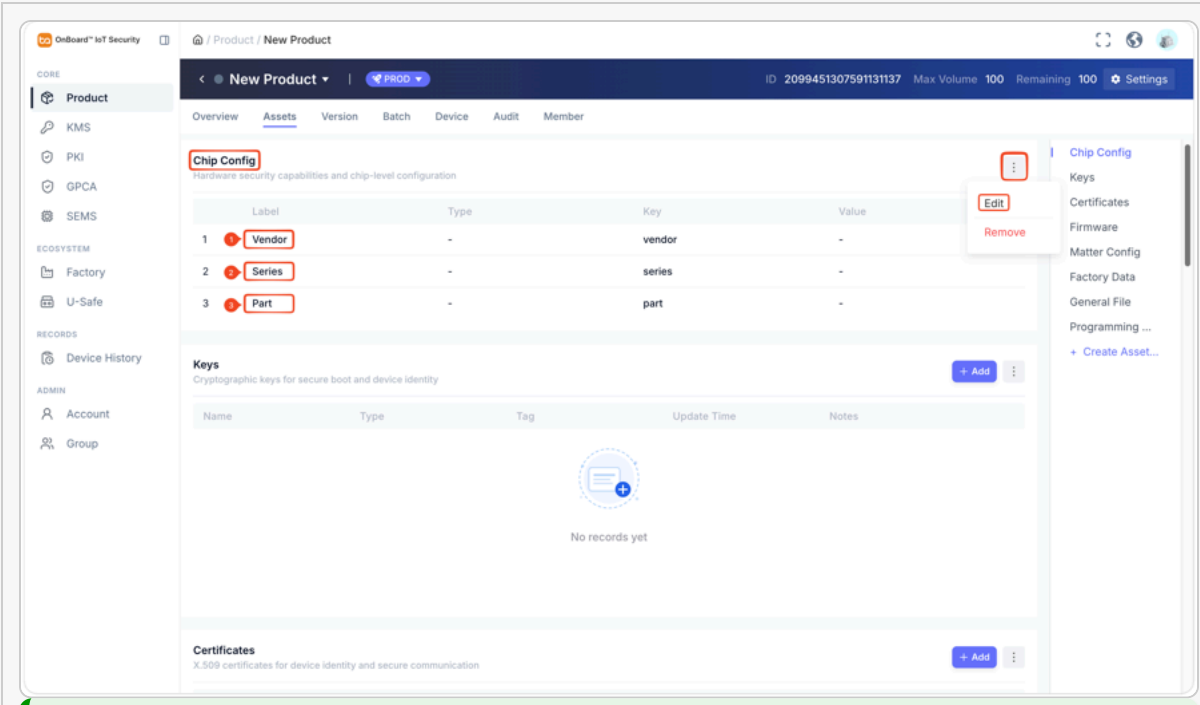
TIP

Chip Config allows you to select the chip part and security options used by your product.

Please refer to the supported chip settings for the current list. Additional chip vendors, series, and parts will be added based on demand.

For more information, refer to the steps for setting Chip Config.

In the **Chip Config** section, click the Options ⋮ icon and then select **Edit**. Select the **Vendor**, **Series**, and **Part**, and then click **Save**.

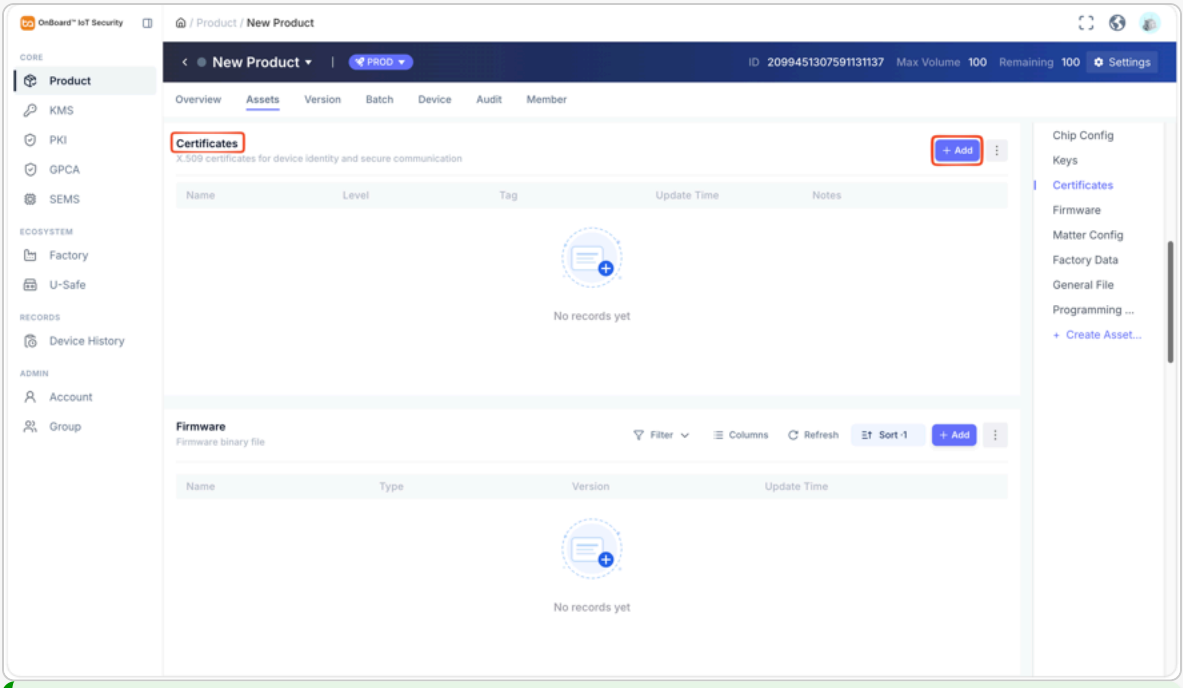


TIP

Certificates allows you to add a DAC template from PKI to your product, making it available for selection during the Matter Config.

DAC templates can be created in PKI. For more information, refer to the steps for creating a certificate.

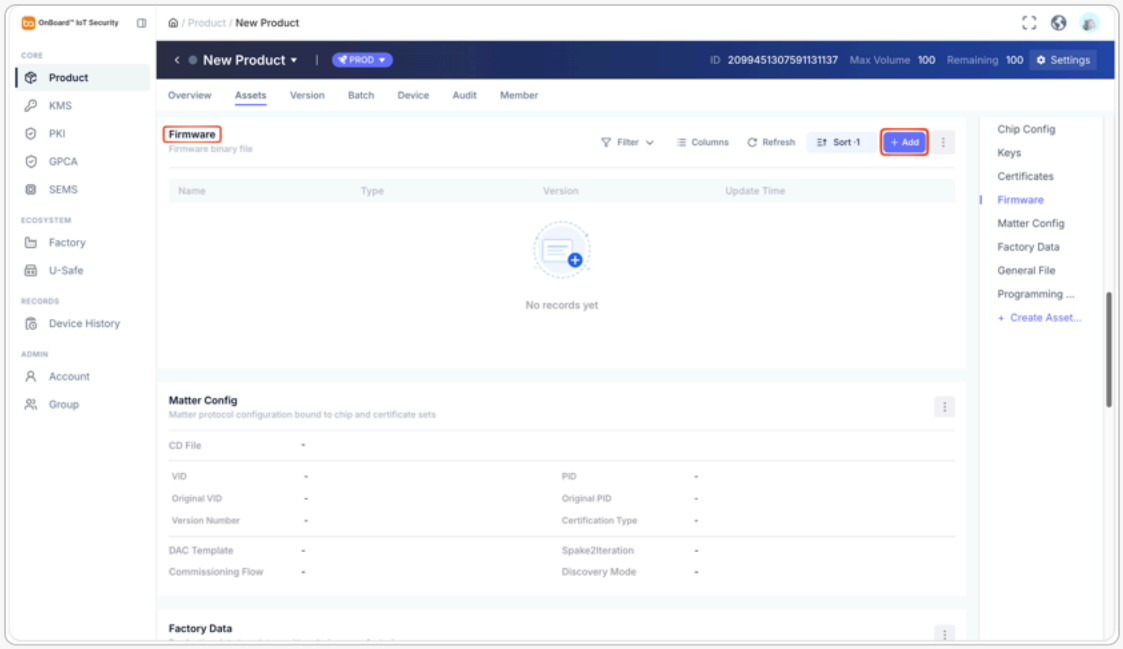
In the **Certificates** section, click **Add**. Then, select the certificate to be assigned and click **Add**.



TIP

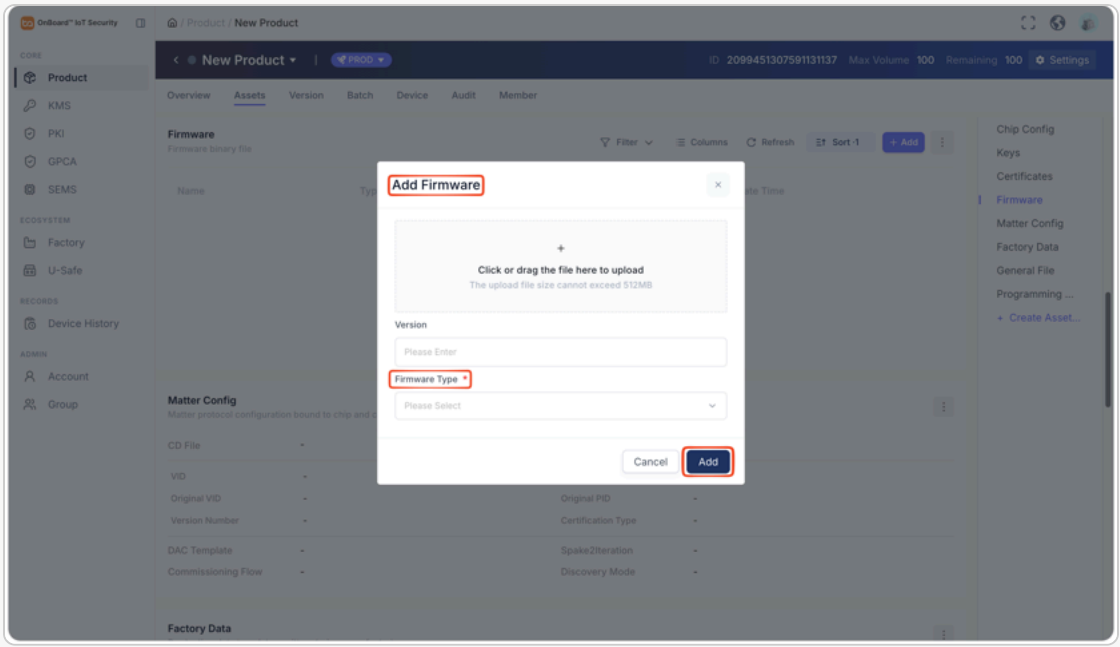
Firmware allows you to upload the firmware files required for programming the product. Firmware formats supported: **.bin**, **.hex**, and **.s37**. Then, the uploaded firmware can be selected when creating a version. You may upload firmware as needed.

i. In the **Firmware** section, click **Add**.



ii. In the **Add Firmware** window, upload the firmware files and select **Firmware Type** (**Application** or **Bootloader**), and then click **Add**.

> **NOTE**
>
> For more information, refer to the description of Firmware information.



TIP

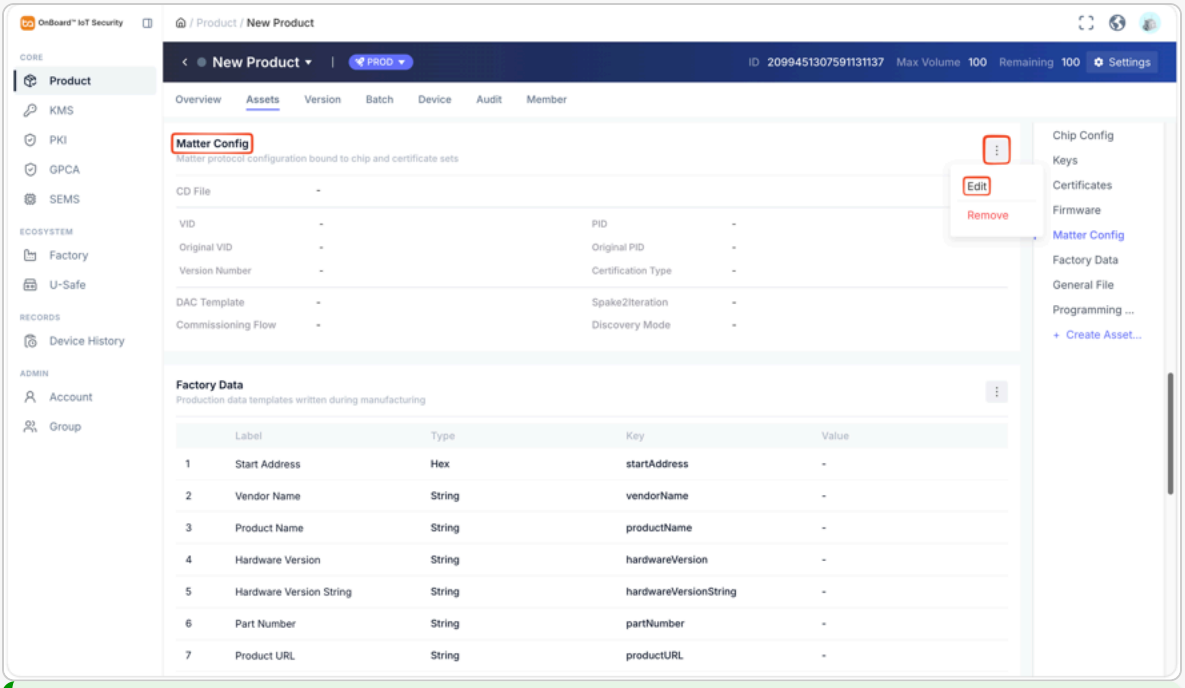
Matter Config allows you to select and configure settings related to the Matter protocol.

In this step, you need to upload the CD file and select the DAC template that was added when configuring Certificates. Please ensure that the VID (Vendor ID) and PID (Product ID) in the CD file match those in the DAC template.

You can replace the CD file as needed when creating a version later.

For more information, refer to the description of Matter Config information.

In the **Matter Config** section, click the Options ⋮ icon and then select **Edit**. Click **Upload File** to select and upload the CD file. Then, select **DAC Template**, **PID**, **Commissioning Flow**, **Spake2Iteration**, and **Discovery Mode**, and click **Save**.

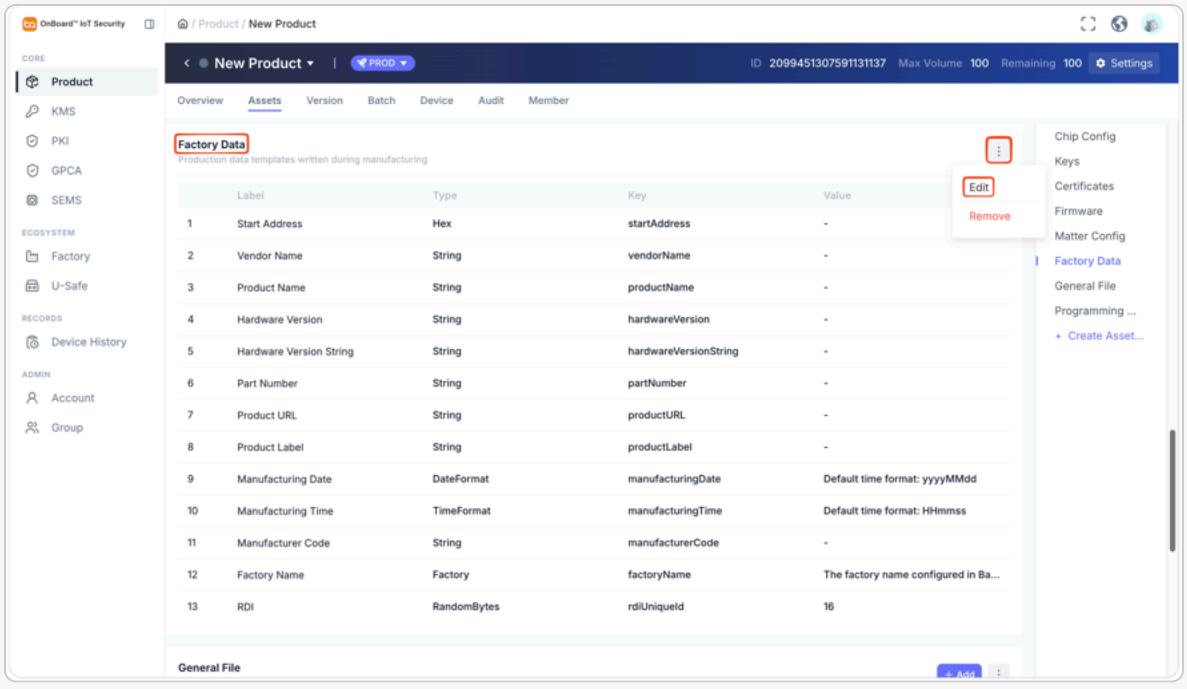


TIP

Factory Data allows you to configure factory-related information and supports all fields required by the Matter specification. You can update the Factory Data as needed when creating a version later.

The Factory Data selected here will be used as a required field when creating a version. For more information, refer to the description of Factory Data information.

In the **Factory Data** section, click the Options ⋮ icon and then select **Edit**. Enter the Factory Data for your product (values can be left empty), and then click **Save**.



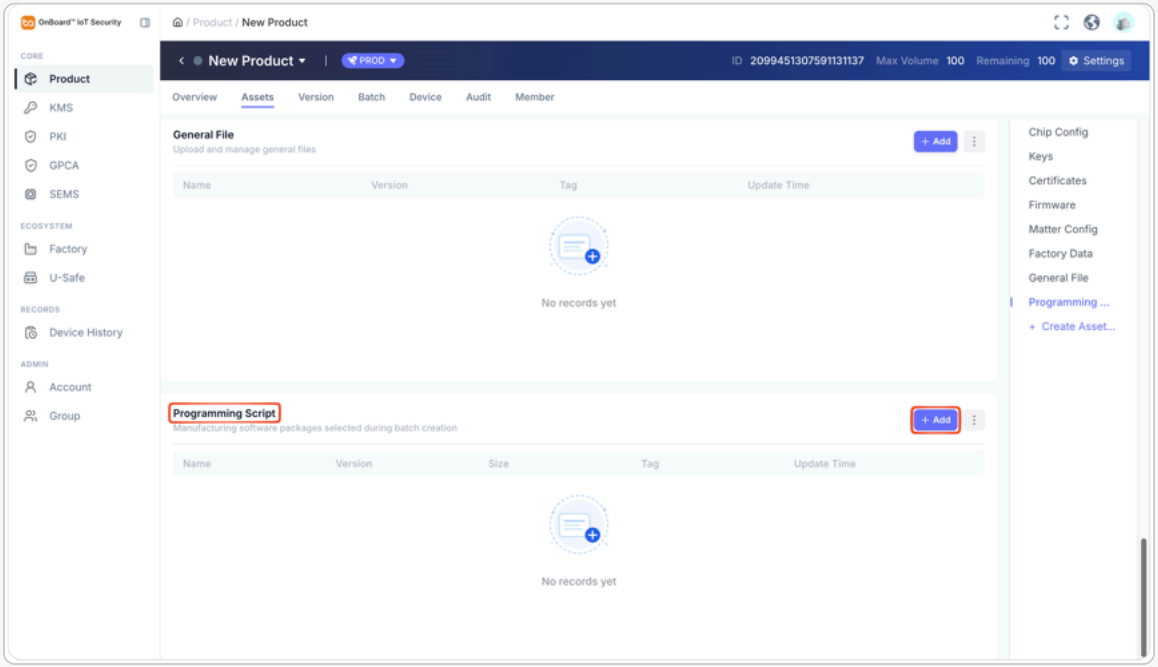
5. In the **Programming Script** section of the **Assets** tab, upload the corresponding files.

> **NOTE**
>
> Files in the **Programming Script** section will be used for batch creation. For more information, refer to the steps for configuring Programming Script.

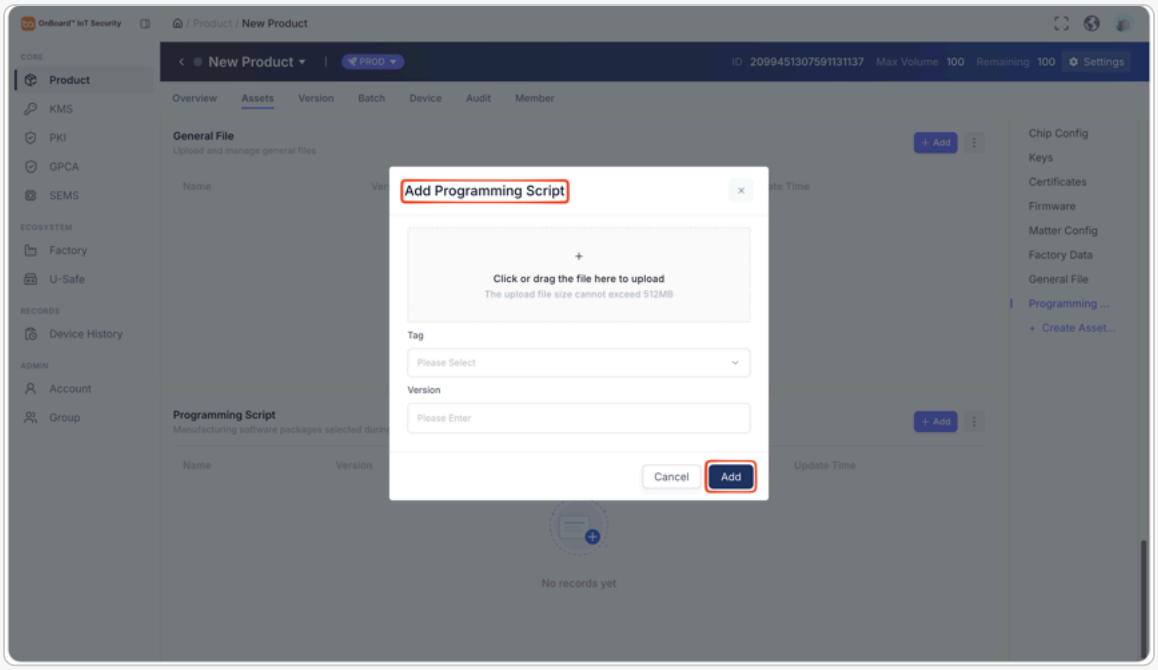
For example, refer to the steps below to upload a programming script.

> **TIP**
>
> **Programming Script** allows you to upload script files used for device programming (any script format is supported). The uploaded programming script can be selected when creating a batch.
>
> You can select and upload the programming script as needed. If it is not required at the moment, you can also select it for a specific batch later in the Programming Station client.

i. In the **Programming Script** section, click **Add**.



ii. In the **Add Programming Script** window, upload the script file and click **Add**.



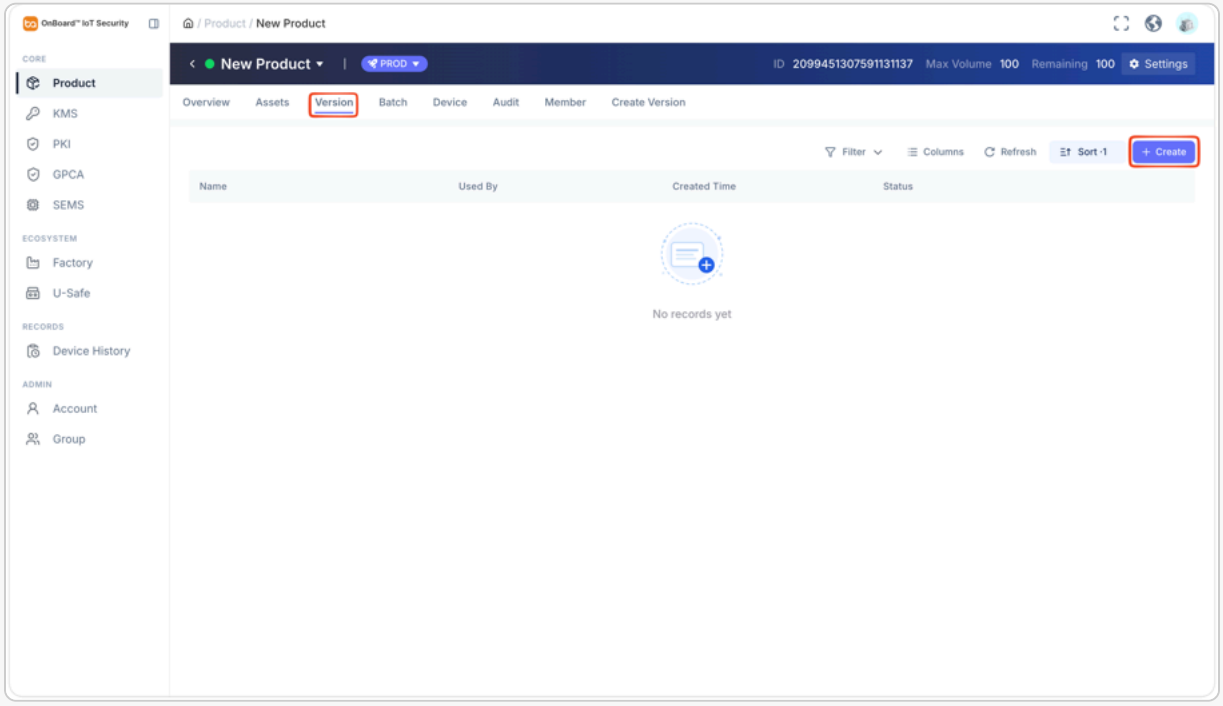
Step two: Create a version

> **TIP**
>
> Each product can create multiple versions.

After your product is created and configured, refer to the steps below to create a version in OBIS:

1. On the product page, select the **Version** tab, and then click **Create**. The page will navigate to the **Create Version** tab.

> **TIP**
>
> If the **Create** button appears grayed out, it is currently unavailable. Please check whether all required assets for your product have been configured. Once everything is properly configured, the **Create** button will be enabled automatically.



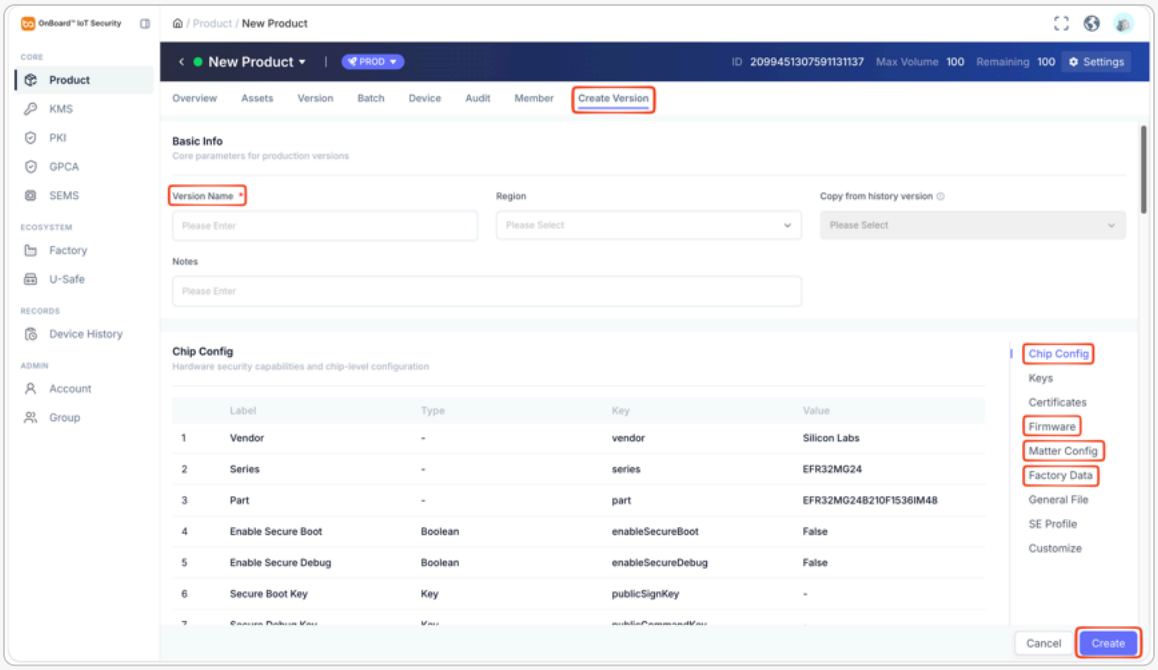
2. On the **Create Version** tab:

> **NOTE**
>
> For more information, refer to the description of version information.

   i. Enter the **Version Name**.

   ii. Check the information in the **Chip Config**, **Firmware**, **Matter Config**, and **Factory Data** sections.

iii. Click **Create**. After the version is created, the page will navigate to the **Version** tab.



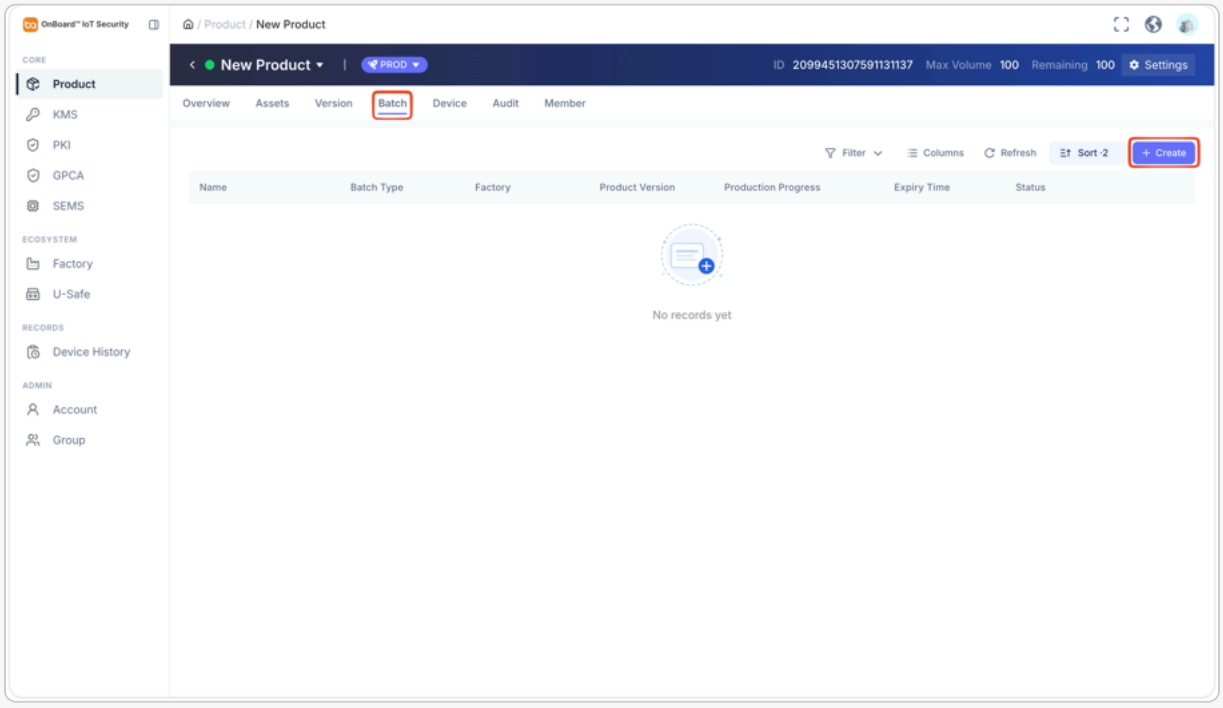
Step three: Create a batch

> **TIP**
>
> Each version can create multiple batches, and a batch represents a production plan based on that version.

After the version is created, refer to the steps below to create a batch in OBIS:

1. On the product page, select the **Batch** tab, and then click **Create**. The page will navigate to the **Create Batch** tab.

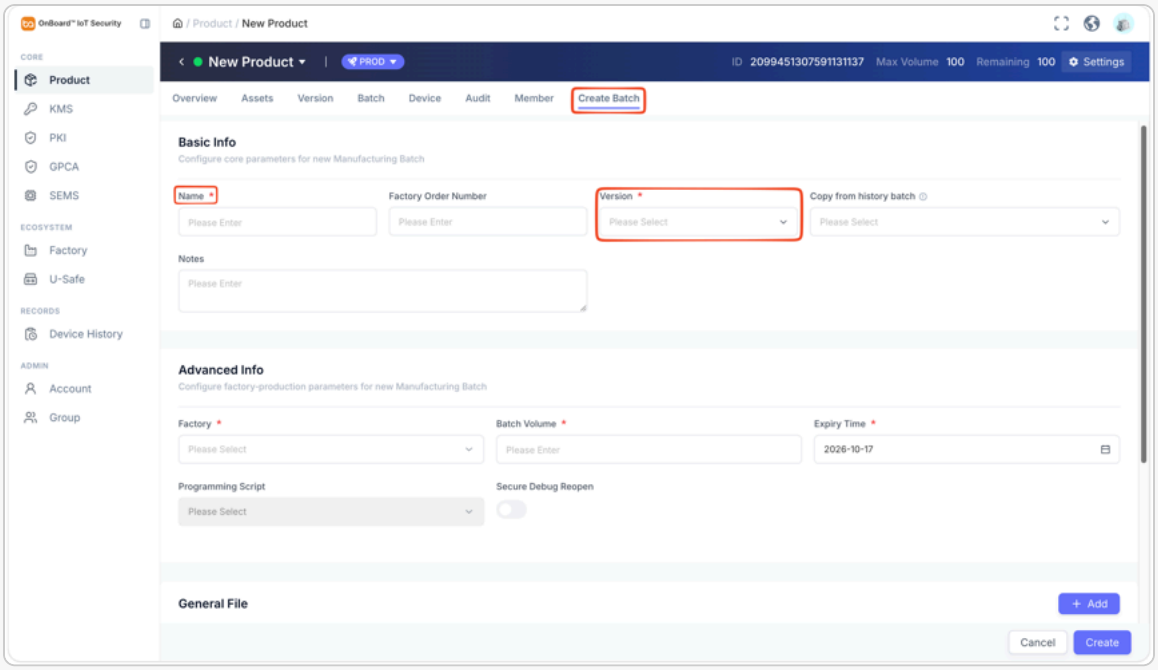
> **TIP**
>
> If the **Create** button appears grayed out, it is currently unavailable. Please check whether a version has been created. After a version is created, the **Create** button will be enabled automatically.



2. On the **Create Batch** tab:

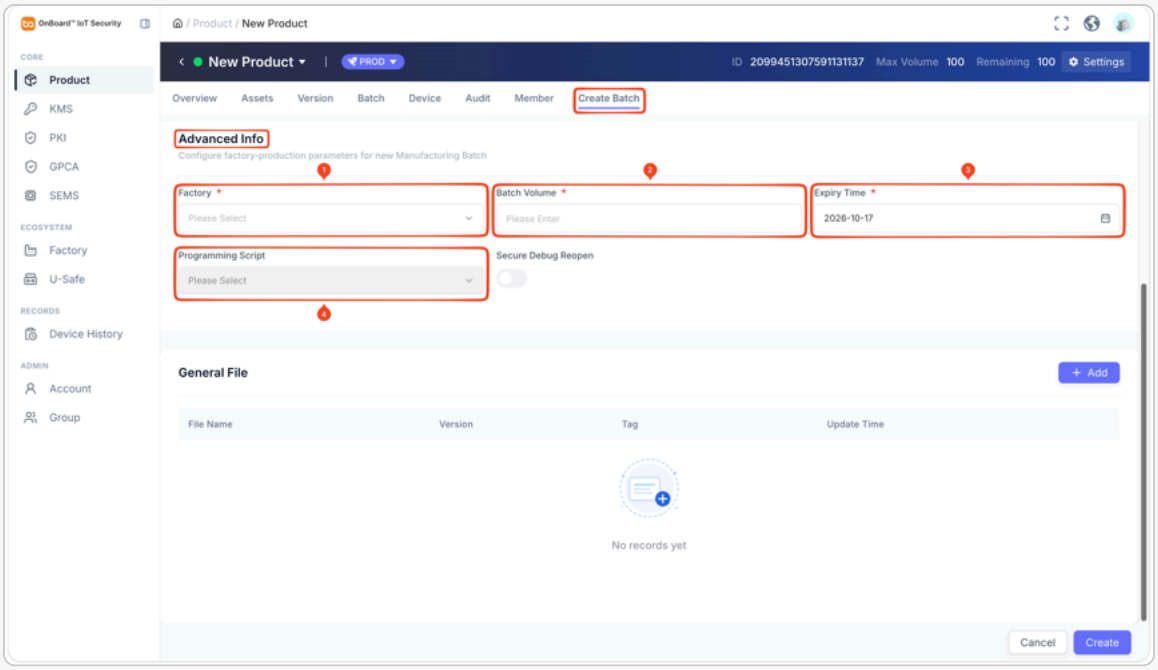
> **NOTE**
>
> For more information, refer to the description of batch information.

   i. Enter the batch name, select the version created in step two.



ii. In the **Advanced Information** section:

- Select the **Factory**
- Enter the **Batch Volume**
- Set the **Expiry Time**
- Select the **Programming Script** (add the programming script uploaded when configuring your product as needed. If it is not required at the moment, you can select the programming script for a specific batch later in the Programming Station client).



iii. Click **Create**. After the batch is created, the page will navigate to the **Batch** tab.

Step four: Assign a programming station to the batch

> **TIP**
>
> The purpose of assigning a programming station to a batch is to bind the production plan to a programming station.

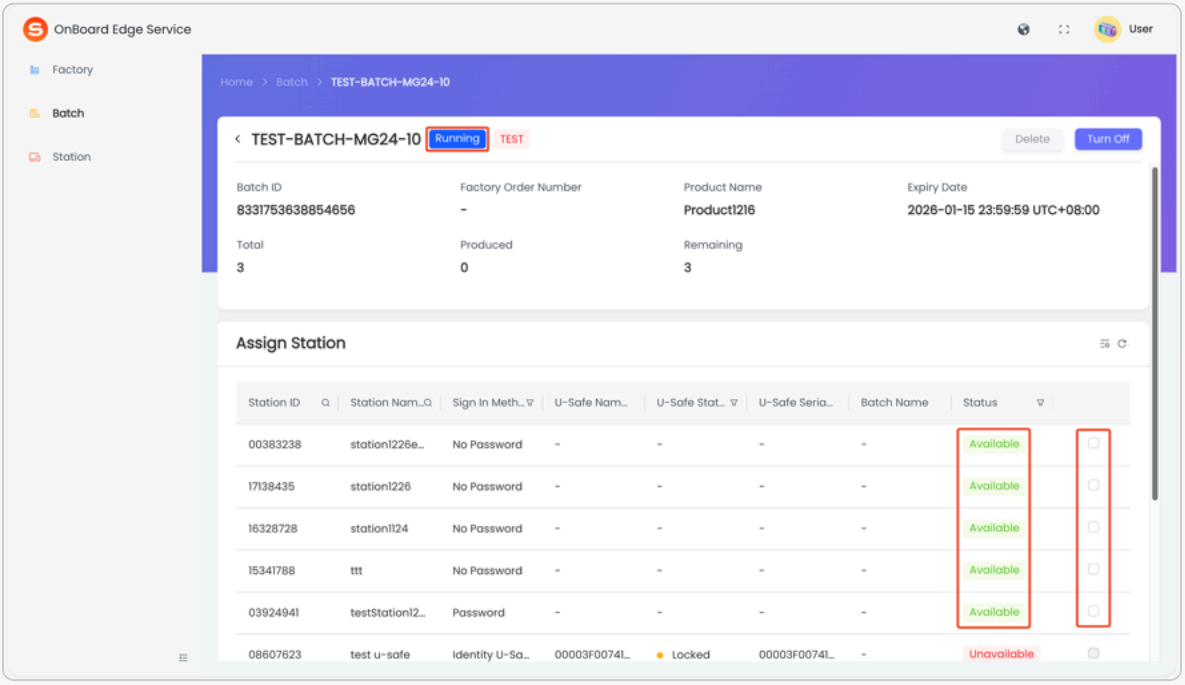
Local Factory | Cloud Factory

Contact Snowball for assistance in deploying the OnBoard Edge Service on the factory side.

After the deployment is complete, you can sign in to the OnBoard Edge Service using the generated service address to manage factories, programming stations, and batches:

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Batch**, and then select the batch created in step three from the **Batch List**.
3. On the batch page, verify that the batch status is **Running**, and then select a programming station with the **Available** status for assignment.

> **NOTE**
>
> For more information, refer to the steps for adding a programming station.

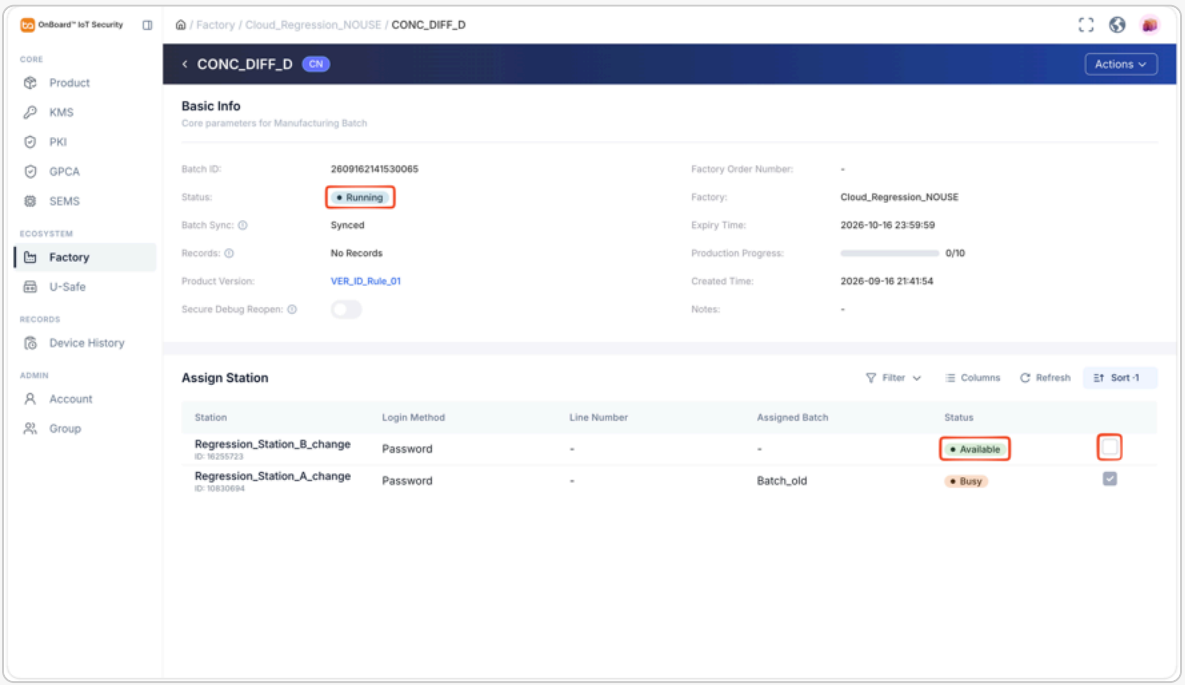


1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page and select the **Batch** tab.

3. Select the batch created in step three, verify that the batch status is **Running**, and then select a programming station with the **Available** status for assignment.

> **NOTE**
>
> For more information, refer to the steps for adding a programming station.

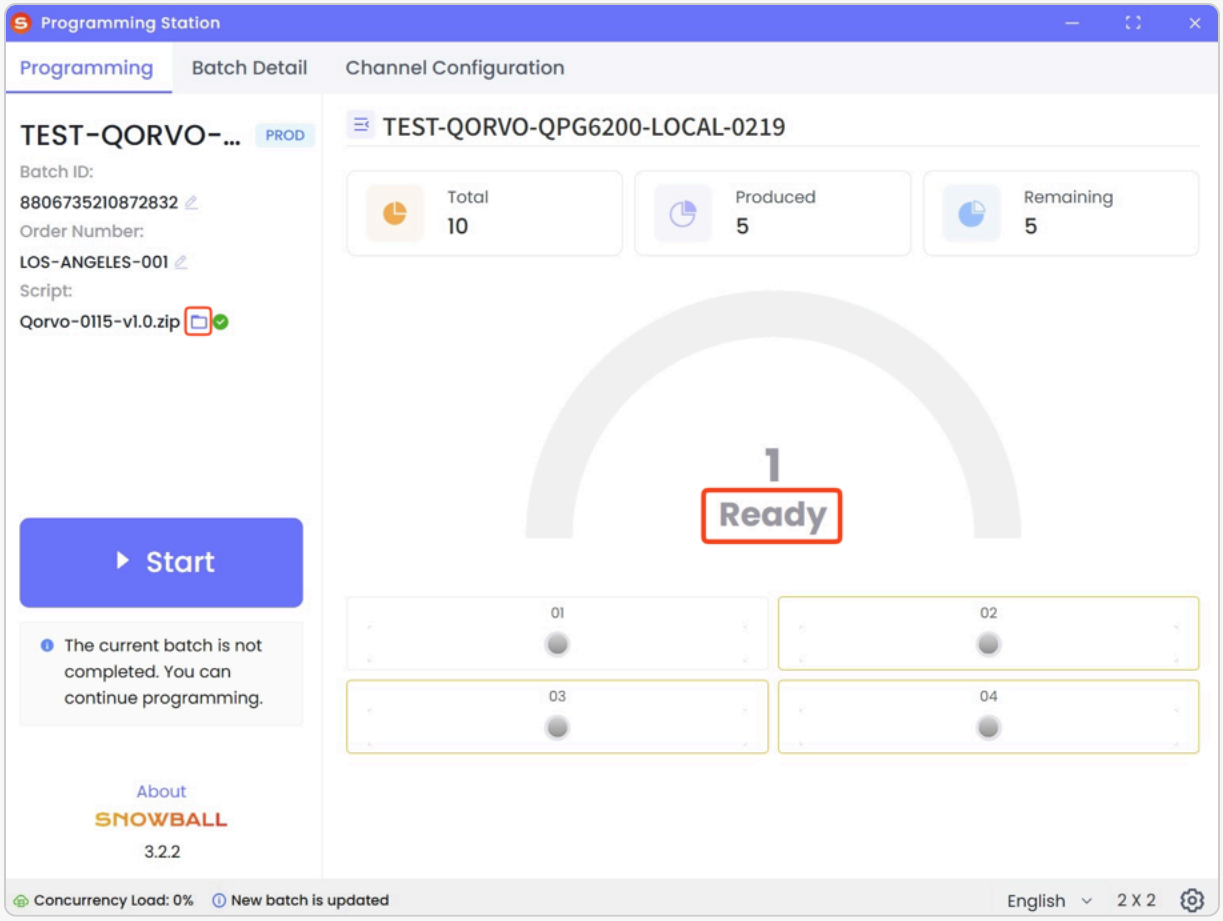


Step five: Device programming

Programming Station is a client for device programming. After assigning a programming station to the batch in the OnBoard Edge Service, refer to the steps below to start programming:

1. Install and sign in to the Programming Station client, verify that the device status is **Ready**.

   > **TIP**
   >
   > If the programming script is not selected when creating a batch, or if you want to select a different programming script, you can click the Folder icon to select the required programming script (any script format is supported).

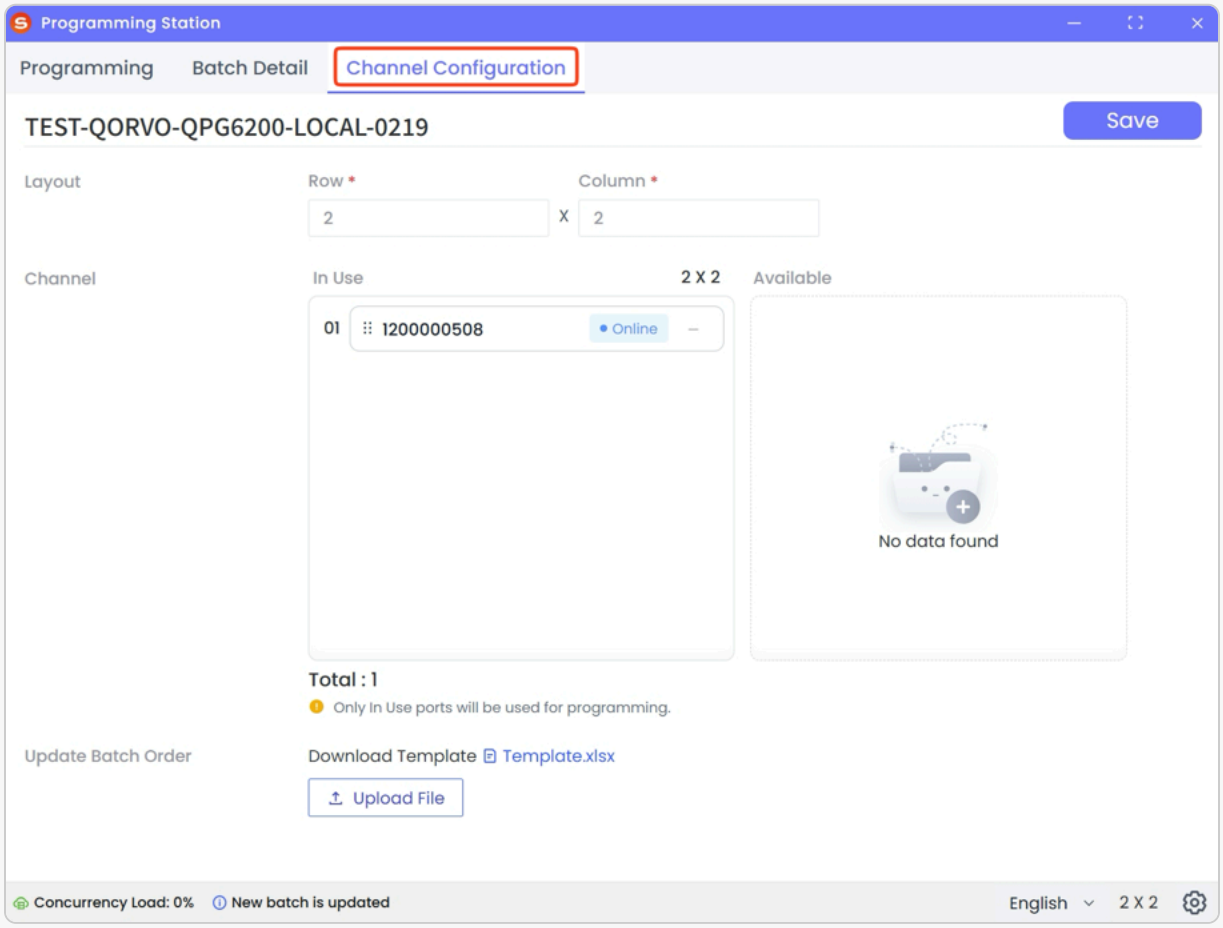


2. In the main window, select the **Channel Configuration** tab and then set the number of programmer connections in the **Layout** area as needed.

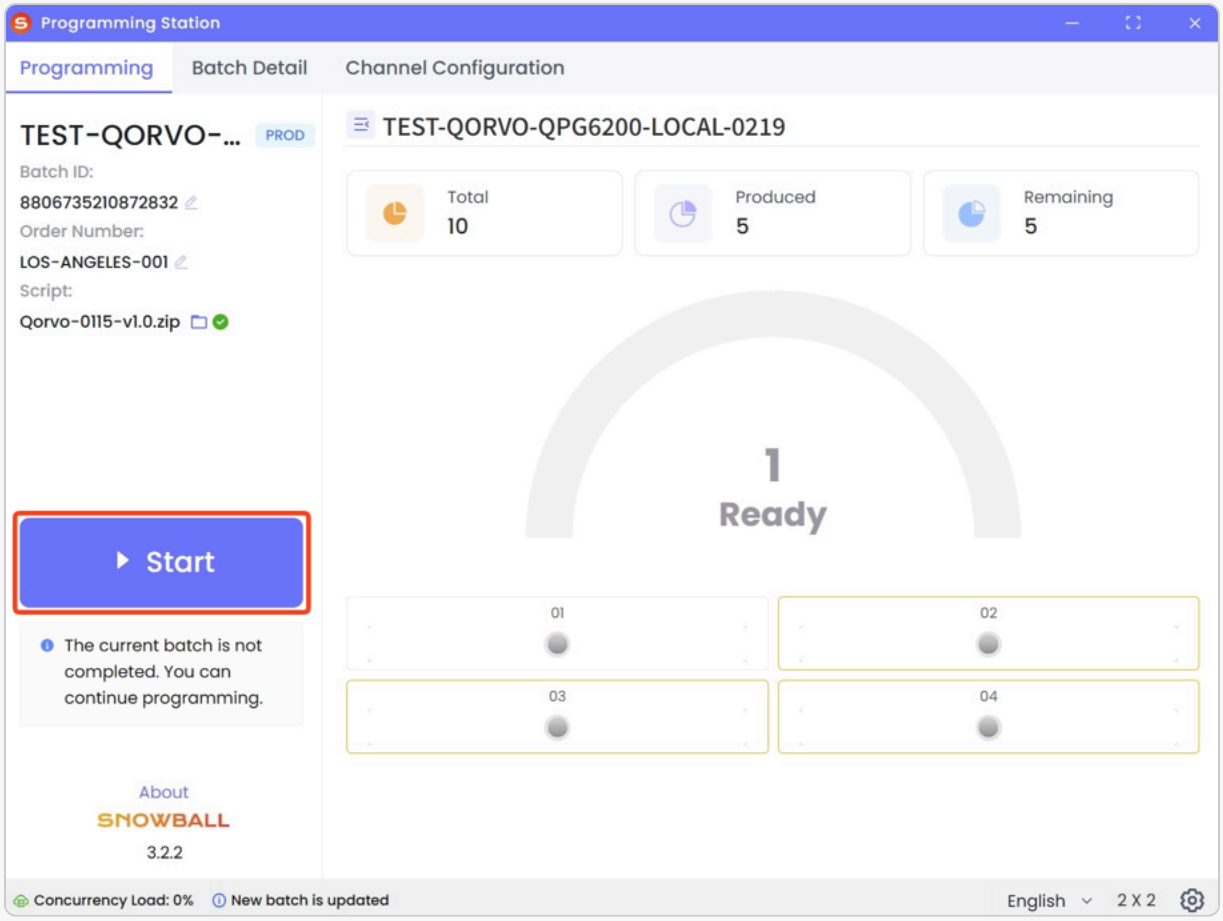
TIP

The number of connections determines how many devices can be programmed simultaneously. The system currently supports a number of connections based on the product of rows and columns in the layout area, which must satisfy the following conditions:

- Both rows and columns must be integers.
- Rows × Columns ≤ 24.
- Neither rows nor columns may exceed 16.
- If the number of rows exceeds 4, the number of columns can only be 1 or 2.

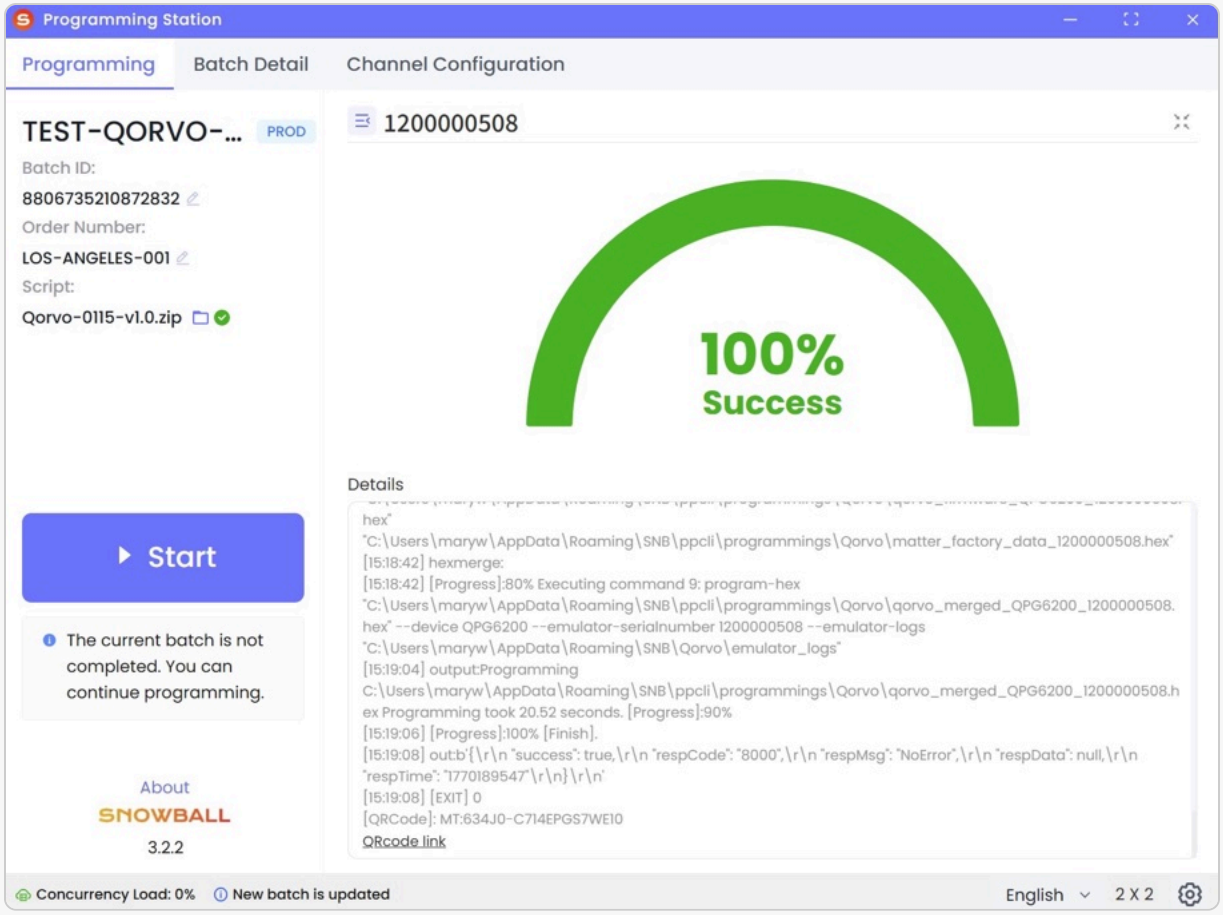


3. In the main window of the Programming Station client, click **Start** to execute device programming.



4. After programming is completed, click the corresponding port to check the device programming details.

> **TIP**
>
> You can also check the device profile and related log information in OnBoard™ IoT Security (OBIS).


Programming Station
Programming
Batch Detail
Channel Configuration
TEST-QORVO-...
PROD
Batch ID:
8806735210872832
Order Number:
LOS-ANGELES-001
Script:
Qorvo-0115-v1.0.zip
1200000508
100%
Success
Details
hex"
"C:\Users\maryw\AppData\Roaming\SNB\ppcli\programmings\Qorvo\matter_factory_data_1200000508.hex"
[15:18:42] hexmerge:
[15:18:42] [Progress]:80% Executing command 9: program-hex
"C:\Users\maryw\AppData\Roaming\SNB\ppcli\programmings\Qorvo\qorvo_merged_QPG6200_1200000508.hex" --device QPG6200 --emulator-serialnumber 1200000508 --emulator-logs
"C:\Users\maryw\AppData\Roaming\SNB\Qorvo\emulator_logs"
[15:19:04] output:Programming
C:\Users\maryw\AppData\Roaming\SNB\ppcli\programmings\Qorvo\qorvo_merged_QPG6200_1200000508.hex Programming took 20.52 seconds. [Progress]:90%
[15:19:06] [Progress]:100% [Finish].
[15:19:08] out:b'{\r\n "success": true,\r\n "respCode": "8000",\r\n "respMsg": "NoError",\r\n "respData": null,\r\n "respTime": "1770189547"\r\n}\r\n'
[15:19:08] [EXIT] 0
[QRCode]: MT:634J0-C714EPGS7WE10
QRcode link
Start
The current batch is not completed. You can continue programming.
About
SNOWBALL
3.2.2
Concurrency Load: 0%
New batch is updated
English
2 X 2

Version: v3.4.0 (Latest)

Feature guide - OnBoard™ IoT Security

OnBoard™ IoT Security provides a comprehensive set of features to manage every stage of the IoT device provisioning lifecycle. This guide covers each core module—including product management, factory management, key and certificate management, user management, U-Safe management, and device record tracking. Select a feature area below to explore its capabilities and related topics.

Product

CORE

- Create a product
- Configure a product
- Manage products
- Create a version
- Create a batch
- Check logs
- Manage members

KMS

CORE

- Create a key
- Check keys
- Manage keys

PKI

CORE

- Create a certificate
- Check certificates
- Manage certificates

GPCA

CORE

- Create a certificate
- Check certificates
- Manage certificates

SEMS

CORE

- Create an SE Profile
- Configure and publish an SE Profile
- Check SE Profiles
- Manage SE Profiles
- Manage scripts

Factory

ECOSYSTEM

LOCAL FACTORY

- Configure and manage factories
- Configure and manage programming stations

CLOUD FACTORY

- Configure and manage factories
- Configure and manage programming stations
- Manage batches and assign programming stations

U-Safe

ECOSYSTEM

- Check U-Safes

Device History RECORDS

- Check device history

Account ADMIN

- Create an account
- Check accounts
- Manage accounts

Group ADMIN

- Create a group
- Check groups
- Manage groups

Version: v3.4.0 (Latest)

How to create a product in OnBoard™ IoT Security

> **INFO**
>
> Currently, products can't be deleted after creation.

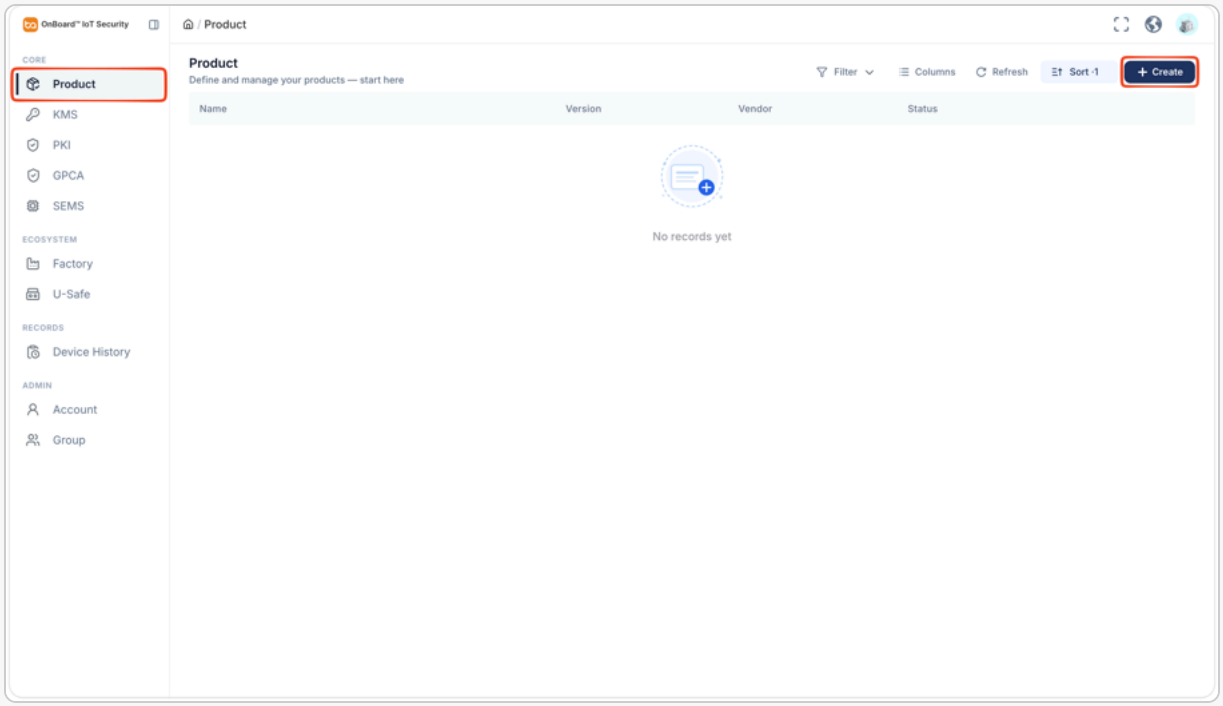
This article will guide you on how to create a product in OnBoard™ IoT Security (OBIS) to configure its basic information and prepare for product materials configuration.

Prerequisites

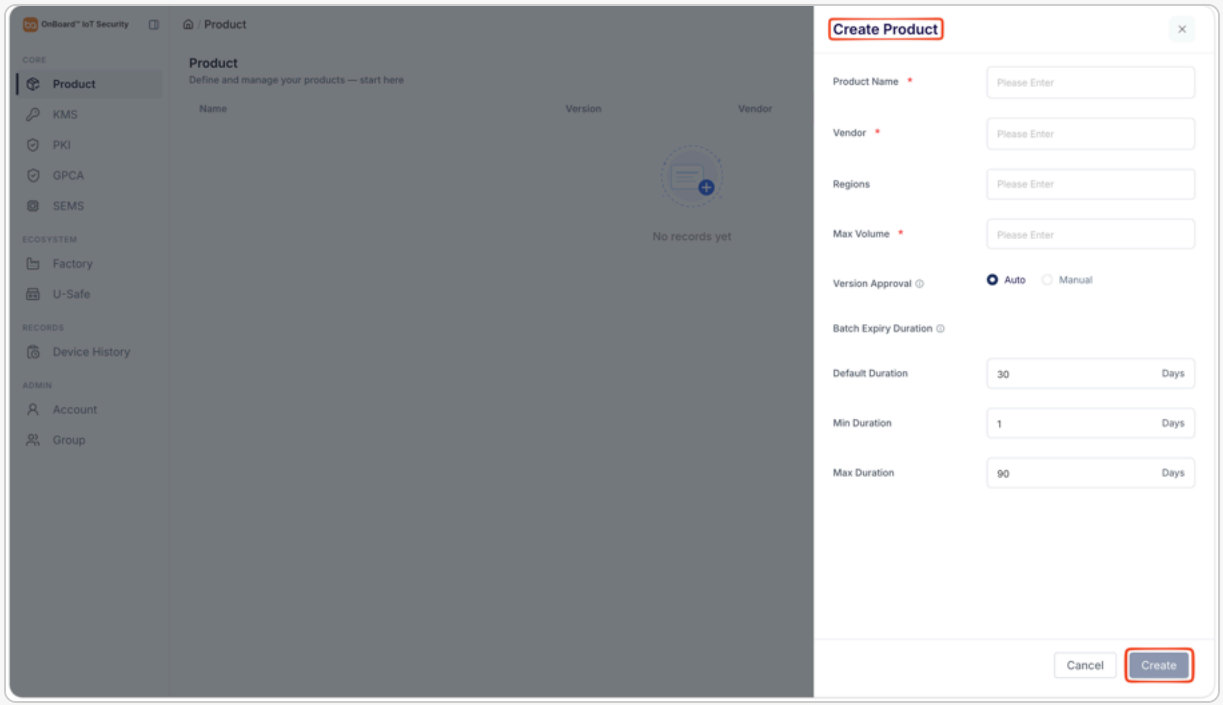
Before getting started, please ensure that you have OBIS role permissions as a System Manager or Product Manager.

Instructions

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then click **Create**.



3. On the **Create Product** panel, select and enter the required product basic information. After verifying that the information is correct, click **Create** to complete the product creation.



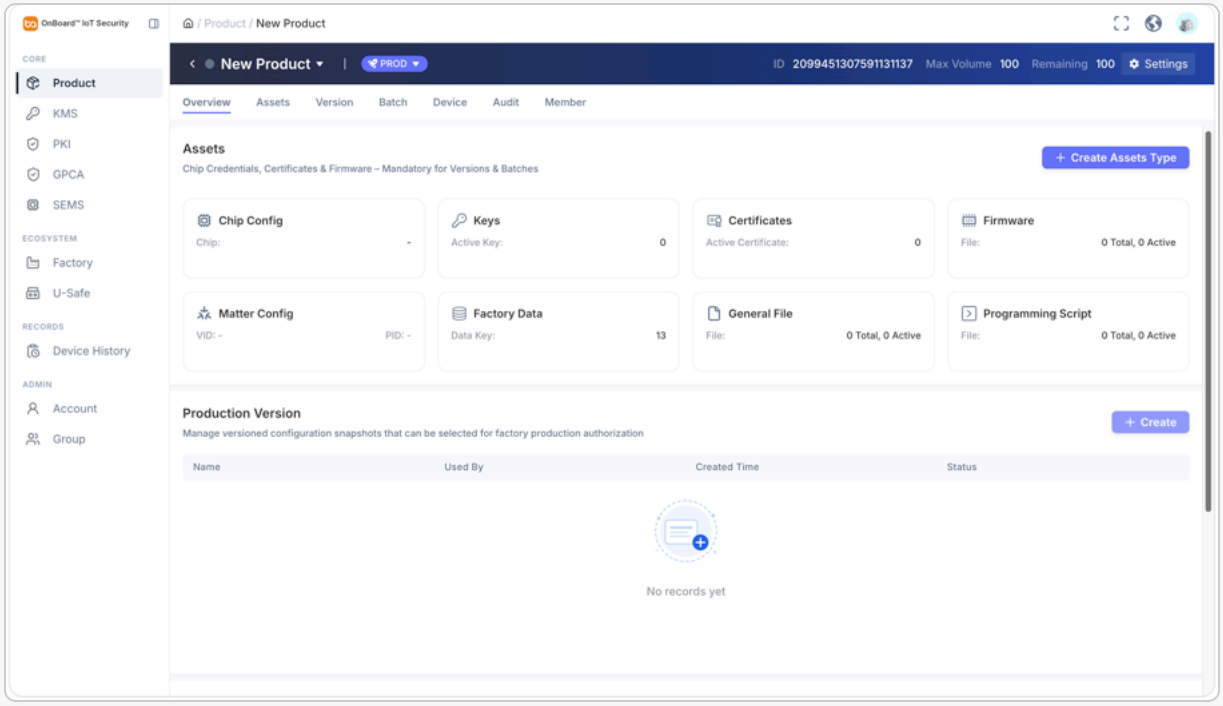
Description of product basic information:

Information	Mandatory	Description
Product Name	Yes	The product name must be unique.
Vendor	Yes	Automatically filled based on the tenant to ensure accuracy and reduce manual errors. You can manually change it if a different vendor name is needed.
Regions	No	Specify the regions where the product is supported. After entering a region, press **Enter** to generate a region label. Multiple region labels can be added. **Note**: When creating a version, the selectable regions will be limited to these specified regions.
Max.Volume	Yes	The maximum production volume of a product can't exceed 999,999,999. The total volume of batches can't exceed this limit.

Information	Mandatory	Description
Version Approval	No	This feature is enabled by default to ensure that all version data used for device production is verified. After you choose **Manual**, any version created in the PROD environment requires manual approval from the Product Owner or Product Manager before it can be used to create a batch。
Batch Expiry Duration	No	You can set the **Default Duration**, **Min Duration**, and **Max Duration** (in days). When creating a batch, the Expiry Time must be within this set range.

4. After the product is created, the page will navigate to the product page.

> **TIP**
>
> By default, the product creator is set as the Product Owner. To change the Product Owner, click the Options ⋮ icon for the Product Owner and select **Transfer Owner** on the **Member** tab, then choose the new Product Owner and click **Confirm**.
>
> After a product is created, its initial status is **Draft**. Once a version is created, the product status will change to **Released**. For more information, refer to the description of product status.


OnBoard™ IoT Security
/ Product / New Product
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
New Product
PROD
ID 2099451307591131137
Max Volume 100
Remaining 100
Settings
Overview
Assets
Version
Batch
Device
Audit
Member
Assets
Chip Credentials, Certificates & Firmware – Mandatory for Versions & Batches
+ Create Assets Type
Chip Config
Chip: -
Keys
Active Key: 0
Certificates
Active Certificate: 0
Firmware
File: 0 Total, 0 Active
Matter Config
VID: -
PID: -
Factory Data
Data Key: 13
General File
File: 0 Total, 0 Active
Programming Script
File: 0 Total, 0 Active
Production Version
Manage versioned configuration snapshots that can be selected for factory production authorization
+ Create
Name
Used By
Created Time
Status
No records yet

Version: v3.4.0 (Latest)

How to configure a product in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS) to configure product materials and prepare for version creation:

- Select the environment
- Configure assets

Prerequisites

Before getting started, please ensure that:

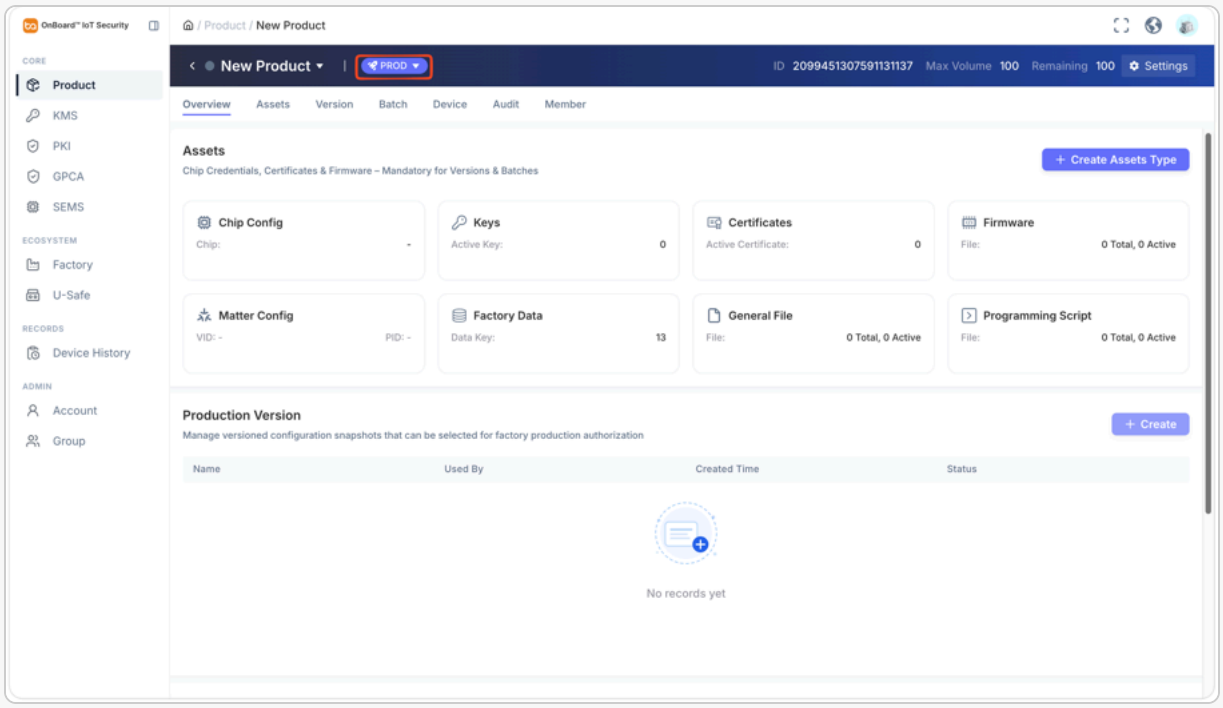
- You have product role permissions for the corresponding product: Product Owner, Product Manager, or Resource Manager.
- The certificates and keys have already been created.

Instructions

Step one: Select the environment

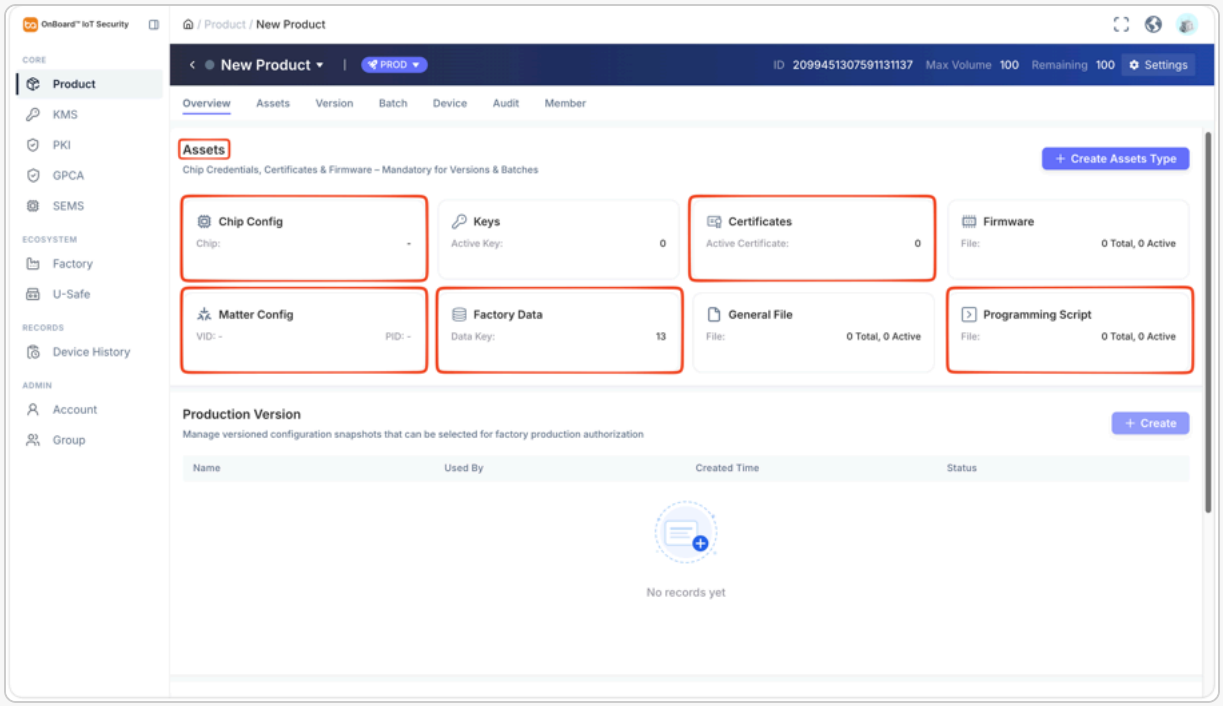
1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. On the product page, select the **TEST** or **PROD** environment.



4. Complete the configuration of relevant assets in the **Assets** section.

> **INFO**
>
> - Configure the necessary assets for the product (**Chip Config**, **Certificates**, **Matter Config**, and **Factory Data**). If the required configuration is not completed, version creation will be blocked, and the product status will remain in **Draft**.
> - Upload the necessary files for programming in **Programming Script**. Alternatively, you can select a programming script for a specific batch later in the Programming Station client.

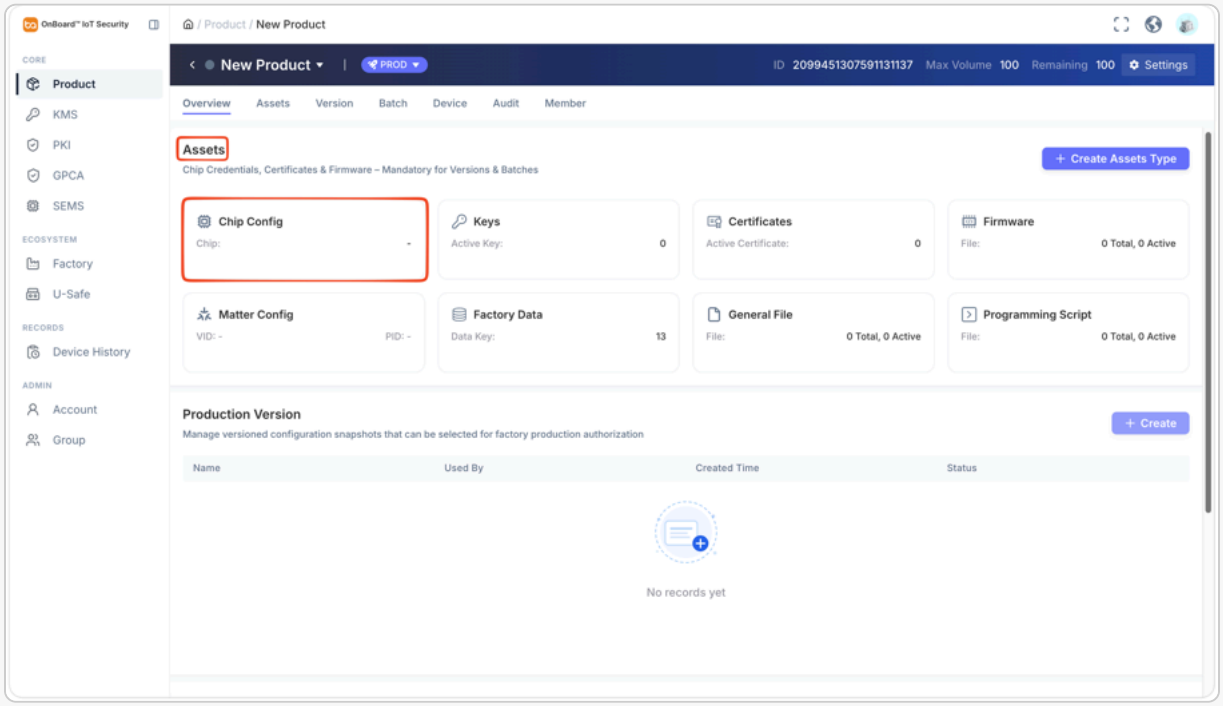

OnBoard™ IoT Security
/ Product / New Product
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
New Product
PROD
ID 2099451307591131137
Max Volume 100
Remaining 100
Settings
Overview
Assets
Version
Batch
Device
Audit
Member
Assets
Chip Credentials, Certificates & Firmware – Mandatory for Versions & Batches
+ Create Assets Type
Chip Config
Chip: -
Keys
Active Key: 0
Certificates
Active Certificate: 0
Firmware
File: 0 Total, 0 Active
Matter Config
VID: -
PID: -
Factory Data
Data Key: 13
General File
File: 0 Total, 0 Active
Programming Script
File: 0 Total, 0 Active
Production Version
Manage versioned configuration snapshots that can be selected for factory production authorization
+ Create
Name
Used By
Created Time
Status
No records yet

Step two: Configure assets

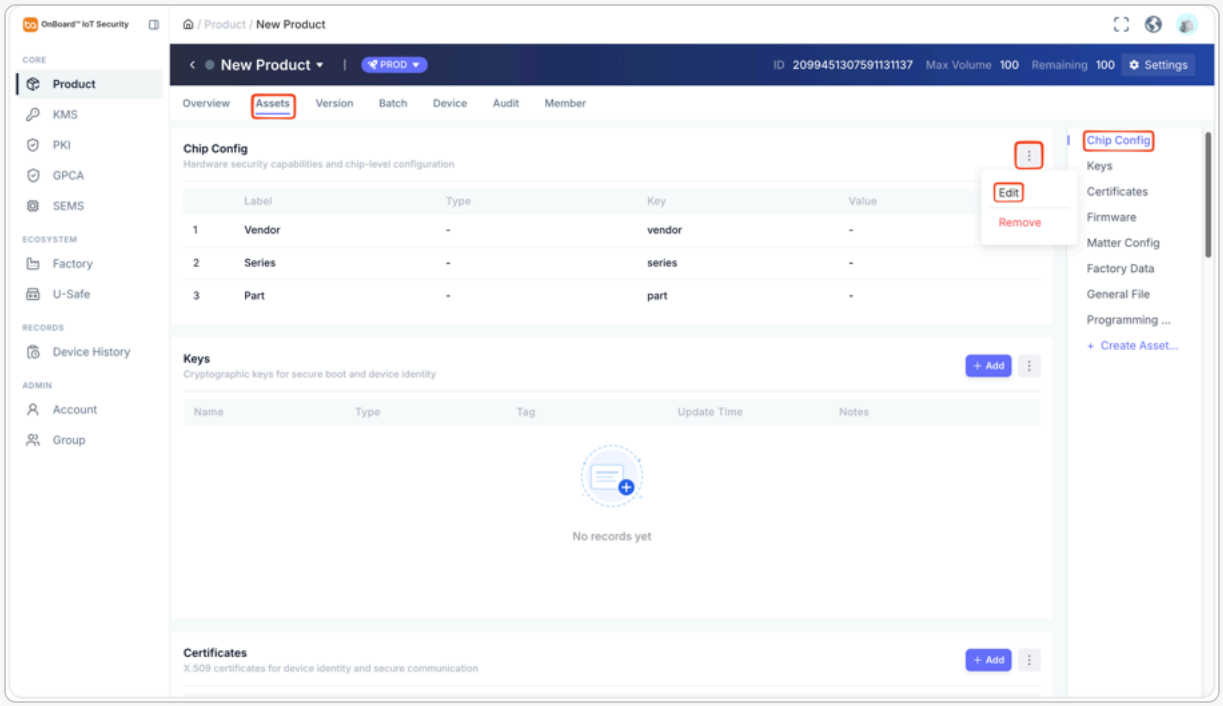
Chip Config (required)

> **TIP**
>
> **Chip Config** allows you to select and set the chip part and security options used by the product. Different chip parts provide corresponding security options, and you can configure them as needed. Once a version is created, the chip configuration can't be modified. To make adjustments, create a new product.
>
> Please refer to the supported chip settings for the detailed list. Additional chip vendors, series, and parts will be added based on demand.

1. On the product page, select **Chip Config** in the **Assets** section to navigate to the **Assets** tab.



2. In the **Chip Config** section, click the Options ⋮ icon and then select **Edit**. Select and enter the chip-related information.



Description of Chip Config information:

> **TIP**
>
> When creating a batch, if you need to enable the Secure Debug Reopen feature to support chip reprogramming, the Secure Debug feature must be enabled first.
>
> The supported data types in the Custom fields include: String, Number, Boolean, Key, Cert, and File.

Information	Mandatory	Type	Description
Vendor	Yes	-	Chip manufacturer. For more information, refer to supported chip settings.

Information	Mandatory	Type	Description
Series	Yes	-	Series of the chip. For more information, refer to supported chip settings.
Part	Yes	-	Part number of the chip. For more information, refer to supported chip settings.
Enable Secure Boot	No	Boolean	Enable the Secure Boot feature as needed. A security protection mechanism that prevents unauthorized software from being loaded.
Enable Secure Debug	No	Boolean	Enable the Secure Debug feature as needed. A security protection mechanism to prevent unauthorized debugging.
Secure Boot Key	No	Key	Select the key added in the **Keys** configuration. The key is used to verify the firmware and ensure the secure boot of the device.
Secure Boot Key Hash	No	Hex	The hash value of the Secure Boot Key.

Information	Mandatory	Type	Description
Secure Debug Key	No	Key	Select the key added in the **Keys** configuration. The key is used to authorize debugging access.
MCU Boot Key	No	Key	Select the key added in the **Keys** configuration. The key is used for device authentication and data encryption.
Debug Plaintext	No	Hex	Unencrypted debug data.
DAC Partition Address	No	Hex	Set the storage address in flash for downloading DAC certificates.

Currently supported chip settings:

Vendor	Series	Part
Silicon Labs	EFR32MG24	◦ EFR32MG24B210F1536IM48 ◦ EFR32MG24B020F1536IM48 ◦ EFR32MG24A110F1024IM48 ◦ EFR32MG24A020F1536IM48 ◦ EFR32MG24A420F1536IM48 ◦ EFR32MG24B020F1536IM40 ◦ EFR32MG24A010F1024IM40 ◦ EFR32MG24A020F1536IM40 ◦ EFR32MG24A420F1536IM40 ◦ EFR32MG24B010F1024IM48 ◦ EFR32MG24A010F1024IM48 ◦ EFR32MG24B110F1536IM48 ◦ EFR32MG24A021F1024IM40 ◦ EFR32MG24B010F1536IM40 ◦ EFR32MG24B220F1536IM48 ◦ EFR32MG24A020F1024IM40 ◦ EFR32MG24A010F1536IM40 ◦ EFR32MG24B010F1536IM48 ◦ EFR32MG24A410F1536IM48 ◦ EFR32MG24A010F1536IM48 ◦ EFR32MG24B120F1536IM48 ◦ EFR32MG24A410F1536IM40 ◦ EFR32MG24B310F1536IM48 ◦ EFR32MG24B020F1024IM48

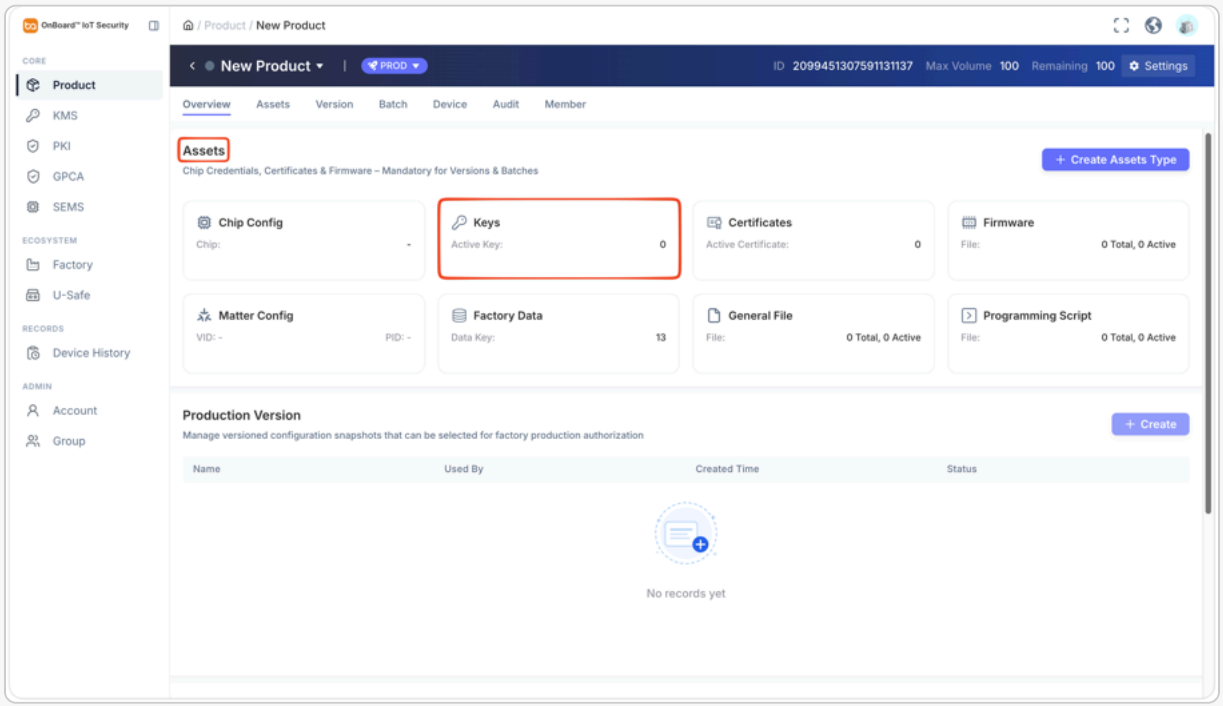
Vendor	Series	Part
		◦ EFR32MG24A020F1024IM48
	SIMG301	SiMG301M103WIH
		SiMG301M113WIH
Telink	TL323x	TL3238C
	TLSR92x	TLSR9268J
Qorvo	QPG6200	QPG6200
ESP	ESP32C3	ESP32C3
Amlogic	A113L	A113L
Nordic	NRF52840	NRF52840
Beken	BK7238	BK7238
NXP	s32k1	s32k144
TI	CC2755	CC2755R10
Realtek	RTL877xG Series	RTL8777G

3. Click **Save** to complete the setting of the Chip Config.

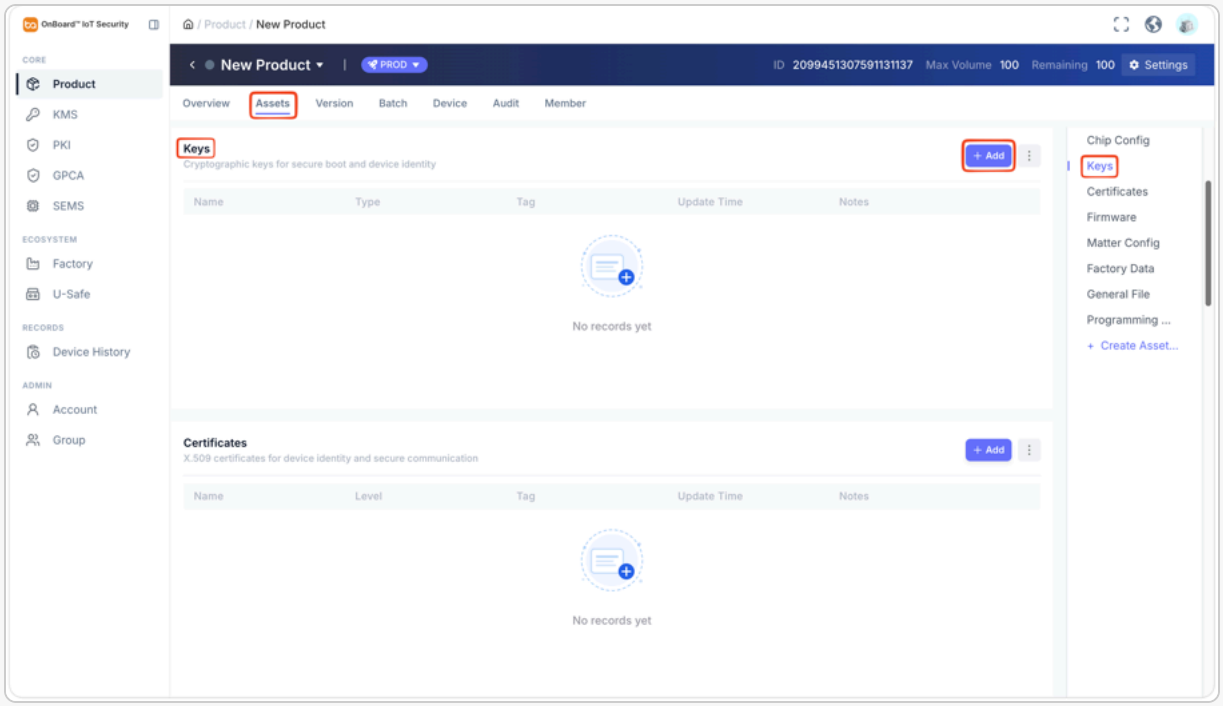
Keys (optional)

> **TIP**
>
> **Keys** allows you to add keys from KMS to the product. Added keys can be selected during the Chip Config.
>
> Keys can be created in KMS. For more information, refer to the steps for creating a key.

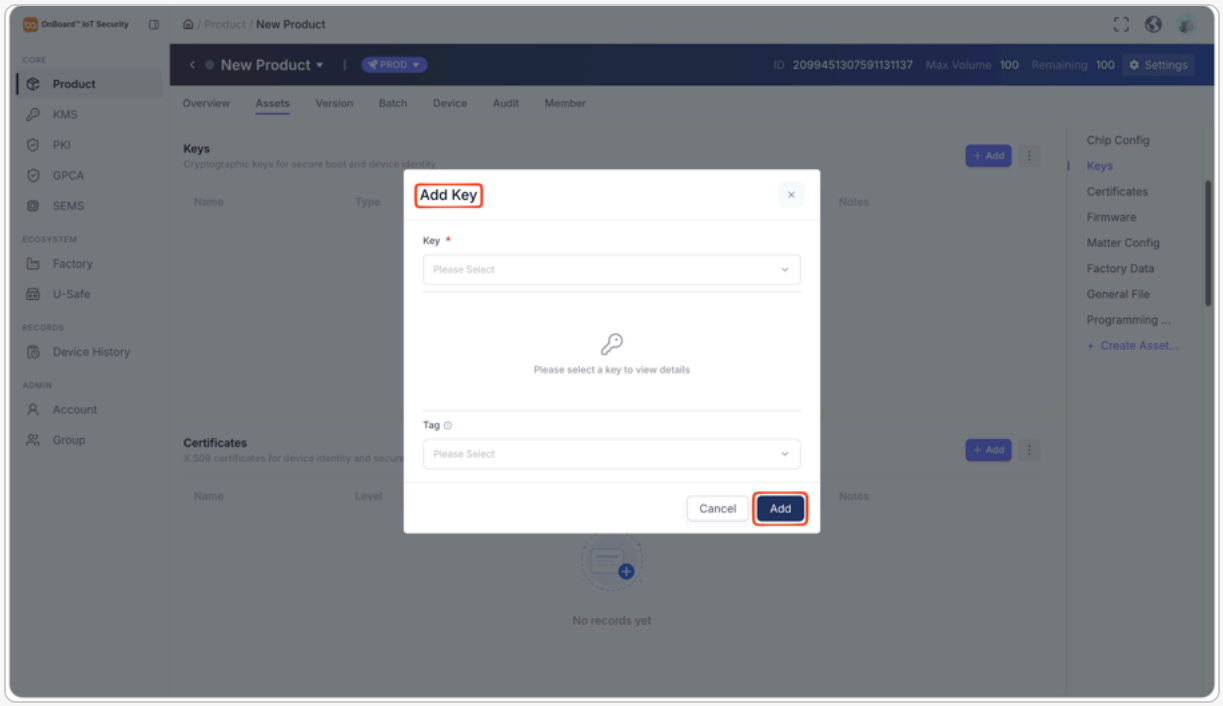
1. On the product page, select **Keys** in the **Assets** section to navigate to the **Assets** tab.



2. In the **Keys** section, click **Add**.



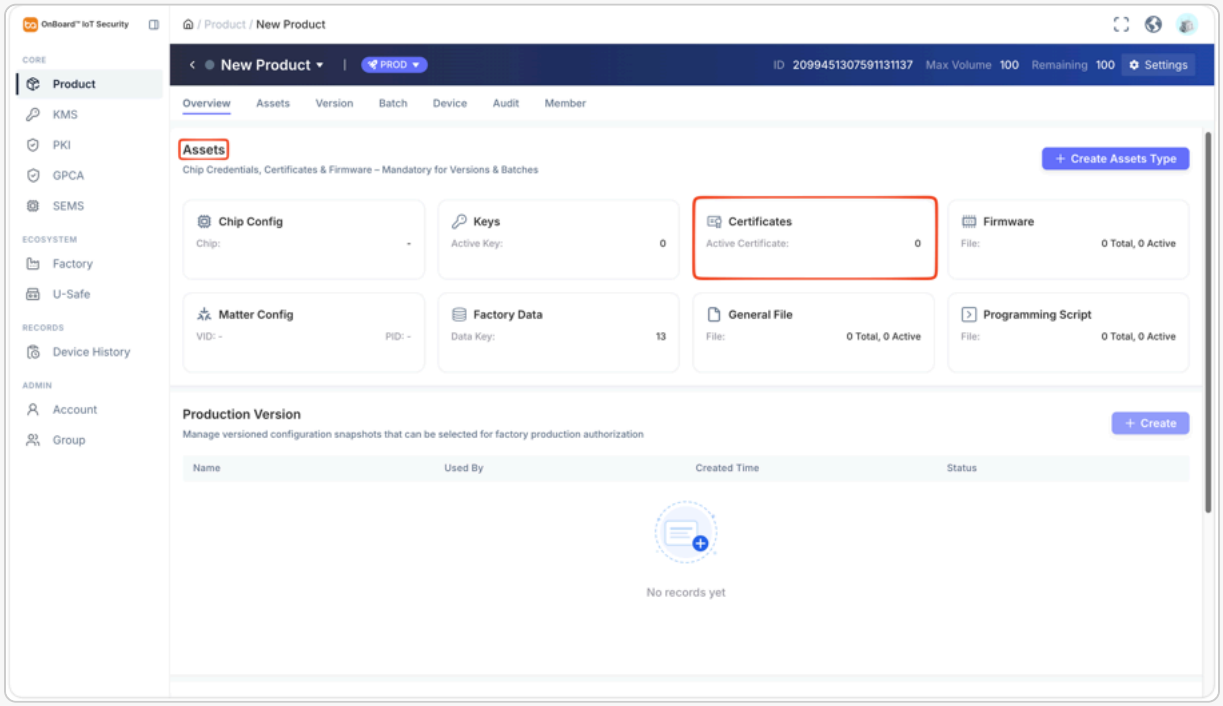
3. In the **Add Key** window, select the key to be assigned and click **Add**. Meanwhile, you can also create and add a custom tag in the **Tag** field as needed (this tag allows programming scripts to automatically identify and select the corresponding key later).


OnBoard™ IoT Security
Product / New Product
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
New Product
PROD
ID 2099451307591131137
Max Volume 100
Remaining 100
Settings
Overview
Assets
Version
Batch
Device
Audit
Member
Keys
Cryptographic keys for secure boot and device identity
+ Add
Name
Type
Notes
Chip Config
Keys
Certificates
Firmware
Matter Config
Factory Data
General File
Programming ...
+ Create Asset...
Add Key
Key *
Please Select
Please select a key to view details
Tag
Please Select
Cancel
Add
Certificates
X.509 certificates for device identity and secure
Name
Level
Notes
No records yet

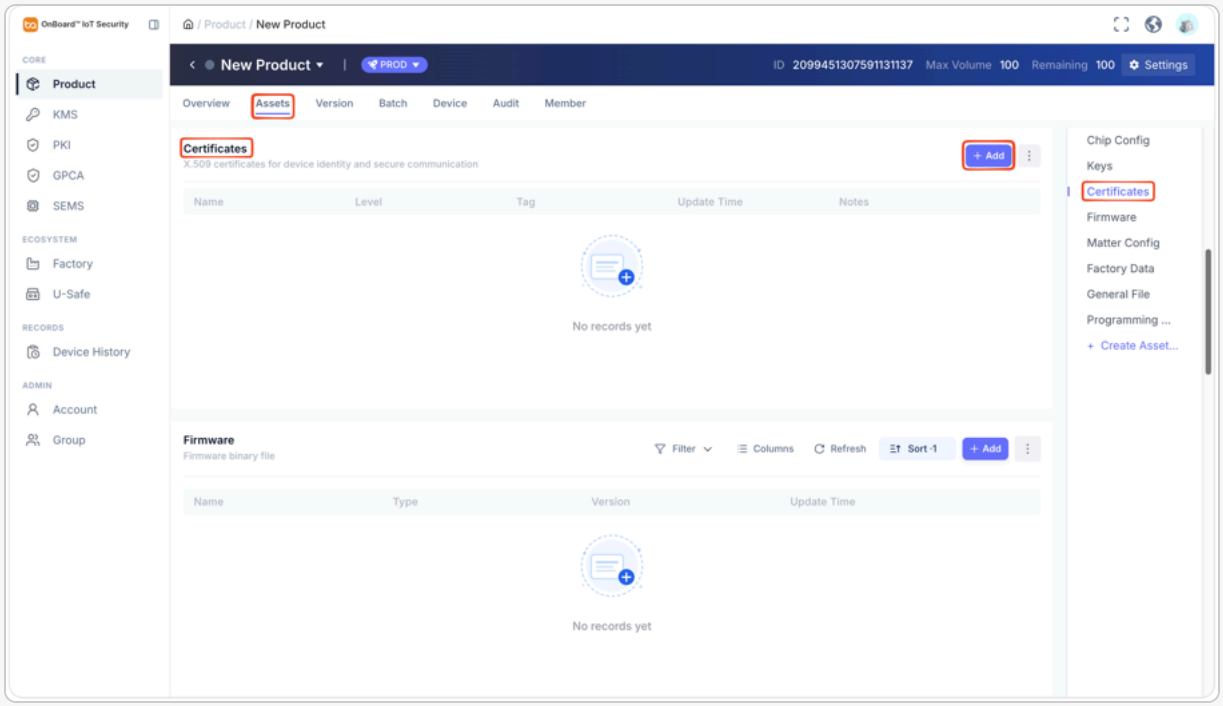
Certificates (required)

> **TIP**
>
> **Certificates** allows you to add CA templates (End Entity templates, DAC templates, or Device templates) from PKI to the product. Added certificates can be selected during the Matter Config.
>
> Certificates can be created in PKI. For more information, refer to the steps to create a certificate.

1. On the product page, select **Certificates** in the **Assets** section to navigate to the **Assets** tab.

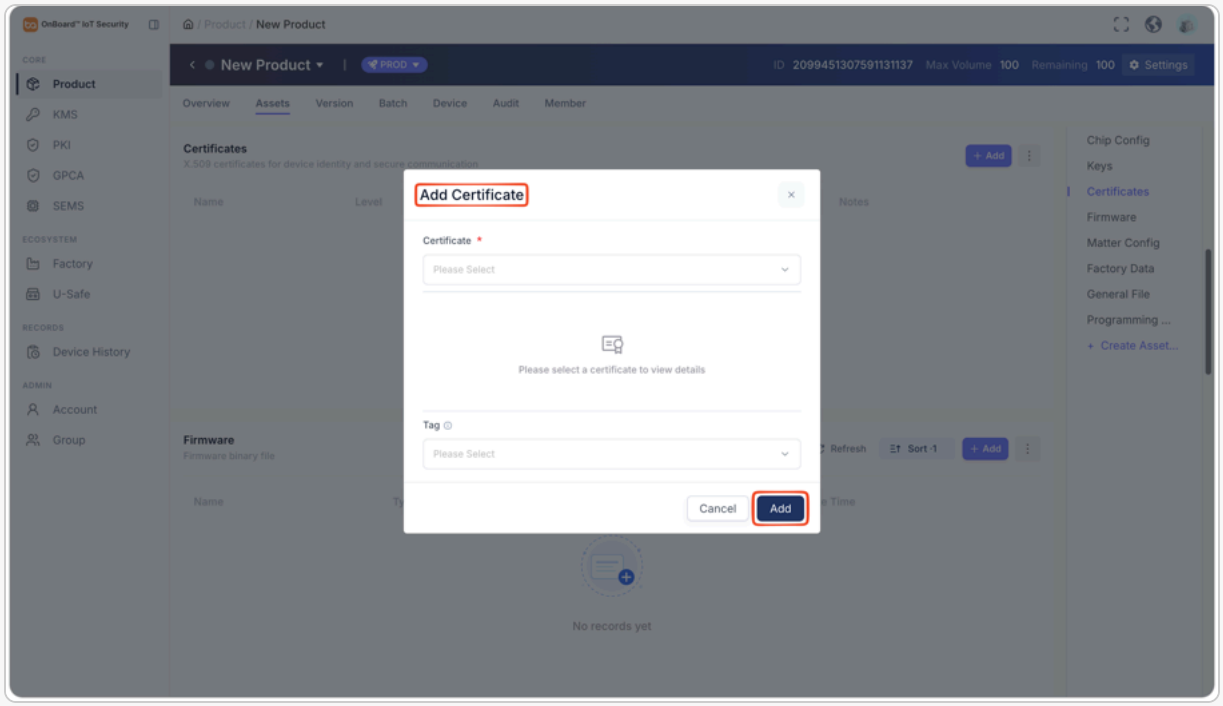


2. In the **Certificates** section, click **Add**.



obis-product-certificate.png (Screenshot displays how to add a certificate)

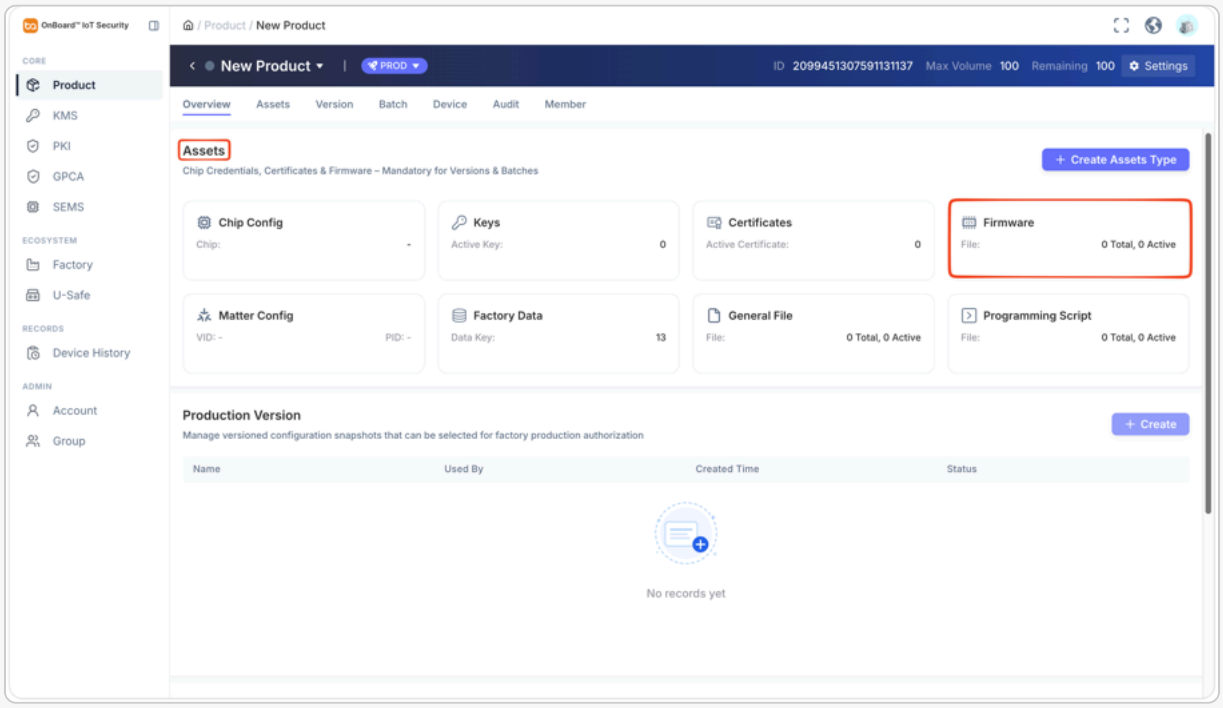
3. In the **Add Certificate** window, select the certificate to be assigned and click **Add**. Meanwhile, you can set the **Tag** to **Matter**, **Google**, or a custom tag as needed (this tag allows programming scripts to automatically identify and select the corresponding certificate later).


OnBoard™ IoT Security
Product / New Product
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
New Product
PROD
ID 2099451307591131137
Max Volume 100
Remaining 100
Settings
Overview
Assets
Version
Batch
Device
Audit
Member
Certificates
X.509 certificates for device identity and secure communication
+ Add
Name
Level
Notes
Chip Config
Keys
Certificates
Firmware
Matter Config
Factory Data
General File
Programming ...
+ Create Asset...
Add Certificate
Certificate *
Please Select
Please select a certificate to view details
Tag
Please Select
Cancel
Add
Firmware
Firmware binary file
Refresh
Sort -1
+ Add
Name
Time
No records yet

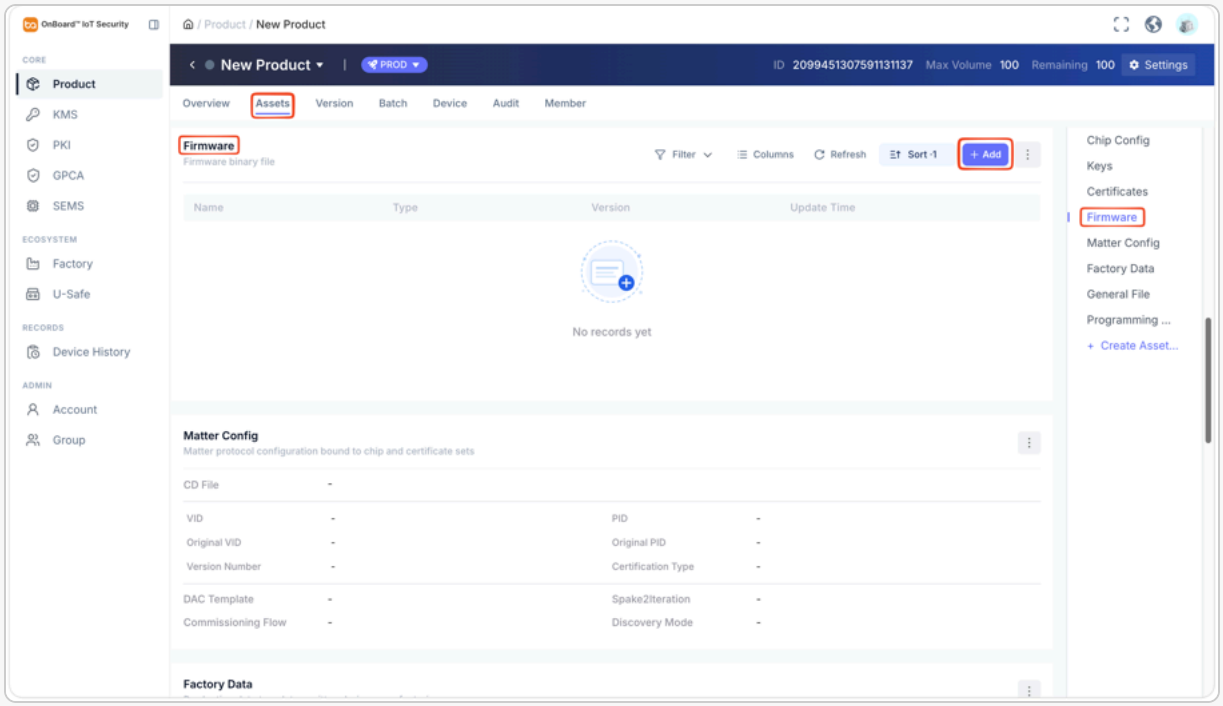
Firmware (optional)

> **TIP**
>
> **Firmware** allows you to upload the firmware files required for programming the product. Firmware formats supported: **.bin**, **.hex**, and **.s37**. Then, the uploaded firmware files can be selected when creating a version. You may upload firmware as needed.
>
> The files uploaded during configuration can be downloaded by users within the same tenant.

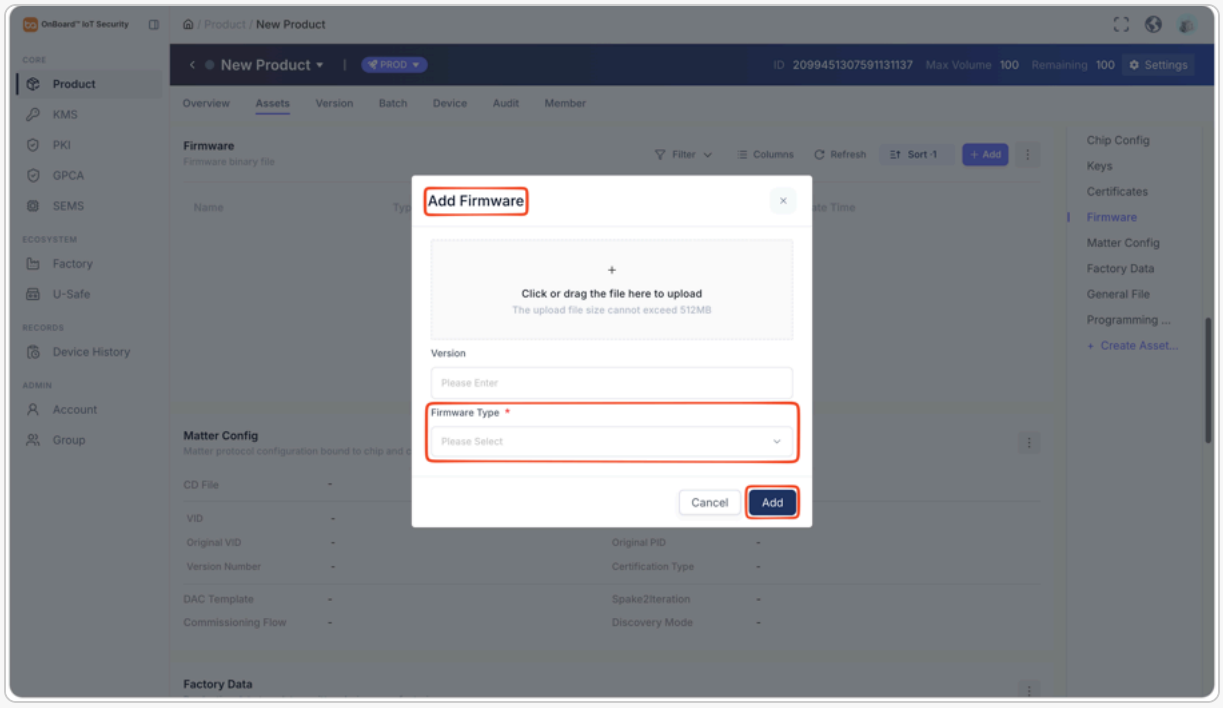
1. On the product page, select **Firmware** in the **Assets** section to navigate to the **Assets** tab.



2. In the **Firmware** section, click **Add**.



3. In the **Add Firmware** window, select and enter the firmware-related information.



Description of Firmware information:

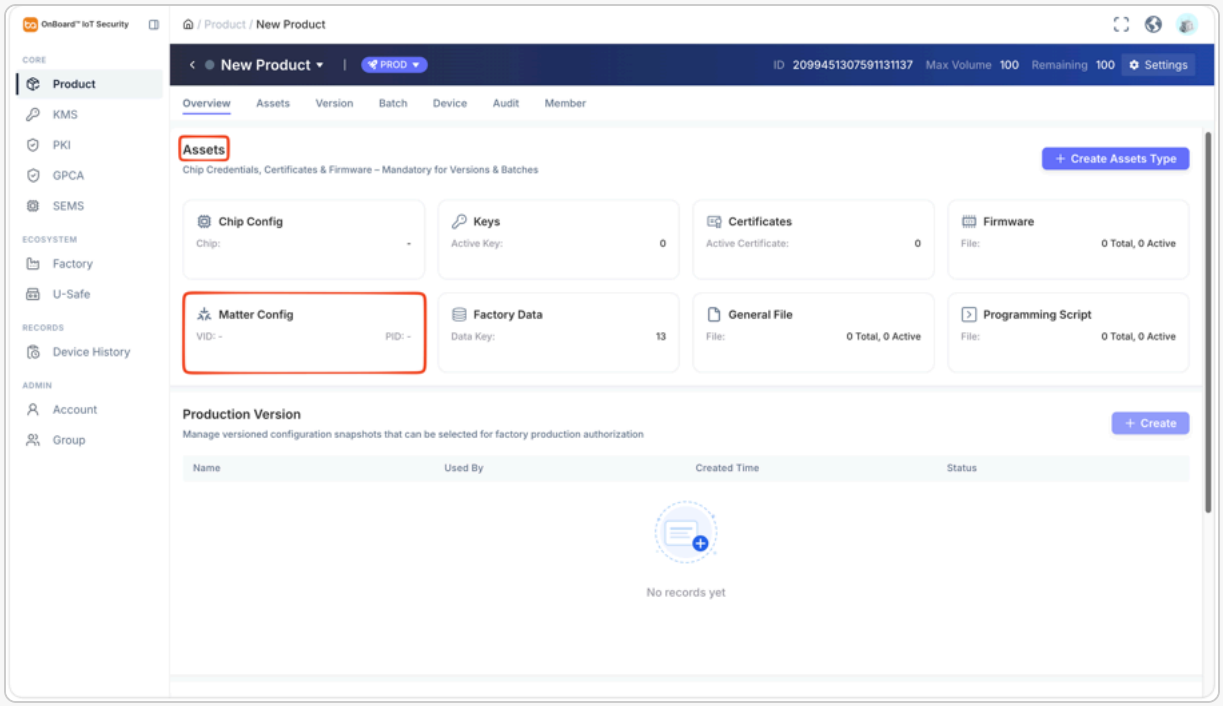
Information	Mandatory	Description
Upload File	Yes	Upload files by selecting the local firmware files. The maximum supported file size is 512 MB. **Note**: When uploading a file in **.bin** format, you need to specify the start address of the firmware.
Version	No	Indicate the firmware version.
Firmware Type	Yes	Two types of firmware are supported: ◦ **Application**: Used to implement device functionality, relying on the environment provided by the Bootloader. ◦ **Bootloader**: Used for hardware initialization, firmware loading, and updates.

4. Click **Add** to complete the configuration of the Firmware.

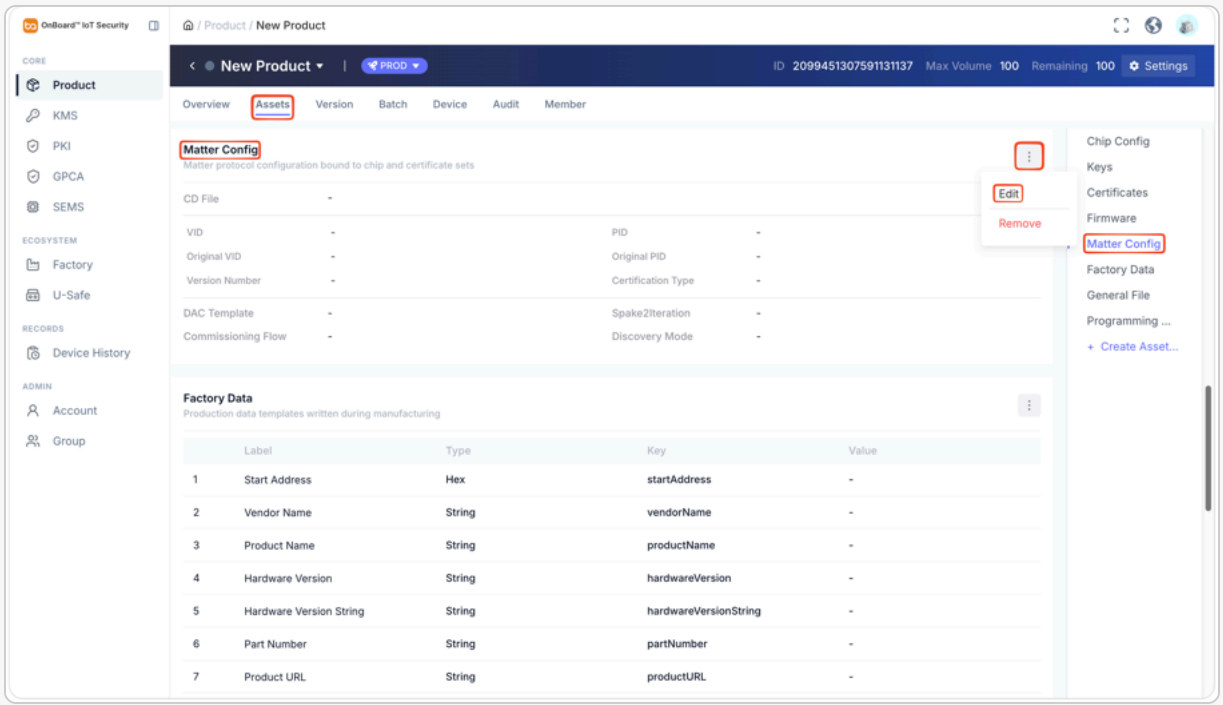
Matter Config (required)

> **TIP**
>
> **Matter Config** allows you to select and configure settings related to the Matter protocol.
>
> In this step, you need to select and upload the CD file and select the DAC template added in the Certificates configuration. Please ensure that the VID (Vendor ID) and PID (Product ID) in the CD file match those in the DAC template.
>
> You can replace the CD file with another one as needed when creating a version later.
>
> The CD files uploaded during configuration can be downloaded by users within the same tenant.

1. On the product page, select **Matter Config** in the **Assets** section to navigate to the **Assets** tab.



2. In the **Matter Config** section, click the Options ⋮ icon and then select **Edit**. Select and enter the Matter Config information.



Description of Matter Config information:

Information	Mandatory	Description
CD File	Yes	Notes for uploading files: ◦ The VID and PID in the CD file must match those in the DAC template. ◦ If the CD file contains multiple PIDs, at least one must match the PID in the DAC template. **Note**: Only **.der** format CD files are supported.
DAC Template	Yes	Select the DAC template configured in **Certificates**. The VID and PID in the DAC template must match those in the CD file. Refer to DAC Template.
PID	Yes	After uploading the CD file, the corresponding PID will be displayed.
Commissioning Flow	Yes	The device commissioning flow, adaptable to different scenarios: ◦ Standard Commissioning Flow ◦ User-Intent Commissioning Flow ◦ Custom Commissioning Flow

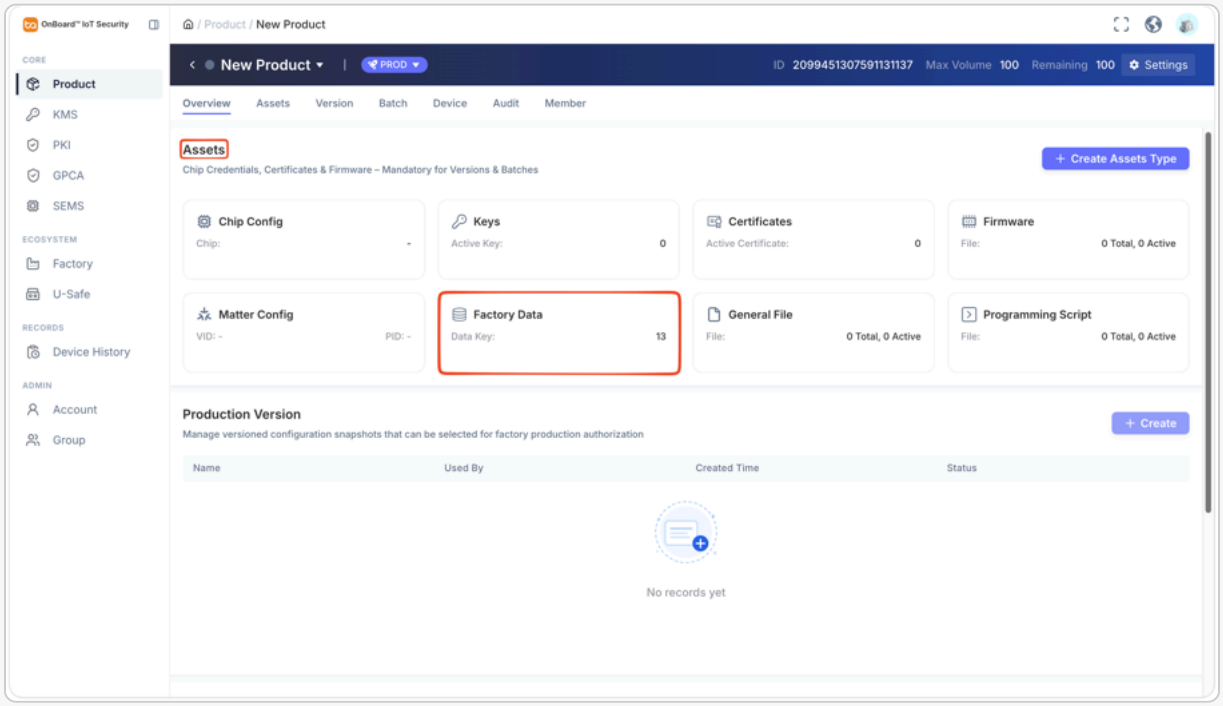
Information	Mandatory	Description
Spake2Iteration	Yes	A parameter of the SPAKE2+ protocol used during Matter commissioning, ensuring the security of the commissioning process.
Discovery Mode	Yes	Supported discovery modes: ◦ BLE: Bluetooth Low Energy. ◦ On IP network: Discovery through an IP network.

3. Click **Save** to complete the setting of the Matter Config.

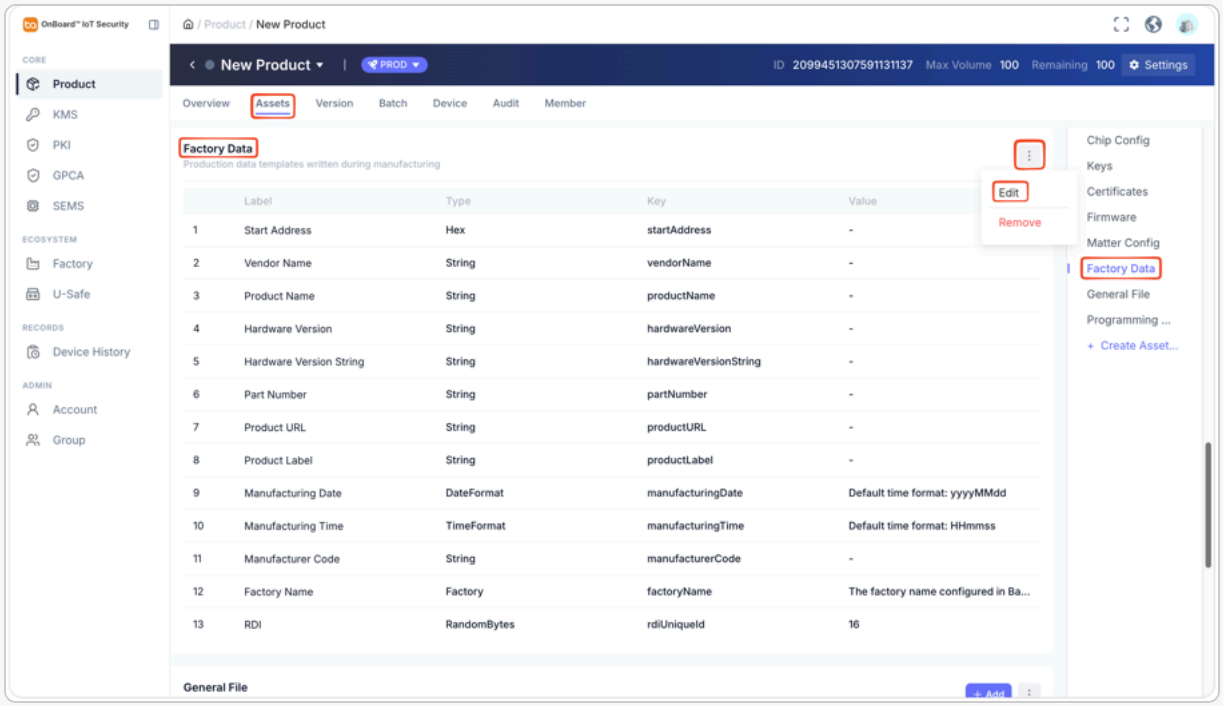
Factory Data (required)

> **TIP**
>
> **Factory Data** allows you to configure factory-related information and supports all fields required by the Matter specification. You can change the Factory Data as needed when creating a version later.
>
> The files uploaded during configuration can be downloaded by users within the same tenant.

1. On the product page, select **Factory Data** in the **Assets** section to navigate to the **Assets** tab.



2. In the **Factory Data** section, click the Options ⋮ icon and then select **Edit**. Enter the Factory Data information of the product (values can be left empty).



> **NOTE**
>
> If the checkbox in the **Mandatory** column of a Factory Data item is selected, members must enter a value for that item when creating a version.

Description of Factory Data information:

> **TIP**
>
> The supported data types include: String, Number, Hex, Factory, DateFormat, TimeFormat, File, and RandomBytes.

Information	Type	Description
Start Address	Hex	Start address.

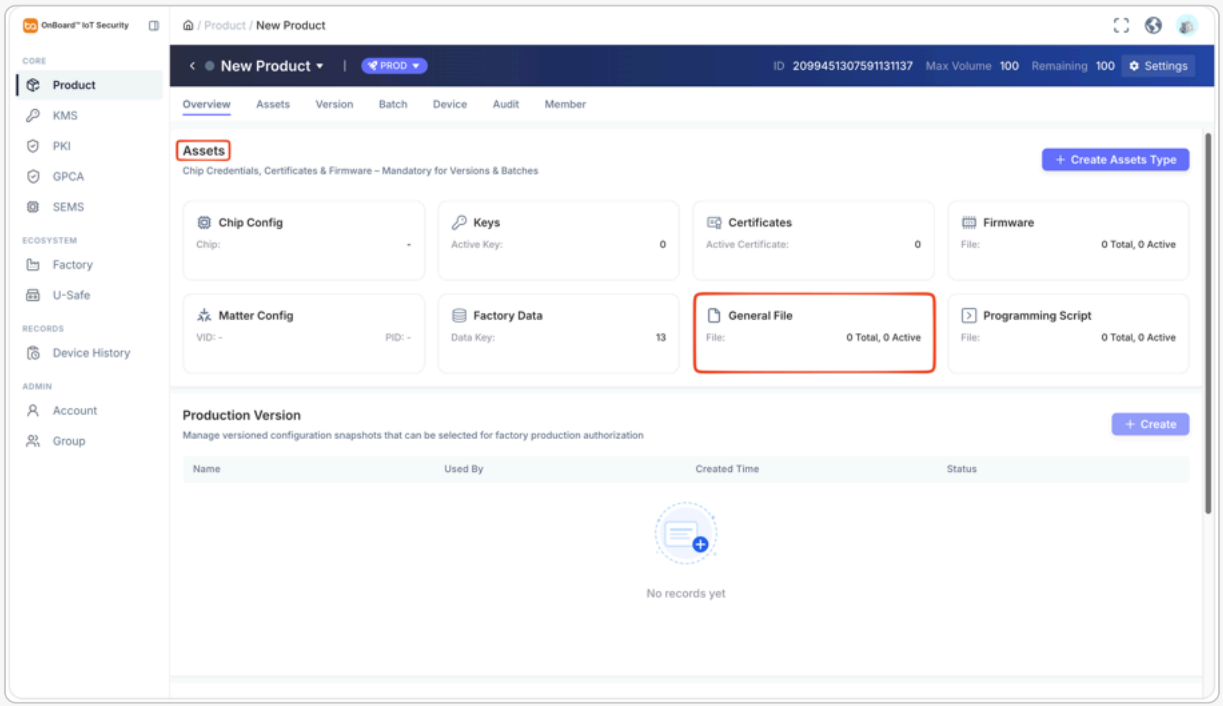
Information	Type	Description
Vendor Name	String	Vendor name.
Product Name	String	Product name.
Hardware Version	String	Hardware version.
Hardware Version String	String	Hardware version information presented as a string, which may include a more detailed version description. For example, HW_V1.0_20240101.
Part Number	String	Part number.
Product URL	String	Product link.
Product Label	String	Product label.
Manufacturing Date	DateFormat	Manufacturing date, default format is yyyyMMdd.
Manufacturing Time	TimeFormat	Manufacturing time, default format is HHmmss.
Manufacturing Code	String	Manufacturing code.
Factory Name	Factory	The factory name configured in batch.

3. Click **Save** to complete the configuration of the Factory Data.

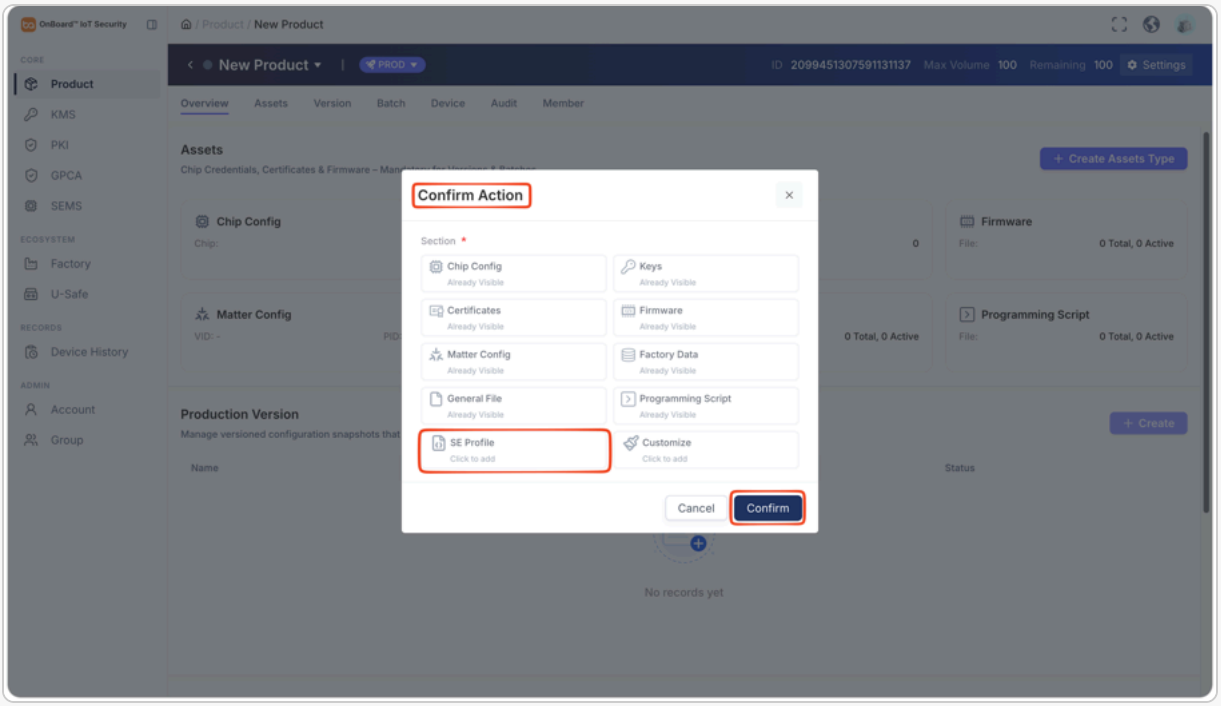
General File (optional)

> **TIP**
>
> **General File** allows you to upload other files required for version and batch creation (excluding firmware and programming scripts). Files in any format are supported.
>
> The uploaded files can be selected when creating a version or batch.
>
> The files uploaded during configuration can be downloaded by users within the same tenant.

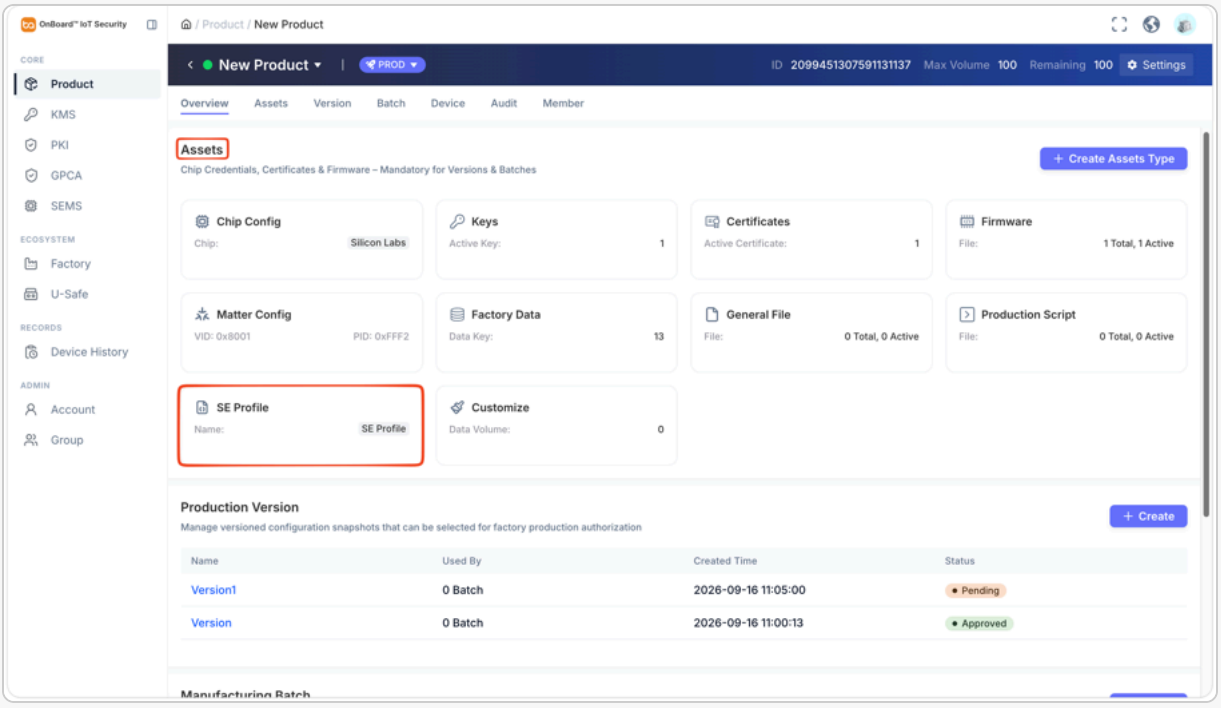
1. On the product page, select **General File** in the **Assets** section to navigate to the **Assets** tab.



2. On the **General File** page, click **Add**.



3. In the **Add General File** window, select and enter the relevant information.



Description of General File information:

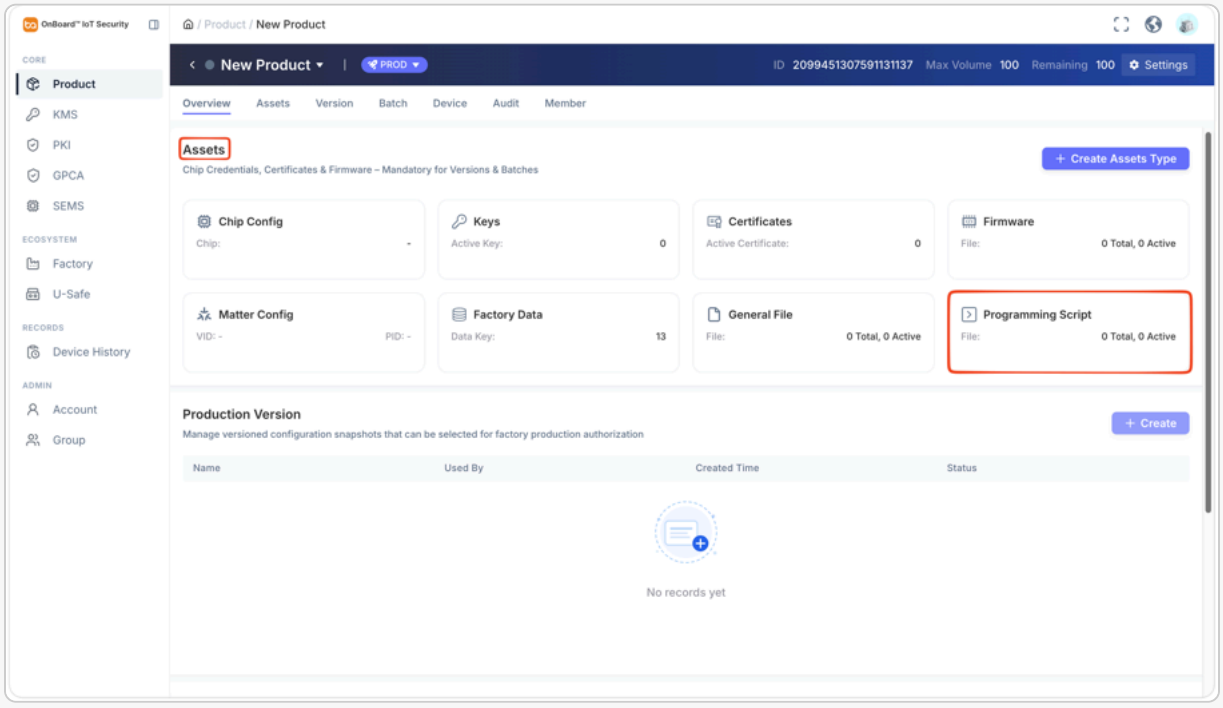
Information	Mandatory	Description
Upload File	Yes	Upload files by selecting the local files. The maximum supported file size is 512 MB.
Tag	Yes	Assign tags to files. During later programming, the programming script can retrieve and use the corresponding files through their tags. **Note**: A file can be assigned multiple unique tags. Meanwhile, the same tag can also be assigned to multiple files. You can add new tags or select from existing tags.
Version	No	Identify the file version and use it to track file changes.

4. Click **Add** to complete the configuration of the General File.

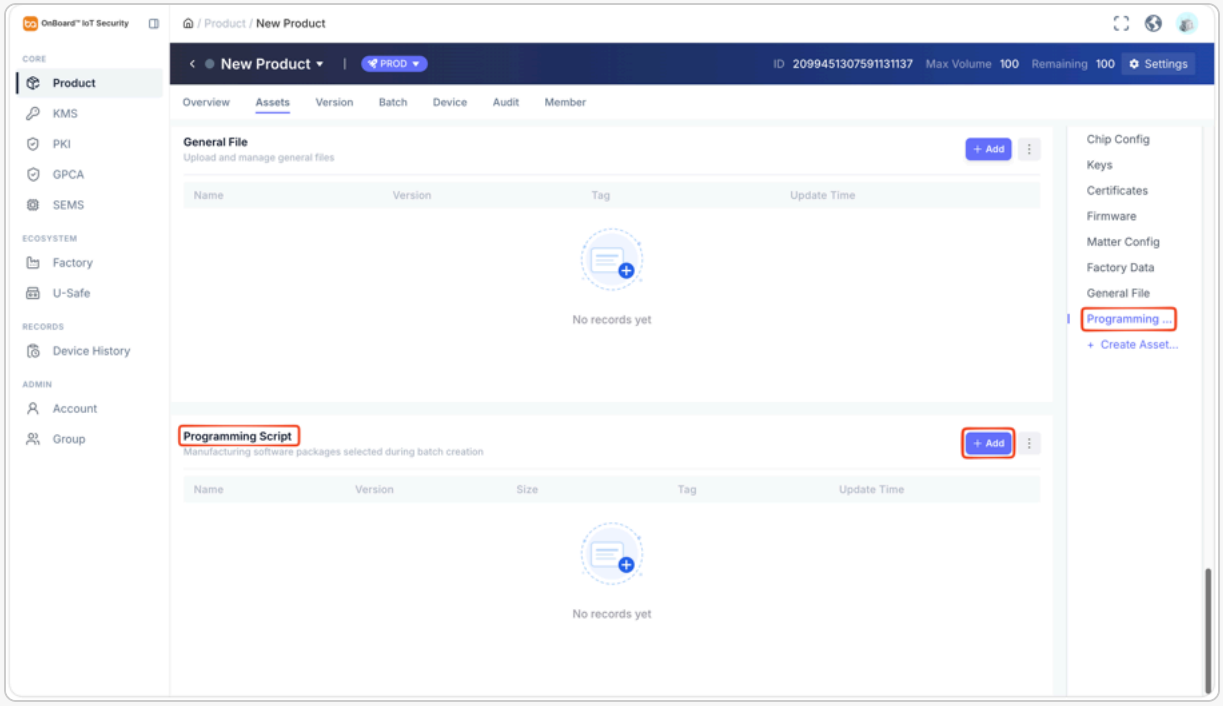
Programming Script (optional)

> **TIP**
>
> Files in the **Programming Script** section will be used for batch creation.
>
> **Programming Script** allows you to upload script files used for device programming (any script format is supported). You can select and upload the programming script as needed. If it is not required at the moment, you can also select it for a specific batch later in the Programming Station client.
>
> The files uploaded during configuration can be downloaded by users within the same tenant.

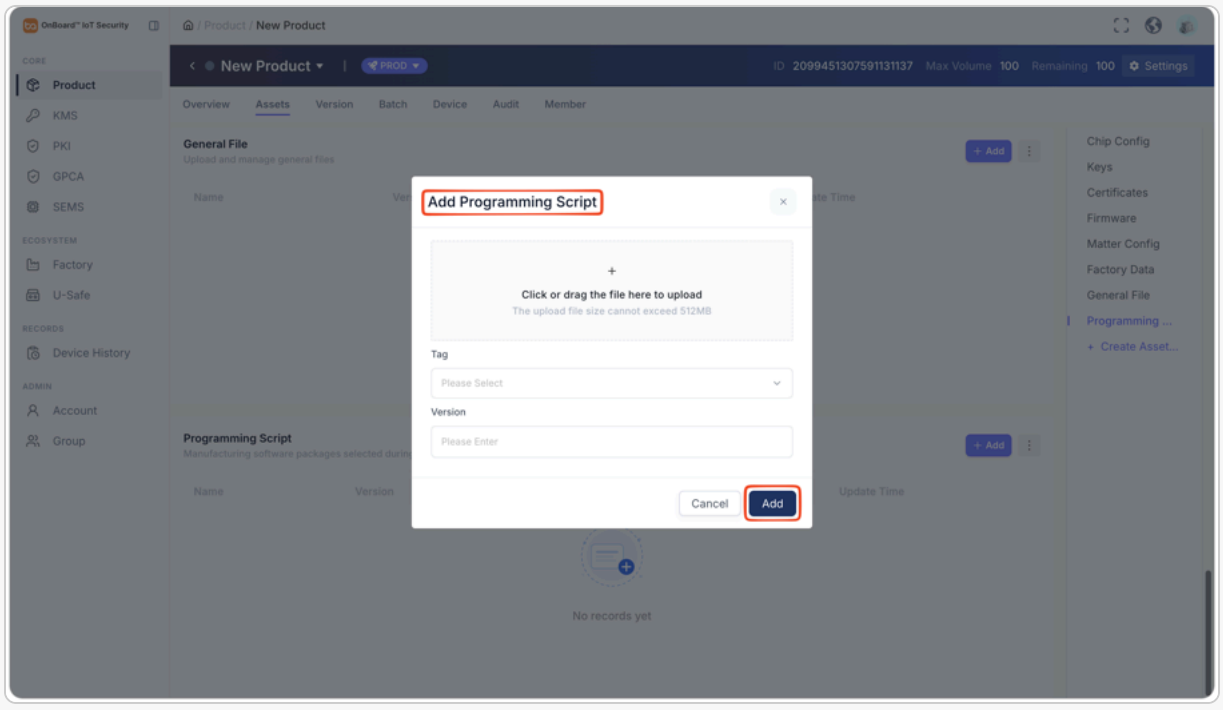
1. On the product page, select **Programming Script** in the **Assets** section to navigate to the **Assets** tab.



2. In the **Programming Script** section, click **Add**.



3. In the **Add Programming Script** window, select and enter the relevant information.



Description of Programming Script information:

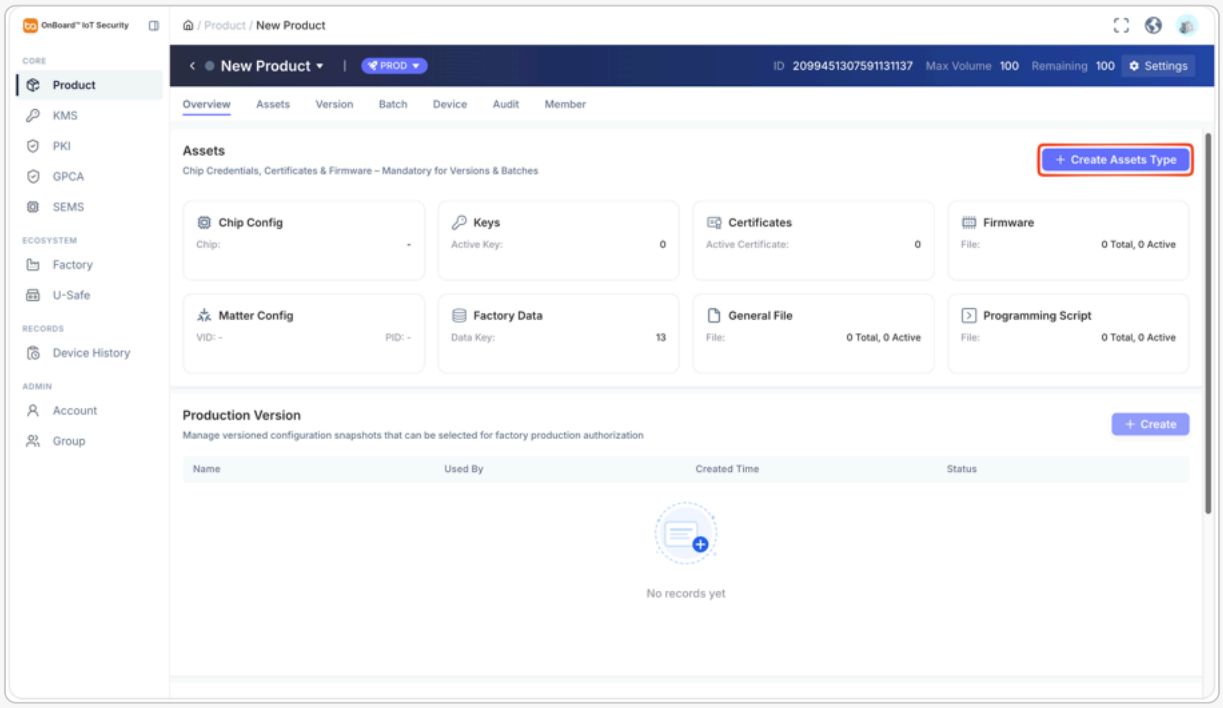
Information	Mandatory	Description
Upload File	Yes	Upload files by selecting the local programming script files. The maximum supported file size is 512 MB.
Version	No	Indicate the version of the programming script.

4. Click **Add** to complete the configuration of the Programming Script.

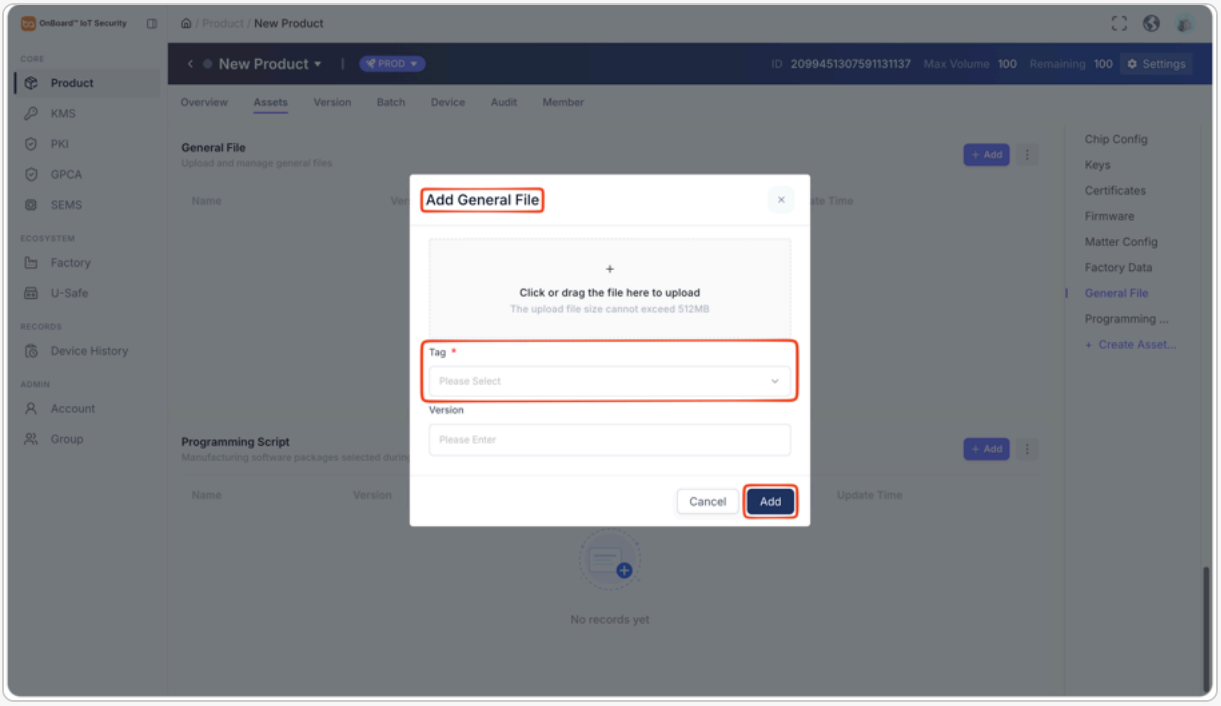
SE Profile (Optional)

> **TIP**
>
> **SE Profile** allows you to add SE Profiles from SEMS to the product.
>
> SE Profiles can be created in SEMS. For more information, refer to the steps to create an SE Profile.

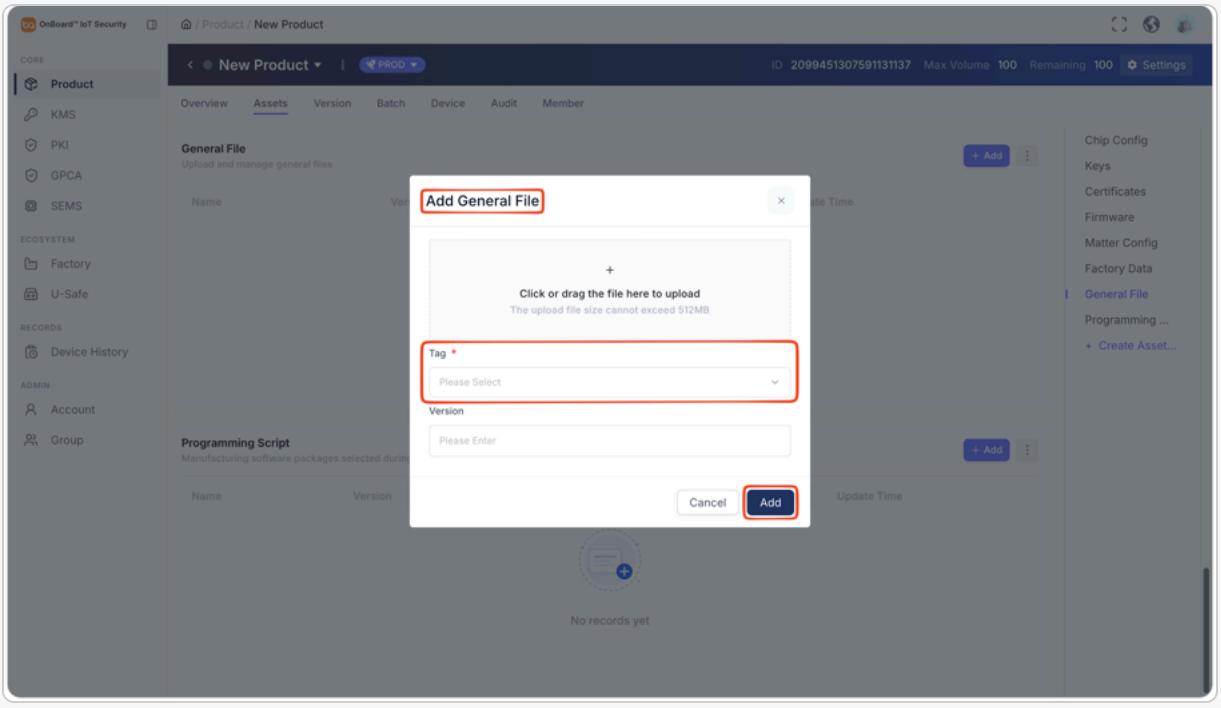
1. On the product page, click **Create Assets Type**.



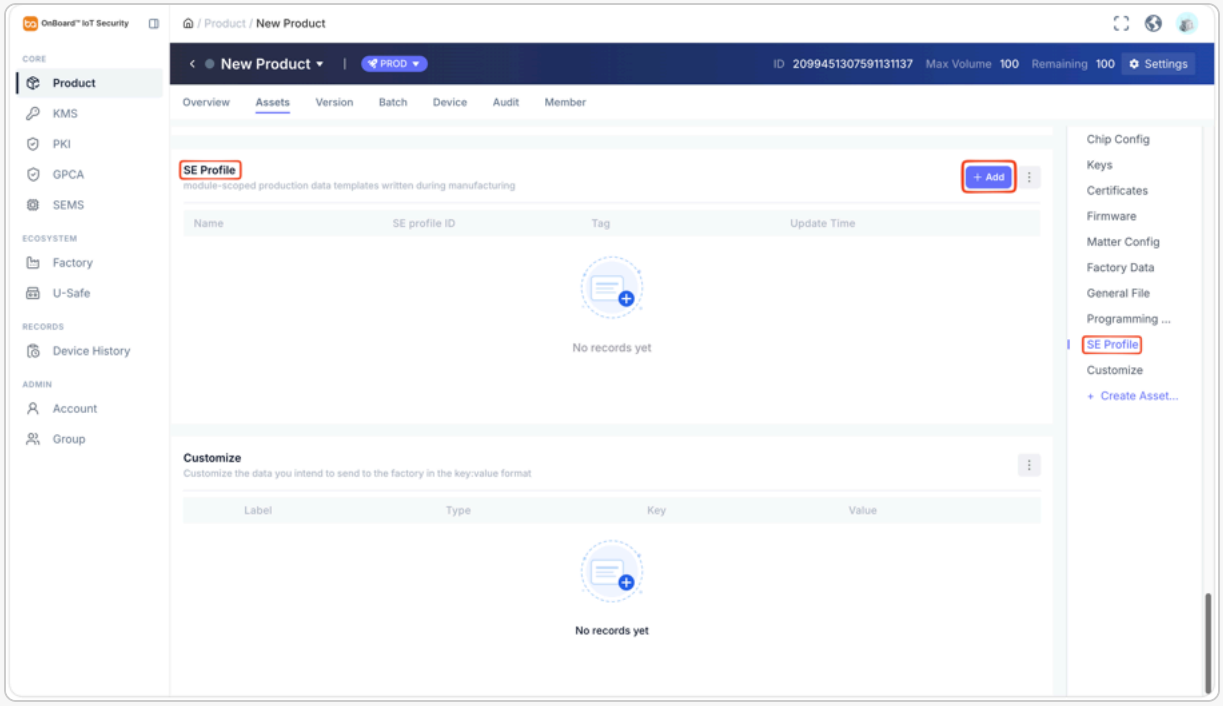
2. In the **Confirm Action** window, select the **SE Profile** asset type, and then click **Confirm** to add the SE Profile asset.



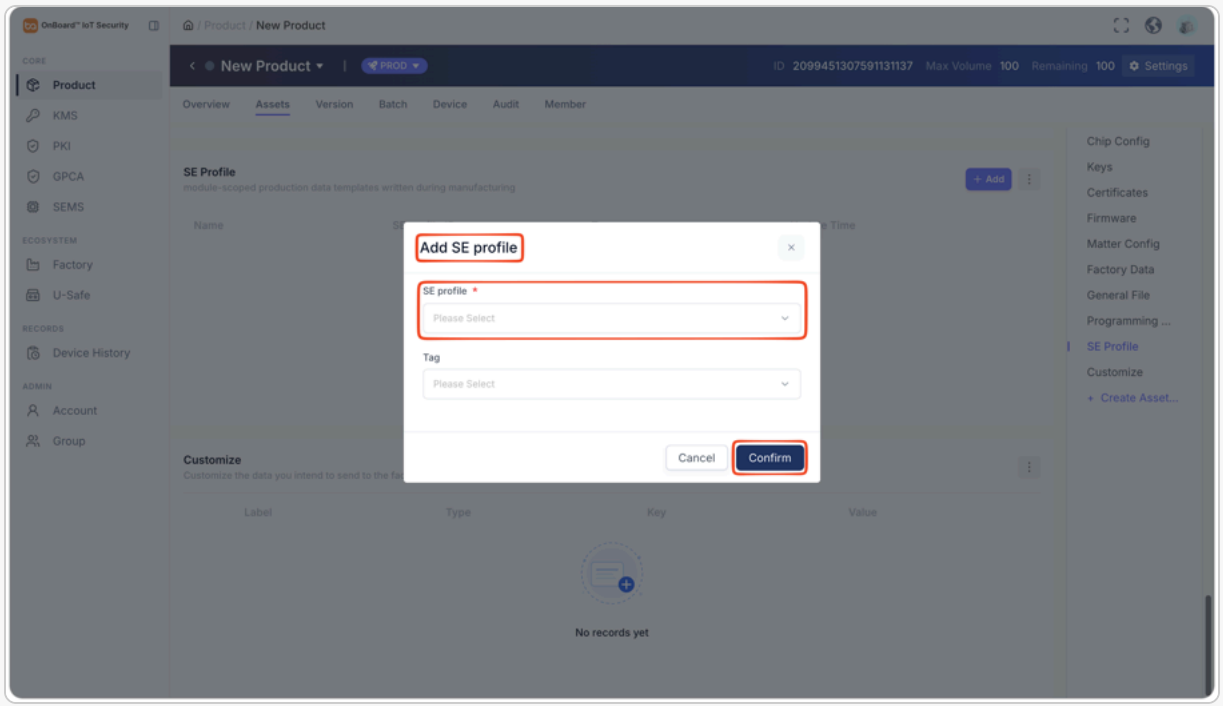
3. Select **SE Profile** in the **Assets** section to navigate to the **Assets** tab.



4. In the **SE Profile** section, click **Add**.



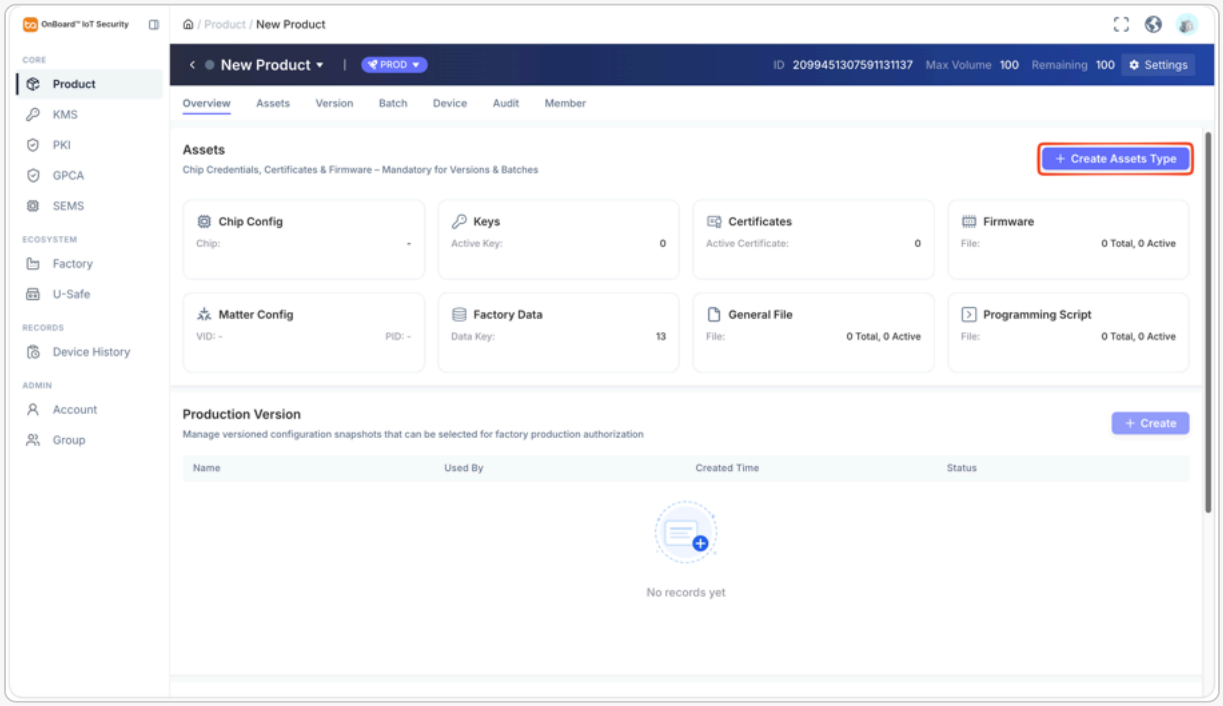
5. In the **Add SE Profile** window, select the SE Profile to be assigned and click **Add**. Meanwhile, you can also create and add a custom tag in the **Tag** field as needed (this tag allows programming scripts to automatically identify and select the corresponding SE Profile later).



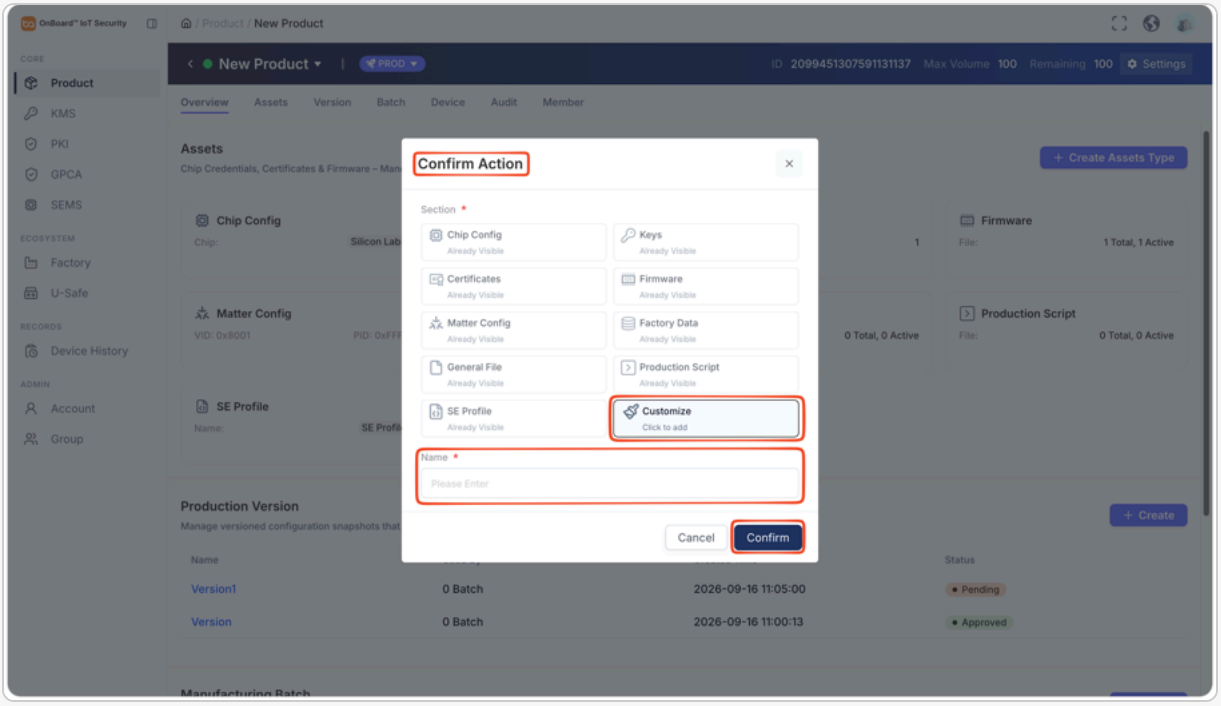
Customize (Optional)

> **TIP**
>
> **Customize** allows you to customize the data that needs to be sent to the factory using the key:value format.

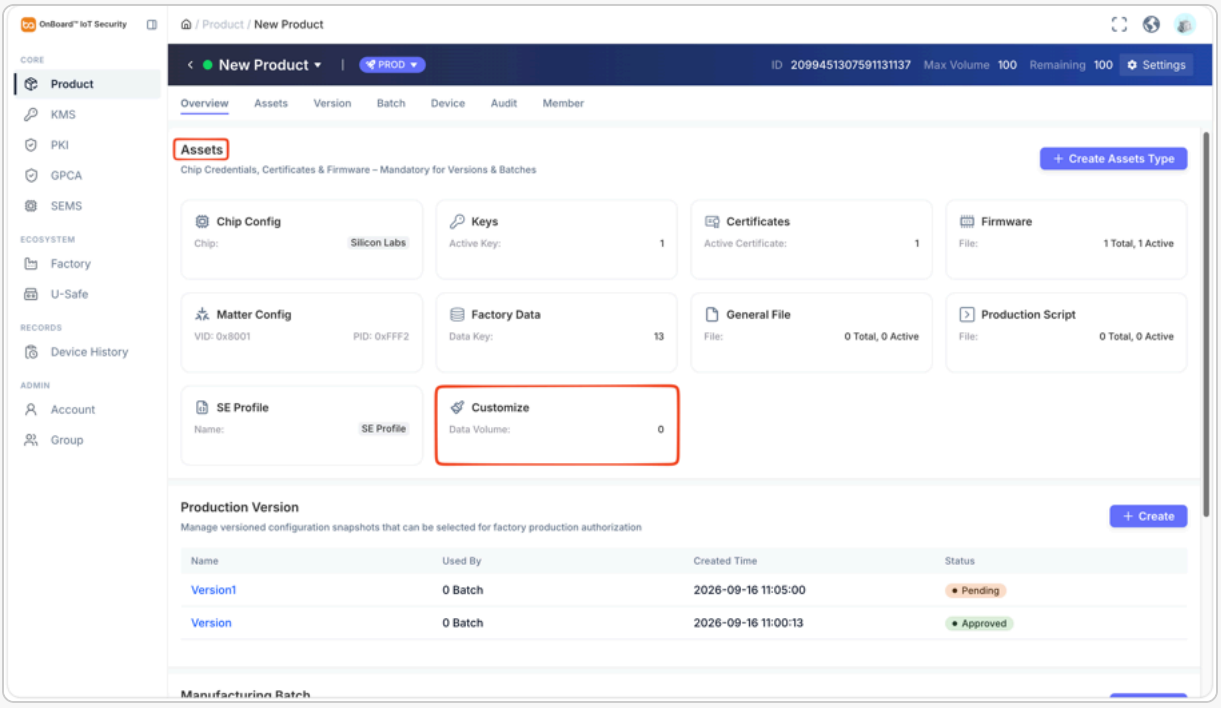
1. On the product page, click **Create Assets Type**.



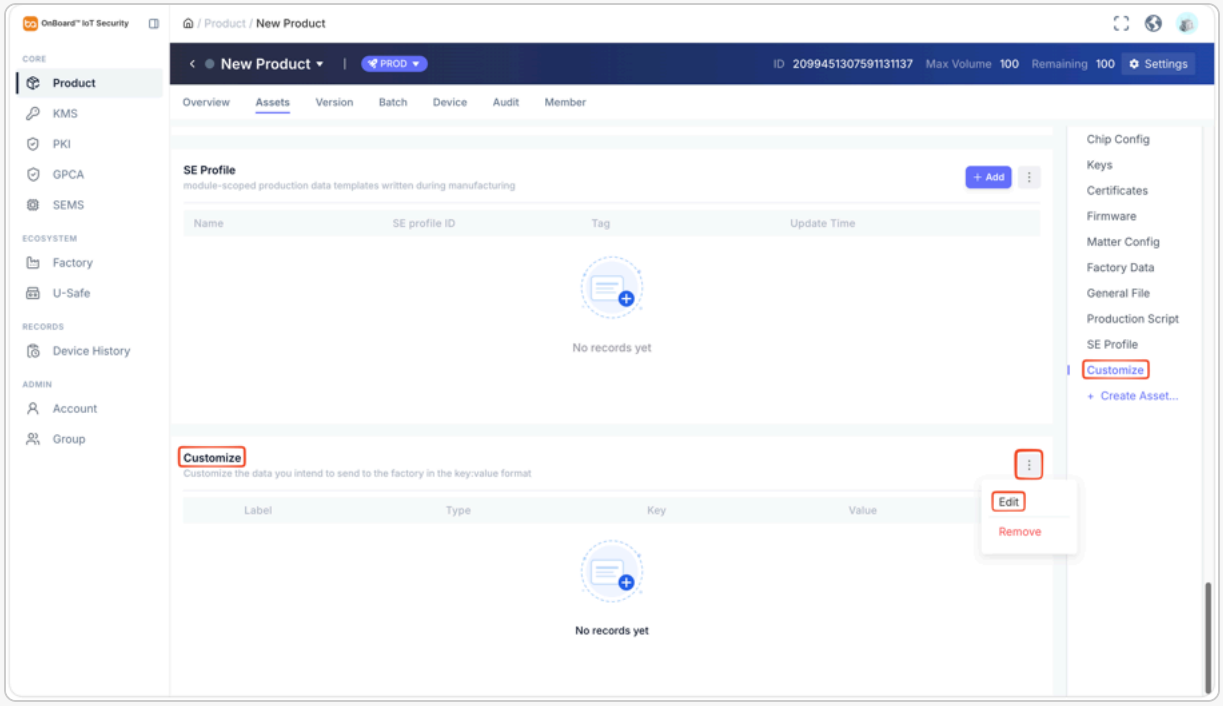
2. In the **Confirm Action** window, select the **Customize** asset type and enter the asset name, then click **Confirm** to add the custom asset.



3. Select **Customize** in the **Assets** section to navigate to the **Assets** tab.



4. In the **Customize** section, click the Options icon and select **Edit**, then you can modify the asset name and enter the relevant information for the custom asset.



Description of custom asset information:

Information	Mandatory	Description
Label	Yes	A label used to identify the custom data.
Type	Yes	The supported data types include: String, Number, Boolean, Key, Certificate, and File.
Key	Yes	Assign keys to files. During later programming, the programming script can retrieve and use the corresponding files through their keys.
Value	Yes	The value corresponding to the custom data.

5. Click **Save** to complete the configuration of the custom asset.

Version: v3.4.0 (Latest)

How to check products in OnBoard™ IoT Security

> **TIP**
>
> In the configuration section of the corresponding asset, users belonging to the same tenant can download the files when configuring Firmware, Matter Config (uploaded CD file), Factory Data (uploaded file), General File, and Programming Script.

This article will guide you on how to check product basic information and configurations in OnBoard™ IoT Security (OBIS).

Prerequisites

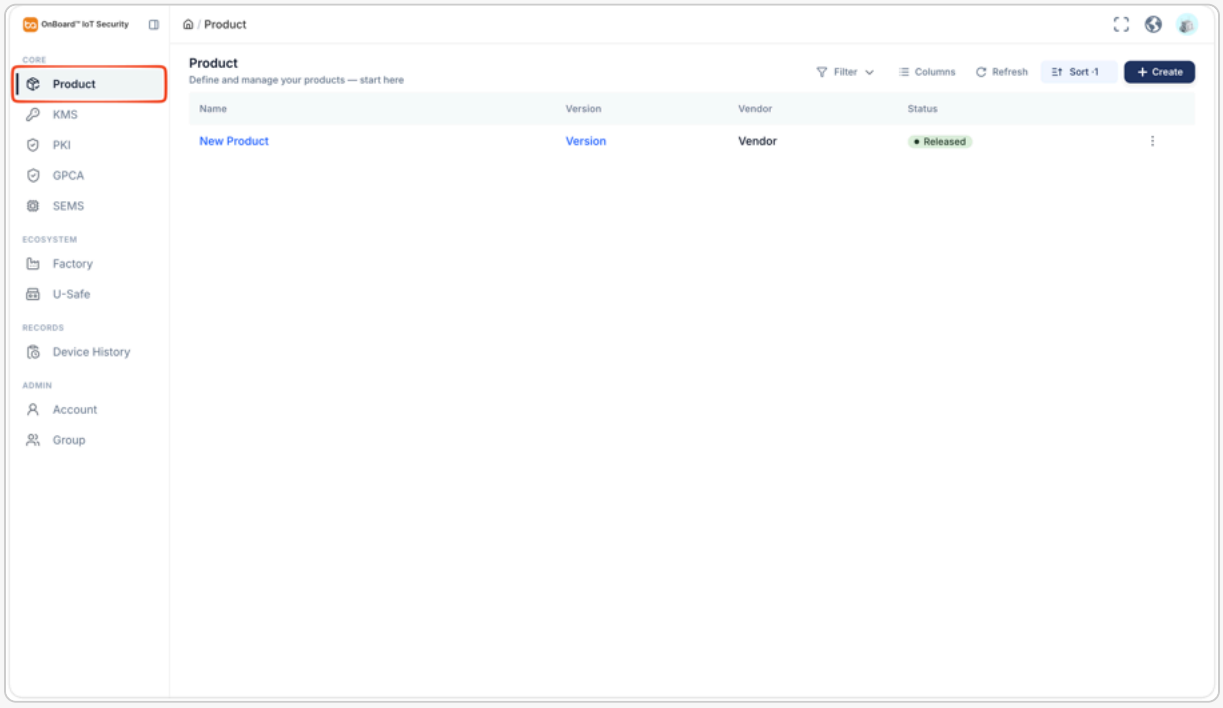
Before getting started, please ensure that you have product role permissions for the corresponding product.

Instructions

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

TIP

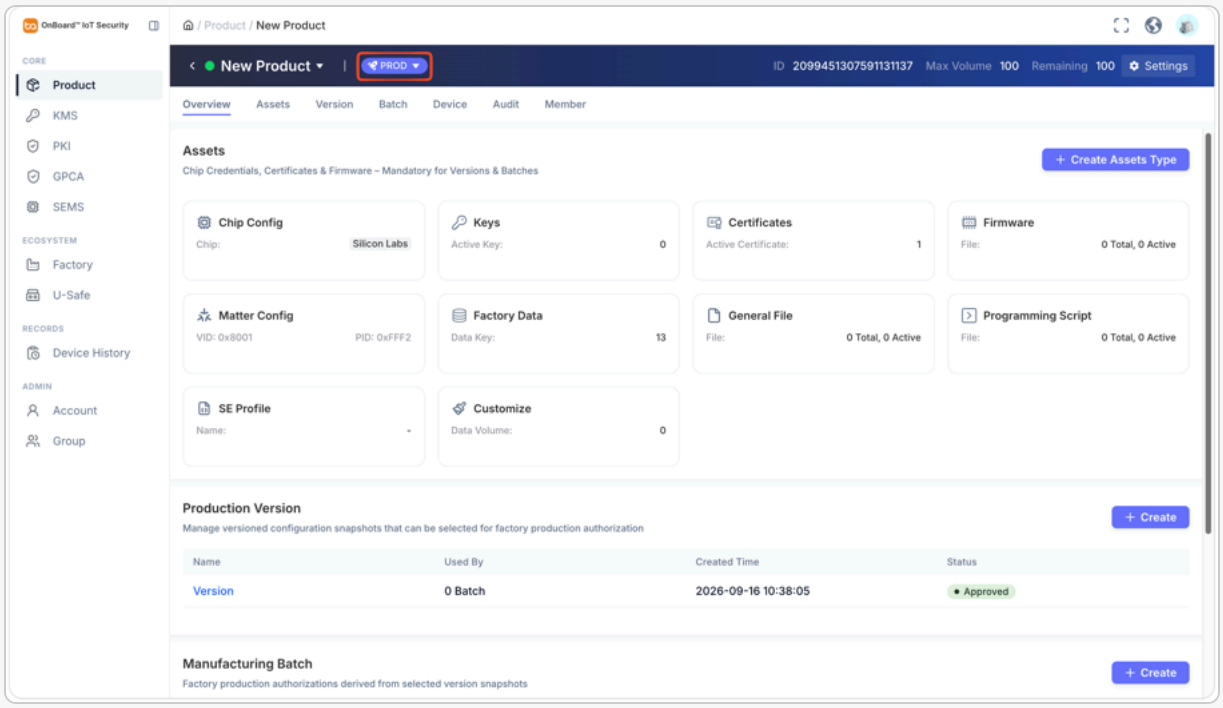
- The product list only displays the products you are involved in.
- Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Description of product status:

Status	Description
Draft	Status before a version is created.
Released	Status after a version is created. **Note**: If all versions of a product are deleted, the product status will revert to **Draft**.

3. On the product page, select the **TEST** or **PROD** environment, you can check the product-related information (such as **Assets**, **Production Version**, and **Manufacturing Batch**).



Version: v3.4.0 (Latest)

How to manage products in OnBoard™ IoT Security

> **TIP**
>
> In the configuration section of the corresponding asset, the following operations can be performed on the files uploaded during asset configuration:
>
> - You can deactivate, activate, or remove the files when configuring Keys, Certificates, Firmware, General File, and Programming Script.
> - Files added during the configuration of Firmware, Matter Config (uploaded CD file), Factory Data (uploaded file), General File, and Programming Script can only be downloaded by users within the same tenant.
>
> Unable to deactivate or remove certificates and keys that are referenced by assets.

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Edit product information
- Archive or unarchive a product
- Deactivate or activate a product resource
- Remove a product resource
- Add a product asset type
- Remove a product asset type

Prerequisites

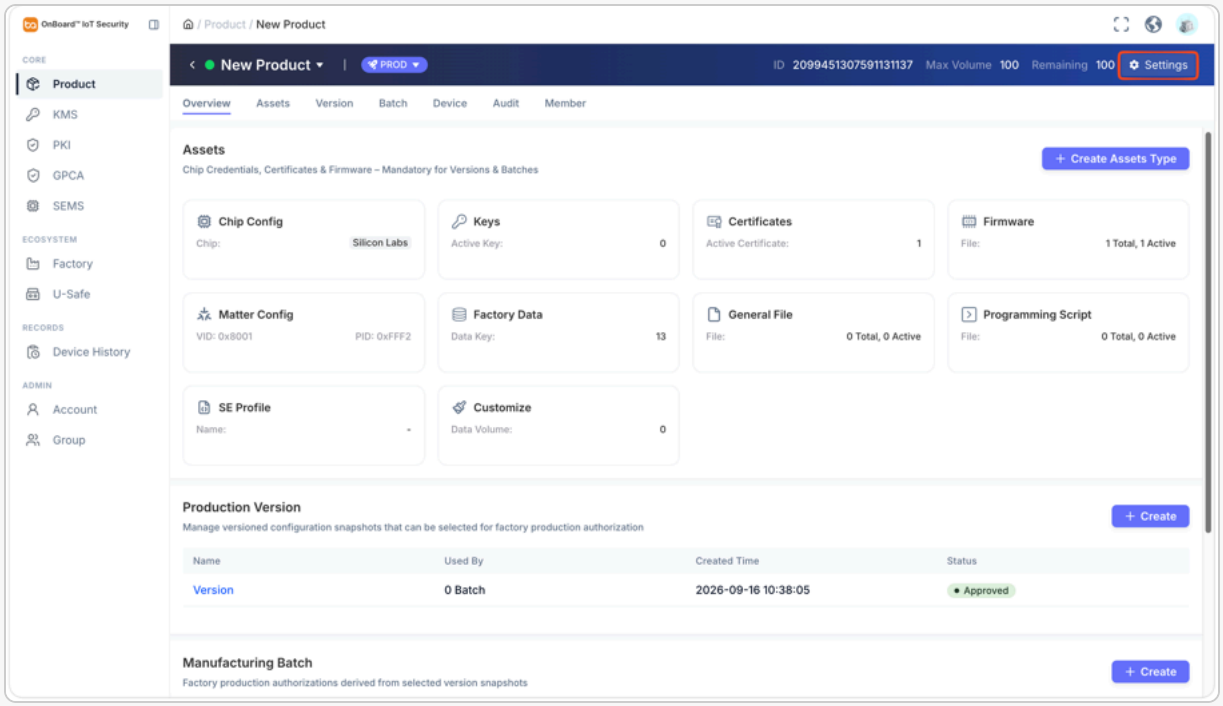
Before getting started, please ensure that you have product role permissions for the corresponding product: Product Owner, Product Manager, or Resource Manager (can only deactivate, activate, or remove product assets).

Edit product information

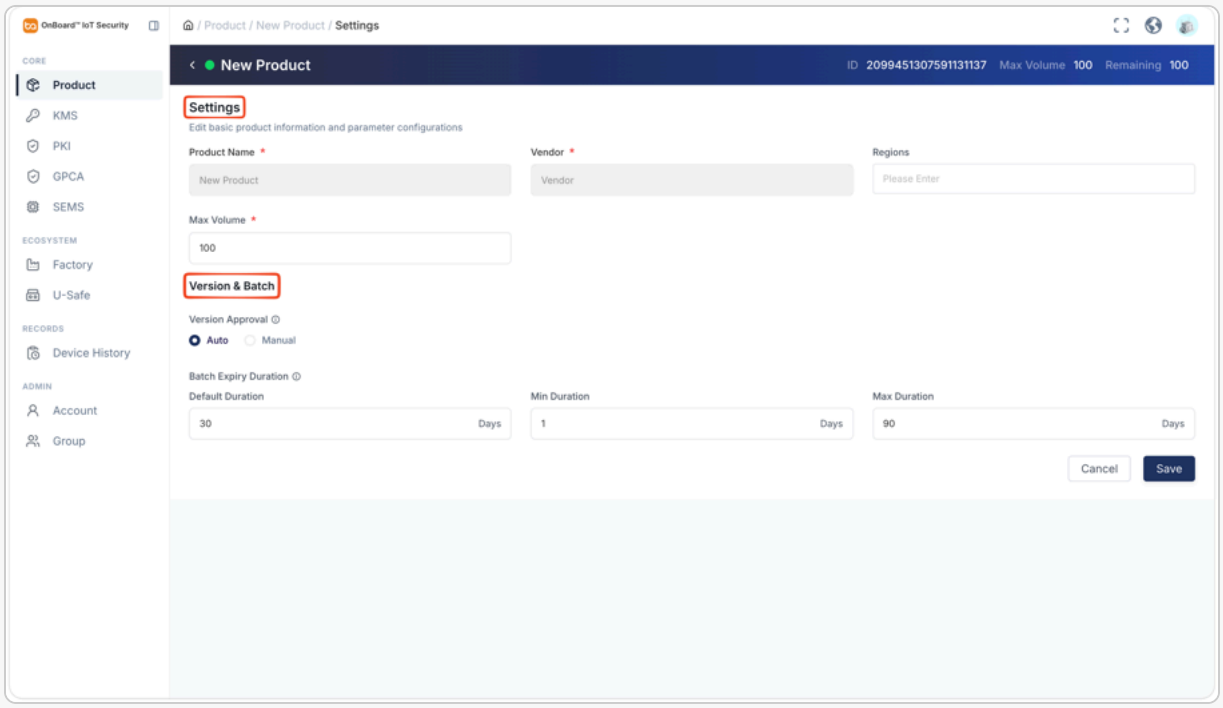
> **TIP**
>
> The Resource Manager doesn't have permission to edit the product information.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. Click **Settings** to edit the corresponding product information.

   > **NOTE**
   >
   > For more information, refer to the description of product basic information.



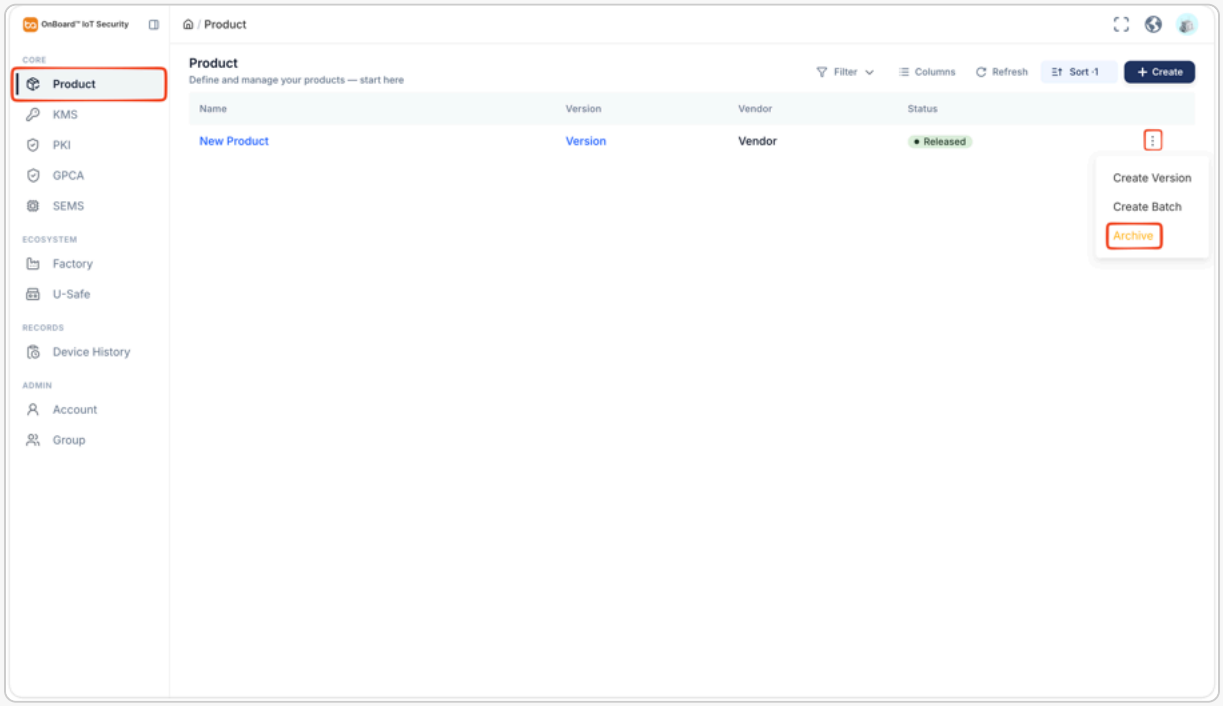
- **Settings** section: **Regions** and **Max.Volume**
- **Version & Batch** section: **Version Approval** and **Batch Expiry Duration**



Archive or unarchive a product

> **TIP**
>
> Once a product is archived, no further editing can be made, including information modifications, resource configuration, version creation, and batch creation. The Resource Manager doesn't have permission to manage product archiving.

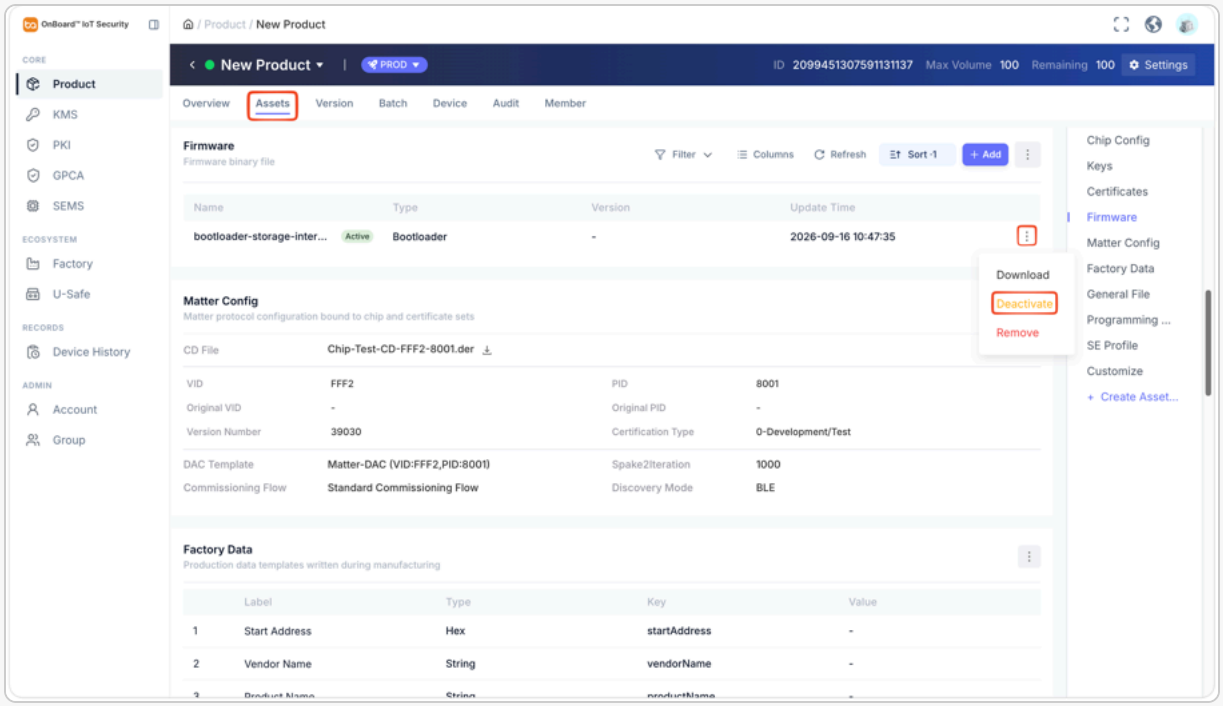
1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**.
3. Click the Options ⋮ icon for the corresponding product and then select **Archive** or **Unarchive** to archive or unarchive the product.



Deactivate or activate a product resource

> **INFO**
>
> When creating a version or batch, you can't select resources that have been deactivated.
>
> Before deactivating a key and certificate, please ensure that it has not been used to create versions or batches. Otherwise, you will see the message "Resource is in use and cannot be deactivated or removed".

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. Select the **Assets** tab, and then find the corresponding resource in the **Keys**, **Certificates**, **Firmware**, **General File**, **Programming Script**, or **SE Profile** section. Then click the Options ⋮ icon and select **Deactivate** or **Active** to deactivate or activate the product resource.



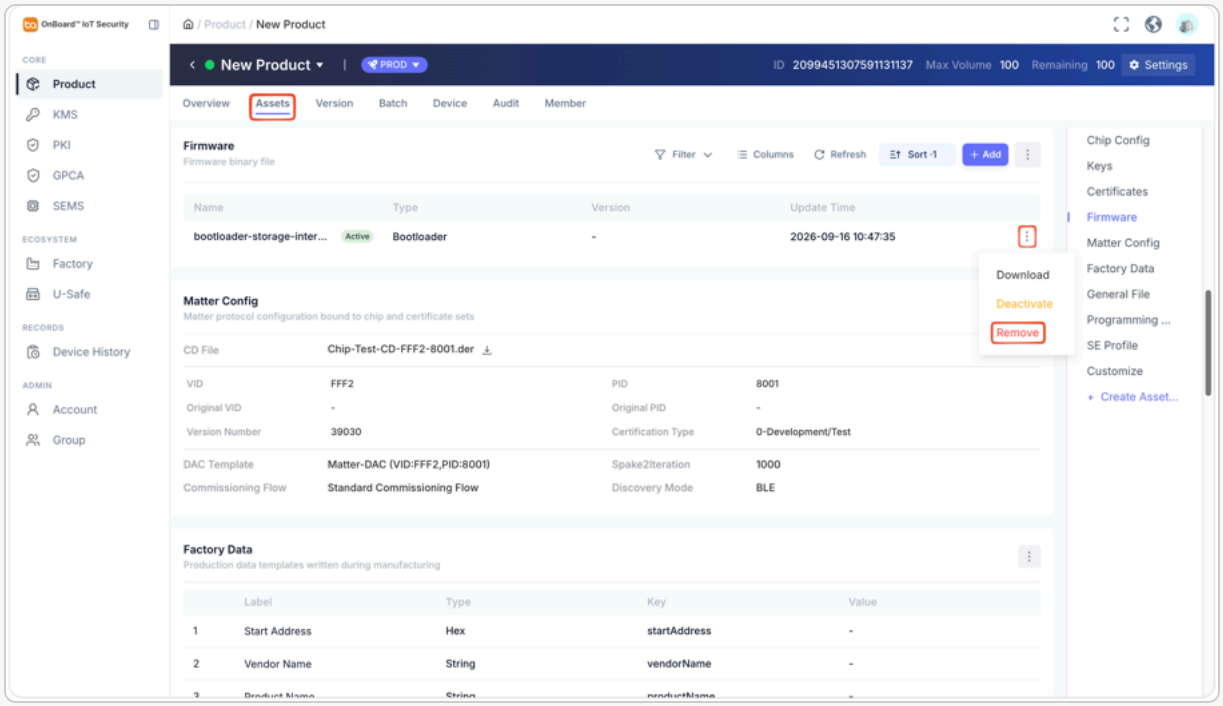
Remove a product resource

> **INFO**
>
> Before removing a key and certificate, please ensure that it has not been used to create versions or batches. Otherwise, you will see the message "Resource is in use and cannot be deactivated or removed".

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. Select the **Assets** tab, and then find the corresponding resource in the **Keys**, **Certificates**, **Firmware**, **General File**, **Programming Script**, or **SE Profile** section. Then click the Options ⋮ icon and select **Remove** to remove the product resource.

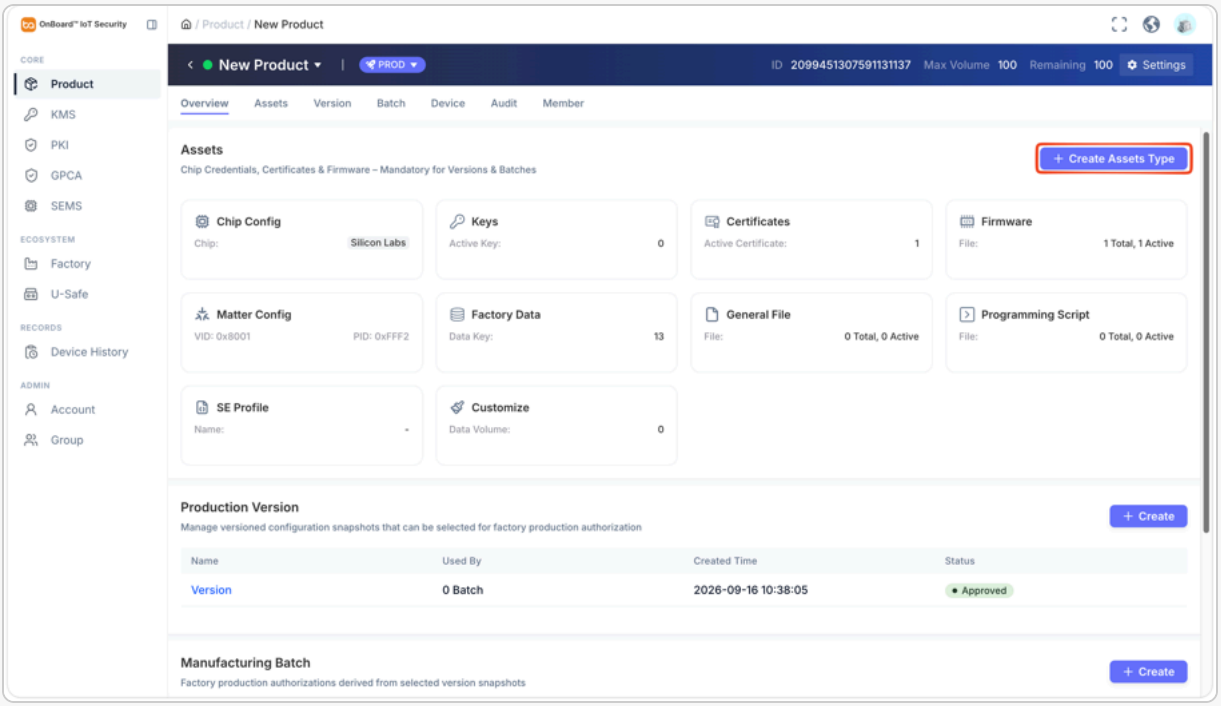


Add a product asset type

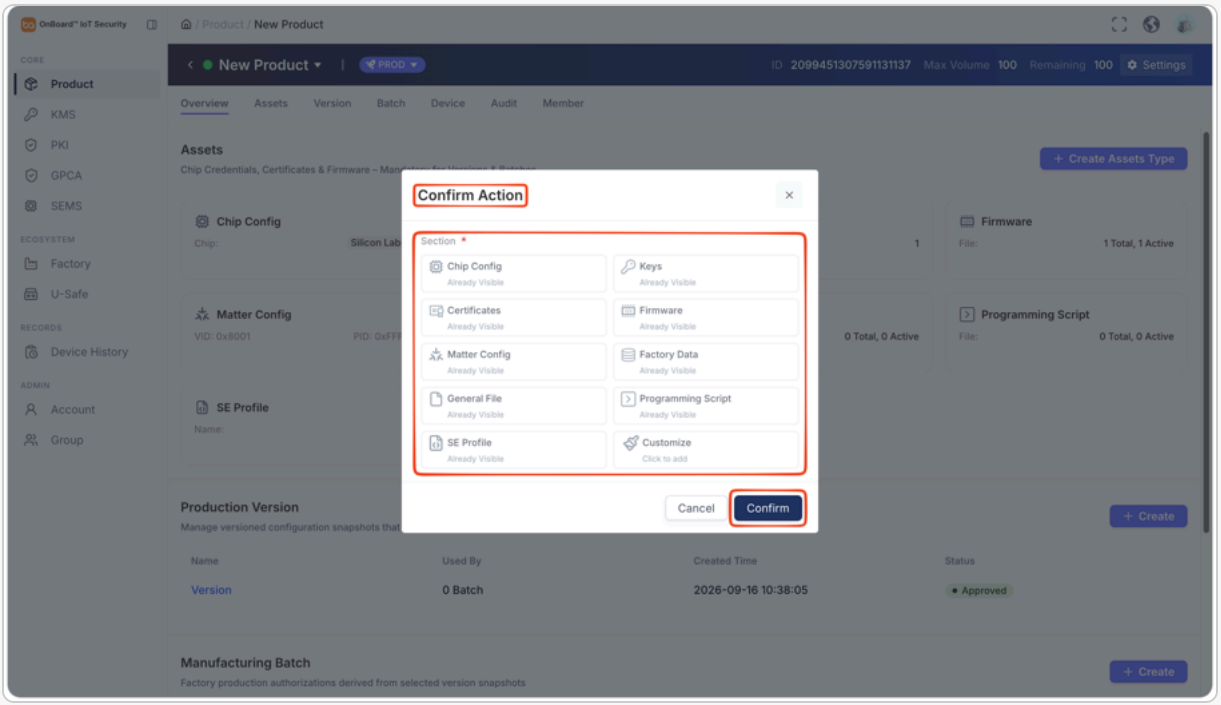
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. On the product page, click **Create Assets Type**.



4. In the **Confirm Action** window, select the asset type that you want to add (assets that already exist can't be added, with the exception of custom assets), and then click **Confirm** to add the asset type.



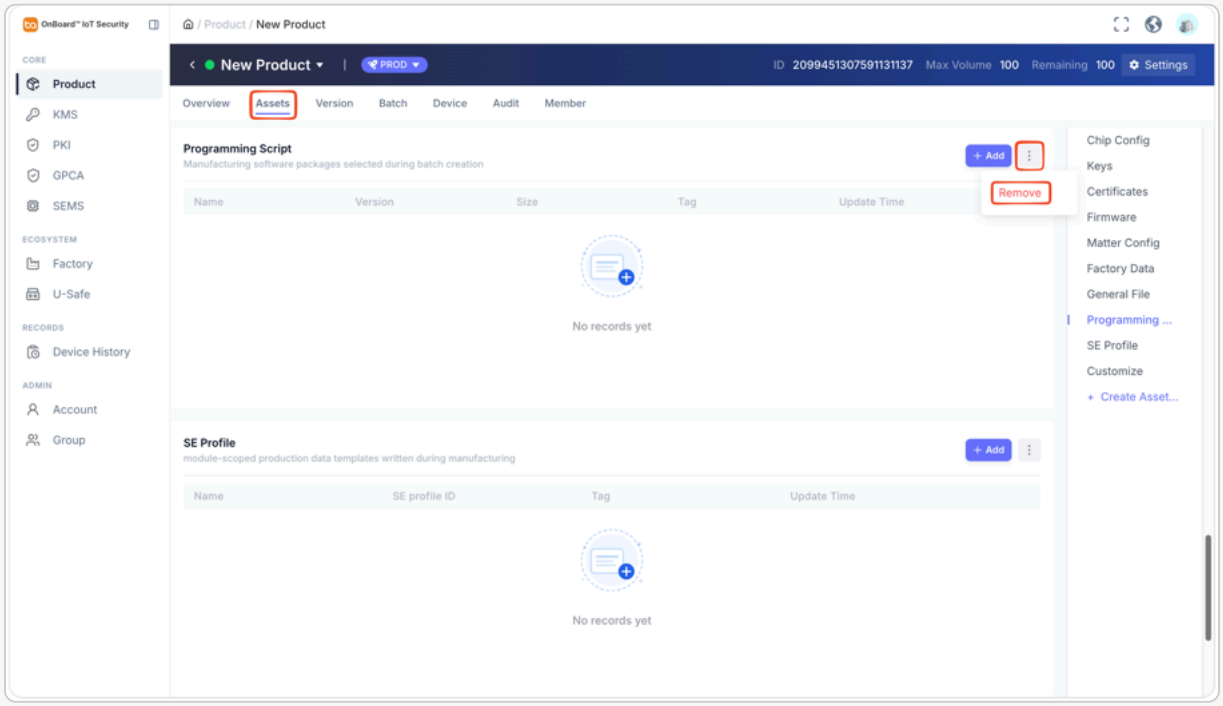
Remove a product asset type

> **TIP**
>
> Before removing an asset type, please ensure that none of the resources under that type have been used to create versions or batches. Otherwise, the **Remove** option will be grayed out and unclickable.

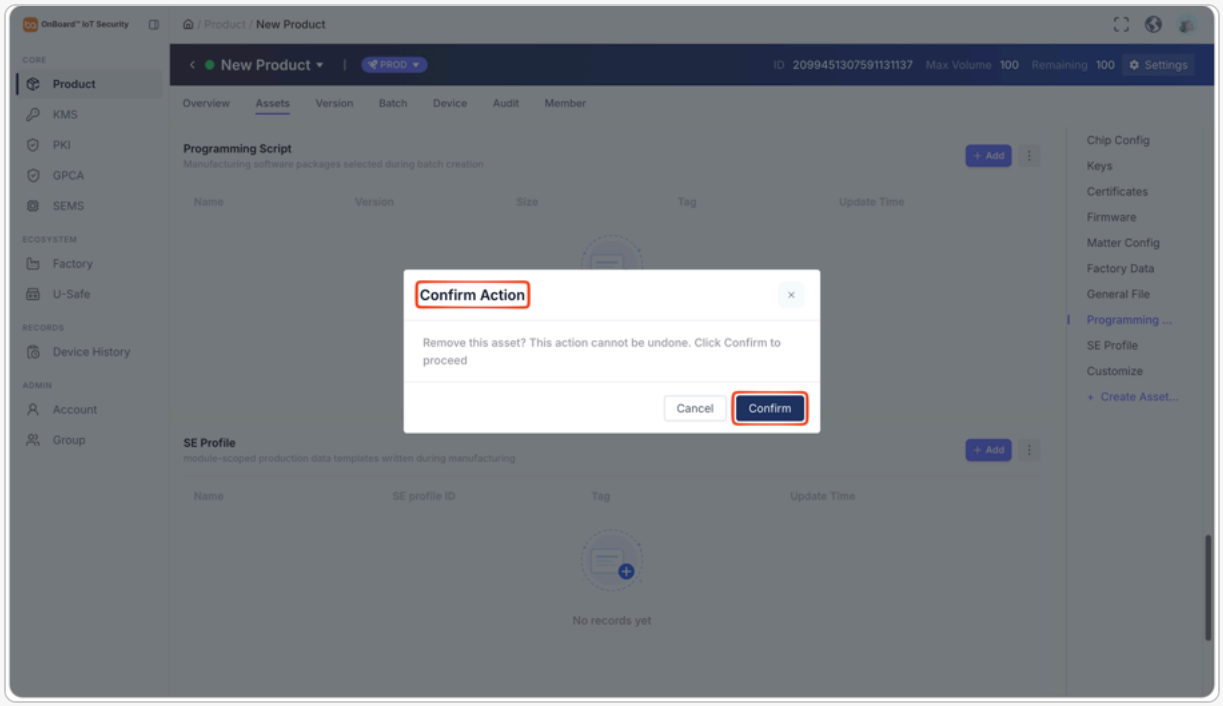
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. Select the **Assets** tab, click the Option icon for the corresponding asset and then select **Remove**.



4. In the **Confirm Action** window, click **Confirm** to remove the asset.



Version: v3.4.0 (Latest)

How to create a version in OnBoard™ IoT Security

This article will guide you on how to create a version in OnBoard™ IoT Security (OBIS) to prepare for batch creation. Each product can create multiple versions.

Prerequisites

Before getting started, please ensure that:

- The product has already been configured.
- You have product role permissions for the corresponding product: Product Owner, Product Manager, or Version Manager.

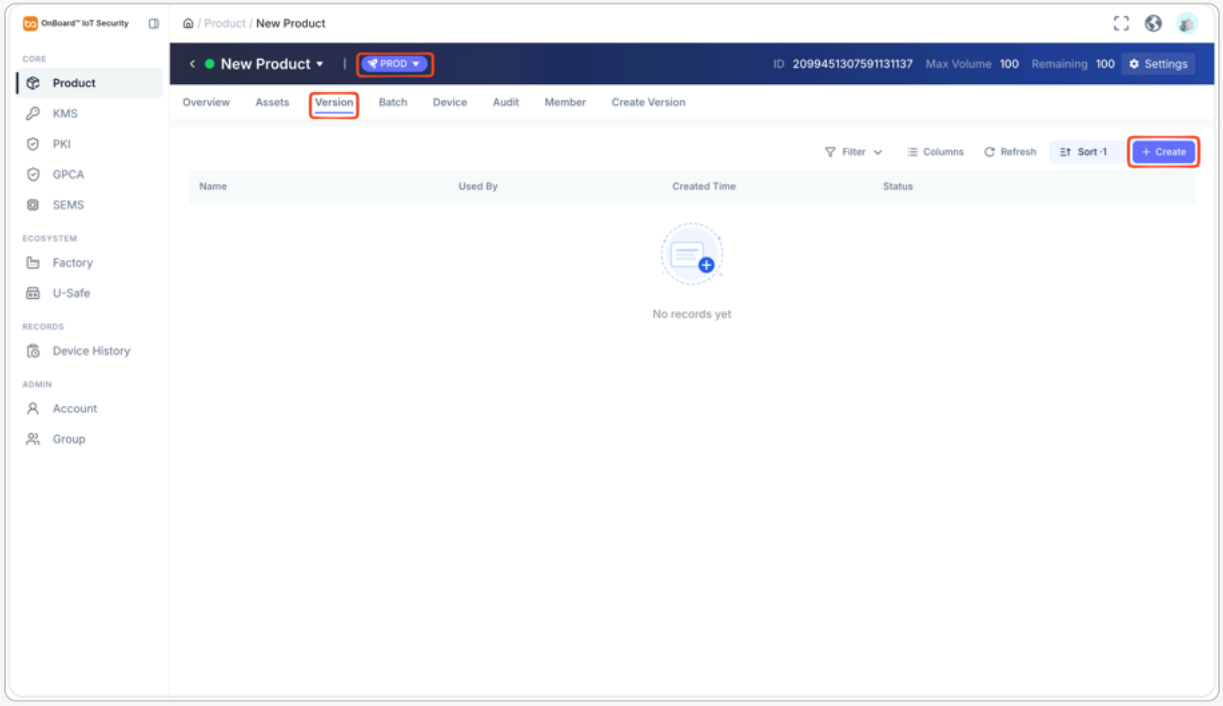
Instructions

> **TIP**
>
> Supports quickly creating a new version based on a historical version. Select the corresponding version on the **Version** tab, then click **Actions** and select **Copy**.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

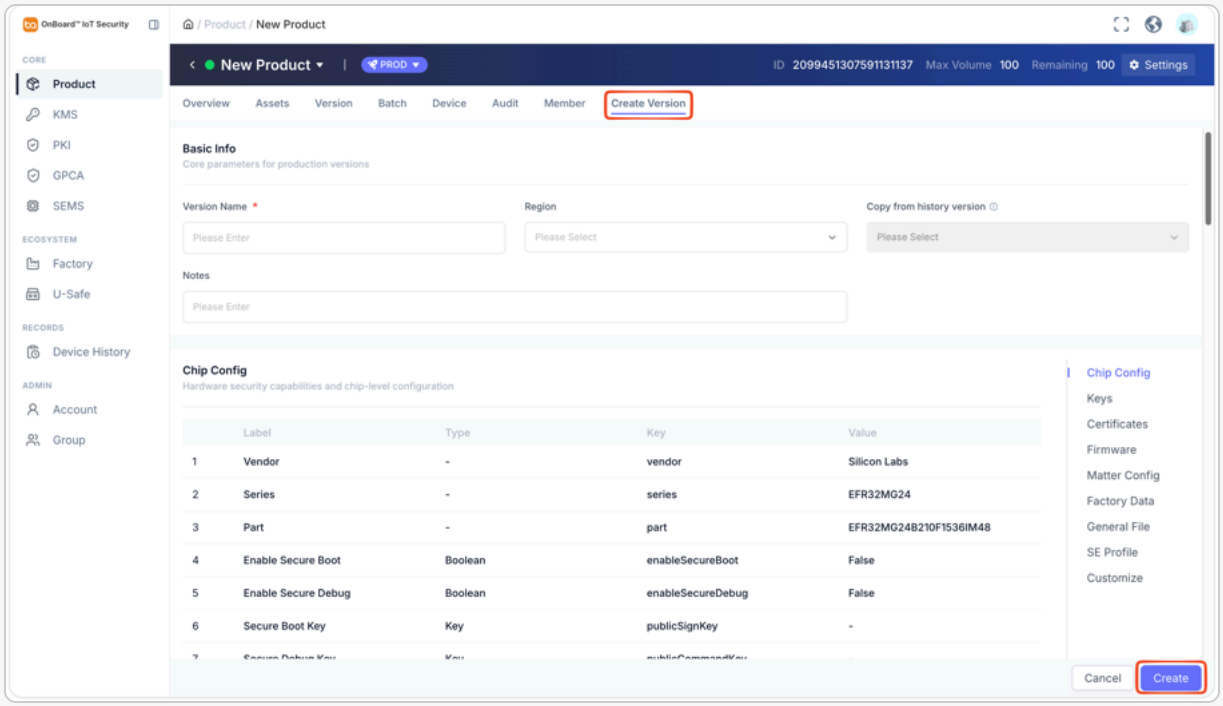
3. On the product page, select the **TEST** or **PROD** environment, select the **Version** tab and then click **Create**. The page will navigate to the **Create Version** tab.

> **TIP**
>
> If the **Create** button appears grayed out, it is currently unavailable. Please check whether all required assets for your product have been configured. Once everything is properly configured, the **Create** button will be enabled automatically.



4. On the **Create Version** tab, select and enter the version-related information.

> **TIP**
>
> When adding product assets, only assets that have not been deactivated can be selected. For more information, refer to Deactivate or activate a product asset.



Description of version information:

Information	Mandatory	Description
Version Name	Yes	The version name must be unique within the same environment.
Region	No	Select and set the region for the version. **Note**: Available regions depend on the supported regions configured when the product was created.
Copy from History Version	No	You can select a historical version as a template for modification.

Information	Mandatory	Description
Notes	No	Provide additional information related to the version, such as special requirements and important notes.
Chip Config	Yes	The Chip Config configured on the **Assets** tab.
Keys	No	The Keys configured on the **Assets** tab.
Certificates	Yes	The Certificates configured on the **Assets** tab.
Firmware	No	The Firmware configured on the **Assets** tab.
Matter Config	Yes	The Matter Config configured on the **Assets** tab. The **CD File** and **PID** can be reselected, while other information can't be modified.
Factory Data	Yes	The Factory Data configured on the **Assets** tab. All values can be modified. **Note**: All **Factory Data** items marked as required must be provided with valid values. Otherwise, the version can't be created.
SE Profile	No	The SE Profile configured on the **Assets** tab.
General File	No	The General File configured on the **Assets** tab.

5. After verifying that all information is correct, click **Create** at the bottom of the page to complete the version creation.

> **TIP**
>
> If manual approval was enabled when the product was created, versions created in the PROD environment will require manual approval by the Product Owner or Product Manager.
>
> - Before the version is approved, the version status is **Pending** and it can't be used to create a batch.
> - Once the version is approved, the version status changes to **Approved**.

Version: v3.4.0 (Latest)

How to check versions in OnBoard™ IoT Security

This article will guide you on how to check version information and configuration in OnBoard™ IoT Security (OBIS).

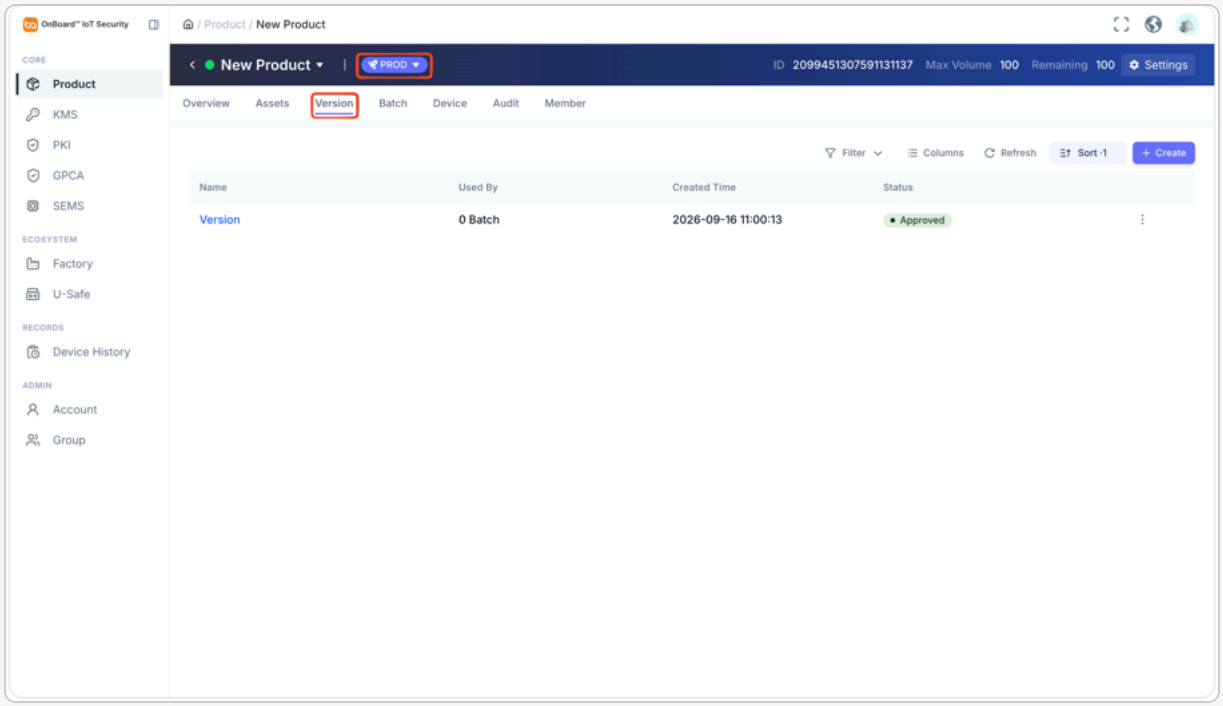
Prerequisites

Before getting started, please ensure that you have product role permissions for the corresponding product.

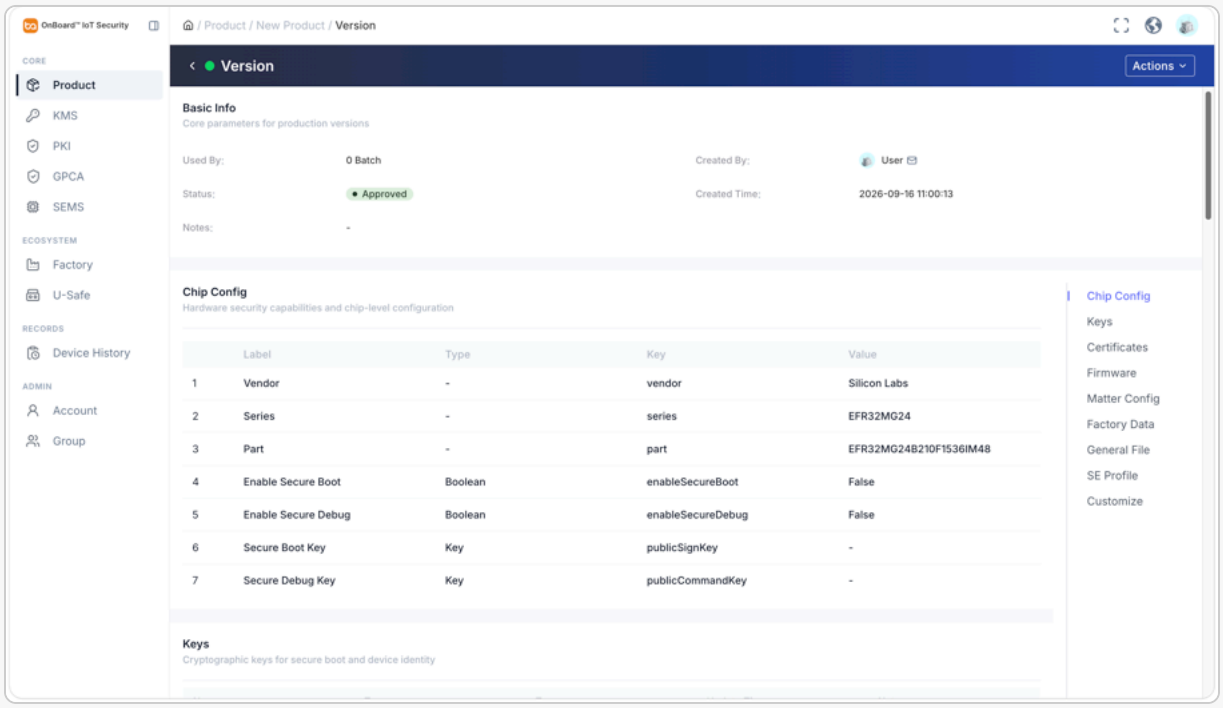
Instructions

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. On the product page, select the **TEST** or **PROD** environment. Select the **Version** tab, and then select the corresponding version to navigate to the version page.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



4. On the version page, you can check the version-related information (such as **Chip Config**, **Certificate**, and **Firmware**).



Version: v3.4.0 (Latest)

How to manage versions in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Approve or reject a version
- Delete a version

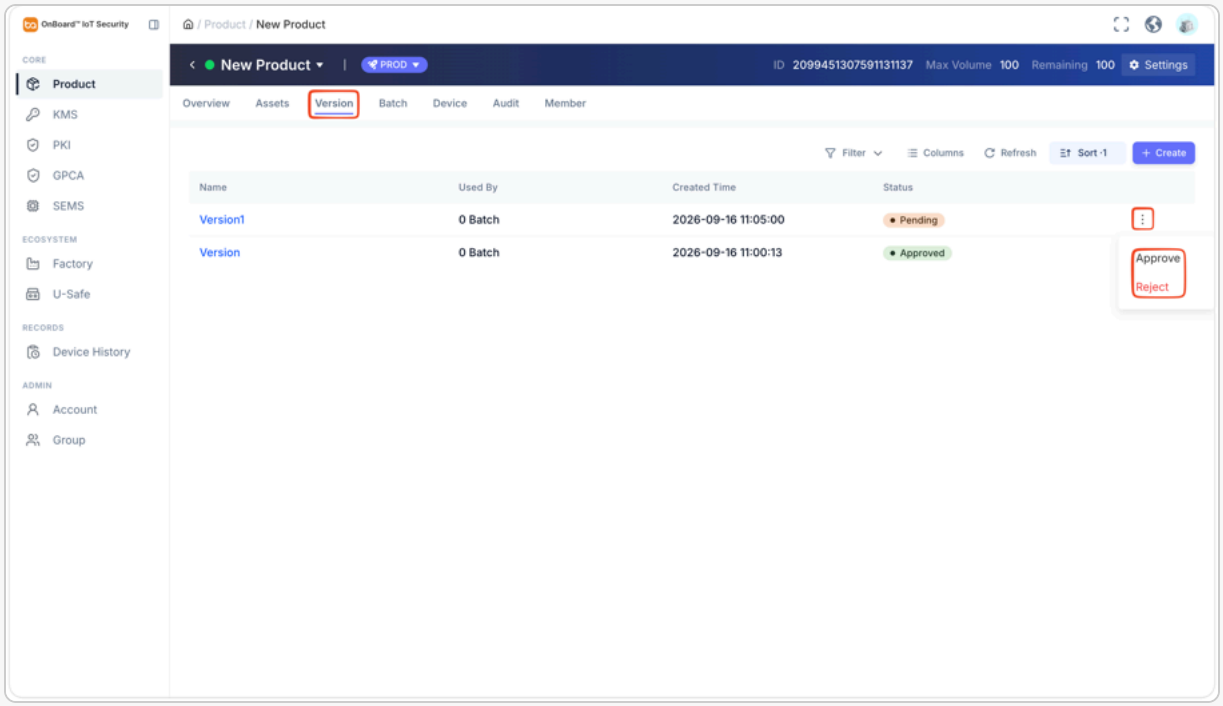
Prerequisites

Before getting started, please ensure that you have product role permissions for the corresponding product: Product Owner, Product Manager, or Version Manager.

Approve or reject a version

> **TIP**
>
> If manual approval was enabled when the product was created, versions created in the PROD environment will require manual approval (approve or reject) by the Product Owner or Product Manager.
>
> - Once the version is approved, the version status will change to **Approved** and it can be used to create a batch.
> - Once the version is rejected, the version status will change to **Rejected**, and a new version needs to be created and submitted for approval.
>
> The Product Owner or Product Manager can disable it in the **Settings** of the product.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. Select the **TEST** or **PROD** environment in the product page. Select the **Version** tab, click the Options ⋮ icon for the corresponding version and then select **Approve** or **Reject**.



Delete a version

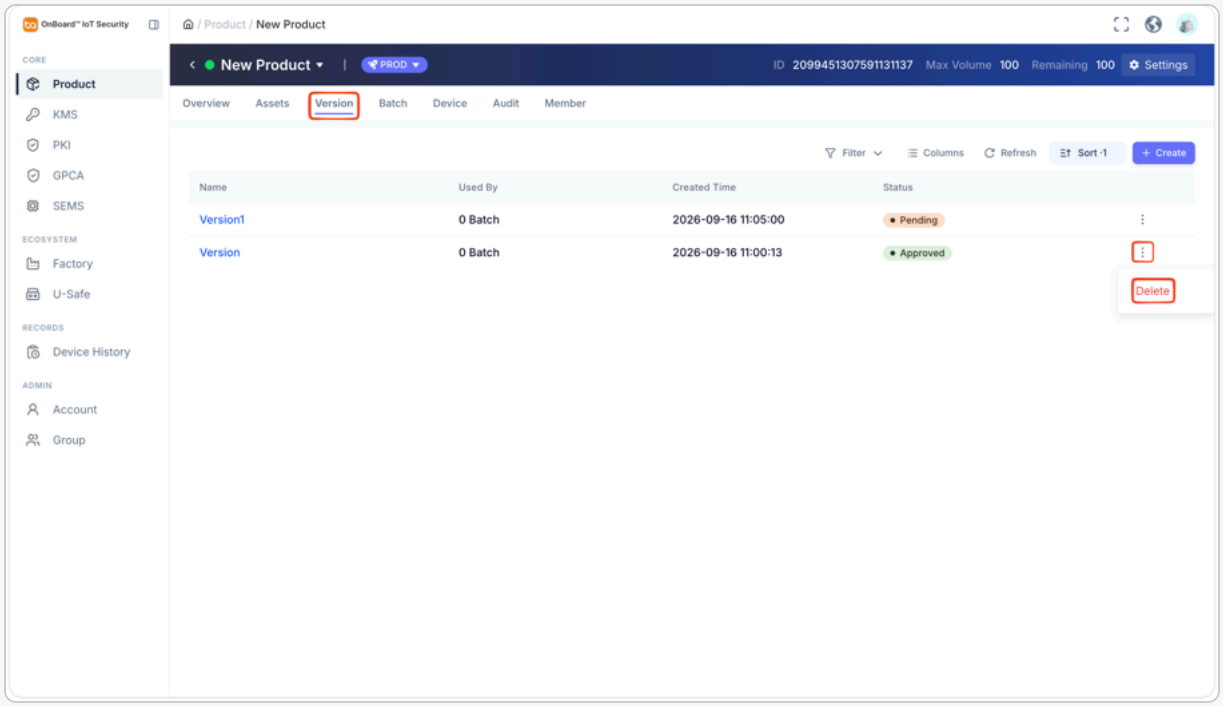
> **WARNING**
>
> Deleted versions cannot be recovered. Please proceed with caution.

> **TIP**
>
> Before deleting a version, please ensure that:
>
> - The version status is not **Pending** (a version in **Pending** can't be deleted).
> - The version is not associated with any batches (once a batch has been created using this version, the version can no longer be deleted).

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. Select the **TEST** or **PROD** environment in the product page. Select the **Version** tab, click the Options ⋮ icon for the corresponding version and then select **Delete**.



Version: v3.4.0 (Latest)

How to create a batch in OnBoard™ IoT Security

> **INFO**
>
> Currently, batches can't be modified or deleted after creation.

This article will guide you on how to create a batch in OnBoard™ IoT Security (OBIS), which can then be assigned to programming stations (local factory & cloud factory) for programming. Each version can create multiple batches, and a batch represents a production plan based on that version.

Prerequisites

Before getting started, please ensure that:

- The version has already been created and its status is **Approved** (If manual approval was enabled when the product was created, versions created in the PROD environment will require manual approval by the Product Owner or Product Manager).
- You have product role permissions for the corresponding product: Product Owner, Product Manager, or Batch Manager.
- The factory has already been created, the HSM U-Safe has already been added (local factory), and the factory status is **Normal**.

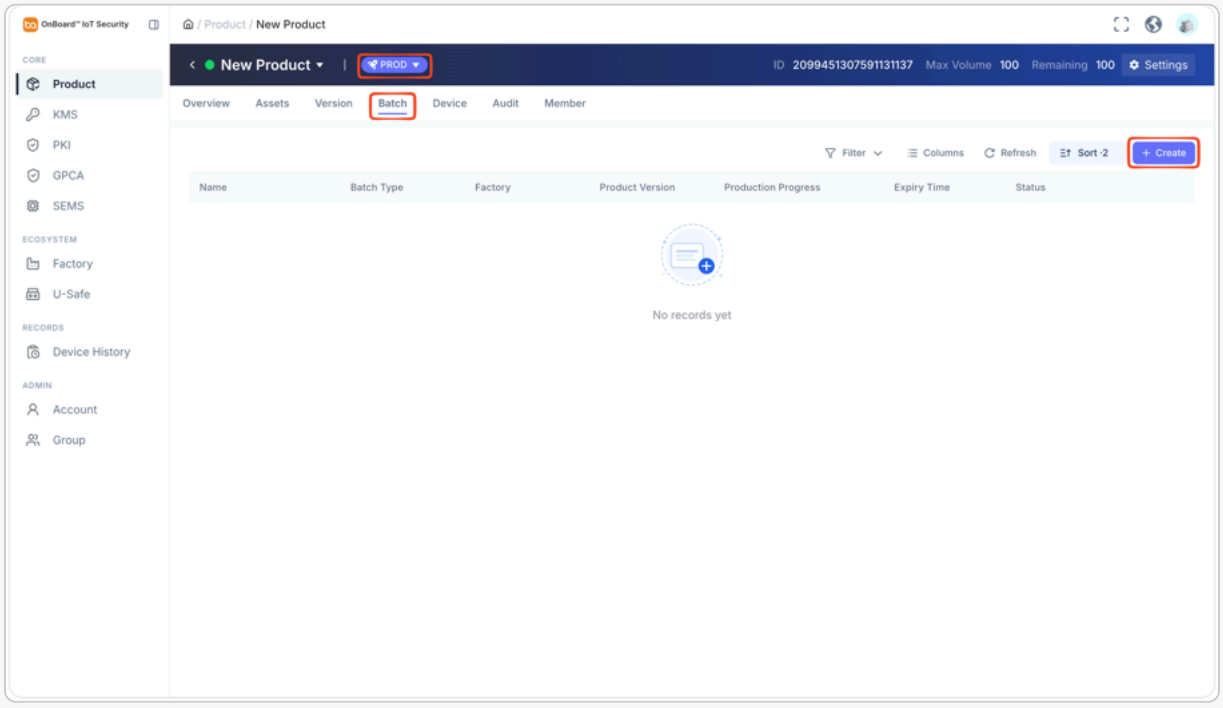
Instructions

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

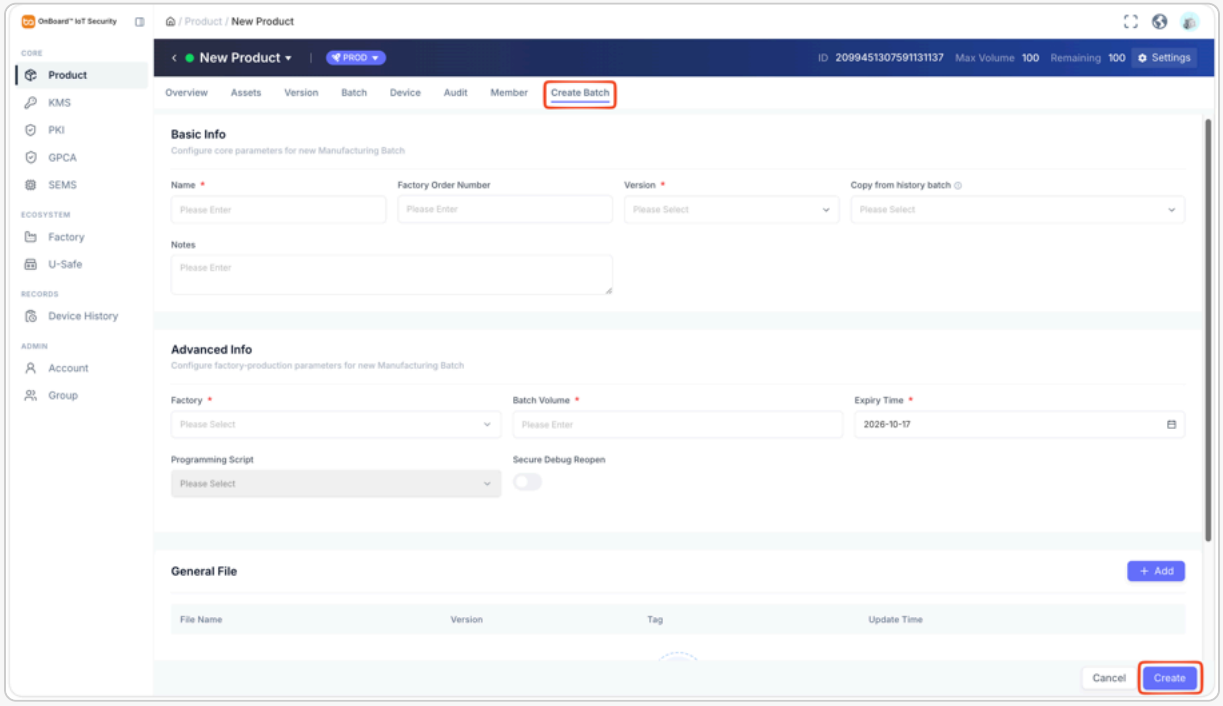
3. On the product page, select the **TEST** or **PROD** environment, select the **Batch** tab and then click **Create**. The page will navigate to the **Create Batch** tab.

> **TIP**
>
> If the **Create** button appears grayed out, it is currently unavailable. Please check whether a version has been created. After a version is created, the **Create** button will be enabled automatically.



4. On the **Create Batch** tab, select and enter the batch-related information.

> **TIP**
>
> When adding product assets, only assets that have not been deactivated can be selected. For more information, refer to Deactivate or activate a product asset。



Description of batch information:

Information	Mandatory	Description
Name	Yes	The batch name must be unique.

Information	Mandatory	Description
Factory Order Number	No	Associate with a specific factory order.
Version	Yes	Select the version with the **Approved** status.
Copy from History Batch	No	You can select a historical batch as a template for modification.
Notes	No	Provide additional information related to the batch, such as special requirements and important Notes.
Factory	Yes	Select a factory with the **Normal** status. **Note**: ◦ Batch data will be synchronized and updated in the factory's Batch List. ◦ When the number of unexpired batches in the factory exceeds 200, new batches cannot be created. Please delete existing unexpired batches in OBIS or OnBoard Edge Service before creating a new one.

Information	Mandatory	Description
Batch Volume	Yes	Set the batch volume. ◦ If the batch is in the TEST environment, this volume will not be deducted from the total. ◦ If the batch is in the PROD environment, this volume will be deducted (the unproduced volume of an expired batch will not be reclaimed). Additionally, the batch volume must be less than or equal to the **Product Volume Balance** (the Max Volume configured when creating the product).
Expiry Time	Yes	Specify the validity period or completion deadline for the batch. **Note**: Expired batches can no longer be used. In OnBoard Edge Service, the batch status will display as **Expired**. Available time depends on the Batch Expiry Duration configured when creating the product.
Programming Script	No	Add the Programming Script configured in the **Assets** tab as needed. If it is not required at the moment, you can select the programming script for a specific batch later in the Programming Station client.

Information	Mandatory	Description
Secure Debug Reopen	No	This feature uses the configured Secure Debug Key to unlock the chip's debug interface and erase the existing data, enabling the chip to be reprogrammed. **Note**: To enable the **Secure Debug Reopen** feature when creating a batch, the Secure Debug feature must be enabled when configuring the product. For more information about enabling the Secure Debug feature, refer to the description of Chip Config information.
General File	No	The Generate File configured in the corresponding version.

5. After verifying that all information is correct, click **Create** at the bottom of the page to complete the batch creation.

> **TIP**
>
> Once the batch is created, it will be synchronized with the factory. If synchronization fails, navigate to the **Batch** tab of the product, click the Options ⋮ icon for the corresponding batch and then select **Resync**. For more information, refer to the description of batch status and batch synchronization status.

Version: v3.4.0 (Latest)

How to check batches in OnBoard™ IoT Security

This article will guide you on how to check batch information and configuration in OnBoard™ IoT Security (OBIS).

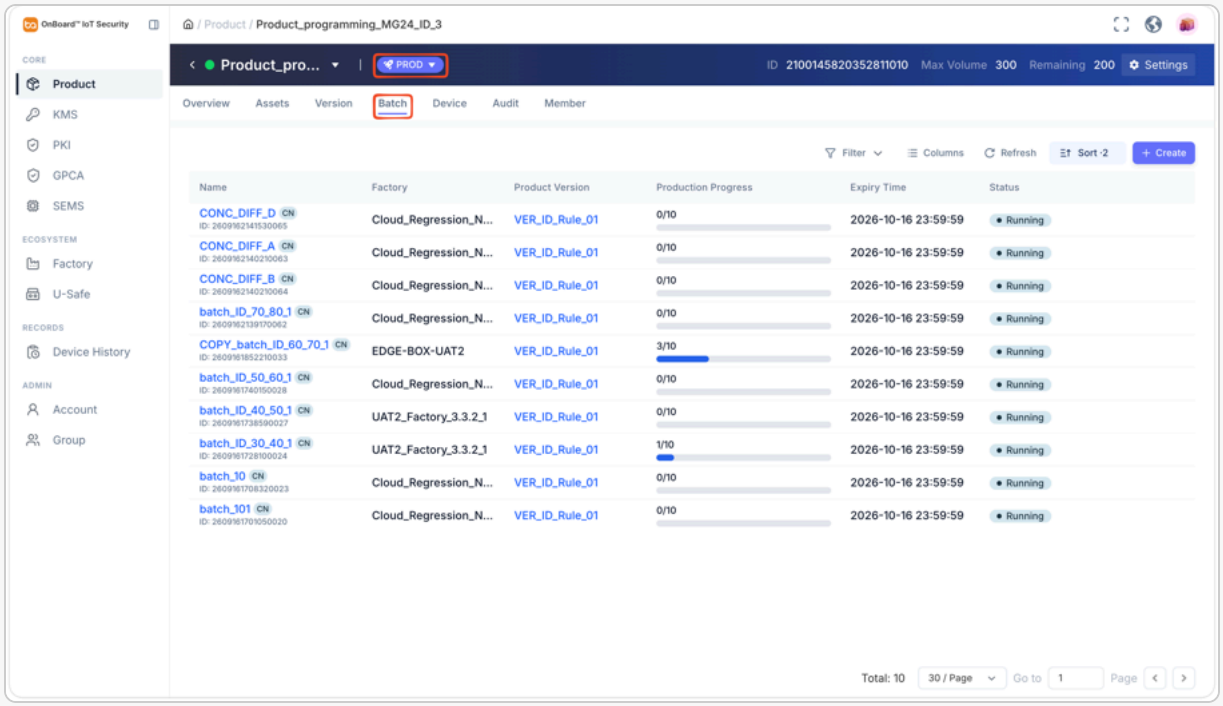
Prerequisites

Before getting started, please ensure that you have product role permissions for the corresponding product.

Instructions

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. On the product page, select the **TEST** or **PROD** environment. Select the **Batch** tab, and then select the corresponding batch to navigate to the batch page.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Description of **Batch Status**:

Status	Description
Generating	The status when the batch is being generated after creation.
Generate Failed	The status after the batch generation fails. You can try to regenerate it: On the **Batch** tab of the product, click the Options ⋮ icon for the corresponding batch and then select **Resync**.
Generated	The status after the batch is successfully generated.
Running	The status after the batch is successfully synchronized with the factory.

Status	Description
Stopped	The status after the batch is stopped.
Finished	The status after the batch programming is finished.
Expired	The batch has expired before the programming is finished.

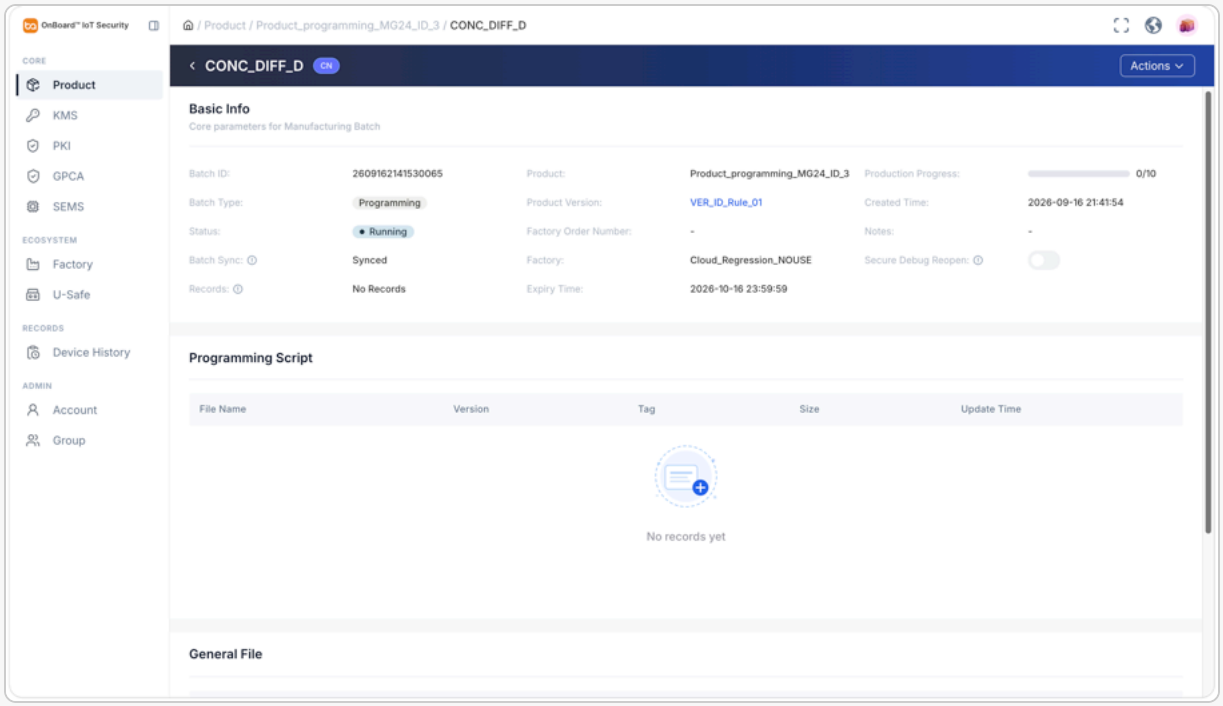
Description of **Batch Sync** (batch synchronization status):

Status	Description
Waiting	The status before the batch is successfully generated.
Syncing	The status when the batch is successfully generated and starts synchronizing with the factory.
Sync Failed	The status after synchronization fails. You can try resynchronizing: On the **Batch** tab of the product, click the Options ⋮ icon for the corresponding batch and then select **Resync**.
Synced	The status after the batch is successfully synchronized with the factory.
Deleted	The status after the batch is deleted.

Description of **Records** (programming data synchronization status):

Status	Description
No Records	The state before the batch starts programming.
Uploading	The status when the batch has started programming but is not yet completed, and the programming data is being uploaded.
Uploaded	The status after the batch programming is finished and all programming data has been fully uploaded.

4. On the batch page, you can check the batch-related information (such as **Batch ID**, **Factory Order Number**, and **Production Progress**).



Version: v3.4.0 (Latest)

How to check programmed devices in OnBoard™ IoT Security

This article will guide you on how to check the programmed device information within the tenant in OnBoard™ IoT Security (OBIS).

Prerequisites

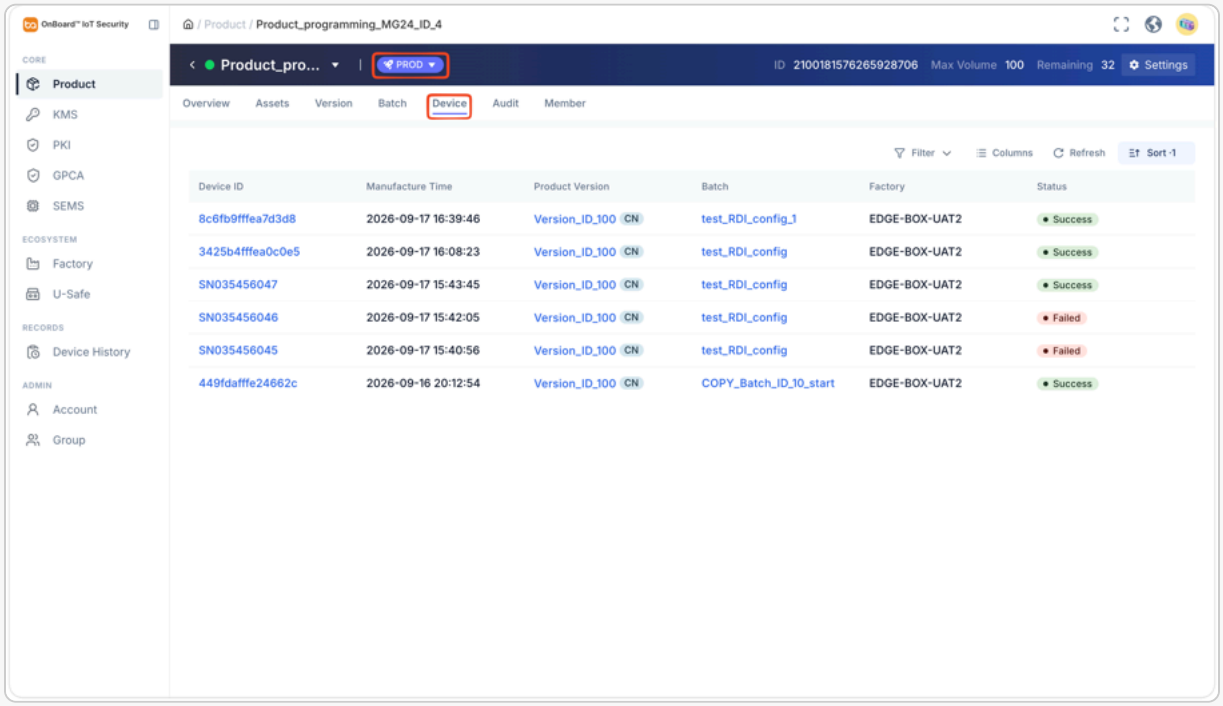
Before getting started, please ensure that:

- The device has already been programmed.
- You have product role permissions for the corresponding product.

Instructions

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. On the product page, select the **TEST** or **PROD** environment, and then select the **Device** tab to check device programming information.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Description of device programming information:

Information	Description
Device ID	Device identifier.
Manufacture Time	The date and time when the device started programming, in the format **YYYY-MM-DD HH:MM:SS**.
Product Version	The version name of the corresponding device.

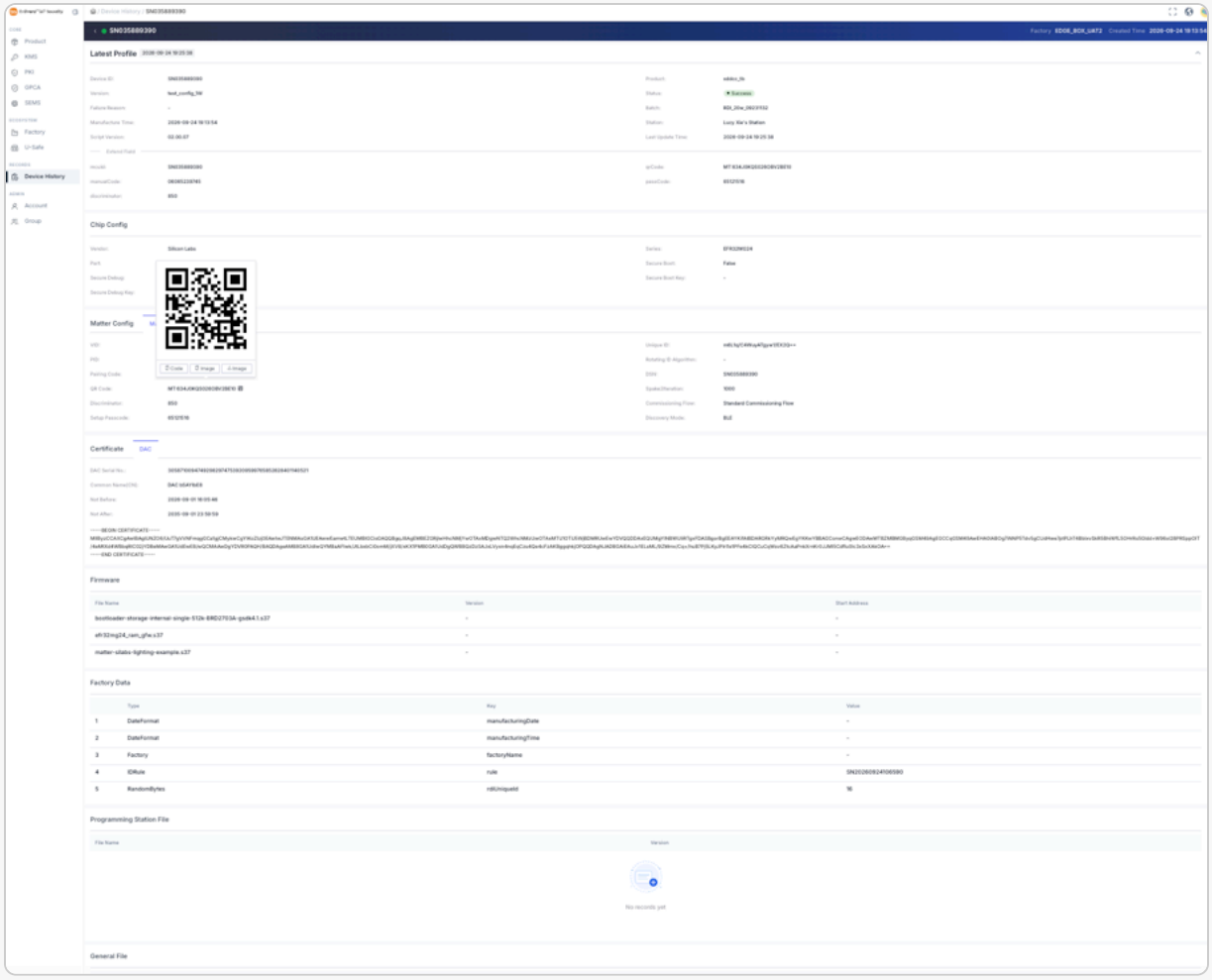
Information	Description
Batch	The batch name of the corresponding device.
Factory	The factory name of the corresponding device.
Station	The station name of the corresponding device.
Status	The status of the device programming result, such as **Success** and **Fail**.

4. Select the corresponding Device ID to navigate to the device page, where you can check the device-related information.

> **TIP**
>
> Hover the mouse over the QR code icon to display the device QR code, which is used for secure and fast commissioning.
>
> - The **Matter Detail** section displays the DAC information (such as **DAC Serial No.**, **Not Before**, and **Not After**). The **DAC Serial No.** can be used to revoke the certification of the corresponding device.
> - The **DAC Certificate** section displays the encoding of the CA certificate. By parsing the encoding of the CA certificate, key certificate attributes such as the issuer information, validity period, and public key can be extracted.

   - System and Extend fields
   - Chip Config
   - Matter Config (Matter Detail and Configuration)

- Certificate (DAC Certificate)
- Firmware
- Factory Data
- Programming Station File
- Attachment File
- General File



Version: v3.4.0 (Latest)

How to check logs in OnBoard™ IoT Security

This article will guide you on how to check the historical operations of the product in OnBoard&trade IoT Security (OBIS).

Prerequisites

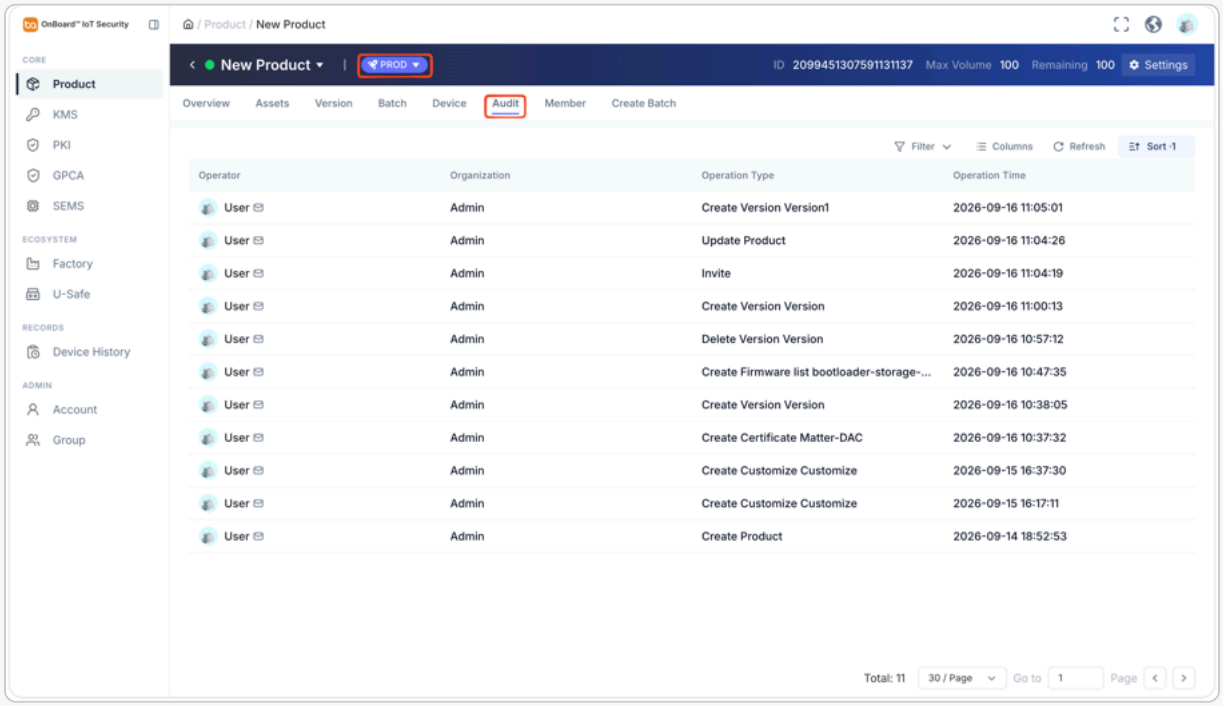
Before getting started, please ensure that you have product role permissions for the corresponding product.

Instructions

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. On the product page, select the **TEST** or **PROD** environment, and then select the **Audit** tab to check the product history (such as **Operator**, **Organization**, **Operation Type**, and **Operation Time**).

TIP

Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Version: v3.4.0 (Latest)

How to manage product members in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS) to manage user access and permissions for a product:

- Add a user
- Update user role
- Remove a user
- Add a user group
- Update user group role
- Remove a user group

Prerequisites

Before getting started, please ensure that:

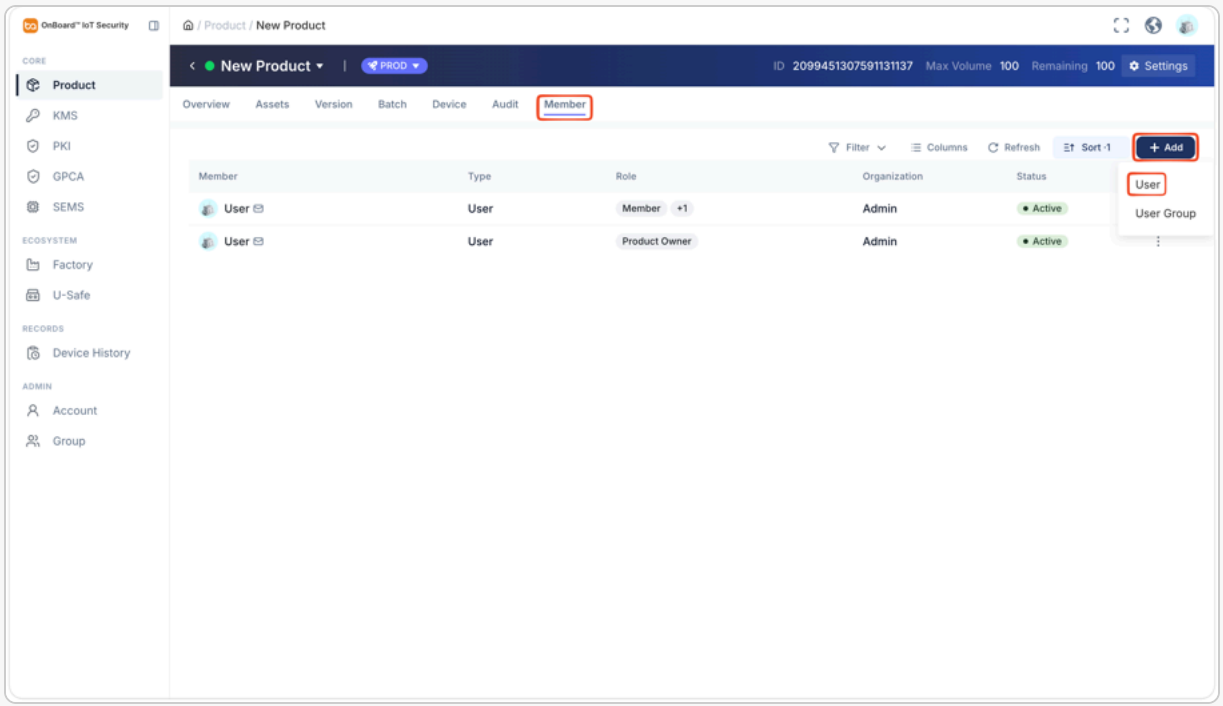
- The users and user groups have already been created.
- You have product role permissions for the corresponding product: Product Owner or Product Manager.

Add a user

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

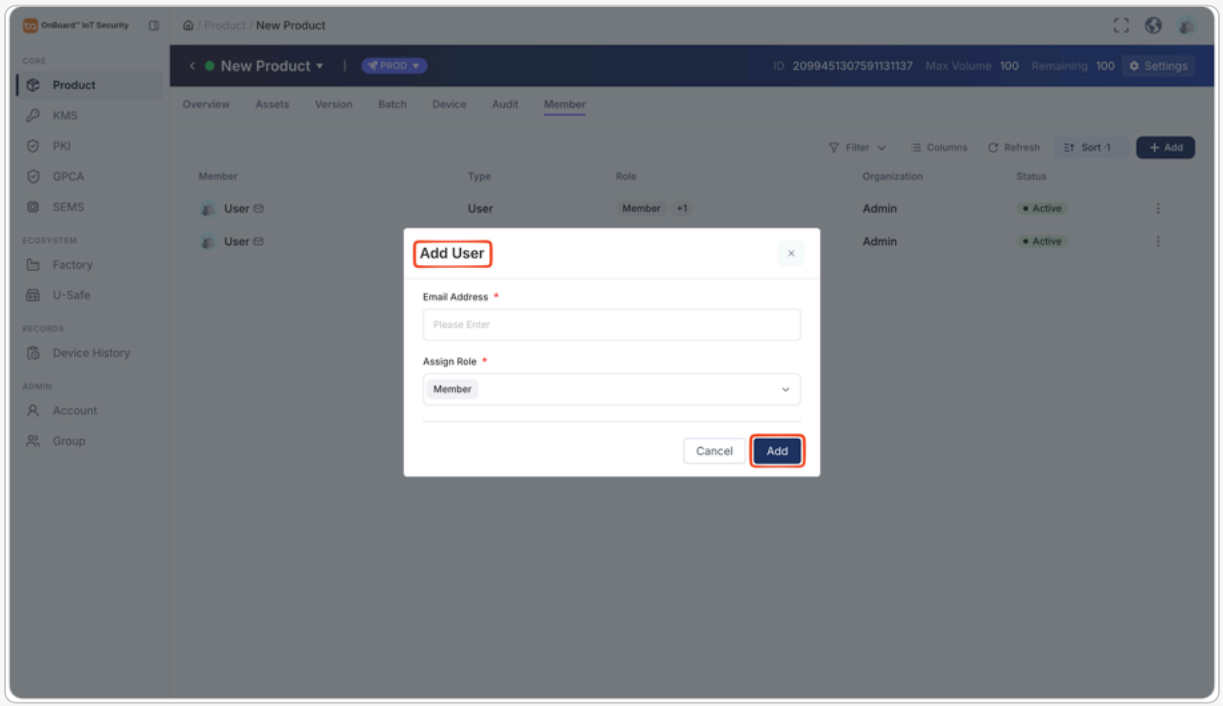
3. On the product page, select the **Member** tab, click **Add** and then select **User**.



4. In the **Add User** window, enter the user's email address and then select the roles.

TIP

- A user can be assigned multiple roles. For more information, refer to the description of product role permissions.
- The added users will receive an email containing a link, through which they can use to access the product details.
- Only users with the **Active** status can be added. Users from other tenants can be added. For example, a Product Manager from Tenant A can add a user from Tenant B to their product team.



5. Click **Add** to complete adding a member.

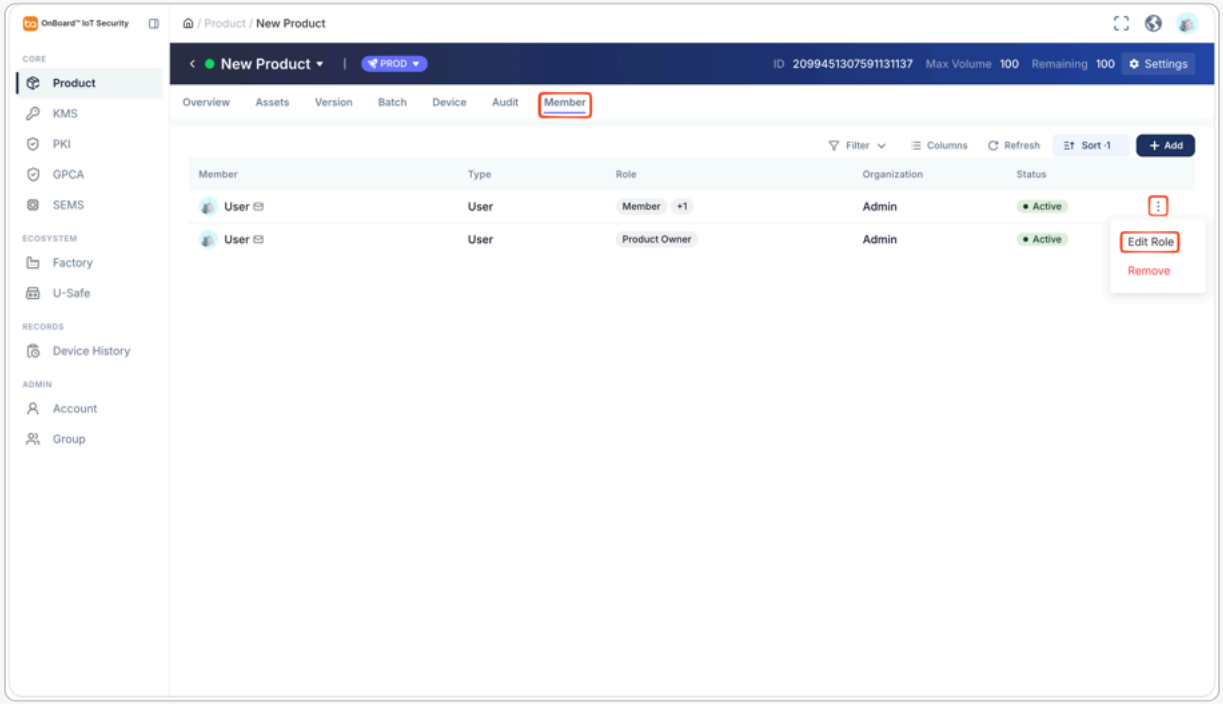
Update user role

> **TIP**
>
> By default, the product creator is set as the Product Owner. To change the Product Owner, click the Options ⋮ icon for the Product Owner and select **Transfer Owner** on the **Member** tab, then choose the new Product Owner and click **Confirm**.

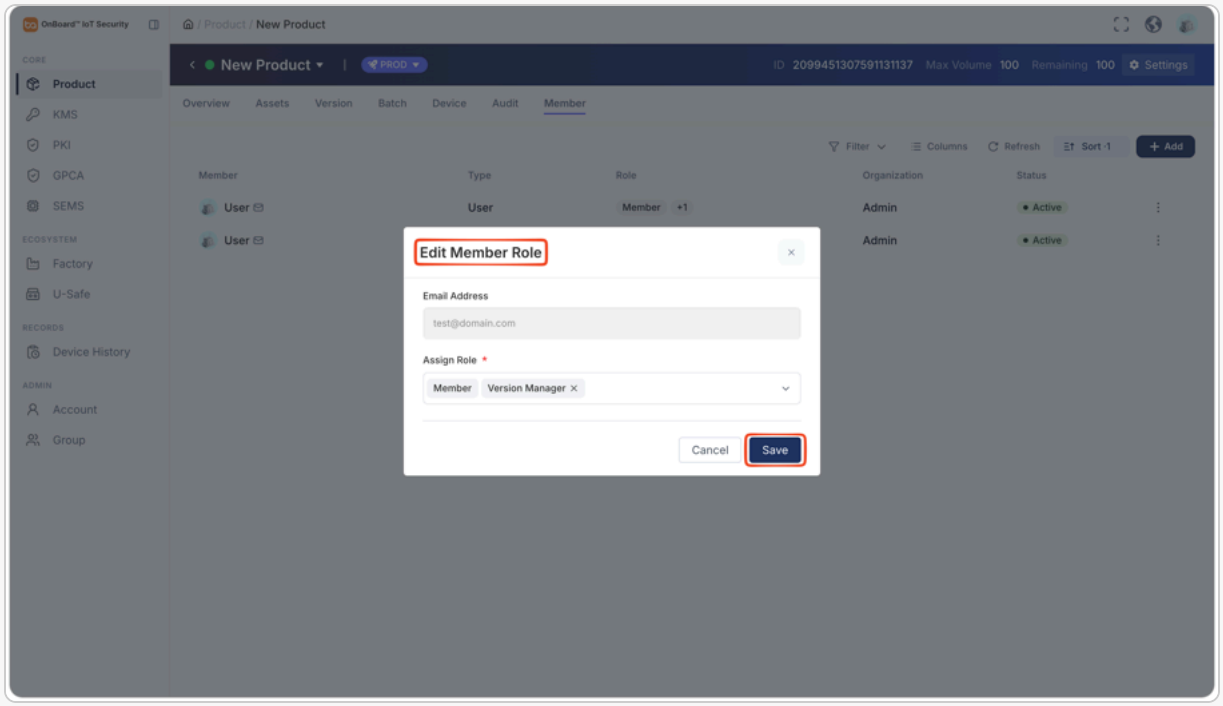
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. On the product page, select the **Member** tab. Click the Options ⋮ icon for the corresponding user and then select **Edit Role**.



4. In the **Edit Member Role** window, select the corresponding roles and then click **Save** to complete the update.

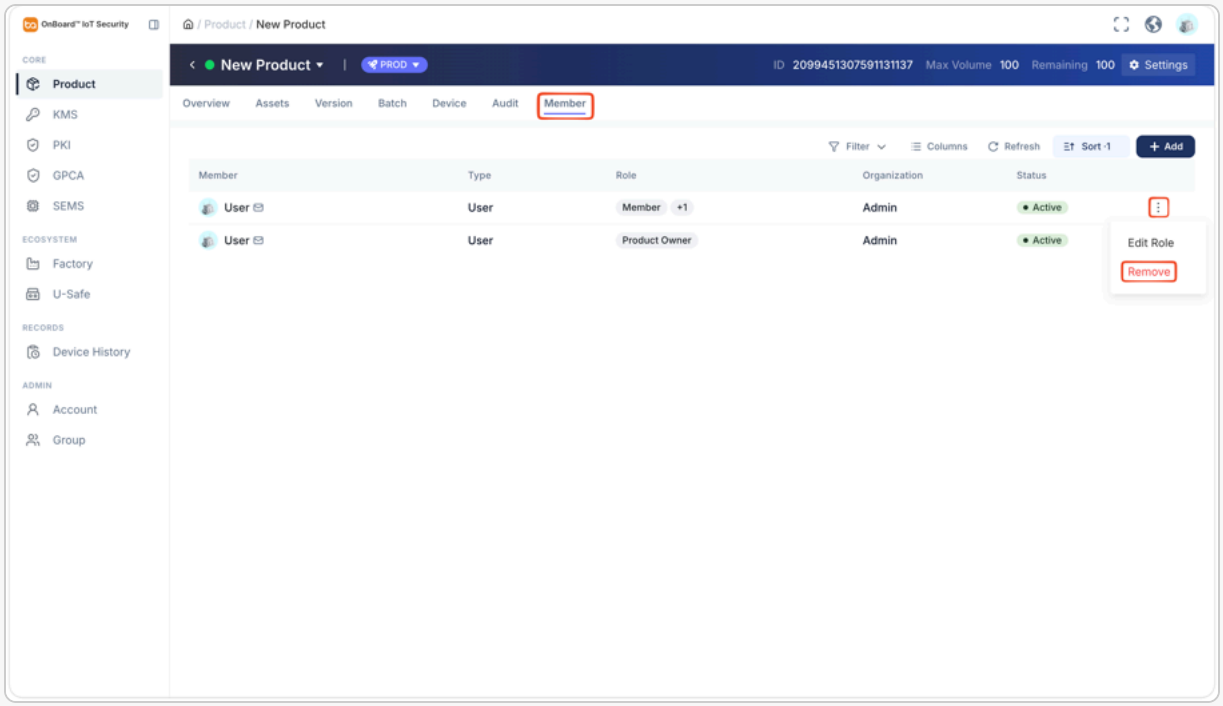


Remove a user

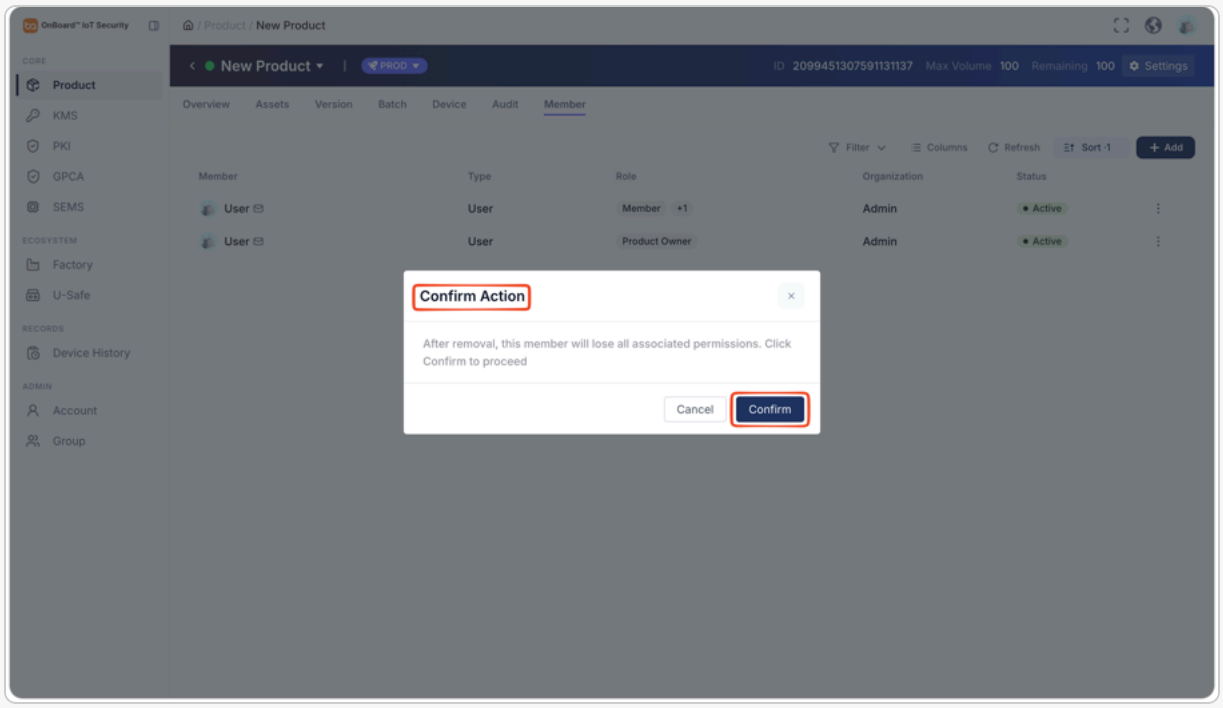
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. On the product page, select the **Member** tab. Click the Options ⋮ icon for the corresponding user and then select **Remove**.



4. In the **Confirm Action** window, verify the information and then click **Confirm** to remove the user.

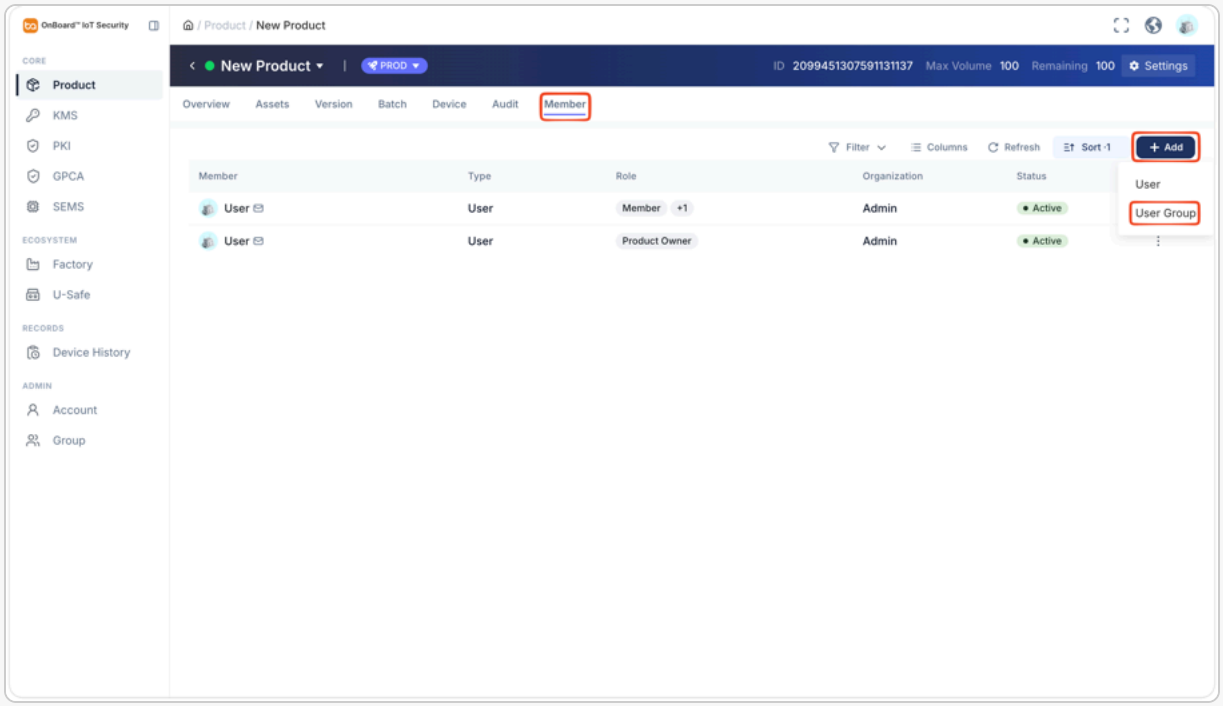


Add a user group

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

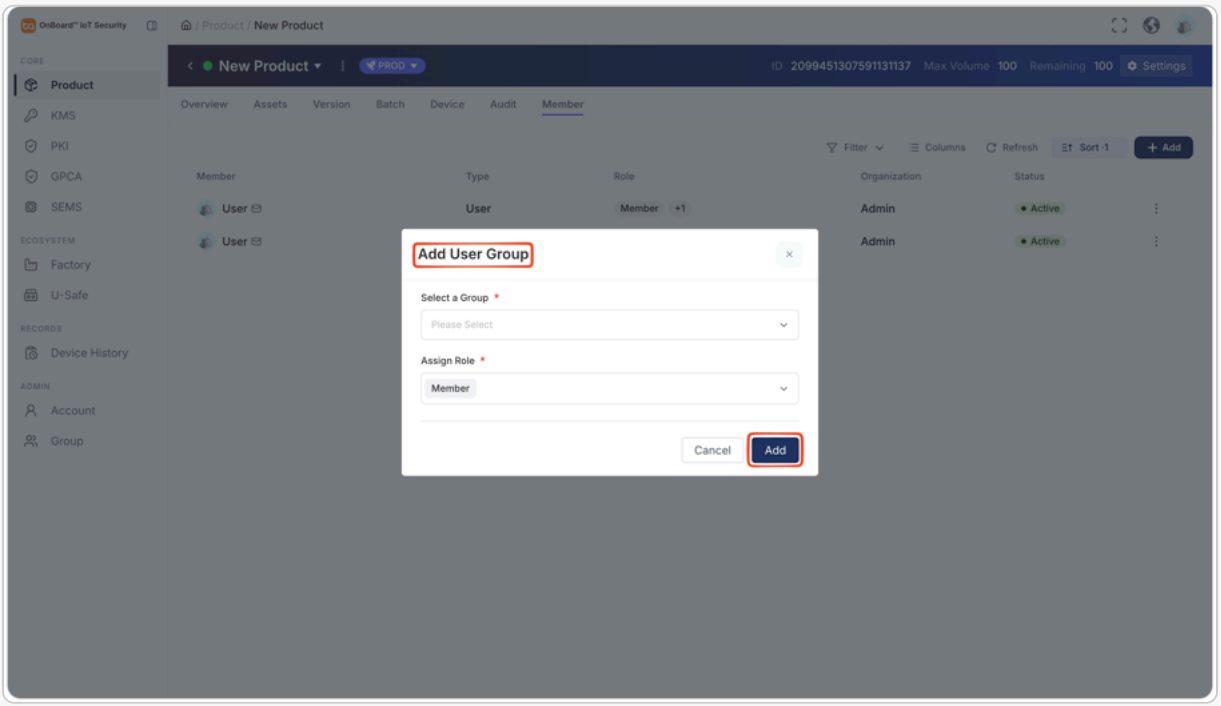
3. On the product page, select the **Member** tab, click **Add** and then select **User Group**.



4. In the **Add User Group** window, select the user group and roles.

TIP

- A user group can be assigned multiple roles. For more information, refer to the description of product role permissions.
- Users within the user group will receive an email containing a link, through which they can use to access the product details.
- Only user groups under the same tenant can be added.



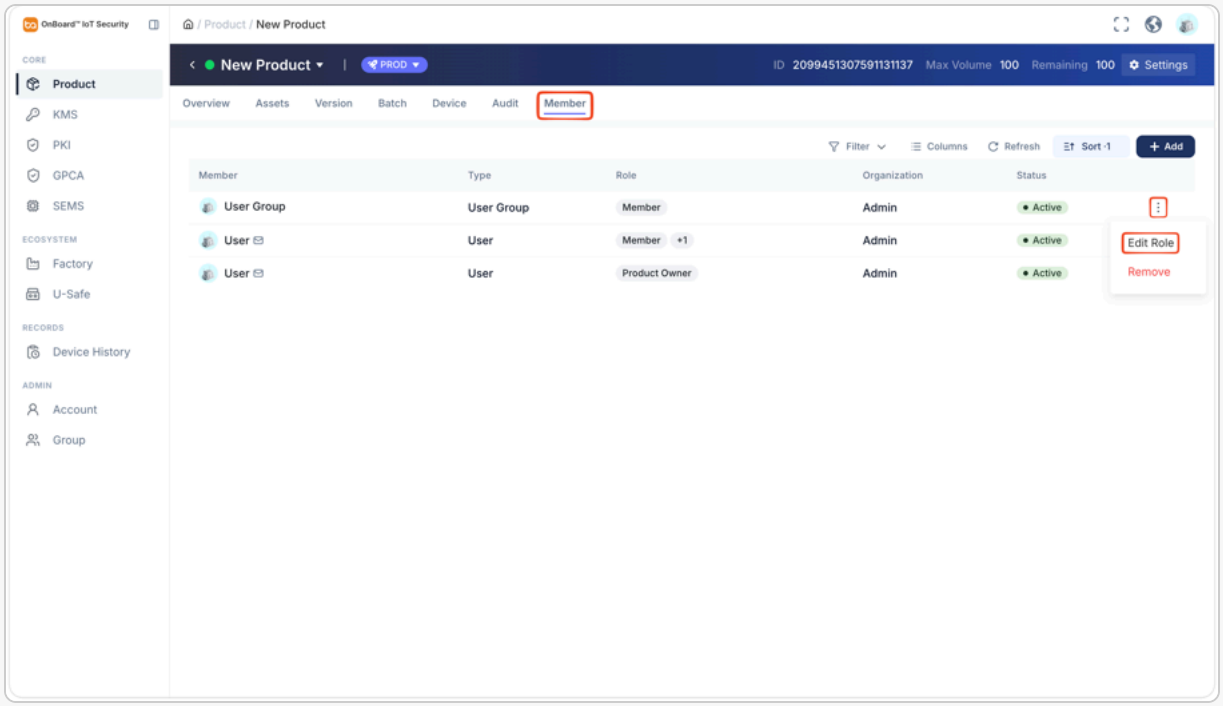
5. Click **Add** to complete adding a user group.

Update a user group role

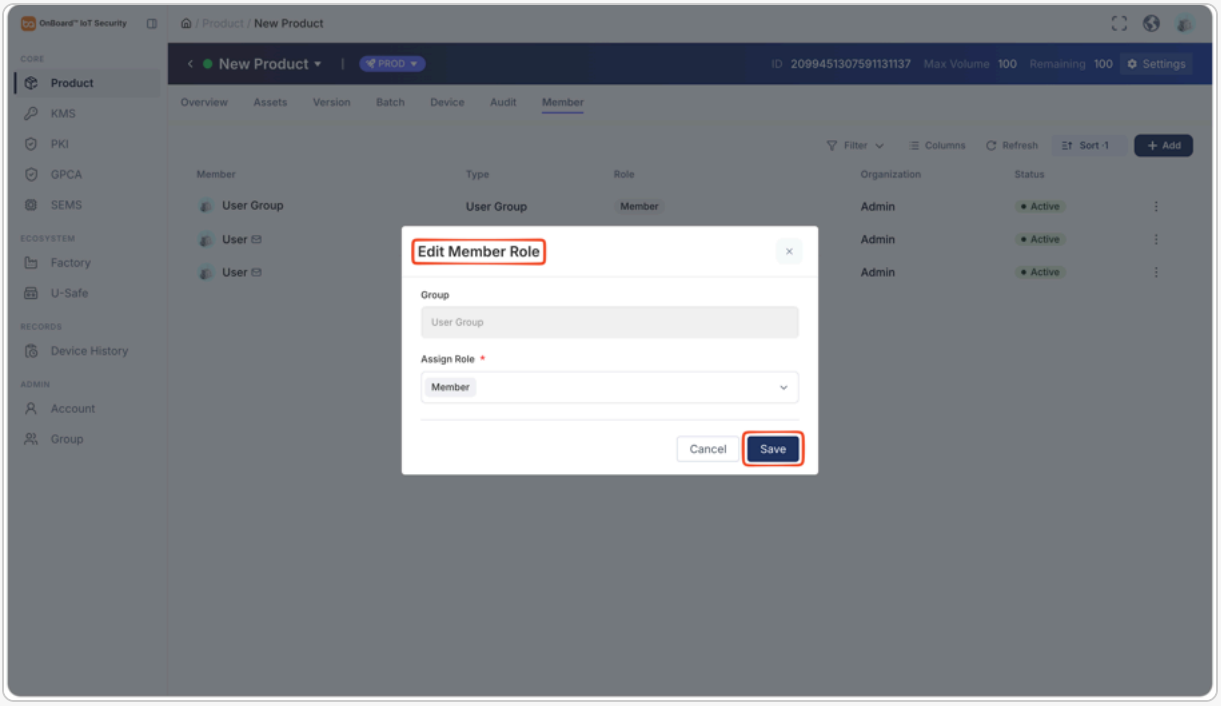
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.

3. On the product page, select the **Member** tab. Click the Options ⋮ icon for the corresponding user group and then select **Edit Role**.

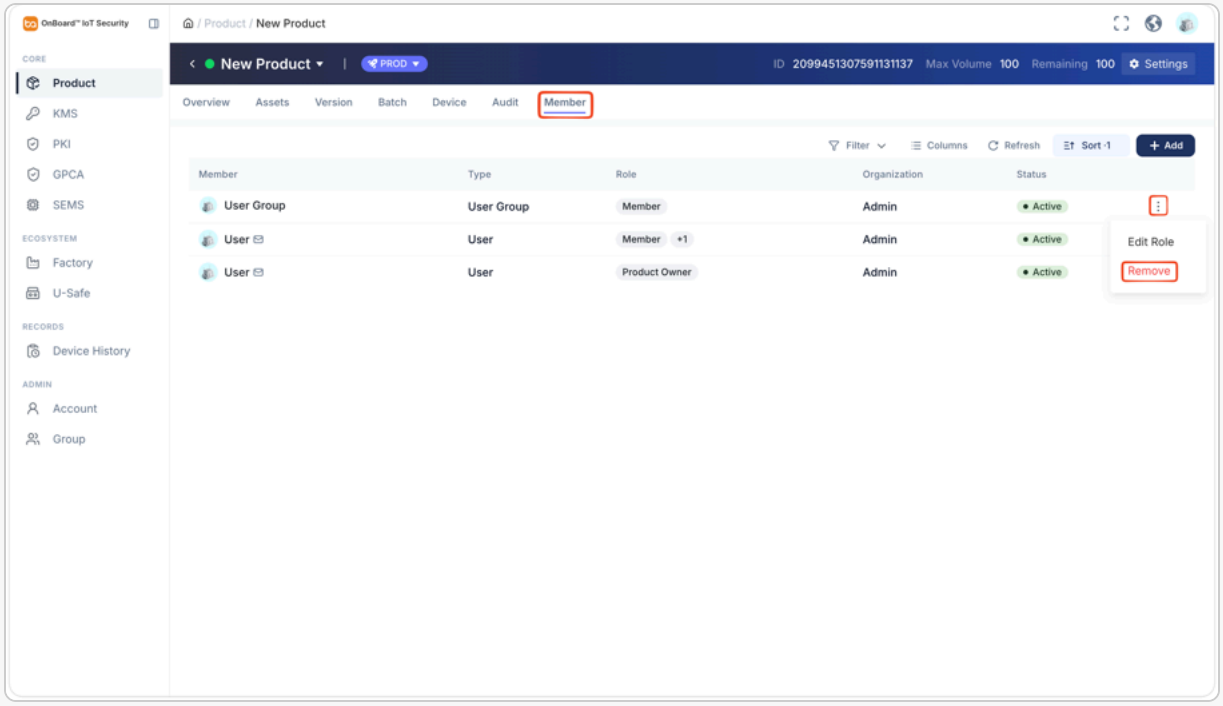


4. In the **Edit Member Role** window, select the corresponding roles and then click **Save** to complete the update.

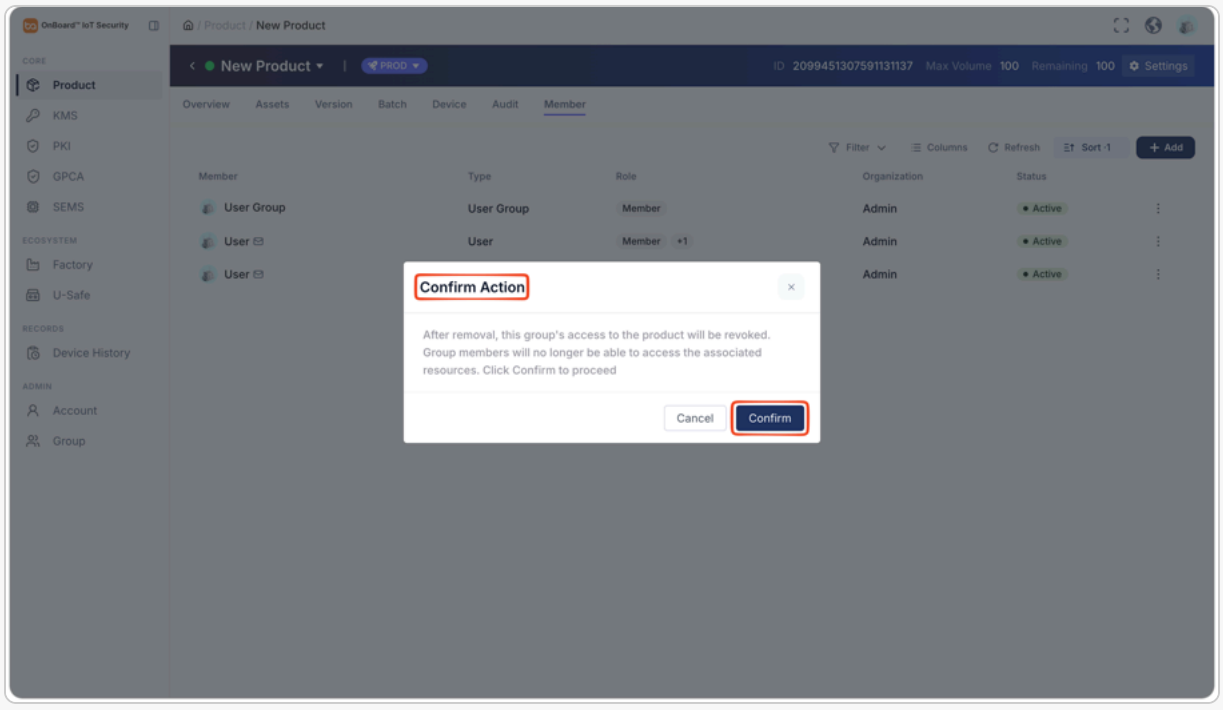


Remove a user group

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **Product**, and then select the corresponding product to navigate to the product page.
3. On the product page, select the **Member** tab. Click the Options ⋮ icon for the corresponding user group and then select **Remove**.



4. In the **Confirm Action** window, verify the information and then click **Confirm** to remove the user group.



Version: v3.4.0 (Latest)

Overview of KMS in OnBoard™ IoT Security

KMS (Key Management Service) in OBIS (OnBoard™ IoT Security) is the core module responsible for key security, which provides secure management and access control of keys. It supports creating, importing, integrating, and managing various types of keys, and leverages HSM (Hardware Security Module) to ensure high-security key generation, storage, and usage.

- Supports both symmetric and asymmetric keys, as well as various key algorithms.
- Supports constraining key usage, environment, validity period, and access permissions.
- Supports creating, importing, and integrating keys by using multiple key sources.
- Supports the use of KMS in multiple scenarios:
  - Resource encryption and decryption
  - Firmware signing and verification
  - Secure boot
  - Secure debug
  - HMAC (Hash-based message authentication code) authentication

The following table summarizes the core capabilities of KMS:

Capability	Description
Key Lifecycle Management	• Symmetric and asymmetric key lifecycle management
Key State & Storage	• Key state management (Active, Suspended, Revoked) • Hardware-backed secure storage and cryptographic execution
Enterprise BYOK (Key Import)	• OEM generates and imports keys into HSM • KMS governs usage via authorization policies
Cloud-Native BYOK (External KMS)	• Keys remain in customer's cloud KMS (e.g., AWS KMS) • KMS invokes operations through secure authenticated APIs

KMS does not mandate where keys must live. It mandates how cryptographic capabilities are governed, constrained, and audited.

Version: v3.4.0 (Latest)

How to create a key in OnBoard™ IoT Security

This article will guide you on how to create a symmetric and asymmetric key in OnBoard™ IoT Security (OBIS).

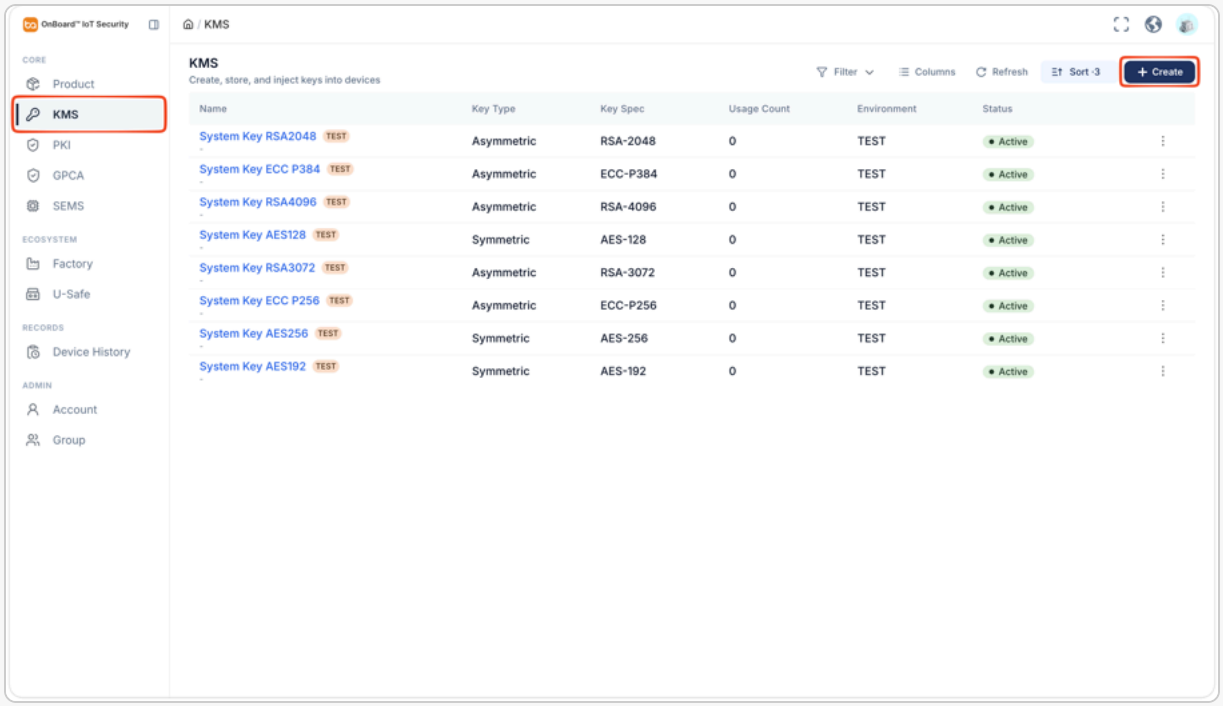
Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager or Resource Manager.

Instructions

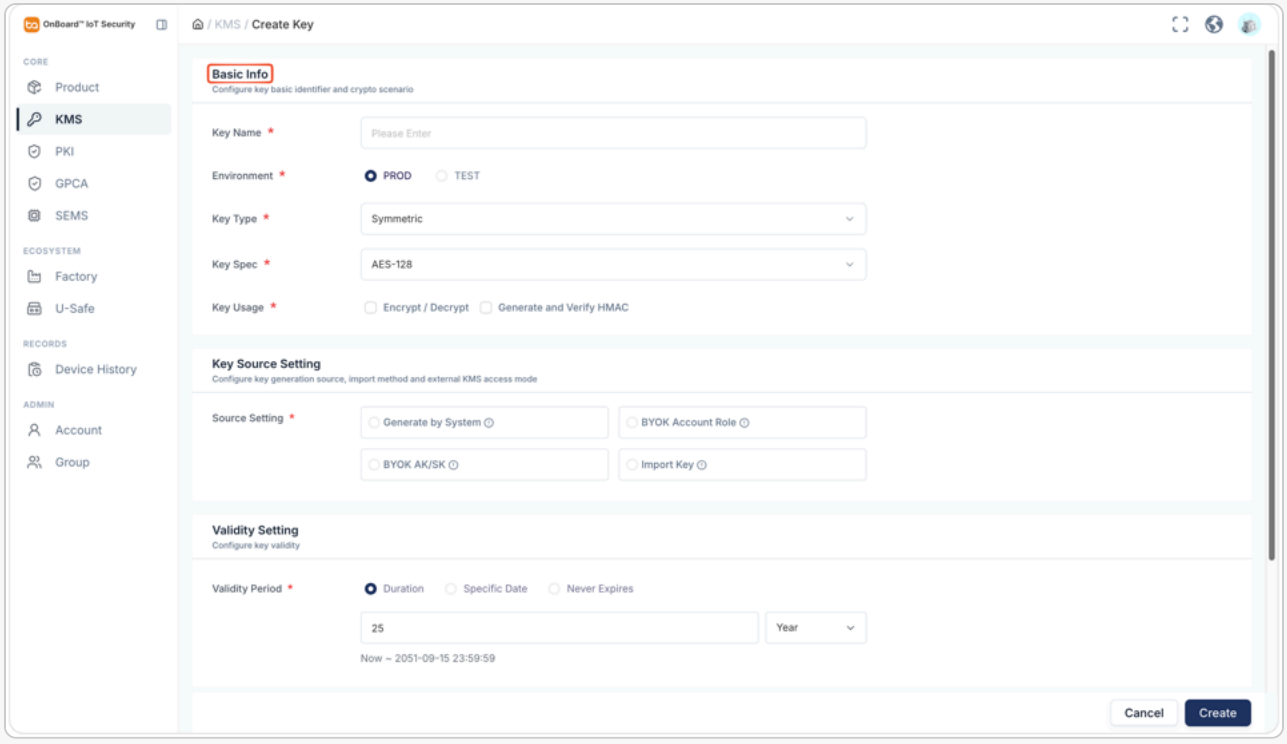
> **TIP**
>
> After a key is created, it can be selected when configuring Keys for a product.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then click **Create** on the **KMS** page.



Step one: Configure the basic information

In the **Basic Info** section, select and enter the key basic information.



Description of key basic information:

Information	Mandatory	Description
Key Name	Yes	The key name must be unique in the same environment.
Environment	Yes	Two environments can be selected: **PROD** and **TEST**.
Key Type	Yes	Two key types can be selected: **Symmetric** and **Asymmetric**.

Information	Mandatory	Description
Key Spec	Yes	Select encryption algorithms for symmetric and asymmetric keys: • Symmetric key: **AES-128**, **AES-192**, or **AES-256** • Asymmetric key: **RSA-2048**, **RSA-3072**, **RSA-4096**, **ECC-P256**, **ECC-P384**, **ECC-P521**, or **ECC-P256K**
Key Usage	Yes	Limit the operations the key is allowed to perform (multiple selections allowed): • **Sign/Verify**: Allows the use of an asymmetric key to generate or verify digital signatures. • **Encrypt/Decrypt**: Allow the use of a symmetric or asymmetric key to encrypt or decrypt data. • **Generate and Verify HMAC**: Allows the use of a symmetric key to generate and verify message authentication codes to ensure data integrity. • **Key Agreement**: Used in key exchange protocols (such as ECDH) for the secure exchange of encryption keys. **Note**: For asymmetric keys, once **Key Agreement** is selected, the Import Public Key option in the **Key Source** area will be unavailable.

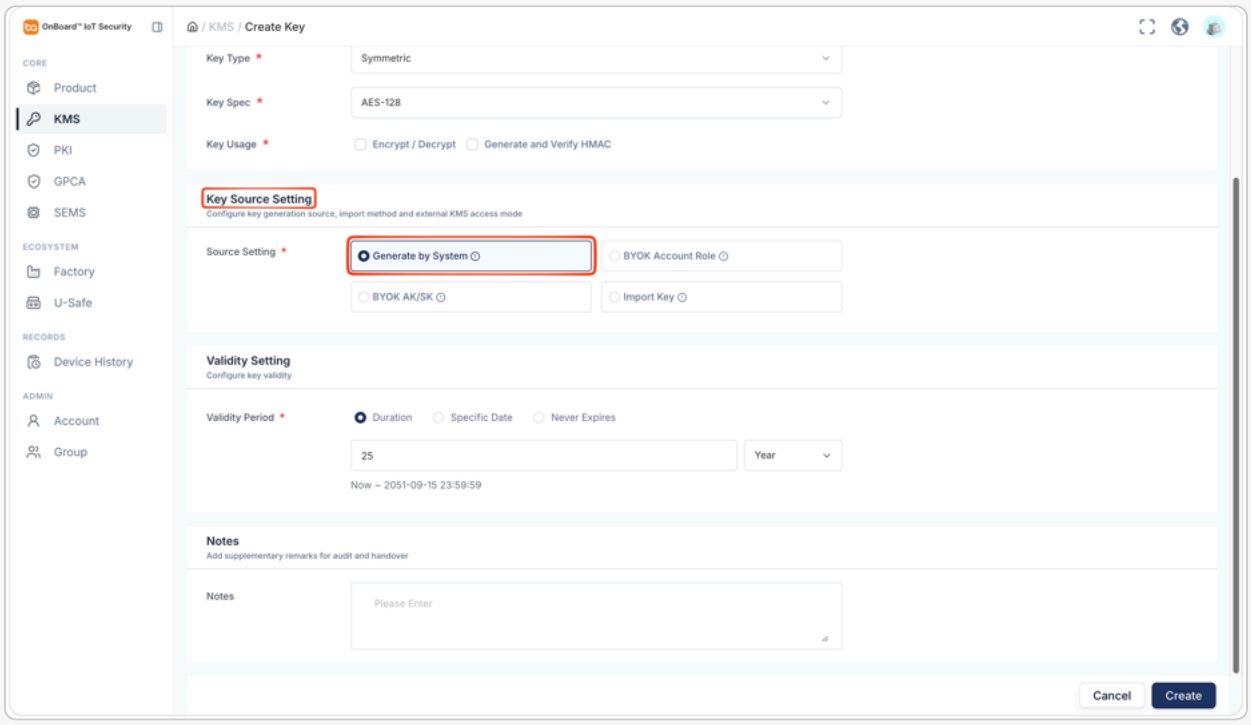
Step two: Configure the key source

Symmetric key

Generated by System | BYOK Account Role | BYOK AK/SK | Import Key

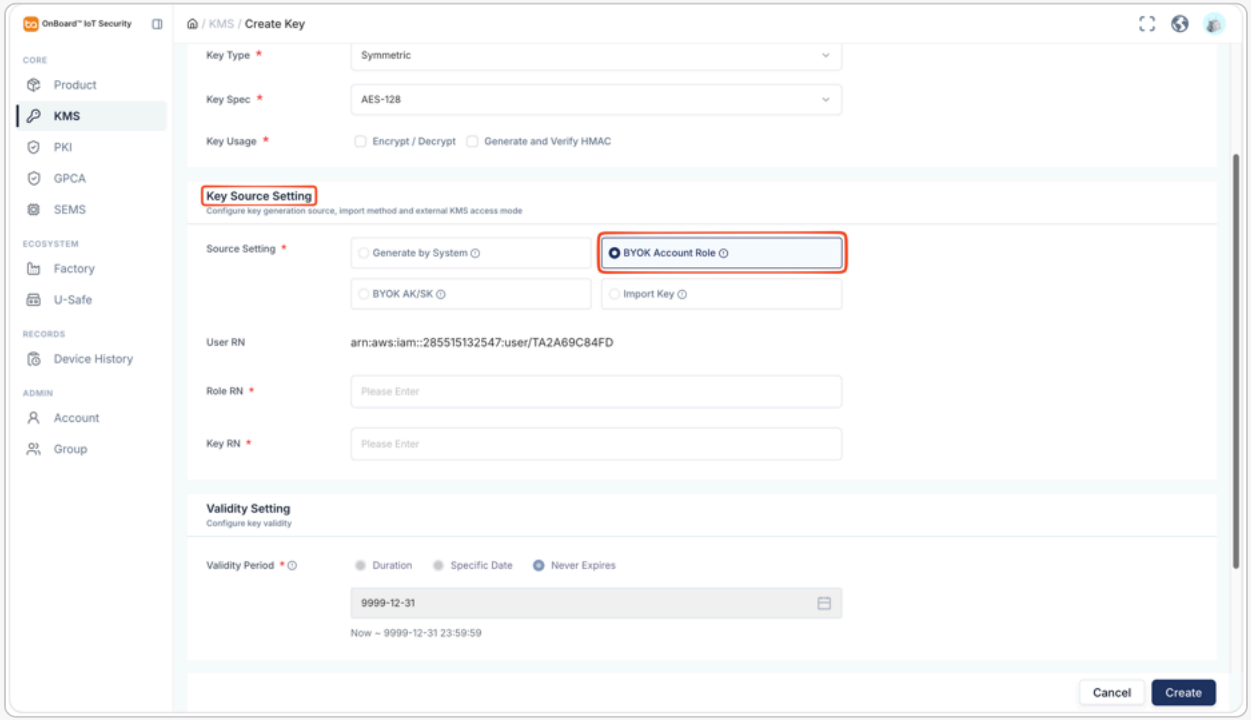
> **TIP**
>
> The system securely generates a random key pair inside a Hardware Security Module (HSM).

In the **Key Source Setting** section, select **Generated by System**.



> **TIP**
>
> Connect to AWS KMS using IAM Role-based access—secure and ideal for cloud-native deployments.

In the **Key Source Setting** section, select **BYOK Account Role**, and then enter the key-related information.



Description of Account Role information:

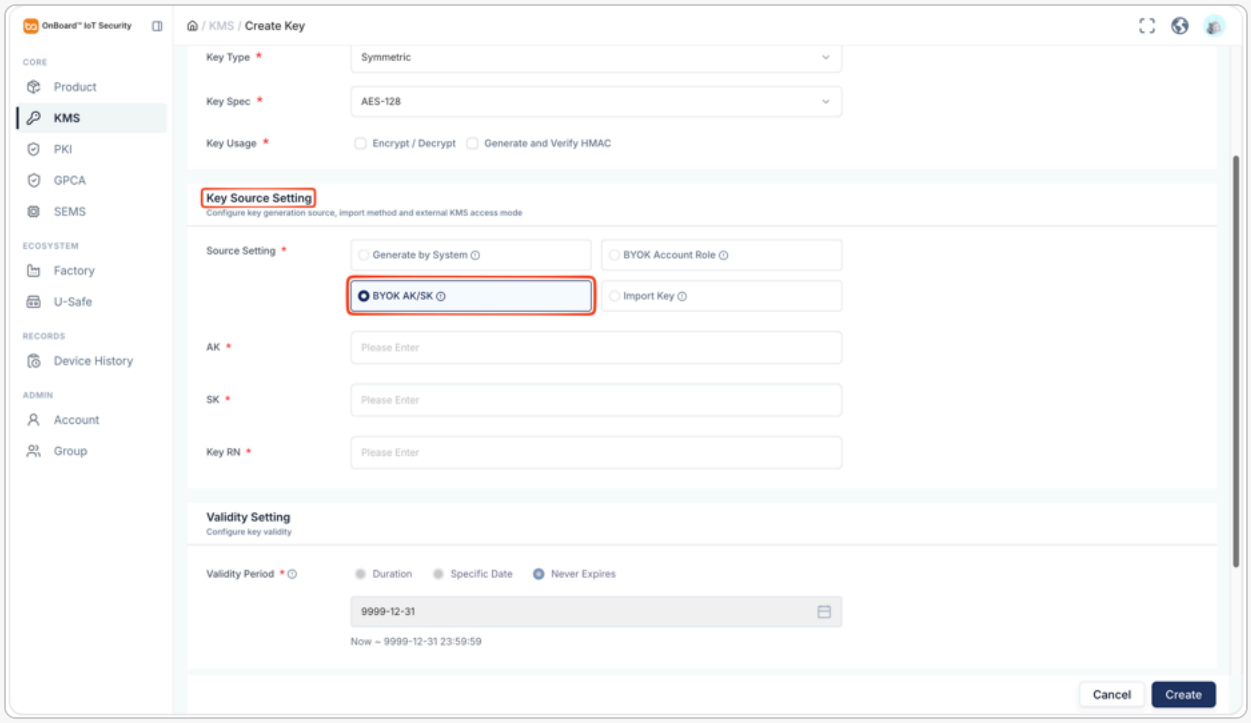
Information	Mandatory	Description
User RN	No	Uniquely identifies a user in AWS IAM (such as an administrator or developer), used for permission assignment and resource access control.

Information	Mandatory	Description
Role RN	Yes	Uniquely identifies a role in AWS IAM, used for temporary permission assignment (such as cross-account access for EC2 instances or Lambda functions).
Key RN	Yes	Uniquely identifies an encryption key in AWS KMS, used for data encryption and decryption.

TIP

Access external keys from third-party KMS using Access Key and Secret Key credentials.

In the **Key Source Setting** section, select **BYOK AK/SK**, and then enter the key-related information.



Description of AK/SK information:

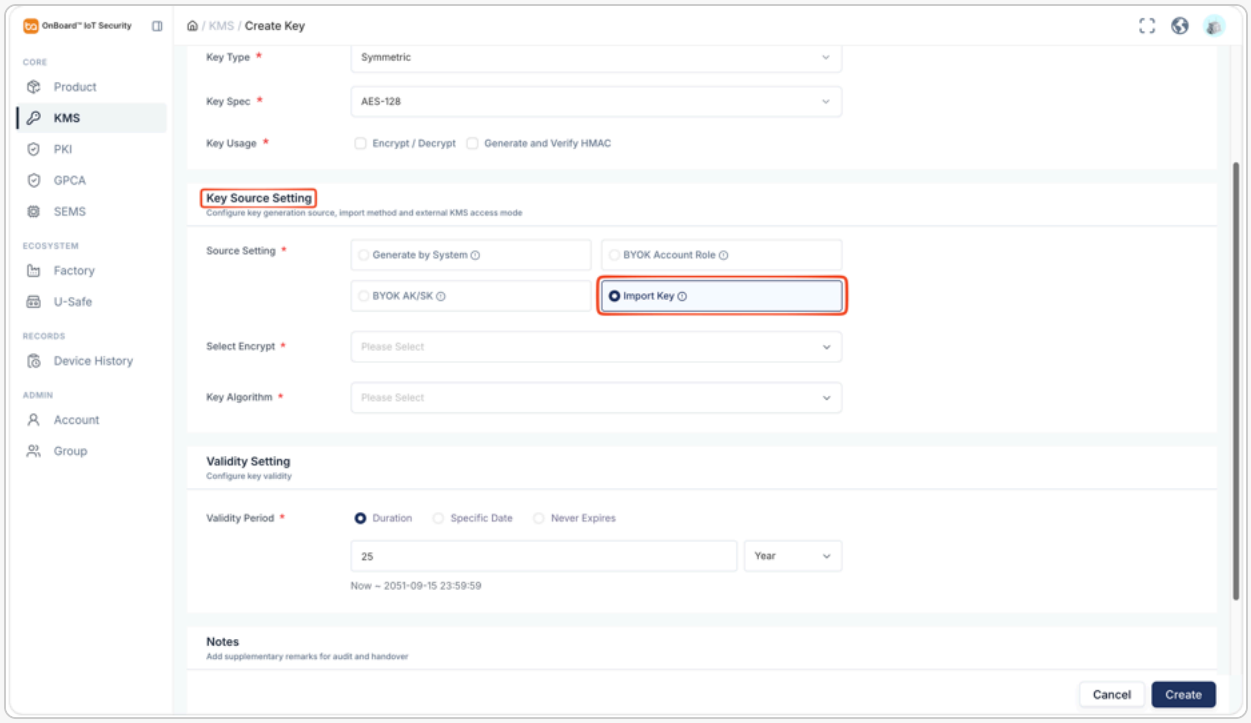
Information	Mandatory	Description
AK	Yes	AK (Access Key ID): • Identity identifier: Uniquely identifies a user in AWS IAM (Identity and Access Management), similar to a username. • Public attribute: Can be safely shared (for example, configured in code or the CLI), but must be used together with the SK to complete authentication.

Information	Mandatory	Description
SK	Yes	SK (Secret Access Key): • Confidential credential: Used to generate request signatures and verify identity, similar to a password. • Strict confidentiality: Disclosure may result in full account compromise and should be protected with the same care as a password.
Key RN	Yes	ARN (Amazon Resource Name): uniquely identifies an encryption key in AWS KMS, used for data encryption and decryption.

TIP

Manually upload an existing symmetric key generated outside the system.

In the **Key Source Setting** section, select **Import Key**. Select the encryption method and key algorithm. Description of Import Key information:



Description of Import Key information:

Information	Mandatory	Description
Select Encrypt	Yes	Select the encryption algorithm. Currently, only **RSA_2048** is supported, which provides a baseline level of security and is suitable for scenarios such as key encryption and digital signatures.
Key Algorithm	Yes	Select the key algorithm: • **RSA_AES_KEY_WRAP_SHA_1** • **RSA_AES_KEY_WRAP_SHA_256**

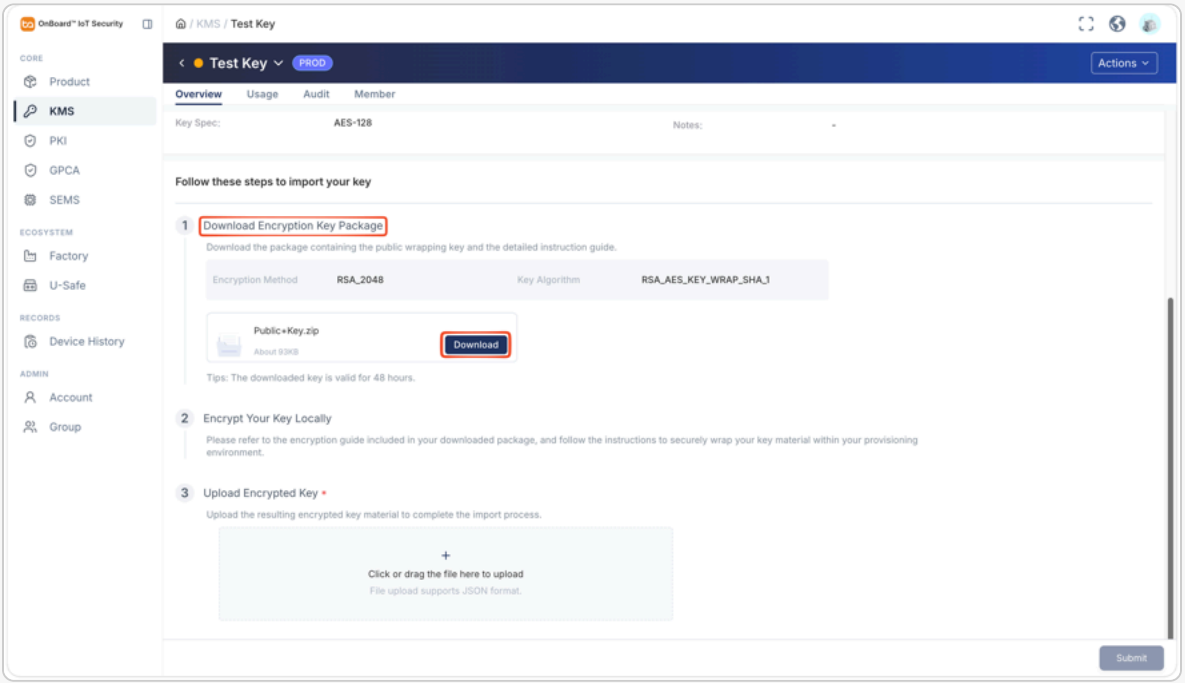
> **TIP**
>
> When the key source is **Import Key**, you need to complete the key encryption configuration after creating the key. Before the key encryption configuration is completed, the key will remain in the **Pending** status and can't be used.

Key encryption configuration

> **TIP**
>
> When the key source is **Import Key**, refer to the following steps to complete the key encryption.

1. On the **KMS** page, select the corresponding key.

2. Locate the **Download Encryption Key Package** section on the key page, and then click **Download** to download the encryption key file.



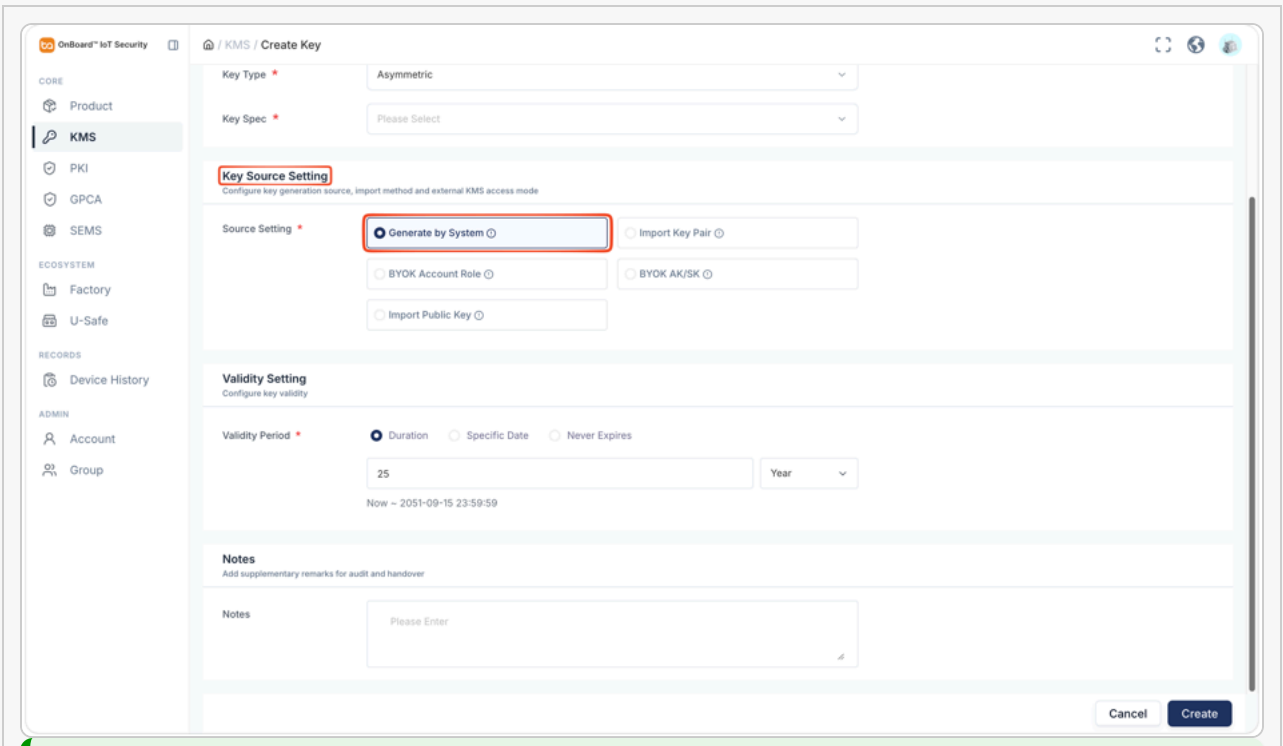
3. Import the downloaded encryption key into your HSM and use it to encrypt the symmetric key.
4. After the symmetric key is encrypted, select and upload the encrypted key file in **.json** format in the **Upload Encrypted Key** section.
5. Click **Submit** to complete the key encryption configuration, and the key status will change to **Active**.

Asymmetric key

Generated by System | **Import Key Pair** | **BYOK Account Role** | **BYOK AK/SK** | **Import Public Key**

> **TIP**
>
> The system securely generates a random key pair inside a Hardware Security Module (HSM).

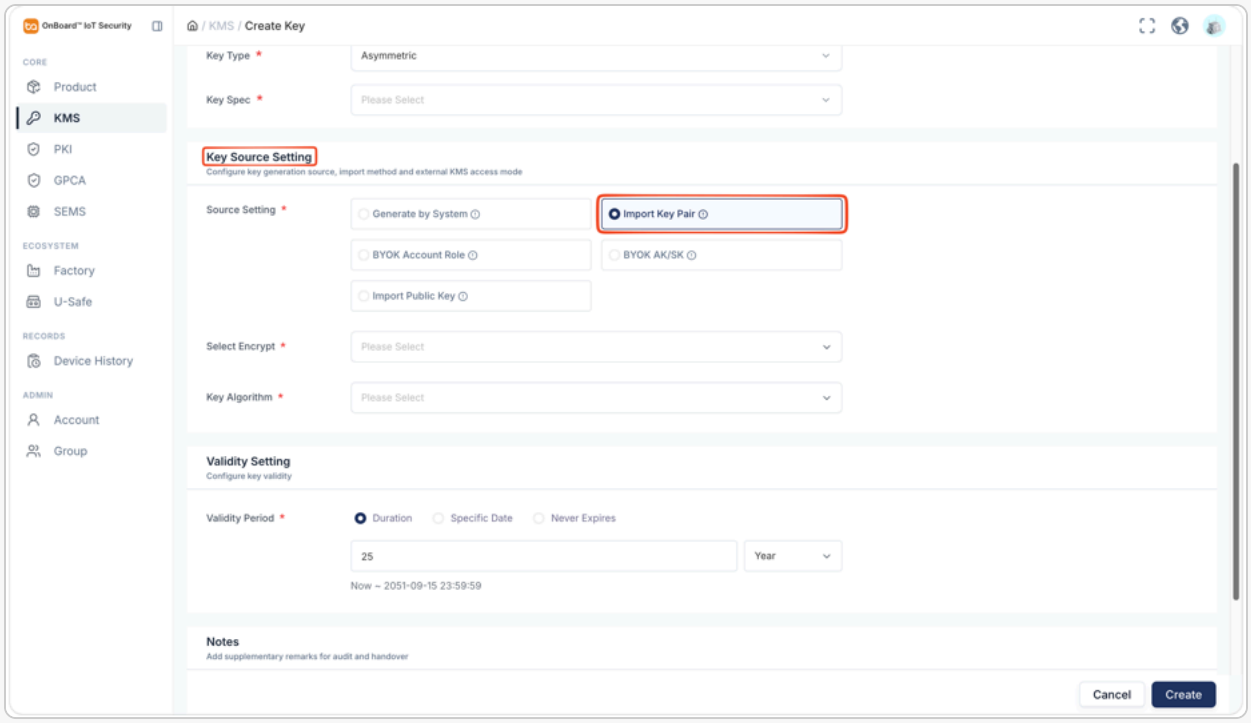
In the **Key Source Setting** section, select **Generated by System**.



TIP

Manually upload an existing asymmetric key pair generated outside the system.

In the **Key Source Setting** section, select **Import Key Pair**. Then, select the encryption method and key algorithm.



Description of Import Key Pair information:

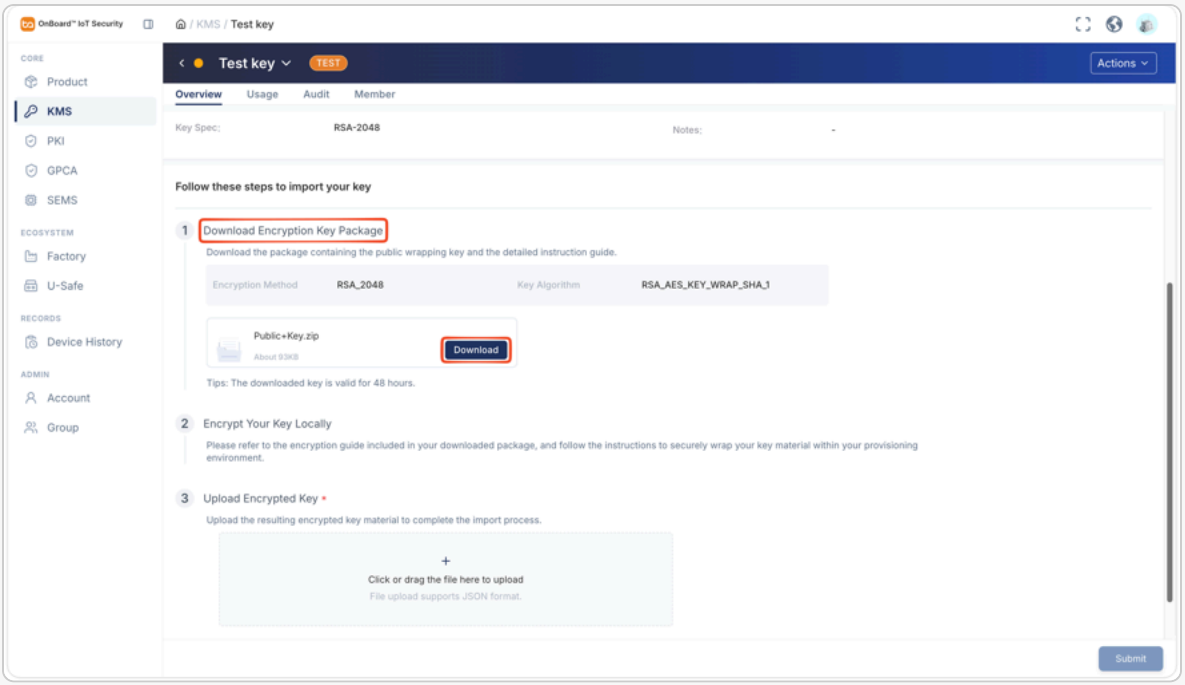
Information	Mandatory	Description
Select Encrypt	Yes	Select the encryption algorithm. Currently, only **RSA_2048** is supported, which provides basic security strength and is suitable for scenarios such as key encryption and digital signatures.
Key Algorithm	Yes	Select the key algorithm: • **RSA_AES_KEY_WRAP_SHA_1** • **RSA_AES_KEY_WRAP_SHA_256**

> **TIP**
>
> When the key source is **Import Key Pair**, you need to complete the key encryption configuration after creating the key. Before the key encryption configuration is completed, the key will remain in the **Pending** status and can't be used.

Key encryption configuration

> **TIP**
>
> When the key source is **Import Key Pair**, refer to the following steps to complete the key encryption.

1. On the **KMS** page, select the corresponding key.
2. Locate the **Download Encryption Key Package** section on the key page, and then click **Download** to download the encryption key file.



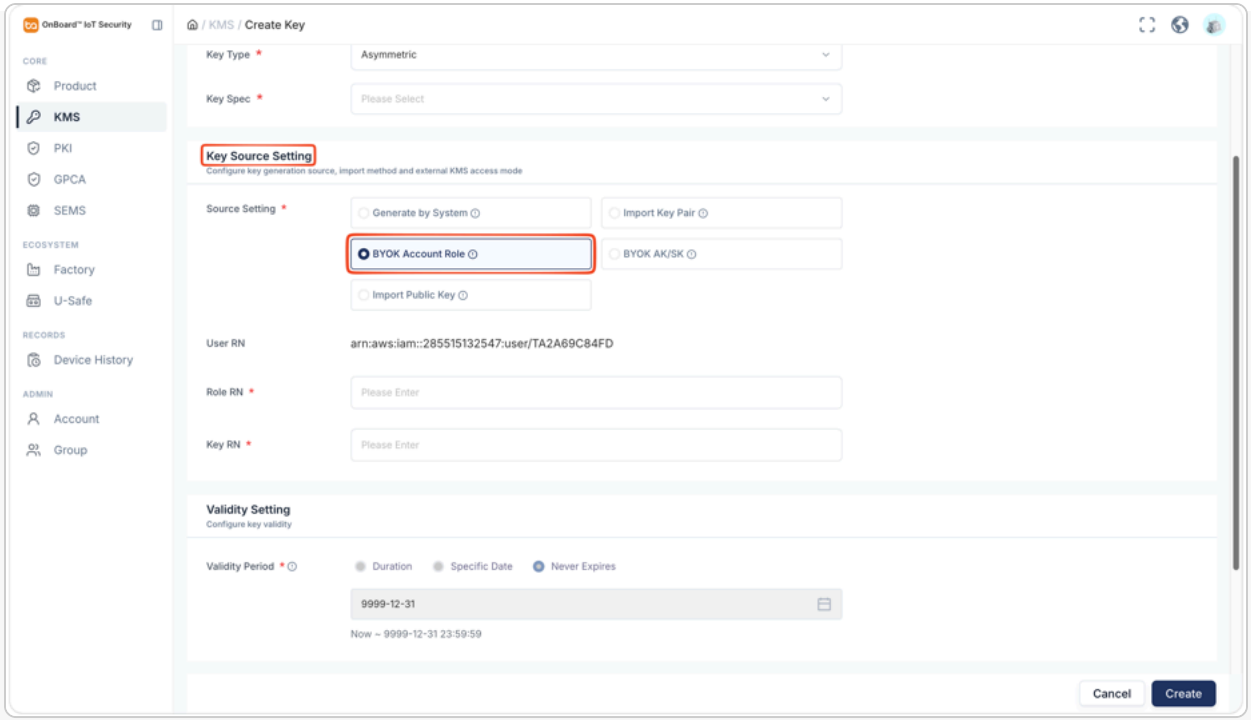
3. Import the downloaded encryption key into your HSM and use it to encrypt the symmetric key.

4. After the symmetric key is encrypted, select and upload the encrypted key file in **.json** format in the **Upload Encrypted Key** section.

5. Click **Submit** to complete the key encryption configuration, and the key status will change to **Active**.

> **TIP**
>
> Connect to AWS KMS using IAM Role-based access—secure and ideal for cloud-native deployments.

In the **Key Source Setting** section, select **BYOK Account Role**, and then enter the key-related information.

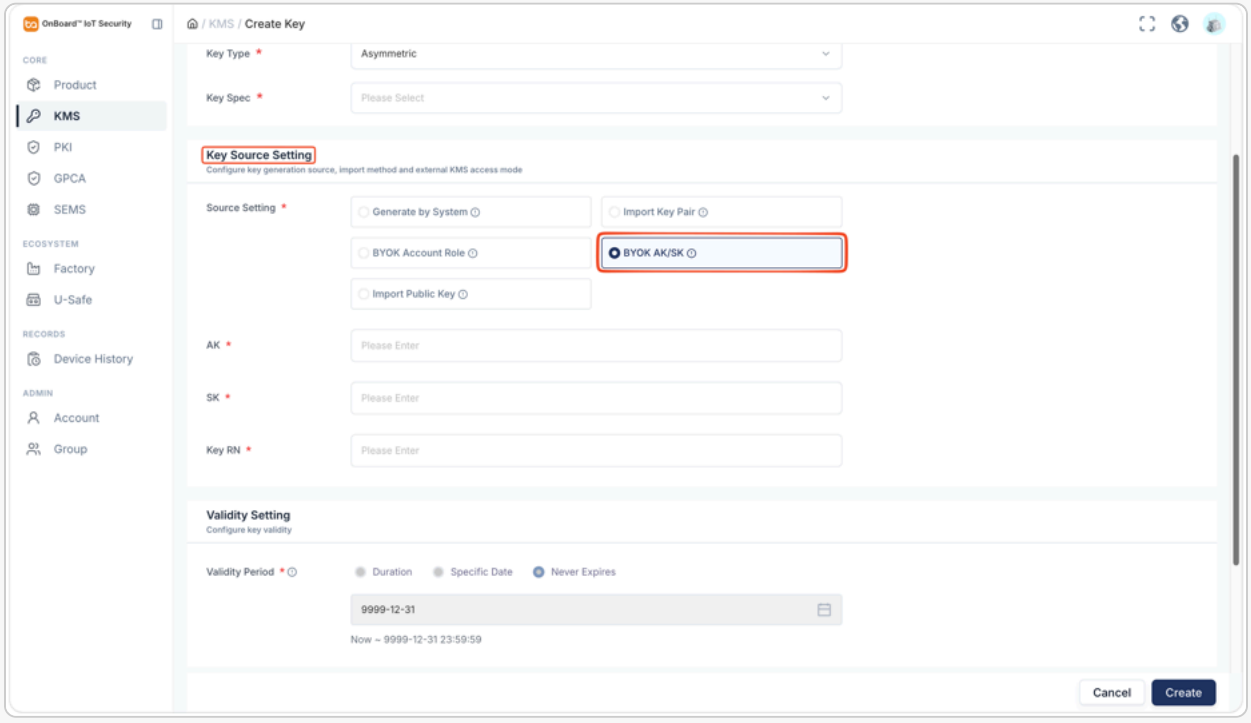


Description of Account Role information:

Information	Mandatory	Description
User RN	No	Uniquely identifies a user in AWS IAM (such as an administrator or developer), used for permission assignment and resource access control.
Role RN	Yes	Uniquely identifies a role in AWS IAM, used for temporary permission assignment (such as cross-account access for EC2 instances or Lambda functions).
Key RN	Yes	Uniquely identifies an encryption key in AWS KMS, used for data encryption and decryption.

> **TIP**
>
> Access external keys from third-party KMS using Access Key and Secret Key credentials.

In the **Key Source Setting** section, select **BYOK AK/SK**, and then enter the key-related information.



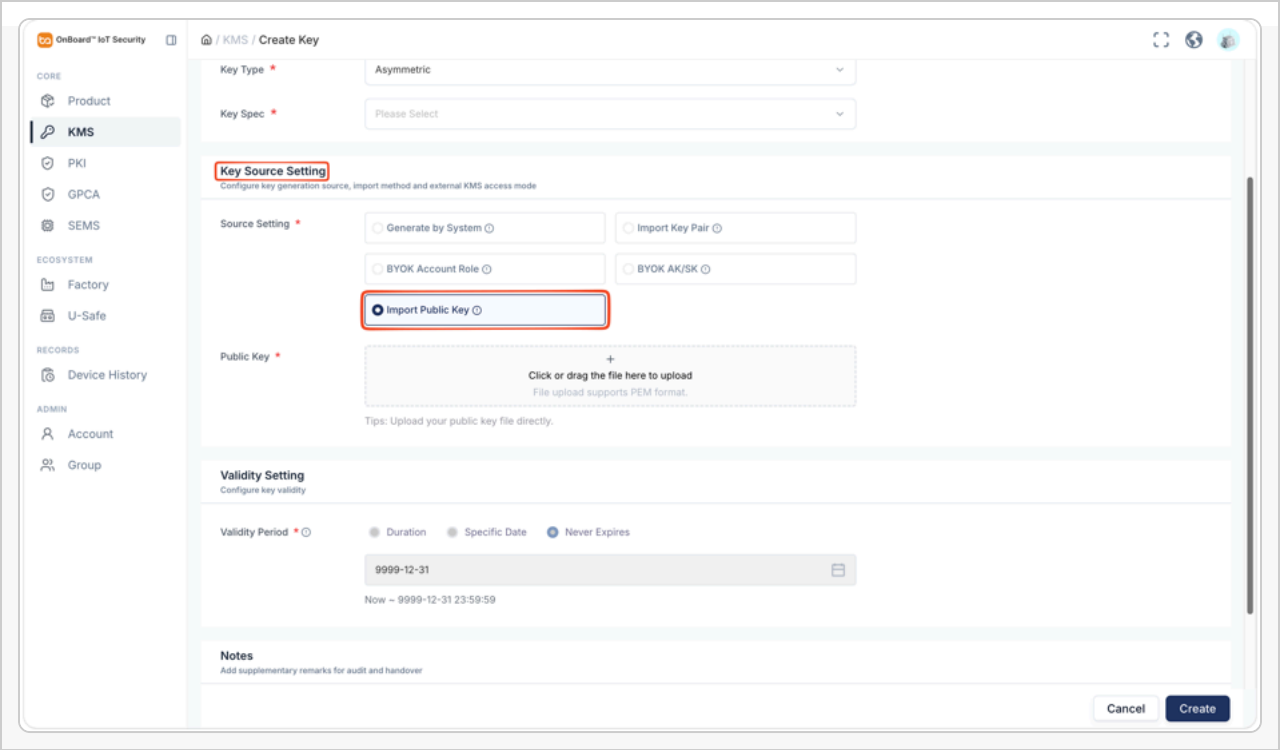
Description of AK/SK information:

Information	Mandatory	Description
AK	Yes	AK (Access Key ID): • Identity identifier: Uniquely identifies a user in AWS IAM (Identity and Access Management), similar to a username. • Public attribute: Can be safely shared (for example, configured in code or the CLI), but must be used together with the SK to complete authentication.
SK	Yes	SK (Secret Access Key): • Confidential credential: Used to generate request signatures and verify identity, similar to a password. • Strict confidentiality: Disclosure may result in full account compromise and should be protected with the same care as a password.
Key RN	Yes	ARN (Amazon Resource Name): uniquely identifies an encryption key in AWS KMS, used for data encryption and decryption.

TIP

Import only a public key for verifying signatures or device identities—no private key required.

In the **Key Source Setting** section, select **Import Public Key**. In the **Public Key** section, upload a public key file in **.pem** format.



Step three: Configure the validity

In the **Validity Setting** section, you can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.

Step four: Add the notes

In the **Notes** section, you can provide additional information related to the key, such as special requirements and important notes.

Step five: Complete the creation

After verifying that the configuration is correct, click **Create**. Once the key is successfully created, it can be checked on the **KMS** page.

TIP

By default, the key creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

Version: v3.4.0 (Latest)

How to check keys in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS).

- Check basic information
- Check usage count
- Check audit
- Check members

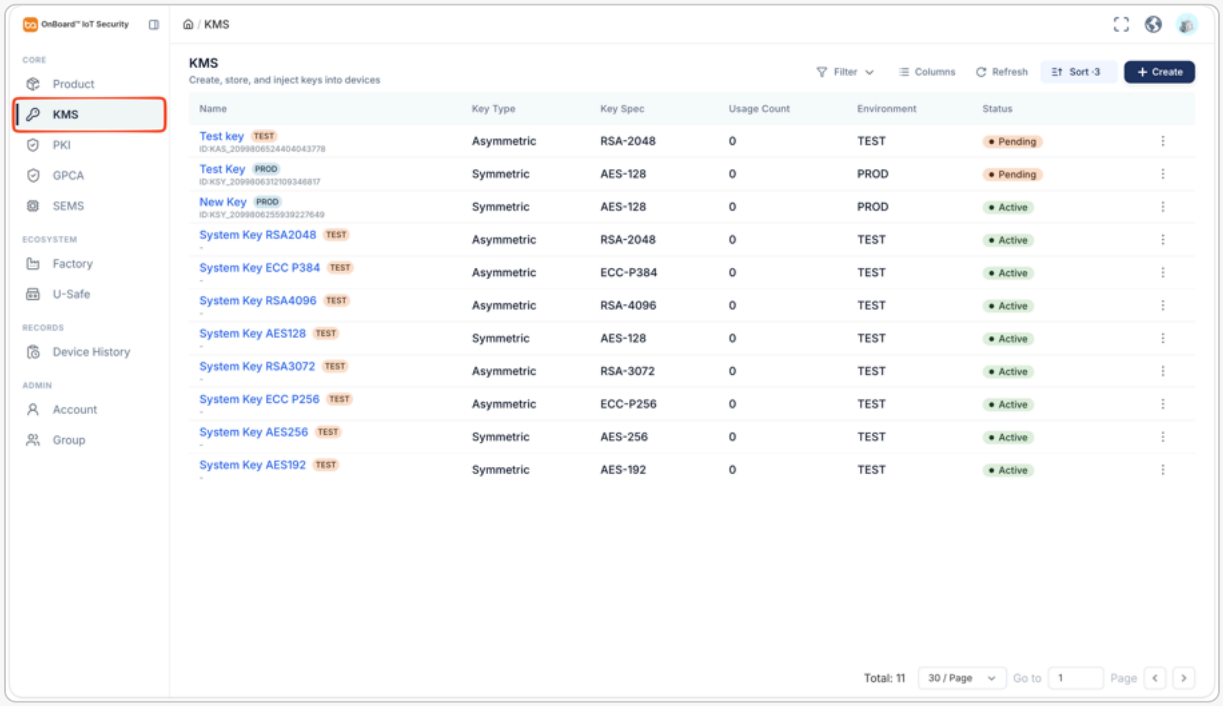
Prerequisites

Before getting started, please ensure that you have permissions for the corresponding key.

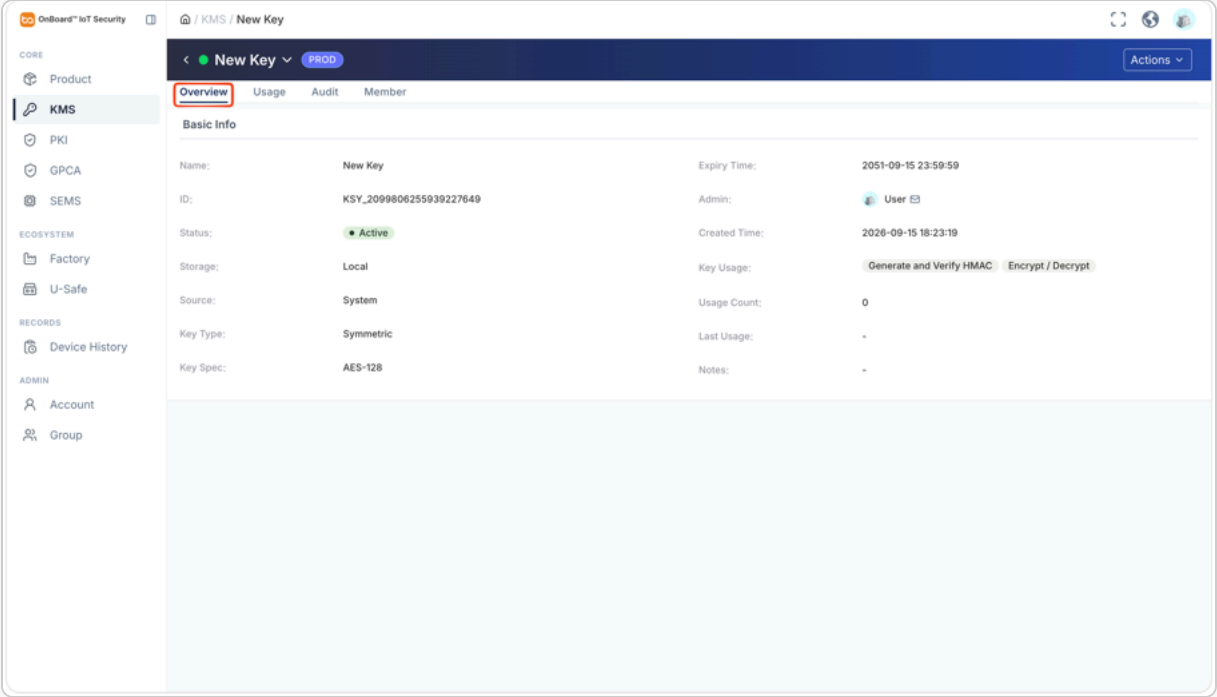
Check basic information

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then select the corresponding key.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



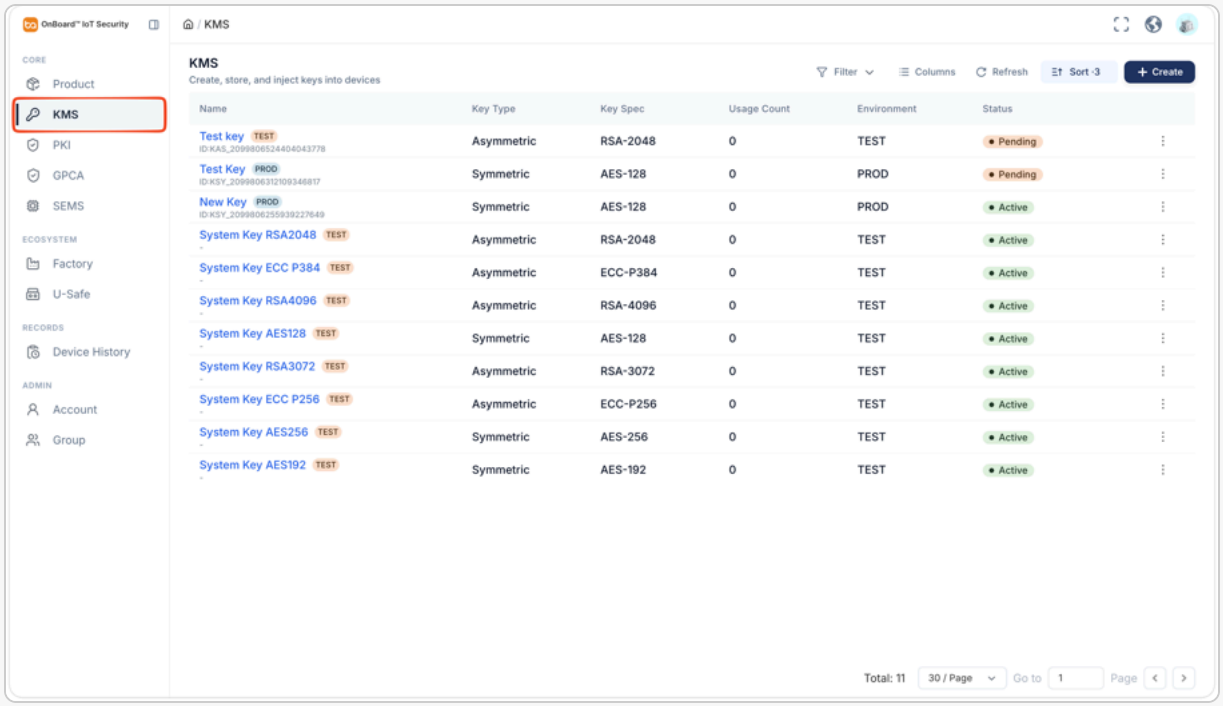
3. On the key page, you can check the key-related information (such as **Key Type**, **Key Spec**, and **Key Usage**).



Check usage count

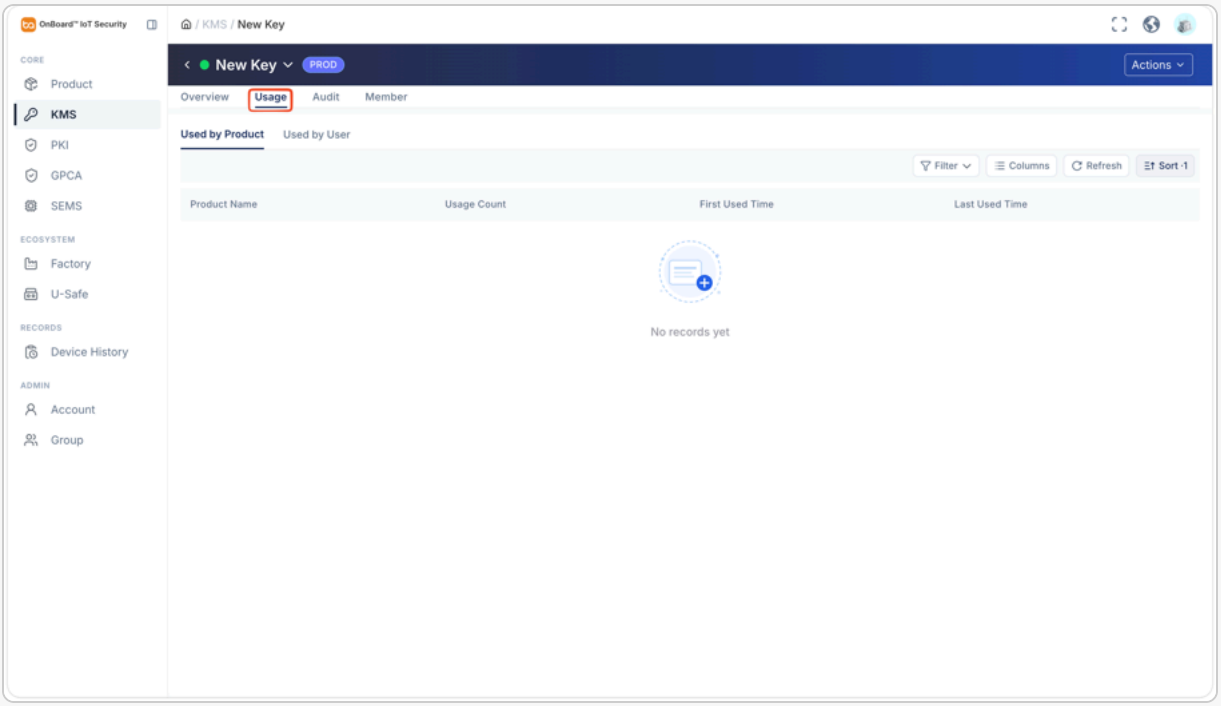
> **TIP**
>
> Key usage count can be used to check key dependencies and impact scope.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then select the corresponding key.



3. On the **Usage Count** tab of the key page, you can check the usage count (such as **Usage Count**, **First Used Time**, and **Last Used Time**) for keys used by users and products.

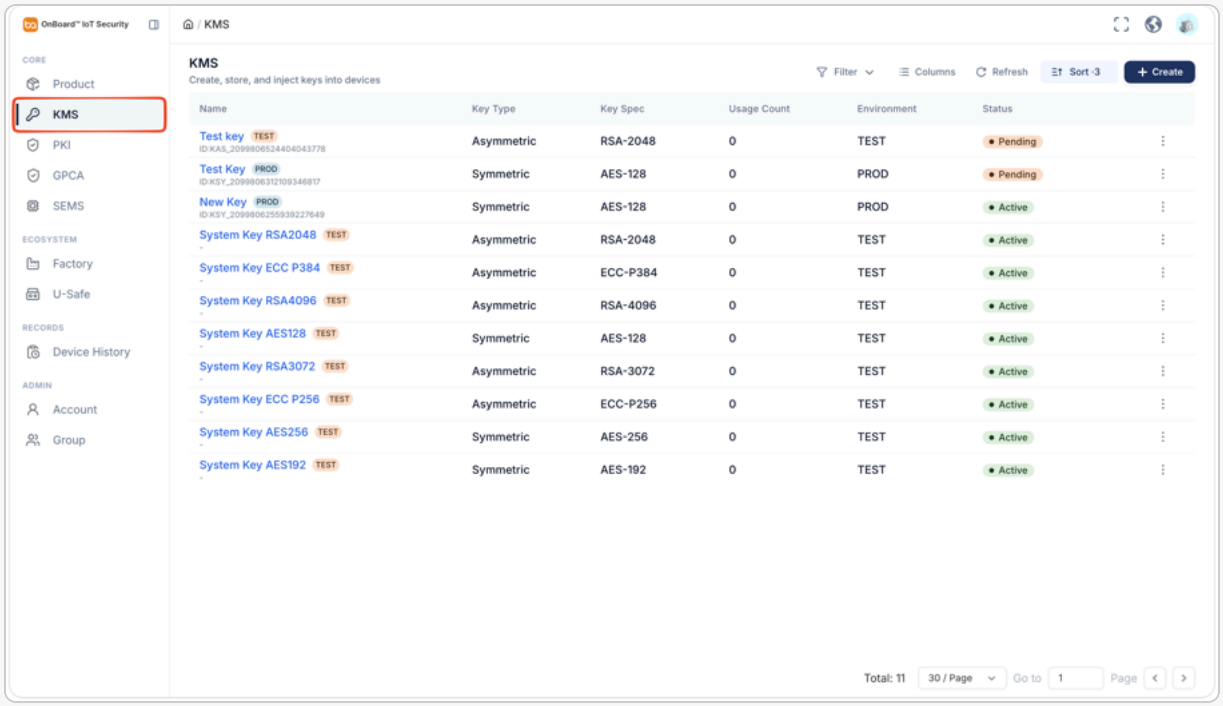
> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Check audit

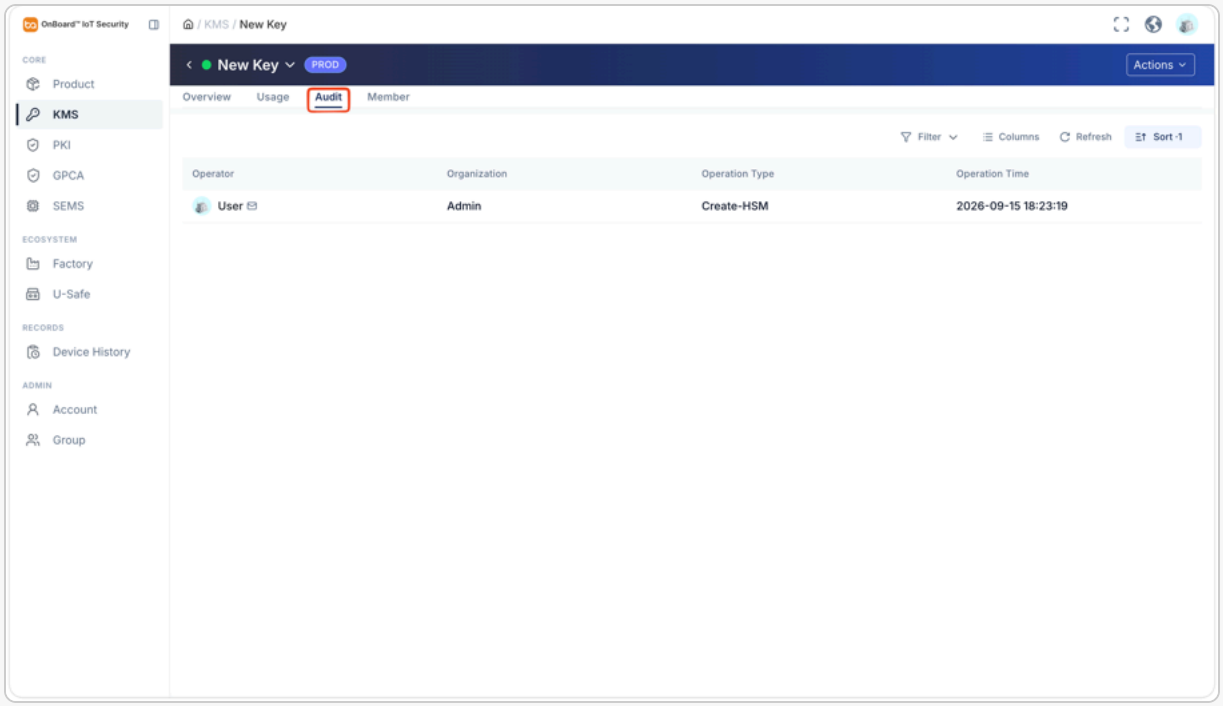
> **TIP**
>
> Through the key operation logs, you can check the historical operations of the key.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then select the corresponding key.



3. On the **Audit** tab of the key page, you can check the key history (such as **Operator**, **Operation Type**, and **Operation Time**).

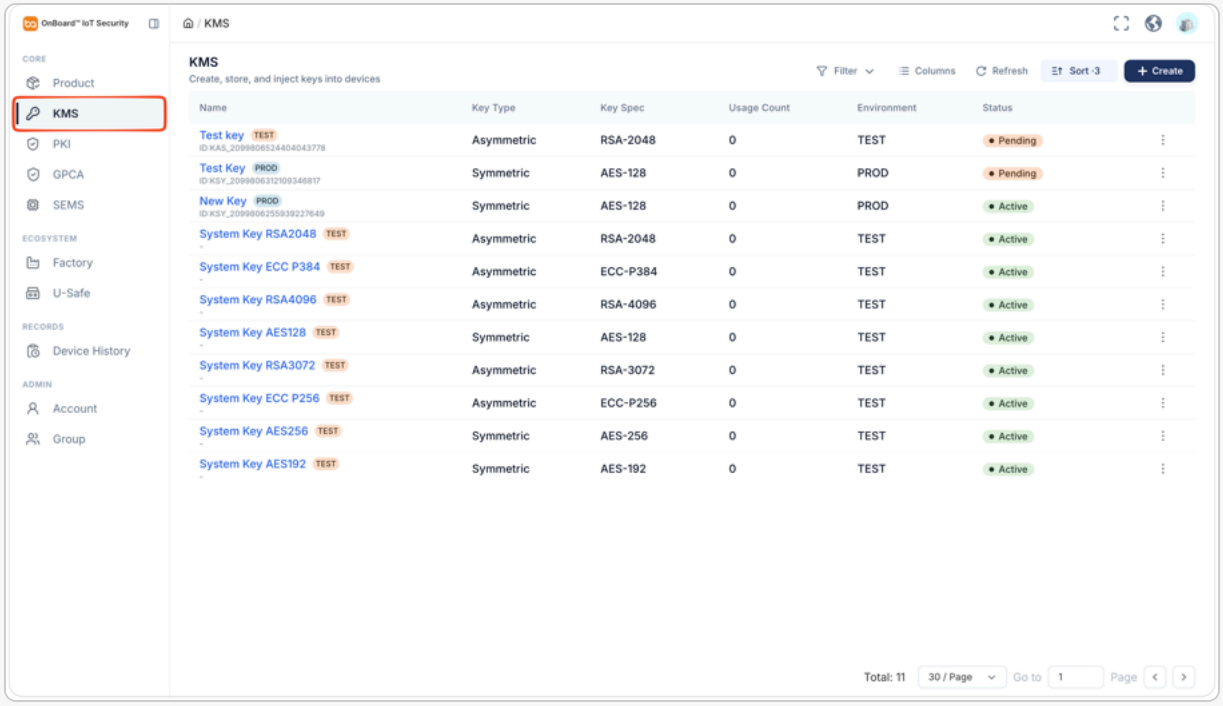
> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Check members

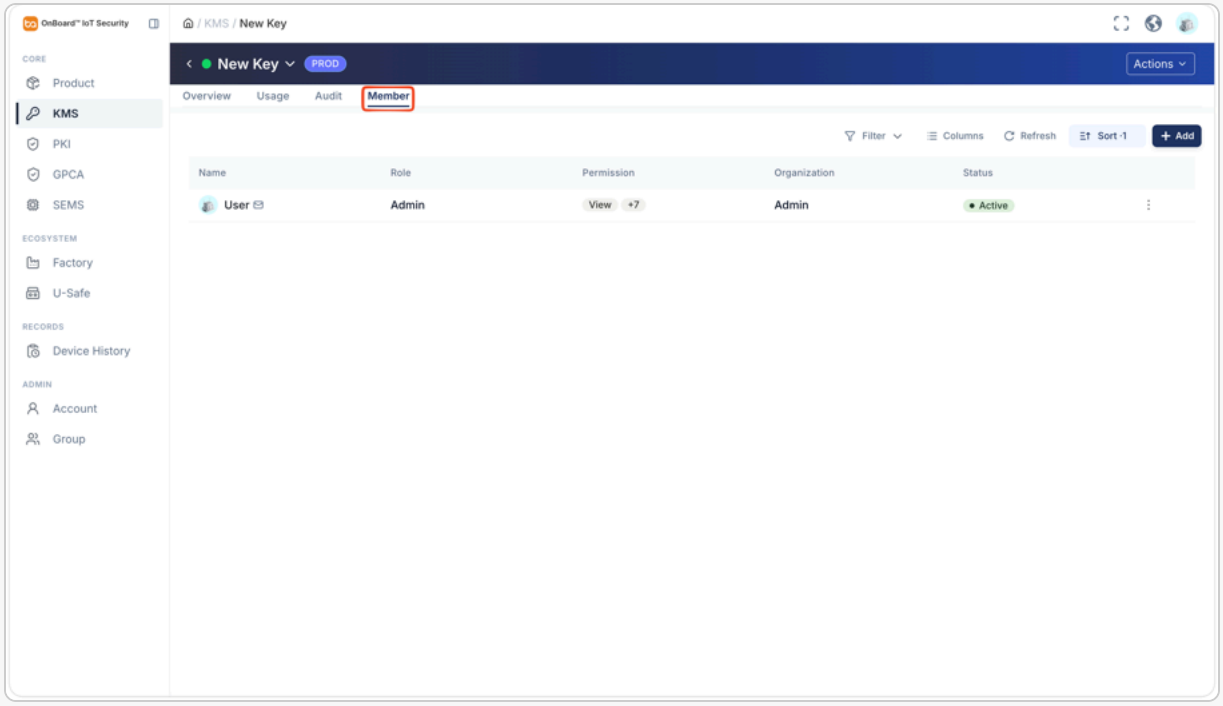
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **KMS**, and then select the corresponding key.



3. On the **Member** tab of the key page, you can check the user permissions for the key (such as **Name**, **Role**, and **Permission**).

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.


OnBoard™ IoT Security
/ KMS / New Key
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
New Key
PROD
Actions
Overview
Usage
Audit
Member
Filter
Columns
Refresh
Sort -1
Add
Name
Role
Permission
Organization
Status
User
Admin
View
+7
Admin
Active

Version: v3.4.0 (Latest)

How to manage keys in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Manage key permissions
- Download a key
- Lock or unlock a key
- Revoke a key
- Destroy a key

Prerequisites

Before getting started, please ensure that you have permissions for the corresponding key.

Manage key permissions

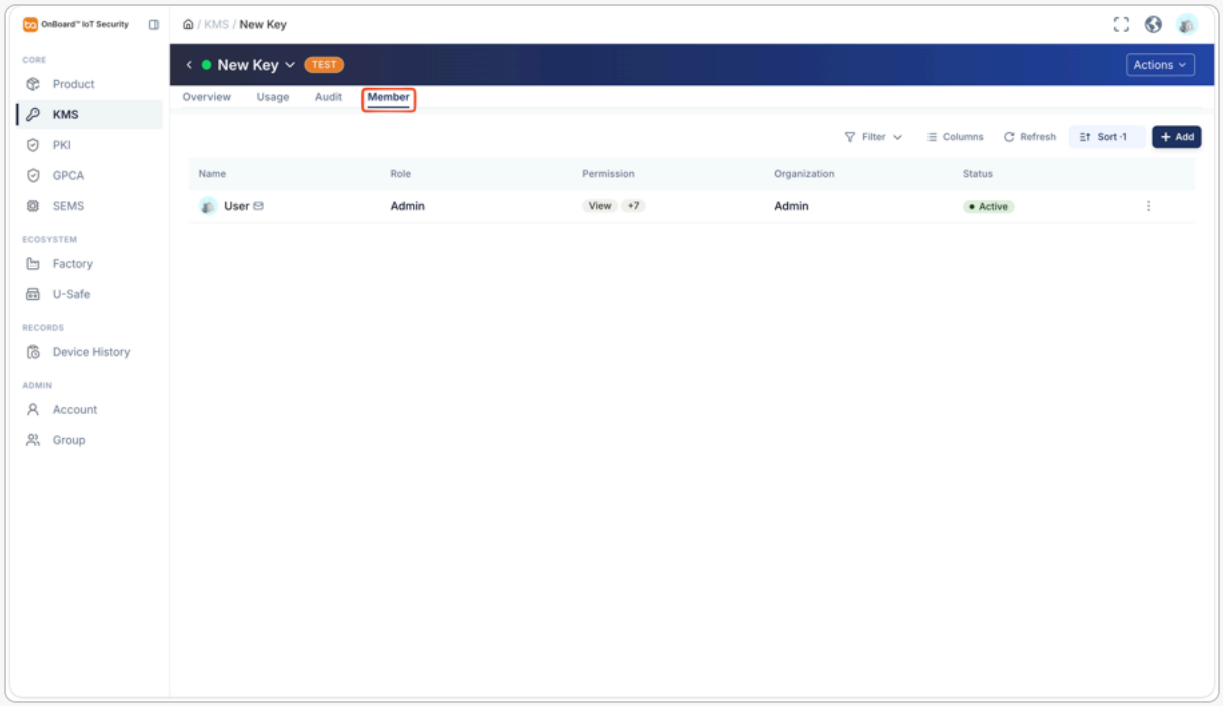
> **TIP**
>
> By default, the key creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

You can assign different operational permissions for the key to different members. The descriptions of these permissions are as follows:

Permissions	Description
View	View key details (read-only).
Edit	Allow cryptographic configuration for the key.
Create Authorization	Allow the key to be referenced in product and SE Profile configurations.
Lock	Lock a key.
unlock	Unlock a locked key.
Add Member	Add members to this key and assign them permissions that do not exceed your own permissions.
Revoke	Revoke a key.
Destroy	Destroy a key.

You can adjust and set user permissions for keys by following these steps:

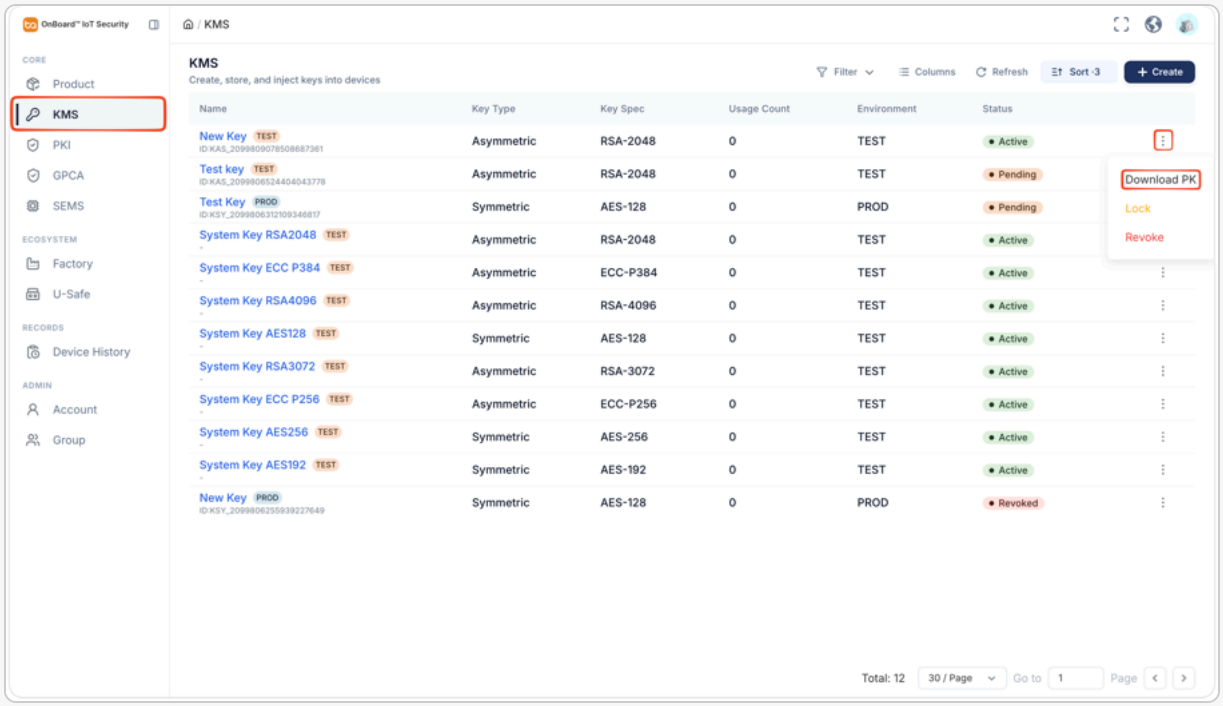
1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then select the corresponding key to navigate to the key page.
3. On the key page, you can manage the user permissions for the key on the **Member** tab.



Download a key

> **TIP**
>
> Download the public key of the asymmetric key for encryption and verification.
>
> Only keys in the **Active** state can be downloaded, and the same user can download the same key a maximum of 10 times per hour.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then click the Options icon for the corresponding asymmetric key and select **Download PK** to download the public key of the asymmetric key.

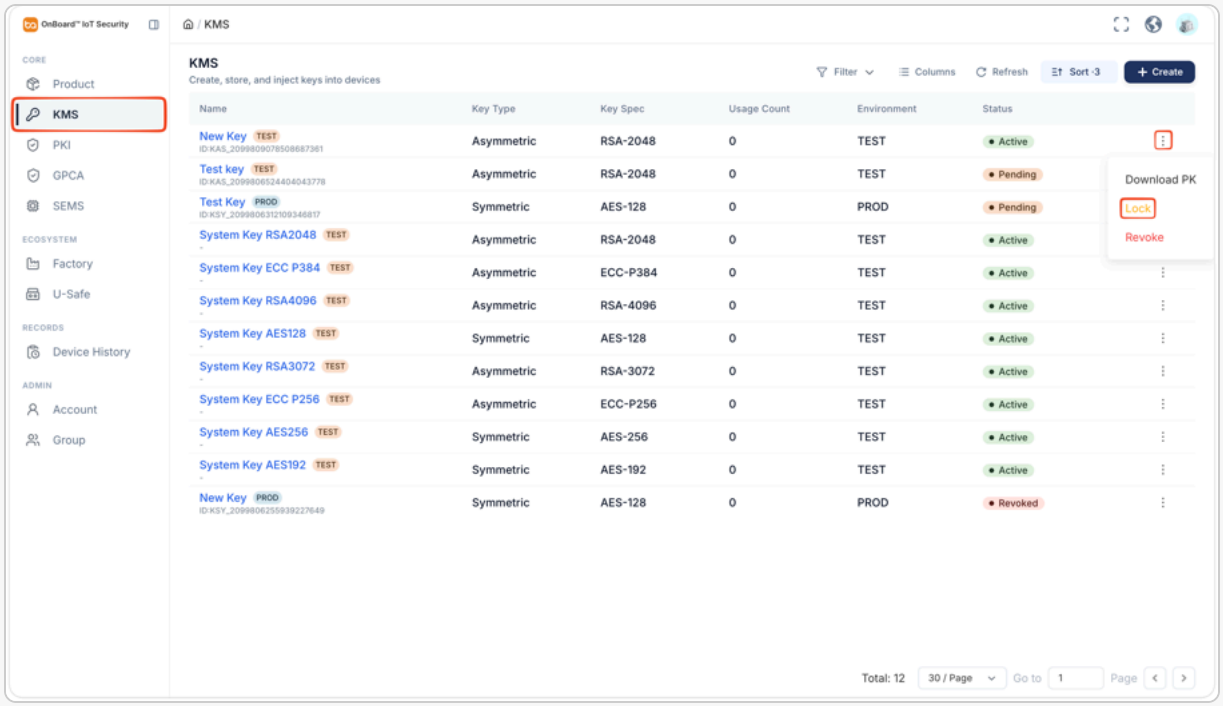


Lock or unlock a key

> **TIP**
>
> After the key is locked, the key can't be selected when configuring Keys for the product.

1. Sign in to OBIS.

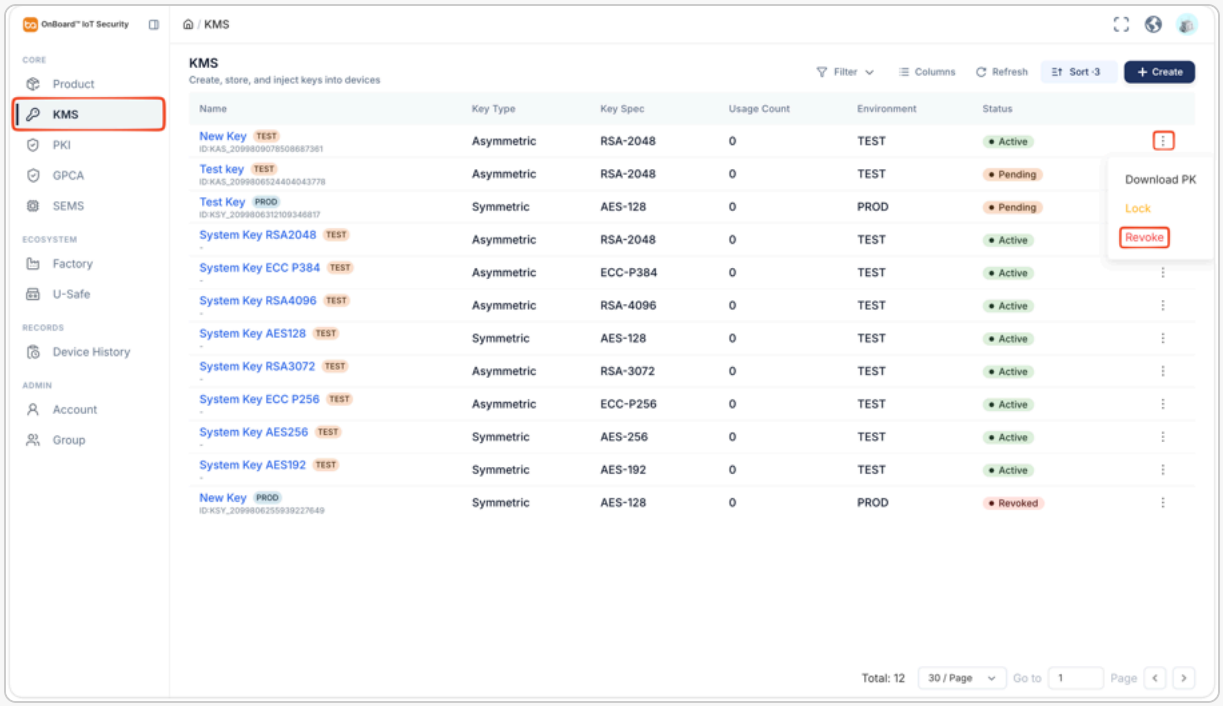
2. In the **Core** section of the left menu, click **KMS**, and then click the Options ⋮ icon for the corresponding key and select **Lock** or **Unlock**. Click **Confirm** to lock or unlock the key. When locking a key, you can optionally provide a reason.



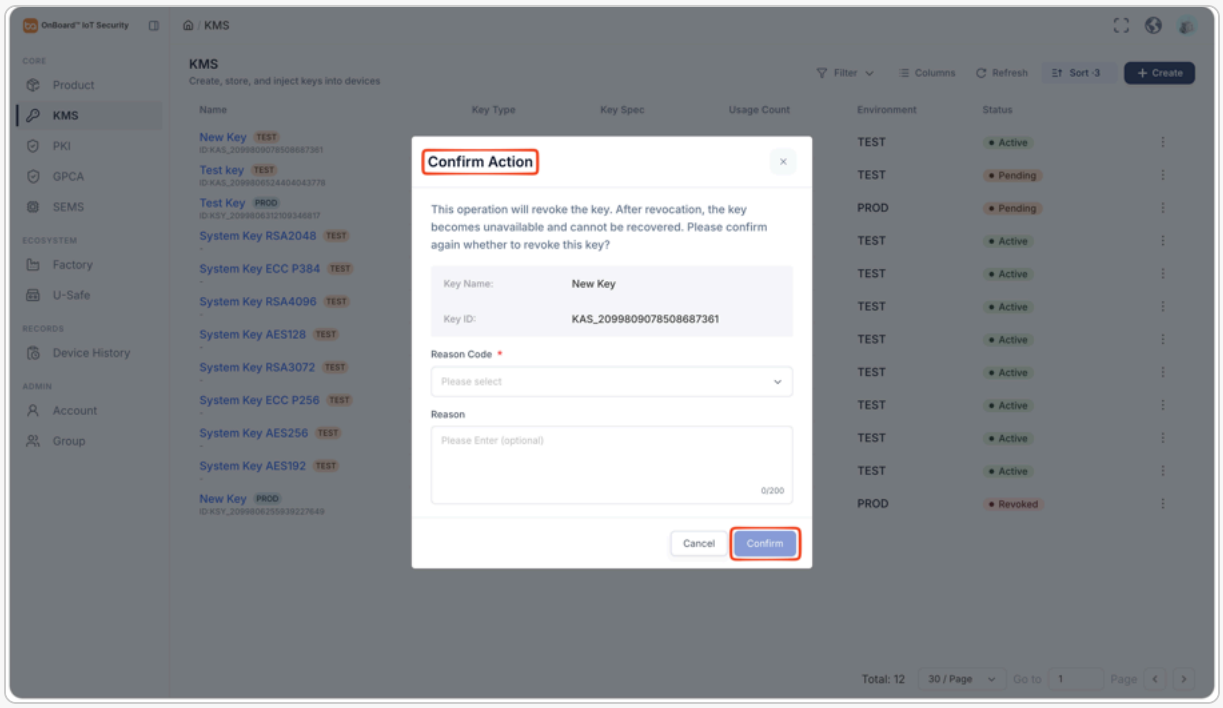
Revoke a key

> **TIP**
>
> After the key is revoked, its service capabilities are terminated to prevent further use.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then click the Options ⋮ icon for the corresponding key and select **Revoke**.



3. In the **Confirm Action** window, select the **Reason Code** and enter the **Reason**, then click **Confirm** to revoke the key.

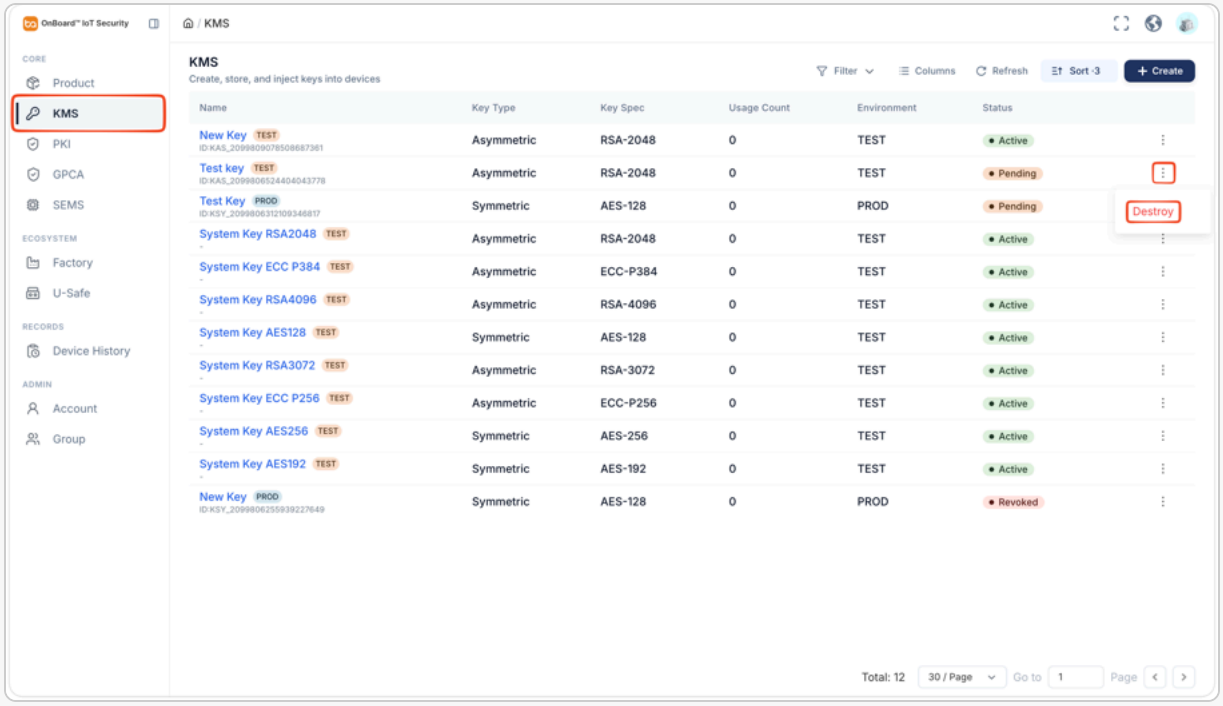


Destroy a key

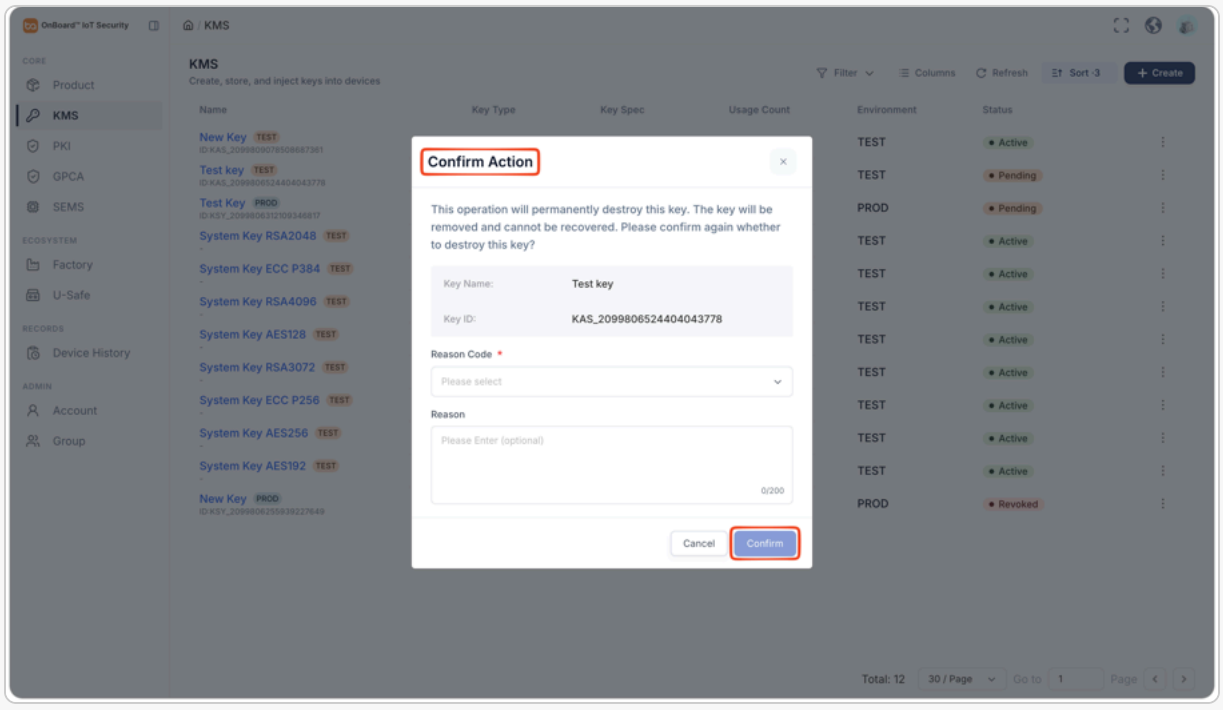
> **WARNING**
>
> Destroyed keys cannot be recovered. Please proceed with caution.

> **TIP**
>
> Only keys with the status of **Pending** or **Revoked** can be destroyed.
>
> Before destroying a key, please ensure that:
>
> - The key is not in use. If the key is currently in use, you will see the message "The key is in use and cannot be destroyed".
> - There are no valid authorizations associated with the key. If the key has been authorized for the product or SEMS, you will see the message "The key has valid authorizations. Please revoke them first".
> - The revoked key exceeded the 90-day audit retention period. If the 90-day period has not yet elapsed, you will see the message "The key audit retention period has not expired. It cannot be destroyed yet".

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **KMS**, and then click the Options icon for the corresponding key and select **Destroy**.



3. In the **Confirm Action** window, select the **Reason Code** and enter the **Reason**, then click **Confirm** to destroy the key.



Version: v3.4.0 (Latest)

Overview of PKI in OnBoard™ IoT Security

PKI (Public Key Infrastructure) in OBIS (OnBoard™ IoT Security) is the core module responsible for certificate security, which provides certificate generation, issuance, and revocation services to ensure secure communication for IoT devices. It is mainly used for:

- Pre-provisioning certificate templates for devices in bulk.
- Using command-line tools to issue end-entity templates.
- Using command-line tools to verify the validity of certificates and certificate chains.

In addition, OBIS provides certificate templates for the Matter protocol, enabling rapid generation of corresponding certificate chains. The following table summarizes the core capabilities of PKI:

Capability	Description
CA Hierarchy Management	• Root CA and Intermediate CA hierarchy management • Certificate chain validation and trust path verification

Capability	Description
Certificate Lifecycle	• Certificate issuance, renewal, and revocation • Certificate templates and policy management • Certificate validity and status monitoring
External PKI Integration (Root CA Delegation)	• OEM retains Root CA ownership in enterprise PKI • PKI operates issuing CAs under delegated authority

Version: v3.4.0 (Latest)

Create a certificate - OnBoard™ IoT Security

OnBoard™ IoT Security provides comprehensive certificate creation capabilities for different IoT provisioning scenarios. This guide covers certificate creation based on the Matter, Google Cast, and Custom specifications. Select a certificate type below to explore its workflow.

Version: v3.4.0 (Latest)

How to create a certificate based on the Matter specification in OnBoard™ IoT Security

This article will guide you on how to create a certificate based on the Matter specification in OnBoard™ IoT Security (OBIS).

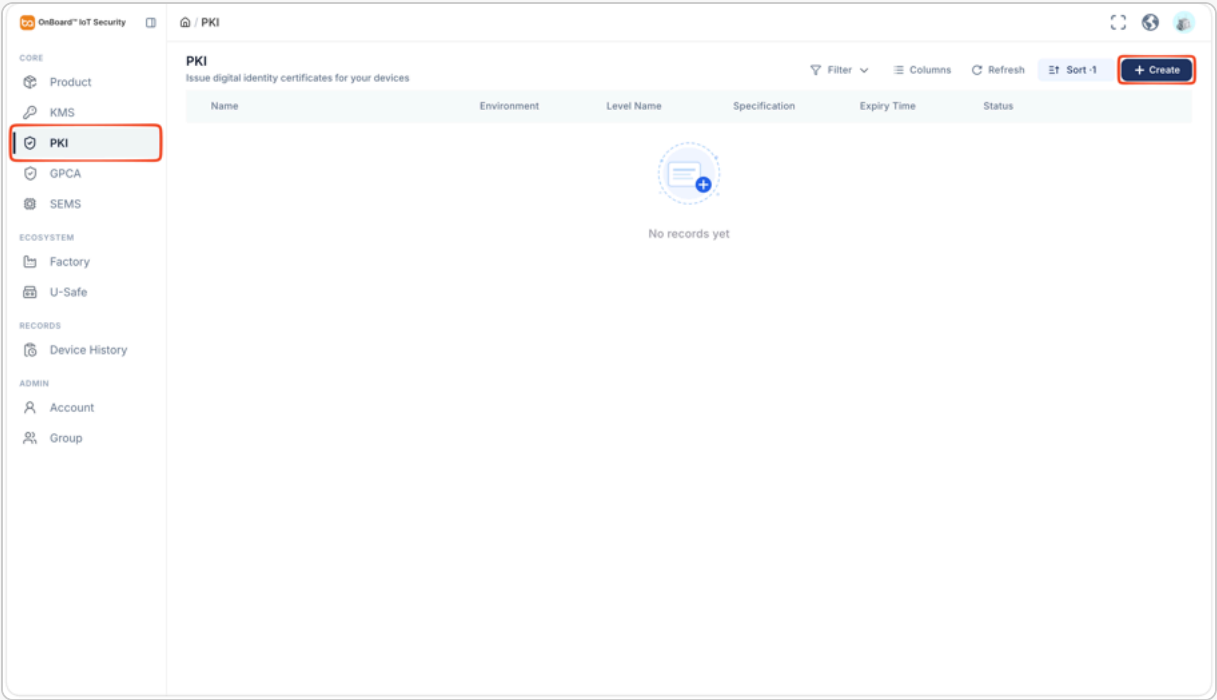
Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager or Resource Manager.

Instructions

> **TIP**
>
> After a certificate template based on the Matter specification is created, it can be selected when configuring Certificates for a product.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **PKI**, and then click **Create** on the **PKI** page.



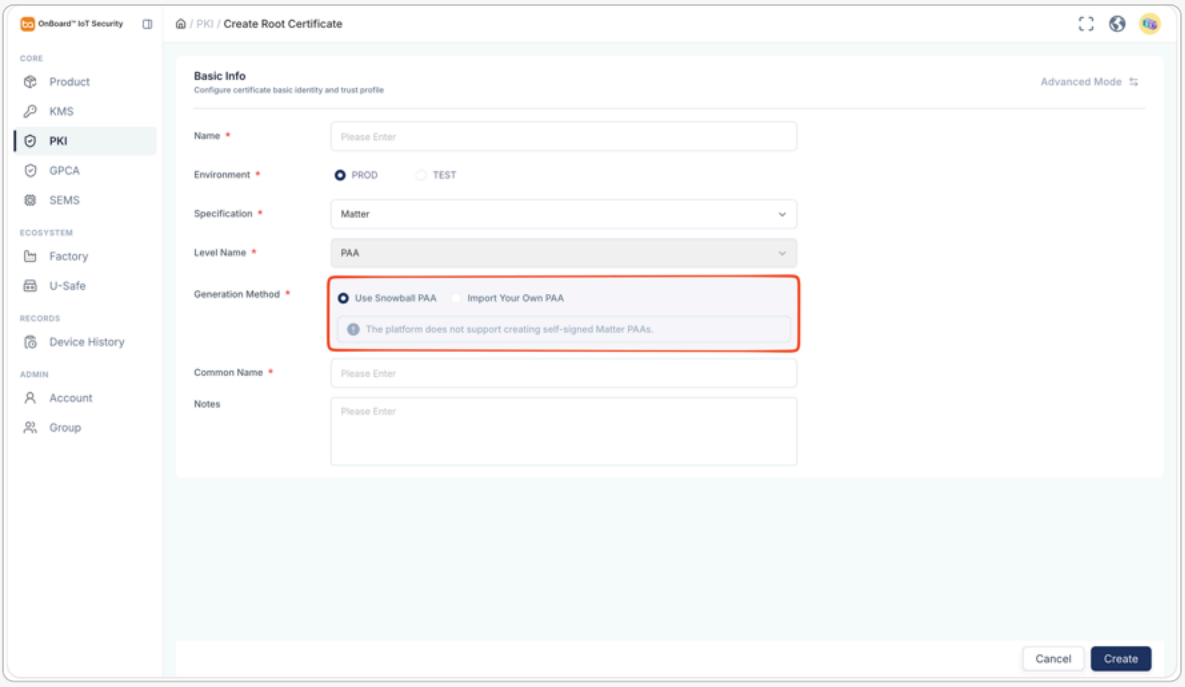
Create a PAA certificate based on the Matter specification

Create a PAI certificate based on the Matter specification

Create a DAC template based on the Matter specification

1. On the **Basic Info** section, select **Use Snowball PAA** or **Import Your Own PAA** as needed.

> **TIP**
>
> If a system-generated PAA certificate already exists in the current environment, select **Import Your Own PAA** to create a new PAA.



Description of PAA certificate basic information:

Information	Use Snowball PAA	Import Your Own PAA
Name	The PAA certificate name must be unique in the same environment.	
Environment	Two environments can be selected: **PROD** and **TEST**.	
Specification	Select the **Matter** specification.	
Level Name	Default is **PAA**.	

Information	Use Snowball PAA	Import Your Own PAA
Generation Method	No file upload is required.	Click the Add + icon to select and upload a PAA certificate in **.pem** format, or directly drag your own PAA certificate into the upload area.
Common Name	Name of certificate holder.	N/A
Notes	Provide additional information related to the PAA certificate, such as special requirements and important notes.	

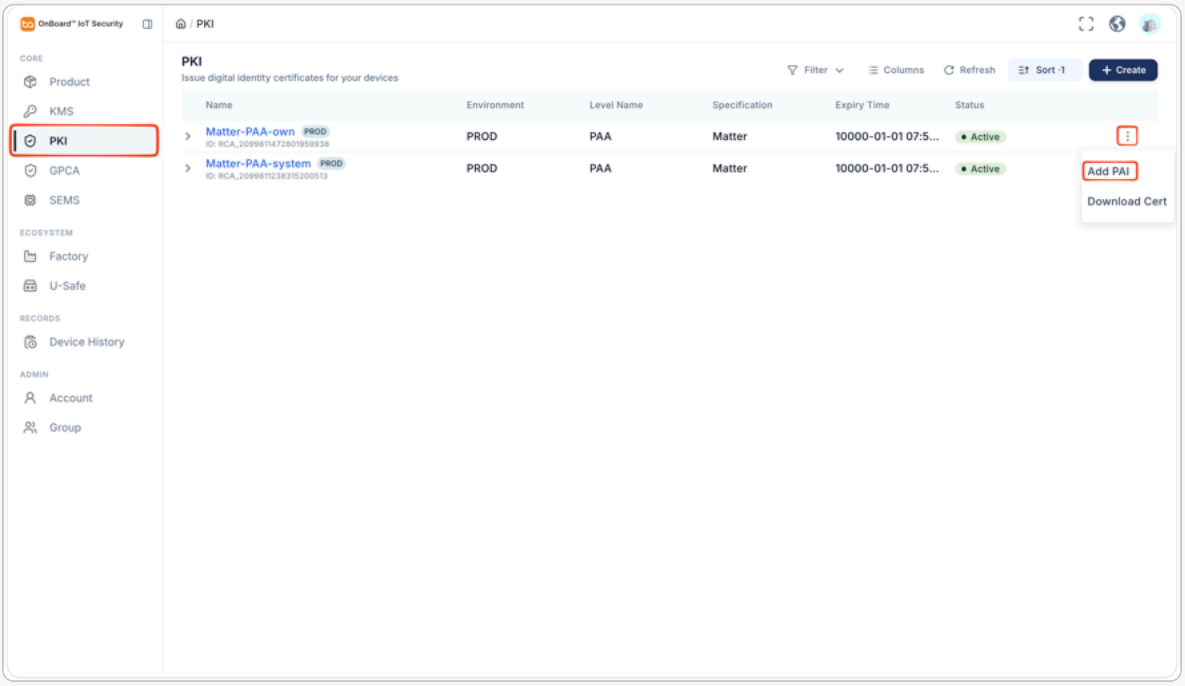
2. After verifying that the information is correct, click **Create** to complete the PAA certificate creation.

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

INFO

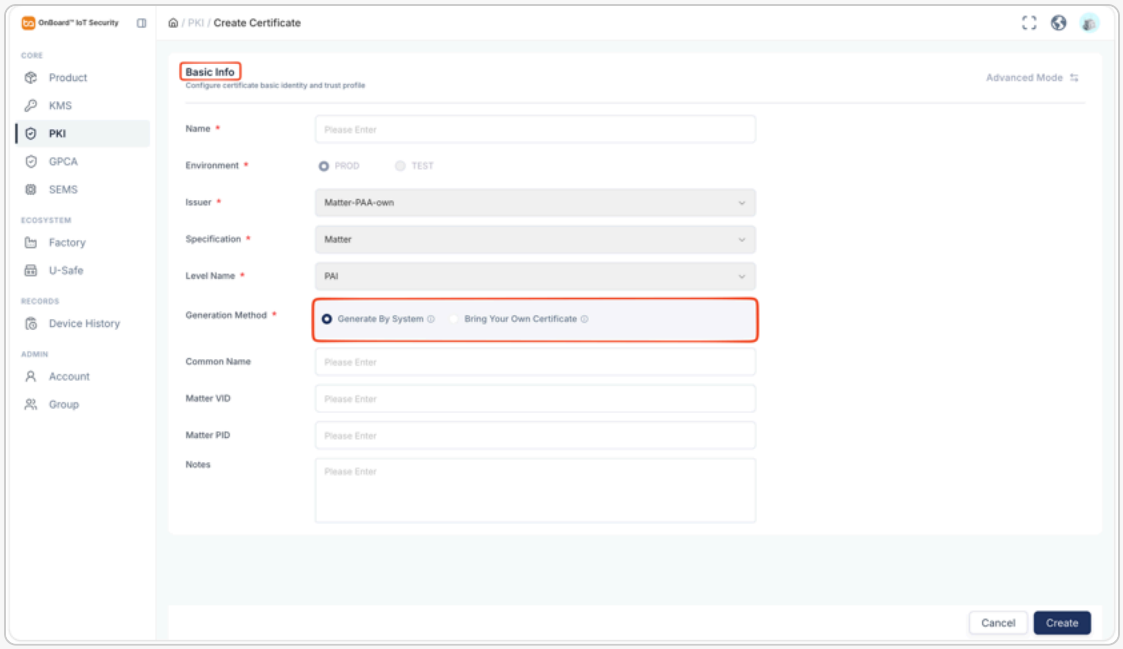
Before creating a PAI certificate based on the Matter specification, please ensure that at least one PAA certificate based on the Matter specification has been created so that it can be selected and inherited during configuration.

1. On the **PKI** page, click the Options ⋮ icon for the corresponding PAA certificate and select **Add PAI**.



2. On the **Basic Info** section, select and enter the basic information.

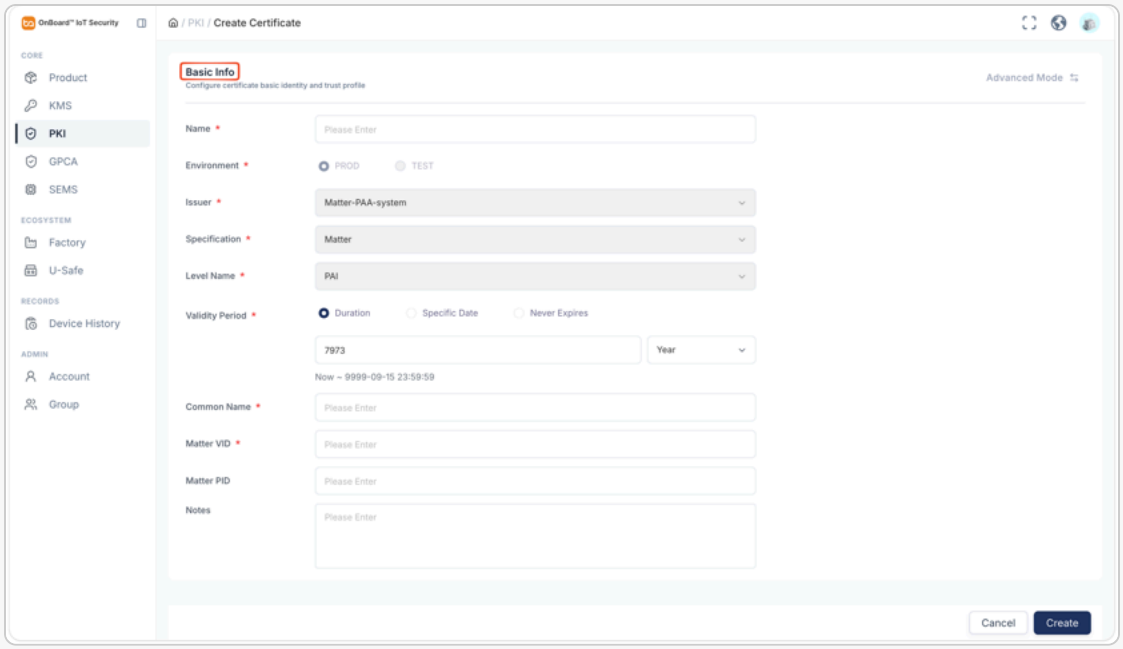
    - If the issuer of the PAI certificate is your own PAA certificate, you can select **Generate by System** or **Bring Your Own Certificate** as needed



Information	Generate by System	Bring Your Own Certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Environment	The environment is inherited from the PAA certificate.	
Issuer	The inherited PAA certificate.	
Specification	Default is **Matter**.	
Level Name	Default is **PAI**.	

Information	Generate by System	Bring Your Own Certificate
Generation Method	No file upload is required.	Click the Add + icon to select and upload a PAI certificate in **.pem** format, or directly drag your own PAI certificate into the upload area.
Common Name	Name of certificate holder.	N/A
Matter VID	Matter vendor ID.	N/A
Matter PID	Matter product ID.	N/A
Notes	Provide additional information related to the PAI certificate, such as special requirements and important notes.	

- If the issuer of the PAI certificate is the system-generated PAA certificate



Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Environment	The environment is inherited from the PAA certificate.
Issuer	The inherited PAA certificate.
Specification	Default is **Matter**.
Level Name	Default is **PAI**.

Information	Description
Validity Period	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed. Setting an expiration date beyond that of the inherited certificate may result in certificate chain validation failures, client trust issues, and audit risks.
Common Name	Name of certificate holder.
Matter VID	Matter vendor ID.
Matter PID	Matter product ID.
Notes	Provide additional information related to the PAI certificate, such as special requirements and important notes.

3. After verifying that the information is correct, click **Create** to complete the PAI certificate creation.

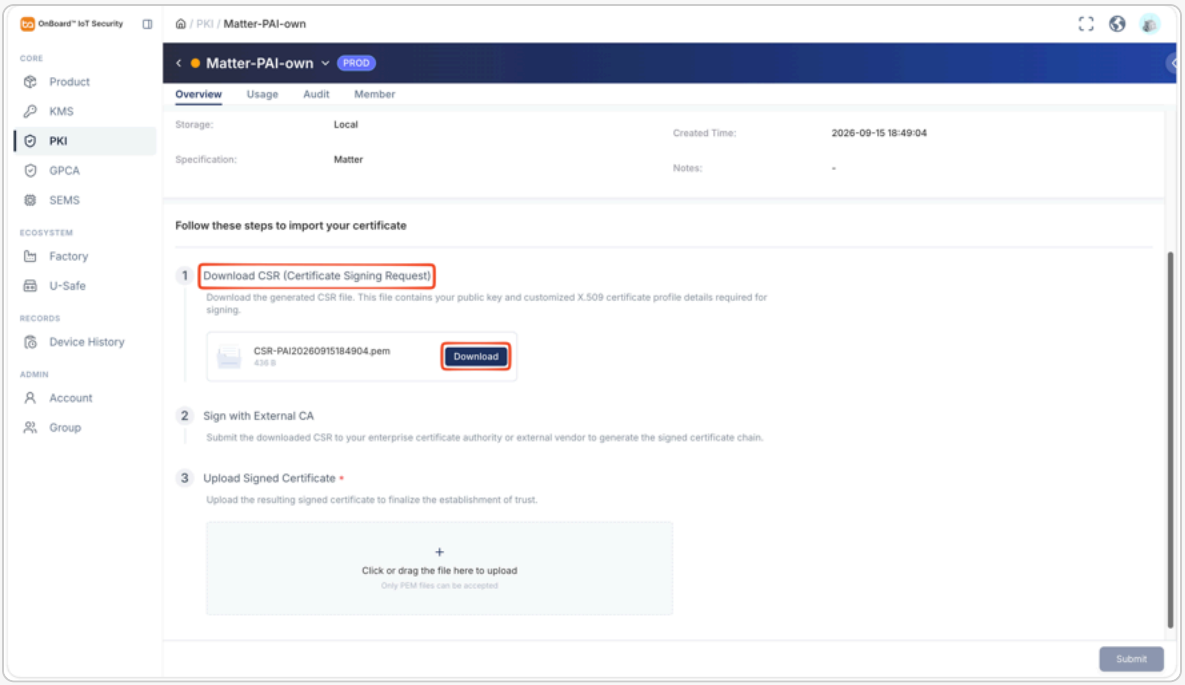
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating a PAI certificate, if the issuer is your own PAA certificate, you must complete the CSR (Certificate Signing Request) configuration for the PAI certificate. Before the CSR configuration is completed, the certificate will remain in the **Pending** status and can't be used.

CSR configuration steps for the PAI certificate

> **TIP**
>
> When creating a PAI certificate, if the issuer is your own PAA certificate, refer to the following steps to complete the CSR configuration.

1. On the **PKI** page, expand the corresponding certificate chain, and then click the corresponding PAI certificate.

2. Locate the **Download CSR (Certificate Signing Request)** section on the certificate page, click **Download** to download the CSR file. Then, use your Root CA to sign the file, thereby generate a PAI certificate signed by the Root CA.

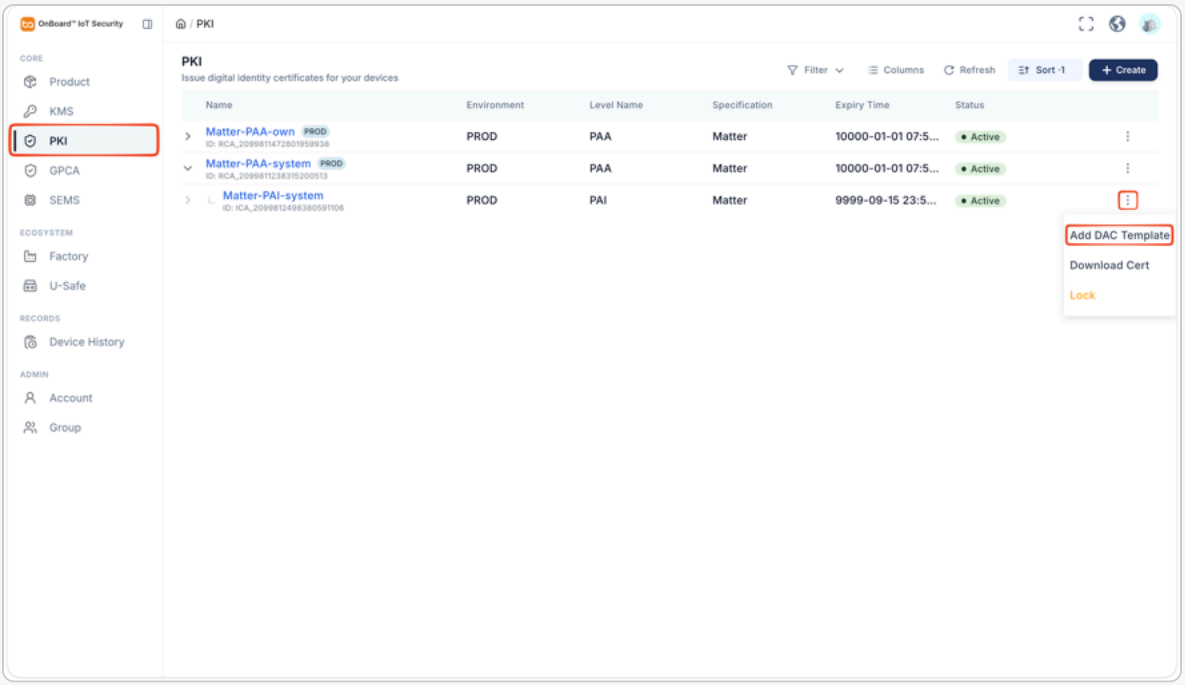


3. After a PAI certificate is generated, click the Add + icon in the upload area, select and upload the PAI certificate in **.pem** format (the maximum supported file size is 512 MB), or directly drag and drop your PAI certificate into the upload area.

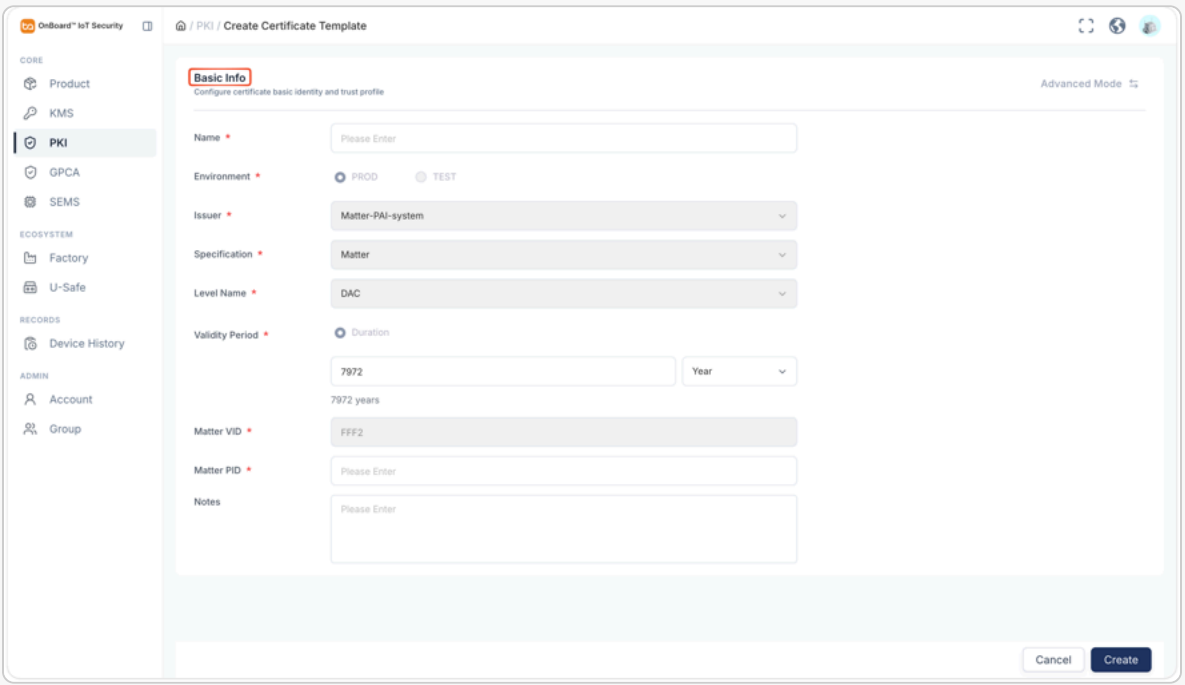
4. Click **Submit**. Once the configuration is completed, the PAI certificate status will change to **Normal**.

> **INFO**
>
> Before creating a DAC template, please ensure that at least one PAI certificate based on the Matter specification has been created so that it can be selected and inherited during configuration.

1. On the **PKI** page, expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding PAI certificate and select **Add DAC Template**.



2. On the **Basic Info** section, select and enter the basic information.



Description of DAC template basic information:

Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Environment	The environment is inherited from the PAI certificate.
Issuer	The inherited PAI certificate.
Specification	Default is **Matter**.
Level Name	Default is **DAC**.
Validity Period	Set the validity period of the DAC template. Setting an expiration date beyond that of the inherited certificate may result in certificate chain validation failures, client trust issues, and audit risks.
Matter VID	Matter vendor ID.
Matter PID	Matter product ID.
Notes	Provide additional information related to the DAC template, such as special requirements and important notes.

3. After verifying that the information is correct, click **Create** to complete the DAC template creation.

TIP

By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

Version: v3.4.0 (Latest)

How to create a certificate based on the Google Cast specification in OnBoard™ IoT Security

This article will guide you on how to create a certificate based on the Google Cast specification in OnBoard™ IoT Security (OBIS).

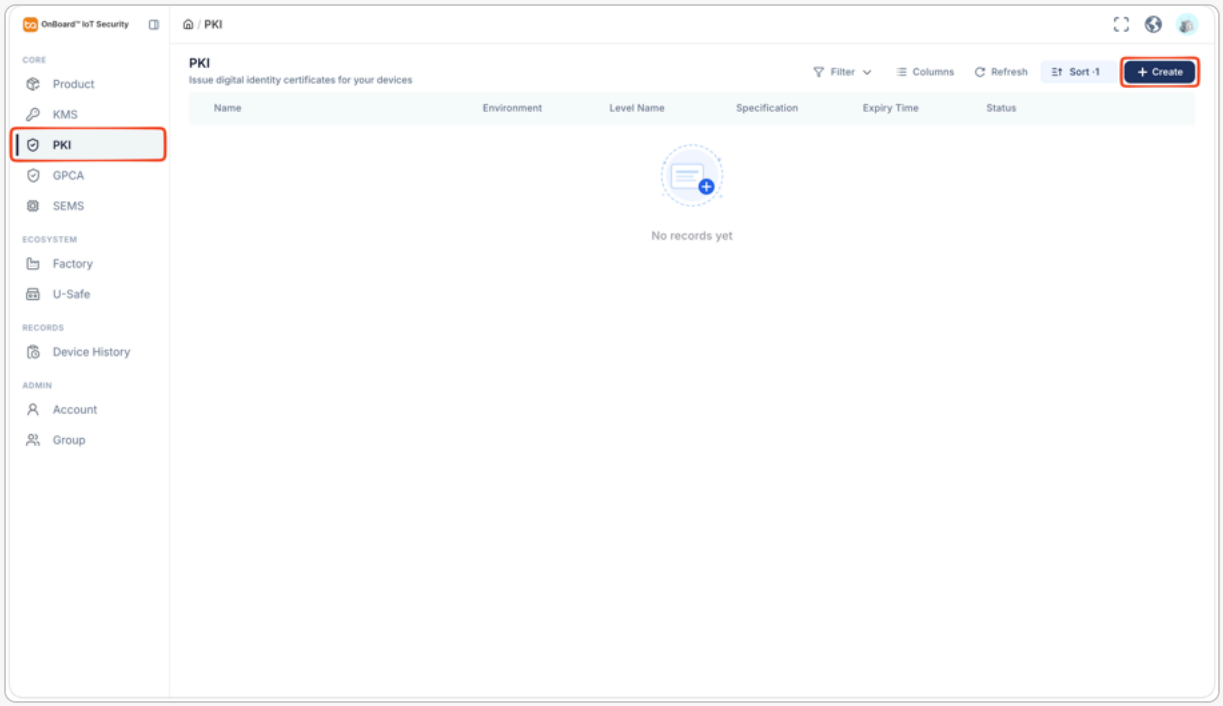
Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager or Resource Manager.

Instructions

> **TIP**
>
> After a certificate template based on the Google Cast specification is created, it can be selected when configuring Certificates for a product.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **PKI**, and then click **Create** on the **PKI** page.



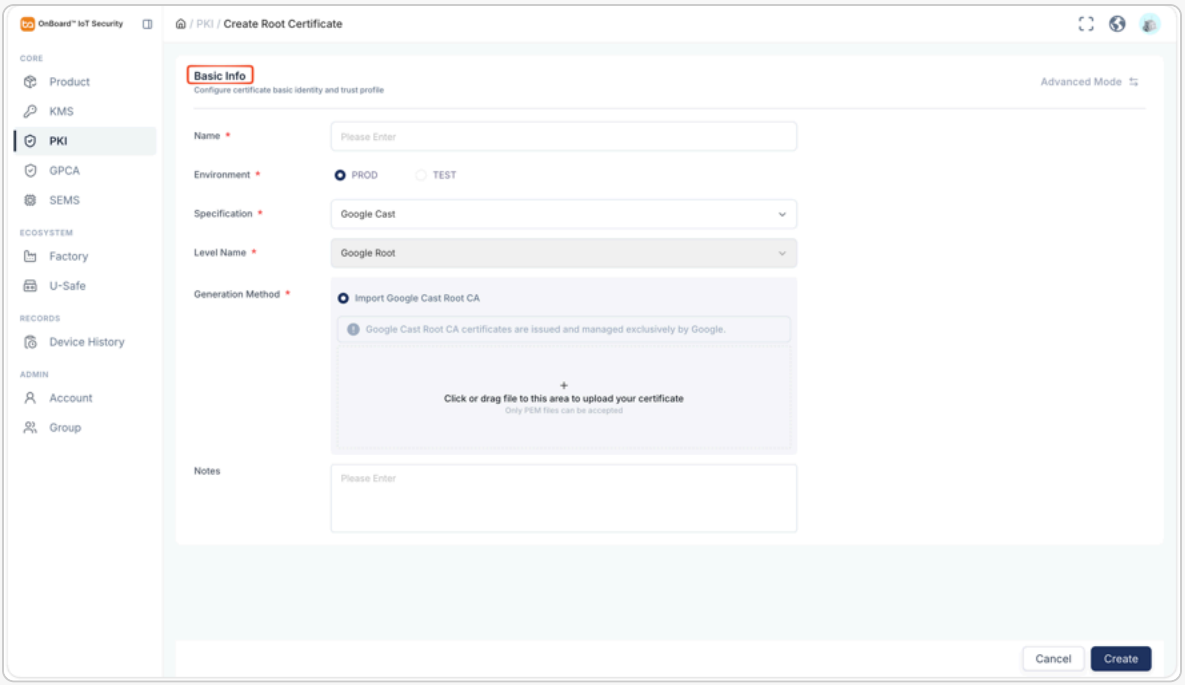
Create a Google Root certificate based on the Google Cast specification

Create a Manufacturer certificate based on the Google Cast specification

Create a Model certificate based on the Google Cast specification

Create a Device template based on the Google Cast specification

1. On the **Basic Info** section, enter and select the basic information.



Description of Google Root certificate basic information:

Information	Description
Name	The Google Root certificate name must be unique in the same environment.
Environment	Two environments can be selected: **TEST** and **PROD**.
Specification	Select the **Google Cast** specification.
Level Name	Default is **Google Root**.
Generation Method	Click the Add + icon to select and upload a Google Root certificate in **.pem** format, or directly drag your own Google Root certificate into the upload area.

Information	Description
Notes	Provide additional information related to the Google Root certificate, such as special requirements and important notes.

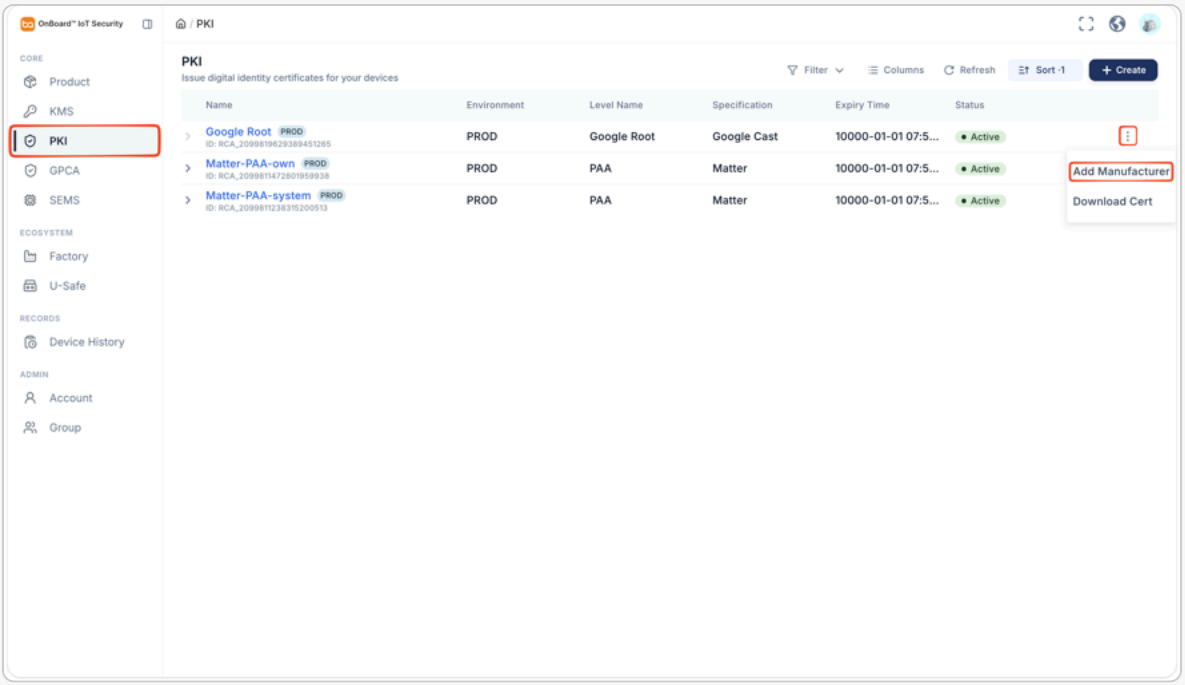
2. After verifying that the information is correct, click **Create** to complete the Google Root certificate creation.

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

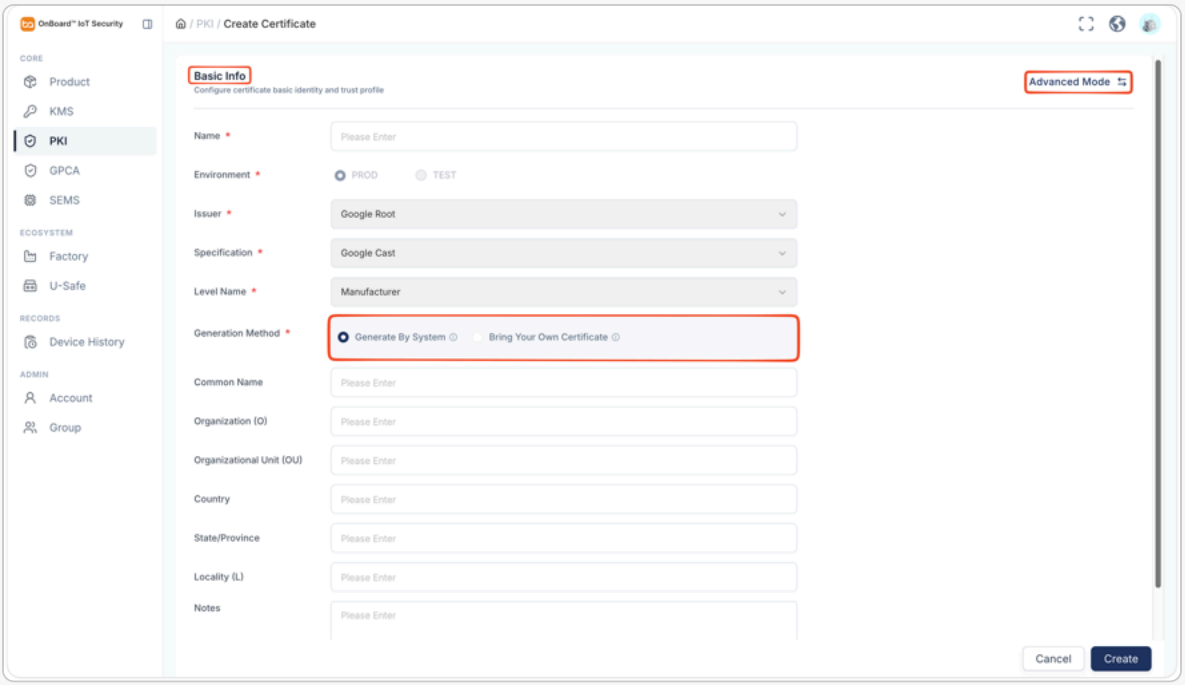
> **INFO**
>
> Before creating a Manufacturer certificate based on the Google Cast specification, please ensure that at least one Google Root certificate based on the Google Cast specification has been created so that it can be selected and inherited during configuration.

> **TIP**
>
> The default mode is simple mode, which requires only basic information. If you need to configure additional fields for the system-generated certificate, you can switch to advanced mode by clicking **Advanced Mode** in the top-right corner of the page.

1. On the **PKI** page, click the Options ⋮ icon for the corresponding Google Root certificate and select **Add Manufacturer**.



2. On the **Basic Info** section, select and enter the basic information. You can select **Generate by System** or **Bring Your Own Certificate** as needed

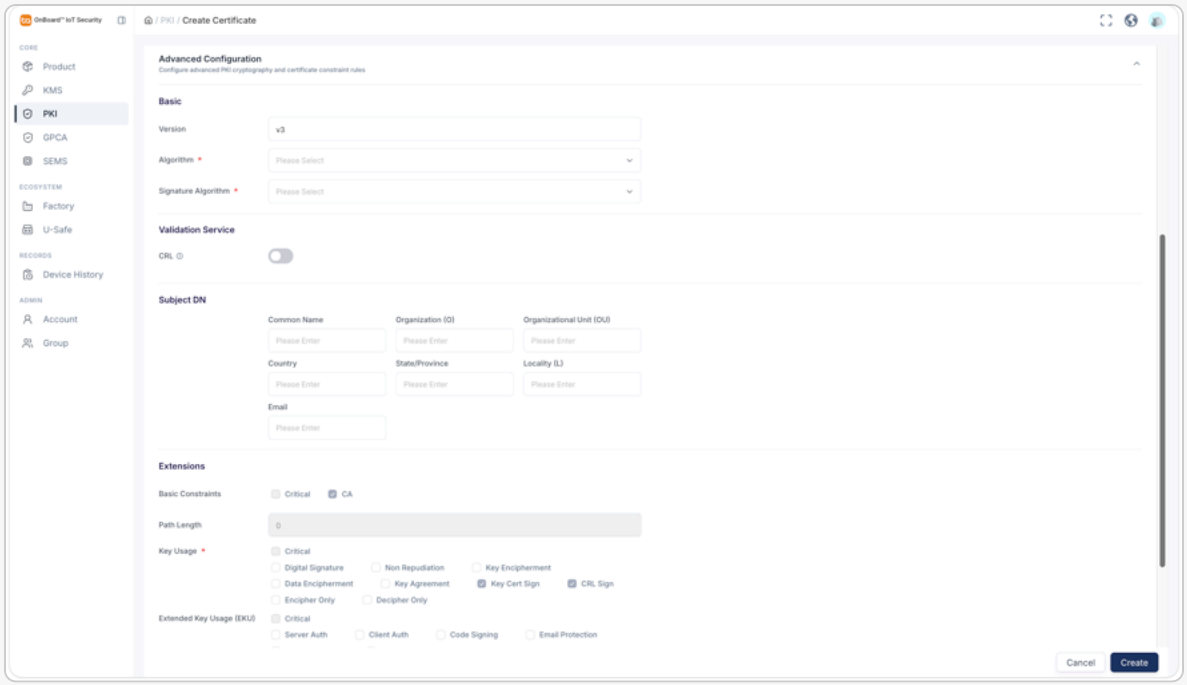


Information	Generate by System	Bring Your Own Certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Environment	The environment is inherited from the Google Root certificate.	
Issuer	The inherited Google Root certificate.	
Specification	Default is **Google Cast**.	
Level Name	Default is **Manufacturer**.	

Information	Generate by System	Bring Your Own Certificate
Generation Method	No file upload is required.	Click the Add + icon to select and upload a Manufacturer certificate in **.pem** format, or directly drag your own Manufacturer certificate into the upload area.
Common Name	Name of certificate holder.	N/A
Organization (O)	Organizational name.	N/A
Organizational Unit (OU)	Organizational unit name.	N/A
Country	Two ISO country codes.	N/A
State / Province	State or province name.	N/A
Locality (L)	City name.	N/A

Information	Generate by System	Bring Your Own Certificate
Notes	Provide additional information related to the Manufacturer certificate, such as special requirements and important notes.	

The configuration of advanced mode



- Description of Basic information:

Information	Description
Version	The standard version and can't be modified.
Algorithm	Automatically parsed from the certificate content and can't be modified.
Signature Algorithm	Automatically parsed from the certificate content and can't be modified.

- Description of Validation Service information:

Information	Description
CRL	Automatically parsed from the certificate content, you can set the **Full Update Period**.

- Description of Subject DN information:

> **TIP**
>
> At least one Subject DN information must be provided.

Information	Description
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.

- Description of Extensions information:

> **TIP**
>
> If the **Critical** checkbox for a certain item is selected, the system must recognize and support that item when processing the certificate; otherwise, the certificate will be rejected.

Information	Description
Basic Constraints	Confirm if it is a CA certificate.
Path Length	Limits the number of sub-certificates.
Key Usage	Optional key usages, such as **Digital Signature**, **Key Cert Sign**, and **CRL Sign**.
Extended Key Usage (EKU)	Optional extended key usages, such as **Server Auth**, **Client Auth**, and **Code Signing**.

3. After verifying that the information is correct, click **Create** to complete the Manufacturer certificate creation.

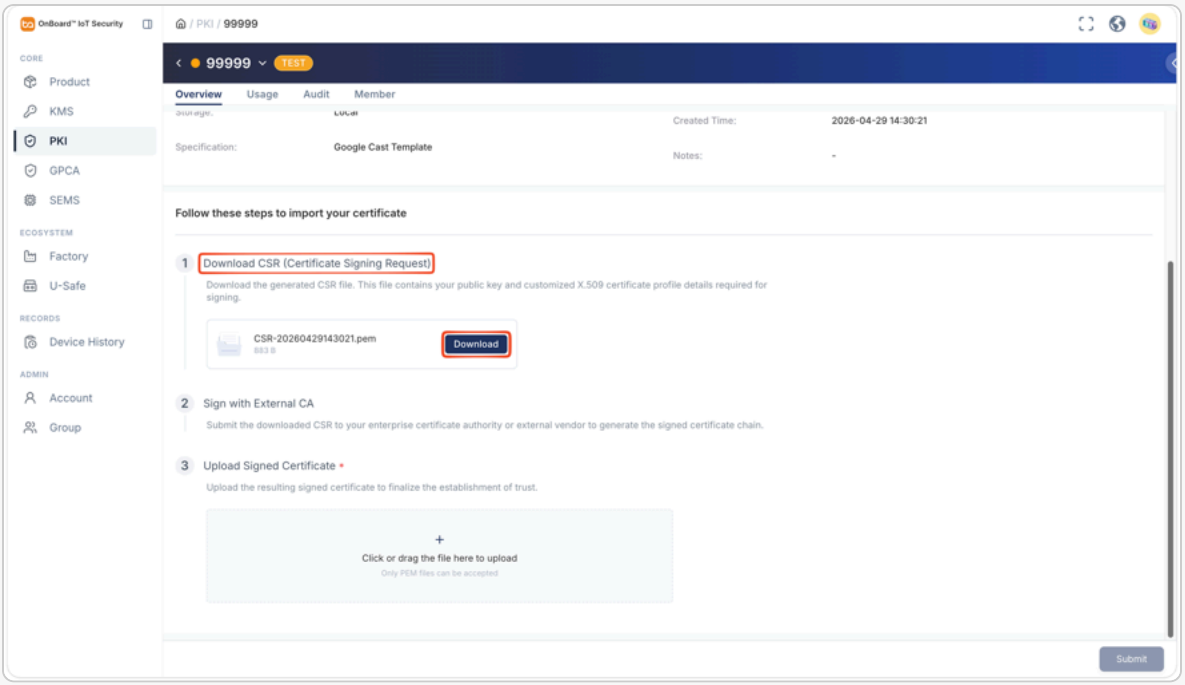
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating a Manufacturer certificate issued by an external CA, you must complete the CSR (Certificate Signing Request) configuration for the Manufacturer certificate. Before the CSR configuration is completed, the certificate will remain in the **Pending** status and can't be used.

CSR configuration steps for the Manufacturer certificate

> **TIP**
>
> When creating a Manufacturer certificate, refer to the following steps to complete the CSR configuration.

1. On the **PKI** page, expand the corresponding certificate chain, and then click the corresponding Manufacturer certificate.

2. Locate the **Download CSR (Certificate Signing Request)** section on the certificate page, click Download to download the CSR file. Then, use your Root CA to sign the file, thereby generate a Manufacturer certificate signed by the Root CA.



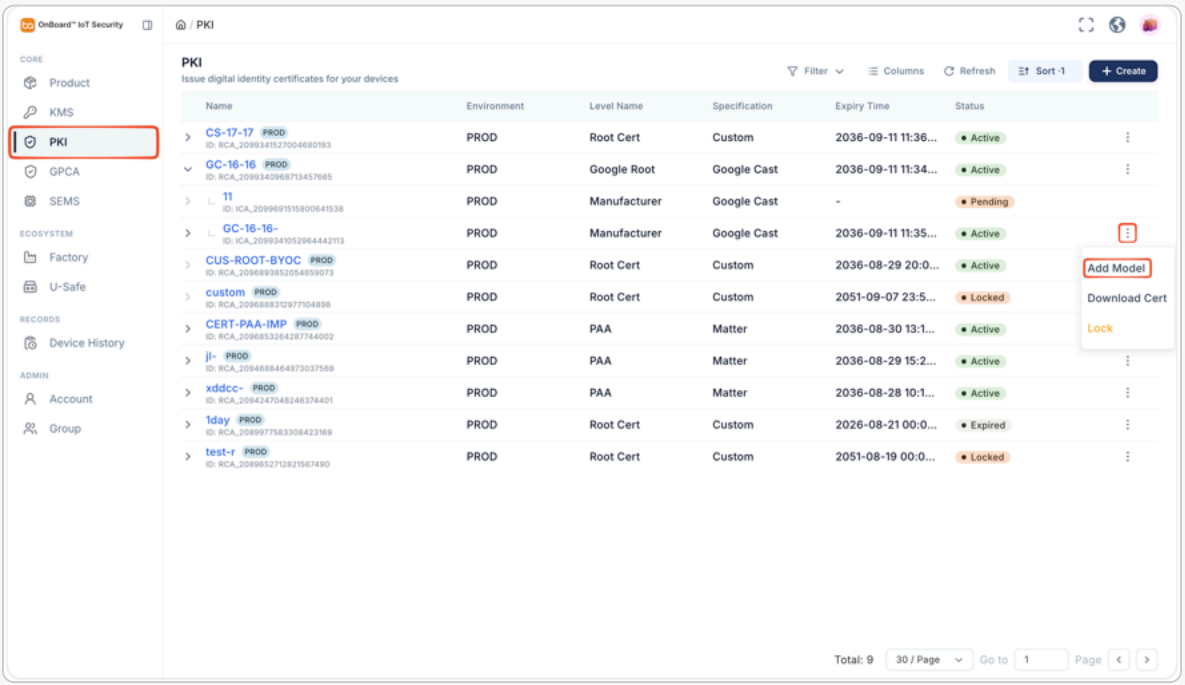
3. After a Manufacturer certificate is generated, click the Add + icon in the upload area, select and upload the Manufacturer certificate in **.pem** format (the maximum supported file size is 512 MB), or directly drag and drop your Manufacturer certificate into the upload area.

4. Click **Submit**. Once the configuration is completed, the Manufacturer certificate status will change to **Normal**.

> **INFO**
>
> Before creating a Model certificate based on the Google Cast specification, please ensure that at least one Manufacturer certificate based on the Google Cast specification has been created so that it can be selected and inherited during configuration.

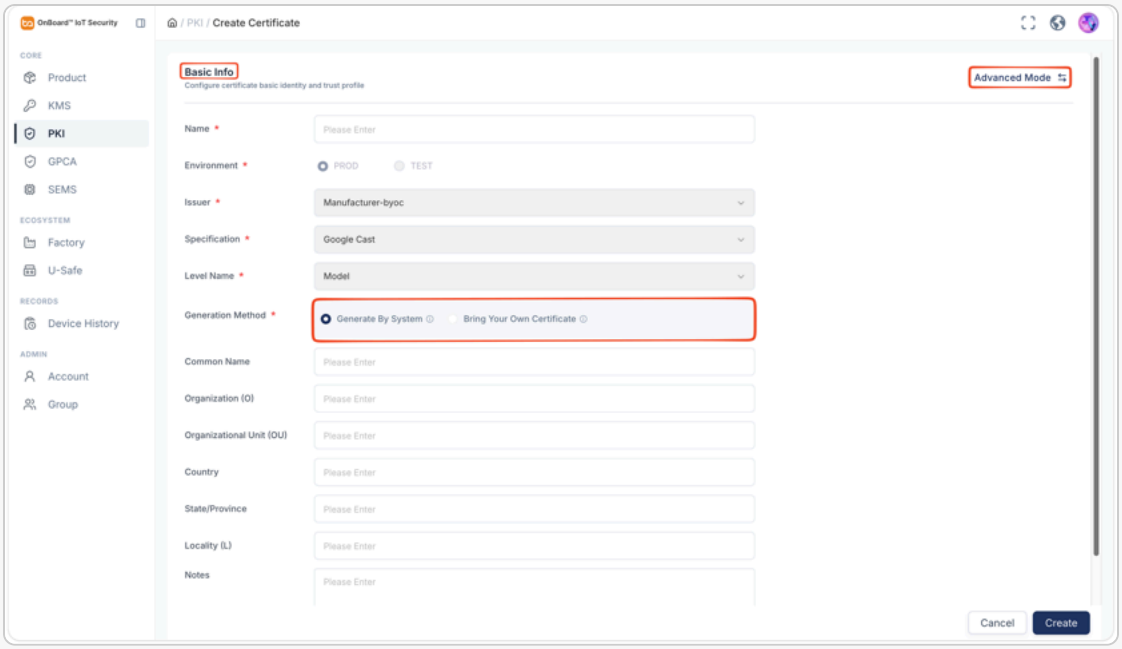
> **TIP**
>
> The default mode is simple mode, which requires only basic information. If you need to configure additional fields for the system-generated certificate, you can switch to advanced mode by clicking **Advanced Mode** in the top-right corner of the page.

1. On the **PKI** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding Manufacturer certificate and select **Add Model**.



2. On the **Basic Info** section, select and enter the basic information.

    - If the issuer of the Model certificate is your own Manufacturer certificate, you can select **Generate by System** or **Bring Your Own Certificate** as needed

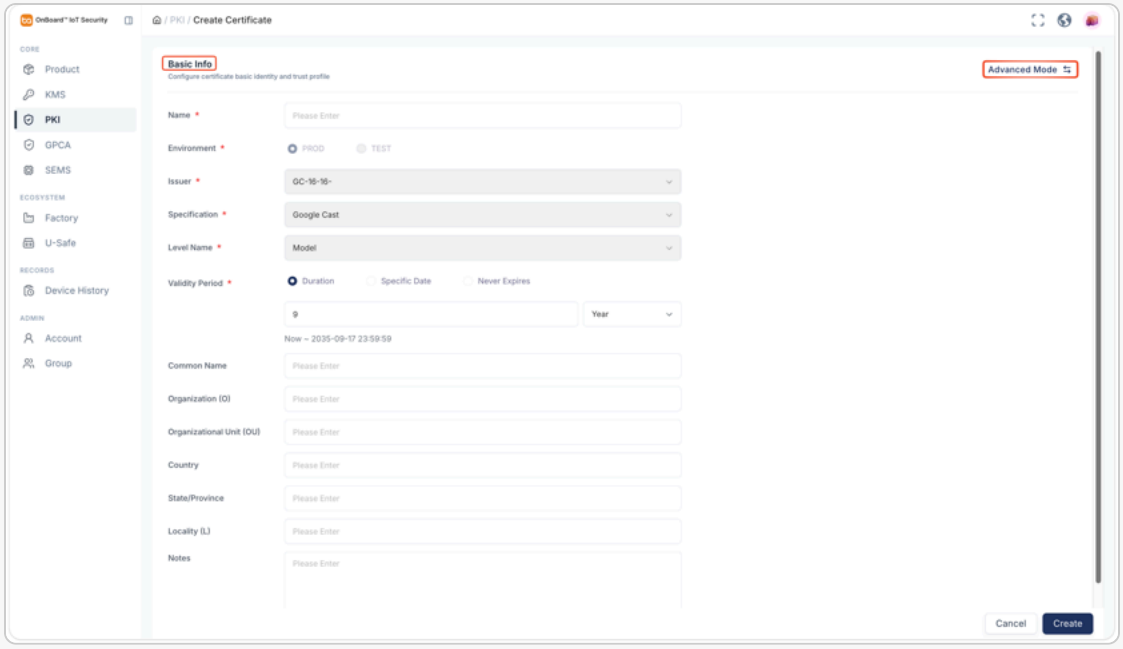


Information	Generate by System	Bring Your Own Certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Environment	The environment is inherited from the Manufacturer certificate.	
Issuer	The inherited Manufacturer certificate.	
Specification	Default is **Google Cast**.	
Level Name	Default is **Model**.	

Information	Generate by System	Bring Your Own Certificate
Generation Method	No file upload is required.	Click the Add + icon to select and upload a Model certificate in **.pem** format, or directly drag your own Model certificate into the upload area.
Common Name	Name of certificate holder.	N/A
Organization (O)	Organizational name.	N/A
Organizational Unit (OU)	Organizational unit name.	N/A
Country	Two ISO country codes.	N/A
State / Province	State or province name.	N/A
Locality (L)	City name.	N/A

Information	Generate by System	Bring Your Own Certificate
Notes	Provide additional information related to the Model certificate, such as special requirements and important notes.	

- If the issuer of the Model certificate the system-generated Manufacturer certificate

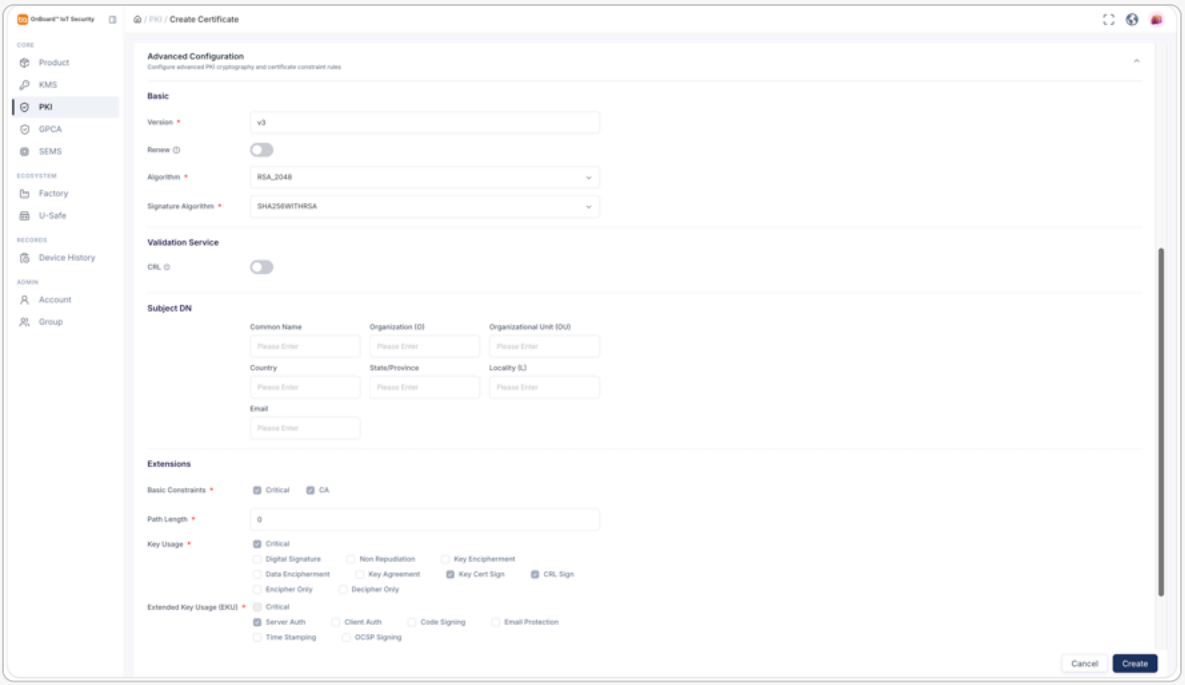


Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.

Information	Description
Environment	The environment is inherited from the Manufacturer certificate.
Issuer	The inherited Manufacturer certificate.
Specification	Default is **Google Cast**.
Level Name	Default is **Model**.
Validity Period	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed. Setting an expiration date beyond that of the inherited certificate may result in certificate chain validation failures, client trust issues, and audit risks.
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.

Information	Description
Locality (L)	City name.
Notes	Provide additional information related to the Model certificate, such as special requirements and important notes.

The configuration of advanced mode



- Description of Basic information:

Information	Description
Version	The standard version and can't be modified.
Renew	When enabled, certificates can be renewed. The existing public key is retained, and a new certificate is issued with an extended validity period.
Algorithm	Automatically parsed from the certificate content and can't be modified.
Signature Algorithm	Automatically parsed from the certificate content and can't be modified.

- Description of Validation Service information:

Information	Description
CRL	Automatically parsed from the certificate content, you can set the **Full Update Period**.

- Description of Subject DN information:

> **TIP**
>
> At least one Subject DN information must be provided.

Information	Description
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.

- Description of Extensions information:

> **TIP**
>
> If the **Critical** checkbox for a certain item is selected, the system must recognize and support that item when processing the certificate; otherwise, the certificate will be rejected.

Information	Description
Basic Constraints	Confirm if it is a CA certificate.
Path Length	Limits the number of sub-certificates.
Key Usage	Optional key usages, such as **Digital Signature**, **Key Cert Sign**, and **CRL Sign**.
Extended Key Usage (EKU)	Optional extended key usages, such as **Server Auth**, **Client Auth**, and **Code Signing**.

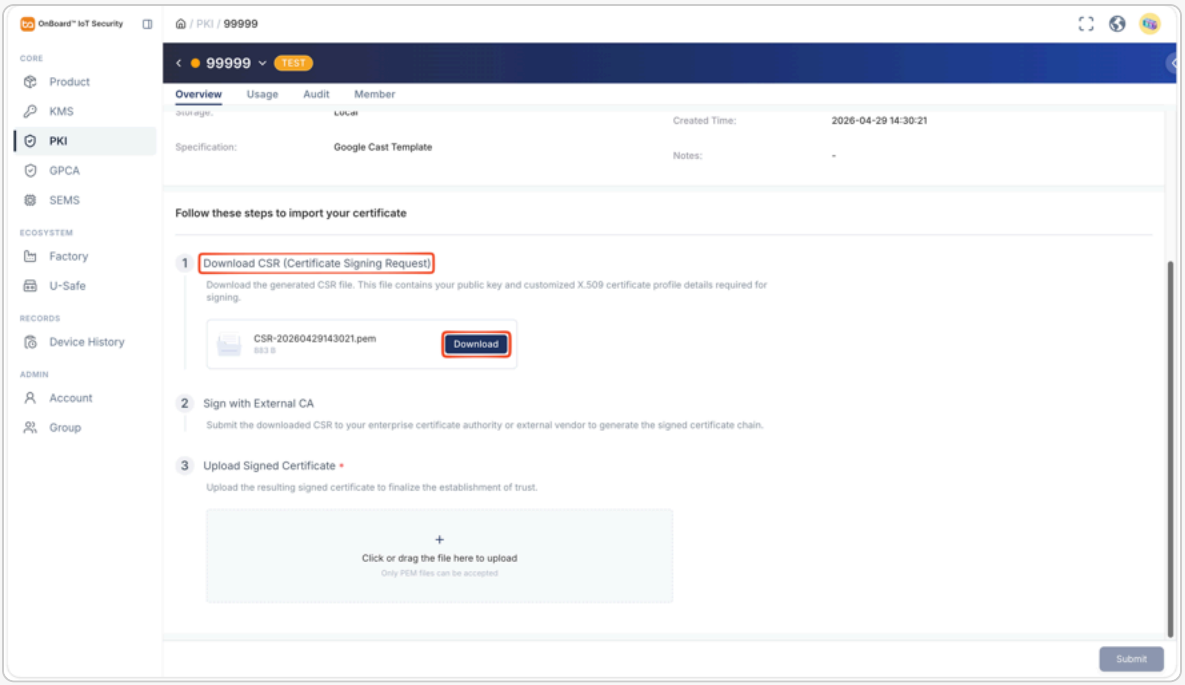
3. After verifying that the information is correct, click **Create** to complete the Model certificate creation.

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating a Model certificate, if the issuer is your own Manufacturer certificate, you must complete the CSR (Certificate Signing Request) configuration for the Model certificate. Before the CSR configuration is completed, the certificate will remain in the **Pending** status and can't be used.

CSR configuration steps for the Model certificate

> **TIP**
>
> When creating a Model certificate, if the issuer is your own Manufacturer certificate, refer to the following steps to complete the CSR configuration.

1. On the **PKI** page, expand the corresponding certificate chain, and then click the corresponding Model certificate.
2. Locate the **Download CSR (Certificate Signing Request)** section on the certificate page, click **Download** to download the CSR file. Then, use your Root CA to sign the file, thereby generate a Model certificate signed by the Root CA.



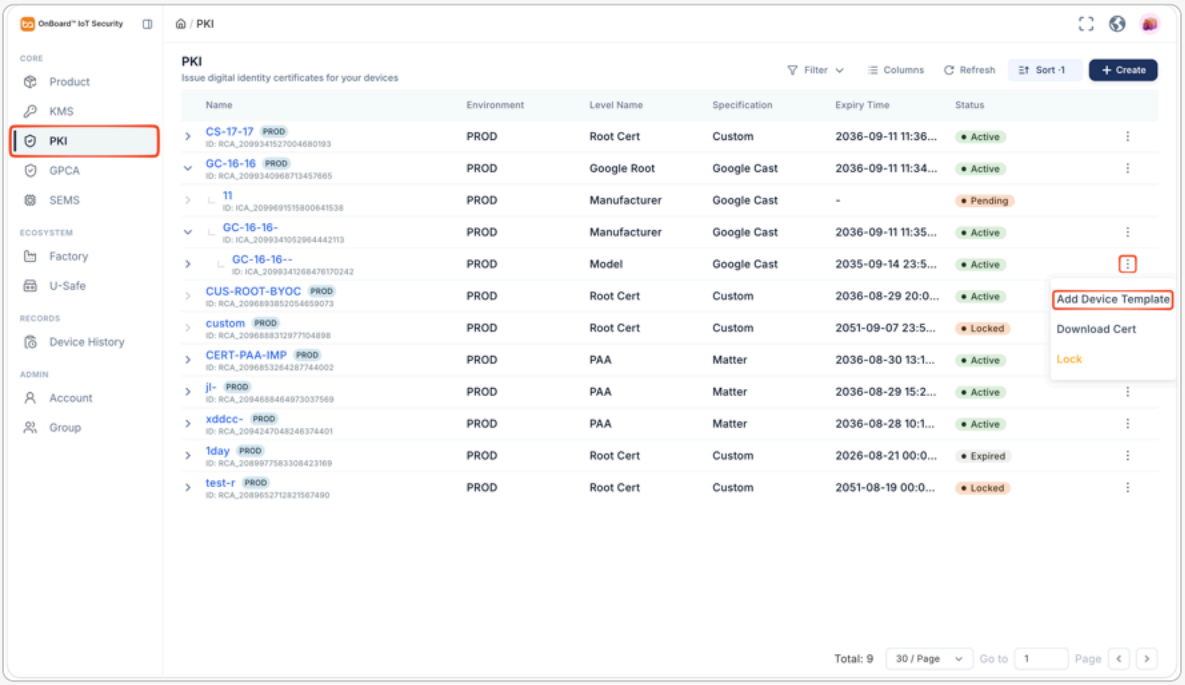
3. After a Model certificate is generated, click the Add + icon in the upload area, select and upload the Model certificate in **.pem** format (the maximum supported file size is 512 MB), or directly drag and drop your Model certificate into the upload area.

4. Click **Submit**. Once the configuration is completed, the Model certificate status will change to **Normal**.

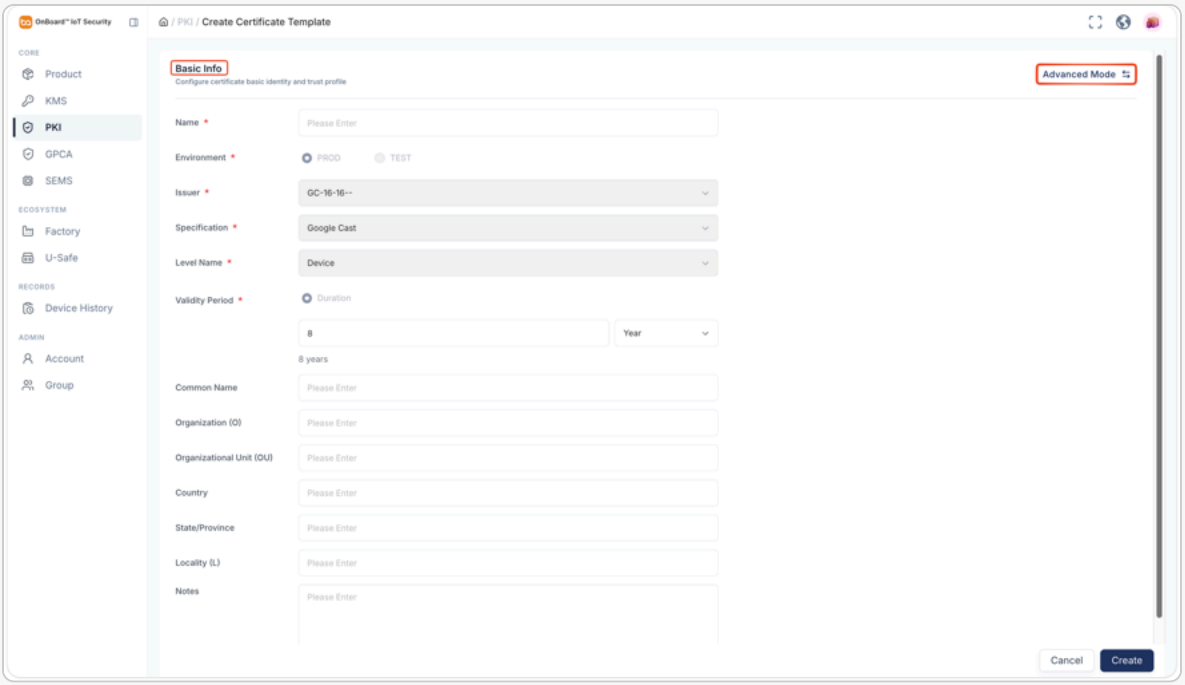
> **INFO**
>
> Before creating a Device template, please ensure that at least one Model certificate based on the Google Cast specification has been created so that it can be selected and inherited during configuration.

> **TIP**
>
> The default mode is simple mode, which requires only basic information. If you need to configure additional fields for the system-generated certificate, you can switch to advanced mode by clicking **Advanced Mode** in the top-right corner of the page.

1. On the **PKI** page, expand the corresponding certificate chain, then click the Options ⋮ icon for the corresponding Model certificate and select **Add Device Template**.



2. On the **Basic Info** section, select and enter the basic information.

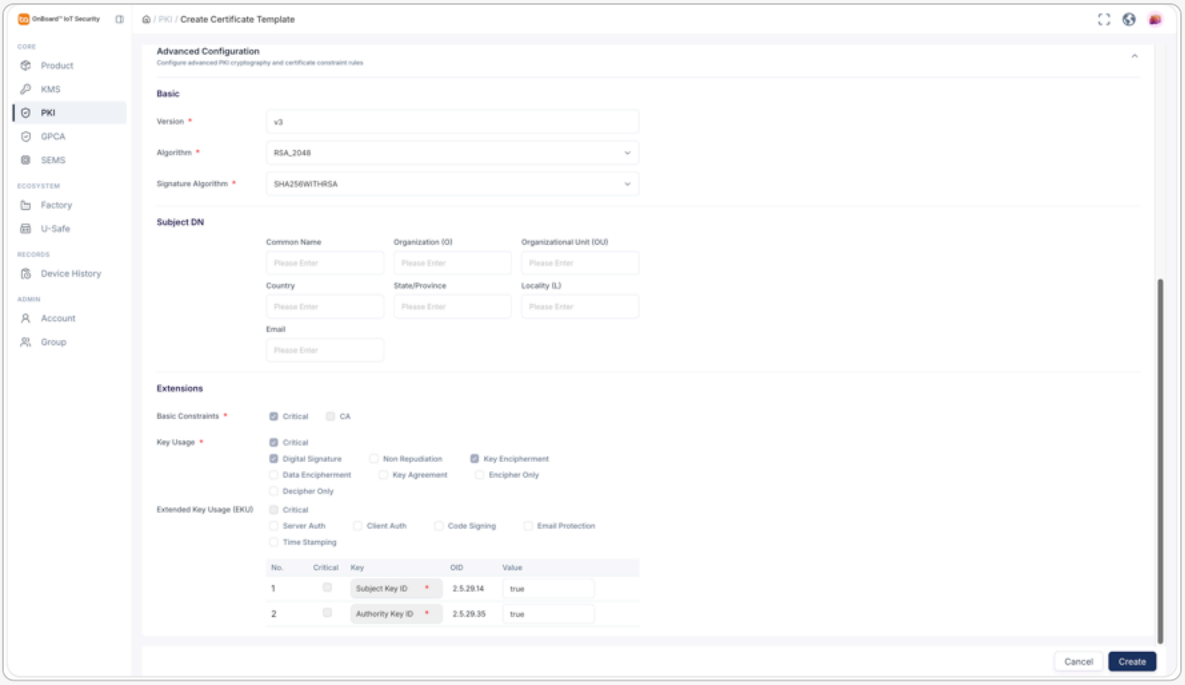


Description of Device template basic information:

Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Environment	The environment is inherited from the Model certificate.
Issuer	The inherited Model certificate.
Specification	Default is **Google Cast**.
Level Name	Default is **Device**.

Information	Description
Validity Period	Set the validity period of the Device template. Setting an expiration date beyond that of the inherited certificate may result in certificate chain validation failures, client trust issues, and audit risks.
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Notes	Provide additional information related to the Device template, such as special requirements and important notes.

The configuration of advanced mode



- Description of Basic information:

Information	Description
Version	The standard version and can't be modified.
Algorithm	Automatically parsed from the certificate content and can't be modified.
Signature Algorithm	Automatically parsed from the certificate content and can't be modified.

- Description of Subject DN information:

> **TIP**
>
> At least one Subject DN information must be provided.

Information	Description
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.

- Description of Extensions information:

> **TIP**
>
> If the **Critical** checkbox for a certain item is selected, the system must recognize and support that item when processing the certificate; otherwise, the certificate will be rejected.

Information	Description
Basic Constraints	Confirm if it is a CA certificate.
Key Usage	Optional key usages, such as **Digital Signature**.

Information	Description
Extended Key Usage (EKU)	Optional extended key usages, such as **Server Auth**, **Client Auth**, and **Code Signing**.

3. After verifying that the information is correct, click **Create** to complete the Device template creation.

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

Version: v3.4.0 (Latest)

How to create a certificate based on the Custom specification in OnBoard™ IoT Security

This article will guide you on how to create a certificate based on the Custom specification in OnBoard™ IoT Security (OBIS).

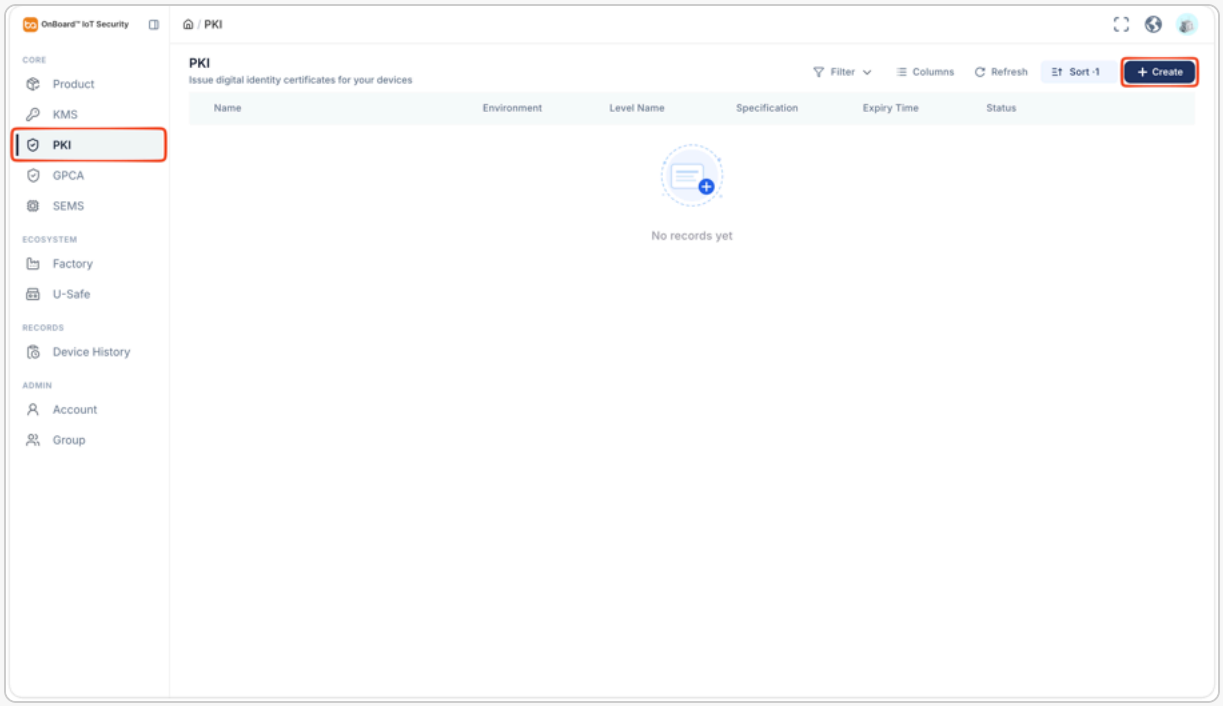
Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager or Resource Manager.

Instructions

> **TIP**
>
> After a custom certificate template is created, it can be selected when configuring Certificates for a product.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **PKI**, and then click **Create** on the **PKI** page.



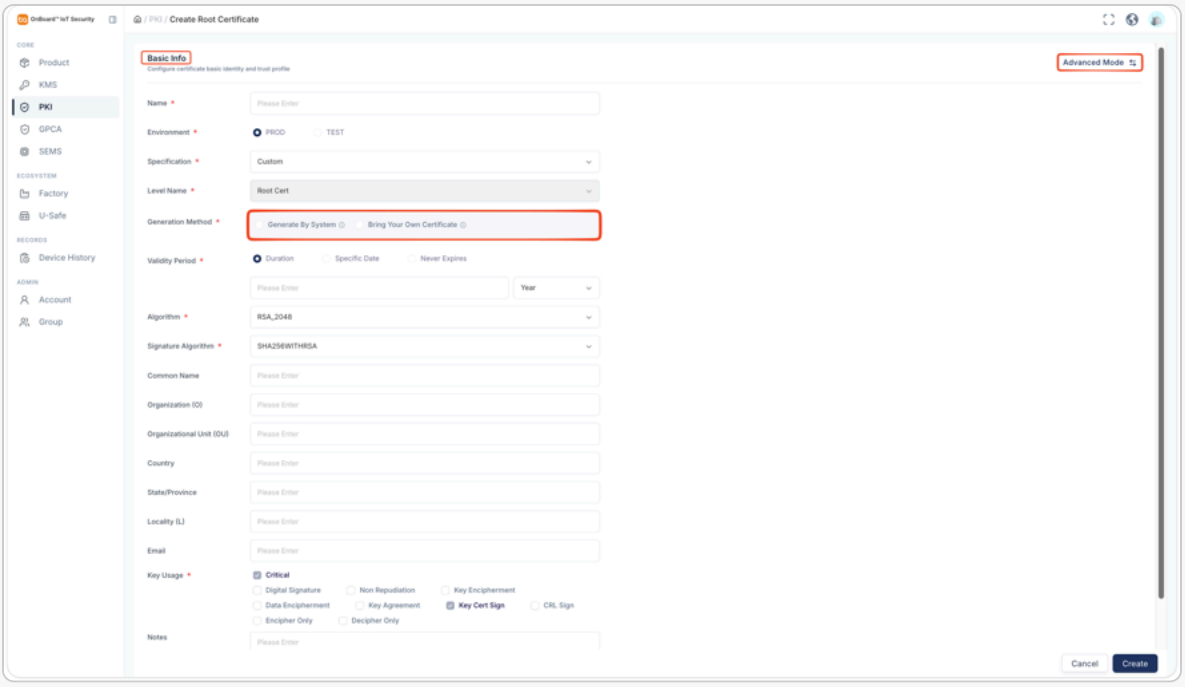
Create a root certificate | Create an intermediate certificate

Create an end entity template

TIP

The default mode is simple mode, which requires only basic information. If you need to configure additional fields for the system-generated certificate, you can switch to advanced mode by clicking **Advanced Mode** in the top-right corner of the page.

1. On the **Basic Info** section, select **Generate by System** or **Bring Your Own Certificate** as needed.



Description of root certificate basic information:

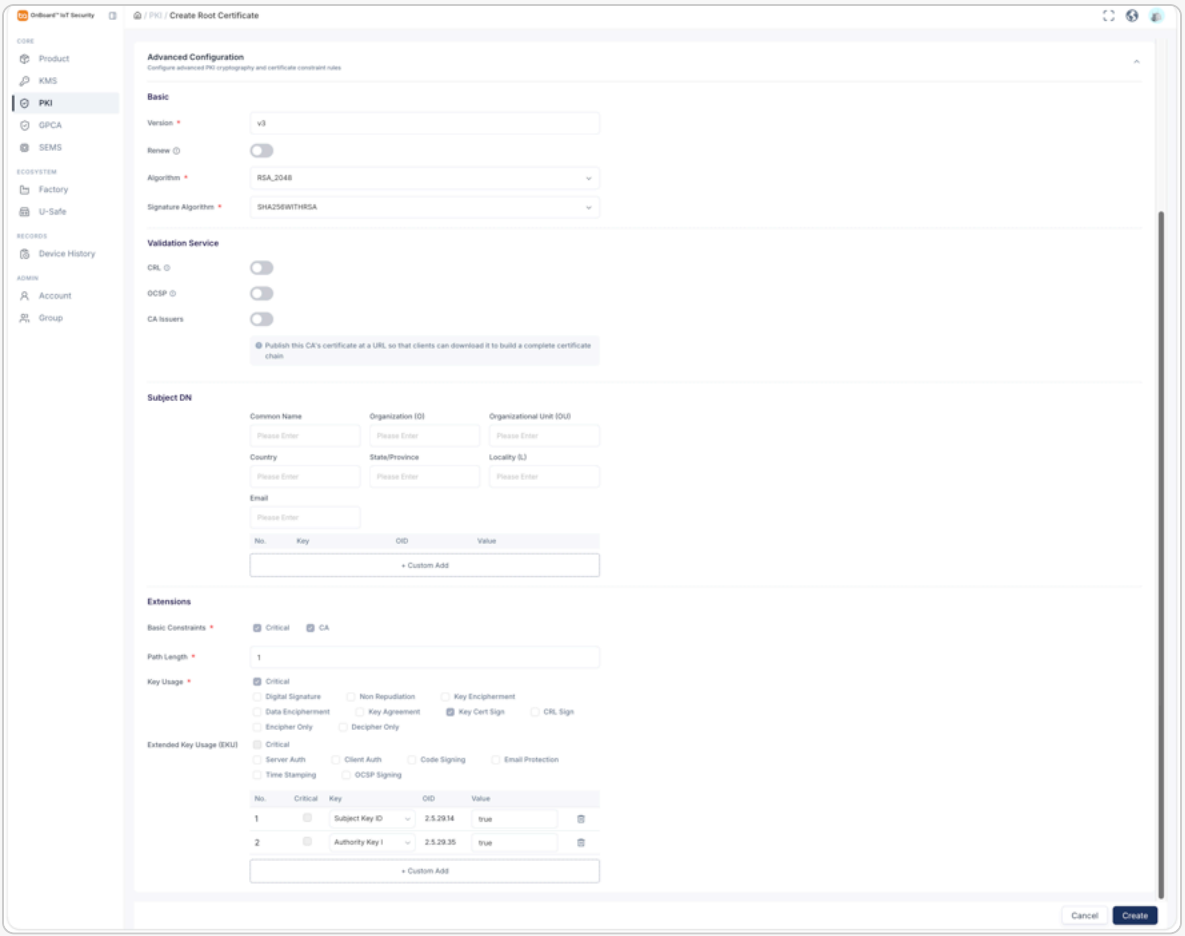
Information	Generate by System	Bring Your Own Certificate
Name	The root certificate name must be unique in the same environment.	
Environment	Two environments can be selected: **TEST** and **PROD**.	
Specification	Select the **Custom** specification.	
Level Name	Default is **Root Cert**.	

Information	Generate by System	Bring Your Own Certificate
Generation Method	No file upload is required.	Click the Add + icon to select and upload a root certificate in **.pem** format, or directly drag and drop your own root certificate into the upload area.
Validity Period	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.	N/A
Algorithm	Available algorithms for the certificates. Options include: ◦ **RSA_2048** ◦ **RSA_3072** ◦ **RSA_4096** ◦ **ECC_P384** ◦ **ECC_P256** ◦ **ECC_P521**	N/A

Information	Generate by System	Bring Your Own Certificate
Signature Algorithm	Signature algorithms for the certificates. Options include: ◦ **SHA256WITHRSA** ◦ **SHA384WITHRSA** ◦ **SHA512WITHRSA** ◦ **SHA256WITHECDSA** ◦ **SHA256WITHECDSA**	N/A
Common Name	Name of certificate holder.	N/A
Organization (O)	Organizational name.	N/A
Organizational Unit (OU)	Organizational unit name.	N/A
Country	Two ISO country codes.	N/A
State / Province	State or province name.	N/A
Locality (L)	City name.	N/A
Email	User email.	N/A

Information	Generate by System	Bring Your Own Certificate
Key Usage	Optional key usages, such as **Digital Signature**, **Non Repudiation**, and **Key Encipherment**.	N/A
Notes	Provide additional information related to the root certificate, such as special requirements and important notes.	

The configuration of advanced mode



- Description of Basic information:

Information	Description
Version	The standard version and can't be modified.
Renew	When enabled, certificates can be renewed. The existing public key is retained, and a new certificate is issued with an extended validity period.

Information	Description
Algorithm	Available algorithms for the certificates. Options include: ▪ **RSA_2048** ▪ **RSA_3072** ▪ **RSA_4096** ▪ **ECC_P384** ▪ **ECC_P256** ▪ **ECC_P521**
Signature Algorithm	Signature algorithms for the certificates. Options include: ▪ **SHA256WITHRSA** ▪ **SHA384WITHRSA** ▪ **SHA512WITHRSA** ▪ **SHA256WITHECDSA** ▪ **SHA256WITHECDSA**

- Description of Validation Service information:

Information	Description
CRL	Automatically parsed from the certificate content, you can set the **Full Update Period**, **Delta Update Period**, and **Overlap Time**.

Information	Description
OSCP	Automatically parsed from the certificate content, you can set the **Response Validity** and **Nonce**.
CA Issuers	When enabled, the issuing CA certificate download service will be provided.

- Description of Subject DN information:

> **TIP**
>
> At least one Subject DN information must be provided.

Information	Description
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.

Information	Description
Custom Add	Custom OIDs can be added.

- Description of Extensions information:

> **TIP**
>
> If the **Critical** checkbox for a certain item is selected, the system must recognize and support that item when processing the certificate; otherwise, the certificate will be rejected.

Information	Description
Basic Constraints	Confirm if it is a CA certificate.
Path Length	Limits the number of sub-certificates.
Key Usage	Optional key usages, such as **Digital Signature**, **Key Cert Sign**, and **CRL Sign**.
Extended Key Usage (EKU)	Optional extended key usages, such as **Server Auth**, **Client Auth**, and **Code Signing**.

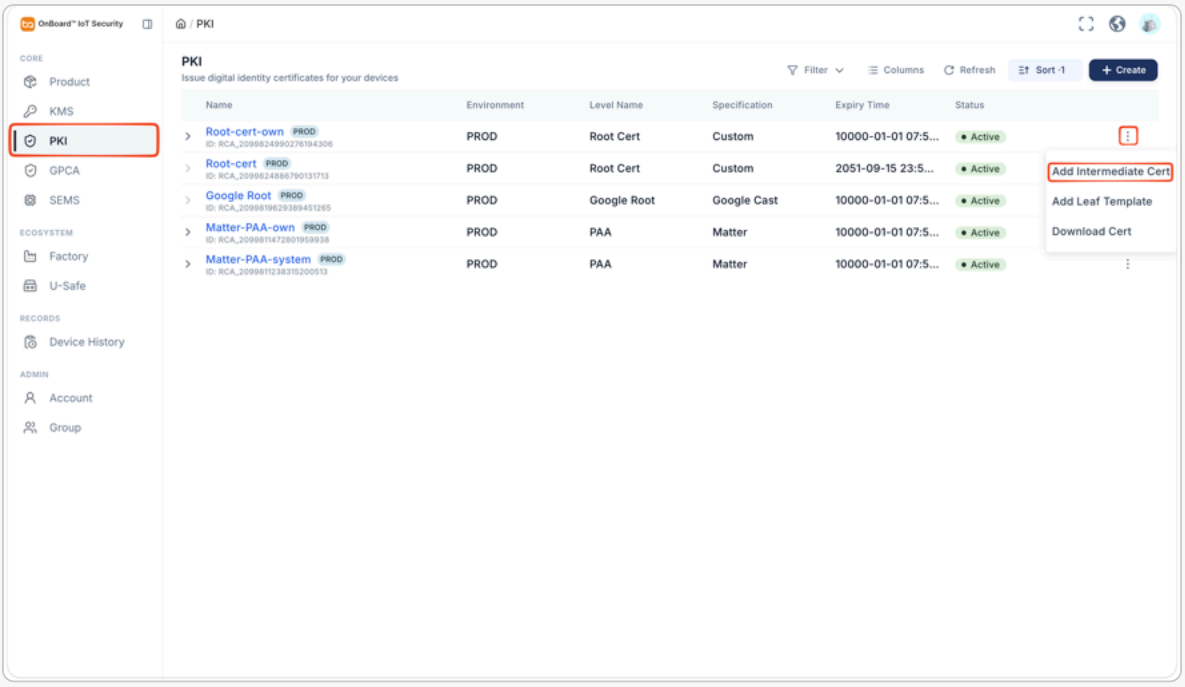
2. After verifying that the information is correct, click **Create** to complete the root certificate creation.

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

> **INFO**
>
> Before creating an intermediate certificate, please ensure that at least one root certificate has been created so that it can be selected and inherited during configuration.

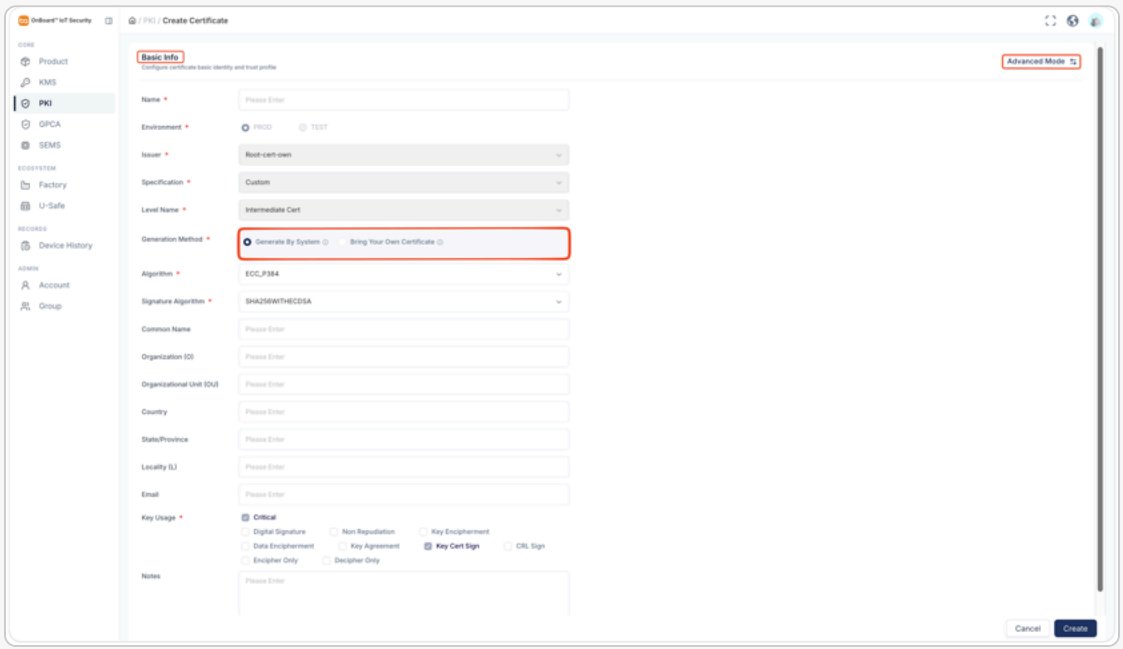
> **TIP**
>
> The default mode is simple mode, which requires only basic information. If you need to configure additional fields for the system-generated certificate, you can switch to advanced mode by clicking **Advanced Mode** in the top-right corner of the page.

1. On the **PKI** page, click the Options ⋮ icon for the corresponding root certificate and select **Add Intermediate Cert**.



2. On the **Basic Info** section, select and enter the basic information.

    - If the issuer of the intermediate certificate your own root certificate, you can select **Generate by System** or **Bring Your Own Certificate** as needed

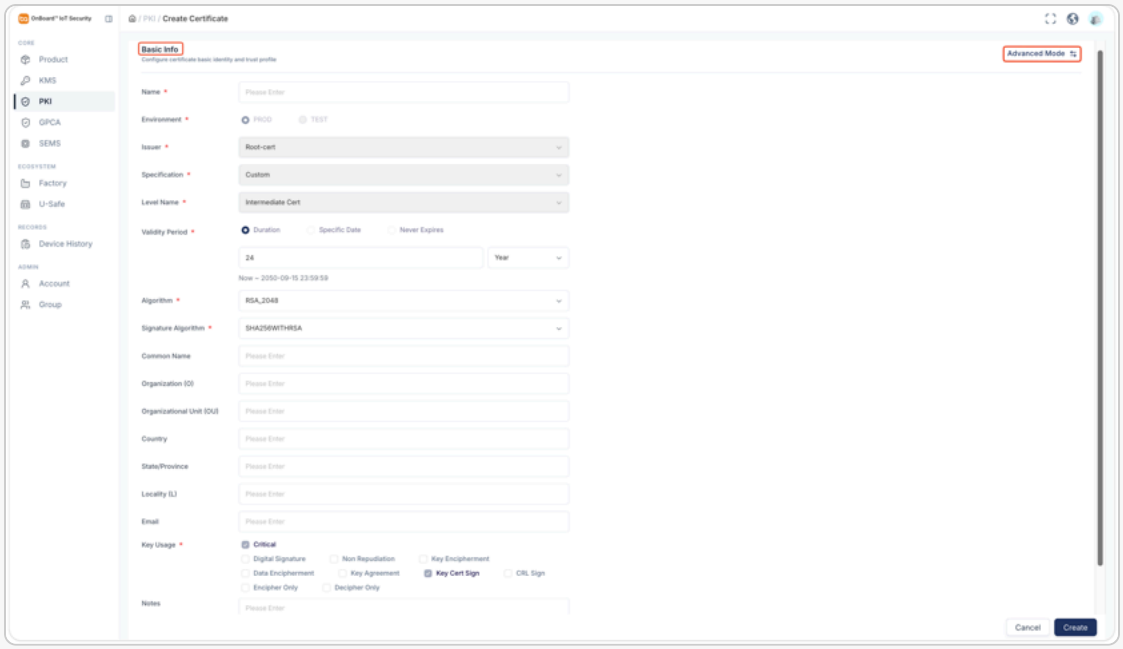


Information	Generate by System	Bring Your Own Certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Environment	The environment is inherited from the root certificate.	
Issuer	The inherited root certificate.	
Specification	Default is **Custom**.	
Level Name	Default is **Sub Cert**.	
Generation Method	No file upload is required.	Click the Add + icon to select and upload a intermediate certificate in **.pem** format, or directly drag your own intermediate certificate into the upload area.

Information	Generate by System	Bring Your Own Certificate
Algorithm	Available algorithms for the certificates. Options include: ▪ **RSA_2048** ▪ **RSA_3072** ▪ **RSA_4096** ▪ **ECC_P384** ▪ **ECC_P256** ▪ **ECC_P521**	N/A
Signature Algorithm	Signature algorithms for the certificates. Options include: ▪ **SHA256WITHRSA** ▪ **SHA384WITHRSA** ▪ **SHA512WITHRSA** ▪ **SHA256WITHECDSA** ▪ **SHA256WITHECDSA**	N/A
Common Name	Name of certificate holder.	N/A
Organization (O)	Organizational name.	N/A

Information	Generate by System	Bring Your Own Certificate
Organizational Unit (OU)	Organizational unit name.	N/A
Country	Two ISO country codes.	N/A
State / Province	State or province name.	N/A
Locality (L)	City name.	N/A
Email	User email.	N/A
Key Usage	Optional key usages, such as **Digital Signature**, **Non Repudiation**, and **Key Encipherment**.	N/A
Notes	Provide additional information related to the intermediate certificate, such as special requirements and important notes.	

- If the issuer of the intermediate certificate is the system-generated root certificate

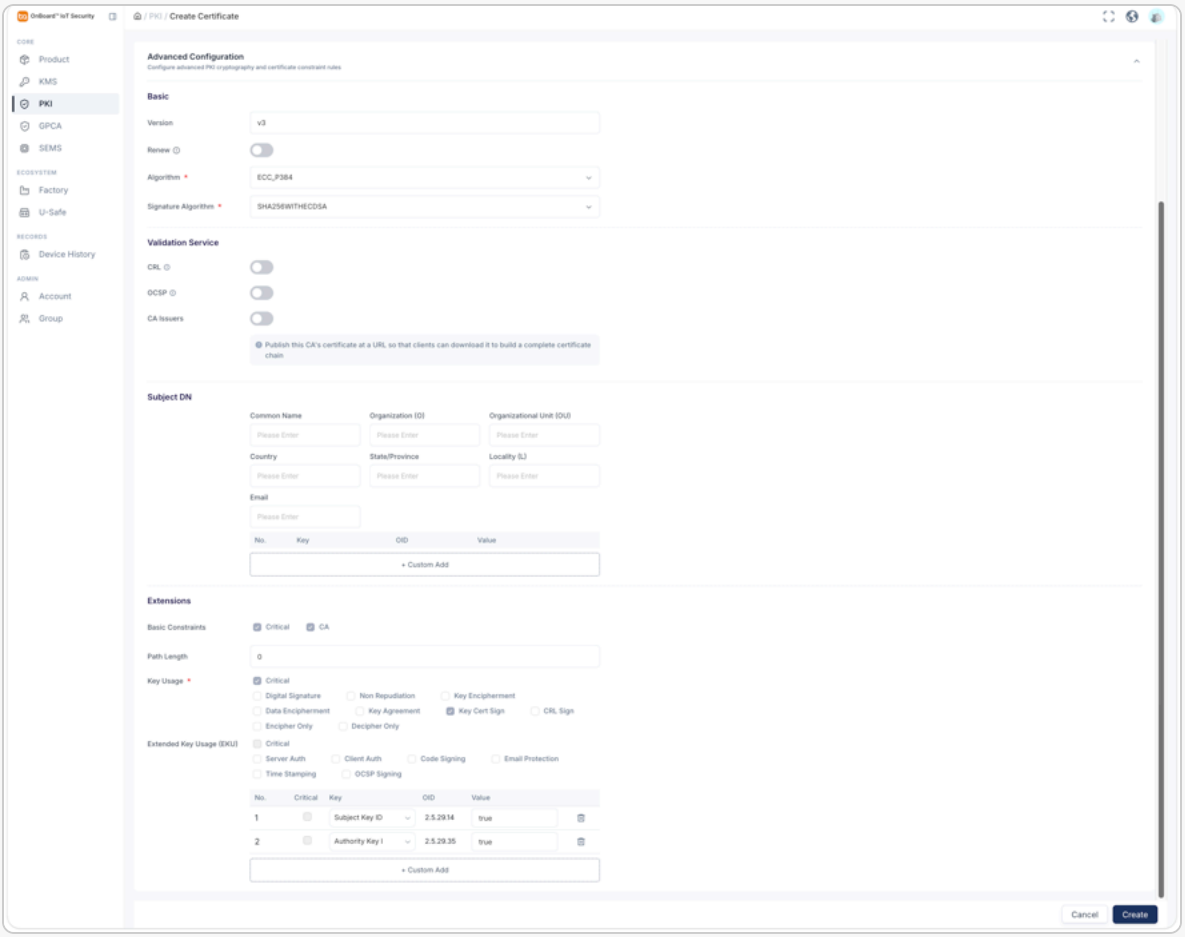


Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Environment	The environment is inherited from the root certificate.
Issuer	The inherited root certificate.
Specification	Default is **Custom**.
Level Name	Default is **Sub Cert**.

Information	Description
Validity Period	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed. Setting an expiration date beyond that of the inherited certificate may result in certificate chain validation failures, client trust issues, and audit risks.
Algorithm	Available algorithms for the certificates. Options include: ▪ **RSA_2048** ▪ **RSA_3072** ▪ **RSA_4096** ▪ **ECC_P384** ▪ **ECC_P256** ▪ **ECC_P521**
Signature Algorithm	Signature algorithms for the certificates. Options include: ▪ **SHA256WITHRSA** ▪ **SHA384WITHRSA** ▪ **SHA512WITHRSA** ▪ **SHA256WITHECDSA** ▪ **SHA256WITHECDSA**
Common Name	Name of certificate holder.

Information	Description
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.
Key Usage	Optional key usages, such as **Digital Signature**, **Non Repudiation**, and **Key Encipherment**.
Notes	Provide additional information related to the intermediate certificate, such as special requirements and important notes.

The configuration of advanced mode



- Description of Basic information:

Information	Description
Version	The standard version and can't be modified.
Renew	When enabled, certificates can be renewed. The existing public key is retained, and a new certificate is issued with an extended validity period.

Information	Description
Algorithm	Available algorithms for the certificates. Options include: ▪ **RSA_2048** ▪ **RSA_3072** ▪ **RSA_4096** ▪ **ECC_P384** ▪ **ECC_P256** ▪ **ECC_P521**
Signature Algorithm	Signature algorithms for the certificates. Options include: ▪ **SHA256WITHRSA** ▪ **SHA384WITHRSA** ▪ **SHA512WITHRSA** ▪ **SHA256WITHECDSA** ▪ **SHA256WITHECDSA**

- Description of Validation Service information:

Information	Description
CRL	Automatically parsed from the certificate content, you can set the **Full Update Period**, **Delta Update Period**, and **Overlap Time**.

Information	Description
OSCP	Automatically parsed from the certificate content, you can set the **Response Validity** and **Nonce**.
CA Issuers	When enabled, the issuing CA certificate download service will be provided.

- Description of Subject DN information:

> **TIP**
>
> At least one Subject DN information must be provided.

Information	Description
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.

Information	Description
Custom Add	Custom OIDs can be added.

- Description of Extensions information:

> **TIP**
>
> If the **Critical** checkbox for a certain item is selected, the system must recognize and support that item when processing the certificate; otherwise, the certificate will be rejected.

Information	Description
Basic Constraints	Confirm if it is a CA certificate.
Path Length	Limits the number of sub-certificates.
Key Usage	Optional key usages, such as **Digital Signature**, **Key Cert Sign**, and **CRL Sign**.
Extended Key Usage (EKU)	Optional extended key usages, such as **Server Auth**, **Client Auth**, and **Code Signing**.

3. After verifying that the information is correct, click **Create** to complete the intermediate certificate creation.

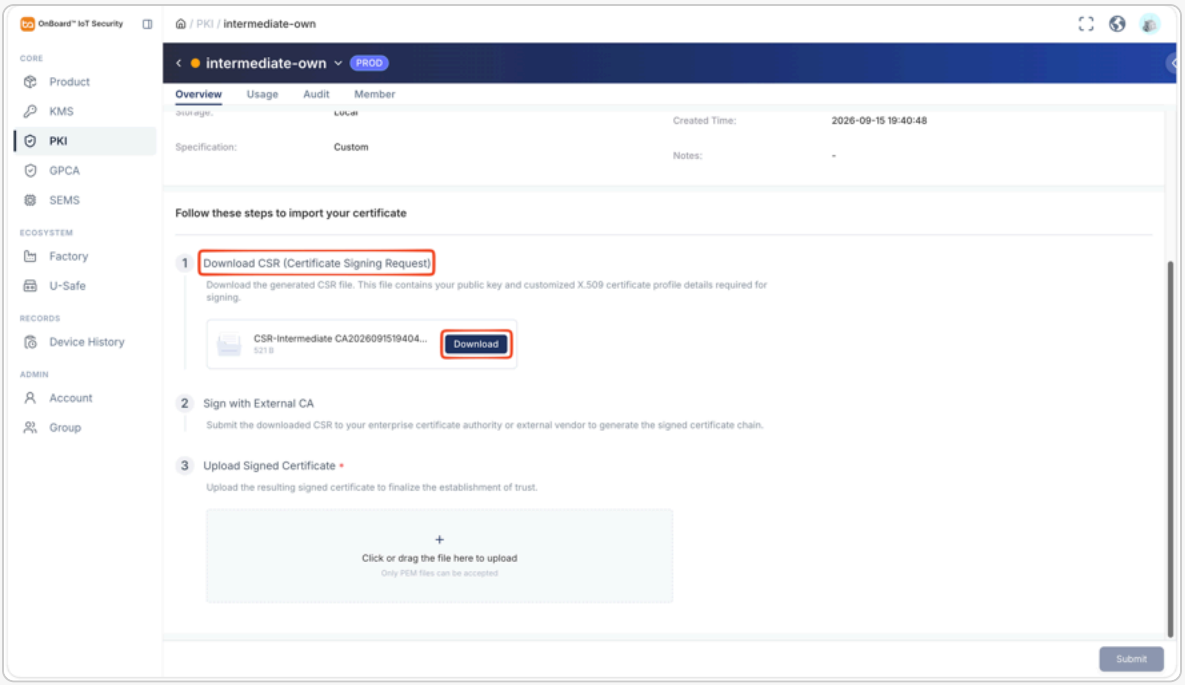
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an intermediate certificate, if the issuer is your own root certificate, you must complete the CSR (Certificate Signing Request) configuration for the intermediate certificate. Before the CSR configuration is completed, the certificate will remain in the **Pending** status and can't be used.

CSR configuration steps for the intermediate certificate

> **TIP**
>
> When creating an intermediate certificate, if the issuer is your own root certificate, refer to the following steps to complete the CSR configuration.

1. On the **PKI** page, expand the corresponding certificate chain, and then click the corresponding intermediate certificate.

2. Locate the **Download CSR (Certificate Signing Request)** section on the certificate page, click **Download** to download the CSR file. Then, use your Root CA to sign the file, thereby generating an intermediate certificate signed by the Root CA.



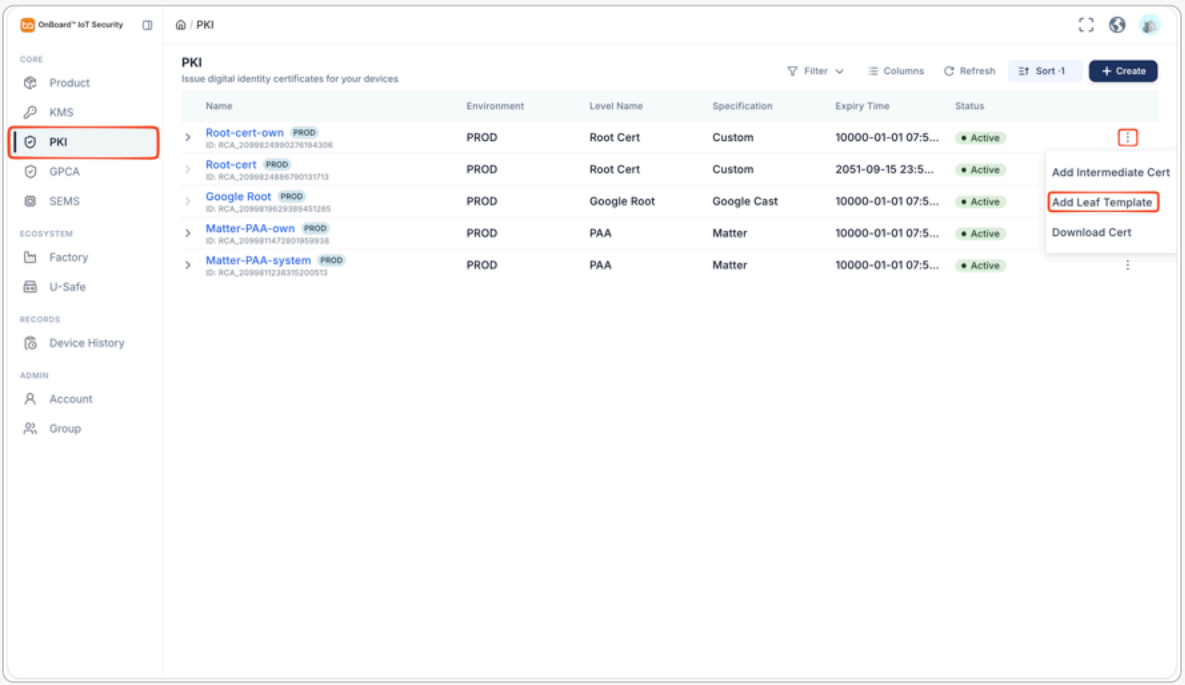
3. After an intermediate certificate is generated, click the Add + icon in the upload area, select and upload the intermediate certificate in **.pem** format (the maximum supported file size is 512 MB), or directly drag and drop your intermediate certificate into the upload area.

4. Click **Submit**. Once the configuration is completed, the intermediate certificate status will change to **Normal**.

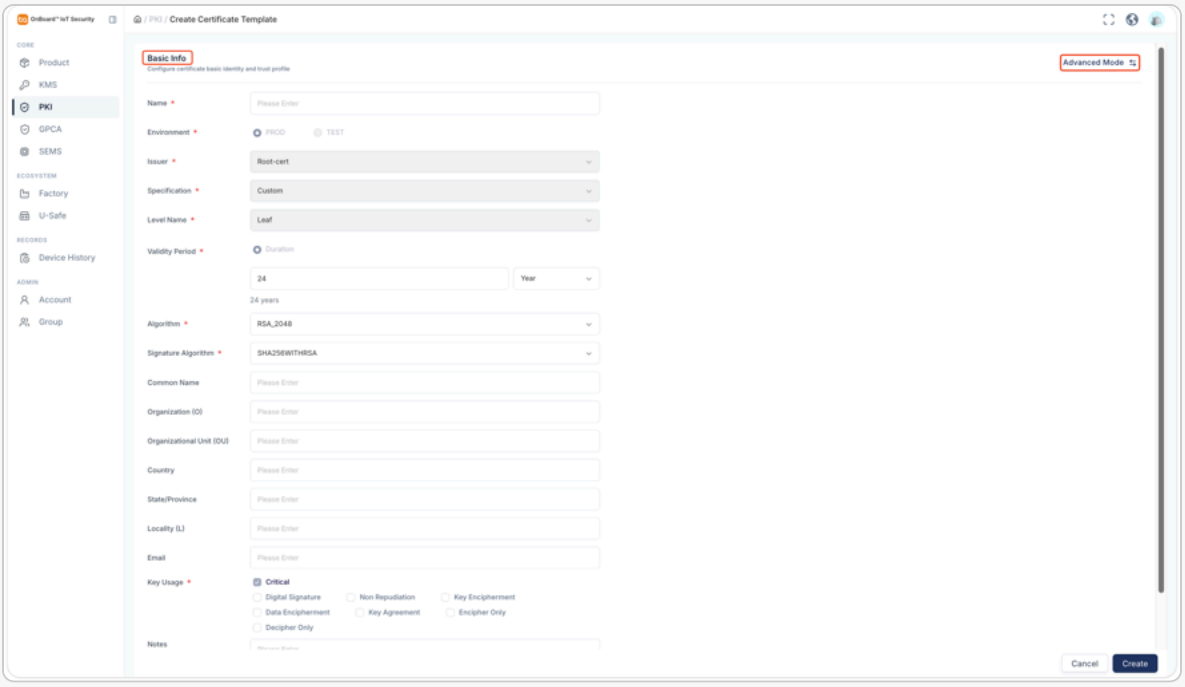
> **INFO**
>
> Before creating an end entity template, please ensure that at least one root certificate or intermediate certificate has been created so that it can be selected and inherited during configuration.

> **TIP**
>
> The default mode is simple mode, which requires only basic information. If you need to configure additional fields for the system-generated certificate, you can switch to advanced mode by clicking **Advanced Mode** in the top-right corner of the page.

1. On the **PKI** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding root or intermediate certificate and select **Add Leaf Template**.



2. On the **Basic Info** section, select and enter the basic information.



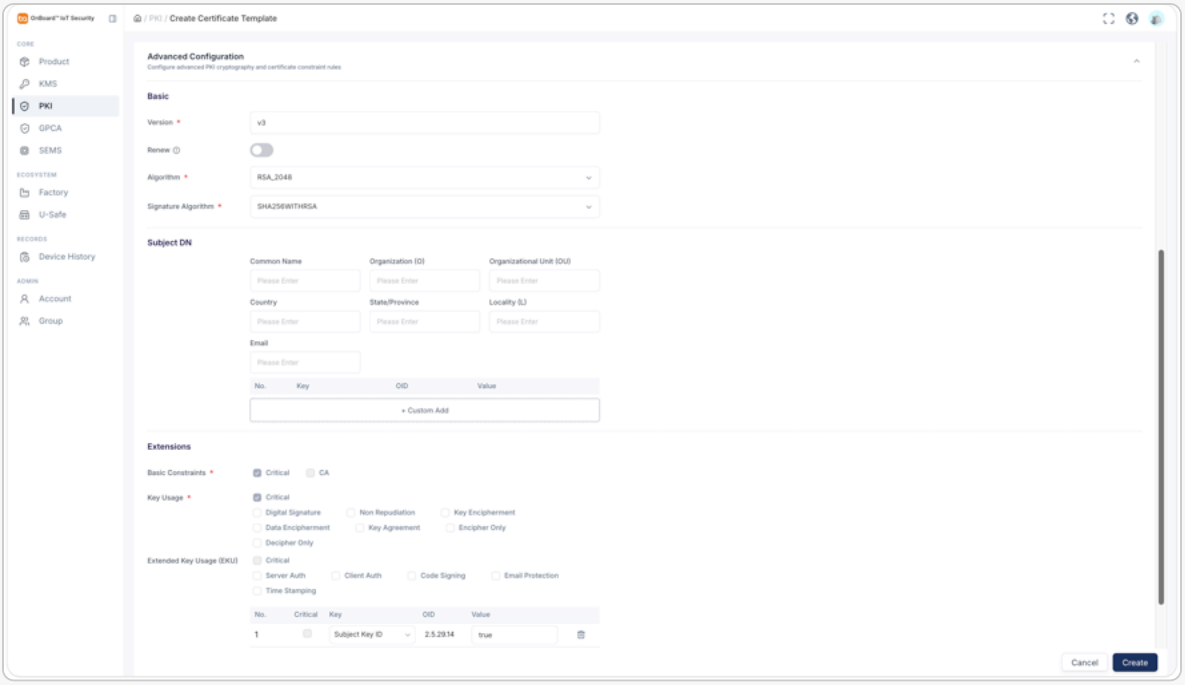
Description of end entity template basic information:

Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Environment	The environment is inherited from the root or intermediate certificate.
Issuer	The inherited root or intermediate certificate.
Specification	Default is **Custom**.
Level Name	Default is **Leaf Cert**.

Information	Description
Validity Period	Set the validity period of the end entity template. Setting an expiration date beyond that of the inherited certificate may result in certificate chain validation failures, client trust issues, and audit risks. **Note**: If the issuer is inherited from your own root or intermediate certificate, the validity period will be inherited from the root or intermediate certificate.
Algorithm	Available algorithms for the certificates. Options include: ◦ **RSA_2048** ◦ **RSA_3072** ◦ **RSA_4096** ◦ **ECC_P384** ◦ **ECC_P256** ◦ **ECC_P521**
Signature Algorithm	Signature algorithms for the certificates. Options include: ◦ **SHA256WITHRSA** ◦ **SHA384WITHRSA** ◦ **SHA512WITHRSA** ◦ **SHA256WITHECDSA** ◦ **SHA256WITHECDSA**

Information	Description
Common Name	Name of certificate holder.
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.
Key Usage	Optional key usages, such as **Digital Signature**, **Non Repudiation**, and **Key Encipherment**.
Notes	Provide additional information related to the end entity certificate, such as special requirements and important notes.

The configuration of advanced mode



- Description of Basic information:

Information	Description
Version	The standard version and can't be modified.
Renew	When enabled, certificates can be renewed. The existing public key is retained, and a new certificate is issued with an extended validity period.

Information	Description
Algorithm	Available algorithms for the certificates. Options include: ▪ **RSA_2048** ▪ **RSA_3072** ▪ **RSA_4096** ▪ **ECC_P384** ▪ **ECC_P256** ▪ **ECC_P521**
Signature Algorithm	Signature algorithms for the certificates. Options include: ▪ **SHA256WITHRSA** ▪ **SHA384WITHRSA** ▪ **SHA512WITHRSA** ▪ **SHA256WITHECDSA** ▪ **SHA256WITHECDSA**

- Description of Subject DN information:

> **TIP**
>
> At least one Subject DN information must be provided.

Information	Description
Common Name	Name of certificate holder.

Information	Description
Organization (O)	Organizational name.
Organizational Unit (OU)	Organizational unit name.
Country	Two ISO country codes.
State / Province	State or province name.
Locality (L)	City name.
Email	User email.
Custom Add	Custom OIDs can be added.

- Description of Extensions information:

> **TIP**
>
> If the **Critical** checkbox for a certain item is selected, the system must recognize and support that item when processing the certificate; otherwise, the certificate will be rejected.

Information	Description
Basic Constraints	Confirm if it is a CA certificate.
Key Usage	Optional key usages, such as **Digital Signature**, **Key Cert Sign**, and **CRL Sign**.

Information	Description
Extended Key Usage (EKU)	Optional extended key usages, such as **Server Auth**, **Client Auth**, and **Code Signing**.

3. After verifying that the information is correct, click **Create** to complete the end entity template creation.

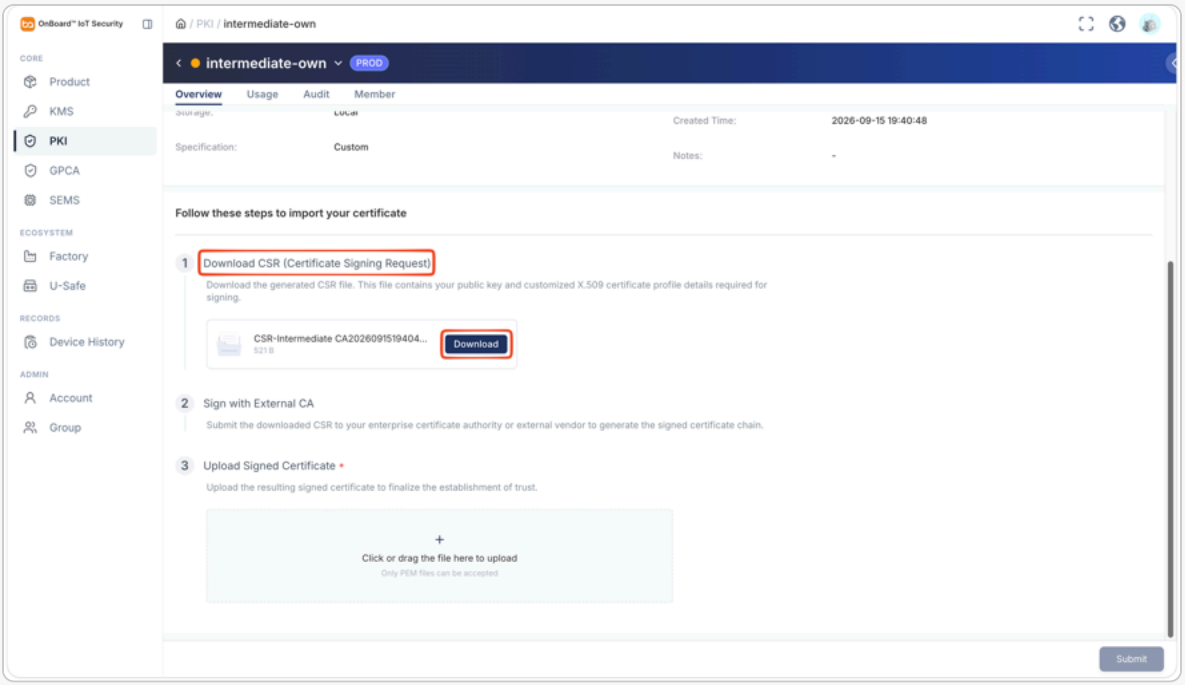
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an end entity template, if the issuer is your own root or intermediate certificate, you must complete the CSR (Certificate Signing Request) configuration for the end entity template. Before the CSR configuration is completed, the template will remain in the **Pending** status and can't be used.

CSR configuration steps for the end entity template

> **TIP**
>
> When creating an end entity template, if the issuer is your own root or intermediate certificate, refer to the following steps to complete the CSR configuration.

1. On the **PKI** page, expand the corresponding certificate chain, and then click the corresponding end entity template.

2. Locate the **Download CSR (Certificate Signing Request)** section on the certificate page, click **Download** to download the CSR file. Then, use your Root CA to sign the file, thereby generating an end entity template signed by the Root CA.



3. After an end entity template is generated, click the Add + icon in the upload area, select and upload the end entity template in **.pem** format (the maximum supported file size is 512 MB), or directly drag and drop your end entity template into the upload area.

4. Click **Submit**. Once the configuration is completed, the end entity template status will change to **Normal**.

Version: v3.4.0 (Latest)

How to check certificates in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Check basic information
- Check usage count
- Check verification service
- Check end-entity certificate
- Check audit
- Check members

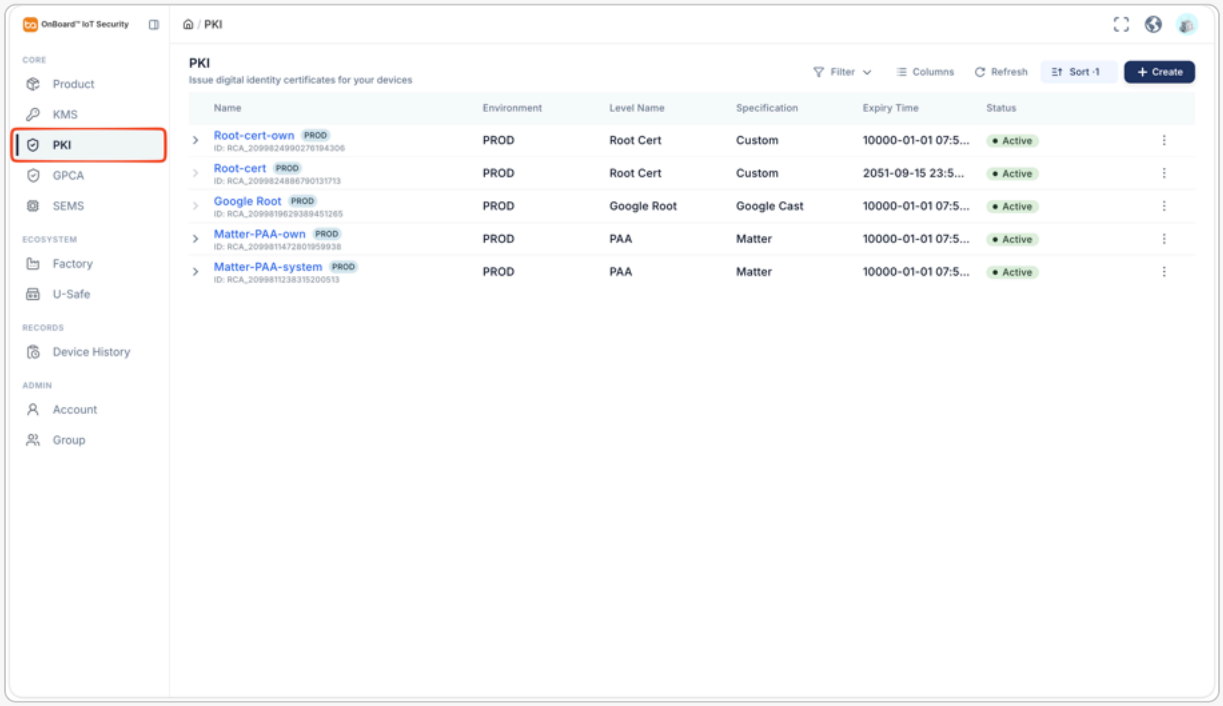
Prerequisites

Before getting started, please ensure that you have permissions for the corresponding certificate.

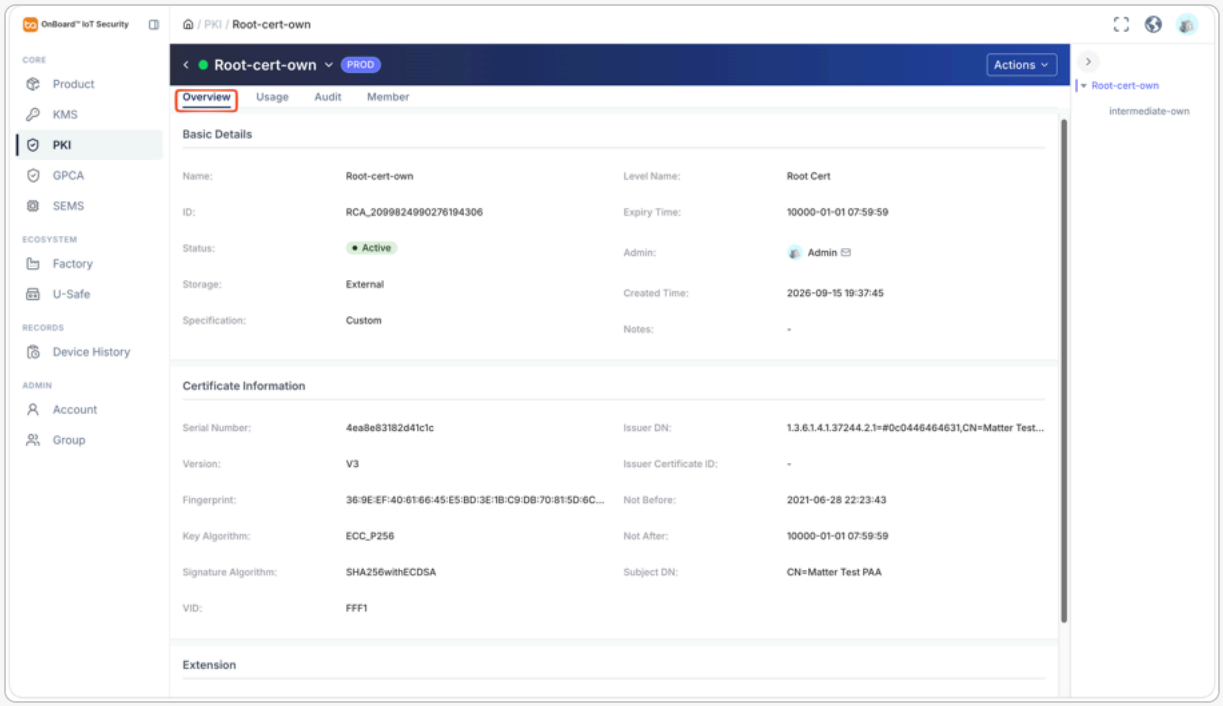
Check basic information

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then select the corresponding certificate.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



3. On the **Overview** tab, you can check the certificate-related information (**Basic Details**, **Certificate Information**, and **Extension**).

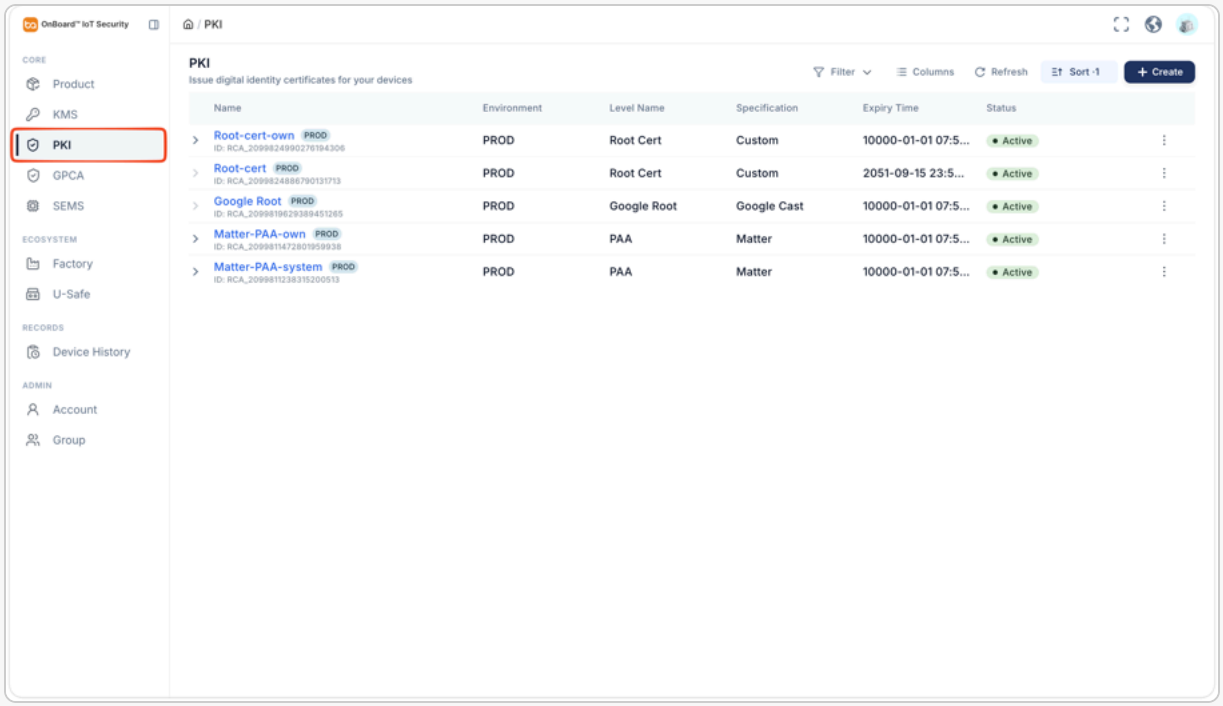


Check usage count

> **TIP**
>
> Certificate usage count can be used to check certificate dependencies and impact scope.

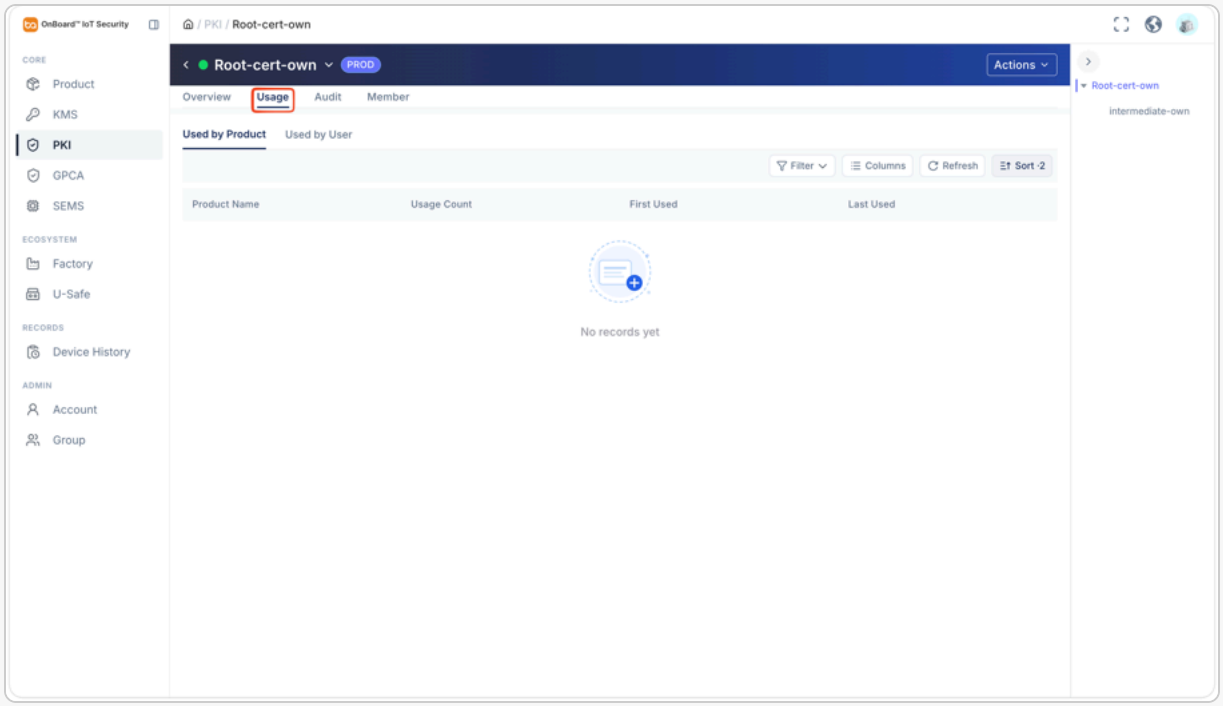
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then select the corresponding certificate.



3. Select the **Usage** tab, you can check the usage count (such as **Usage Count**, **First Used**, and **Last Used**) for certificates used by users and products.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.

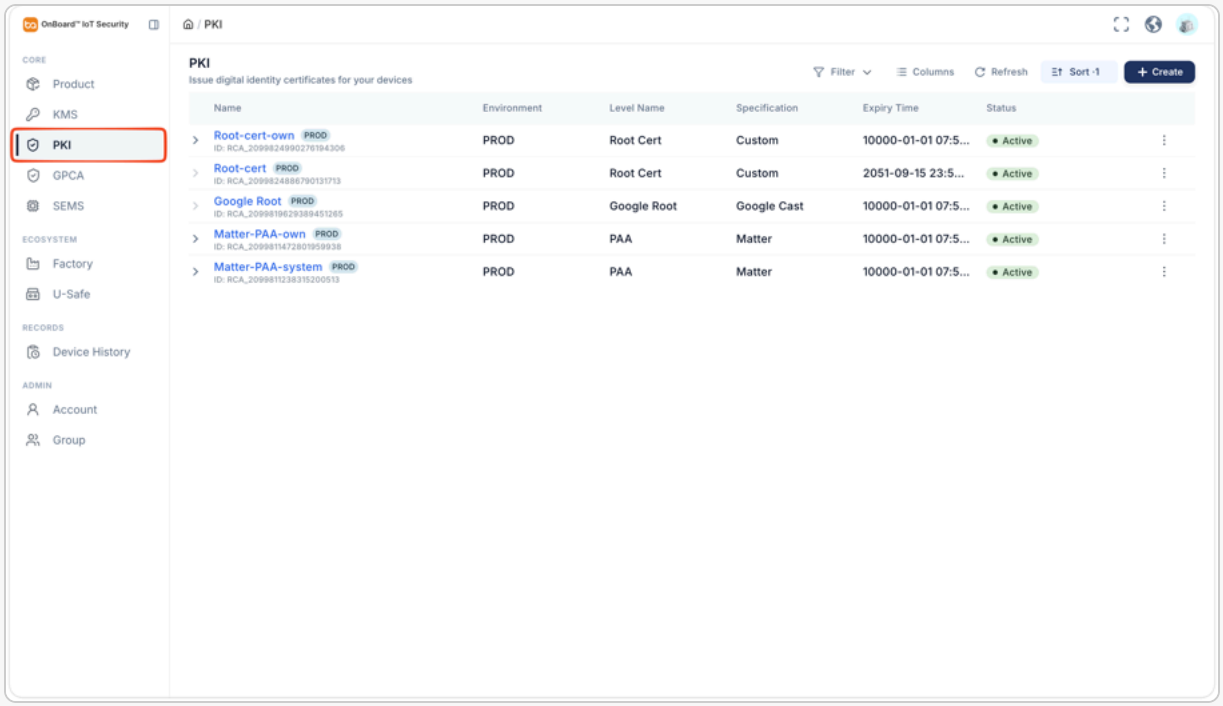


Check verification service

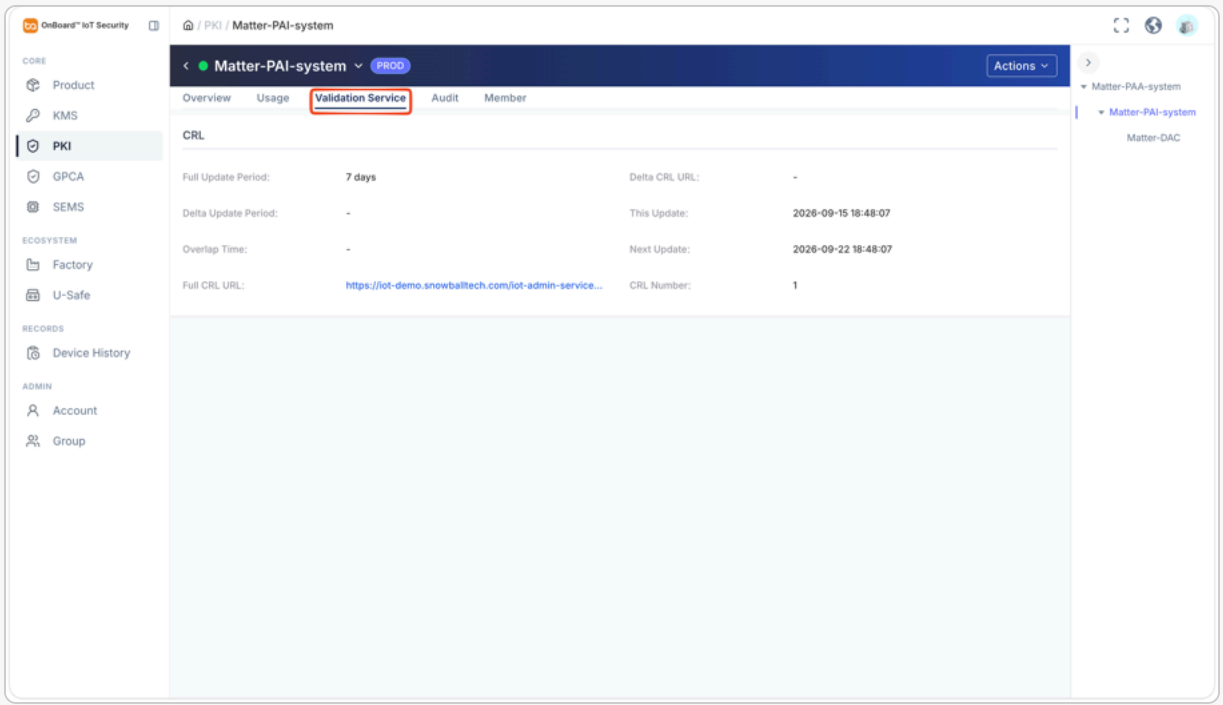
> **TIP**
>
> The **Verification Services** tab is displayed only for system-generated intermediate certificates (PAI, Manufacturer, Model, and Sub Cert certificates).

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then select the corresponding certificate.



3. Select the **Verification Services** tab, you can check the verification service information (such as **CRL**, **OSCP**, and **CA Issuers**).

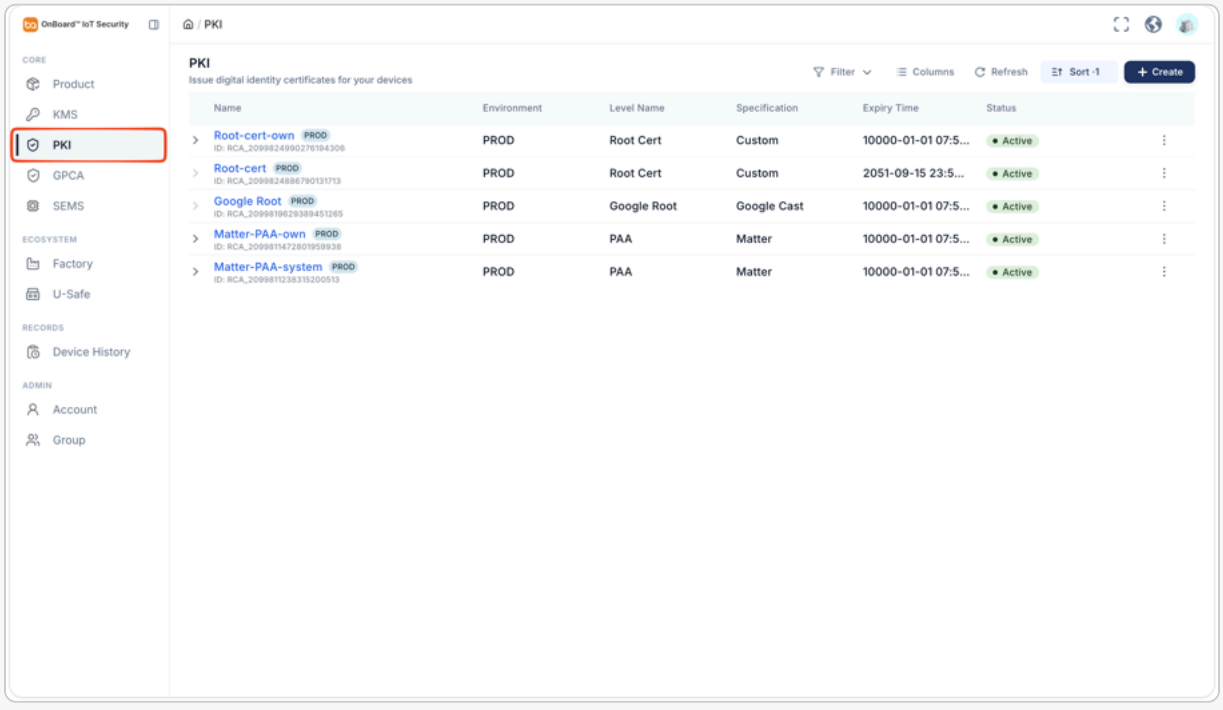


Check end-entity certificate

> **TIP**
>
> The end-entity certificate displays all end-entity certificates issued from the template, providing visibility into the template's actual issuance status.

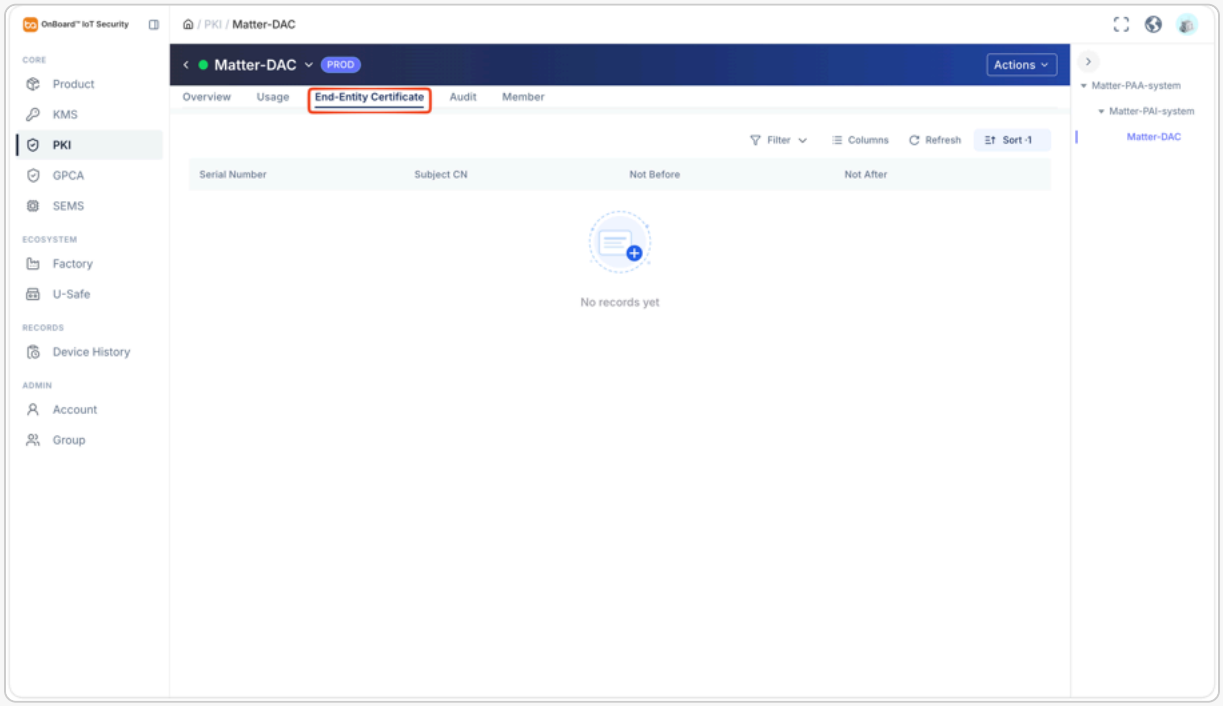
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then select the corresponding certificate template (**DAC Template**, **Device Template**, and **Leaf Template**).



3. Select the **End-Entity Certificate** tab, you can check the relevant end-entity certificate information (such as **Serial Number**, **Subject CN**, **Not Before**, and **Not After**).

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.

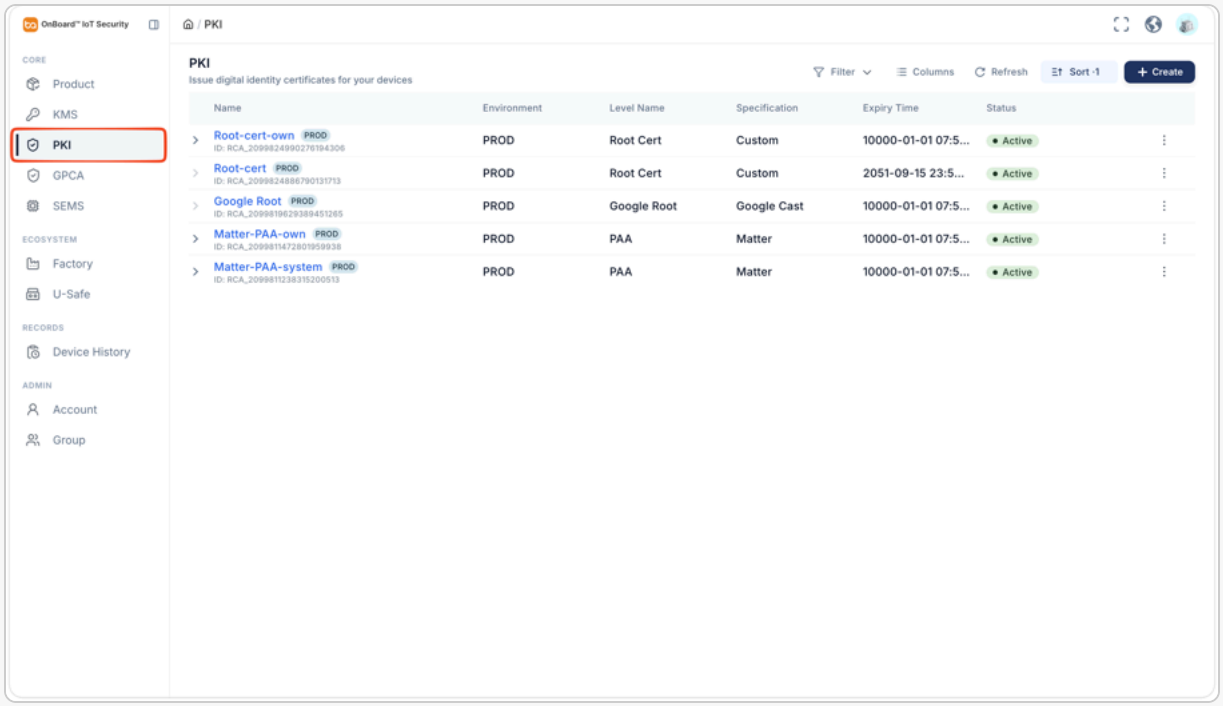


Check audit

> **TIP**
>
> Through the certificate logs, you can check the historical operations of the certificate.

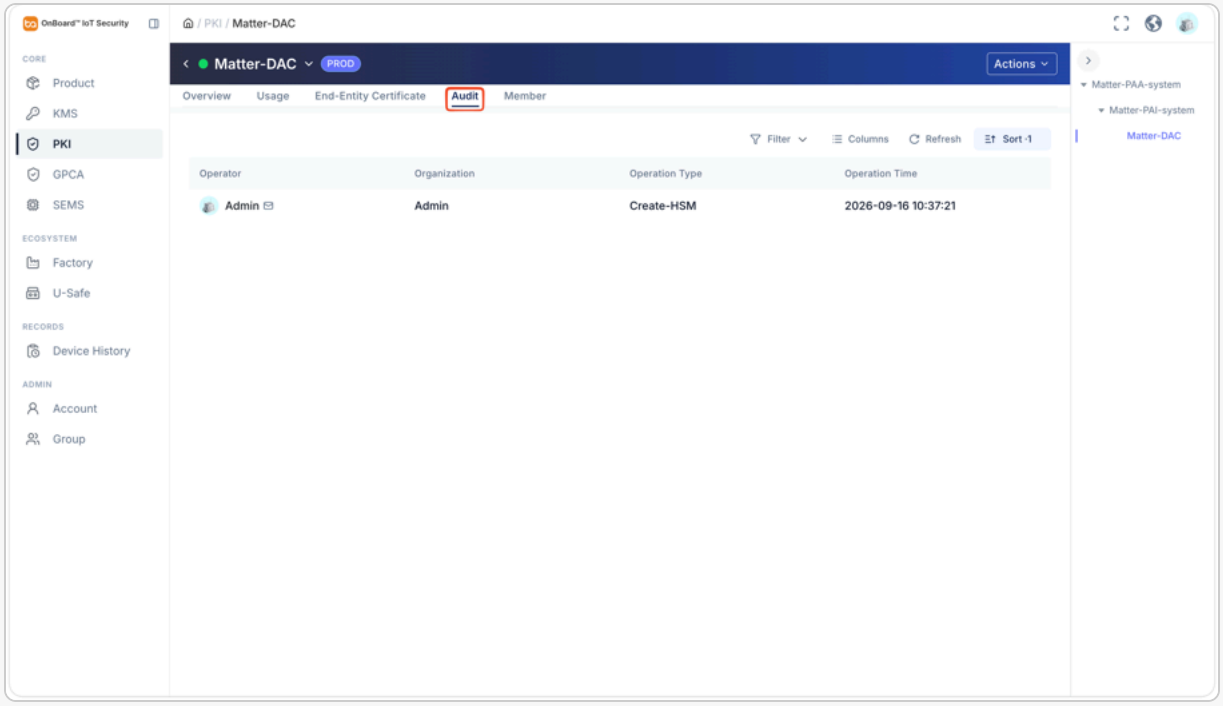
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then select the corresponding certificate.



3. Select the **Audit** tab, you can check the certificate's historical records (such as **Operator**, **Operation Type**, and **Operation Time**).

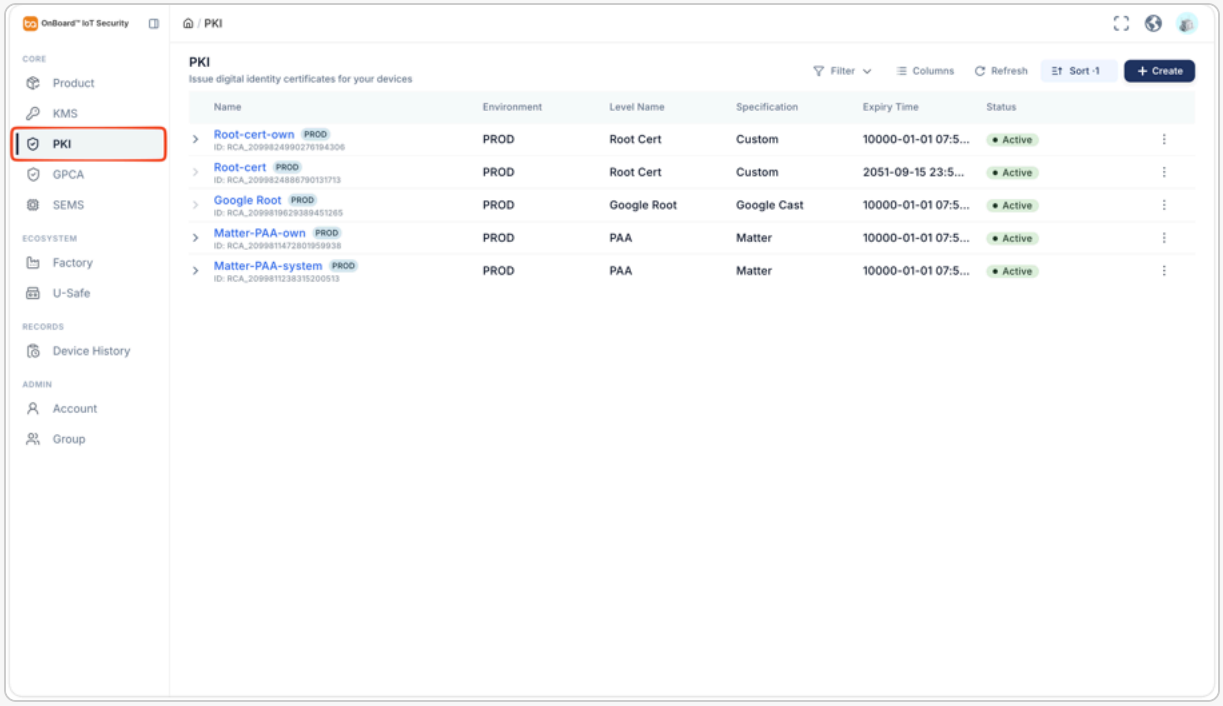
> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Check members

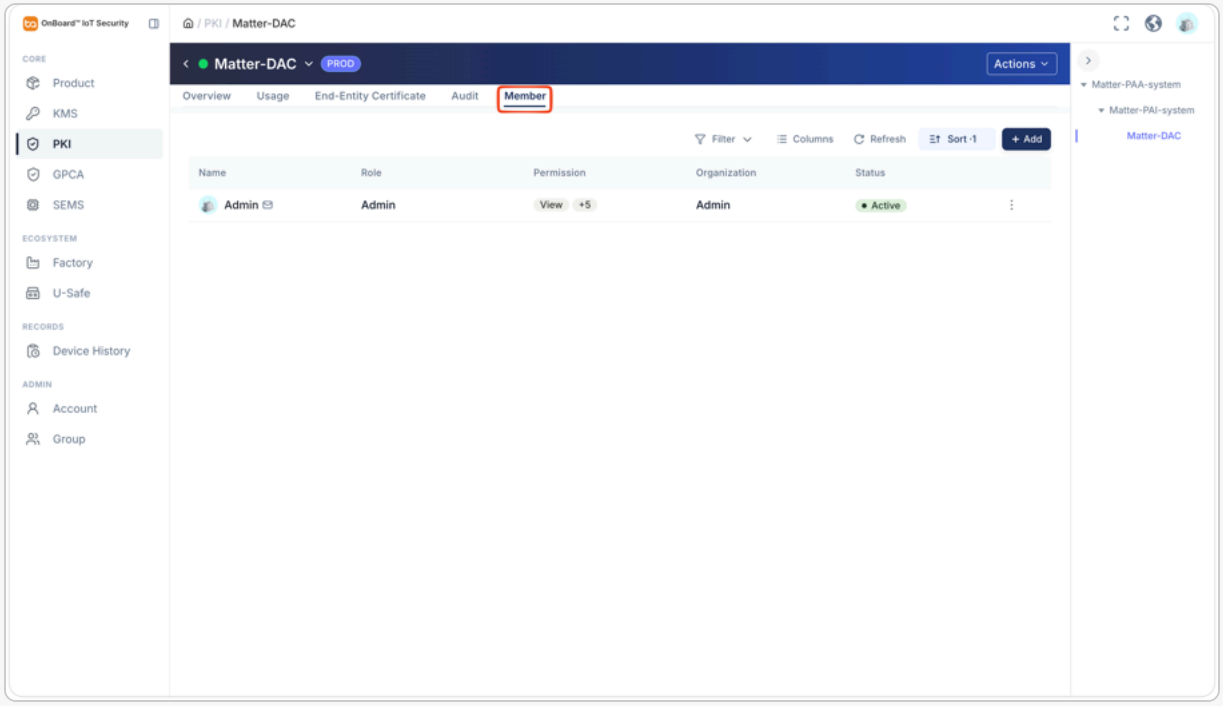
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then select the corresponding certificate.



3. Select the **Member** tab , you can check the user permissions for the certificate (such as **Name**, **Role**, and **Permission**).

> **TIP**
>
> Click the Filter , Sort , Refresh , and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.


OnBoard™ IoT Security
/ PKI / Matter-DAC
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
Matter-DAC
PROD
Actions
Overview
Usage
End-Entity Certificate
Audit
Member
Filter
Columns
Refresh
Sort · 1
+ Add
Name
Role
Permission
Organization
Status
Admin
Admin
View
+5
Admin
Active
Matter-PAA-system
Matter-PAI-system
Matter-DAC

Version: v3.4.0 (Latest)

How to manage certificates in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Manage certificate permissions
- Download a certificate
- Lock or unlock a certificate

Prerequisites

Before getting started, please ensure that you have permissions for the corresponding certificate.

Manage certificate permissions

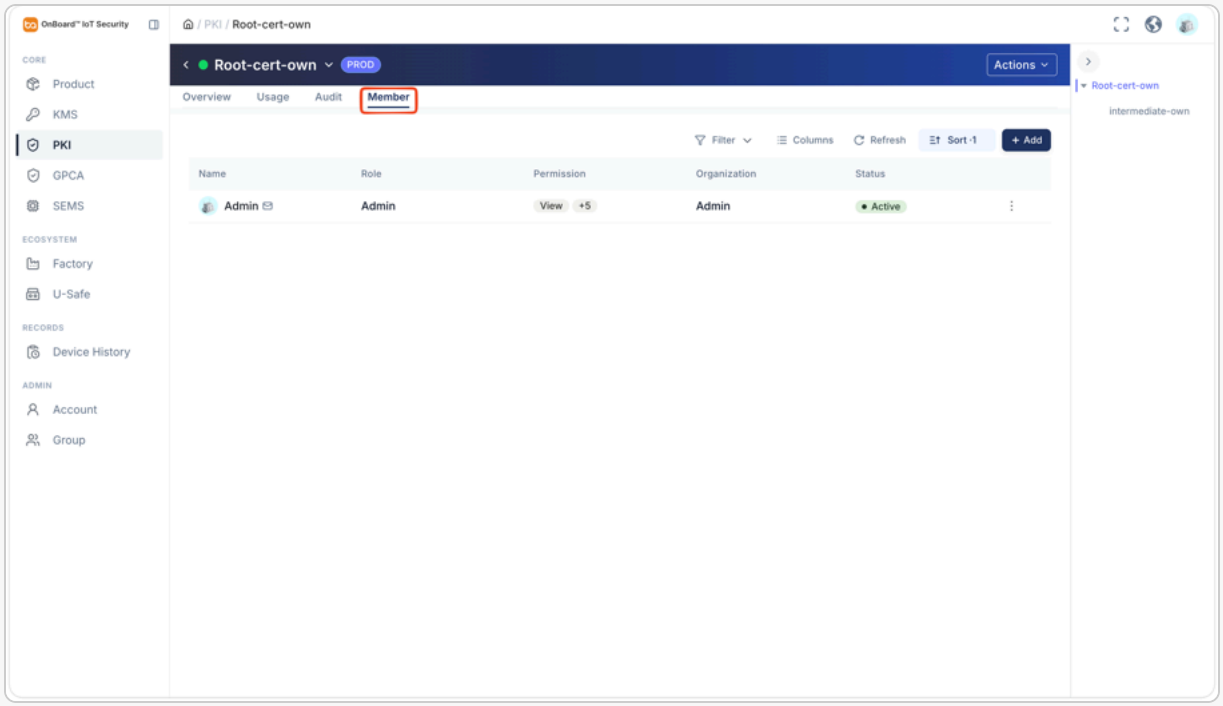
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

You can assign different operational permissions for the certificate to different members. The descriptions of these permissions are as follows:

Permissions	Description
View	View certificate details (read-only).
Edit	Allow cryptographic configuration for the certificate.
Create Authorization	Allow the certificate to be referenced in product and SE Profile configurations.
Lock	Lock a certificate.
unlock	Unlock a locked certificate.
Add Member	Add members to this certificate and assign them permissions that do not exceed your own permissions.
Revoke	Revoke a certificate.
Destroy	Destroy a certificate.

You can adjust and set user permissions for certificates by following these steps:

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain and then select the corresponding certificate.
3. On the certificate page, you can manage the user permissions for the certificate on the **Member** tab.

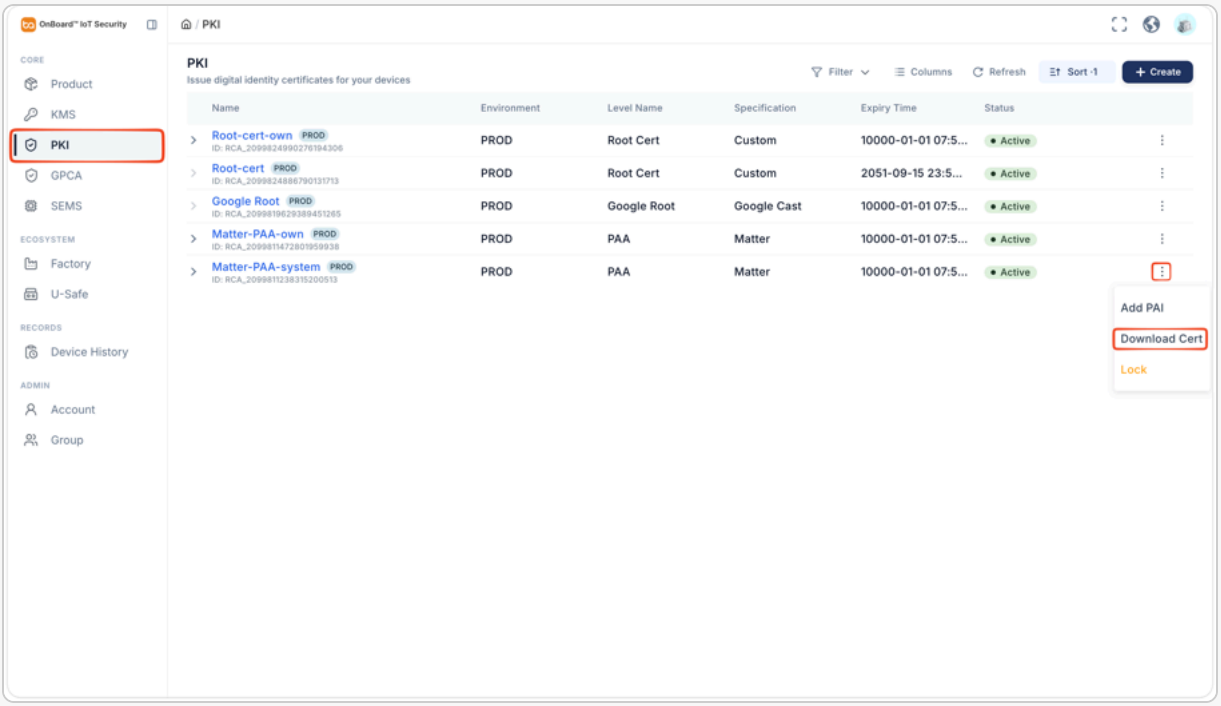


Download a certificate

> **TIP**
>
> Only certificates in the **Active** state can be downloaded, and the same user can download the same certificate a maximum of 10 times per hour.

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding certificate and select **Download Cert**.

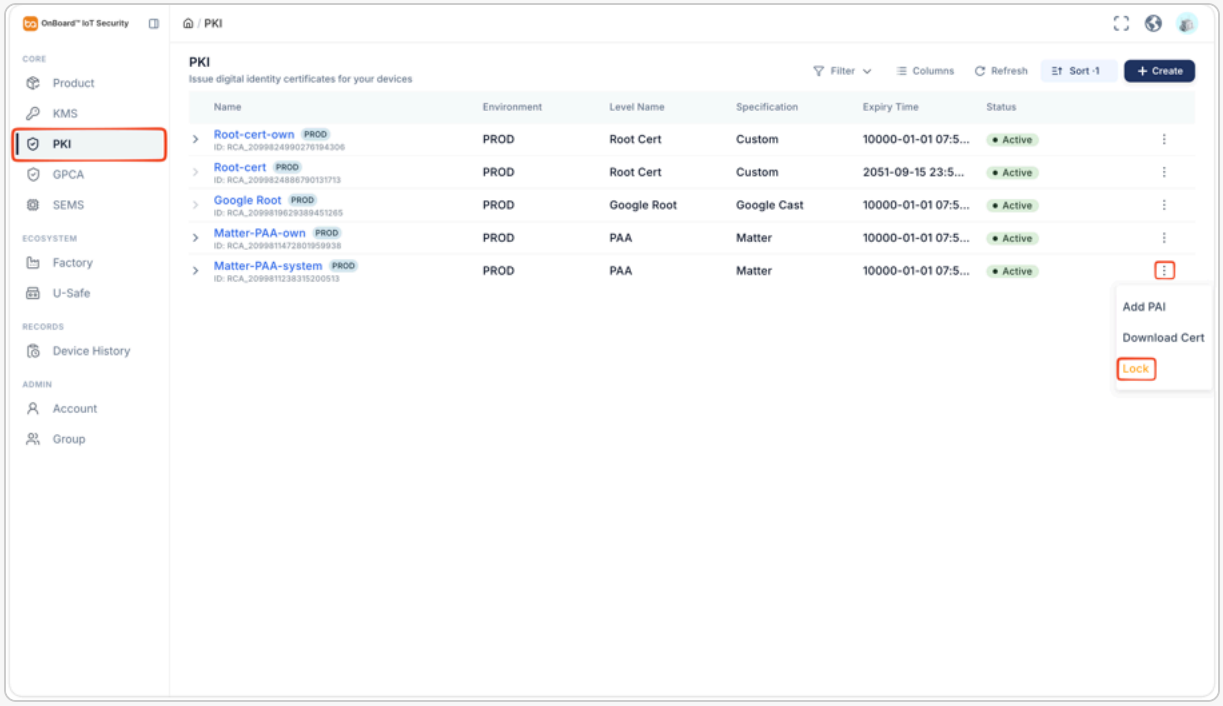


Lock or unlock a certificate

> **TIP**
>
> Once the certificate is locked, it can't be selected when configuring Certificates for the product.

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **PKI**. Expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding certificate and select **Lock** or **Unlock**. Click **Confirm** to lock or unlock the certificate. When locking a certificate, you can optionally provide a reason.


OnBoard™ IoT Security
PKI
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
PKI
Issue digital identity certificates for your devices
Filter
Columns
Refresh
Sort -1
+ Create
Name
Environment
Level Name
Specification
Expiry Time
Status
Root-cert-own PROD
ID: RCA_209982499027819430 6
PROD
Root Cert
Custom
10000-01-01 07:5...
Active
Root-cert PROD
ID: RCA_209982488679013171 3
PROD
Root Cert
Custom
2051-09-15 23:5...
Active
Google Root PROD
ID: RCA_209981962938945126 5
PROD
Google Root
Google Cast
10000-01-01 07:5...
Active
Matter-PAA-own PROD
ID: RCA_209981147280195993 8
PROD
PAA
Matter
10000-01-01 07:5...
Active
Matter-PAA-system PROD
ID: RCA_209981123831520051 3
PROD
PAA
Matter
10000-01-01 07:5...
Active
Add PAI
Download Cert
Lock

Version: v3.4.0 (Latest)

Overview of GPCA in OnBoard™ IoT Security

The GP CA (GlobalPlatform Certificate Authority) in OBIS (OnBoard IoT Security) is a dedicated certificate service for GlobalPlatform SCP11c, responsible for certificate issuance, management, and private key operations. It is mainly used for:

- Managing CA, Key Authority (KA), OCE (Off-Card Entity) 和 SD (Security Domain) certificates and their trust chains.
- Providing OCE private key operation services, ensuring that private keys never leave the GP CA.
- Providing authorization for certificate signing and encrypted key export to the EdgeHSM.

The GP CA operates independently of SE Profile configuration management, supporting collaboration across teams and organizations. The following table summarizes the core capabilities of the GP CA:

Capability	Description
GP PKI Hierarchy Management	• Manage CA-KLCC and CA-KLOC root CAs • Manage subordinate KA, OCE, and SD certificates • Maintain certificate trust chains

Capability	Description
Certificate Lifecycle Management	• Support certificate issuance and status management • Support notifications for certificate status changes • Specific operations depend on object type and key source
Private Key Operation and Authorization	• Perform ECDH operations using OCE private keys; private keys do not leave the GP CA • Authorize certificate signing and encrypted key export for EdgeHSM • Supports usage count and validity period limits
Collaboration and Permission Control	• Support object-level collaborator management • Assign permissions such as View, Use, Create Authorization, and Manage Status as needed
External CA Support	• Support import of external root CAs and KAs • Support offline issuance
SD Certificate Archiving	• Centrally archive Mode A and Mode B SD certificates • Support queries by certificate serial

Version: v3.4.0 (Latest)

Create a GlobalPlatform certificate - OnBoard™ IoT Security

OnBoard™ IoT Security provides comprehensive GlobalPlatform certificate creation capabilities, supporting SD (Security Domain), OCE (Off-Card Entity), and Mixed certificate chains. Select a certificate chain below to explore its creation workflow.

Version: v3.4.0 (Latest)

How to create a certificate based on the SD certificate chain in OnBoard™ IoT Security

This article will guide you on how to create a certificate based on the SD (Security Domain) certificate chain in OnBoard™ IoT Security (OBIS).

Prerequisites

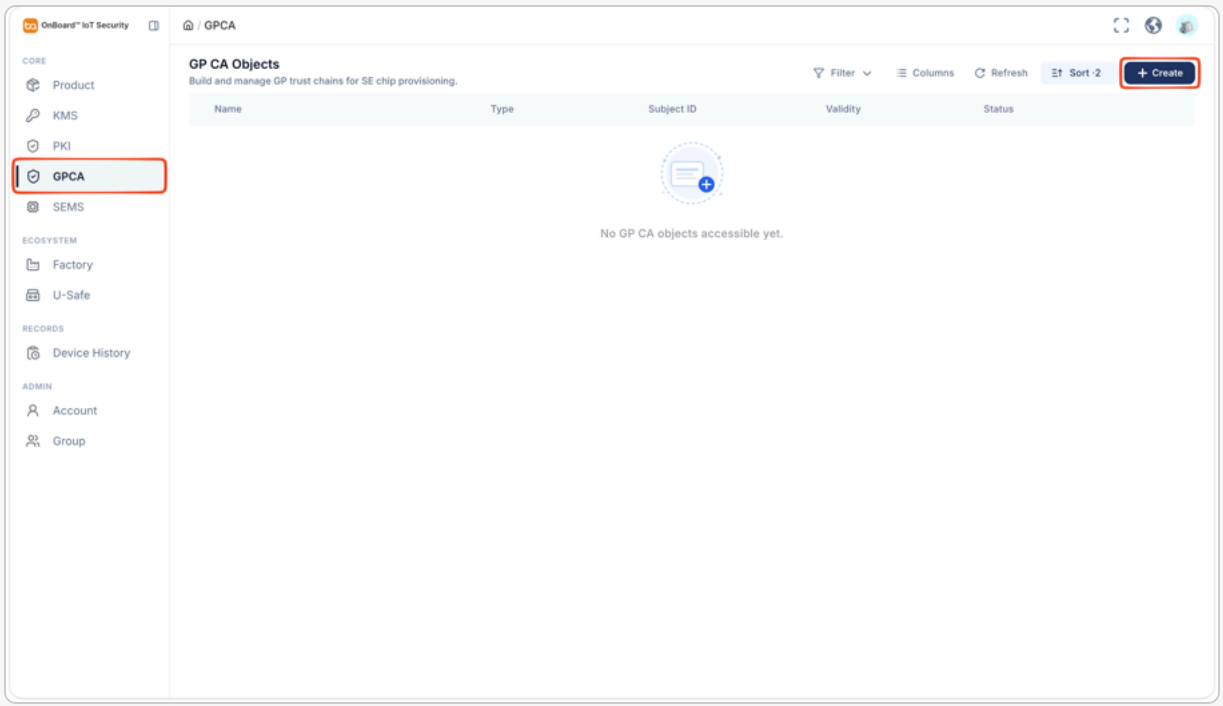
Before getting started, please ensure that you have OBIS role permissions as a System Manager or SE Resource Manager.

Instructions

> **TIP**
>
> After an SD certificate chain is created, when configuring the SE Profile in SEMS, you can select the corresponding CA-KLCC (Controlling Authority for Confidential Key Loading Card Certificates), KA-KLCC (Intermediate Key Authority for Confidential Key Loading Card Certificates), or SD certificate in the SCP11c Configuration.

1. Sign in to OBIS。

2. In the **Core** section of the left menu, click **GPCA**, and then click **Create** on the **GP CA Objects** page.

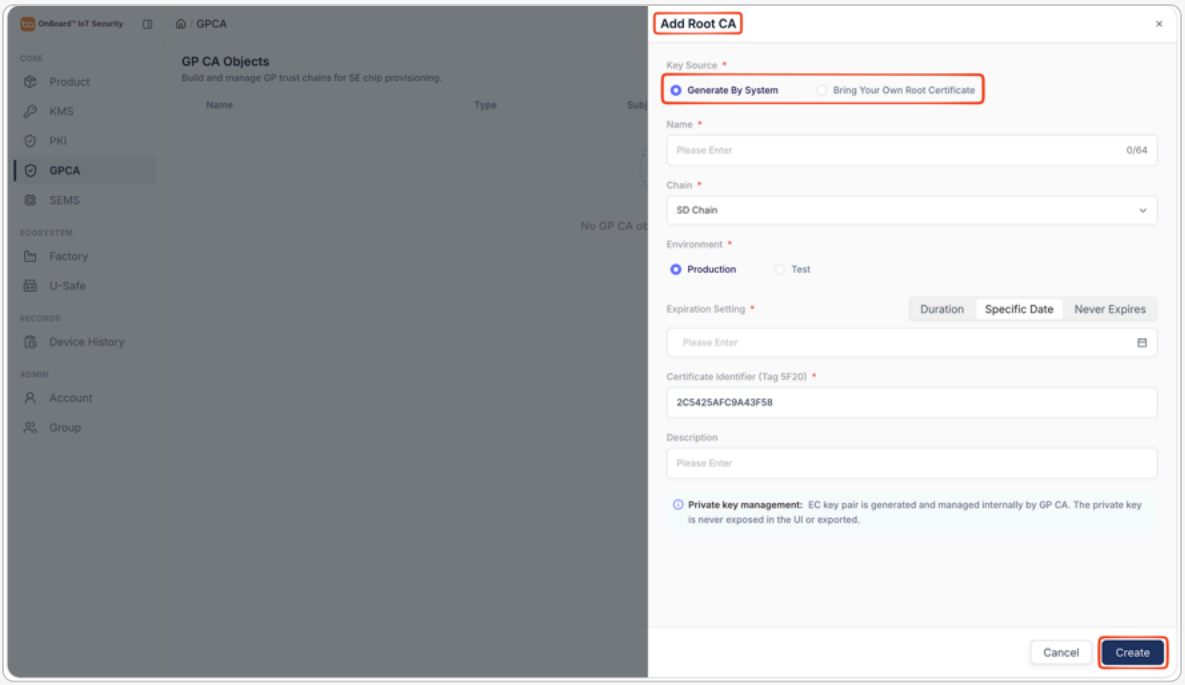


Create a Root CA (CA-KLCC) | Create an Intermediate KA (KA-KLCC)

Create an SD certificate

> **TIP**
>
> CA-KLCC is the root CA of the SD certificate chain and is used to issue and manage the subordinate KA-KLCC and SD certificates.

1. On the **Add Root CA** panel, select **Generate by System** or **Bring Your Own Root Certificate** as needed.



Description of Root CA basic information:

Information	Generate by System	Bring Your Own Root Certificate
Certificate Data (7F21 Hex)	N/A	Enter the Hex certificate data in the GlobalPlatform certificate format (must start with 7F21). **Note**: The Issuer Identifier and Subject Identifier of the certificate must match.

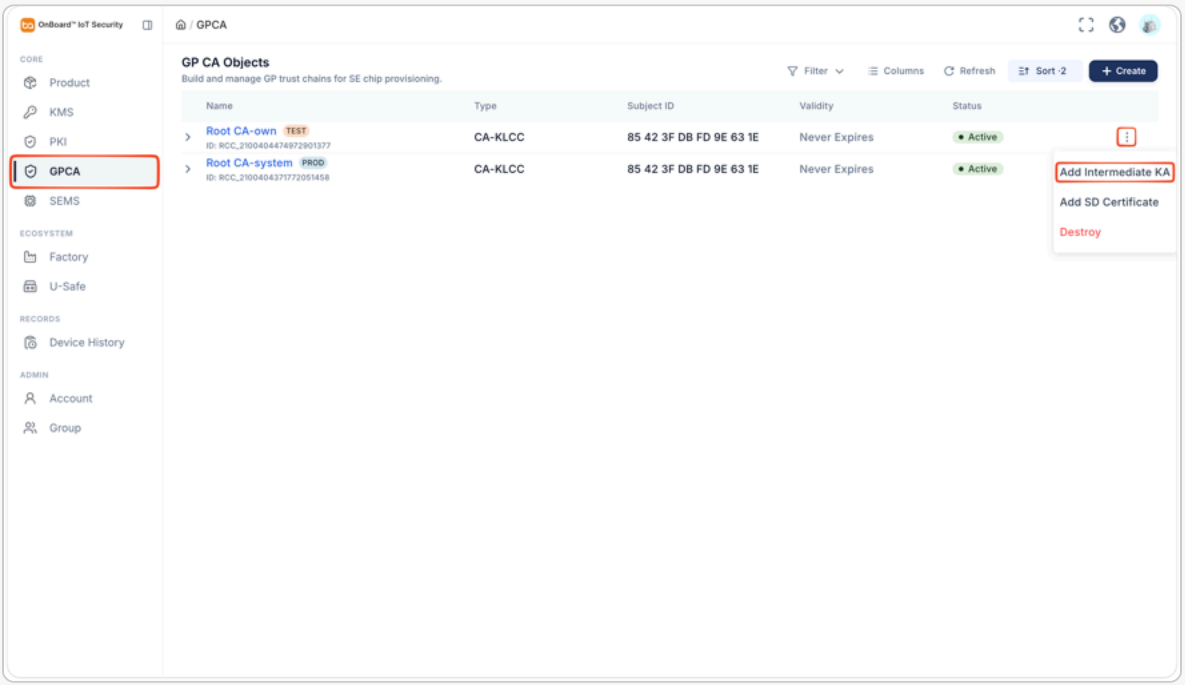
Information	Generate by System	Bring Your Own Root Certificate
Name	The Root CA name must be unique in the same environment.	
Chain	Select the **SD Chain**.	
Environment	Two environments can be selected: **Production** or **Test**.	
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.	N/A
Certificate Identifier (Tag 5F20)	Hex-encoded data for the certificate identifier. The system generates a 16-byte random value by default, which can be manually modified.	
Description	Provide additional information related to the Root CA, such as special requirements and important notes.	

2. After verifying that the information is correct, click **Create** to complete the Root CA creation.

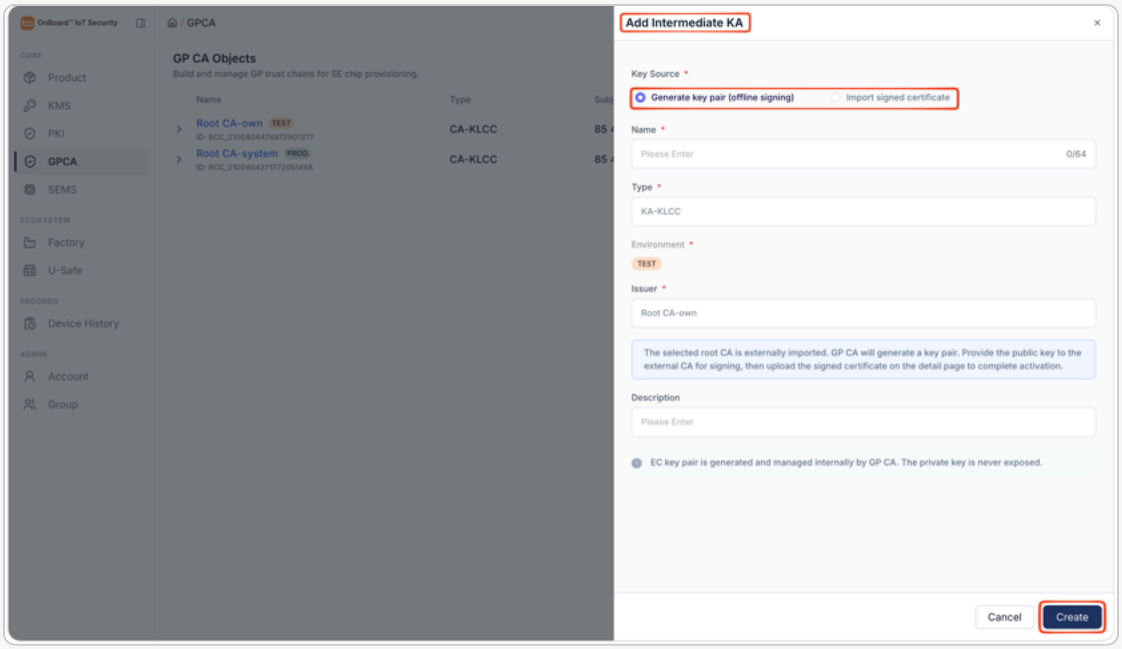
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

> **INFO**
>
> Before creating an Intermediate KA, please ensure that at least one Root CA has been created so that it can be selected and inherited during configuration.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding Root CA and select **Add Intermediate KA**.



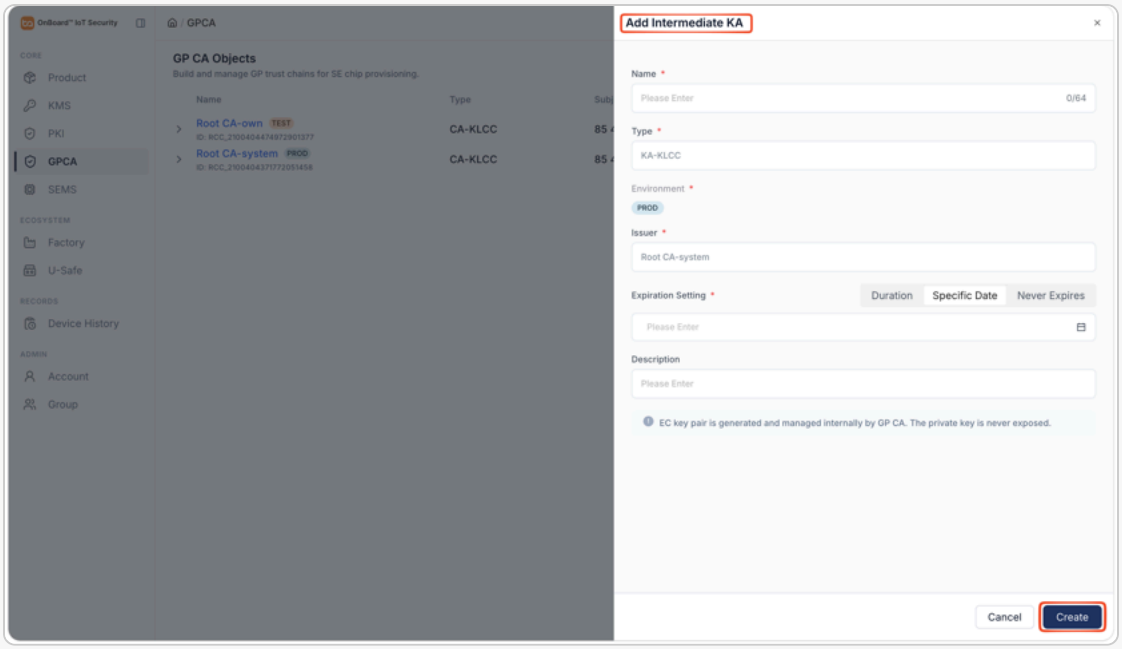
2. On the **Add Intermediate KA** panel, select and enter the basic information.
    - If the issuer of the intermediate KA is your own Root CA, you can select **Generate key pair (offline signing)** or **Import signed certificate** (your own intermediate KA) as needed



Information	Generate key pair (offline signing)	Import signed certificate
Certificate Data (7F21 Hex)	N/A	Enter the Hex certificate data in the GlobalPlatform certificate format (must start with 7F21). **Note**: The Issuer Identifier and Subject Identifier of the certificate must match.

Information	Generate key pair (offline signing)	Import signed certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Type	Default is **KA-KLCC**.	
Environment	The environment is inherited from the Root CA.	
Issuer	The inherited Root CA.	
Description	Provide additional information related to the Intermediate KA, such as special requirements and important notes.	

- If the issuer of the intermediate KA is the system-generated Root CA



Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Type	Default is **KA-KLCC**.
Environment	The environment is inherited from the Root CA.
Issuer	The inherited Root CA.
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.
Description	Provide additional information related to the Intermediate KA, such as special requirements and important notes.

3. After verifying that the information is correct, click **Create** to complete the Intermediate KA creation.

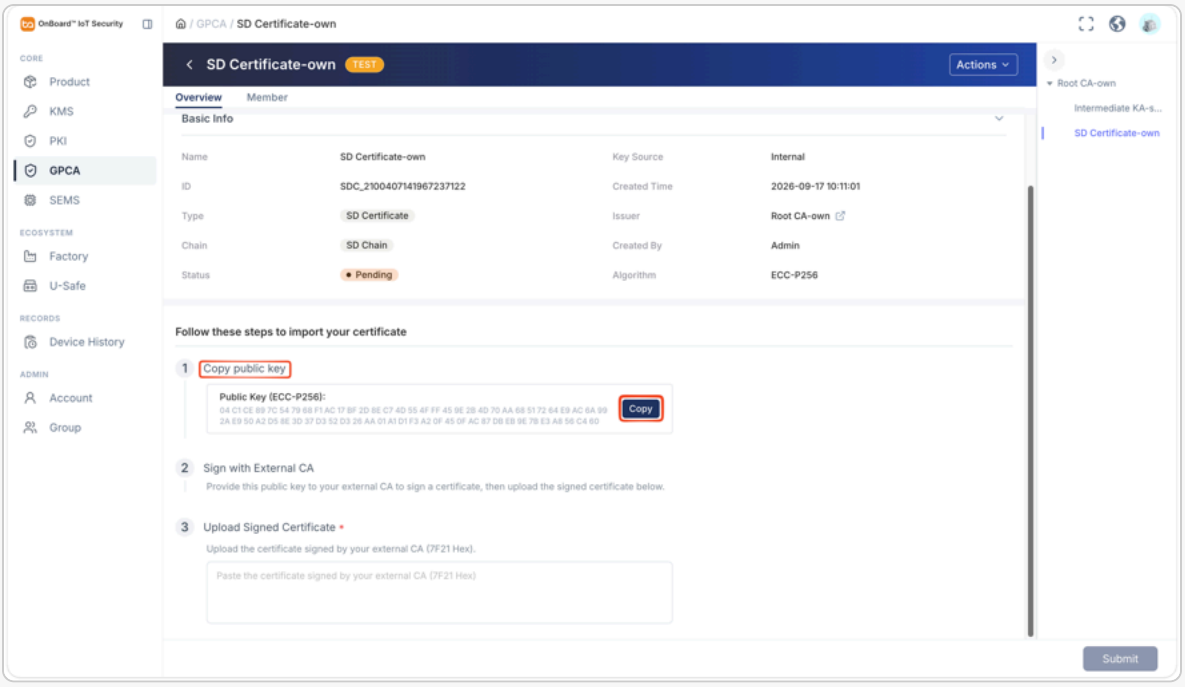
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an Intermediate KA, if the issuer is your own Root CA, you must complete the external issuance steps for the Intermediate KA. Before the external issuance is completed, the certificate will remain in the **Pending** status and can't be used.

External issuance steps for the Intermediate KA

> **TIP**
>
> When creating an Intermediate KA, if the issuer is your own root CA, refer to the following steps to complete the external issuance.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, and then click the corresponding Intermediate KA.

2. Locate the **Copy public key** section on the certificate page, click **Copy**. Then, use your external CA to sign this public key, thereby generating an intermediate CA certificate issued by the external CA.

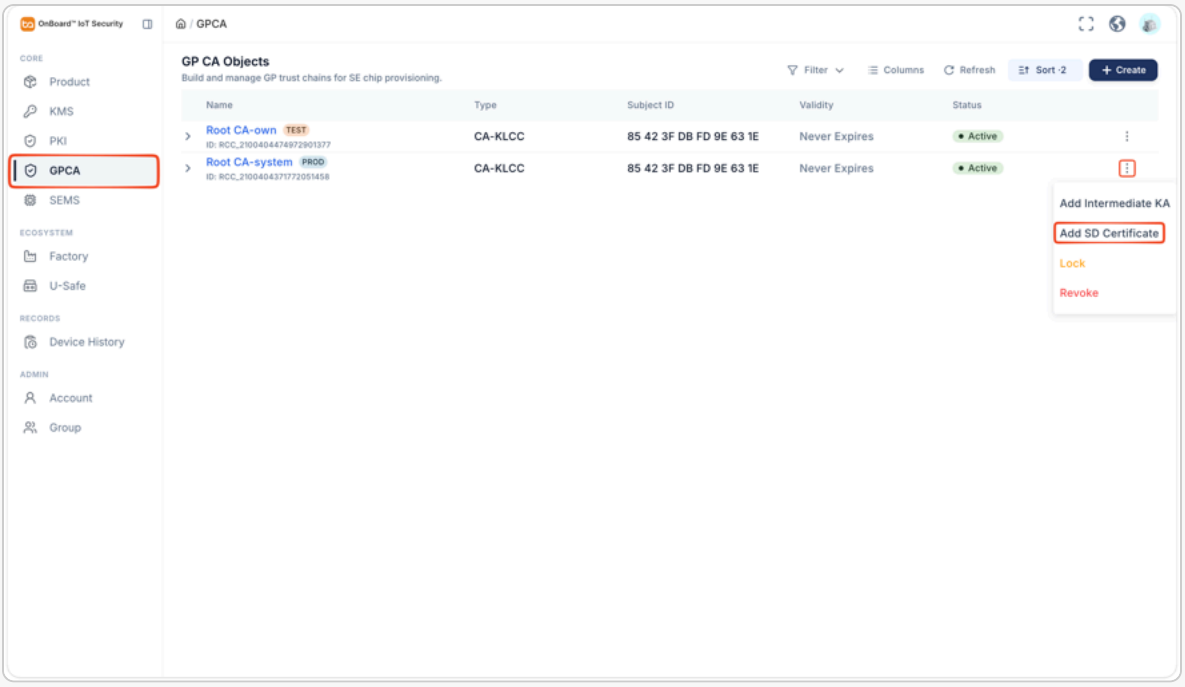


3. After issuance is complete, enter the certificate data (7F21 Hex) issued by the external CA in the **Upload Signed Certificate** section.

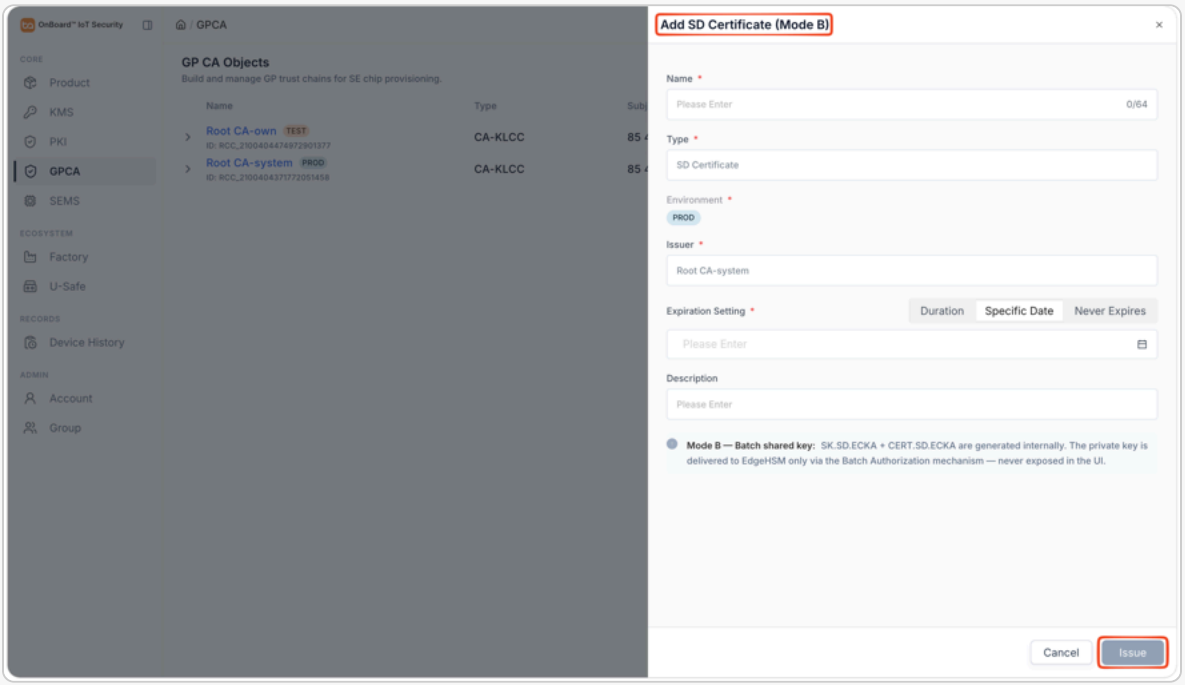
4. Click **Submit**. Once the configuration is completed, the Intermediate KA status will change to **Active**.

> **INFO**
>
> Before creating an SD certificate, please ensure that at least one Root CA or Intermediate KA has been created so that it can be selected and inherited during configuration.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding root or Intermediate KA and select **Add SD Certificate**.



2. On the **Add SD Certificate (Mode B)** page, select and enter the basic information.



Description of SD certificate basic information:

Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Type	Default is **SD Certificate**.
Environment	The environment is inherited from the Root CA or Intermediate KA.
Issuer	The inherited Root CA or Intermediate KA.
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed. **Note**: If the issuer is your own Root CA or Intermediate KA, the validity period will be inherited from the Root CA or Intermediate KA.
Description	Provide additional information related to the SD certificate, such as special requirements and important notes.

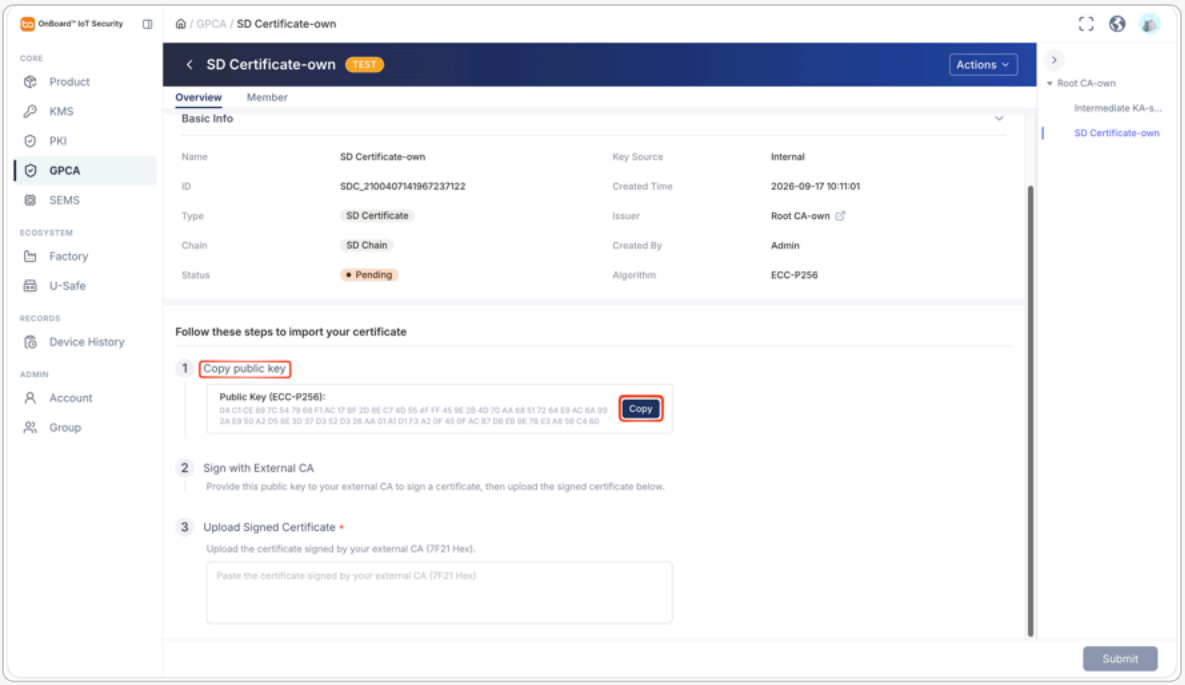
3. After verifying that the information is correct, click **Issue** to complete the SD certificate creation.

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an SD certificate, if the issuer is your own Root CA or Intermediate KA, you must complete the external issuance steps for the SD certificate. Before the external issuance is completed, the template will remain in the **Pending** status and can't be used.

External issuance steps for the SD certificate

> **TIP**
>
> When creating an SD certificate, if the issuer is your own Root CA or Intermediate KA, refer to the following steps to complete the external issuance.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, and then click the corresponding SD certificate.
2. Locate the **Copy public key** section on the certificate page, click **Copy**. Then, use your Root CA or Intermediate KA to sign the file, thereby generating an SD certificate signed by the Root CA or Intermediate KA.



3. After issuance is complete, enter the certificate data (7F21 Hex) issued by the external Root CA or Intermediate KA in the **Upload Signed Certificate** section.

4. Click **Submit**. Once the configuration is completed, the SD certificate status will change to **Active**.

Version: v3.4.0 (Latest)

How to create a certificate based on the OCE certificate chain in OnBoard™ IoT Security

This article will guide you on how to create a certificate based on the OCE (Off-Card Entity) certificate chain in OnBoard™ IoT Security (OBIS).

Prerequisites

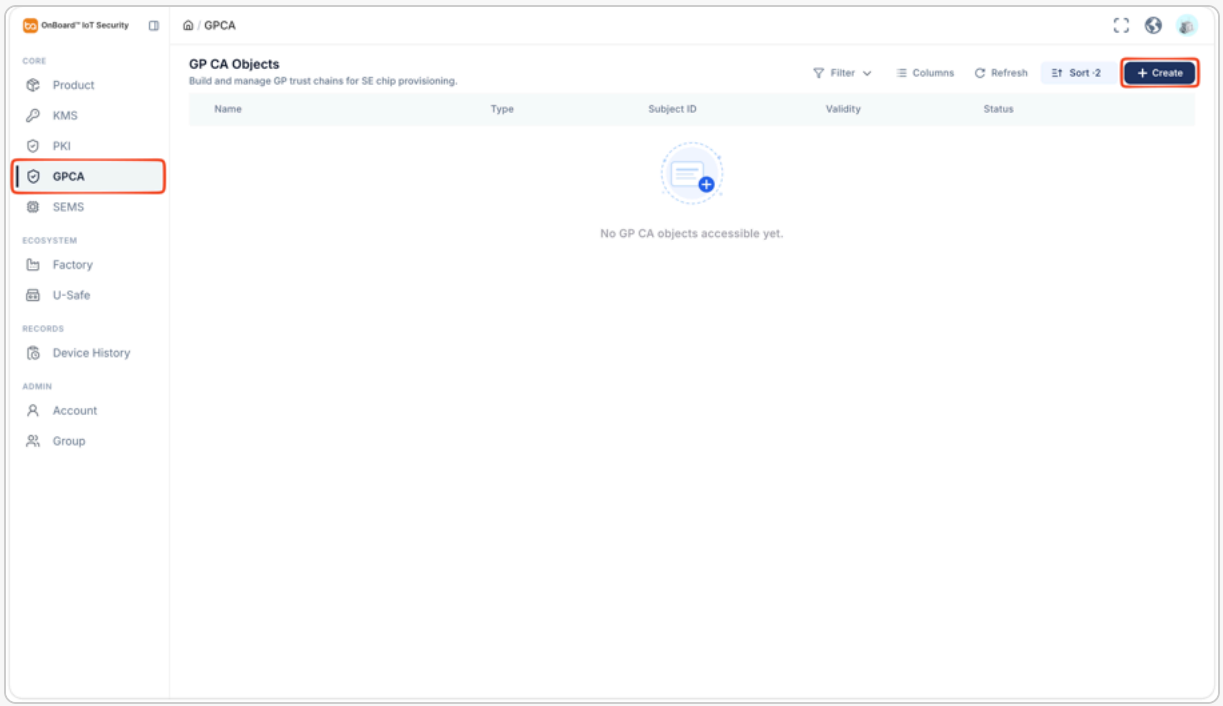
Before getting started, please ensure that you have OBIS role permissions as a System Manager or SE Resource Manager.

操作步驟

> **TIP**
>
> After an OCE certificate chain is created, when configuring an SE Profile in SEMS, you can select the corresponding CA-KLOC (Controlling Authority for Confidential Key Loading OCE Certificates), KA-KLOC (Intermediate Key Authority for Confidential Key Loading OCE Certificates), or OCE (Off-Card Entity) certificate in the SCP11c configuration.

1. Sign in to OBIS。

2. In the **Core** section of the left menu, click **GPCA**, and then click **Create** on the **GP CA Objects** page.

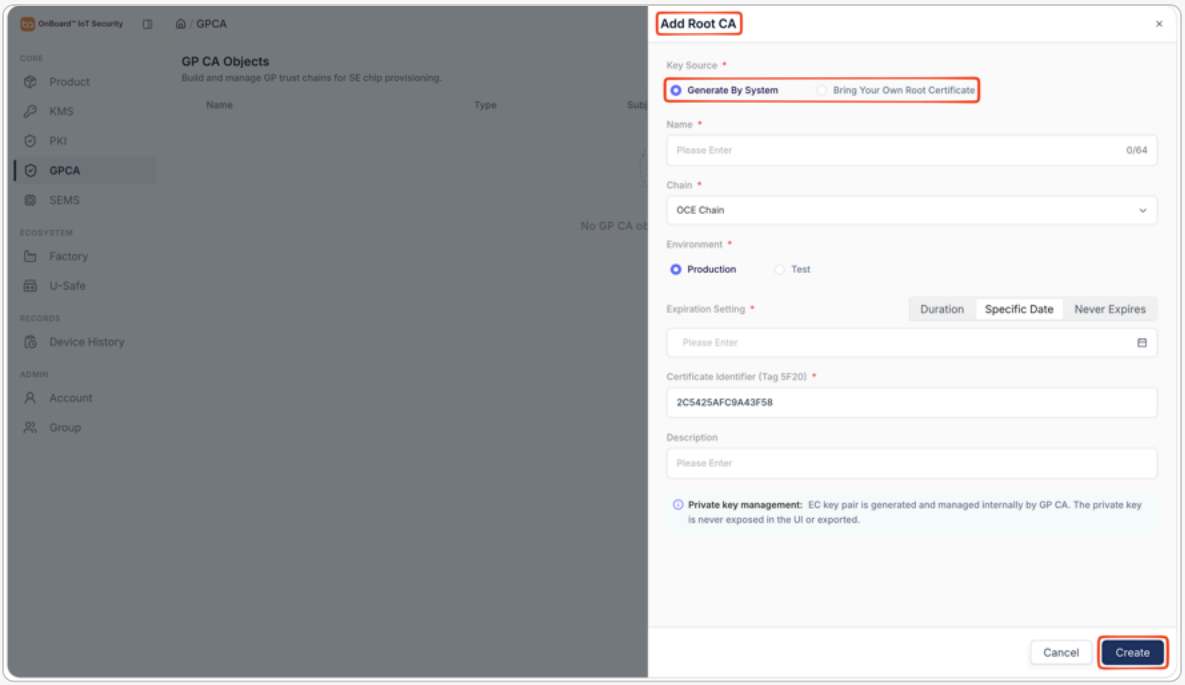


Create a Root CA (CA-KLOC) | Create an Intermediate KA (KA-KLOC)

Create an OCE certificate

> **TIP**
>
> CA-KLOC is the root CA of the OCE certificate chain and is used to issue and manage the subordinate KA-KLOC and OCE certificates.

1. On the **Add Root CA** panel, select **Generate by System** or **Bring Your Own Root Certificate** as needed.



Description of Root CA basic information:

Information	Generate by System	Bring Your Own Root Certificate
Certificate Data (7F21 Hex)	N/A	Enter the Hex certificate data in the GlobalPlatform certificate format (must start with 7F21). **Note**: The Issuer Identifier and Subject Identifier of the certificate must match.

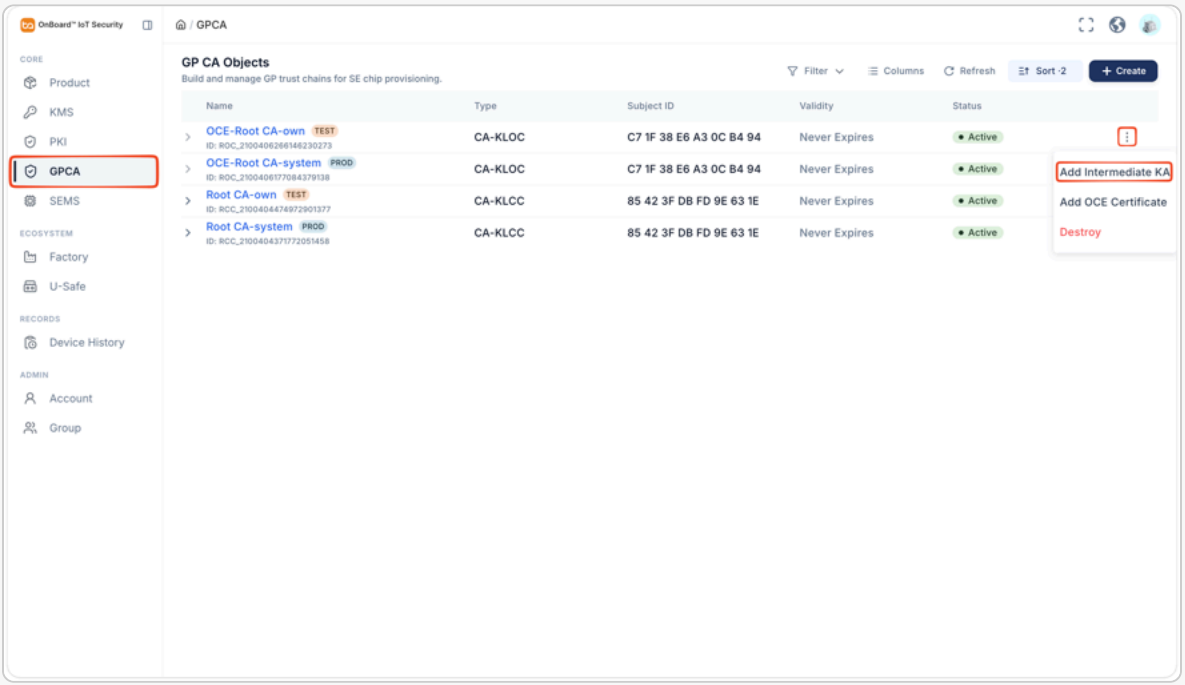
Information	Generate by System	Bring Your Own Root Certificate
Name	The Root CA name must be unique in the same environment.	
Chain	Select the **OCE Chain**.	
Environment	Two environments can be selected: **Production** or **Test**.	
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.	N/A
Certificate Identifier (Tag 5F20)	Hex-encoded data for the certificate identifier. The system generates a 16-byte random value by default, which can be manually modified.	
Description	Provide additional information related to the Root CA, such as special requirements and important notes.	

2. After verifying that the information is correct, click **Create** to complete the Root CA creation.

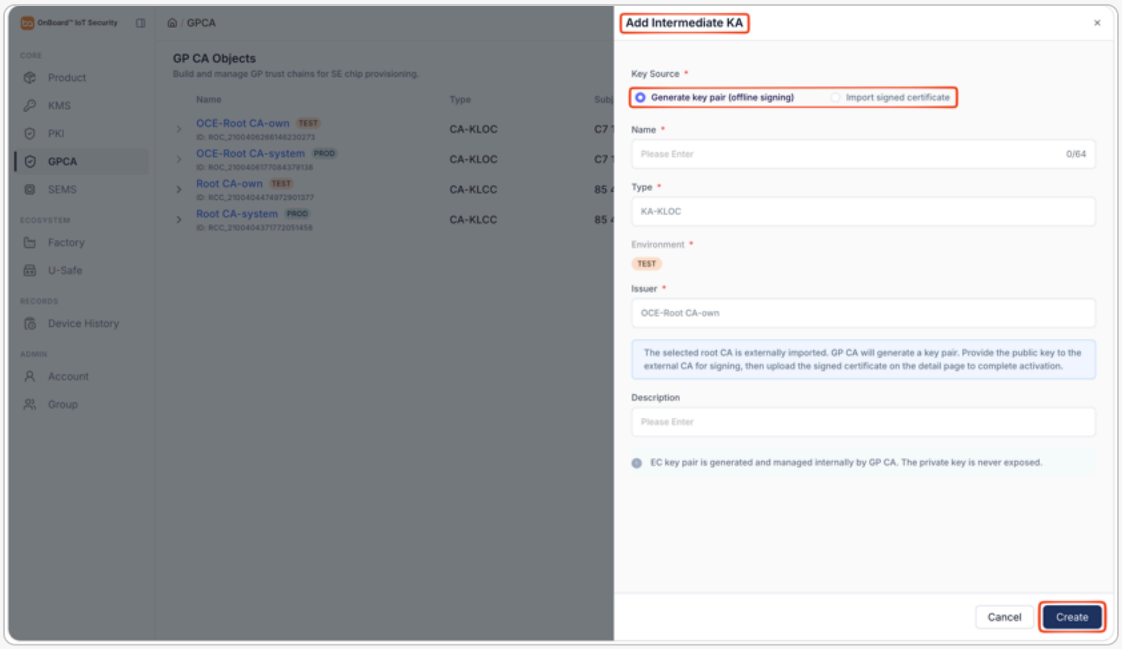
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

> **INFO**
>
> Before creating an Intermediate KA, please ensure that at least one Root CA has been created so that it can be selected and inherited during configuration.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding Root CA and select **Add Intermediate KA**.



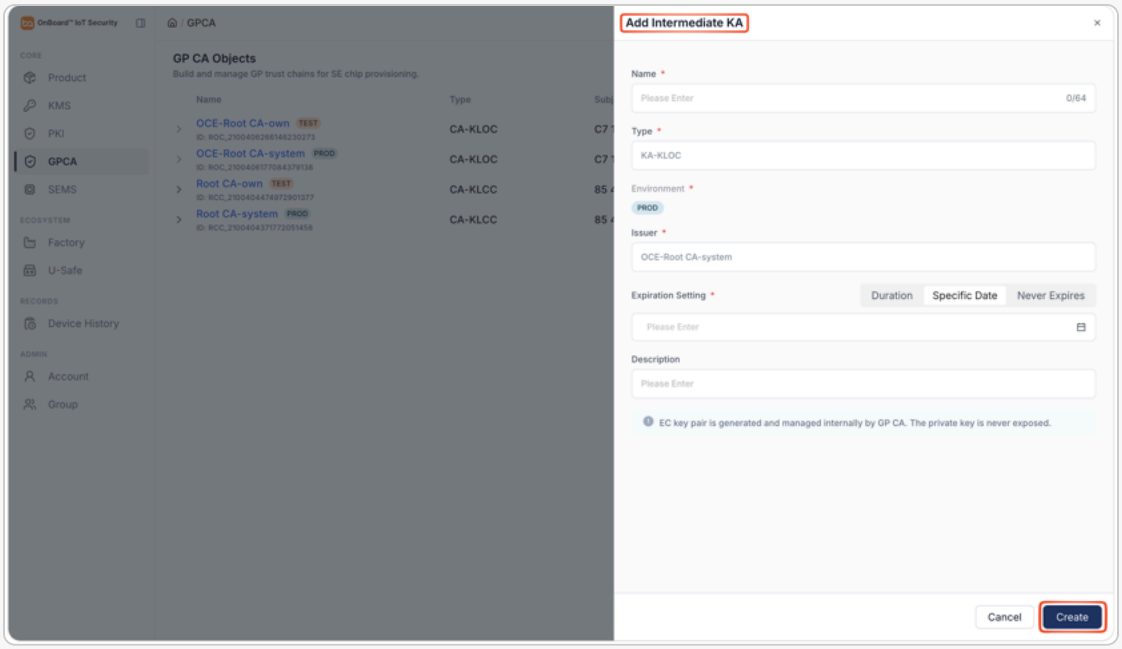
2. On the **Add Intermediate KA** panel, select and enter the basic information.
    - If the issuer of the intermediate KA is your own Root CA, you can select **Generate key pair (offline signing)** or **Import signed certificate** (your own intermediate KA) as needed



Information	Generate key pair (offline signing)	Import signed certificate
Certificate Data (7F21 Hex)	N/A	Enter the Hex certificate data in the GlobalPlatform certificate format (must start with 7F21). **Note**: The Issuer Identifier and Subject Identifier of the certificate must match.

Information	Generate key pair (offline signing)	Import signed certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Type	Default is **KA-KLOC**.	
Environment	The environment is inherited from the Root CA.	
Issuer	The inherited Root CA.	
Description	Provide additional information related to the Intermediate KA, such as special requirements and important notes.	

- If the issuer of the intermediate KA is the system-generated Root CA



Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Type	Default is **KA-KLOC**.
Environment	The environment is inherited from the Root CA.
Issuer	The inherited Root CA.
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.
Description	Provide additional information related to the Intermediate KA, such as special requirements and important notes.

3. After verifying that the information is correct, click **Create** to complete the Intermediate KA creation.

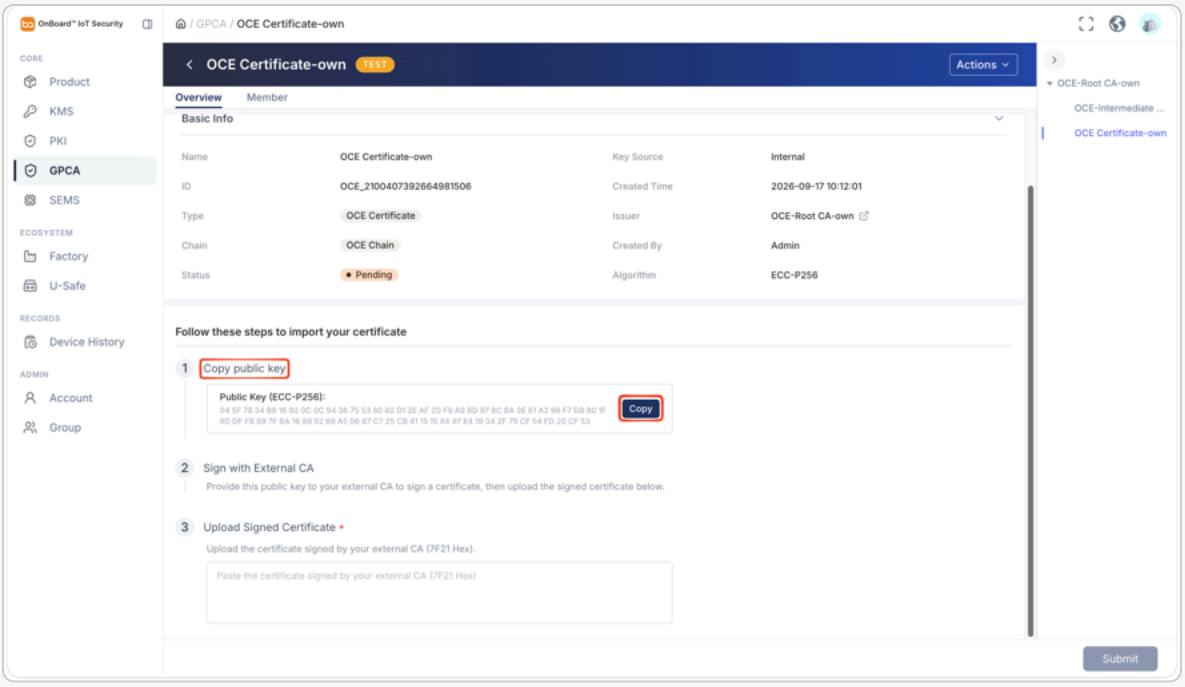
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an Intermediate KA, if the issuer is your own Root CA, you must complete the external issuance steps for the Intermediate KA. Before the external issuance is completed, the certificate will remain in the **Pending** status and can't be used.

External issuance steps for the Intermediate KA

> **TIP**
>
> When creating an Intermediate KA, if the issuer is your own root CA, refer to the following steps to complete the external issuance.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, and then click the corresponding Intermediate KA.

2. Locate the **Copy public key** section on the certificate page, click **Copy**. Then, use your external CA to sign this public key, thereby generating an intermediate CA certificate issued by the external CA.

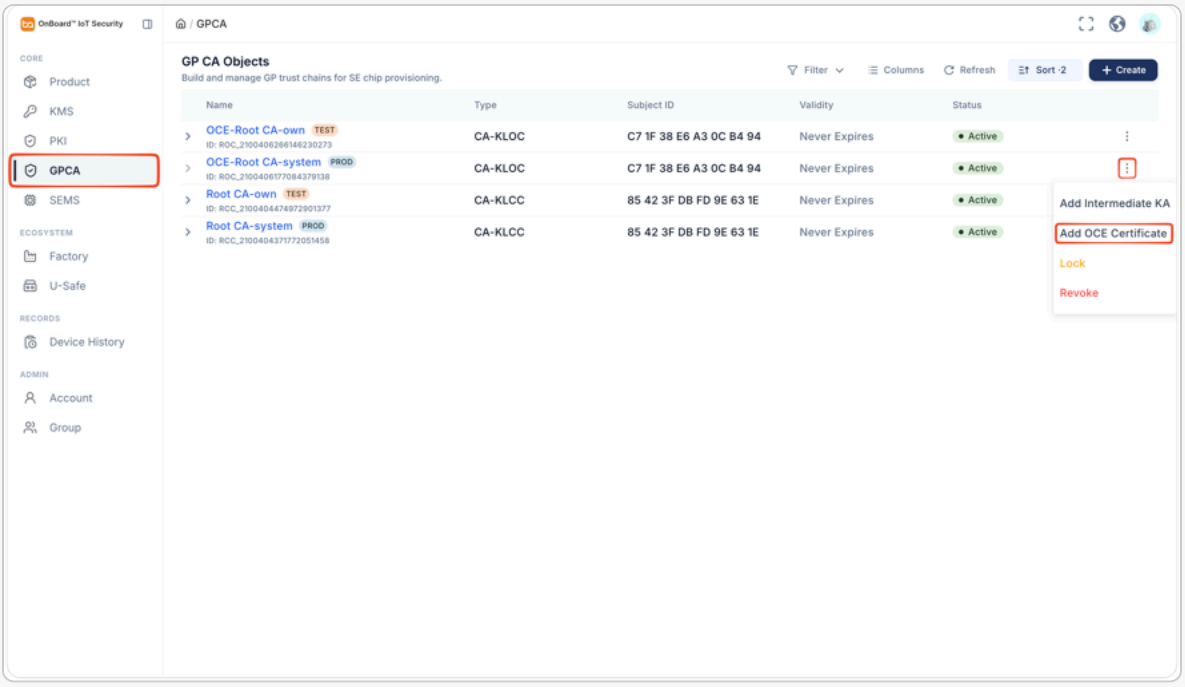


3. After issuance is complete, enter the certificate data (7F21 Hex) issued by the external CA in the **Upload Signed Certificate** section.

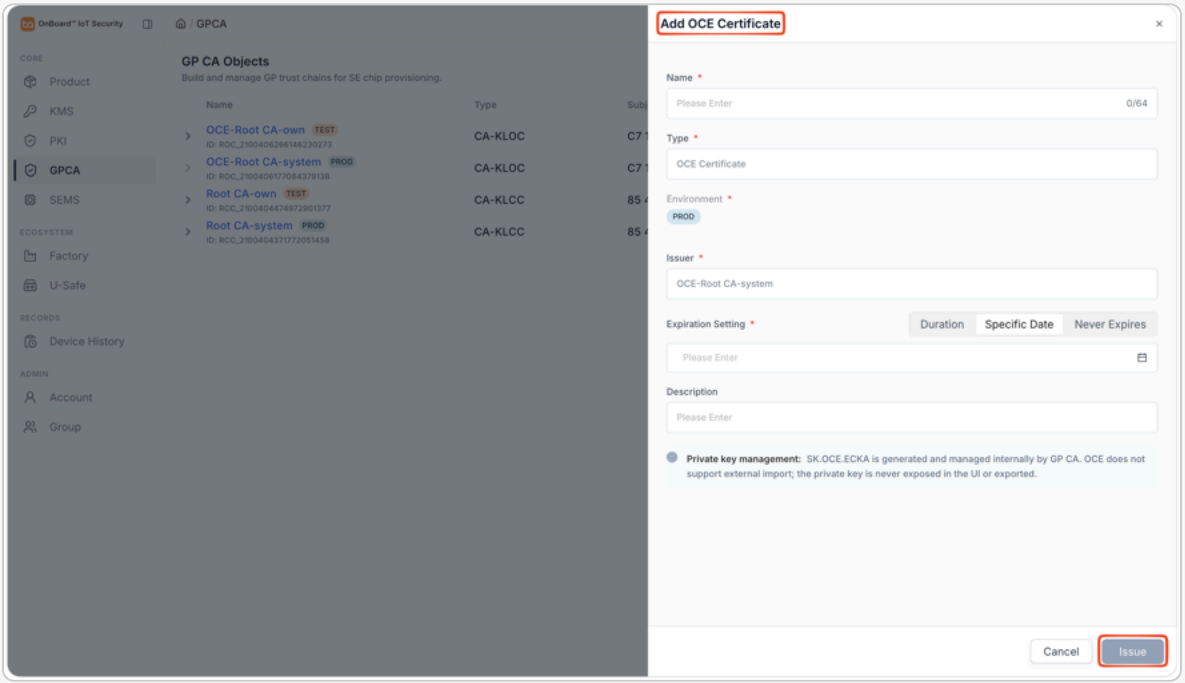
4. Click **Submit**. Once the configuration is completed, the Intermediate KA status will change to **Active**.

> **INFO**
>
> Before creating an OCE certificate, please ensure that at least one Root CA or Intermediate KA has been created so that it can be selected and inherited during configuration.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding root or Intermediate KA and select **Add OCE Certificate**.



2. On the **Add OCE Certificate** page, select and enter the basic information.



Description of OCE certificate basic information:

Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Type	Default is **OCE Certificate**.
Environment	The environment is inherited from the Root CA or Intermediate KA.
Issuer	The inherited Root CA or Intermediate KA.
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed. **Note**: If the issuer is your own Root CA or Intermediate KA, the validity period will be inherited from the Root CA or Intermediate KA.
Description	Provide additional information related to the OCE certificate, such as special requirements and important notes.

3. After verifying that the information is correct, click **Issue** to complete the OCE certificate creation.

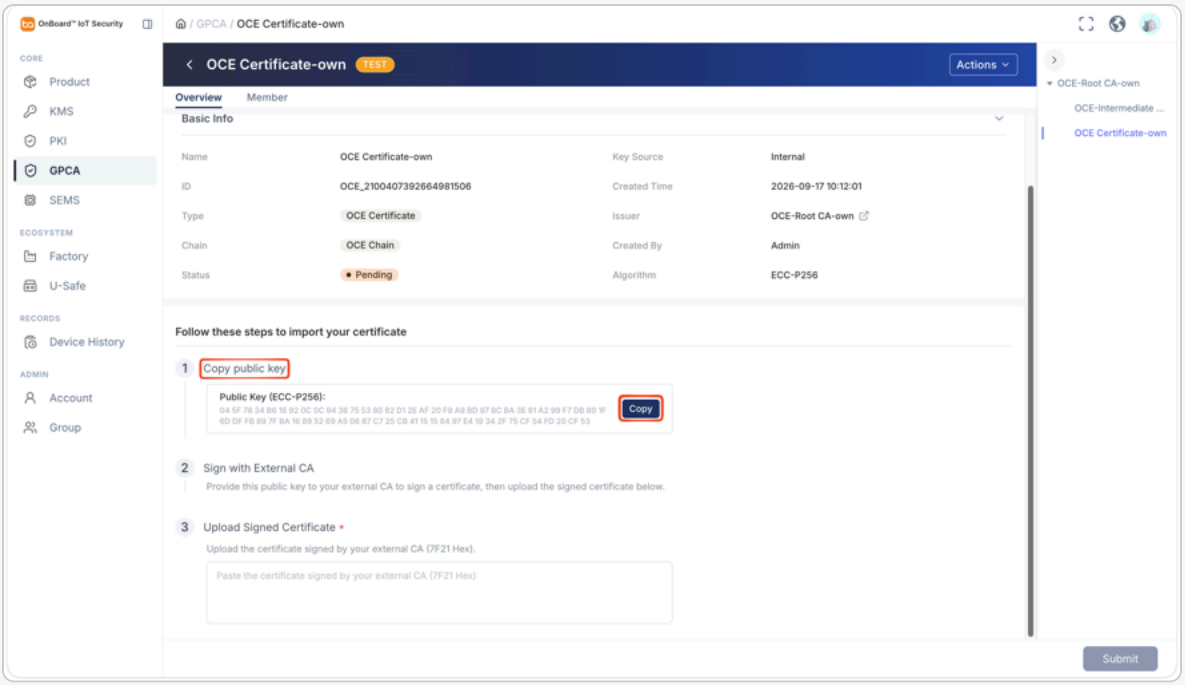
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an OCE certificate, if the issuer is your own Root CA or Intermediate KA, you must complete the external issuance steps for the OCE certificate. Before the external issuance is completed, the template will remain in the **Pending** status and can't be used.

External issuance steps for the OCE certificate

> **TIP**
>
> When creating an OCE certificate, if the issuer is your own Root CA or Intermediate KA, refer to the following steps to complete the external issuance.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, and then click the corresponding OCE certificate.

2. Locate the **Copy public key** section on the certificate page, click **Copy**. Then, use your Root CA or Intermediate KA to sign the file, thereby generating an OCE certificate signed by the Root CA or Intermediate KA.



3. After issuance is complete, enter the certificate data (7F21 Hex) issued by the external Root CA or Intermediate KA in the **Upload Signed Certificate** section.

4. Click **Submit**. Once the configuration is completed, the OCE certificate status will change to **Active**.

Version: v3.4.0 (Latest)

How to create a certificate based on the Mixed certificate chain in OnBoard™ IoT Security

This article will guide you on how to create a certificate for a mixed certificate chain in OnBoard™ IoT Security (OBIS).

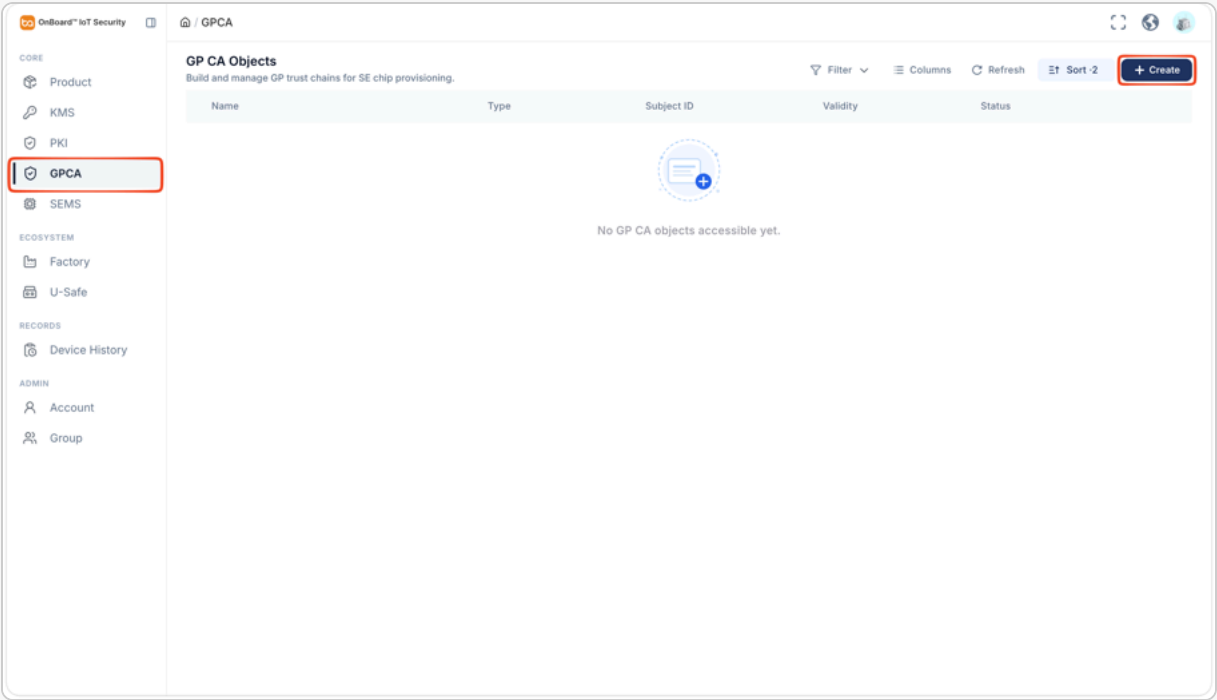
Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager or SE Resource Manager.

操作步骤

> **TIP**
>
> After a mixed certificate chain is created, when configuring the SE Profile in SEMS, you can select the corresponding CA-KLCC (Controlling Authority for Confidential Key Loading Card Certificates), CA-KLOC (Controlling Authority for Confidential Key Loading OCE Certificates), KA-KLCC (Intermediate Key Authority for Confidential Key Loading Card Certificates), KA-KLOC (Intermediate Key Authority for Confidential Key Loading OCE Certificates), SD certificate, or OCE (Off-Card Entity) certificate in the SCP11c configuration.

1. Sign in to OBIS。
2. In the **Core** section of the left menu, click **GPCA**, and then click **Create** on the **GP CA Objects** page.



Create a Root CA (CA-KLCC / CA-KLOC)

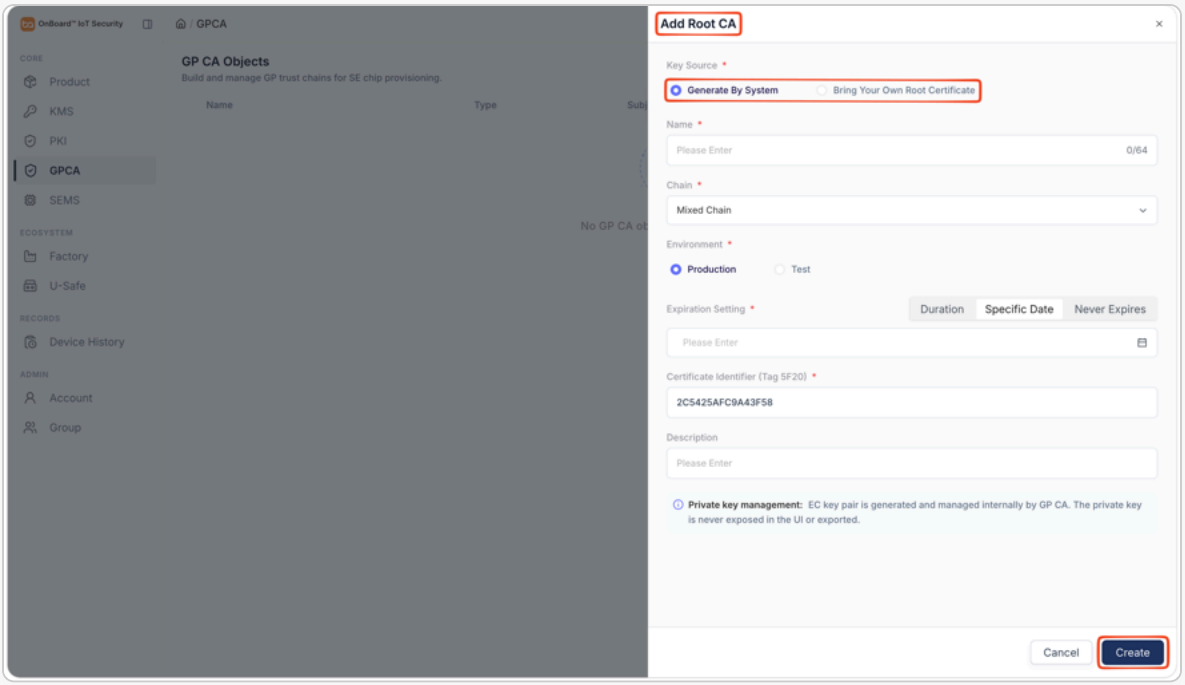
Create an Intermediate KA (KA-KLCC or KA-KLOC)

Create an SD or OCE certificate

TIP

- CA-KLCC is the root CA for the SD certificate chain and is used to issue and manage subordinate KA-KLCC and SD certificates.
- CA-KLOC is the root CA for the OCE certificate chain and is used to issue and manage subordinate KA-KLOC and OCE certificates.

1. On the **Add Root CA** panel, select **Generate by System** or **Bring Your Own Root Certificate** as needed.



Description of Root CA basic information:

Information	Generate by System	Bring Your Own Root Certificate
Certificate Data (7F21 Hex)	N/A	Enter the Hex certificate data in the GlobalPlatform certificate format (must start with 7F21). **Note**: The Issuer Identifier and Subject Identifier of the certificate must match.

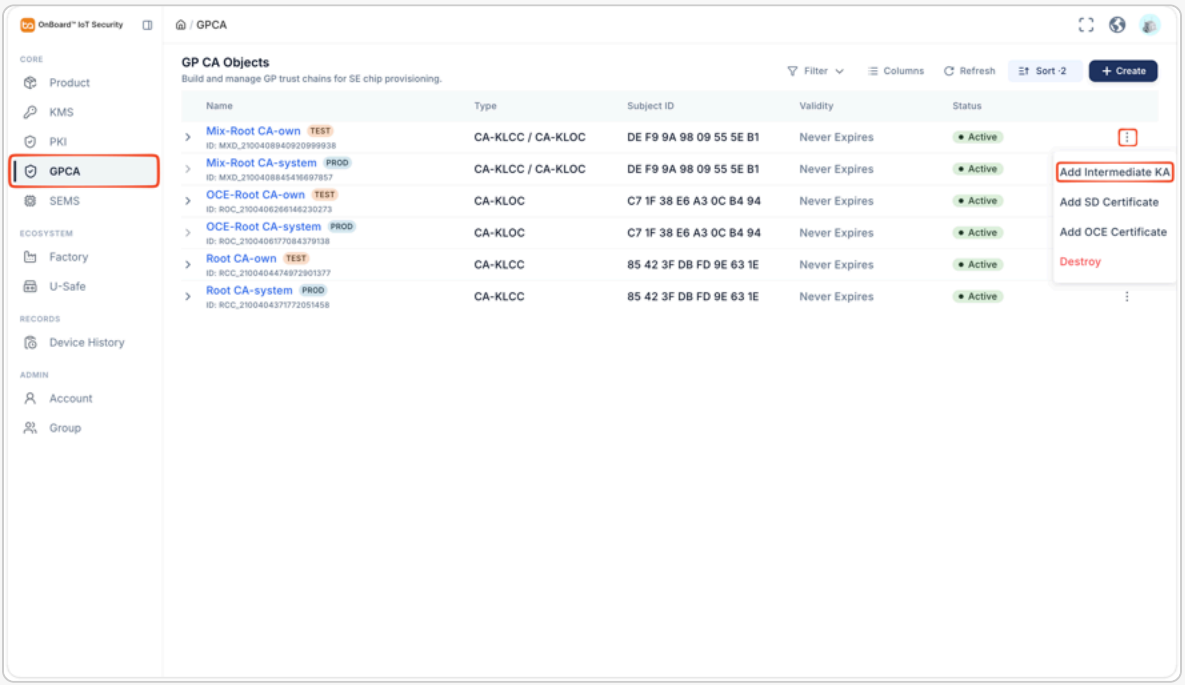
Information	Generate by System	Bring Your Own Root Certificate
Name	The Root CA name must be unique in the same environment.	
Chain	Select the **Mixed Chain**.	
Environment	Two environments can be selected: **Production** or **Test**.	
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.	N/A
Certificate Identifier (Tag 5F20)	Hex-encoded data for the certificate identifier. The system generates a 16-byte random value by default, which can be manually modified.	
Description	Provide additional information related to the Root CA, such as special requirements and important notes.	

2. After verifying that the information is correct, click **Create** to complete the Root CA creation.

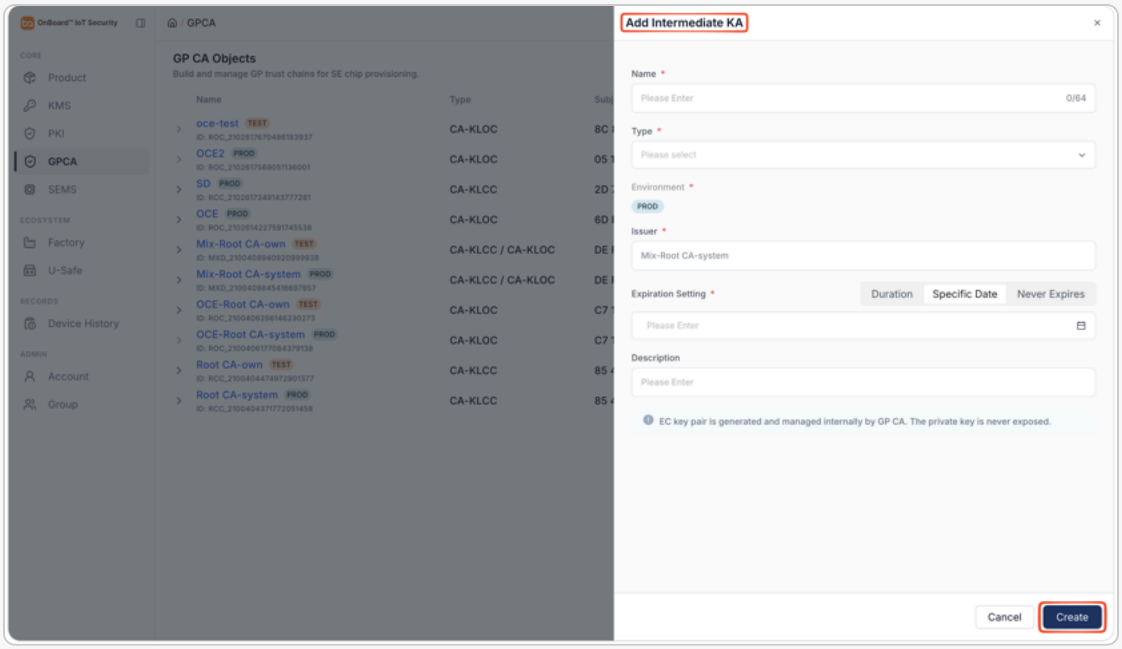
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

> **INFO**
>
> Before creating an Intermediate KA, please ensure that at least one Root CA has been created so that it can be selected and inherited during configuration.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding Root CA and select **Add Intermediate KA**.



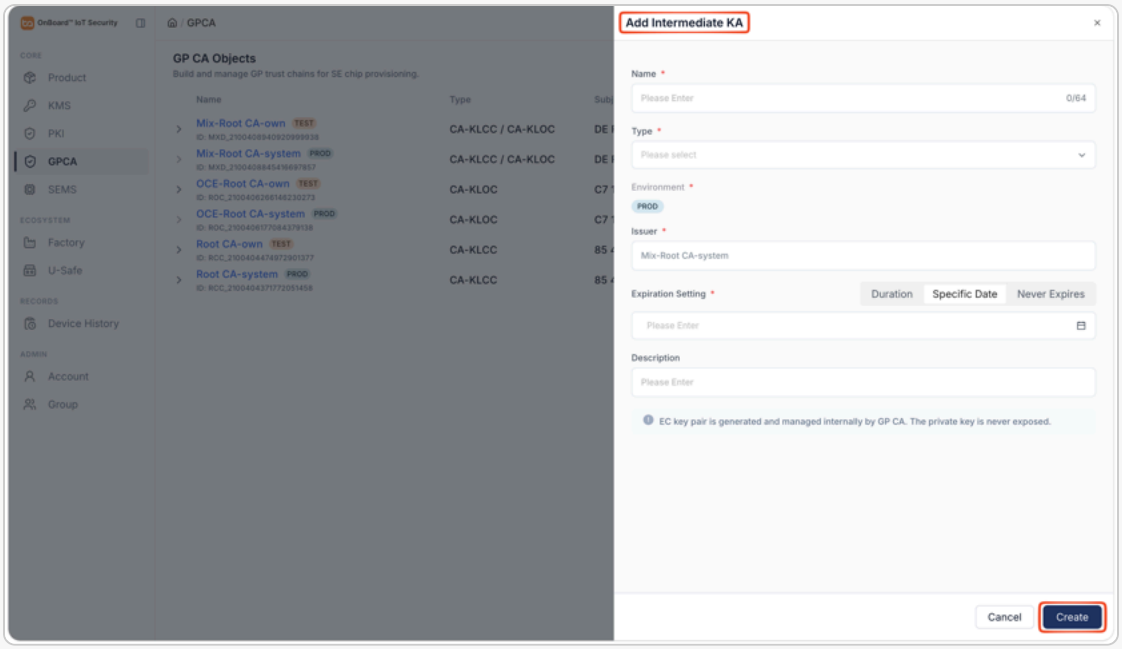
2. On the **Add Intermediate KA** panel, select and enter the basic information.
    - If the issuer of the intermediate KA is your own Root CA, you can select **Generate key pair (offline signing)** or **Import signed certificate** (your own intermediate KA) as needed



Information	Generate key pair (offline signing)	Import signed certificate
Certificate Data (7F21 Hex)	N/A	Enter the Hex certificate data in the GlobalPlatform certificate format (must start with 7F21). **Note**: The Issuer Identifier and Subject Identifier of the certificate must match.

Information	Generate key pair (offline signing)	Import signed certificate
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.	
Type	Two types can be selected: **KA-KLCC** or **KA-KLOC**.	
Environment	The environment is inherited from the Root CA.	
Issuer	The inherited Root CA.	
Description	Provide additional information related to the Intermediate KA, such as special requirements and important notes.	

- If the issuer of the intermediate KA is the system-generated Root CA



Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Type	Two types can be selected: **KA-KLCC** or **KA-KLOC**.
Environment	The environment is inherited from the Root CA.
Issuer	The inherited Root CA.
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed.
Description	Provide additional information related to the Intermediate KA, such as special requirements and important notes.

3. After verifying that the information is correct, click **Create** to complete the Intermediate KA creation.

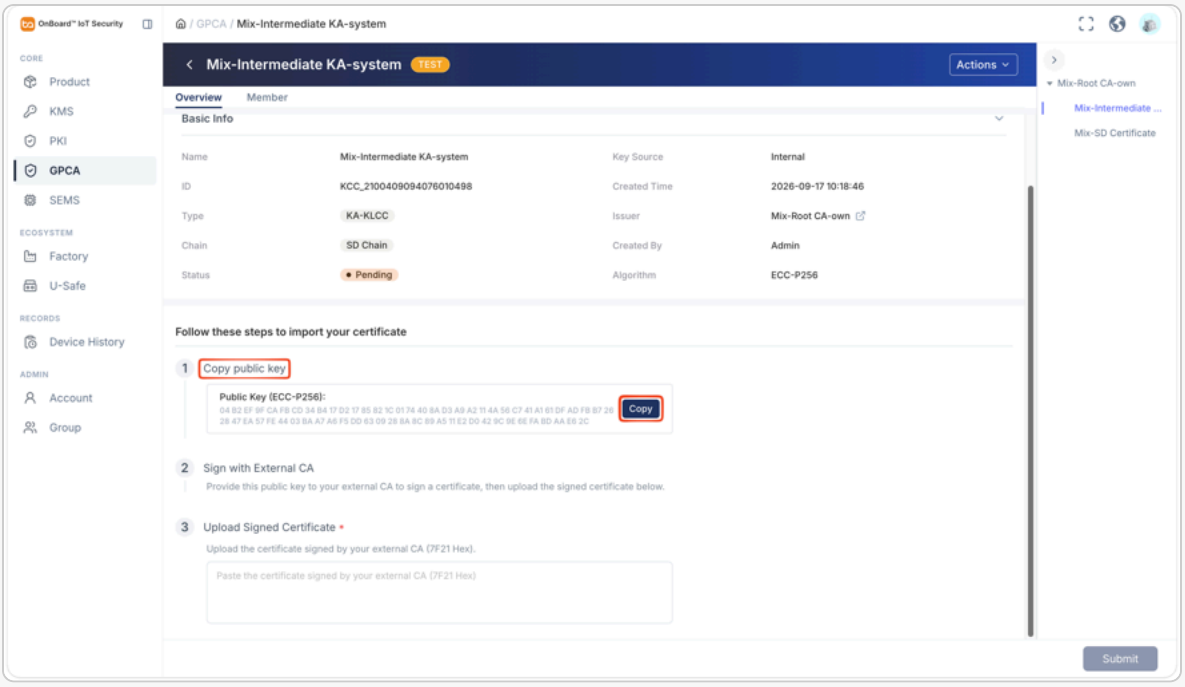
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an Intermediate KA, if the issuer is your own Root CA, you must complete the external issuance steps for the Intermediate KA. Before the external issuance is completed, the certificate will remain in the **Pending** status and can't be used.

External issuance steps for the Intermediate KA

> **TIP**
>
> When creating an Intermediate KA, if the issuer is your own root CA, refer to the following steps to complete the external issuance.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, and then click the corresponding Intermediate KA.

2. Locate the **Copy public key** section on the certificate page, click **Copy**. Then, use your external CA to sign this public key, thereby generating an intermediate CA certificate issued by the external CA.

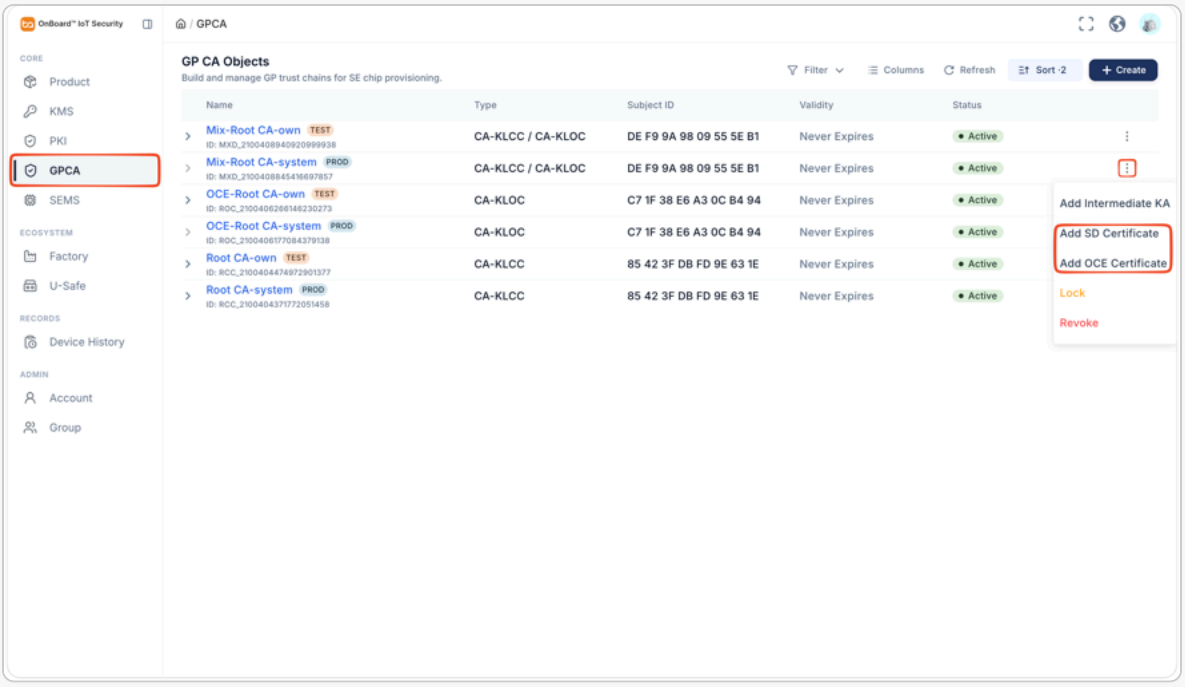


3. After issuance is complete, enter the certificate data (7F21 Hex) issued by the external CA in the **Upload Signed Certificate** section.

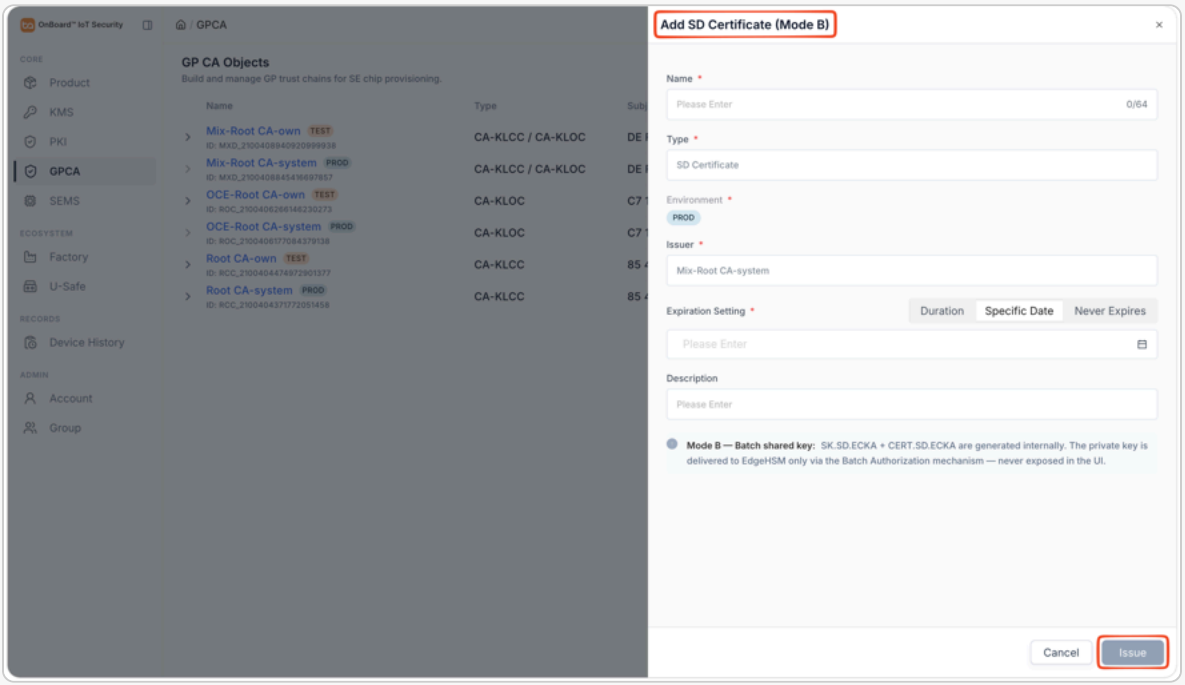
4. Click **Submit**. Once the configuration is completed, the Intermediate KA status will change to **Active**.

> **INFO**
>
> Before creating an SD or OCE certificate, please ensure that at least one Root CA or Intermediate KA has been created so that it can be selected and inherited during configuration.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, click the Options ⋮ icon for the corresponding root or Intermediate KA and select **Add SD Certificate** or **Add OCE Certificate**.



2. On the **Add SD Certificate (Mode B)** or **Add OCE Certificate** page, select and enter the basic information.



Description of SD or OCE certificate basic information:

Information	Description
Name	Within the same certificate chain, certificate names at the same hierarchy level must be unique.
Type	Default is **SD Certificate** or **OCE Certificate**.
Environment	The environment is inherited from the Root CA or Intermediate KA.
Issuer	The inherited Root CA or Intermediate KA.
Expiration Setting	You can choose **Duration**, **Specific Date**, or **Never Expires** to set the validity period as needed. **Note**: If the issuer is your own Root CA or Intermediate KA, the validity period will be inherited from the Root CA or Intermediate KA.
Description	Provide additional information related to the OCE certificate, such as special requirements and important notes.

3. After verifying that the information is correct, click **Issue** complete the SD or OCE certificate creation.

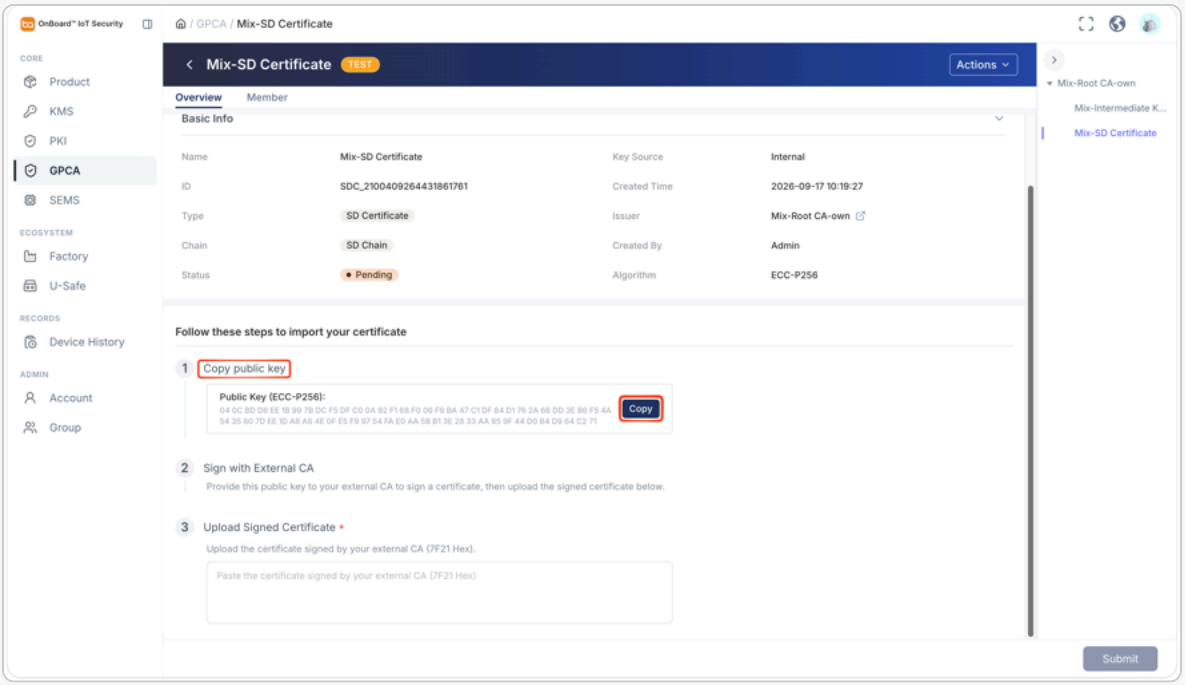
> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> When creating an SD or OCE certificate, if the issuer is your own Root CA or Intermediate KA, you must complete the external issuance steps for the SD or OCE certificate. Before the external issuance is completed, the template will remain in the **Pending** status and can't be used.

External issuance steps for the SD or OCE certificate

> **TIP**
>
> When creating an SD or OCE certificate, if the issuer is your own Root CA or Intermediate KA, refer to the following steps to complete the external issuance.

1. On the **GP CA Objects** page, expand the corresponding certificate chain, and then click the corresponding SD or OCE certificate.

2. Locate the **Copy public key** section on the certificate page, click **Copy**. Then, use your Root CA or Intermediate KA to sign the file, thereby generating an SD or OCE certificate signed by the Root CA or Intermediate KA.



3. After issuance is complete, enter the certificate data (7F21 Hex) issued by the external Root CA or Intermediate KA in the **Upload Signed Certificate** section.

4. Click **Submit**. Once the configuration is completed, the SD or OCE certificate status will change to **Active**.

Version: v3.4.0 (Latest)

How to check GlobalPlatform certificates in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Check basic information
- Check members

Prerequisites

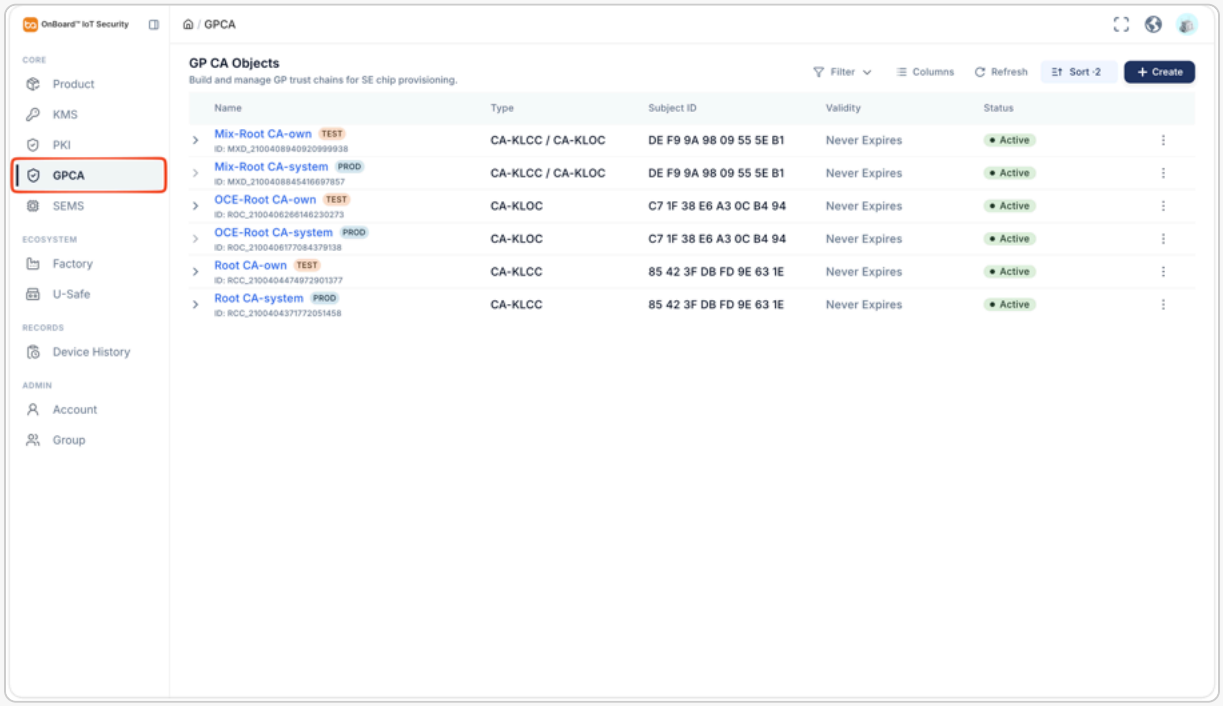
Before getting started, please ensure that:

- You have OBIS role permissions as a System Manager or SE Resource Manager.
- You have permissions for the corresponding certificate.

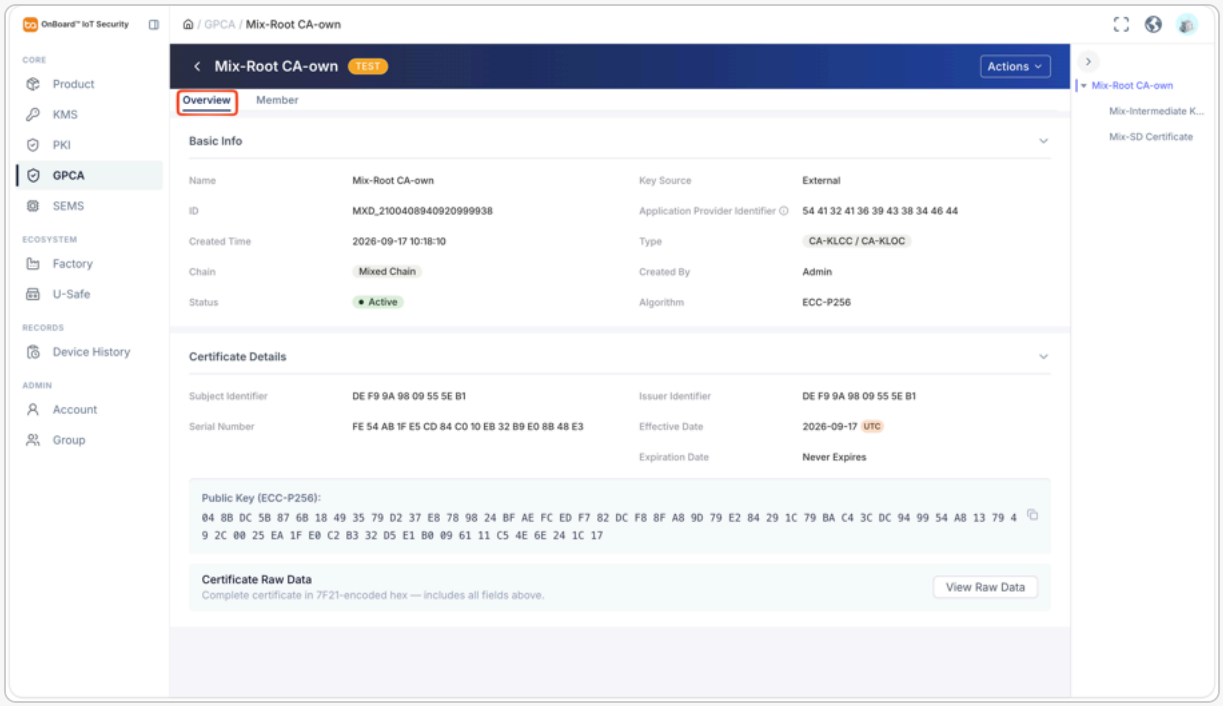
Check basic information

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain, and then select the corresponding certificate.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



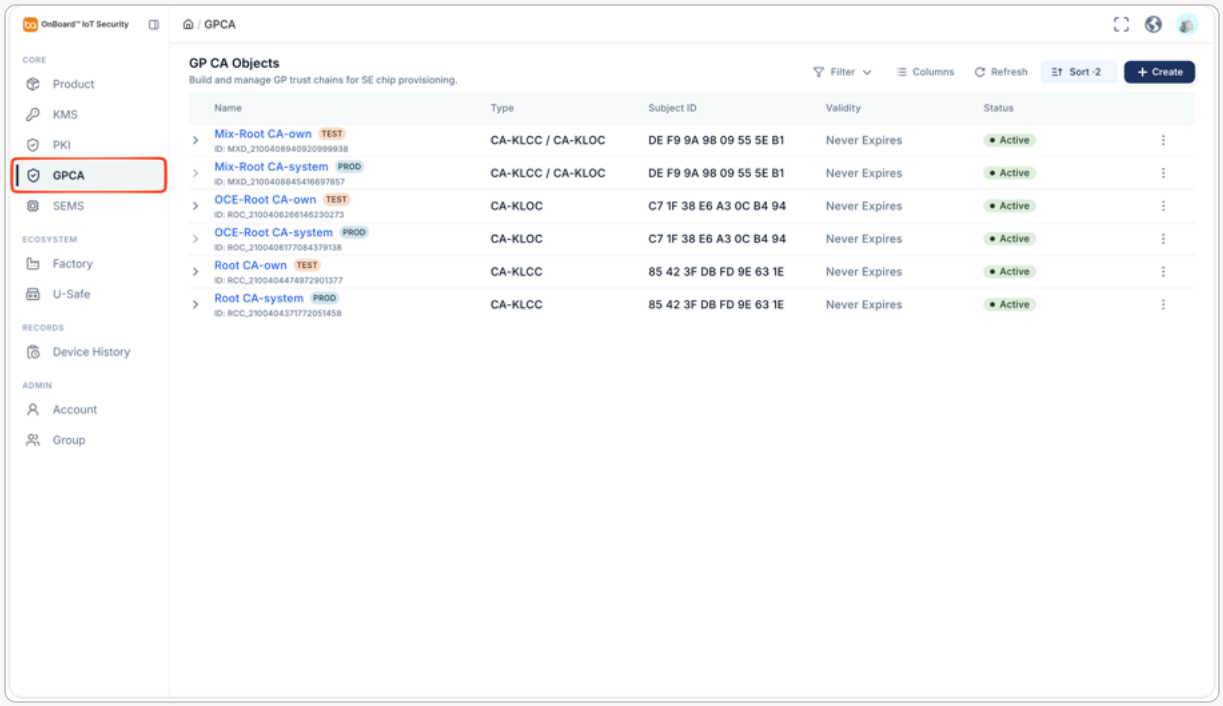
3. On the **Overview** tab, you can check the certificate-related information (**Basic Info** and **Certificate Details**).



Check members

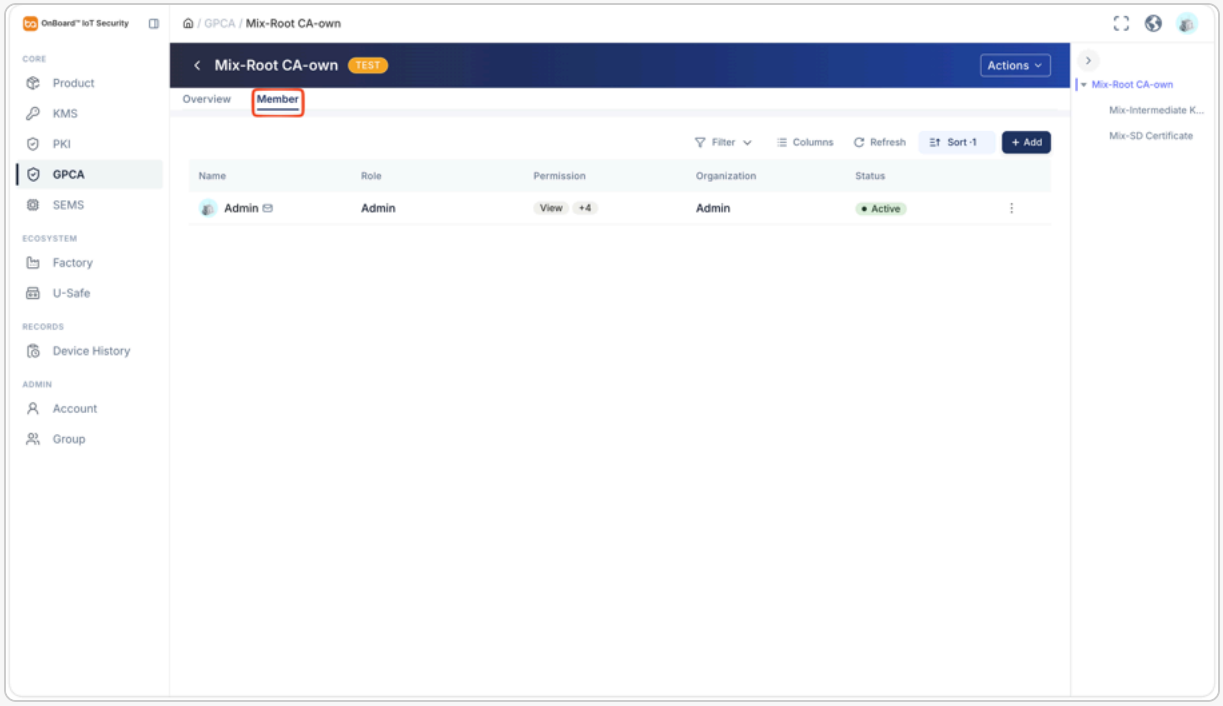
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain, and then select the corresponding certificate.



3. Select the **Member** tab, you can check the user permissions for the certificate (such as **Name**, **Role**, and **Permission**).

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.


OnBoard™ IoT Security
/ GPCA / Mix-Root CA-own
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
Mix-Root CA-own
TEST
Actions
Overview
Member
Filter
Columns
Refresh
Sort -1
+ Add
Name
Role
Permission
Organization
Status
Admin
Admin
View +4
Admin
Active
Mix-Root CA-own
Mix-Intermediate K...
Mix-SD Certificate

Version: v3.4.0 (Latest)

How to manage GlobalPlatform certificates in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Manage certificate permissions
- Lock or unlock a certificate
- Discard a certificate
- Revoke a certificate
- Destroy a certificate

Prerequisites

Before getting started, please ensure that:

- You have OBIS role permissions as a System Manager or SE Resource Manager.
- You have permissions for the corresponding certificate.

Manage certificate permissions

> **TIP**
>
> By default, the certificate creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

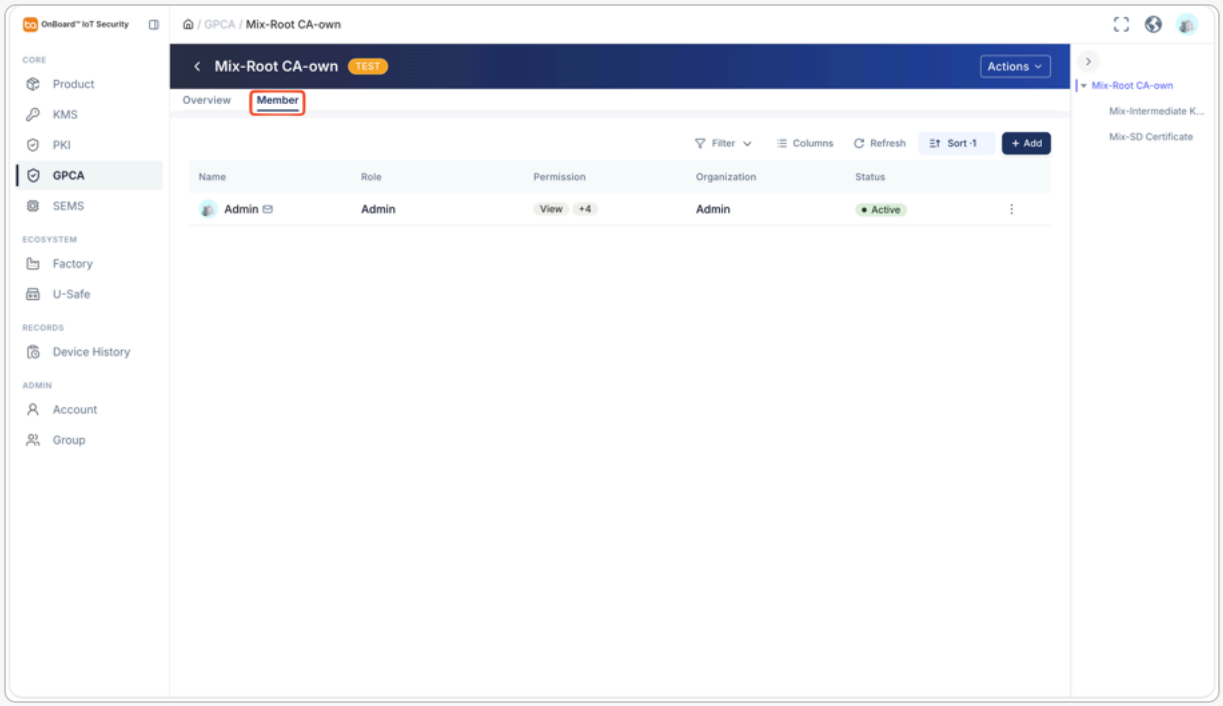
You can assign different operational permissions for the certificate to different members. The scope and descriptions of these permissions are as follows:

Permissions	Applicable certificates	Description
View	All certificates	View certificate details (read-only).
Add Member	All certificates	Add members to this certificate and assign them permissions that do not exceed your own permissions.
Use	All certificates (excluding SD certificates)	CA / KA can be used to issue corresponding subordinate certificates; certificates in an OCE chain with this permission can be referenced in the SCP11c configuration of an SE Profile.

Permissions	Applicable certificates	Description
Create Authorization	Certificates in an SD chain	Certificates in an SD chain with this permission can be referenced in the SCP11c configuration of an SE Profile.
Manage Status	All certificates	Lock, unlock, or revoke a certificate.
Destroy	All certificates	Destroy certificates that have been revoked or have expired.

You can adjust and set user permissions for certificates by following these steps:

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain and then select the corresponding certificate.
3. On the certificate page, you can manage the user permissions for the certificate on the **Member** tab.

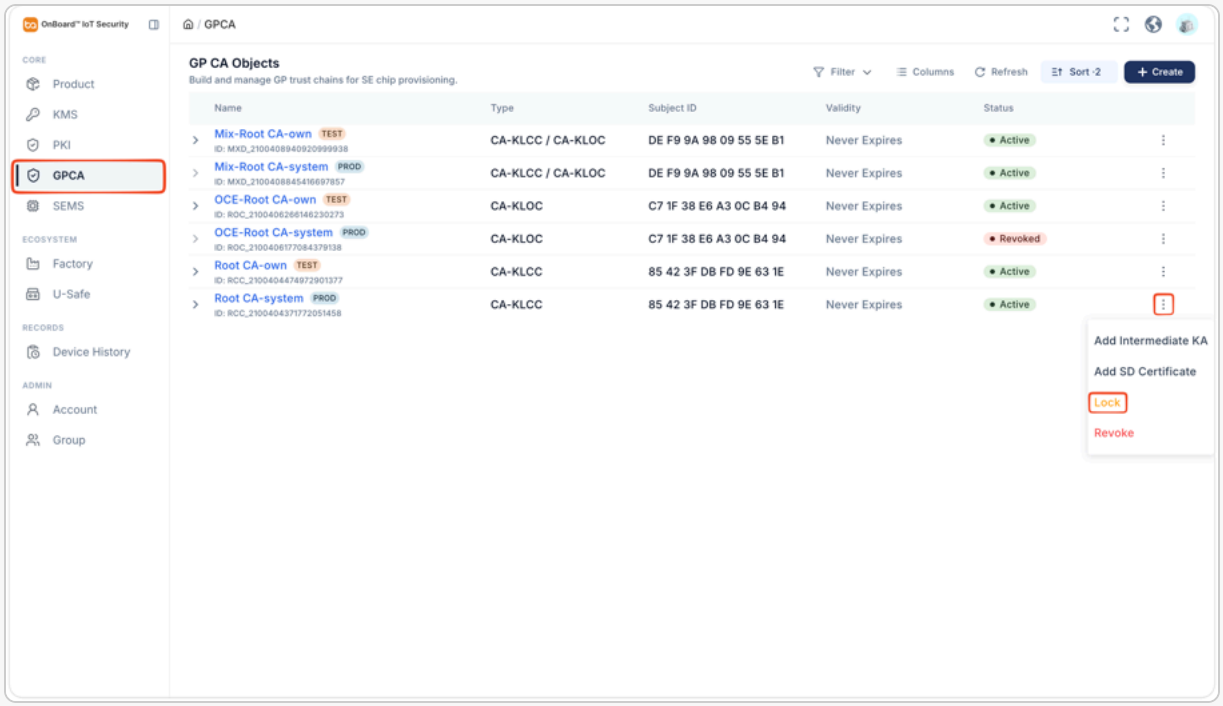


Lock or unlock a certificate

> **TIP**
>
> Once the certificate is locked, it can't be referenced by new configurations; existing references remain unaffected. Once unlocked, the certificate can be referenced as usual.

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding certificate and select **Lock** or **Unlock**. Click **Confirm** to lock or unlock the certificate. When locking a certificate, you can optionally provide a reason.



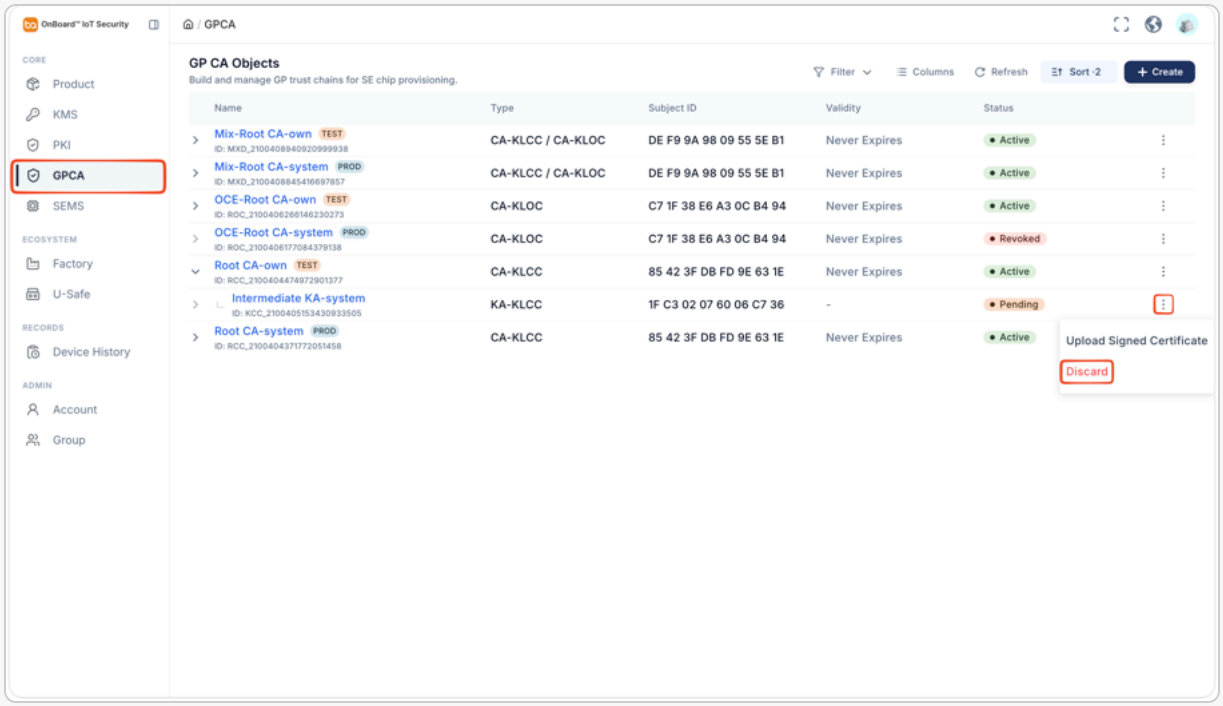
Discard a certificate

> **WARNING**
>
> Discarded certificates cannot be recovered. Please proceed with caution.

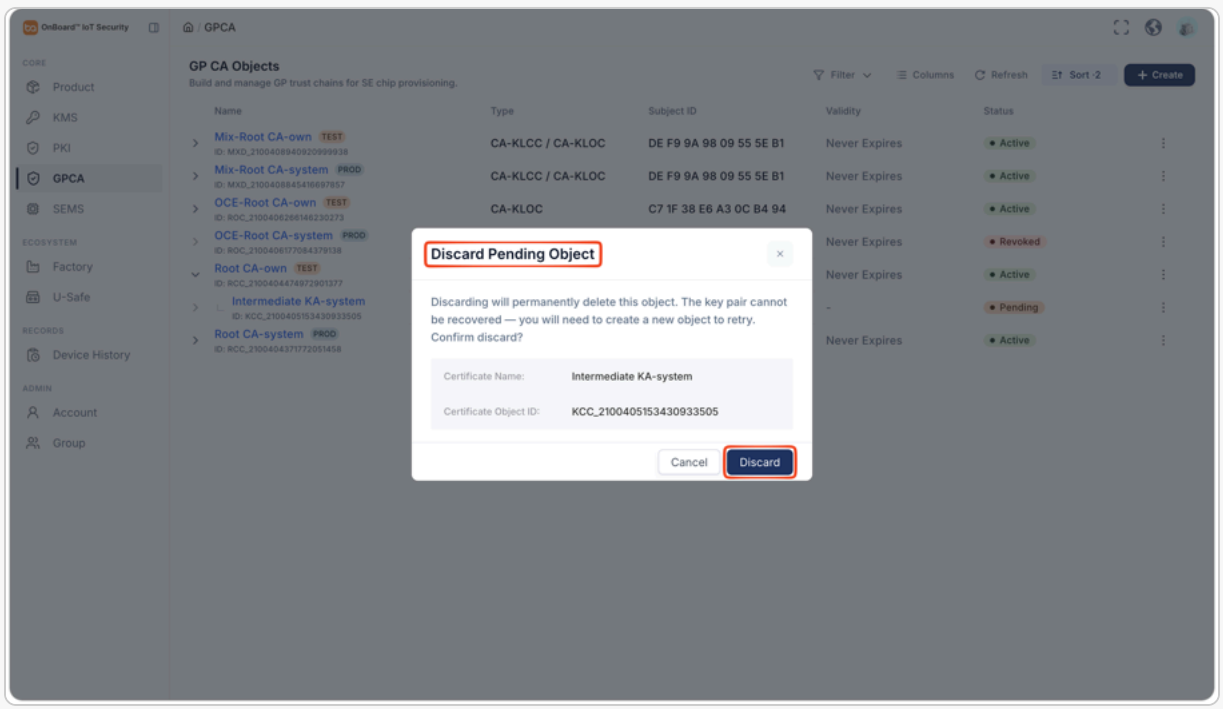
> **TIP**
>
> Only certificates with a status of **Pending** can be discarded.

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding certificate and select **Discard**.



3. In the **Discard Pending Object** window, click **Discard** to discard the certificate.

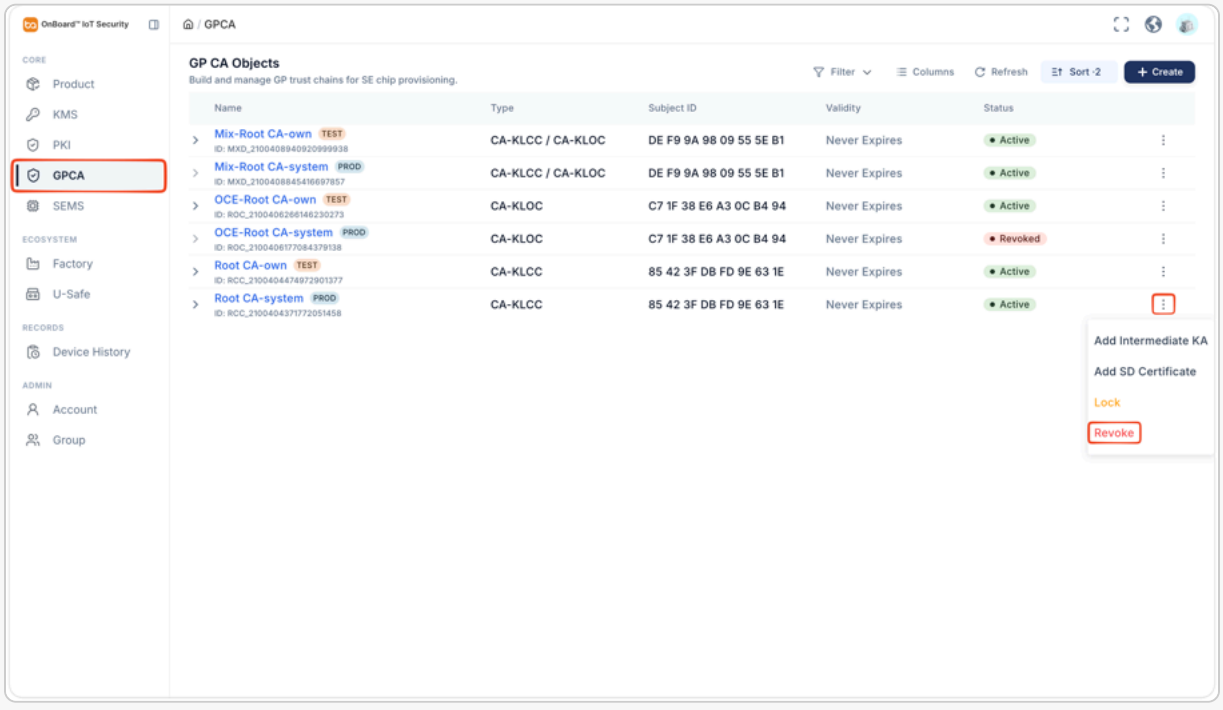


Revoke a certificate

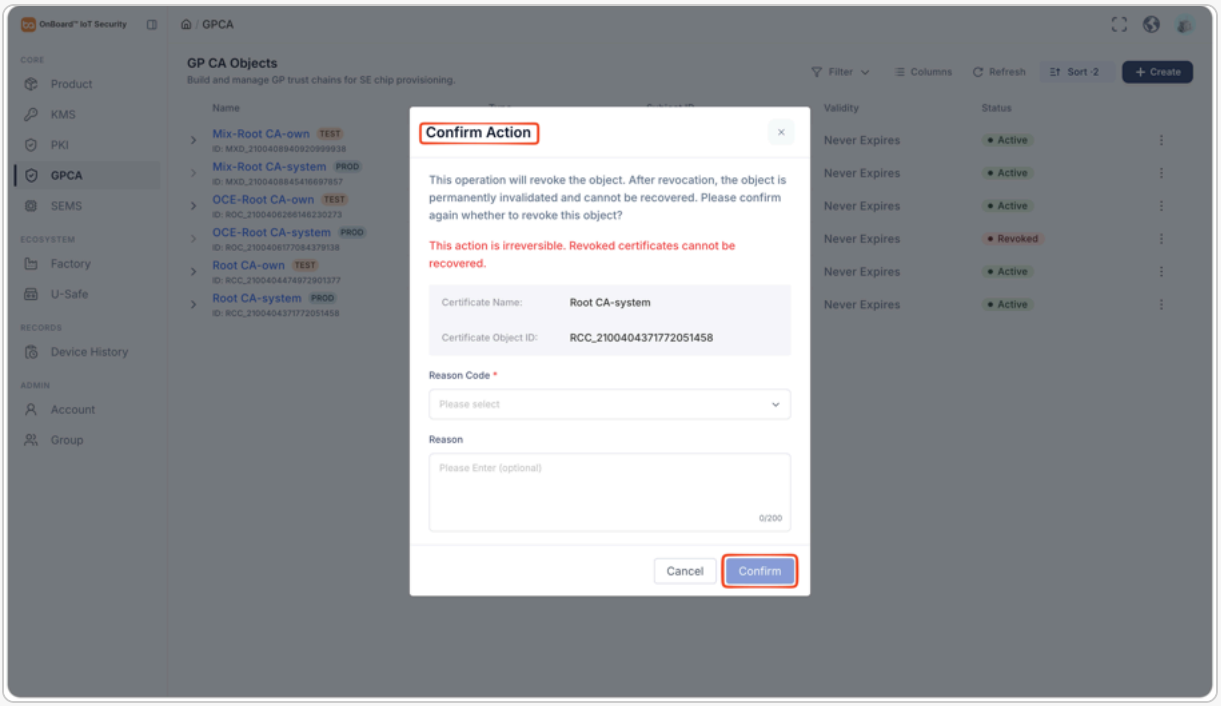
> **WARNING**
>
> Revoked certificates will become permanently invalid. Please proceed with caution.

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding certificate and select **Revoke**.



3. In the **Confirm Action** window, select the **Reason Code** and enter the **Reason**, then click **Confirm** to revoke the certificate.



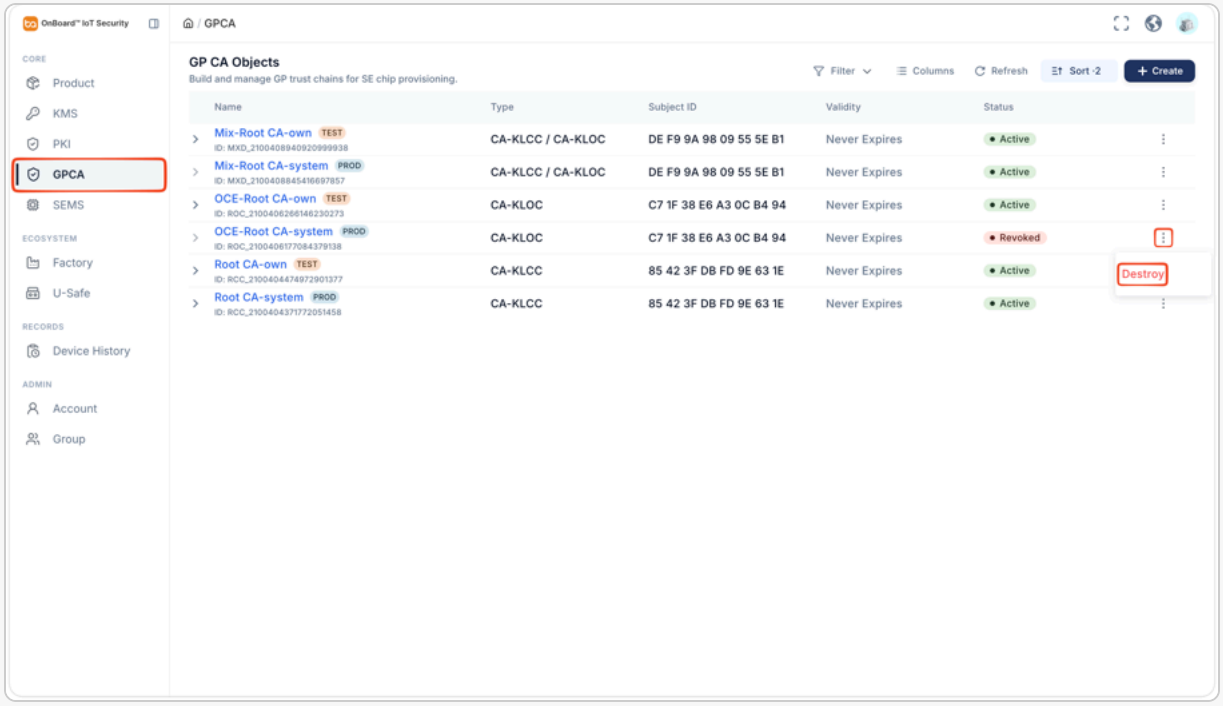
Destroy a certificate

> **WARNING**
>
> Destroyed certificates cannot be recovered. Please proceed with caution.

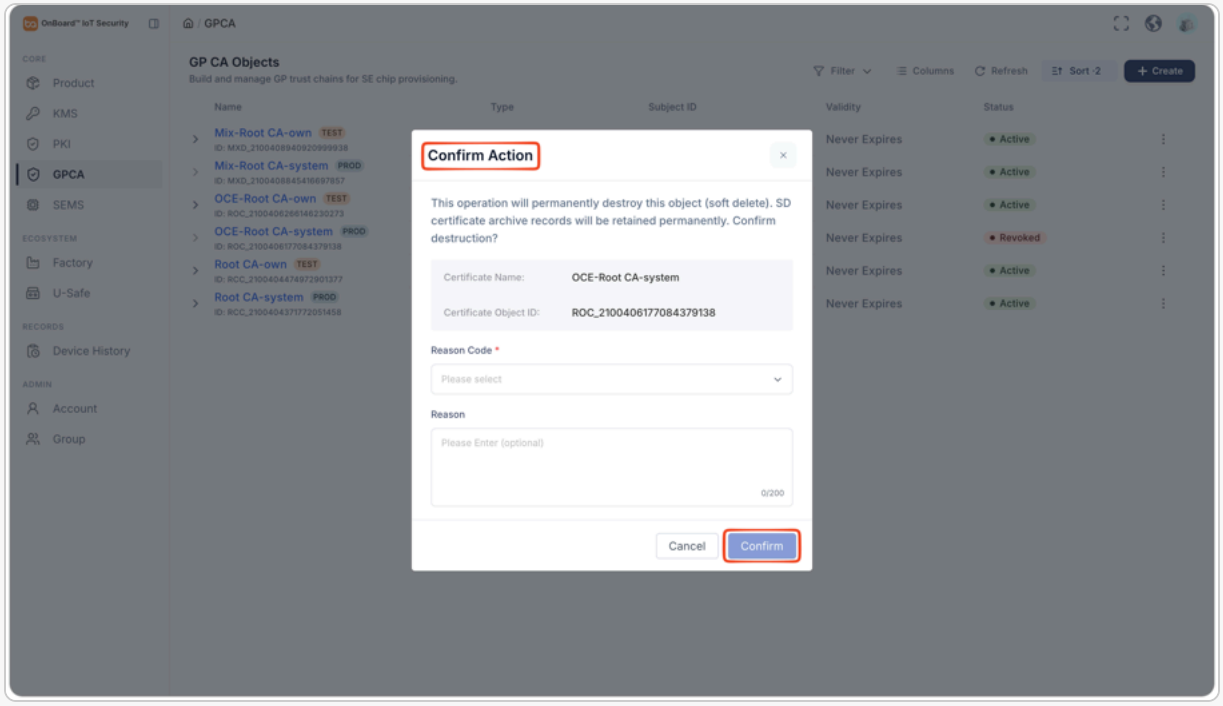
> **TIP**
>
> Only certificates with a status of **Revoked** or **Expired** can be destroyed.
>
> Before destroying a certificate, ensure that all its sub-certificates are in the **Revoked** or **Expired** status. If any sub-certificates are in the **Active**, **Locked**, or **Pending** status, you will see the message "This object still has Active, Locked, or Pending Signature sub-certificates. Please revoke, discard, or wait for them to expire before destroying this object".

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **GPCA**. Expand the corresponding certificate chain, and then click the Options ⋮ icon for the corresponding certificate and select **Destroy**.



3. In the **Confirm Action** window, select the **Reason Code** and enter the **Reason**, then click **Confirm** to destroy the certificate.


OnBoard™ IoT Security
GPCA
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
GP CA Objects
Build and manage GP trust chains for SE chip provisioning.
Filter
Columns
Refresh
Sort · 2
+ Create
Name
Type
Subject ID
Validity
Status
Mix-Root CA-own TEST
Mix-Root CA-system PROD
OCE-Root CA-own TEST
OCE-Root CA-system PROD
Root CA-own TEST
Root CA-system PROD
Never Expires
Active
Revoked
Confirm Action
This operation will permanently destroy this object (soft delete). SD certificate archive records will be retained permanently. Confirm destruction?
Certificate Name:
OCE-Root CA-system
Certificate Object ID:
ROC_2100406177084379138
Reason Code *
Please select
Reason
Please Enter (optional)
0/200
Cancel
Confirm

Version: v3.4.0 (Latest)

Overview of SEMS in OnBoard™ IoT Security

The SEMS (Secure Element Management System) in OBIS (OnBoard IoT Security) is responsible for managing SE (Secure Element) profile configurations. It defines the factory state, target provisioning configuration, and secure communication parameters of the secure element for provisioning on the production line. It is mainly used for:

- Creating and managing SE Profiles for use within product workspaces.
- Integrating KMS (Key Management System) keys and GP CA certificates to configure SCP03 and SCP11c secure channels.
- Encapsulating external GP scripts using the SCP11c protocol, resulting in secure scripts that can be executed offline.

The following table summarizes the core capabilities of the SEMS:

Capability	Description
SE Profile Management	• Manage the creation, configuration, and lifecycle of SE Profiles • Configure elements such as ISD, AMSD, SSD, CAP, and Instances • Support freezing profiles after activation and deleting drafts.

Capability	Description
Secure Channel Configuration	• Reference SCP03 keys via KMS without storing plaintext keys • Reference GP CA certificates to configure SCP11c secure channels
SCP11c Script Encapsulation	• Receive external GP scripts and invoke the OCE (Off-Card Entity) private key service of the GP CA to complete secure encapsulation • Output secure scripts for offline execution without exposing the underlying GP command content
Collaboration and Permission Management	• Manage collaborators for SE Profiles and their associated object permissions
Production Integration	• Provide SE Profile definitions to the product workspace • Provide interfaces for configuration, status, and production authorization
Security State Synchronization	• Lock or revoke the relevant profiles based on the status of upstream certificates or keys • Automatically restore profiles to the **Active** state once all locking conditions are cleared

The SEMS manages the design-time configuration of SEs; It is not responsible for real-time management on the device side.

Version: v3.4.0 (Latest)

How to create an SE Profile in OnBoard™ IoT Security

This article will guide you on how to create an SE Profile in OnBoard™ IoT Security (OBIS).

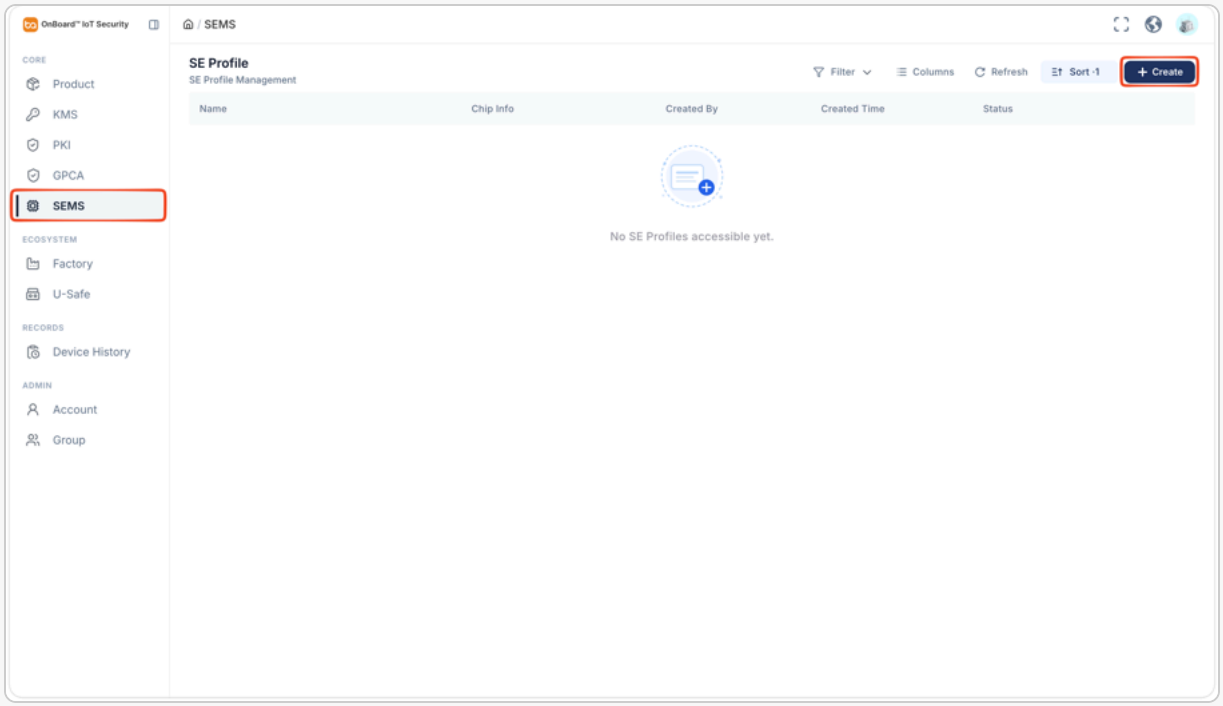
Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager or SE Resource Manager.

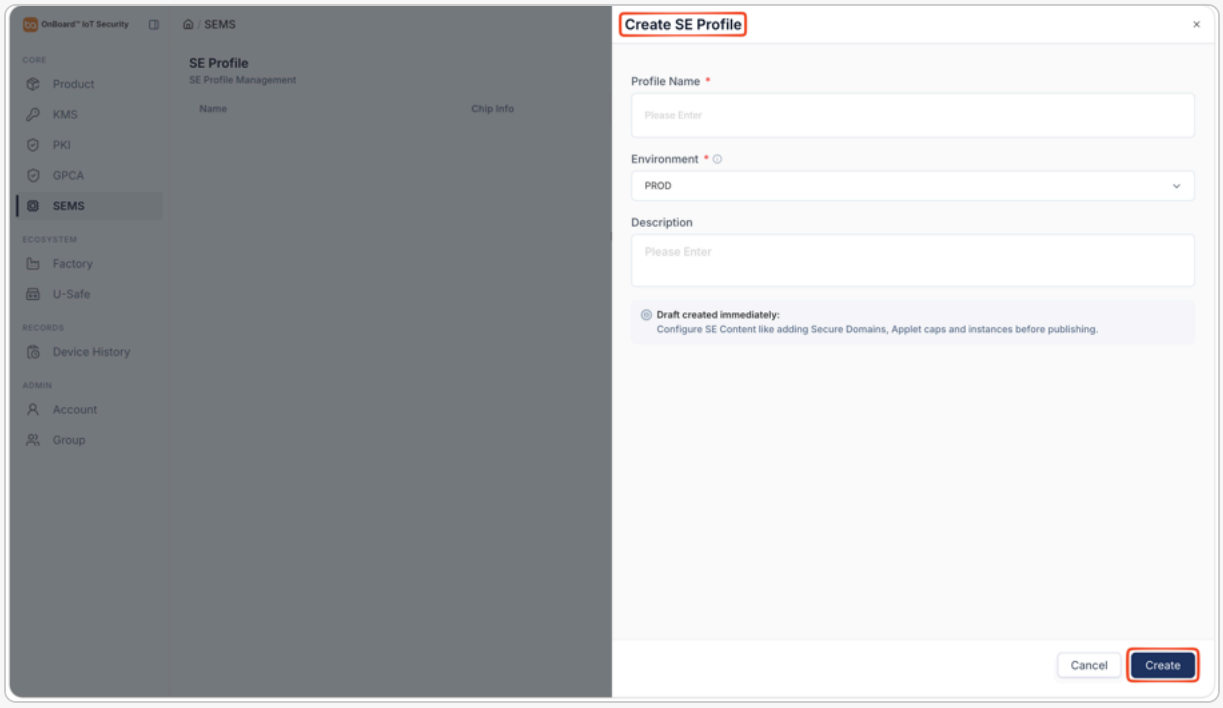
Instructions

> **TIP**
>
> After an SE Profile is created and configured, it can be selected when configuring an SE Profile for a product.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then click **Create** on the **SE Profile** page.



3. In the **Create SE Profile** panel, select and enter the SE Profile basic information.



Description of SE Profile basic Information:

Information	Mandatory	Description
Profile Name	Yes	The SE Profile name must be unique in the same environment.
Environment	Yes	Two environments can be selected: **PROD** and **TEST**.
Description	No	Provide additional information related to the SE Profile, such as special requirements and important notes.

4. Click **Create** to complete the creation of the SE Profile.

> **TIP**
>
> By default, the SE Profile creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> After an SE Profile is created, its initial status is **Draft**. Once it's published, the SE Profile status will change to **Active**.

Version: v3.4.0 (Latest)

How to configure and publish an SE Profile in OnBoard™ IoT Security

> **TIP**
>
> You can configure the SE Profile only when it is in the **Draft** state.

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Configure basic information
- Configure Initial Profile
- Configure Post-Provision Profile
- Publish the SE Profile

Prerequisites

Before getting started, please ensure that:

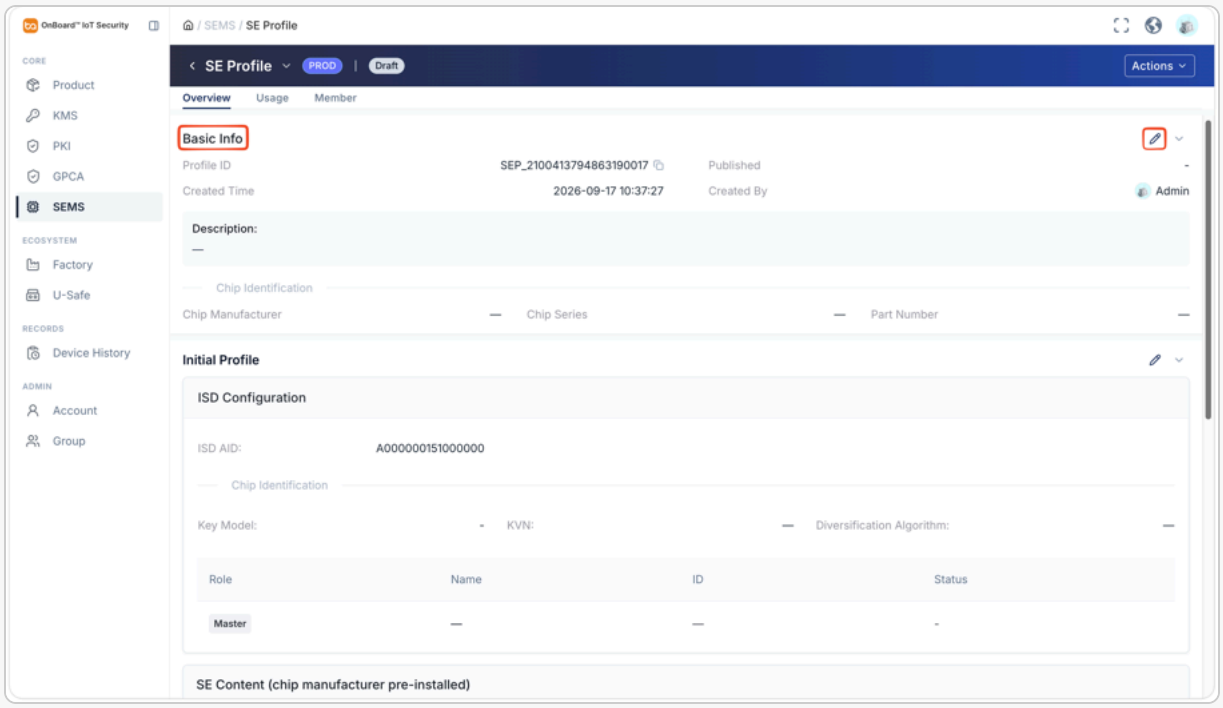
- You have OBIS role permissions as a System Manager or SE Resource Manager.
- You have permissions for the corresponding SE Profile.
- The certificates and keys have already been created.

Configure basic information

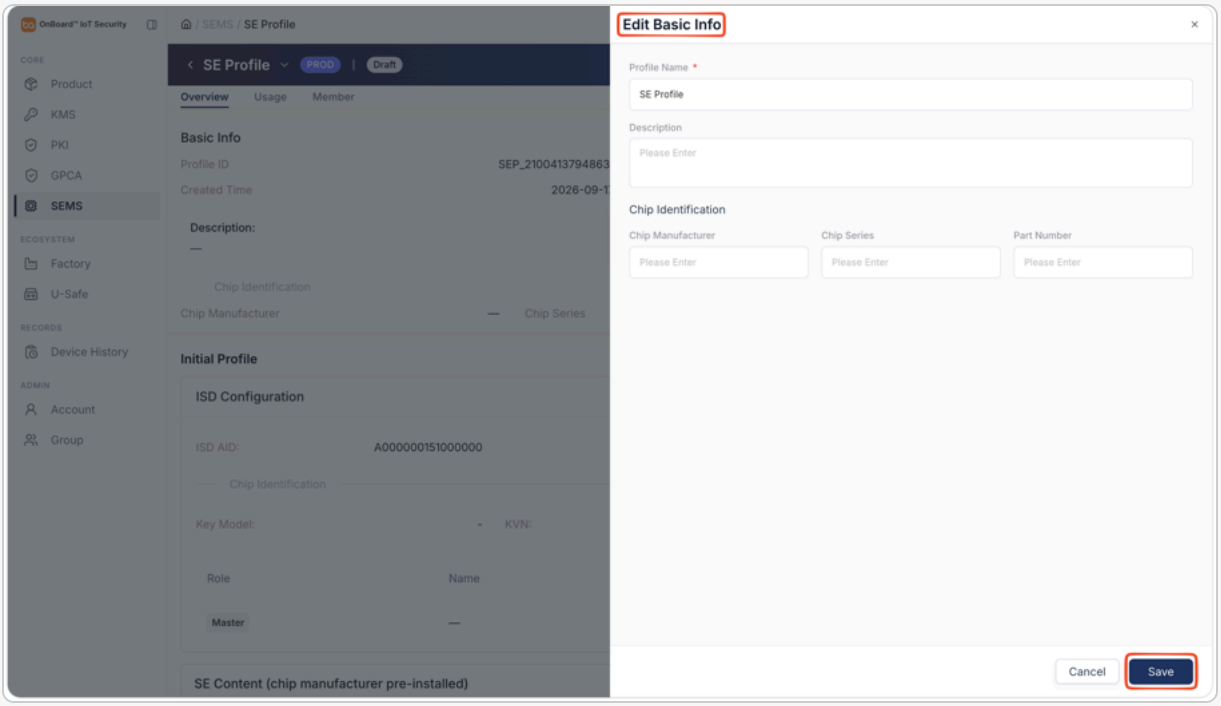
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile to navigate to the SE Profile page.

3. In the **Basic Info** section of the SE Profile page, click the Edit icon.



4. In the **Edit Basic Info** panel, verify the SE Profile name and description, and then enter the corresponding chip identification (chip manufacturer, series, and part number).



5. After verifying that the information is correct, click **Save**.

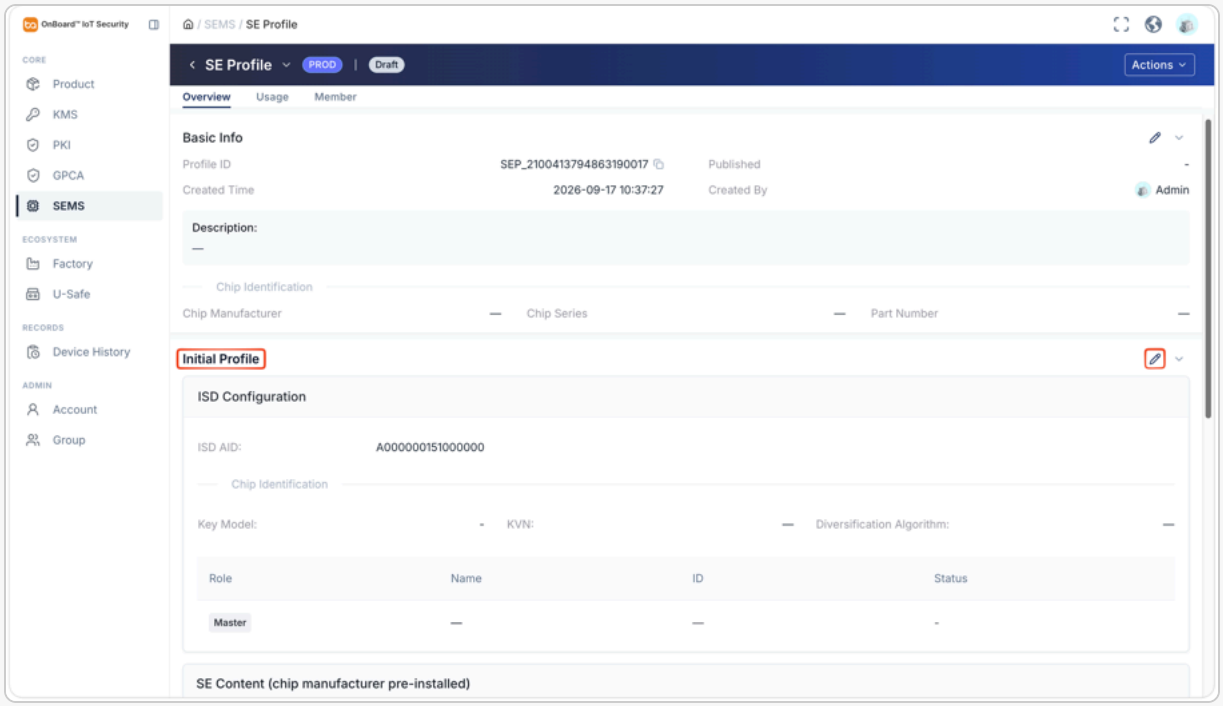
Configure Initial Profile

1. Sign in to OBIS.

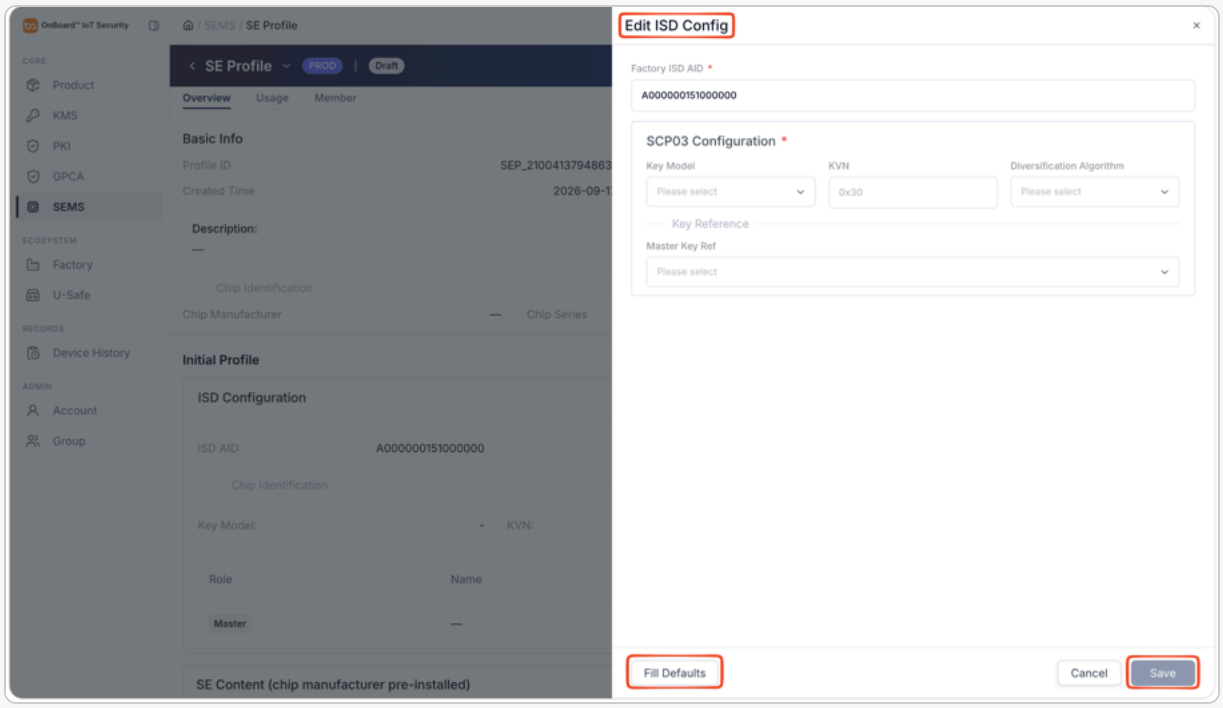
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile to navigate to the SE Profile page.

Configure ISD

1. In the **Initial Profile** section, click the Edit icon.



2. In the **Edit ISD Config** panel, enter and select the relevant information. You may also click **Fill Defaults**.



Description of the ISD configuration information:

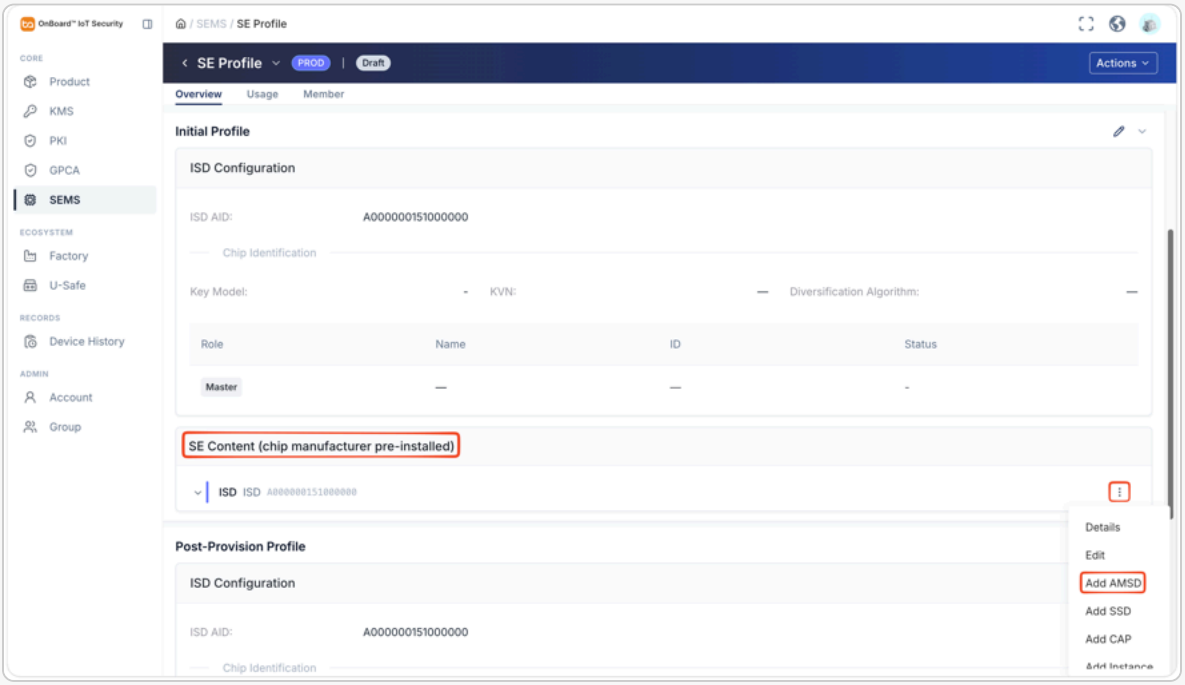
Information	Description
Factory ISD AID	The AID (Application Identifier) used to identify the Factory ISD (Issuer Security Domain) on the SE chip, which remains constant throughout the chip's lifecycle. The default value is **A000000151000000**.
Key Model	Two key models can be selected: **Single Master Key** and **Triple Keys (ENC/MAC/DEK)**. The default setting is **Single Master Key**.
KVN	The key version number used within the current security domain to establish an SCP03 secure channel. The default value is **0x30**.
Diversification Algorithm	Three diversification algorithms can be selected: **EMV_CPS**, **AES_CMAC**, and **None**. The default setting is **EMV_CPS**.
Master Key Ref	Select the key that has been created in KMS. **Note**: When the key model is **Triple Keys (ENC/MAC/DEK)**, you must specify the ENC key, MAC key, and DEK key individually.

3. After verifying that the information is correct, click **Save**.

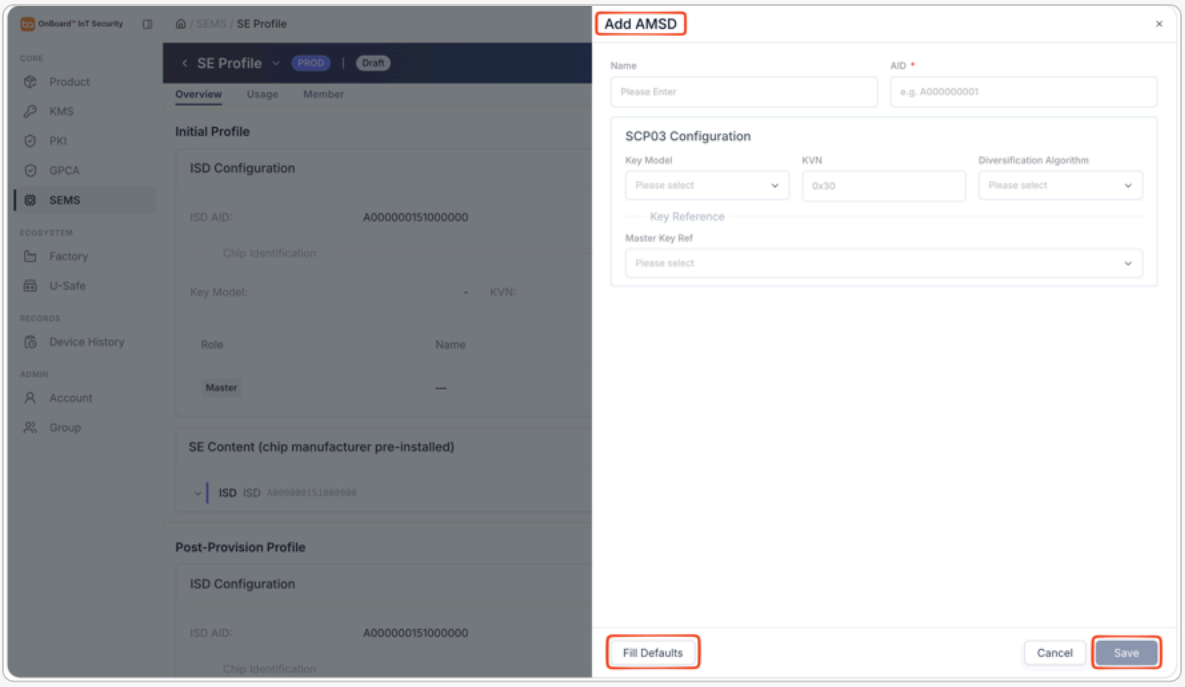
Configure SE Content

Configure AMSD | Configure SSD | Configure CAP | Configure Instance

1. In the **SE Content (chip manufacturer pre-installed)** subsection, click the Options ⋮ icon for the ISD and then select **Add AMSD**.



2. In the **Add AMSD** panel, enter and select the relevant information. You may also click **Fill Defaults**.



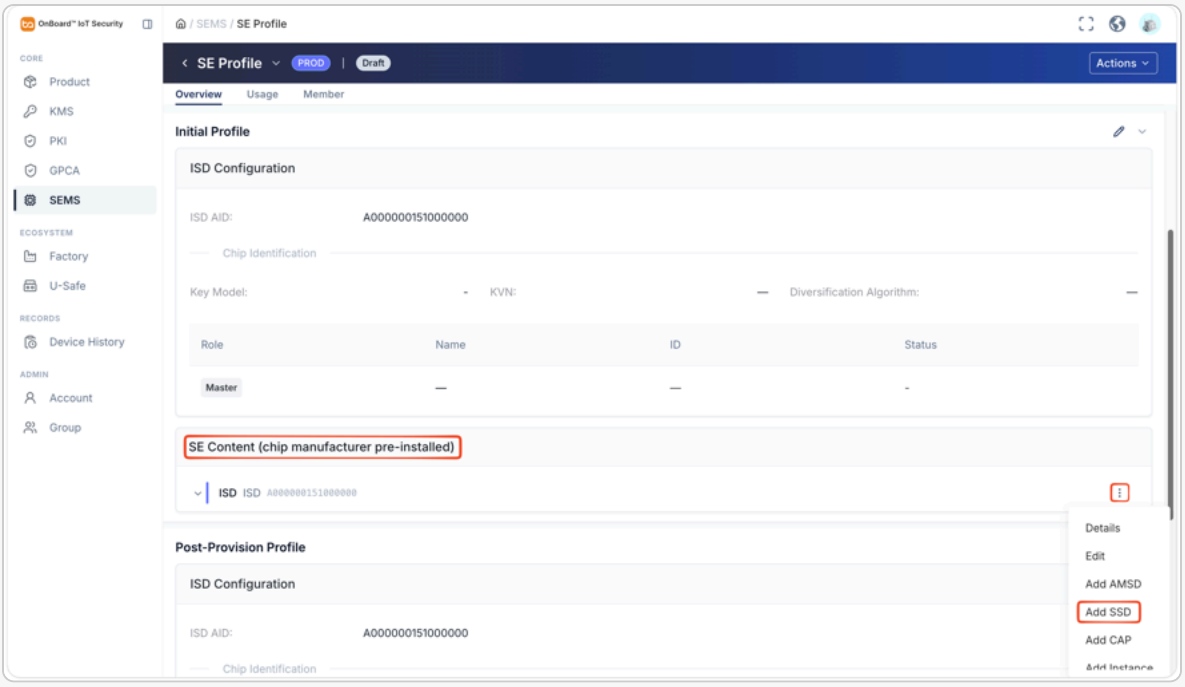
Description of the AMSD configuration information:

Information	Description
Name	The AMSD (Application Management Security Domain) name must be unique.
AID	The AID (Application Identifier) used to identify an AMSD must be unique.
Key Model	Two key models can be selected: **Single Master Key** and **Triple Keys (ENC/MAC/DEK)**. The default setting is **Single Master Key**.

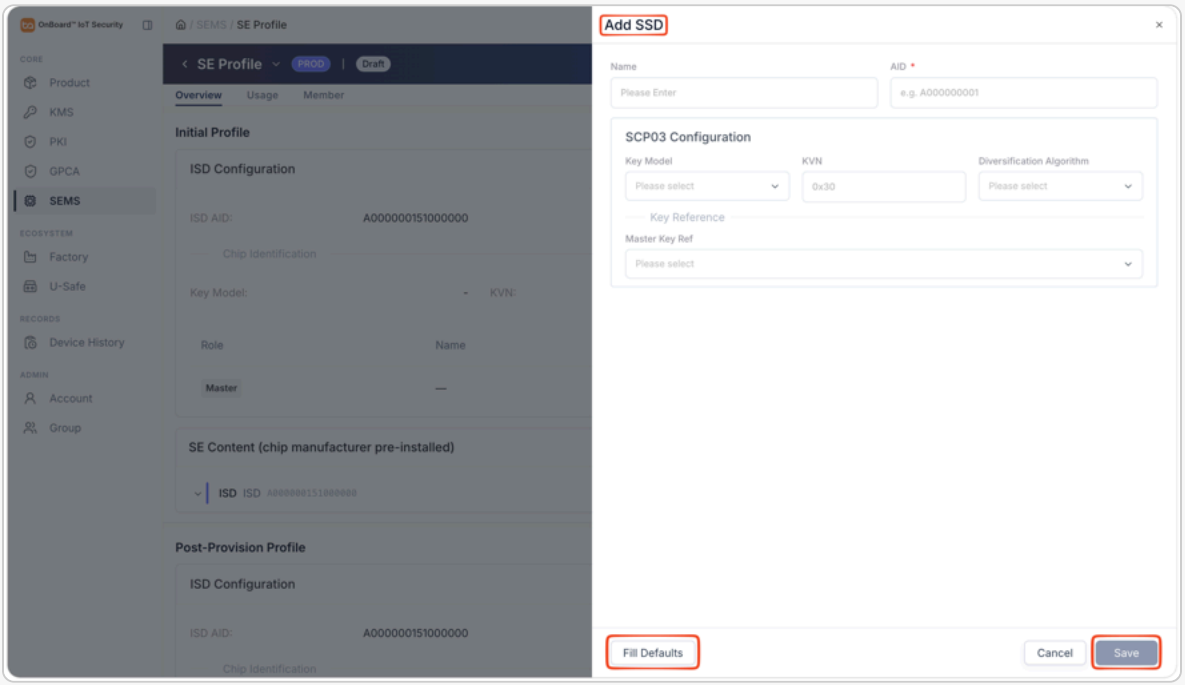
Information	Description
KVN	The key version number used within the current security domain to establish an SCP03 secure channel. The default value is **0x30**.
Diversification Algorithm	Three diversification algorithms can be selected: **EMV_CPS**, **AES_CMAC**, and **None**. The default setting is **EMV_CPS**.
Master Key Ref	Select the key that has been created in KMS. **Note**: When the key model is **Triple Keys (ENC/MAC/DEK)**, you must specify the ENC key, MAC key, and DEK key individually.

3. After verifying that the information is correct, click **Save**.

1. In the **SE Content (chip manufacturer pre-installed)** subsection, click the Options ⋮ icon for the ISD or the corresponding AMSD, and then select **Add SSD**.



2. In the **Add SSD** panel, enter and select the relevant information. You may also click **Fill Defaults**.

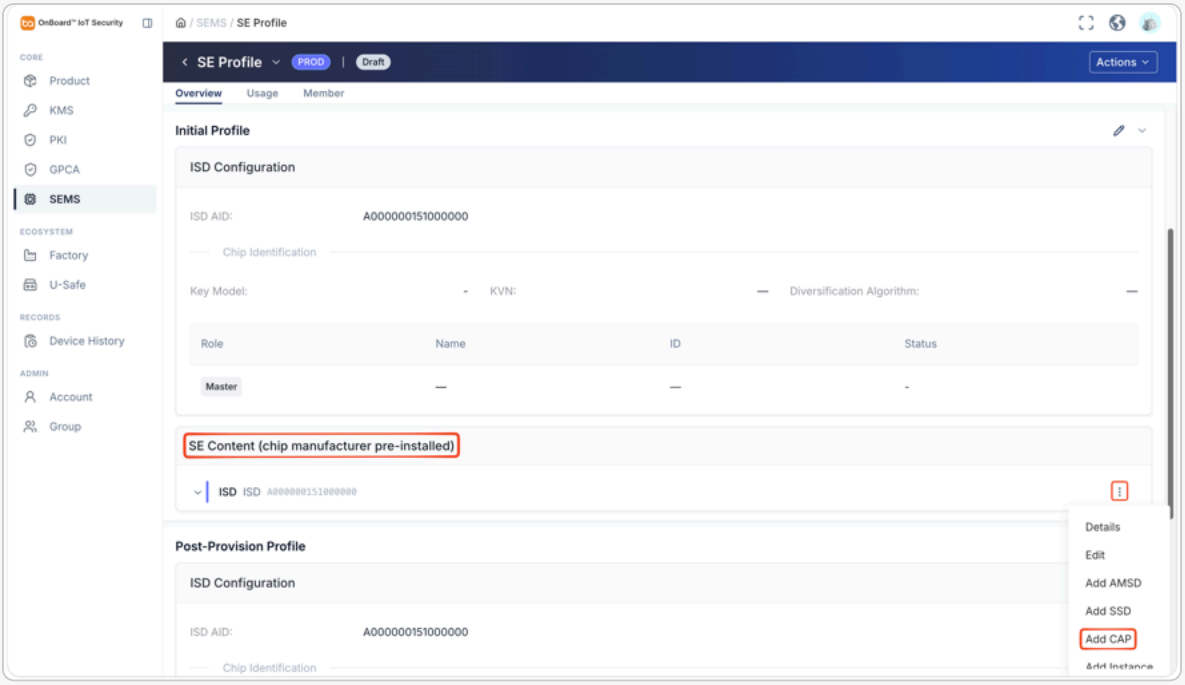


Description of the SSD configuration information:

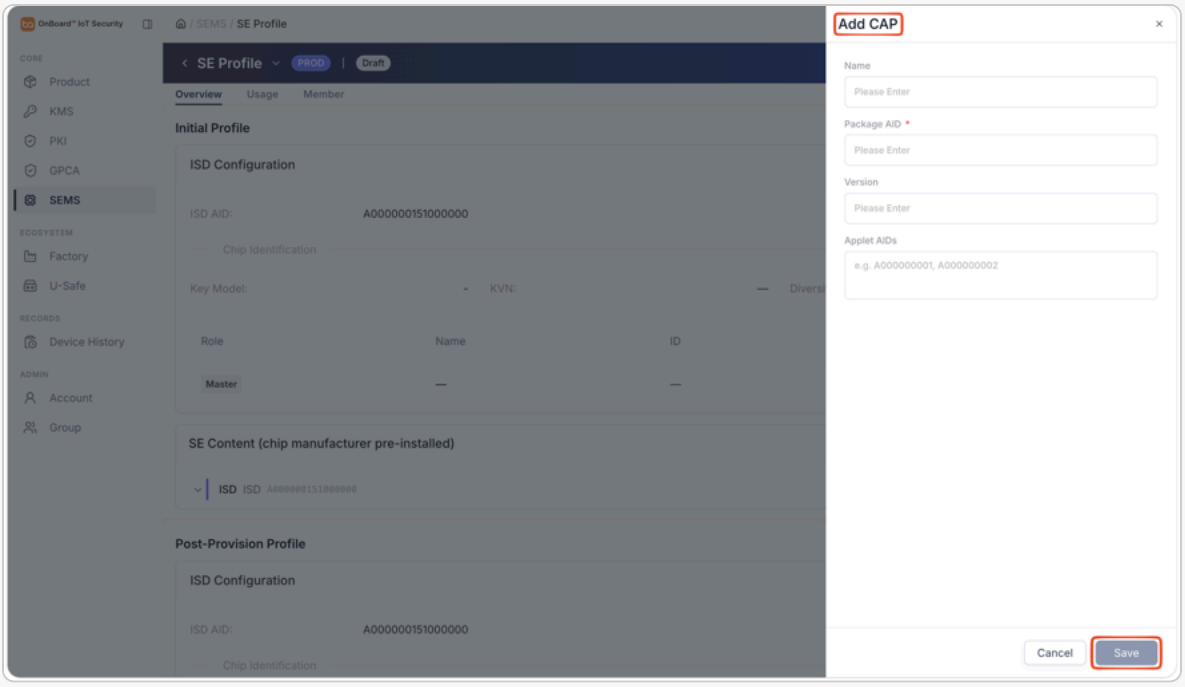
Information	Description
Name	The SSD (Supplementary Security Domain) name must be unique.
AID	The AID (Application Identifier) used to identify an AMSD must be unique.
Key Model	Two key models can be selected: **Single Master Key** and **Triple Keys (ENC/MAC/DEK)**. The default setting is **Single Master Key**.
KVN	The key version number used within the current security domain to establish an SCP03 secure channel. The default value is **0x30**.
Diversification Algorithm	Three diversification algorithms can be selected: **EMV_CPS**, **AES_CMAC**, and **None**. The default setting is **EMV_CPS**.
Master Key Ref	Select the key that has been created in KMS. **Note**: When the key model is **Triple Keys (ENC/MAC/DEK)**, you must specify the ENC key, MAC key, and DEK key individually.

3. After verifying that the information is correct, click **Save**.

1. In the **SE Content (chip manufacturer pre-installed)** subsection, click the Options ⋮ icon for the ISD or the corresponding AMSD, and then select **Add CAP**.



2. In the **Add CAP** panel, enter and select the relevant information.

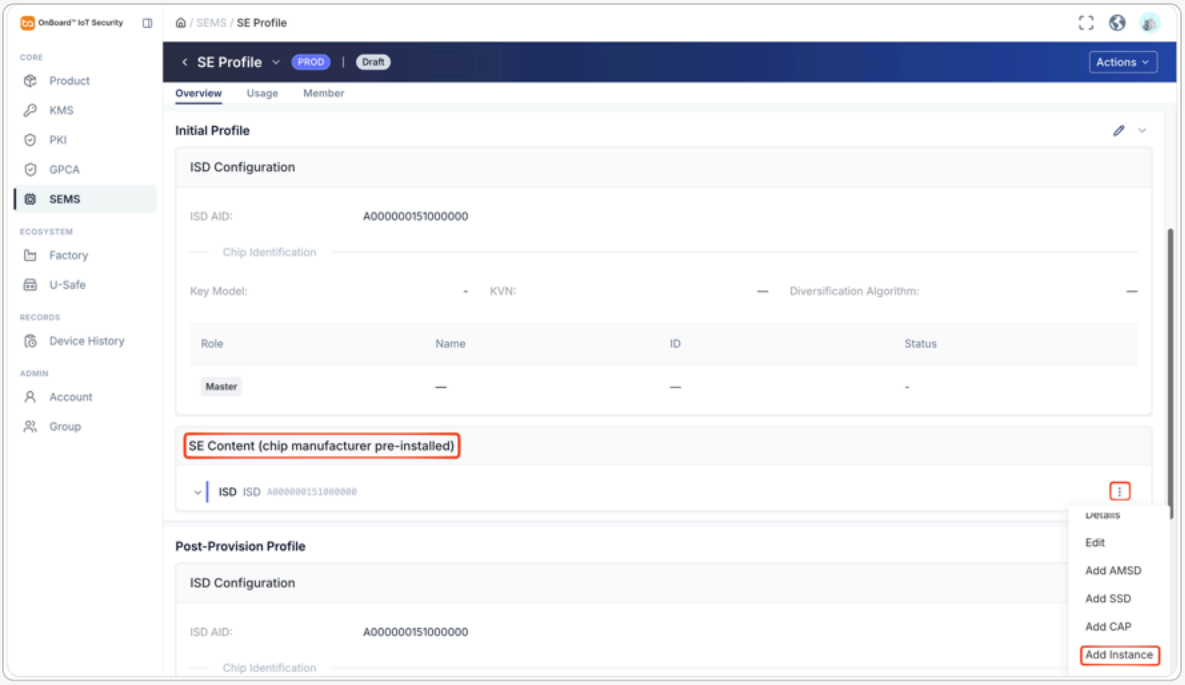


Description of the CAP configuration information:

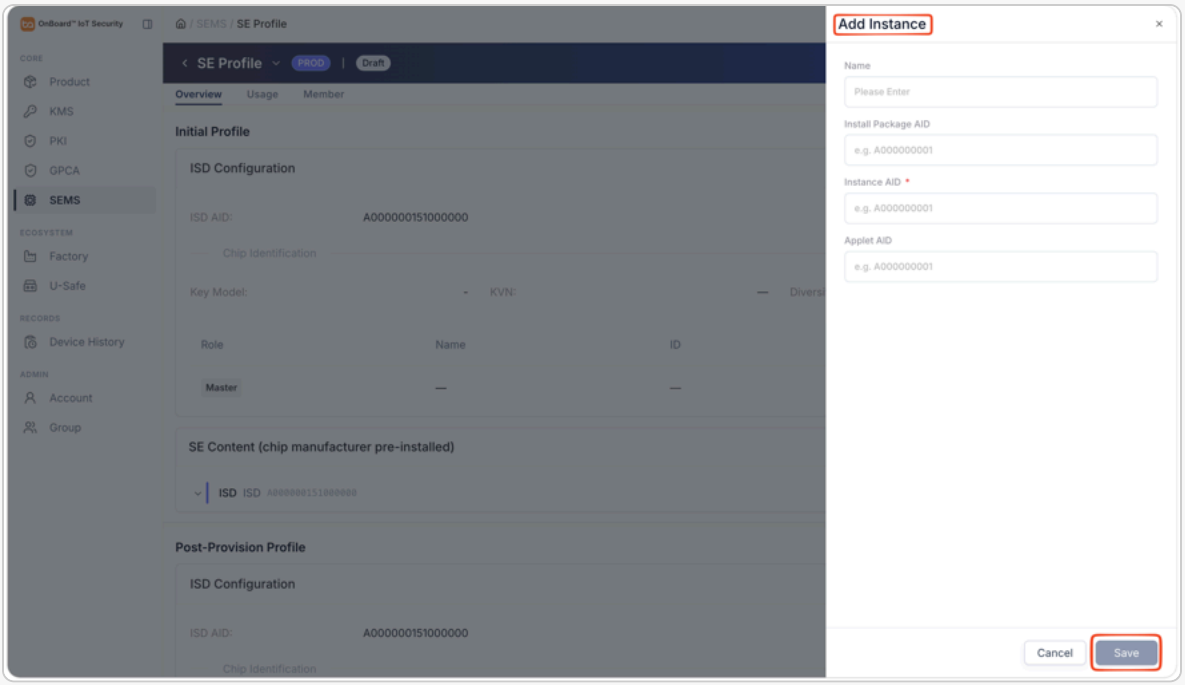
Information	Description
Name	The CAP (Card Application Package) name must be unique.
Package AID	The AID (Application Identifier) used to identify the CAP installation package must be unique.
Version	The version information is used to identify a CAP.
Applet AIDs	The AIDs used to identify the Applets within a CAP installation package must be unique.

3. After verifying that the information is correct, click **Save**.

1. In the **SE Content (chip manufacturer pre-installed)** subsection, click the Options ⋮ icon for the ISD, the corresponding AMSD, or the corresponding SSD, and then select **Add Instance**.



2. In the **Add Instance** panel, enter and select the relevant information.



Description of the Instance configuration information:

Information	Description
Name	The Instance name must be unique.
Install Package AID	The AID (Application Identifier) used to identify the installation package that created this Instance must be unique.
Instance AID	The AID used to identify the Instance must be unique.
Applet AIDs	The AID of the Applet used to create this Instance must be unique.

3. After verifying that the information is correct, click **Save**.

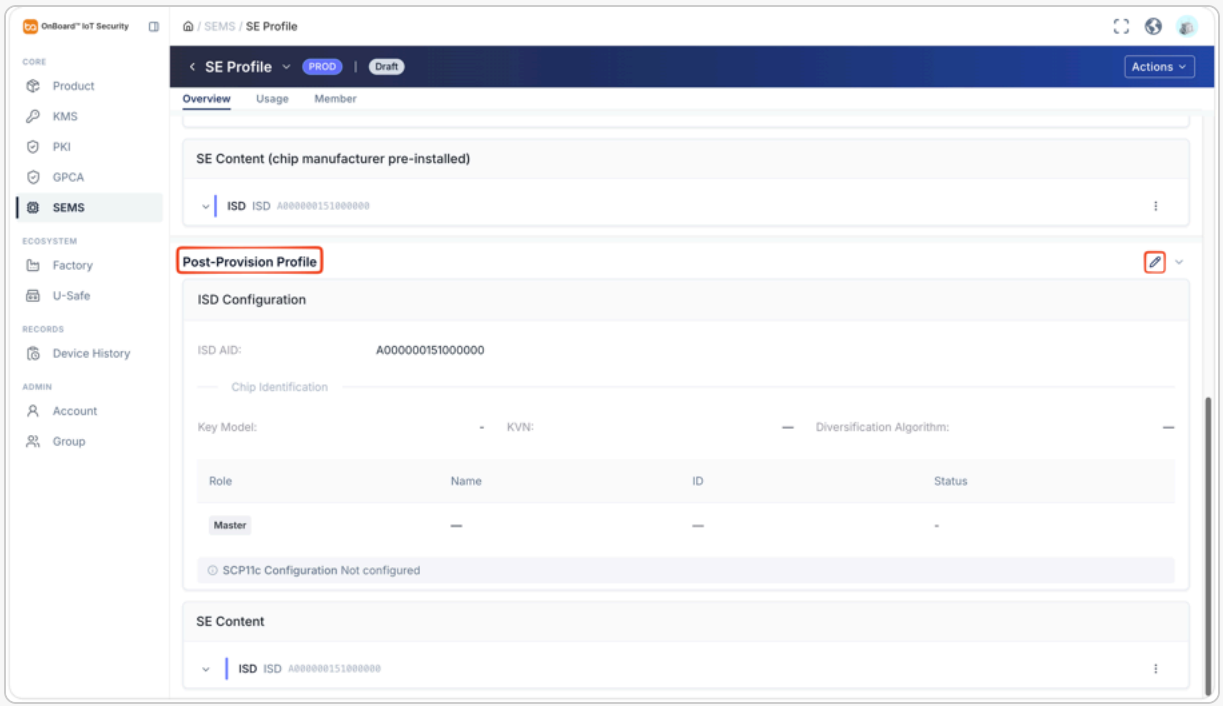
Configure Post-Provision Profile

1. Sign in to OBIS.

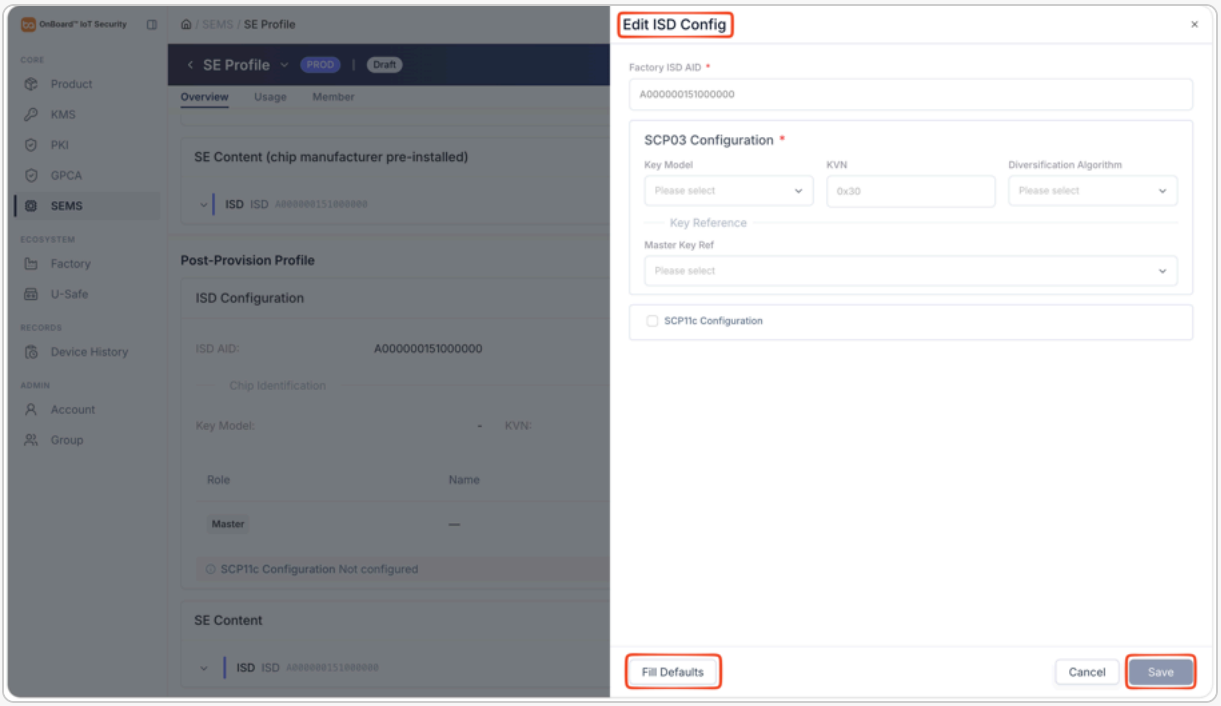
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile to navigate to the SE Profile page.

Configure ISD

1. In the **Post-Provision Profile** section, click the Edit icon.



2. In the **Edit ISD Config** panel, enter and select the relevant information. You may also click **Fill Defaults**.



Description of the ISD configuration information:

Information		Description
General Configuration	Factory ISD AID	The AID (Application Identifier) used to identify the Factory ISD (Issuer Security Domain) on the SE chip, which remains constant throughout the chip's lifecycle. The default value is **A000000151000000**.
SCP03 Configuration	Key Model	Two key models can be selected: **Single Master Key** and **Triple Keys (ENC/MAC/DEK)**. The default setting is **Single Master Key**.

Information		Description
	KVN	The key version number used within the current security domain to establish an SCP03 secure channel. The default value is **0x30**.
	Diversification Algorithm	Three diversification algorithms can be selected: **EMV_CPS**, **AES_CMAC**, and **None**. The default setting is **EMV_CPS**.
	Master Key Ref	Select the key that has been created in KMS. **Note**: When the key model is **Triple Keys (ENC/MAC/DEK)**, you must specify the ENC key, MAC key, and DEK key individually.
SCP11c Configuration	Mode	Two modes can be selected: **Mode A (on-device generation)** and **Mode B (cloud pre-generation)**.

Information		Description
	SD Issuance Chain / SD Certificate	Select the SD source based on the SD certificate generation mode: For Mode A, select either CA-KLCC or KA-KLOC from the GPCA; For Mode B, select an SD certificate from the GPCA. The system displays only the available objects for which you have the authorization to create, within the current environment.
	SD KVN	Identifies the SD key version number used within the current security domain to establish an SCP11c secure channel.
	CA-KLOC	Select the CA-KLOC used to verify the OCE certificate chain, and the system will write its public key to the SE as an OCE trust anchor.
	OCE KVN	Identifies the version number of the CA-KLOC trust anchor used within the current security domain to verify the OCE certificate chain.

3. After verifying that the information is correct, click **Save**.

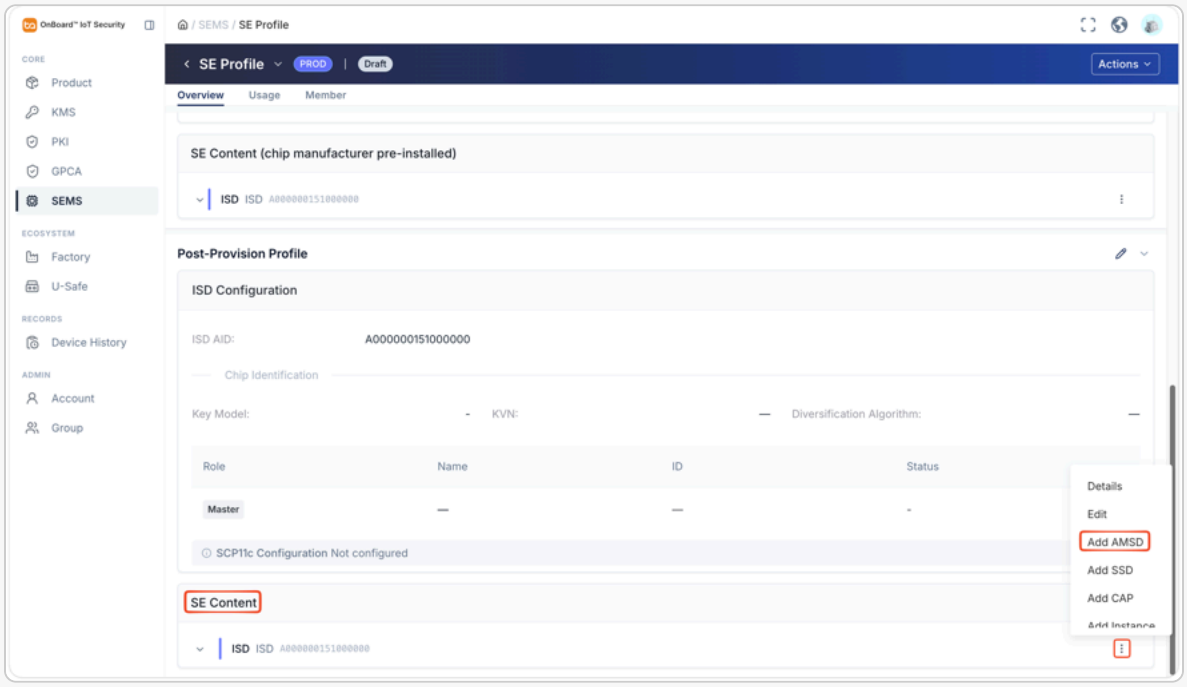
Configure SE Content

Configure AMSD | Configure SSD | Configure CAP | Configure Instance

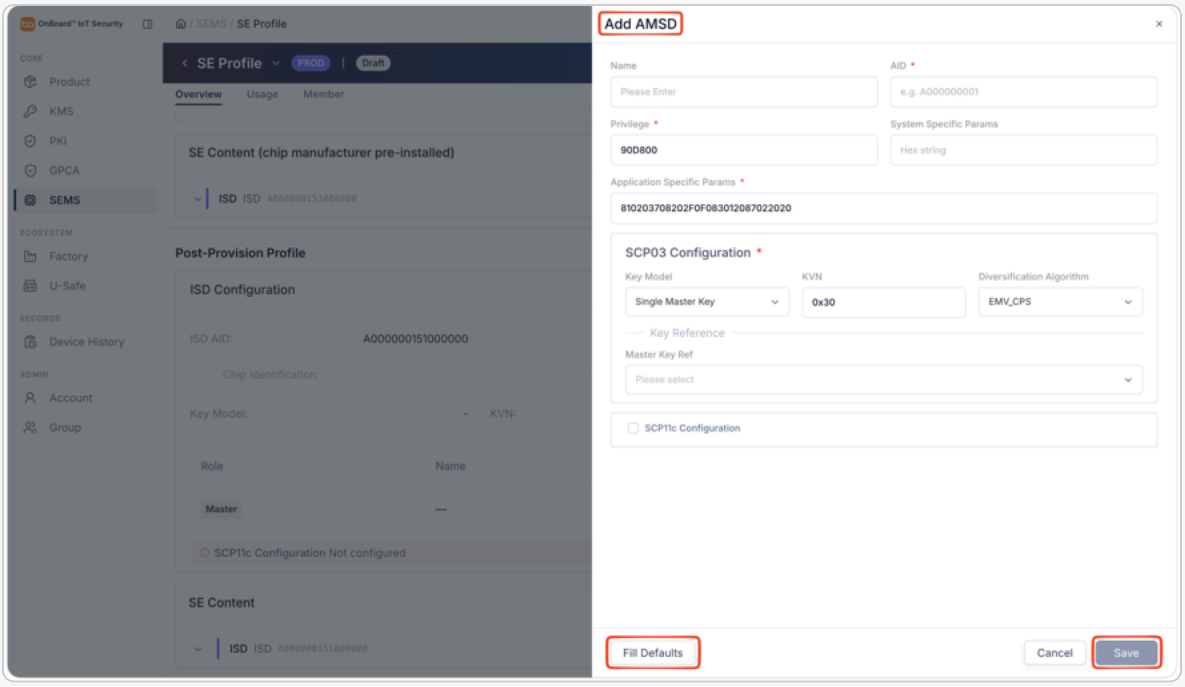
TIP

Supports adjusting the positions of AMSD (Application Management Security Domain) nodes via drag-and-drop within an ISD, enabling flexible reconfiguration of the security domain structure and the download sequence for Java Card content.

1. In the **SE Content** subsection, click the Options ⋮ icon for the ISD and then select **Add AMSD**.



2. In the **Add AMSD** panel, enter and select the relevant information. You may also click **Fill Defaults**.



Description of the AMSD configuration information:

Information		Description
General Configuration	Name	The AMSD name must be unique.
	AID	The AID (Application Identifier) used to identify an AMSD must be unique.
	Privilege	It is used to configure the GlobalPlatform management privileges of an AMSD within the SE and is represented as a 3-byte hexadecimal value.

Information		Description
	System Specific Params	It is used to configure parameters related to the SE platform or system implementation.
	Application Specific Params	It is used to configure parameters related to specific applications or business requirements.
SCP03 Configuration	Key Model	Two key models can be selected: **Single Master Key** and **Triple Keys (ENC/MAC/DEK)**. The default setting is **Single Master Key**.
	KVN	The key version number used within the current security domain to establish an SCP03 secure channel. The default value is **0x30**.
	Diversification Algorithm	Three diversification algorithms can be selected: **EMV_CPS**, **AES_CMAC**, and **None**. The default setting is **EMV_CPS**.

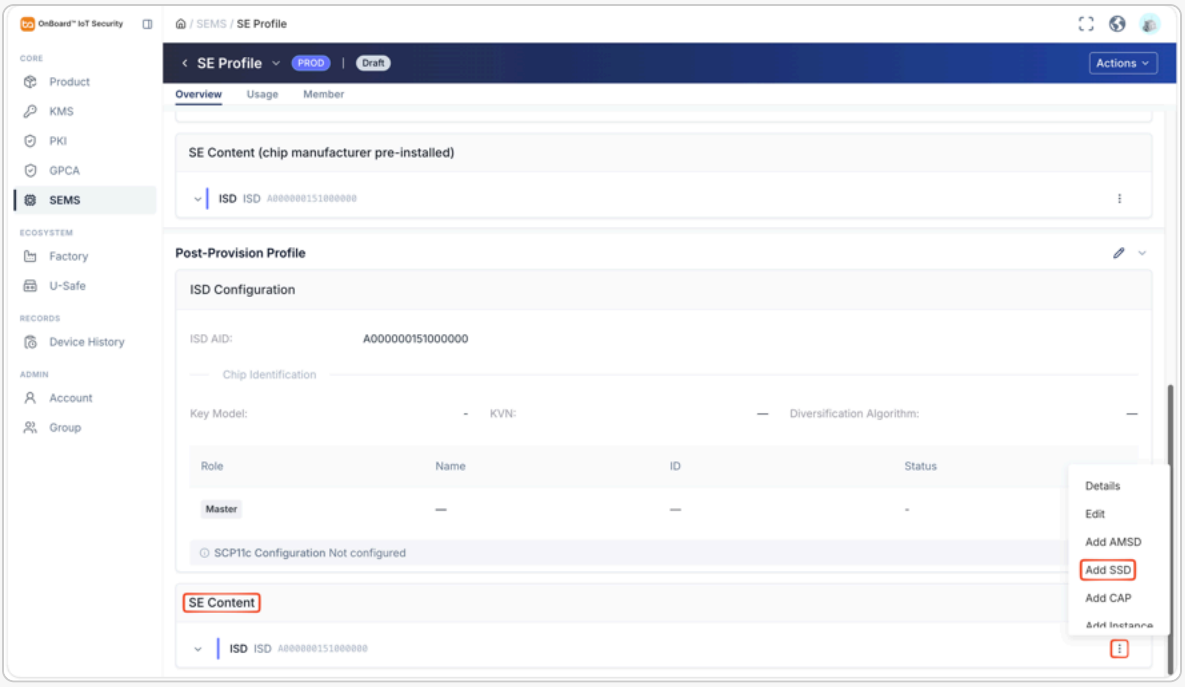
Information		Description
	Master Key Ref	Select the key that has been created in KMS. **Note**: When the key model is **Triple Keys (ENC/MAC/DEK)**, you must specify the ENC key, MAC key, and DEK key individually.
SCP11c Configuration	Mode	Two modes can be selected: **Mode A (on-device generation)** and **Mode B (cloud pre-generation)**.
	SD Issuance Chain / SD Certificate	Select the SD source based on the SD certificate generation mode: For Mode A, select either CA-KLCC or KA-KLOC from the GPCA; For Mode B, select an SD certificate from the GPCA. The system displays only the available objects for which you have the authorization to create, within the current environment.
	SD KVN	Identifies the SD key version number used within the current security domain to establish an SCP11c secure channel.

Information		Description
	CA-KLOC	Select the CA-KLOC used to verify the OCE certificate chain, and the system will write its public key to the SE as an OCE trust anchor.
	OCE KVN	Identifies the version number of the CA-KLOC trust anchor used within the current security domain to verify the OCE certificate chain.

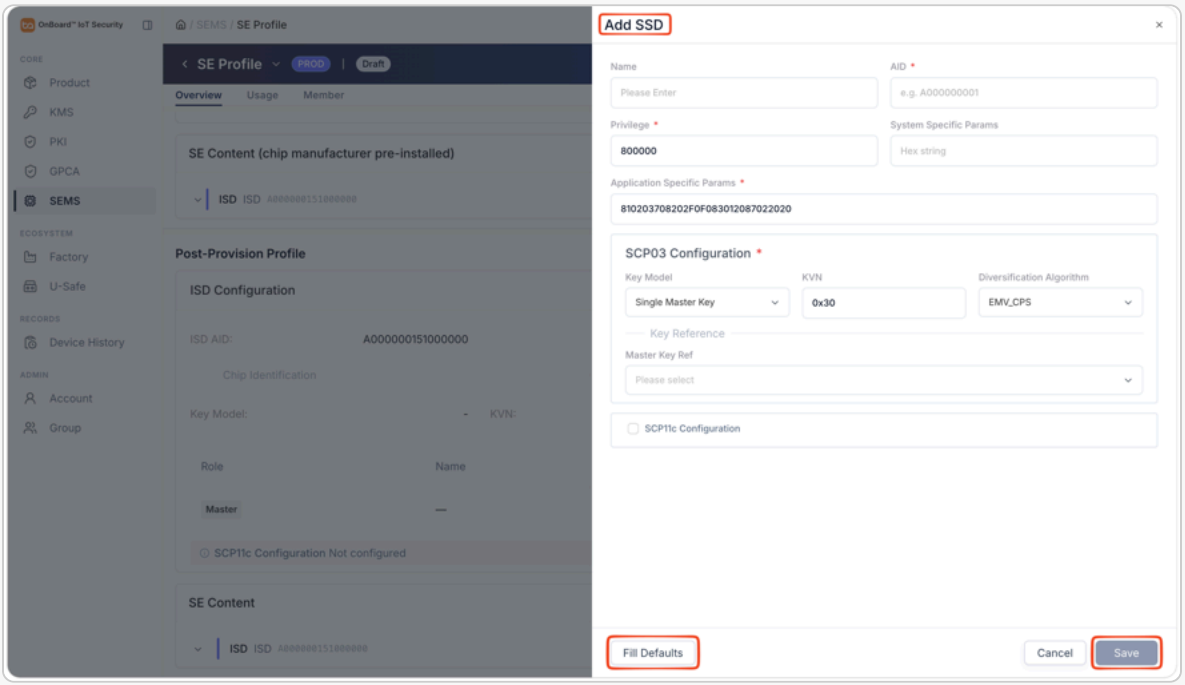
3. After verifying that the information is correct, click **Save**.

> **TIP**
>
> Supports adjusting the position of SSD (Supplementary Security Domain) nodes via drag-and-drop within an ISD or AMSD, as well as moving them across different AMSDs, enabling flexible configuration of the security domain structure and the download sequence for Java Card content.

1. In the **SE Content** subsection, click the Options ⋮ icon for the ISD or the corresponding AMSD, and then select **Add SSD**.



2. In the **Add SSD** panel, enter and select the relevant information. You may also click **Fill Defaults**.



SSD Configuration Information Description:

Information		Description
General Configuration	Name	The SSD name must be unique.
	AID	The AID (Application Identifier) used to identify an SSD must be unique.
	Privilege	It is used to configure the GlobalPlatform management privileges of an SSD within the SE and is represented as a 3-byte hexadecimal value.
	System Specific Params	It is used to configure parameters related to the SE platform or system implementation.
	Application Specific Params	It is used to configure parameters related to specific applications or business requirements.
SCP03 Configuration	Key Model	Two key models can be selected: **Single Master Key** and **Triple Keys (ENC/MAC/DEK)**. The default setting is **Single Master Key**.

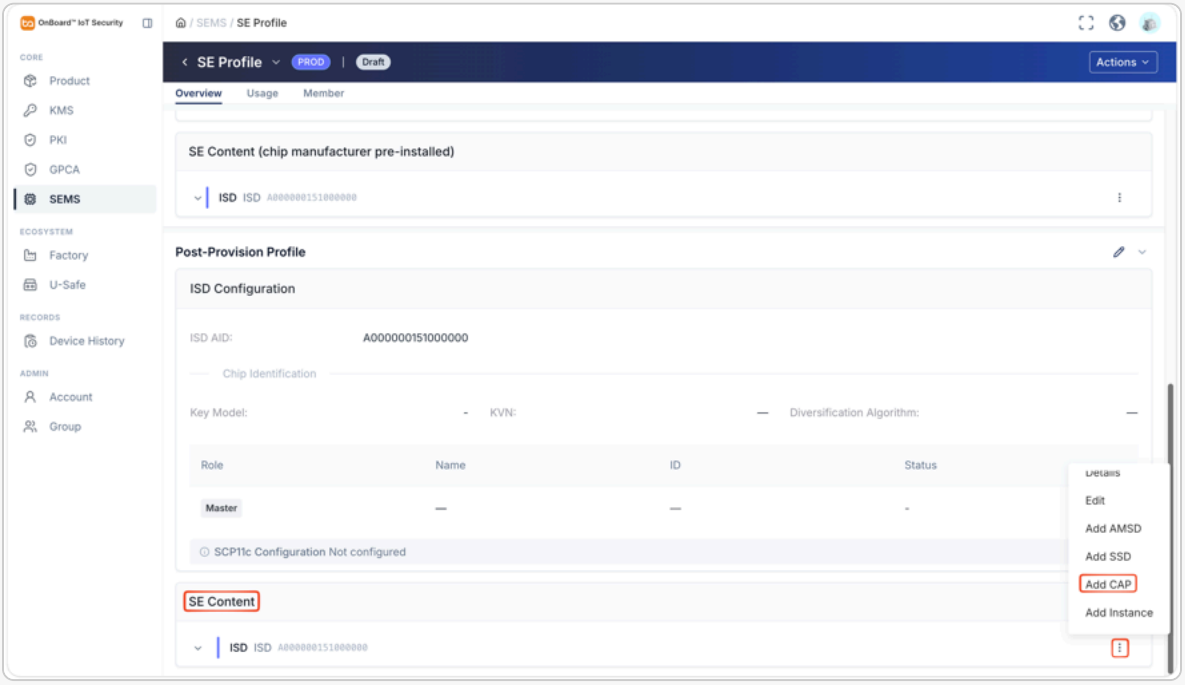
Information		Description
	KVN	The key version number used within the current security domain to establish an SCP03 secure channel. The default value is **0x30**.
	Diversification Algorithm	Three diversification algorithms can be selected: **EMV_CPS**, **AES_CMAC**, and **None**. The default setting is **EMV_CPS**.
	Master Key Ref	Select the key that has been created in KMS. **Note**: When the key model is **Triple Keys (ENC/MAC/DEK)**, you must specify the ENC key, MAC key, and DEK key individually.
SCP11c Configuration	Mode	Two modes can be selected: **Mode A (on-device generation)** and **Mode B (cloud pre-generation)**.

Information		Description
	SD Issuance Chain / SD Certificate	Select the SD source based on the SD certificate generation mode: For Mode A, select either CA-KLCC or KA-KLOC from the GPCA; For Mode B, select an SD certificate from the GPCA. The system displays only the available objects for which you have the authorization to create, within the current environment.
	SD KVN	Identifies the SD key version number used within the current security domain to establish an SCP11c secure channel.
	CA-KLOC	Select the CA-KLOC used to verify the OCE certificate chain, and the system will write its public key to the SE as an OCE trust anchor.
	OCE KVN	Identifies the version number of the CA-KLOC trust anchor used within the current security domain to verify the OCE certificate chain.

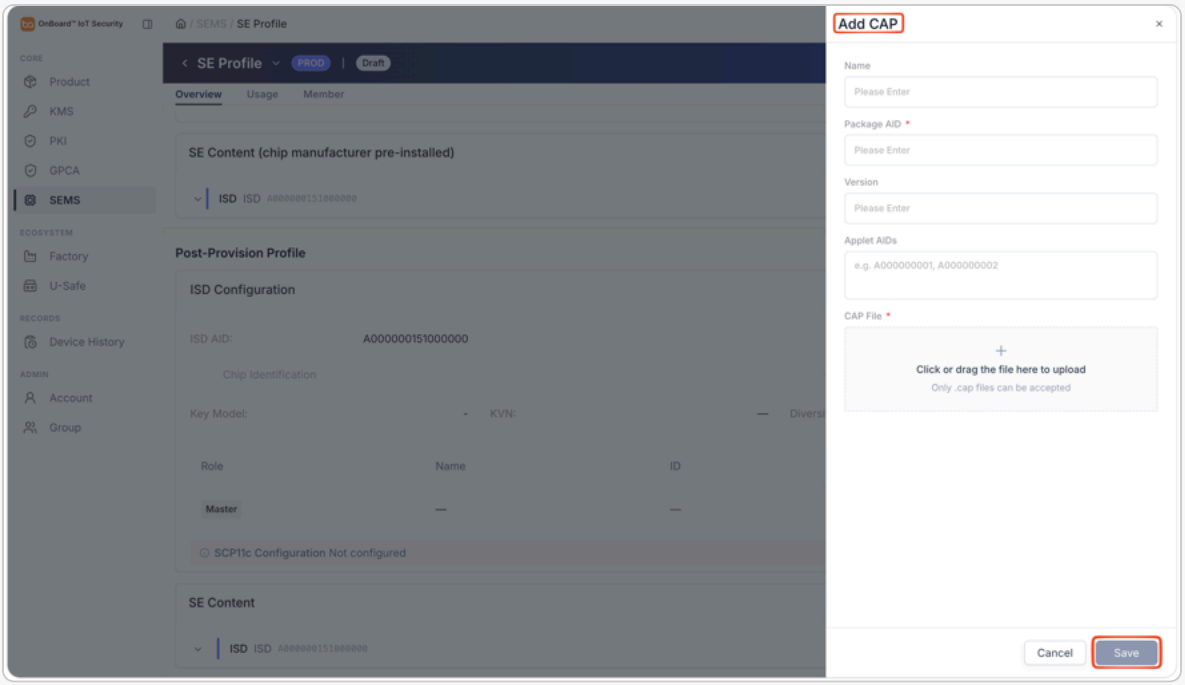
3. After verifying that the information is correct, click **Save**.

> **TIP**
>
> Supports adjusting the position of CAP (Card Application Package) nodes via drag-and-drop within an ISD or AMSD, as well as moving them across different AMSDs, enabling flexible reordering of Java Card content downloads.

1. In the **SE Content** subsection, click the Options ⋮ icon for the ISD or the corresponding AMSD, and then select **Add CAP**.



2. In the **Add CAP** panel, enter and select the relevant information.



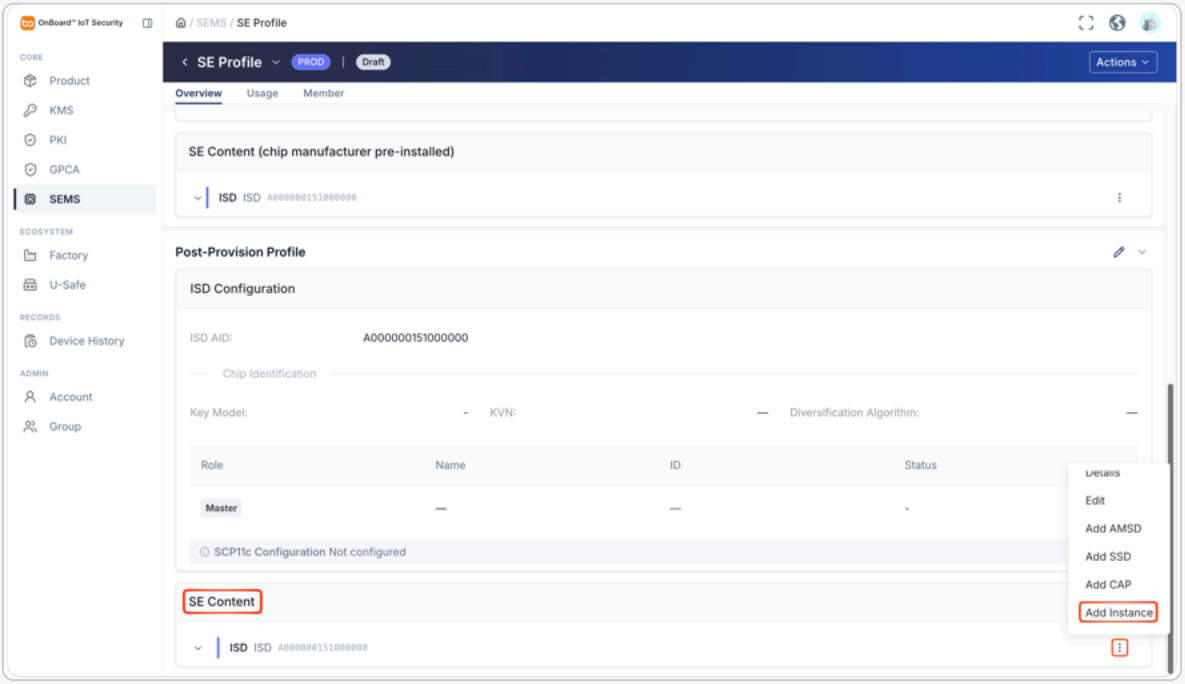
Description of the CAP configuration information:

Information	Description
Name	The CAP (Card Application Package) name must be unique.
Package AID	The AID (Application Identifier) used to identify the CAP installation package must be unique.
Version	The version information is used to identify a CAP.
Applet AIDs	The AIDs used to identify the Applets within a CAP installation package must be unique.
CAP File	Click the Add + icon to select and upload a CAP file in .cap format, or directly drag your CAP file into the upload area.

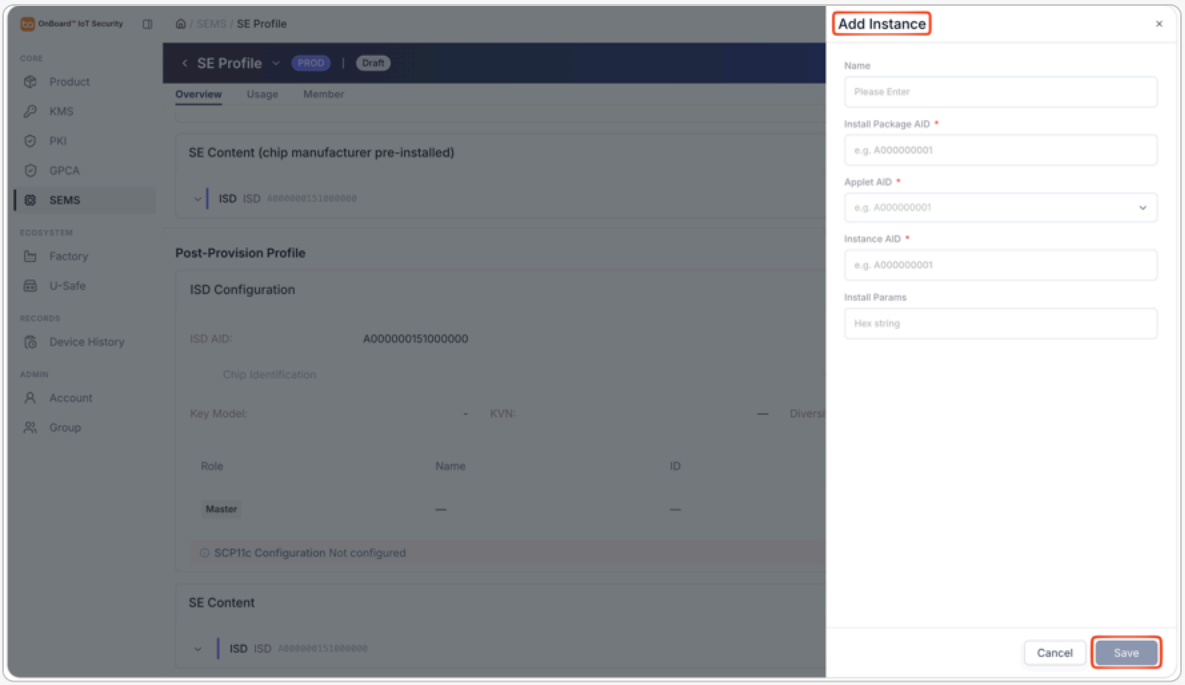
3. After verifying that the information is correct, click **Save**.

> **TIP**
>
> Supports adjusting the position of Instance nodes via drag-and-drop within an ISD, AMSD, or SSD, as well as moving them across different AMSDs or SSDs, enabling flexible adjustment of the Java Card content download sequence.

1. In the **SE Content** subsection, click the Options ⋮ icon for the ISD, the corresponding AMSD, or the corresponding SSD, and then select **Add Instance**.



2. In the **Add Instance** panel, enter and select the relevant information.



Description of the Instance configuration information:

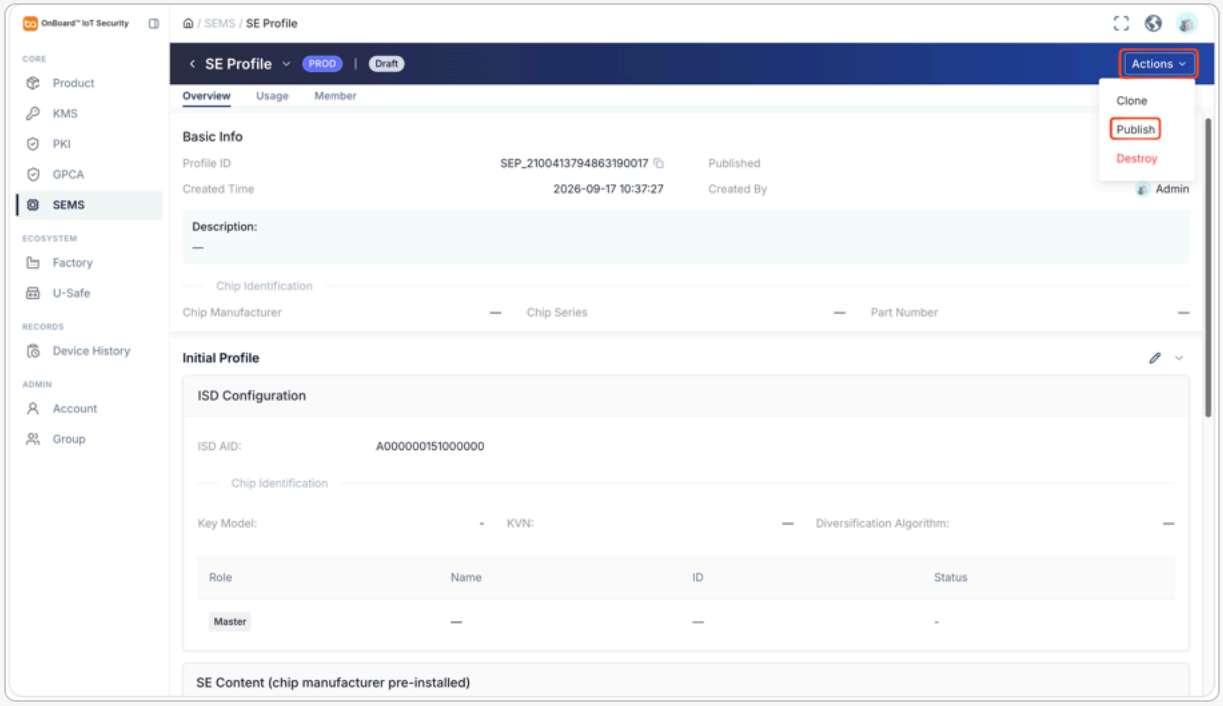
Information	Description
Name	The Instance name must be unique.
Install Package AID	The AID (Application Identifier) used to identify the installation package that created this Instance must be unique.
Applet AID	Select the Applet AID from the CAP file to specify the applet used to create the Instance.
Instance AID	The AID used to identify the Instance must be unique.
Install Params	Enter the installation parameters to be passed to the applet when the Instance is created.

3. After verifying that the information is correct, click **Save**.

Publish the SE Profile

> **TIP**
>
> You can publish an SE Profile only when it is in the **Draft** state and you have the necessary publishing permissions.
>
> Once published, the SE Profile will be permanently locked, and none of its fields can be edited further.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile to navigate to the SE Profile page.
3. Verify that the following conditions are met, then click **Actions** and select **Publish**.



- The ISDs for both the initial profile and the Post-Provision Profile have been configured.
- All keys and GPCA objects referenced by any node are in the **Active** state.
- The SCP (SCP03 or SCP11c) for all security domains has been configured.

4. In the **Confirm Publish** window, click **Confirm Publish** to complete the publication of the SE Profile.

Version: v3.4.0 (Latest)

How to check SE Profiles in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS).

- Check basic information
- Check usage
- Check scripts
- Check members

Prerequisites

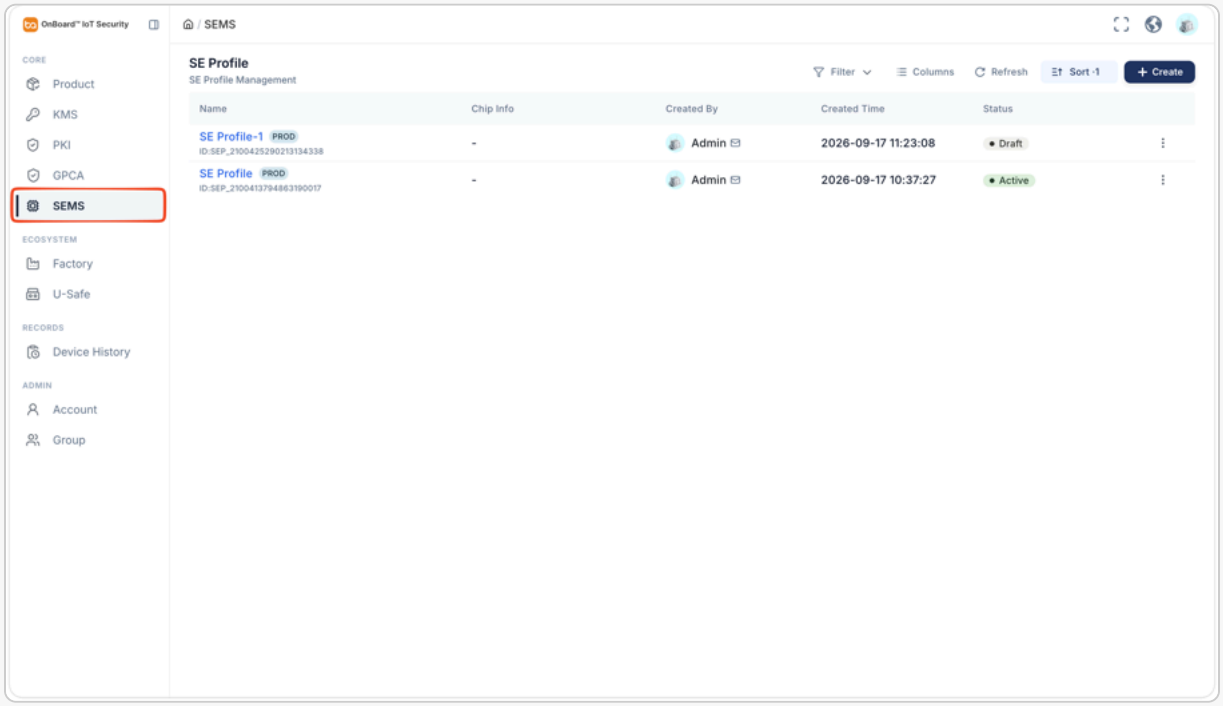
Before getting started, please ensure that:

- You have OBIS role permissions as a System Manager or SE Resource Manager.
- You have permissions for the corresponding SE Profile.

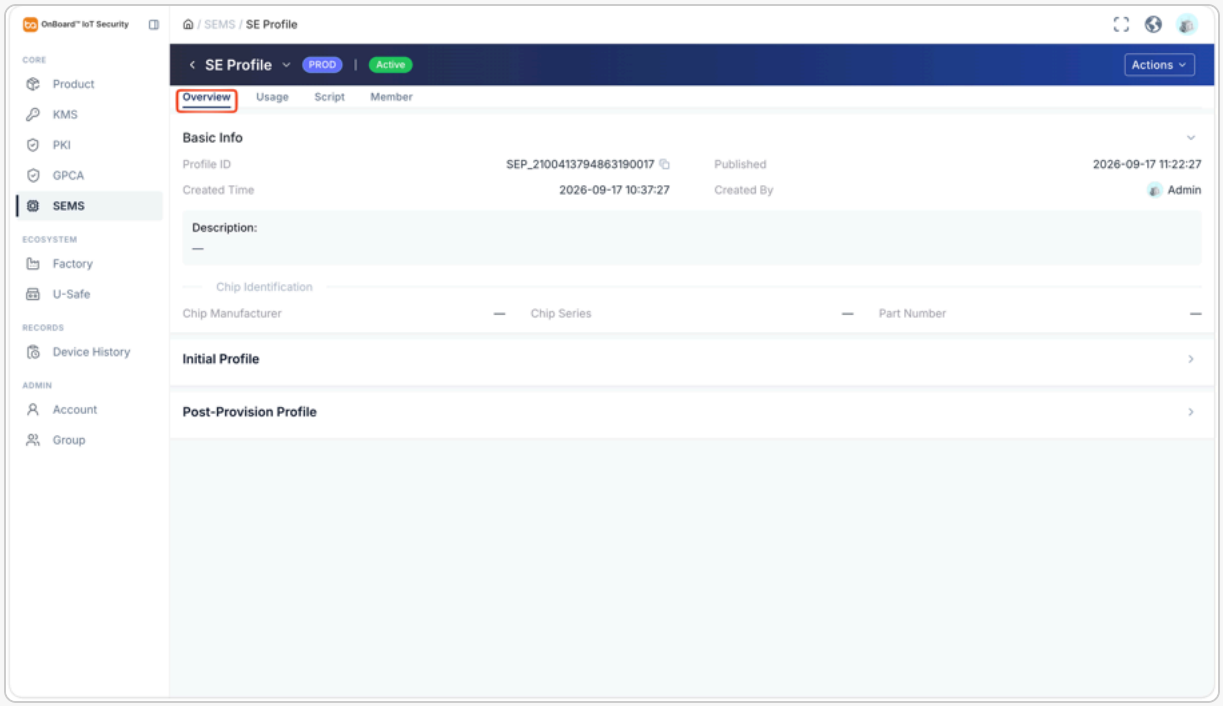
Check basic information

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



3. On the SE Profile page, you can check the SE Profile related information (**Basic Info**, **Initial Profile**, and **Post-Provision Profile**).

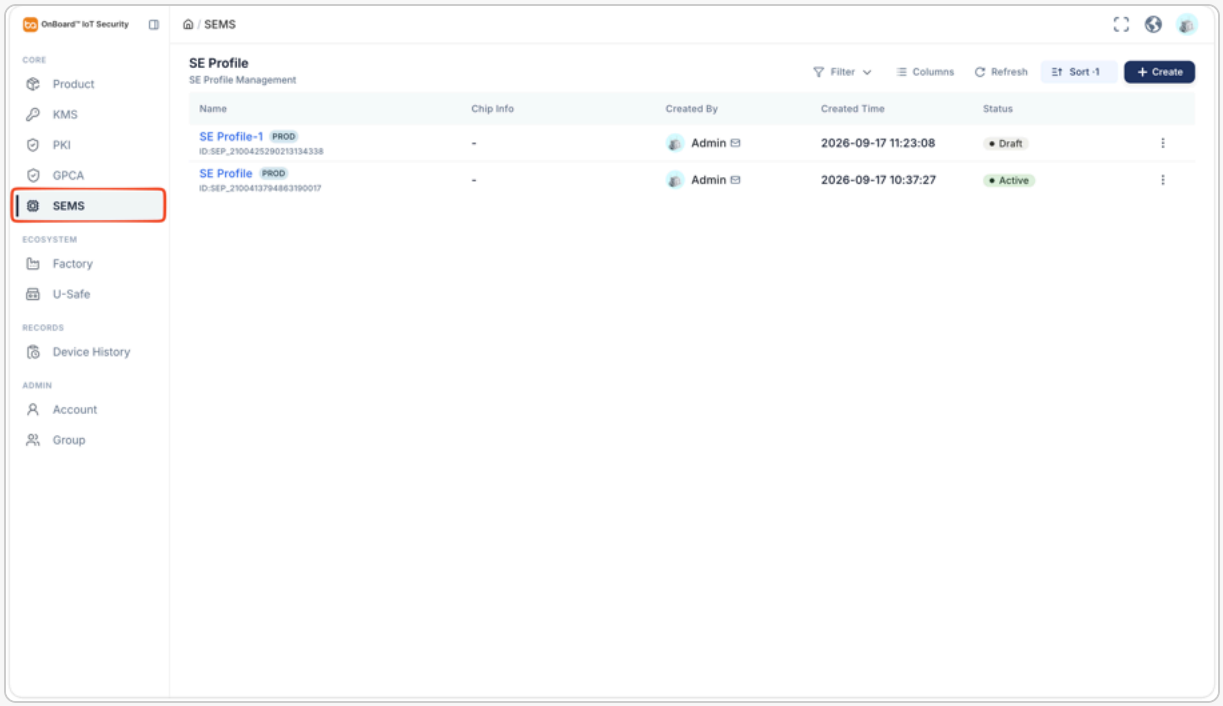


Check usage

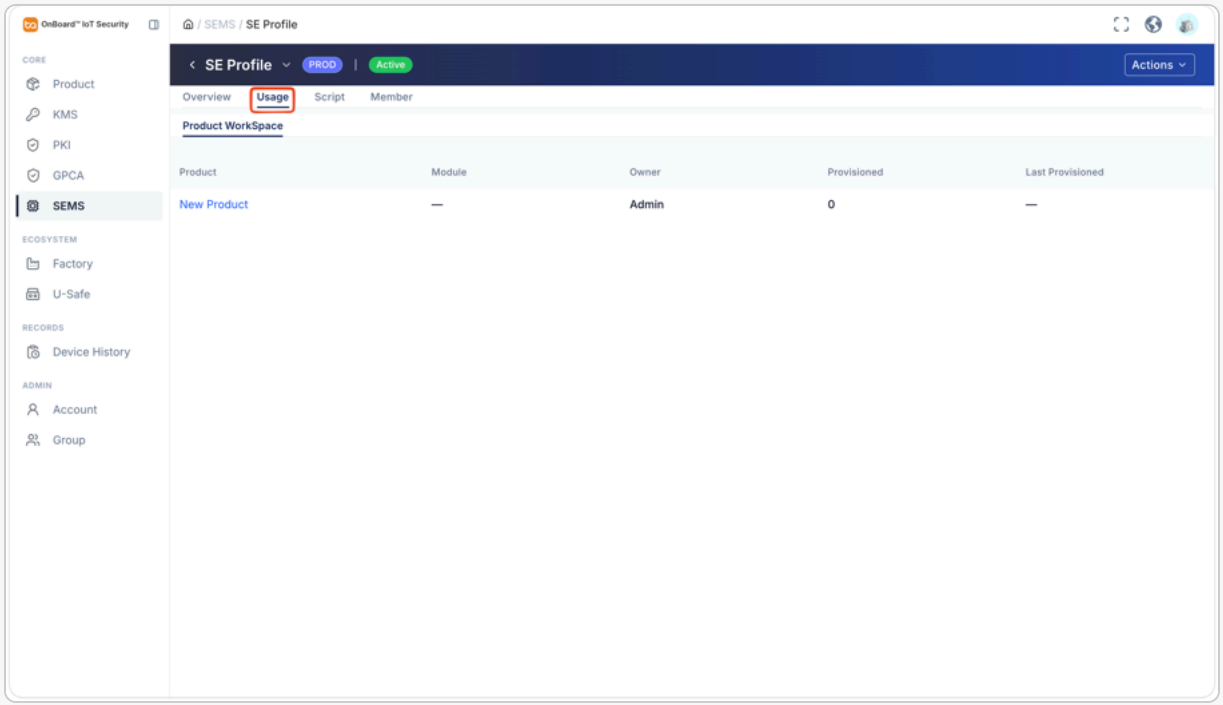
> **TIP**
>
> SE Profile usage can be used to check its reference records and the current data status of the associated objects.

1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.



3. On the **Usage** tab of the SE Profile page, you can check the usage details for the SE Profile (such as associated products and the number of times it has been provisioned).

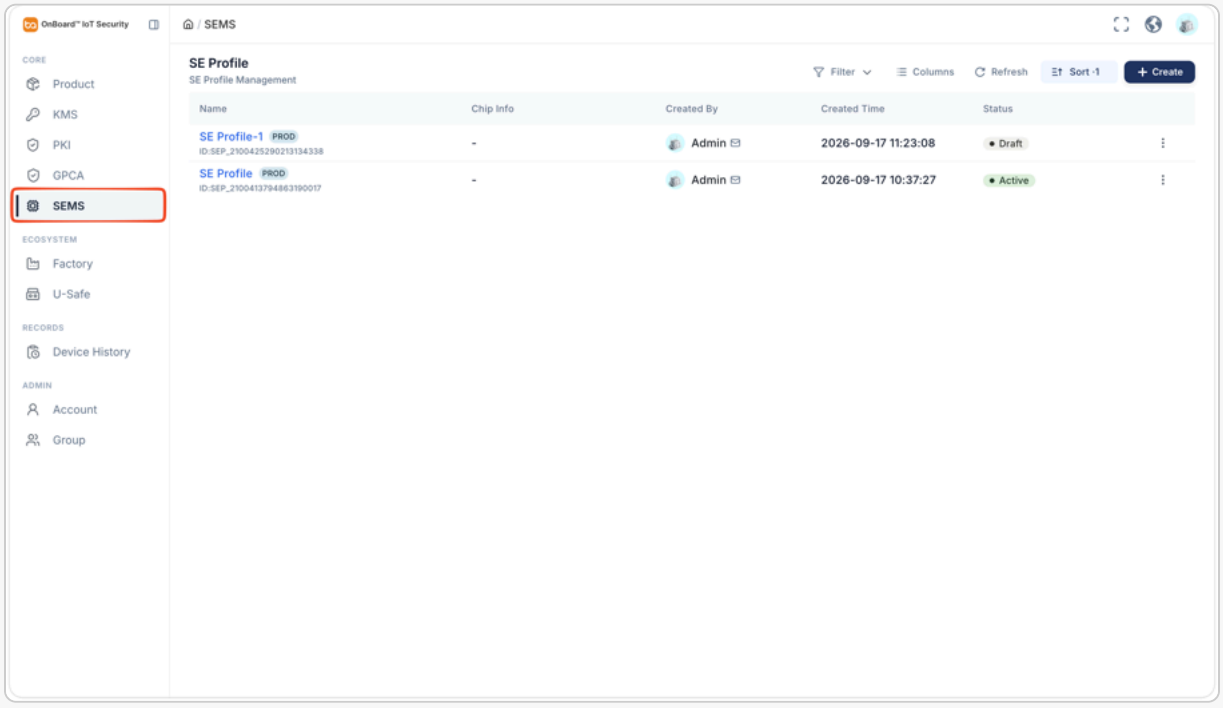


Check scripts

> **TIP**
>
> When the SE Profile is in the **Draft** state, the **Script** tab will not be displayed.

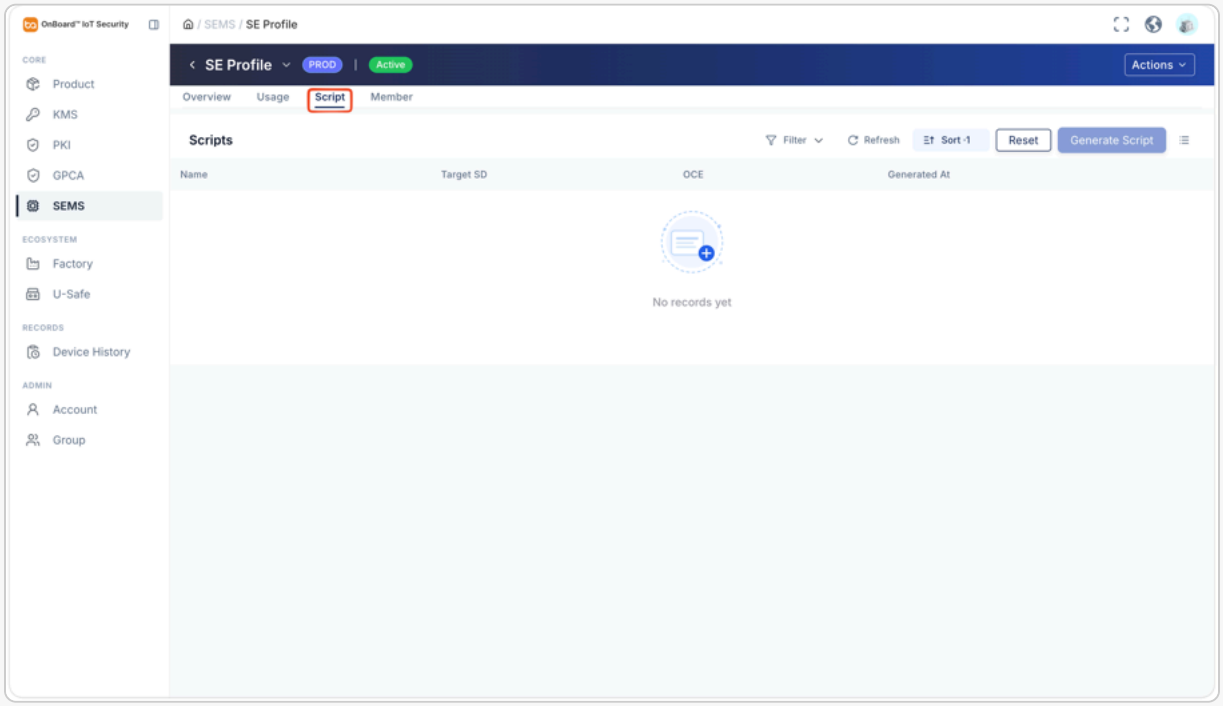
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.



3. On the **Script** tab of the SE Profile page, you can check the scripts information (such as **Name**, **Target SD**, and **OCE**).

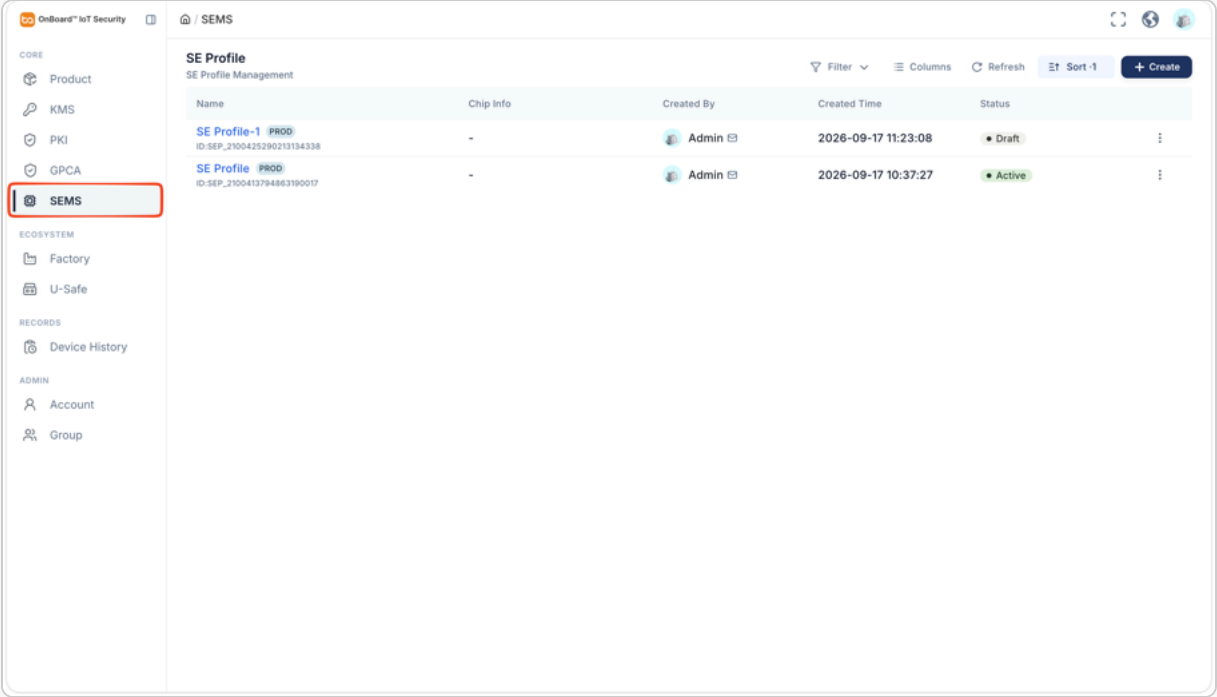
> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Check members

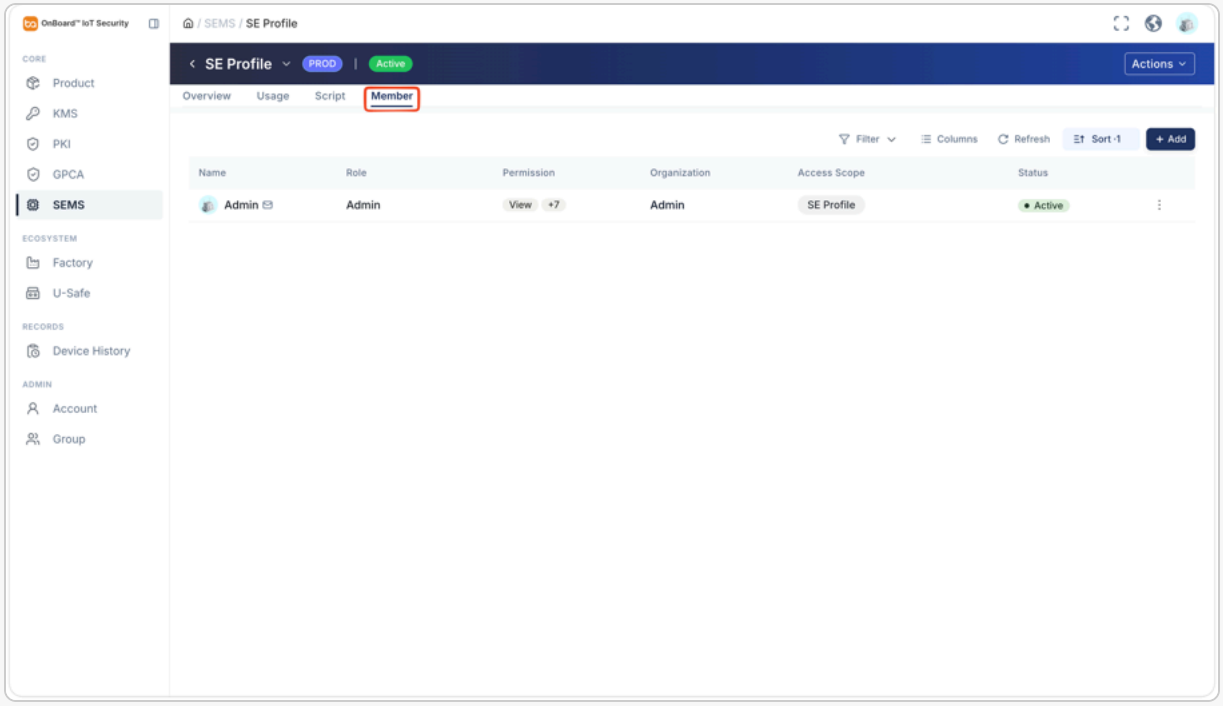
> **TIP**
>
> AMSD collaborators don't have permission to check the **Member** tab.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.



3. On the **Member** tab of the SE Profile page, you can check the permissions that members have for this SE Profile (such as **Name**, **Role**, **Permission**, and **Access Scope**).

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.


OnBoard™ IoT Security
/ SEMS / SE Profile
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
SE Profile
PROD
Active
Actions
Overview
Usage
Script
Member
Filter
Columns
Refresh
Sort · 1
+ Add
Name
Role
Permission
Organization
Access Scope
Status
Admin
Admin
View
+7
Admin
SE Profile
Active

Version: v3.4.0 (Latest)

How to manage SE Profiles in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Manage SE Profile permissions
- Clone an SE Profile
- Edit basic information
- Edit SE Profile content
- Delete SE Profile content
- Invite AMSD members
- Lock or unlock an SE Profile
- Archive an SE Profile
- Revoke an SE Profile
- Destroy an SE Profile

Prerequisites

Before getting started, please ensure that:

- You have OBIS role permissions as a System Manager or SE Resource Manager.
- You have permissions for the corresponding SE Profile.

Manage SE Profile permissions

> **TIP**
>
> By default, the SE Profile creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.

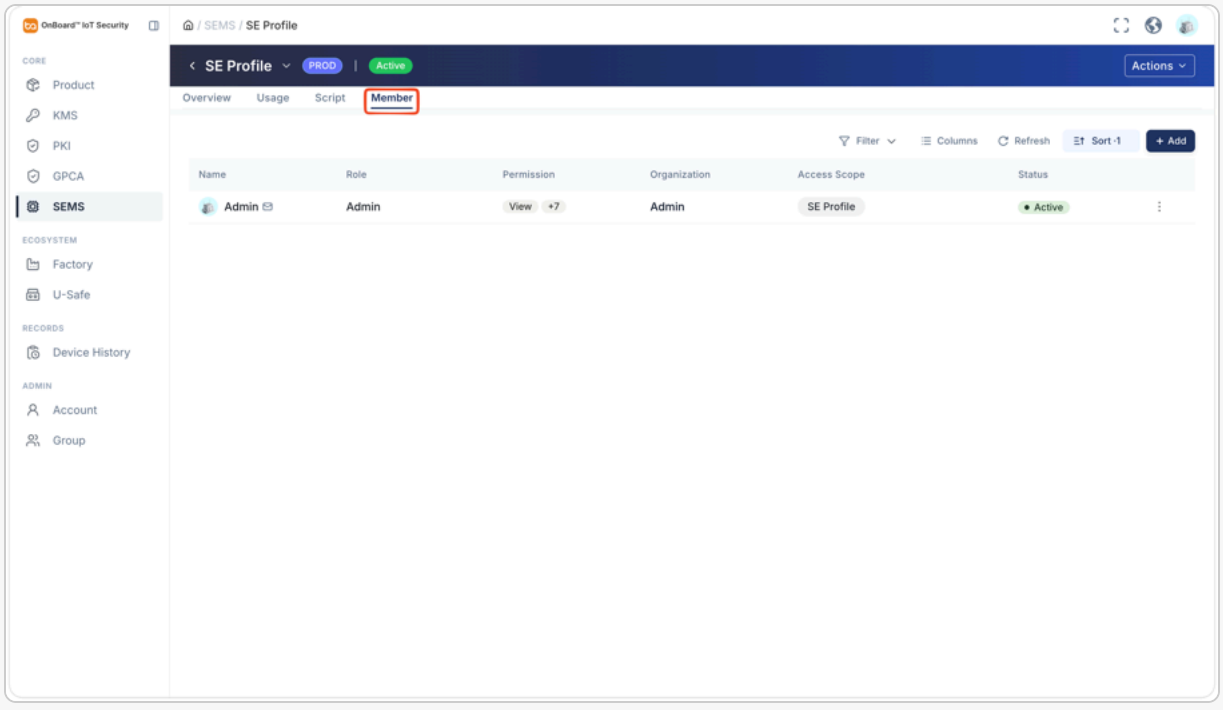
You can assign different operational permissions for the SE Profile to different members. The descriptions of these permissions are as follows:

Permissions	Description
View	View SE Profile details (read-only).
Add Member	Add members to this SE Profile and assign them permissions that do not exceed your own permissions.
Edit	Allow configuring unpublished SE Profiles.
Publish	Publish an SE Profile.
Manage Scripts	Allow generating and deleting scripts. Generating scripts also requires **Use** permission for the OCE chain certificates referenced in the SCP11c configuration.
Grant	Allow an SE Profile to be referenced within product configurations.

Permissions	Description
Lock / Revoke / Archive	Allow locking, revoking, and archiving operations to be performed on an SE Profile.
Destroy	Destroy an SE Profile.

You can adjust and set user permissions for SE Profiles by following these steps:

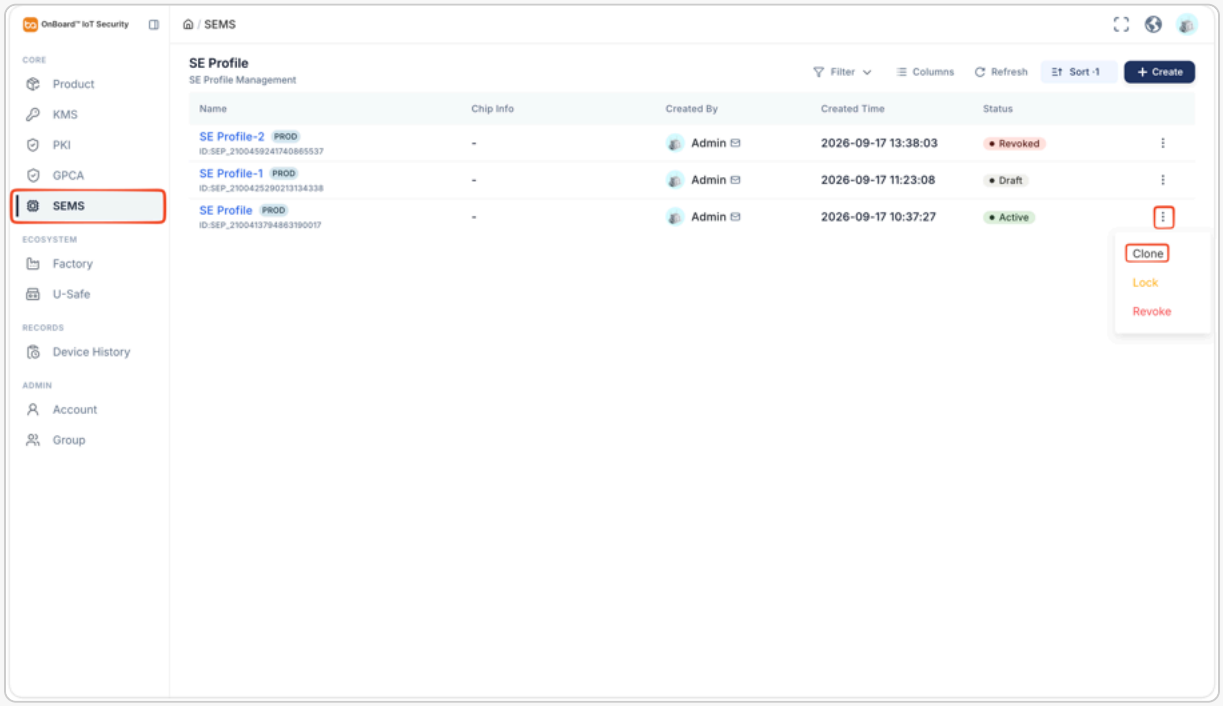
1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.
3. On the SE Profile page, you can manage the user permissions for the SE Profile on the **Member** tab.



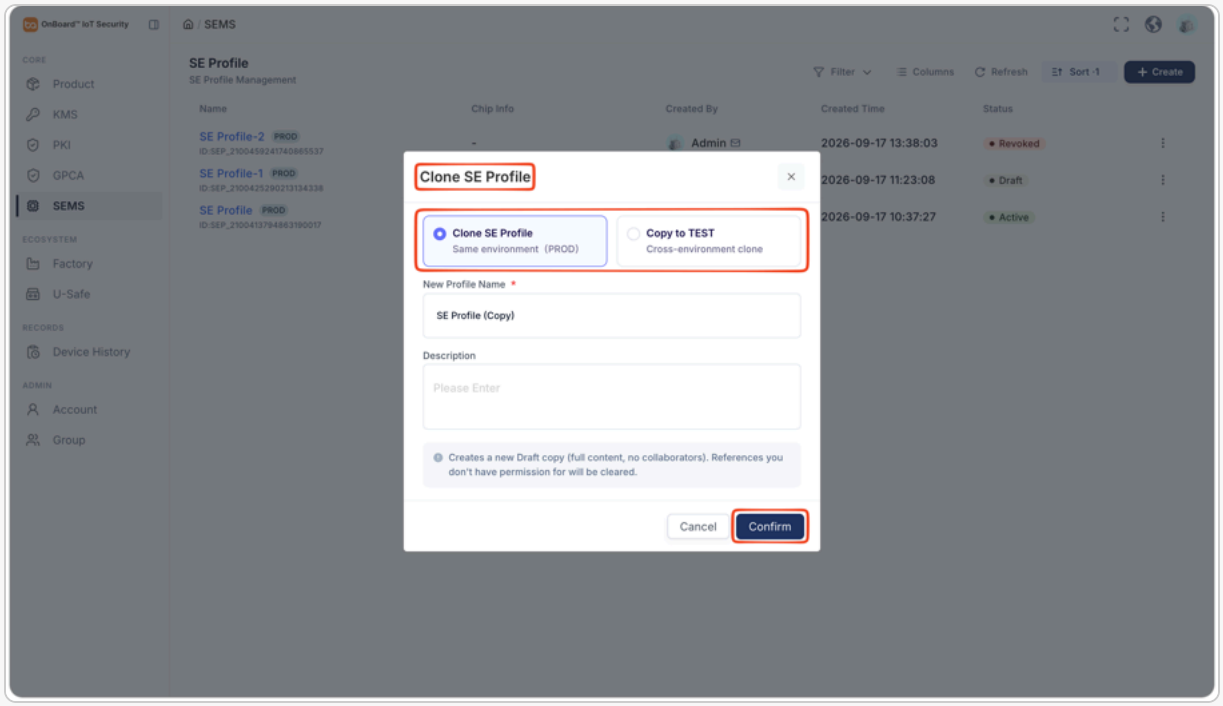
Clone an SE Profile

> **TIP**
>
> When cloning an SE Profile, the configuration content for which you have permissions will be copied, but membership associations will not be included. When cloning across environments, cryptographic references (such as key references or GPCA certificates) will be cleared. These references must be reconfigured in the target environment before the SE Profile can be published.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then click the Options icon for the corresponding SE Profile and select **Clone**.



3. In the **Clone SE Profile** window, select the option to clone the SE Profile or copy it to another environment, then enter a new name and description.



4. After verifying that the information is correct, click **Confirm** to clone the SE Profile.

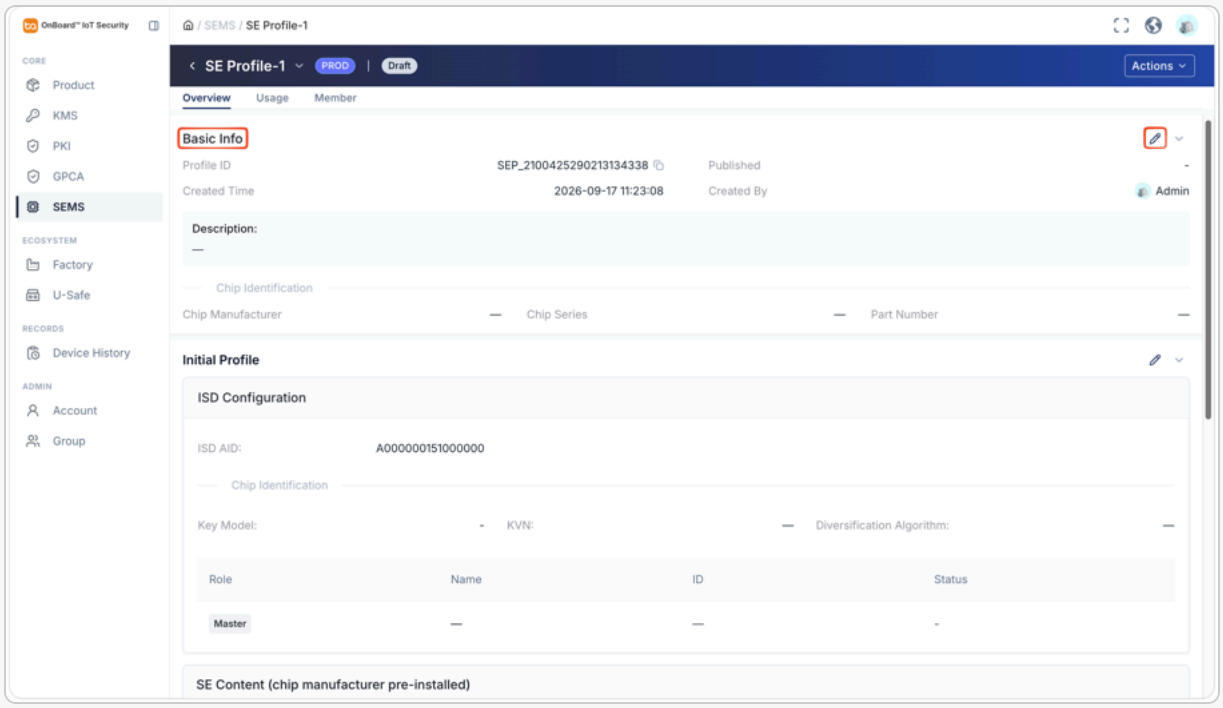
Edit basic information

> **TIP**
>
> You can configure the SE Profile basic information only when it is in the **Draft** state.

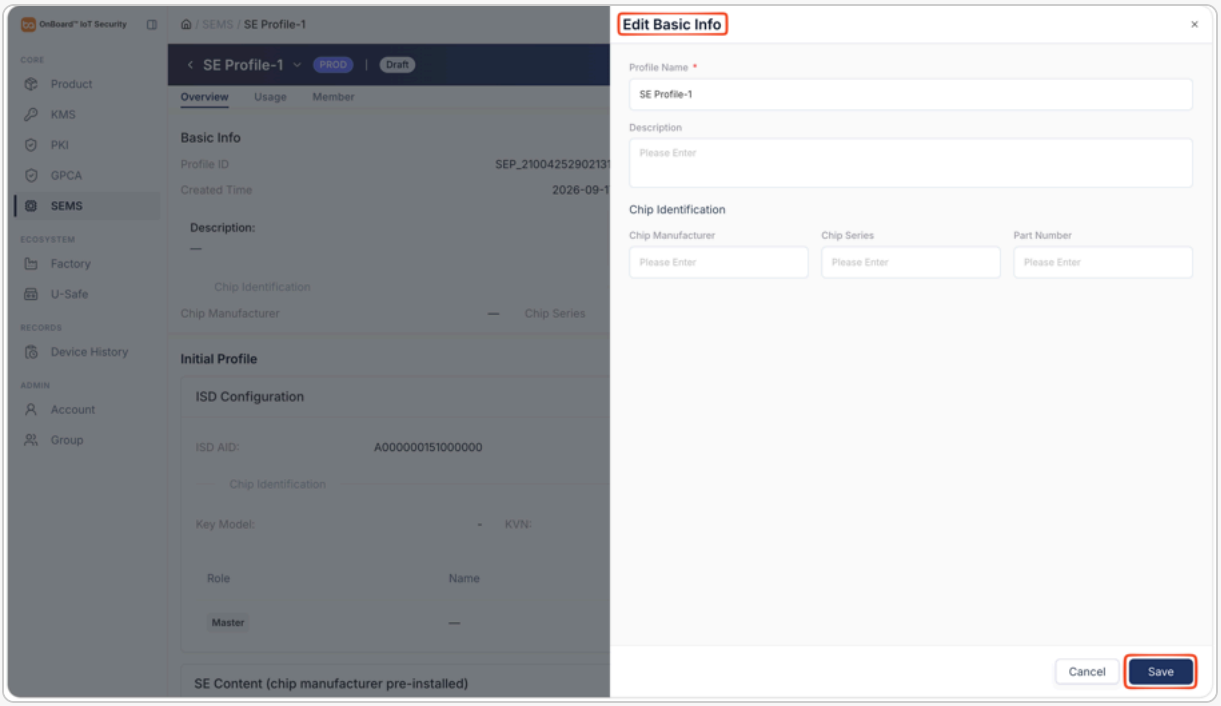
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.

3. On the SE Profile page, click the Edit icon in the **Basic Info** section.



4. In the **Edit Basic Info** panel, update the SE Profile name and description, then enter the corresponding chip Identification (chip manufacturer, series, and part number).



5. After verifying that the information is correct, click **Save**.

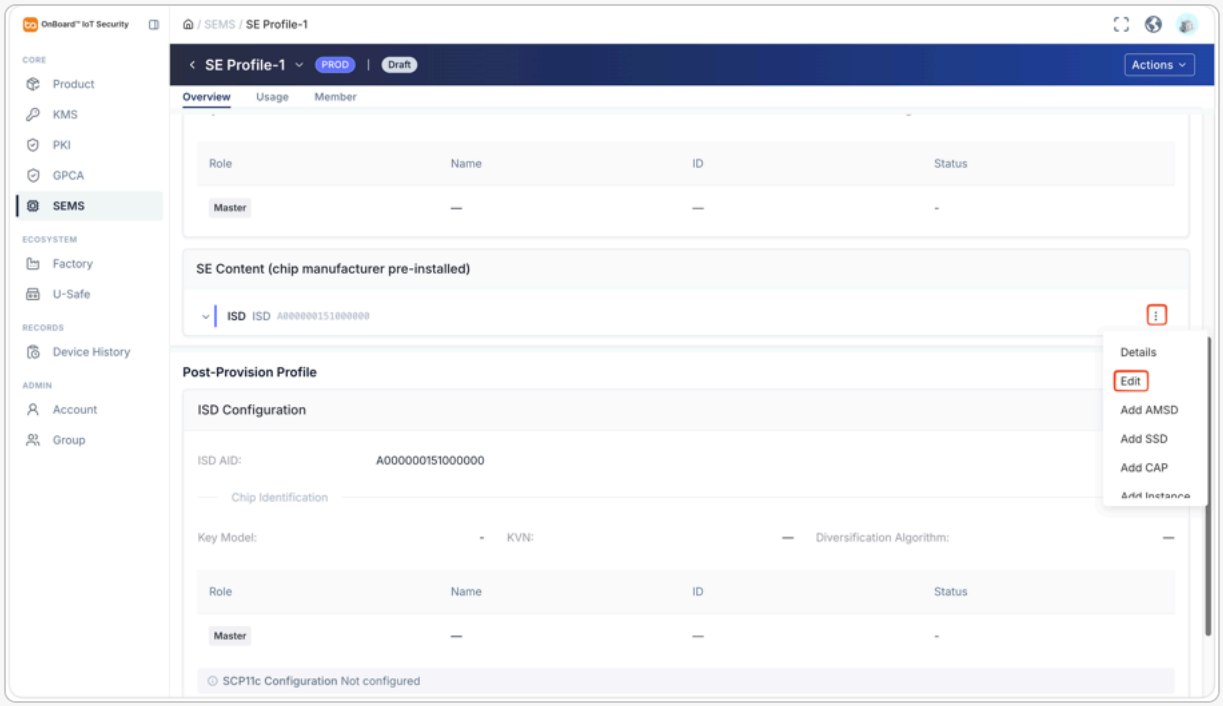
Edit SE Profile content

> **TIP**
>
> You can configure the SE Profile content only when it is in the **Draft** state.

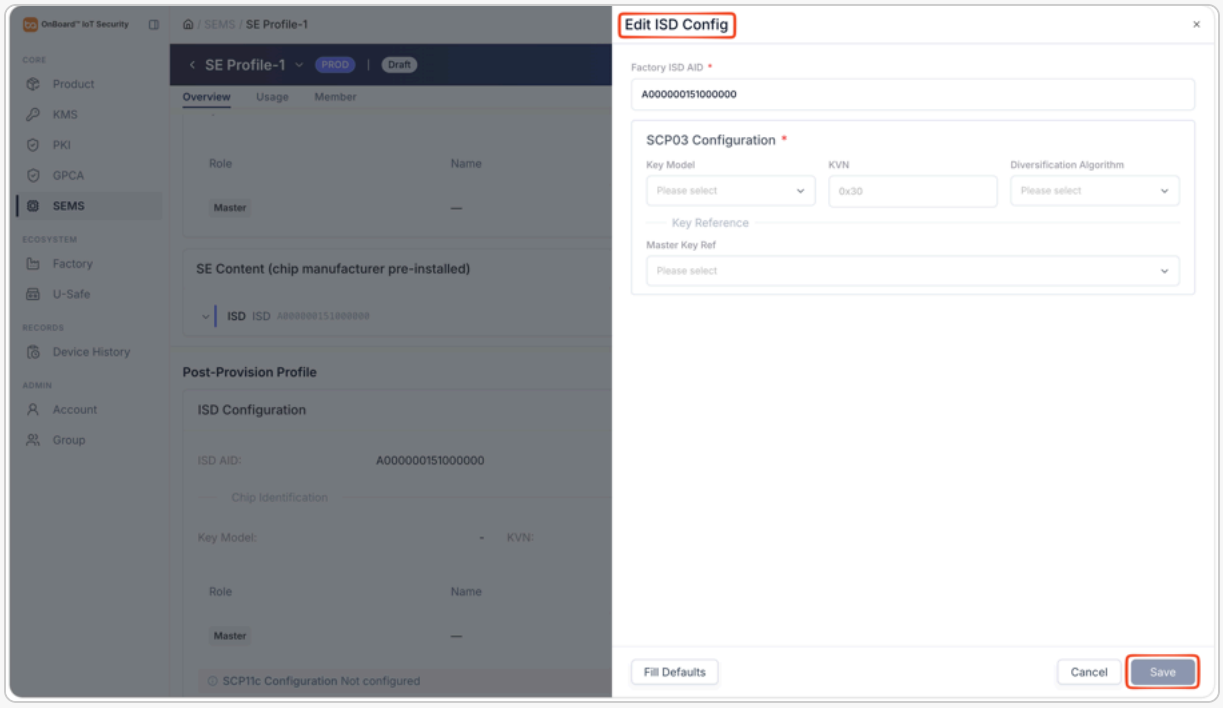
1. Sign in to OBIS.

2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.

3. On the SE Profile page, click the Options ⋮ icon for the corresponding node (ISD, AMSD, SSD, CAP, or Instance) and select **Edit**.



4. In the editing panel, enter and select the relevant information.

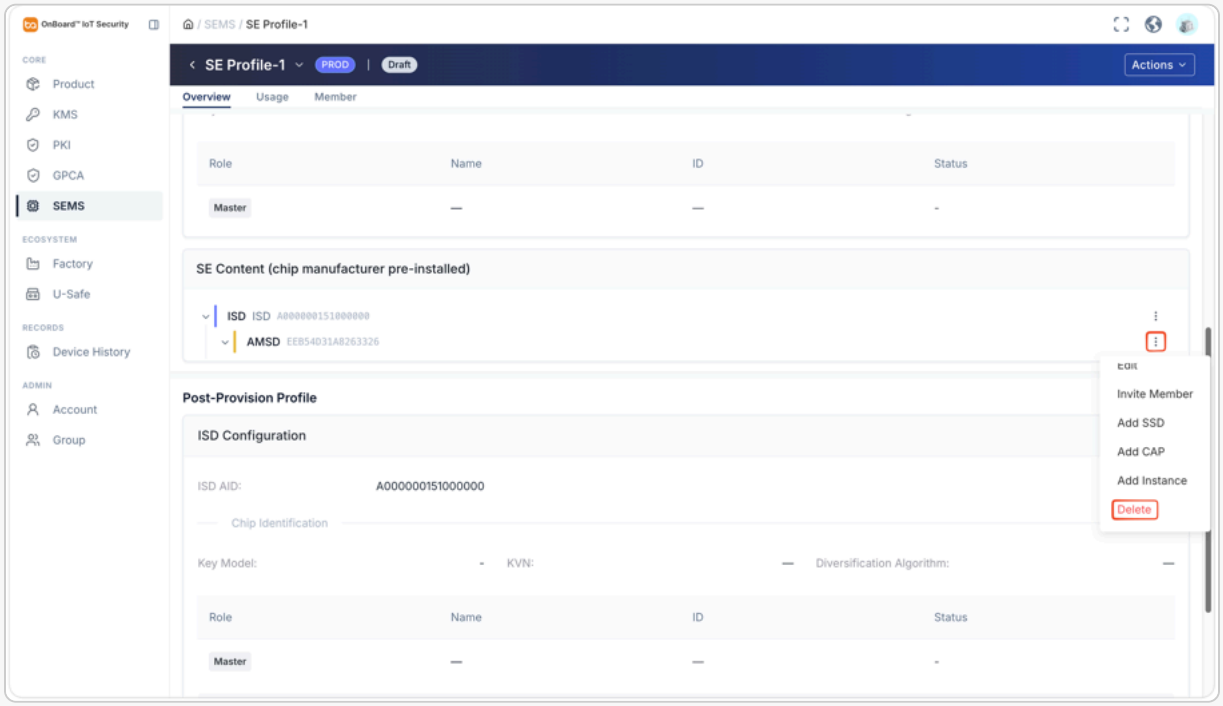


5. After verifying that the information is correct, click **Save**.

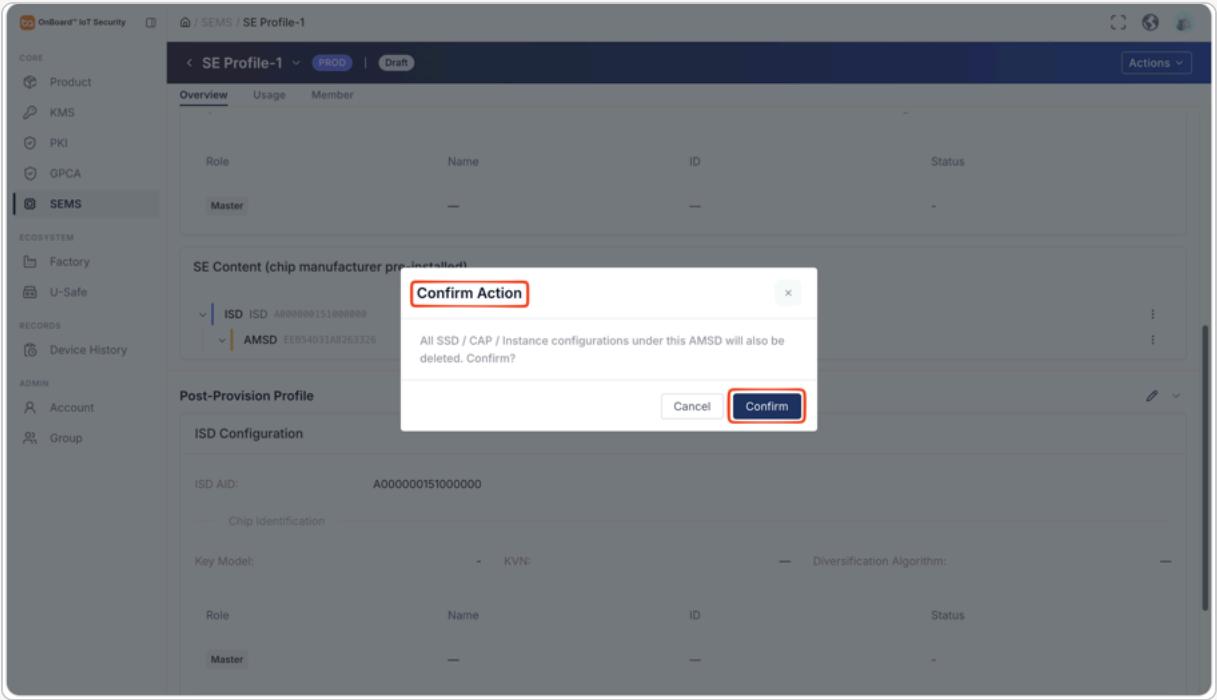
Delete SE Profile content

> **TIP**
>
> You can delete SE Profile content only when the SE Profile is in the **Draft** state.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.
3. On the SE Profile page, click the Options ⋮ icon for the corresponding node (ISD, AMSD, SSD, CAP, or Instance) and select **Delete**.



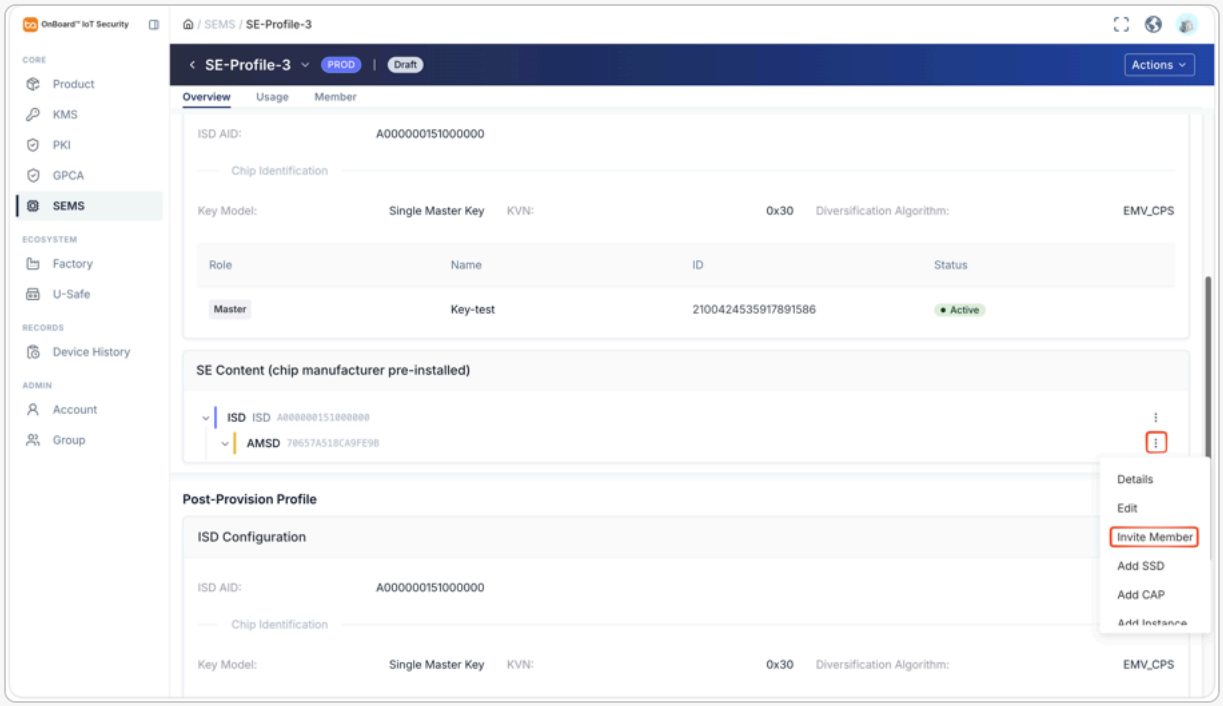
4. In the **Confirm Action** window, click **Confirm** to delete the content of this SE Profile.



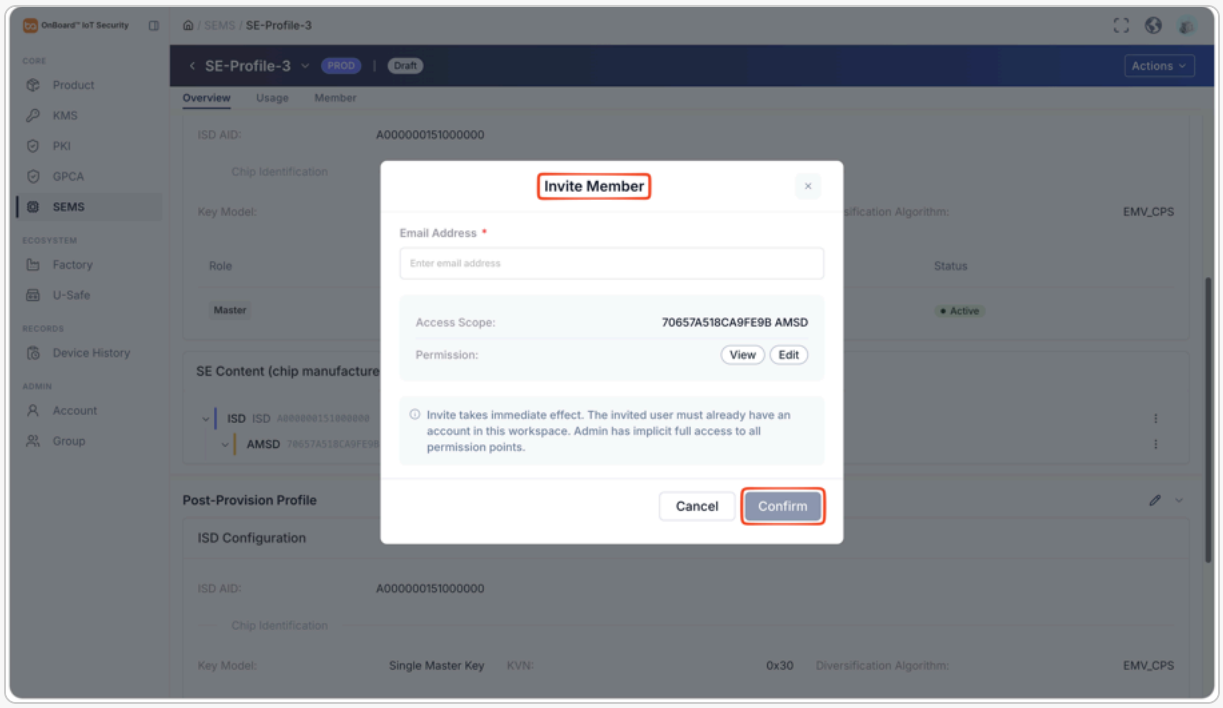
Invite AMSD members

> **TIP**
>
> You can invite AMSD members only when an SE Profile is in the **Draft** state. AMSD members are permitted to edit only the AMSD content.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.
3. On the SE Profile page, click the Options ⋮ icon for the AMSD and select **Invite Member**.



4. In the **Invite Member** window, enter the user email address and confirm the access scope and permissions. The added user must be in the **Active** state.



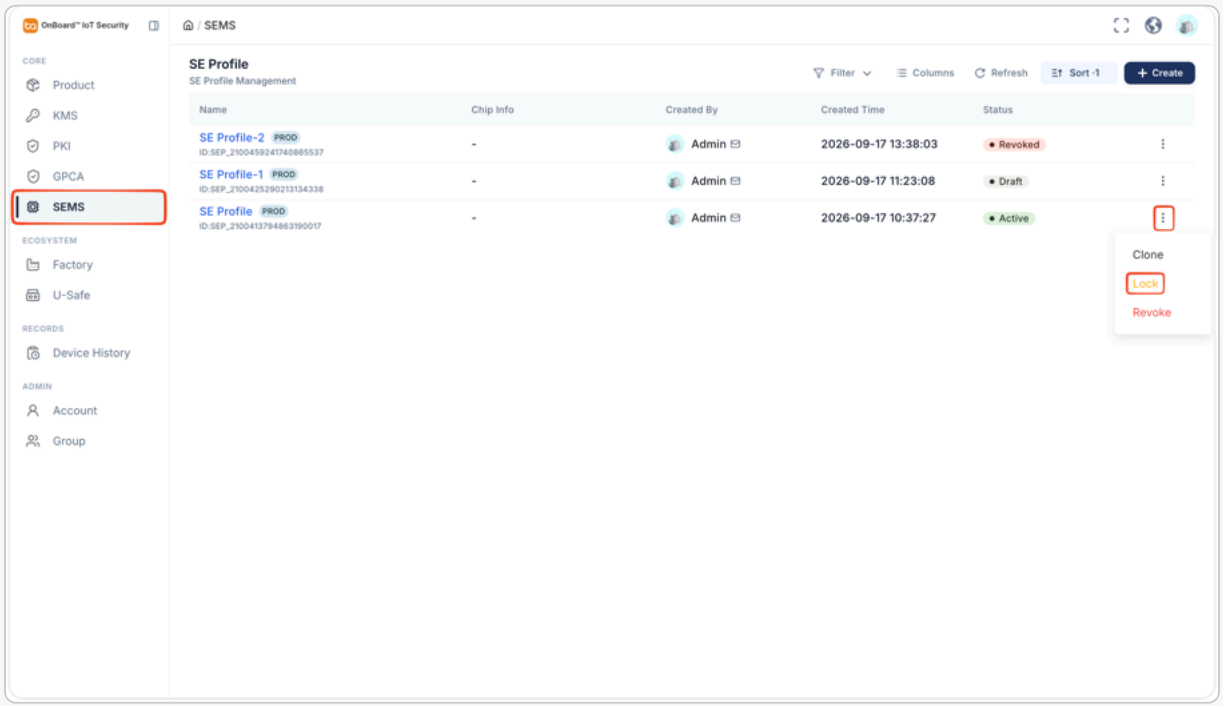
5. Click **Confirm** to invite AMSD members.

Lock or unlock an SE Profile

> **TIP**
>
> Only SE Profiles with the status of **Active** can be locked or unlocked. Lock the SE Profile to prevent its use. Once locked, its status will change to **Locked**.

1. Sign in to OBIS.

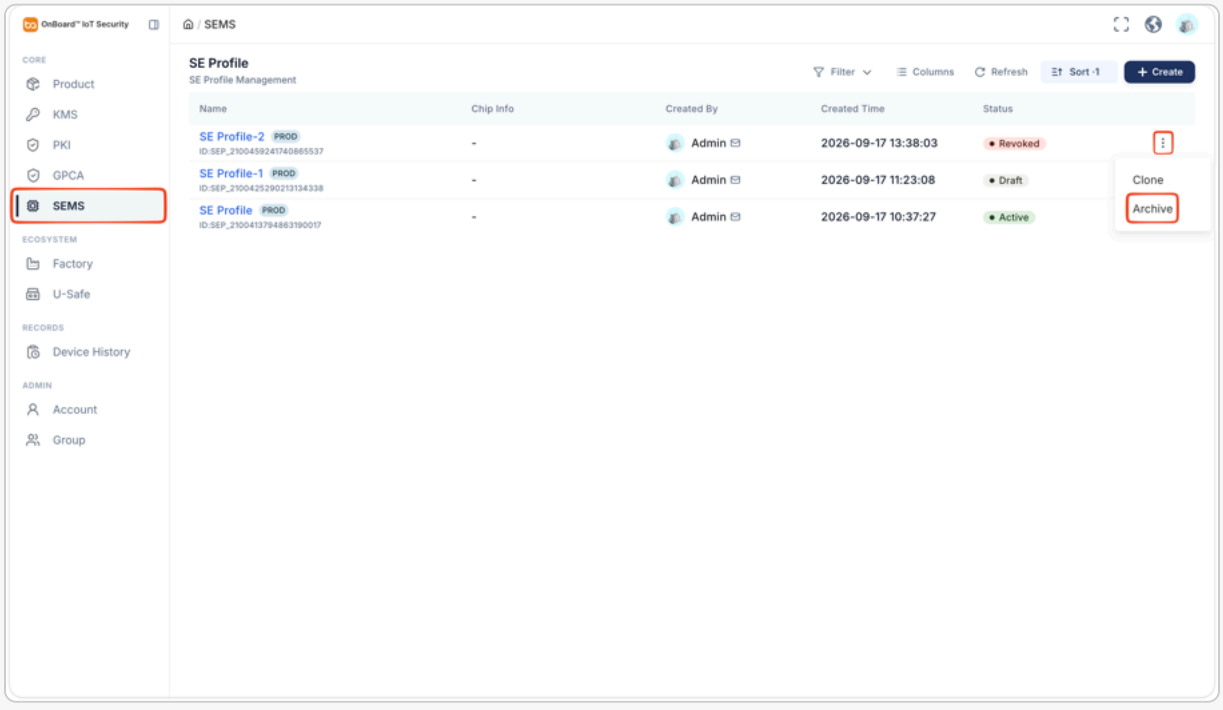
2. In the **Core** section of the left menu, click **SEMS**, and then click the Options icon for the SE Profile and select **Lock** or **Unlock**. Click **Confirm** to lock or unlock the SE Profile. When locking an SE Profile, you can optionally provide a reason.



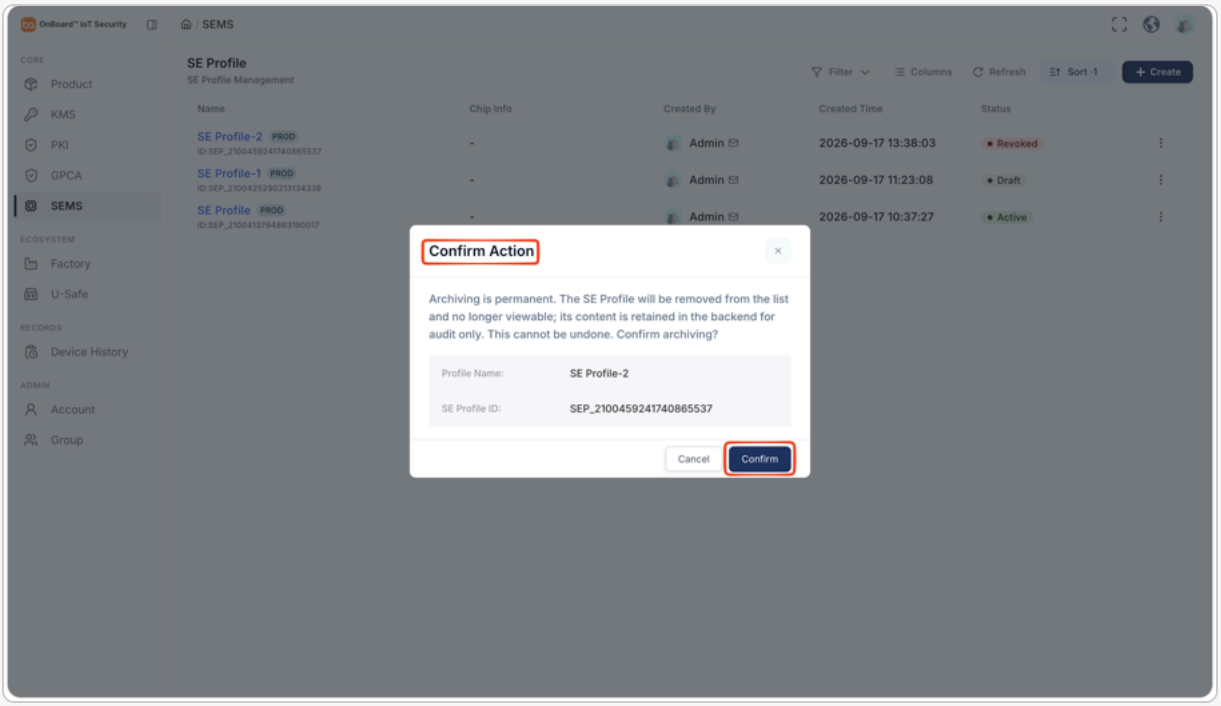
Archive an SE Profile

> **TIP**
>
> Only SE Profiles with the status of **Revoked** can be archived. Once archived, the SE Profile can't be edited, and its content will be retained solely in the backend for audit purposes and can't be restored.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then click the Options icon for the SE Profile and select **Archive**.



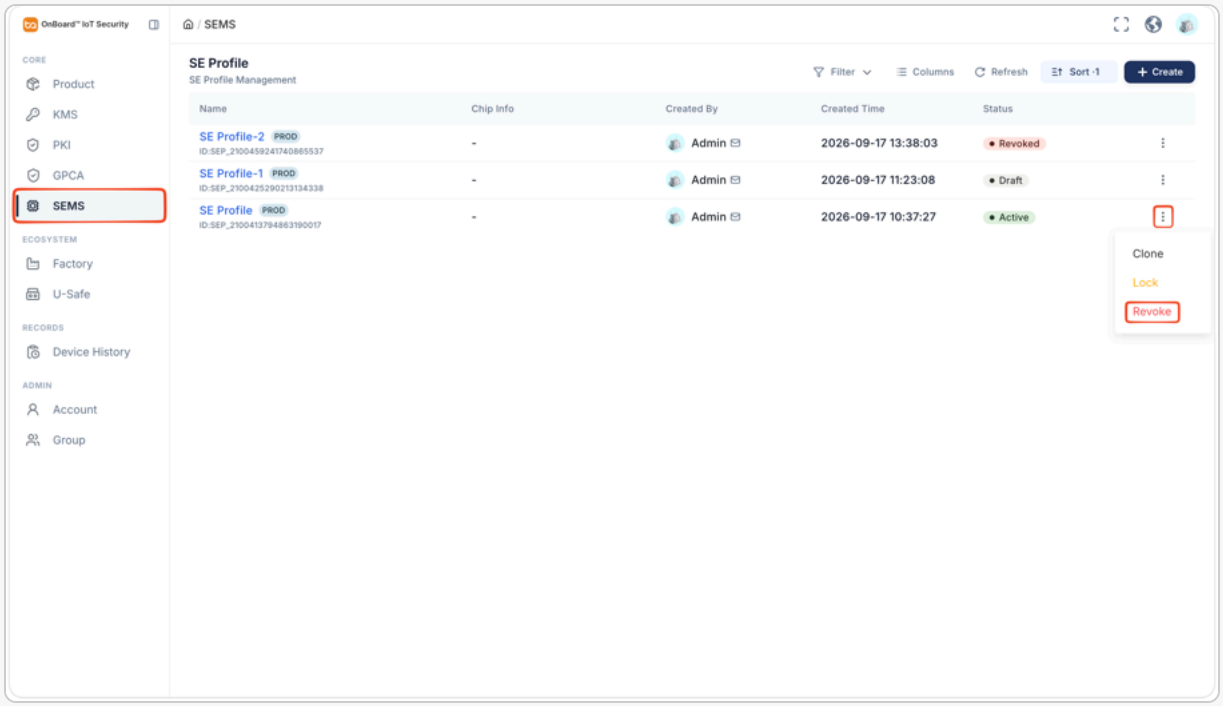
3. In the **Confirm Action** window, click **Confirm** to revoke the SE Profile.



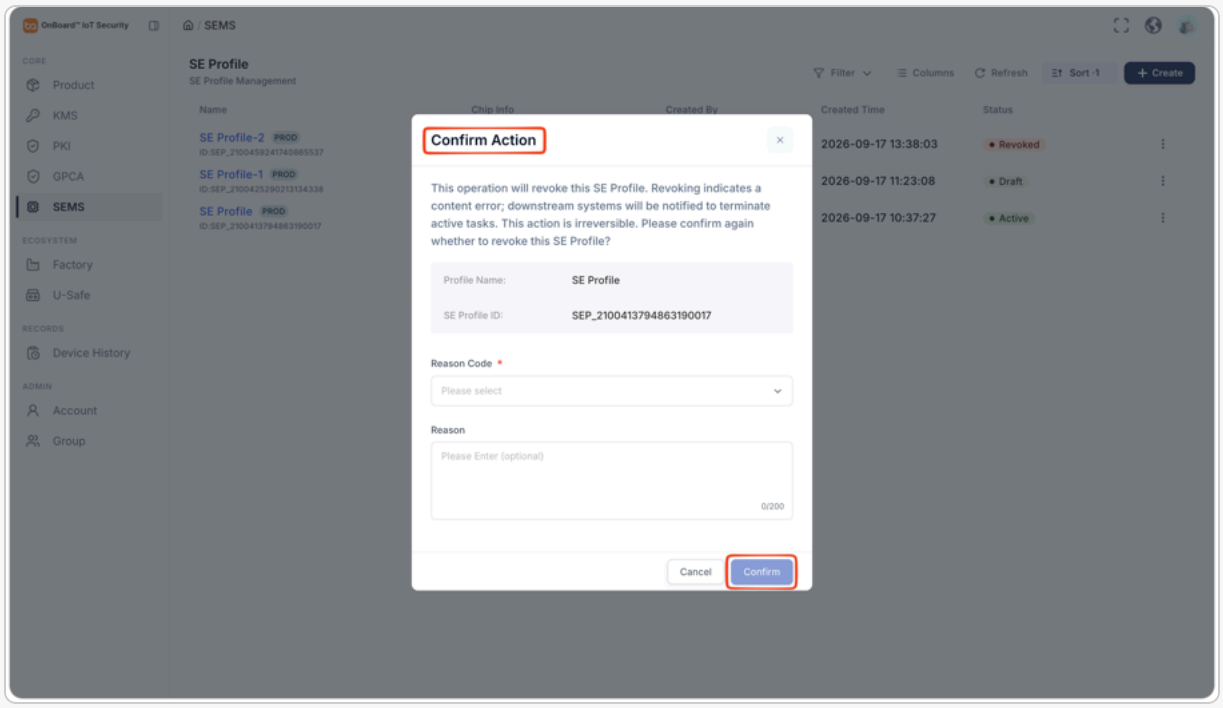
Revoke an SE Profile

> **TIP**
>
> Only SE Profiles with the status of **Active** can be revoked. Once revoked, downstream systems will be notified to terminate any ongoing tasks associated with that SE Profile.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then click the Options ⋮ icon for the SE Profile and select **Revoke**.



3. In the **Confirm Action** window, select the **Reason Code** and enter the **Reason**, then click **Confirm** to revoke the SE Profile.

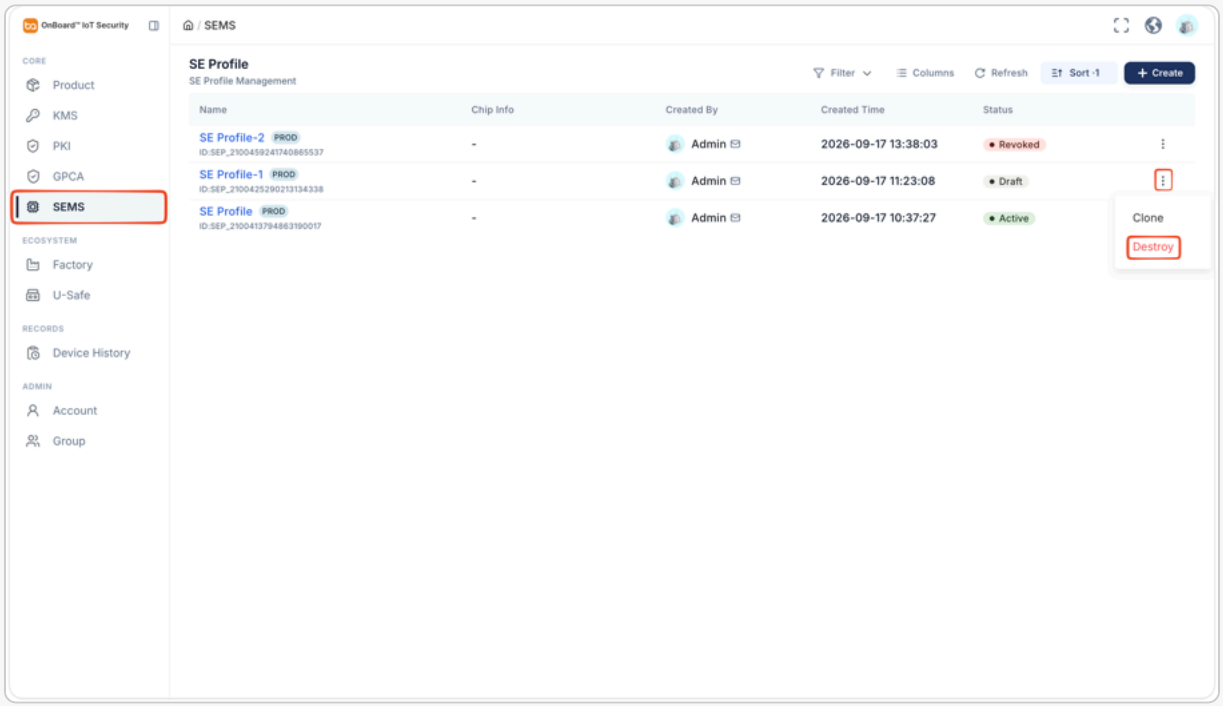


Destroy an SE Profile

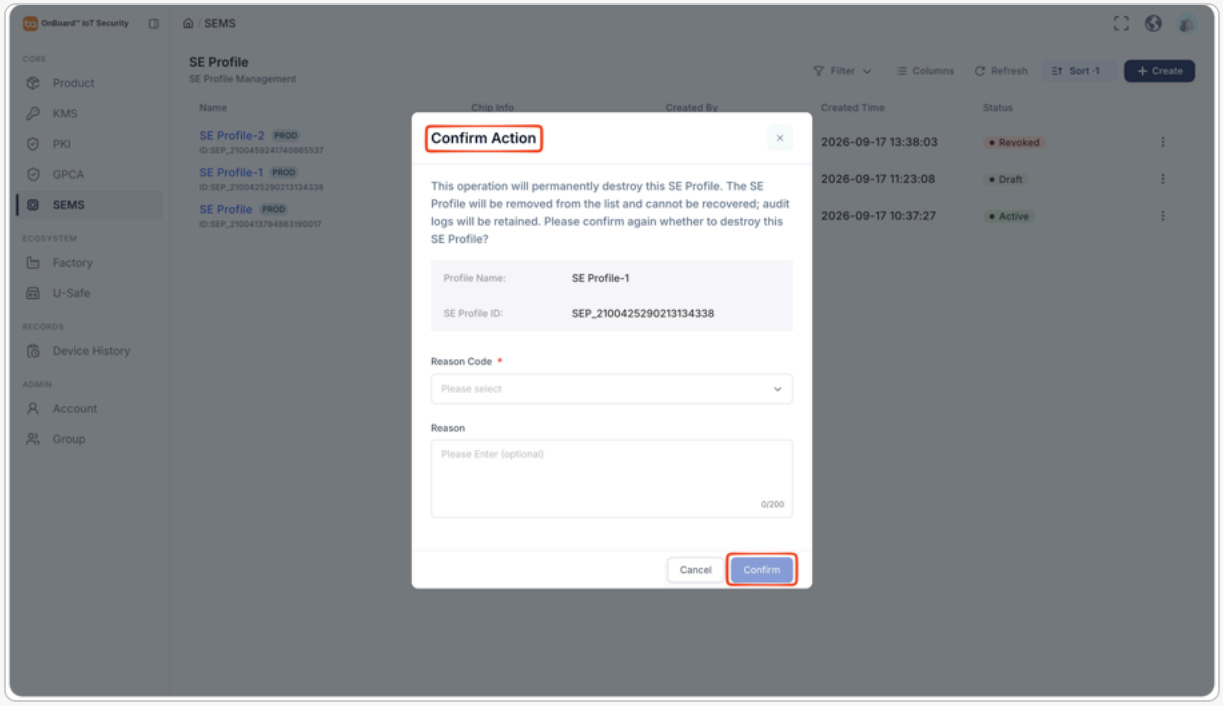
> **WARNING**
>
> Destroyed SE Profiles cannot be recovered. Please proceed with caution.

> **TIP**
>
> Only SE Profiles with the status of **Draft** can be destroyed.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then click the Options icon for the SE Profile and select **Destroy**.



3. In the **Confirm Action** window, select the **Reason Code** and enter the **Reason**, then click **Confirm** to destroy the SE Profile.


OnBoard™ IoT Security
SEMS
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
SE Profile
SE Profile Management
Filter
Columns
Refresh
Sort ·1
+ Create
Name
Chip Info
Created By
Created Time
Status
SE Profile-2 PROD
SE Profile-1 PROD
SE Profile PROD
2026-09-17 13:38:03
Revoked
2026-09-17 11:23:08
Draft
2026-09-17 10:37:27
Active
Confirm Action
This operation will permanently destroy this SE Profile. The SE Profile will be removed from the list and cannot be recovered; audit logs will be retained. Please confirm again whether to destroy this SE Profile?
Profile Name:
SE Profile-1
SE Profile ID:
SEP_2100425290213134338
Reason Code *
Please select
Reason
Please Enter (optional)
0/200
Cancel
Confirm

Version: v3.4.0 (Latest)

How to manage scripts in OnBoard™ IoT Security

> **TIP**
>
> When the SE Profile is in the **Draft** state, the **Script** tab is not displayed.

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Generate a script
- Download a script
- Delete a script

Prerequisites

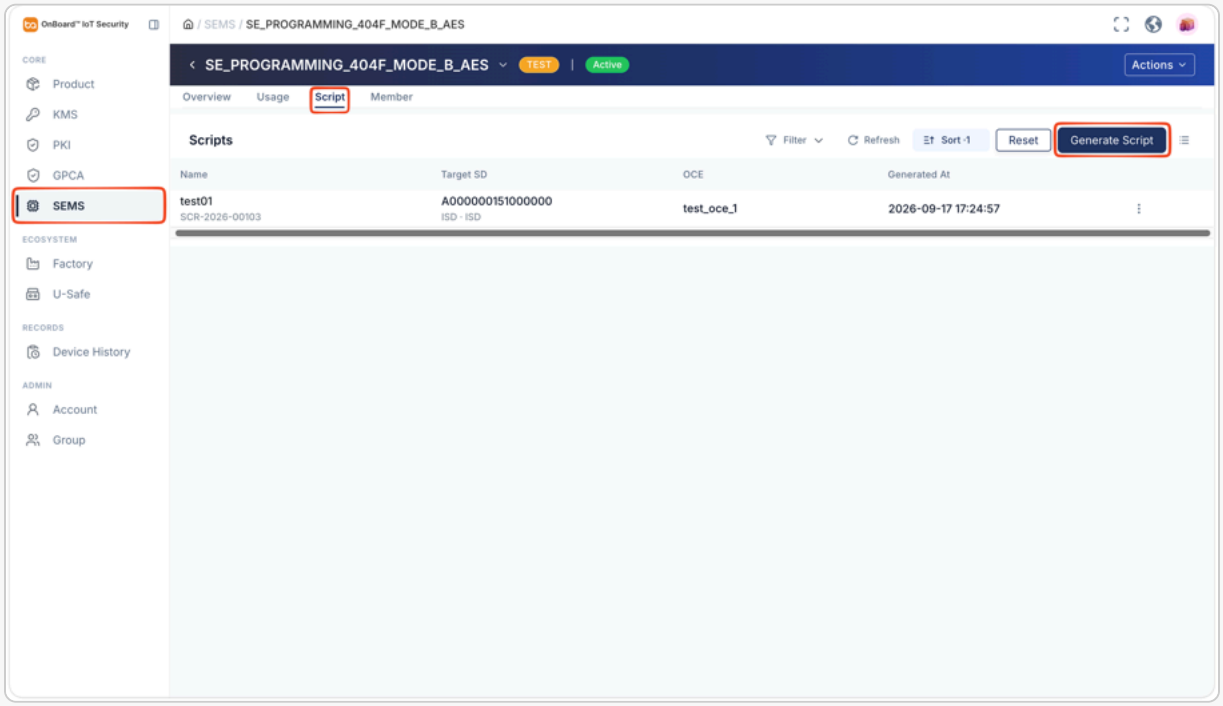
Before getting started, please ensure that:

- You have OBIS role permissions as a System Manager or SE Resource Manager.
- You have permissions for the corresponding SE Profile.

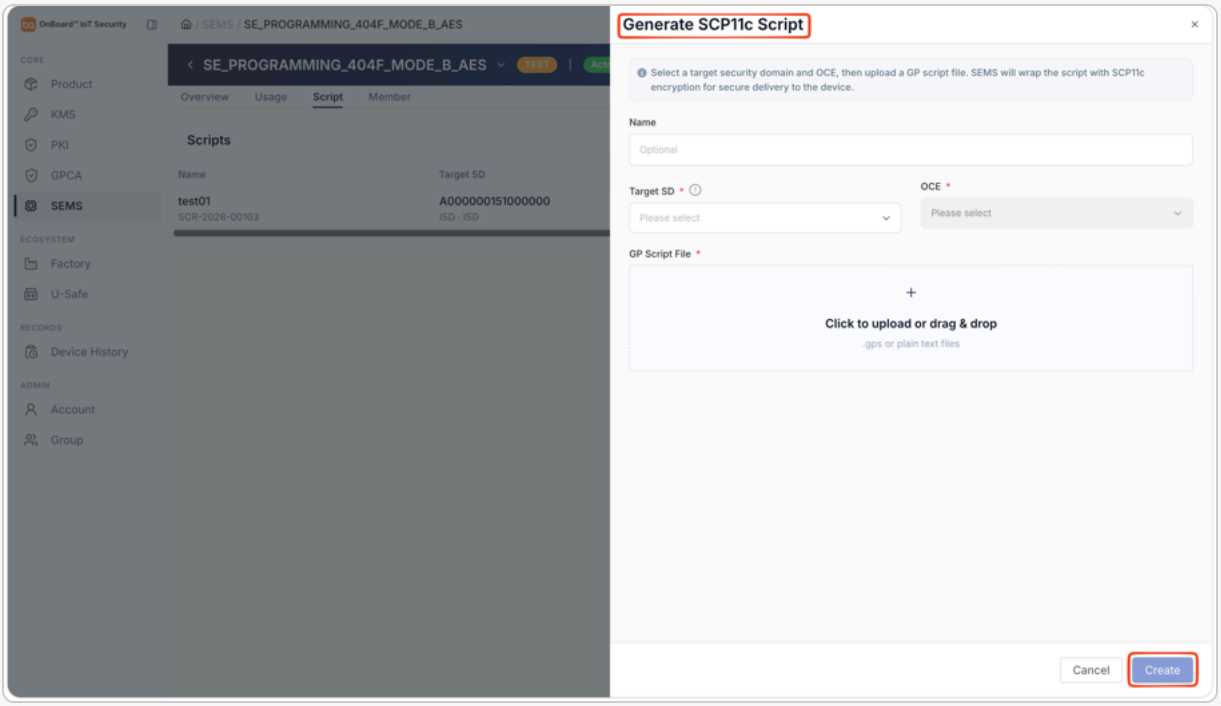
Generate a script

> **TIP**
>
> SEMS uses the SCP11c security protocol to encrypt and encapsulate scripts, ensuring their secure delivery to devices.

1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.
3. On the **Scripts** tab of the SE Profile page, click **Generate Script**.



4. In the **Generate SCP11c Script** panel, select and upload the relevant information.



Description of the script information:

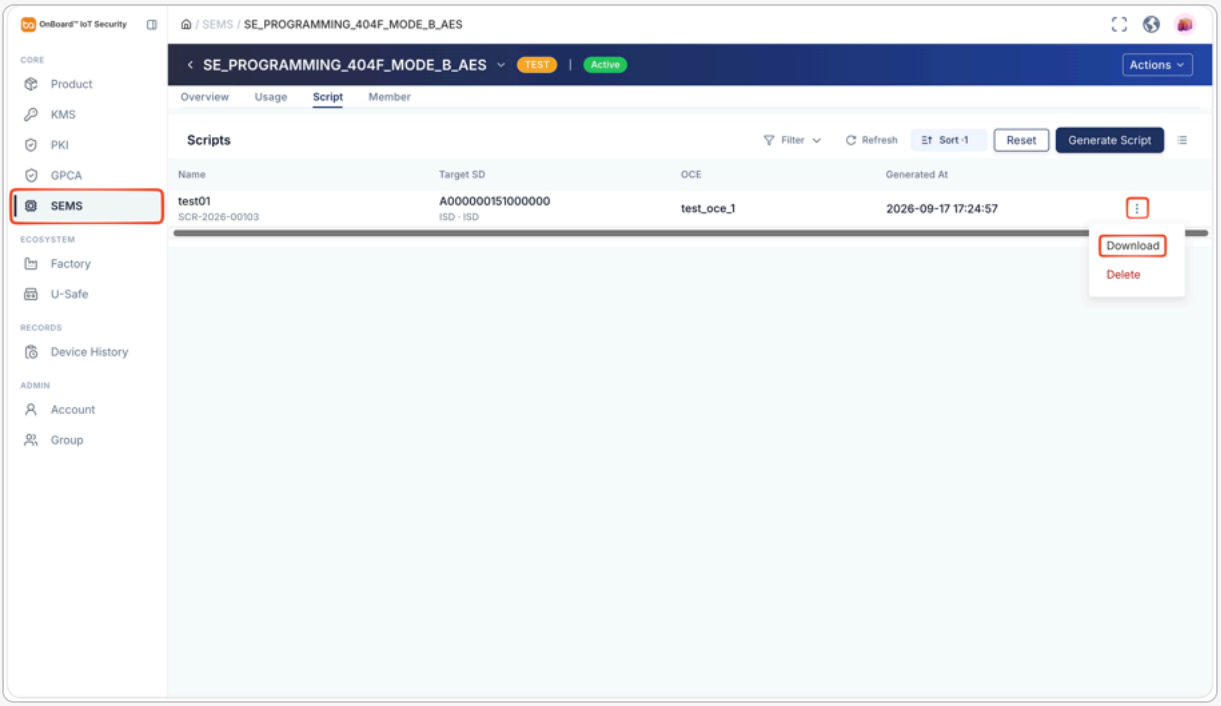
Information	Description
Name	The script name.
Target SD	Select the target security domain for which the script is to be generated.
OCE	Select the OCE certificate to be associated with the script. The available options are the OCE certificates defined under CA-KLOC within the SCP11c configuration of the target security domain.

Information	Description
GP Script File	In the **GP Script File** area, click the Add + icon to select and upload a file in .gps or .txt format, or directly drag the script file into the upload area. The maximum supported file size is 1 MB.

5. Click **Create** to generate the script.

Download a script

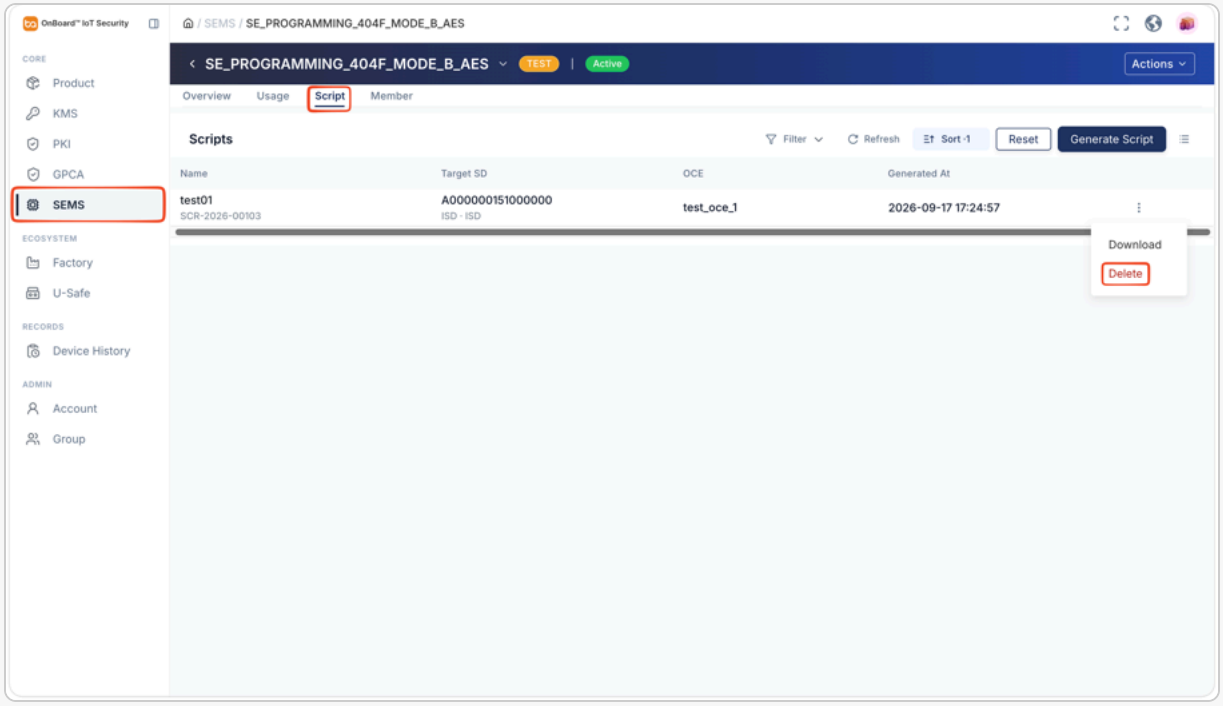
1. Sign in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, and then select the corresponding SE Profile.
3. On the **Scripts** tab of the SE Profile, click the Options ⋮ icon for the corresponding script and select **Download**.



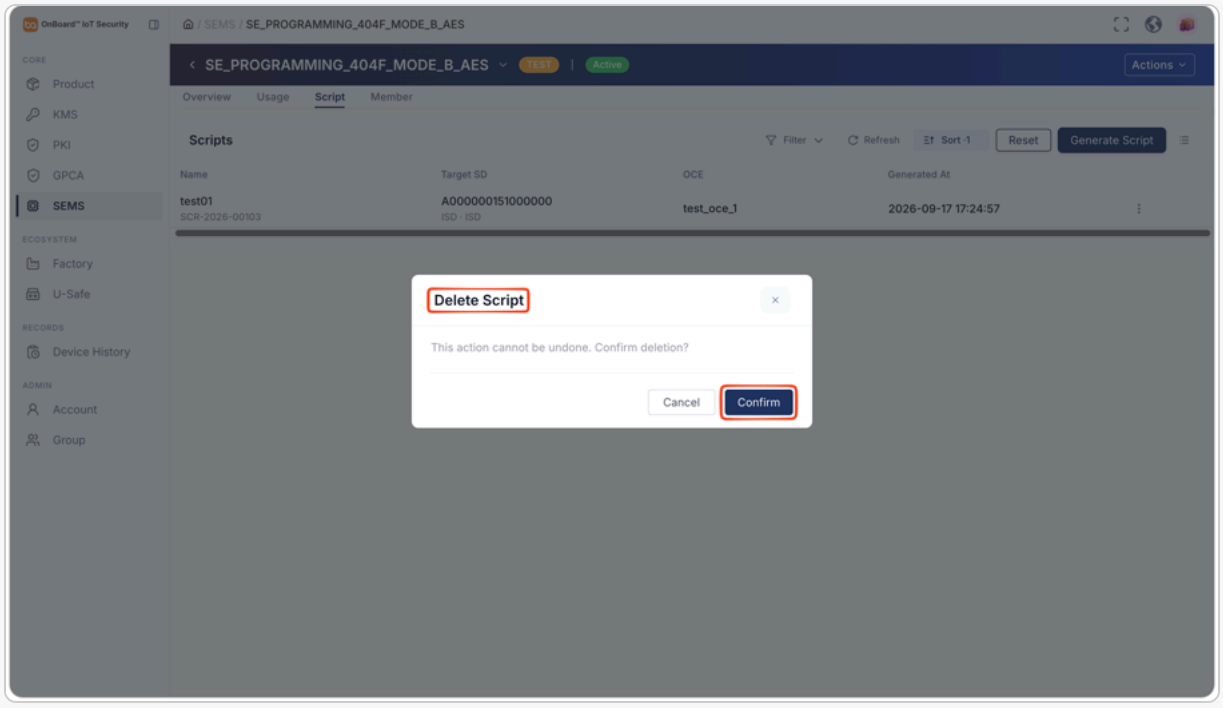
Delete a script

> **WARNING**
>
> The deleted script cannot be recovered. Please proceed with caution.

1. Log in to OBIS.
2. In the **Core** section of the left menu, click **SEMS**, then select the corresponding SE Profile.
3. On the **Script** tab of the SE Profile, click the Options ⋮ icon for the corresponding script and select **Delete**.



4. In the **Delete Script** window, click **Confirm** to delete the script.



Version: v3.4.0 (Latest)

How to create a factory in OnBoard™ IoT Security

> **INFO**
>
> Currently, factories can't be deleted after creation.

This article will guide you on how to create a factory in OnBoard™ IoT Security (OBIS) to configure its basic information, preparing for configuring factory managers, HSM U-Safe, Identity U-Safe, and programming stations.

Factory type

OBIS supports the creation of local factories and cloud factories:

- Local factory: Requires an OnBoard Edge Service deployment on the factory side, typically hosted on a local factory server, to provide on-site production management capabilities. Each local factory is associated with a dedicated OnBoard Edge Service. Once the batch information is synchronized to OnBoard Edge Service, the factory can execute offline programming without requiring a real-time network connection during the process.
- Cloud factory: Production management capabilities are provided through the cloud. A real-time network connection is required during the programming process to ensure batch information synchronization, production data upload, and status updates.

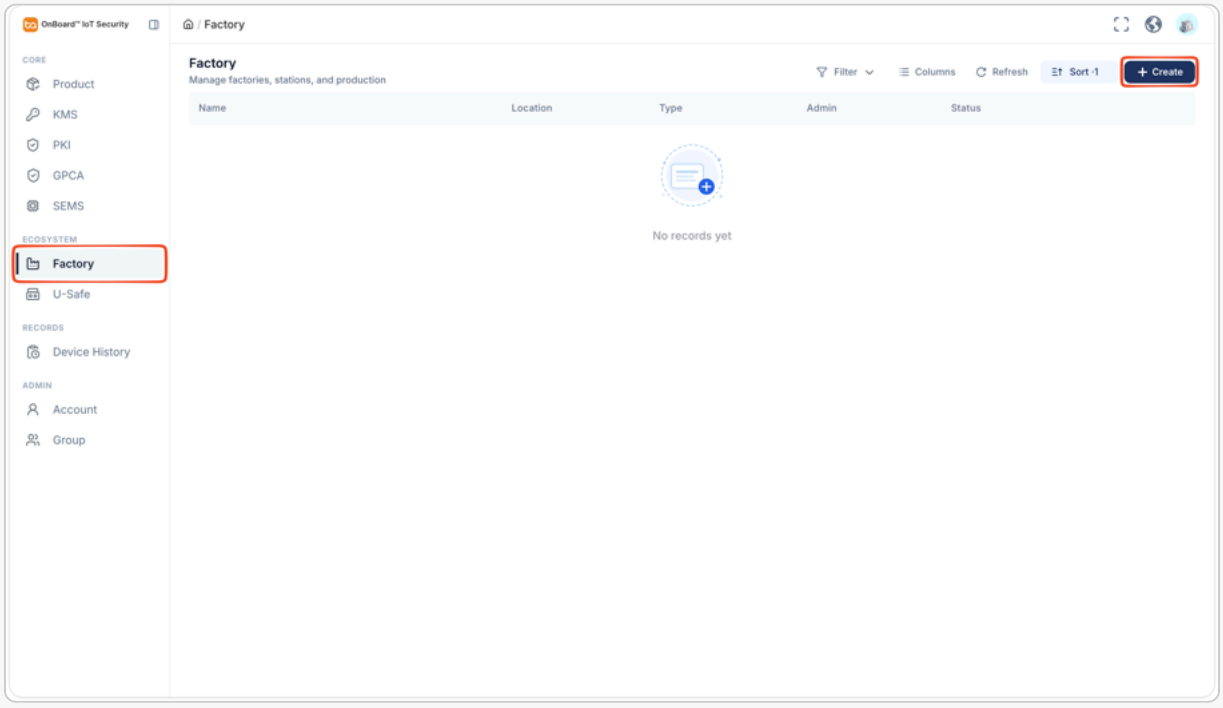
> **TIP**
>
> You can contact Snowball for assistance in deploying OnBoard Edge Service.

Prerequisites

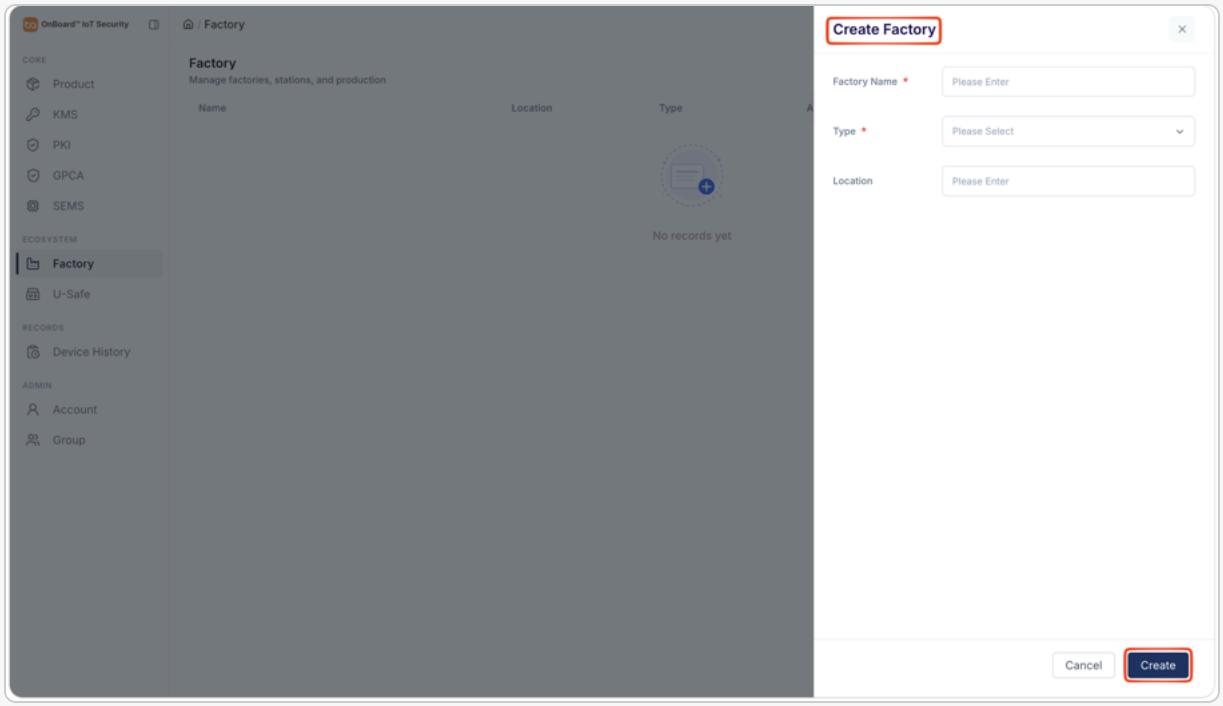
Before getting started, please ensure that you have OBIS role permissions as a System Manager or Factory Manager.

Instructions

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then click **Create**.



3. On the **Create Factory** panel, select and enter the required factory basic information.

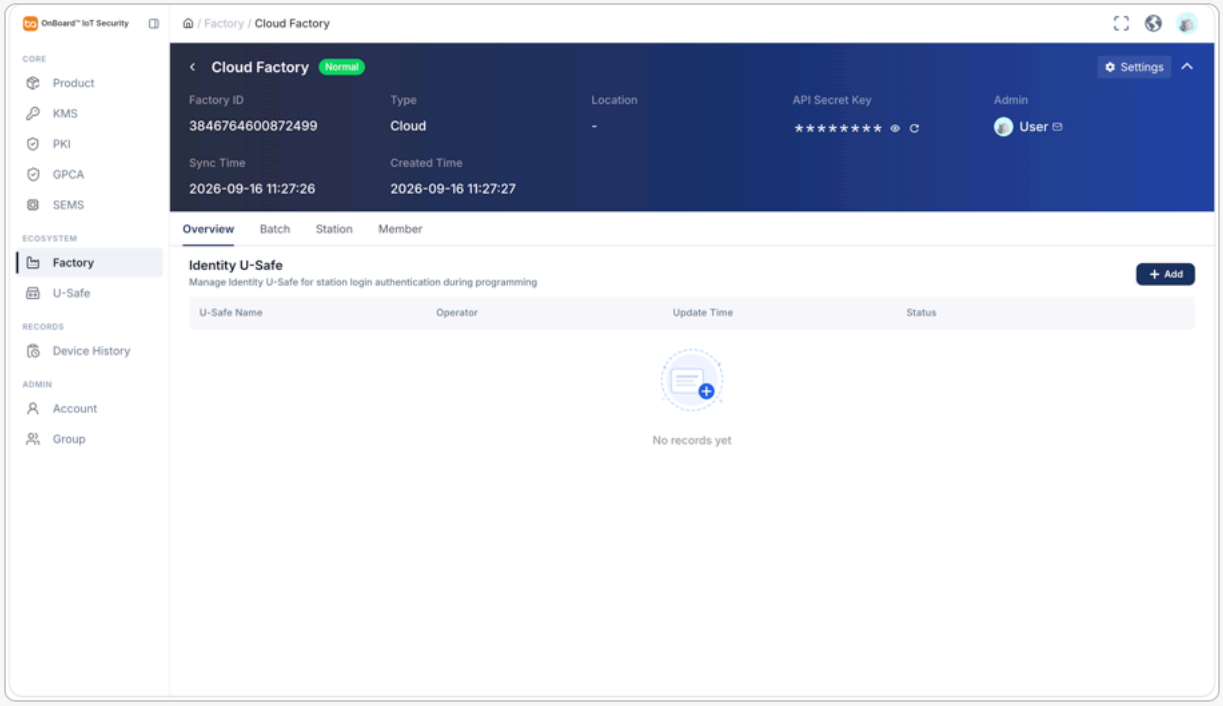


Description of factory basic information:

Information	Mandatory	Description
Factory Name	Yes	The factory name must be unique.
Type	Yes	Two types can be selected: **Local** and **Cloud**.
Location	No	It is recommended to provide the factory address.

4. Click **Create** to complete the factory creation. After creation, you can check the factory-related information on the factory page.

> **TIP**
>
> By default, the factory creator is set as the Admin. To change the Admin, click the Options ⋮ icon for the Admin and select **Transfer Admin** on the **Member** tab, then choose the new Admin and click **Confirm**.
>
> After the factory is created, you can only modify the **Factory Name** and **Location** in **Settings**.
>
> - The initial status of a local factory is **Pending**. Once an HSM U-Safe is added to the local factory, the status will change from **Pending** to **Normal**. For more information, refer to the description of factory status.
> - The initial status of a cloud factory is **Normal**.


OnBoard™ IoT Security
/ Factory / Cloud Factory
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
Cloud Factory
Normal
Settings
Factory ID
3846764600872499
Type
Cloud
Location
-
API Secret Key
****
Admin
User
Sync Time
2026-09-16 11:27:26
Created Time
2026-09-16 11:27:27
Overview
Batch
Station
Member
Identity U-Safe
Manage Identity U-Safe for station login authentication during programming
+ Add
U-Safe Name
Operator
Update Time
Status
No records yet

Version: v3.4.0 (Latest)

How to configure and manage factories in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Add a Factory Manager
- Reset the Factory Admin or Factory Manager password
- Remove a Factory Manager
- Add an HSM U-Safe
- Lock or unlock an HSM U-Safe
- Add an Identity U-Safe
- Unbind, lock, or unlock an Identity U-Safe
- Lock or unlock a factory

Prerequisites

Before getting started, please ensure that:

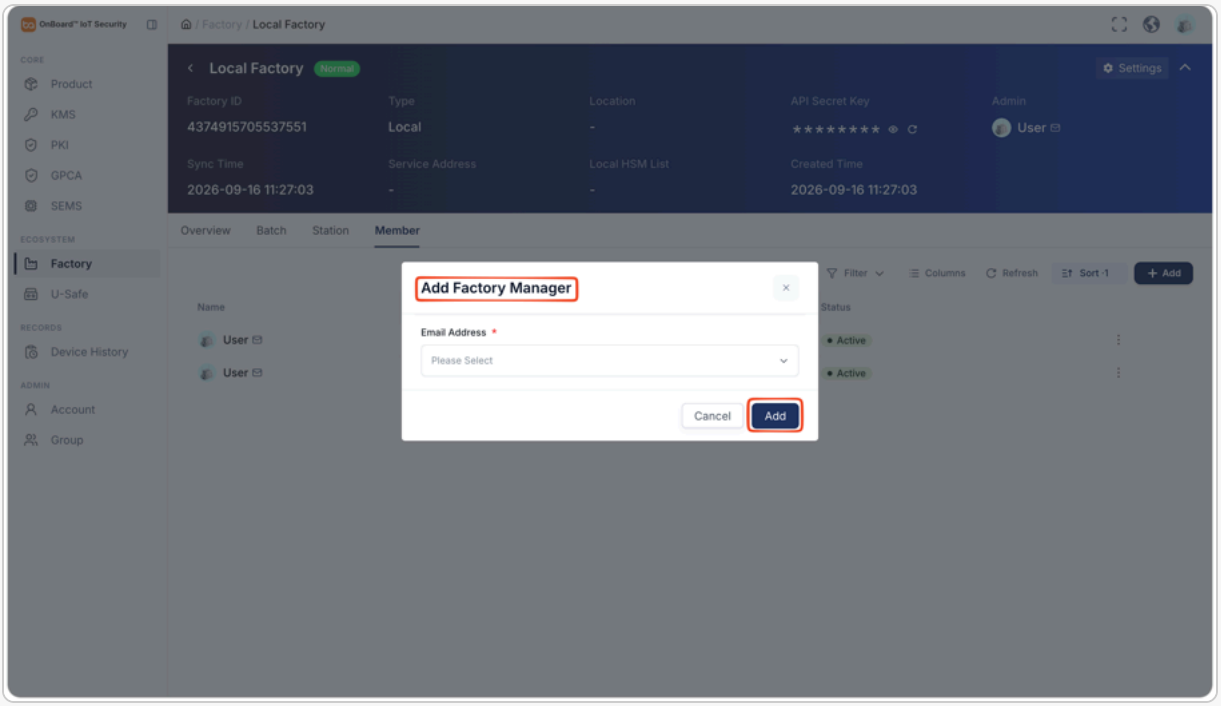
- You have factory role permissions as a Factory Admin or Factory Manager.
- You have obtained the HSM U-Safe and Identity U-Safe required for identity authentication from Snowball.

Add a Factory Manager

> **TIP**
>
> Factory managers can manage and operate factory-related business, and sign in to OnBoard Edge Service using either the "Email + Password" or "Email + Verification code" method.
>
> **Notes**:
>
> - When the Internet is disconnected, OnBoard Edge Service only supports identity verification using the "Email + Password" method.
> - After a Factory Manager is added, the system automatically generates an initial password and sends it to the corresponding email address. Currently, this randomly generated password can be reset, but custom modification is not yet supported.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. Select the **Member** tab, and then click **Add**. In the **Add Factory Manager** window, select and enter the email address of the new Factory Manager.

   > **TIP**
   >
   > The Factory Manager being added must be an **Active** user within the same tenant.



4. Click **Add** to complete adding a Factory Manager.

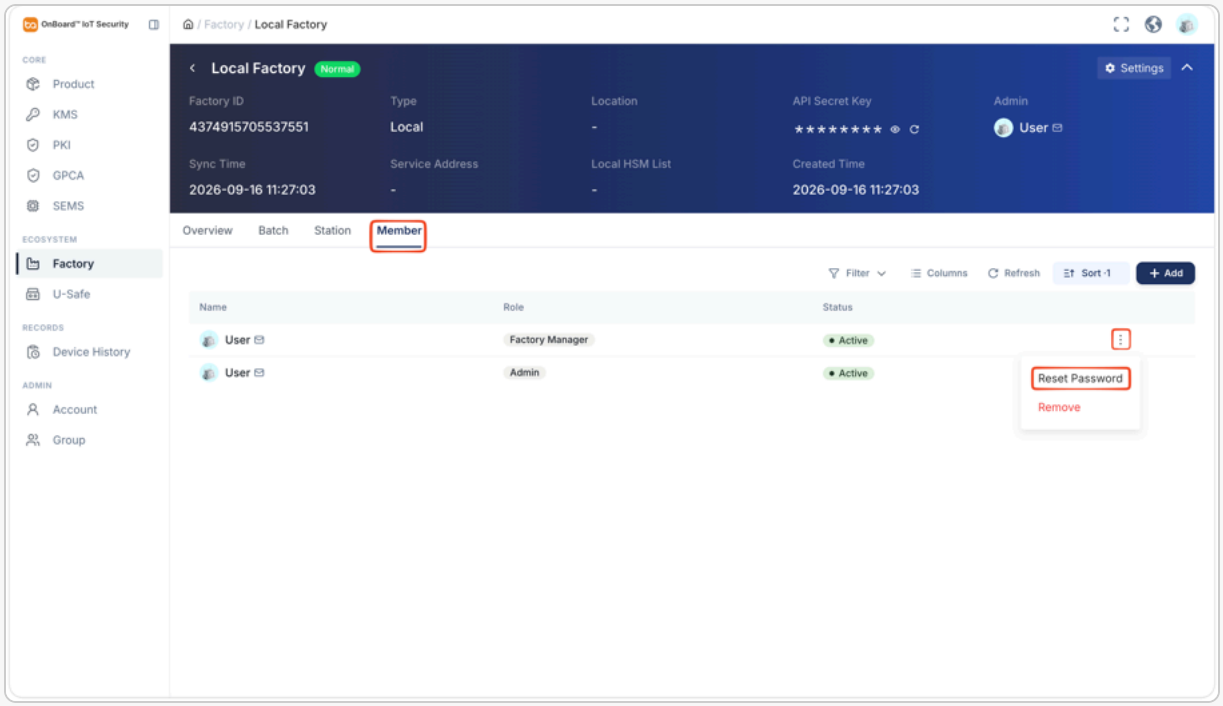
Reset the Factory Admin or Factory Manager password

> **TIP**
>
> After the password is reset, the system automatically generates a random password and sends it to the corresponding email address.

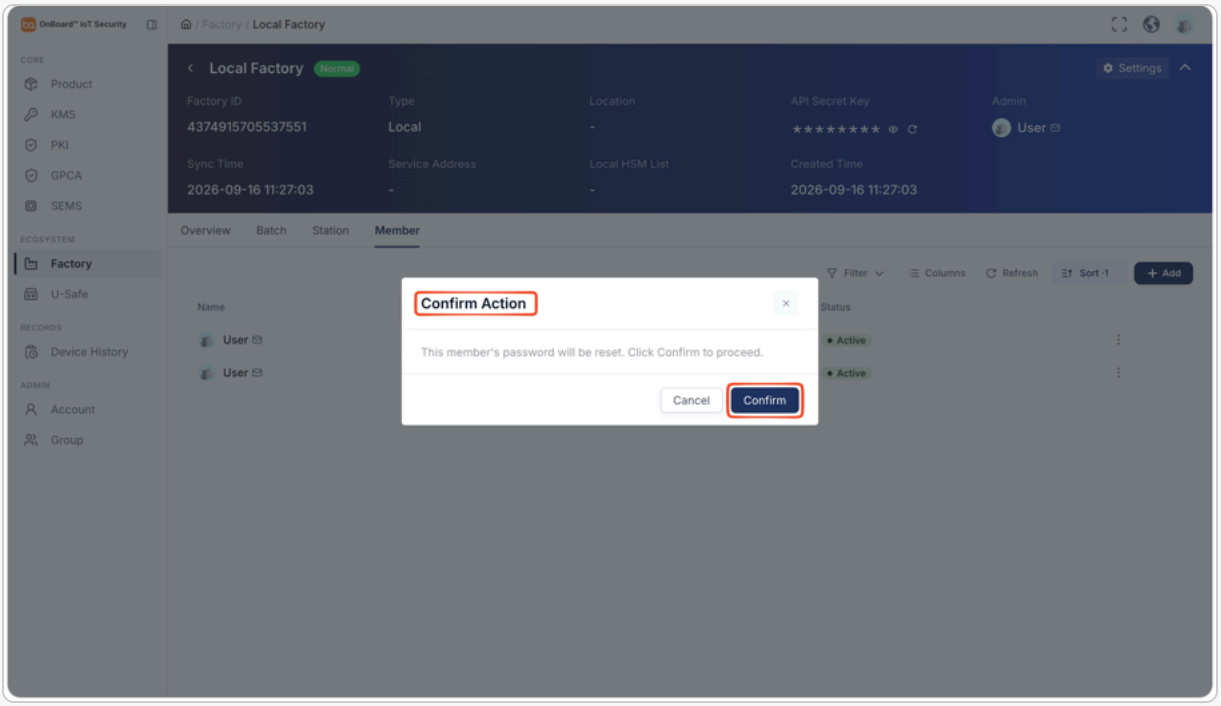
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. Select the **Member** tab, click the Options ⋮ icon for the corresponding Factory Admin or Factory Manager and select **Reset Password**.

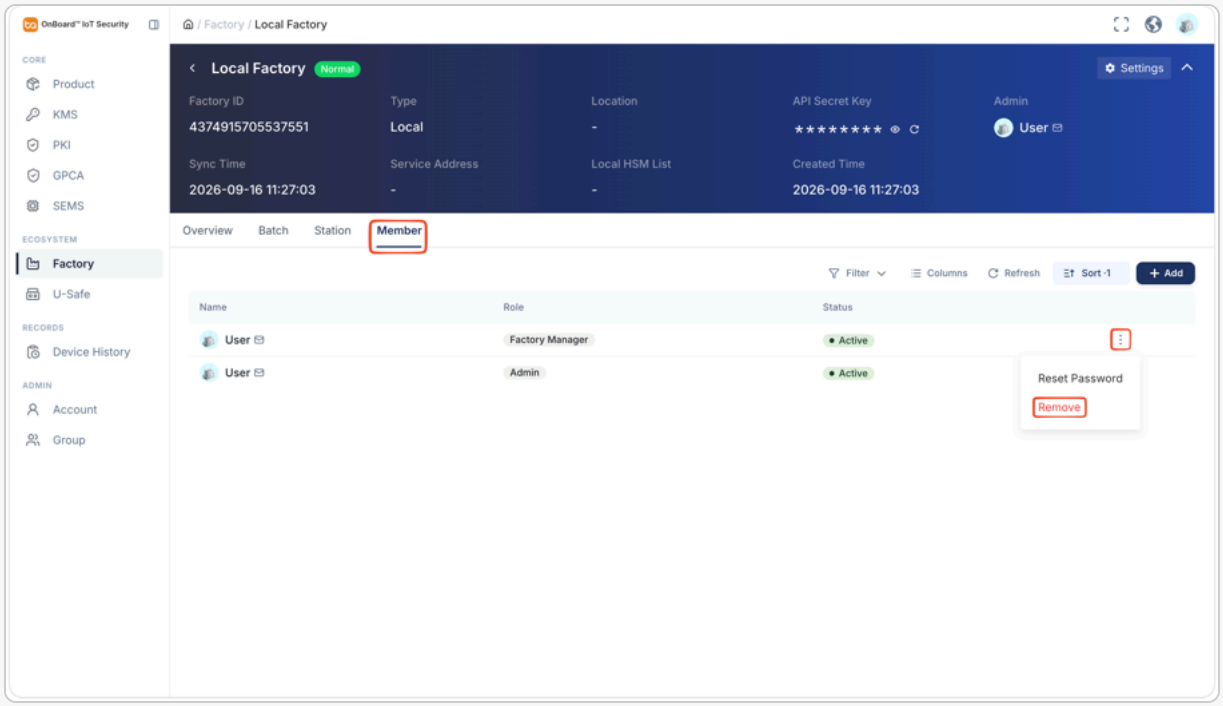


4. In the **Confirm Action** window, click **Confirm** to reset the password.

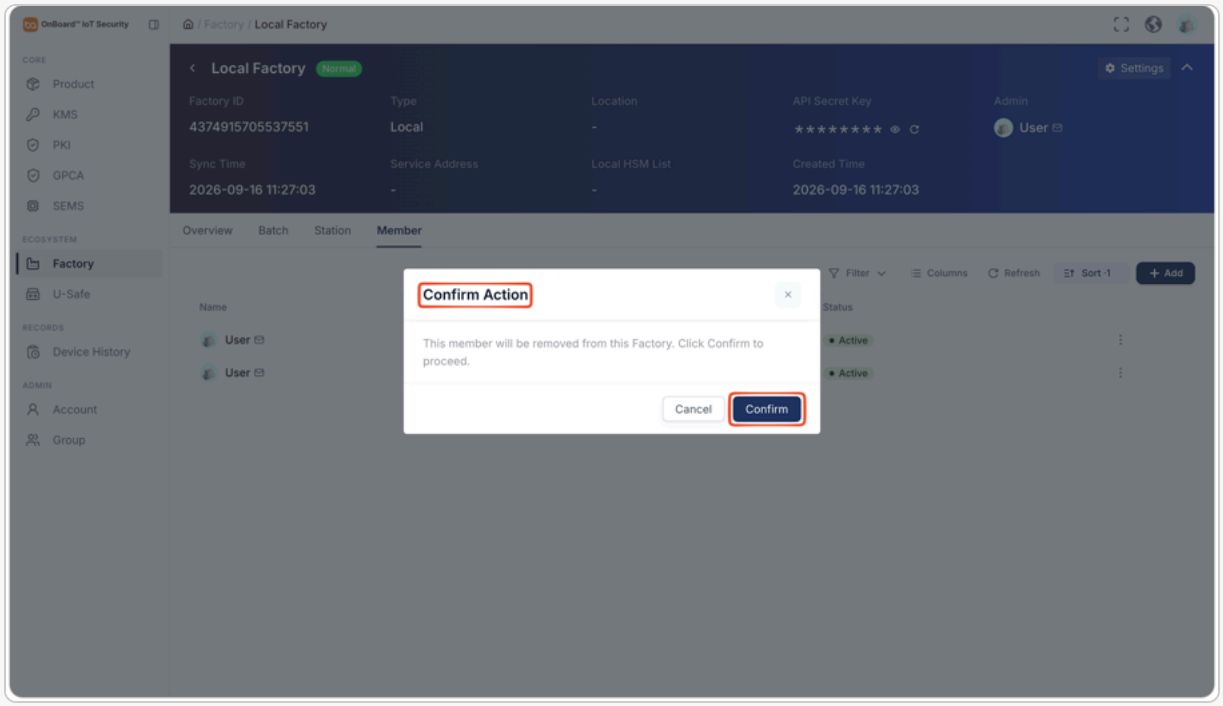


Remove a Factory Manager

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. Select the **Member** tab, click the Options ⋮ icon for the corresponding Factory Manager and select **Remove**.



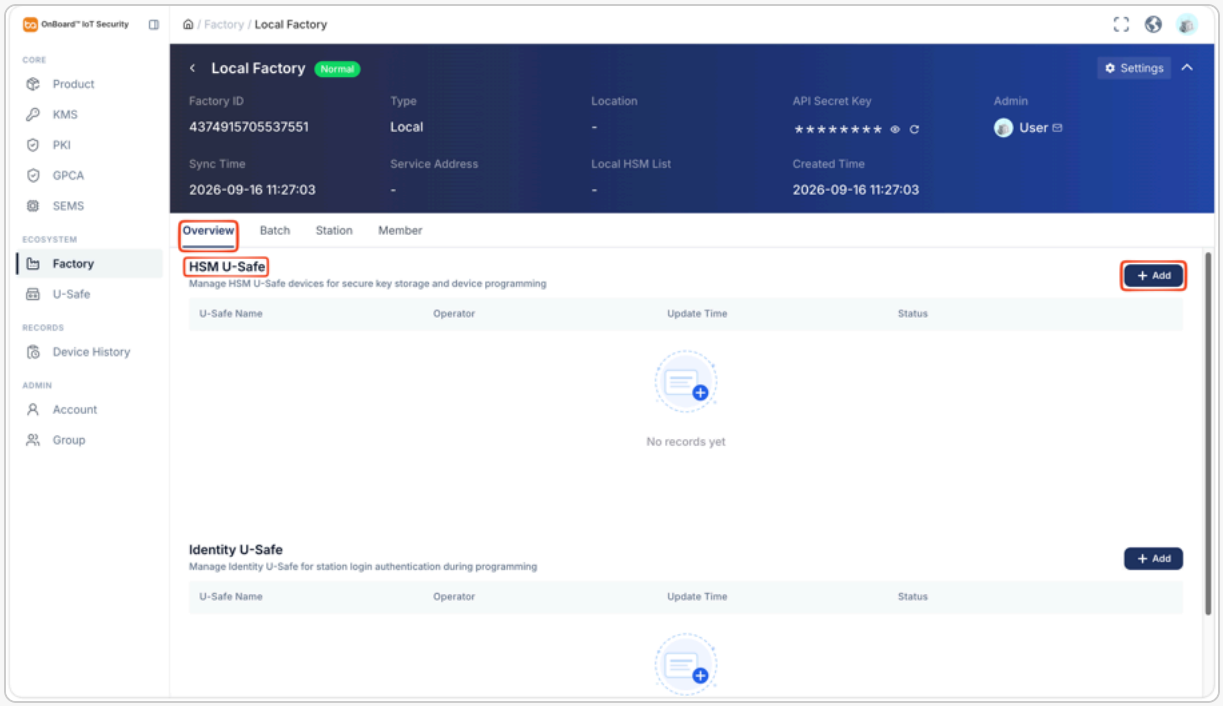
4. In the **Confirm Action** window, click **Confirm** to remove the Factory Manager.



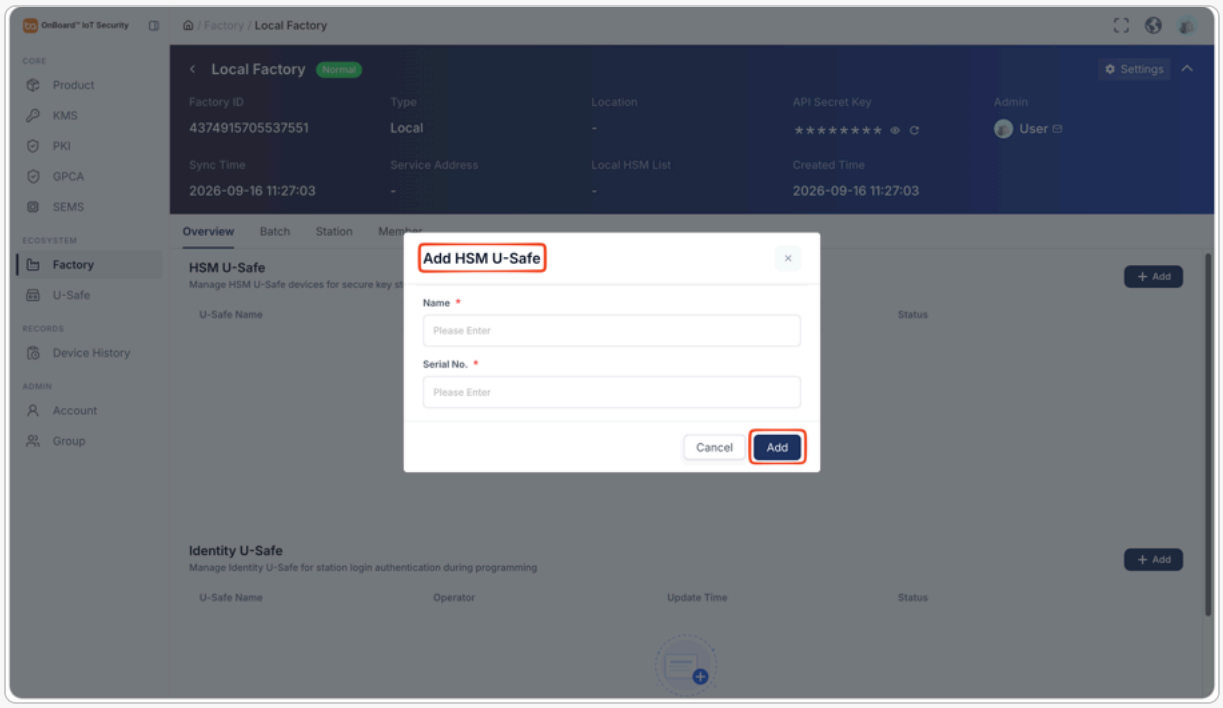
Add an HSM U-Safe

> **TIP**
>
> The purpose of adding an HSM U-Safe is to bind it to the corresponding factory and use it for signing in to OnBoard Edge Service. Meanwhile, secure key storage and device programming support are achieved through the HSM U-Safe management.
>
> Once an HSM U-Safe is added to the factory, the factory status will change from **Pending** to **Normal**.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, locate the **HSM U-Safe** section and then click **Add**.



4. In the **Add HSM U-Safe** window, enter the **Name** (customizable) and **Serial No.** (which can be found on the device) of the HSM U-Safe you want to bind.

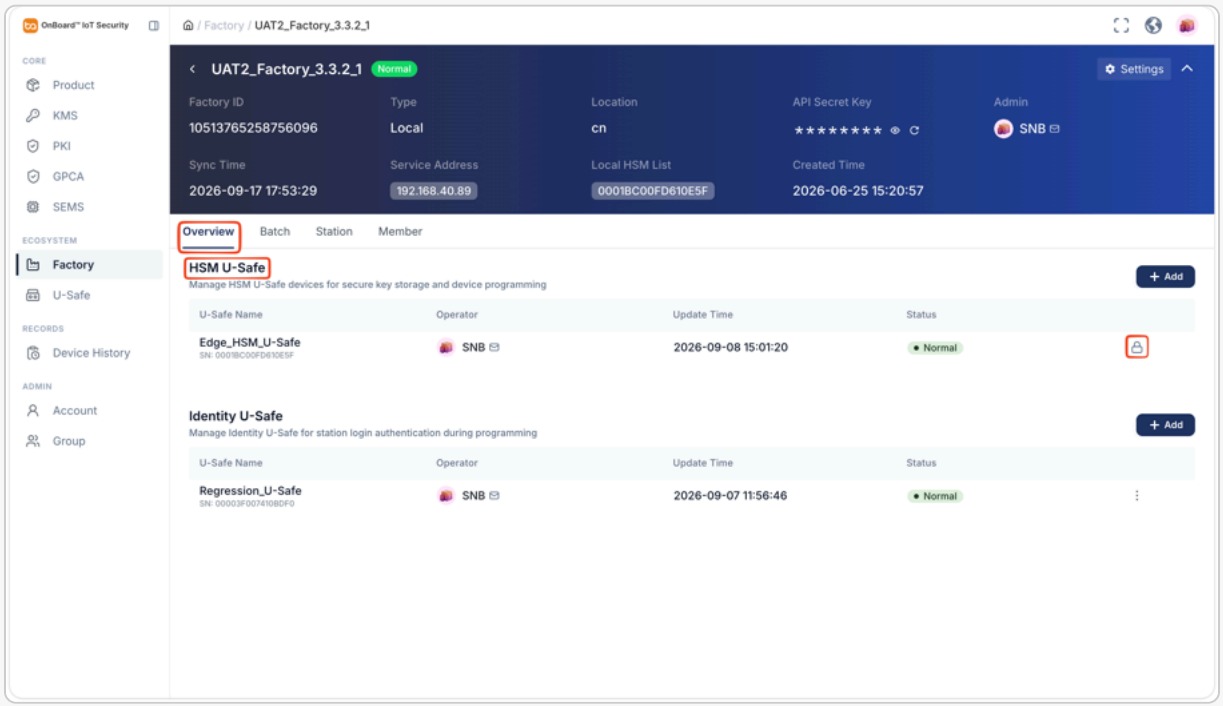


5. Click **Add** to bind the HSM U-Safe.

Lock or unlock an HSM U-Safe

> **TIP**
>
> Lock the HSM U-Safe to prevent its use. Once locked, its status will change to **Locked**.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, locate the **HSM U-Safe** section, and then click the Lock or Unlock icon for the corresponding HSM U-Safe.

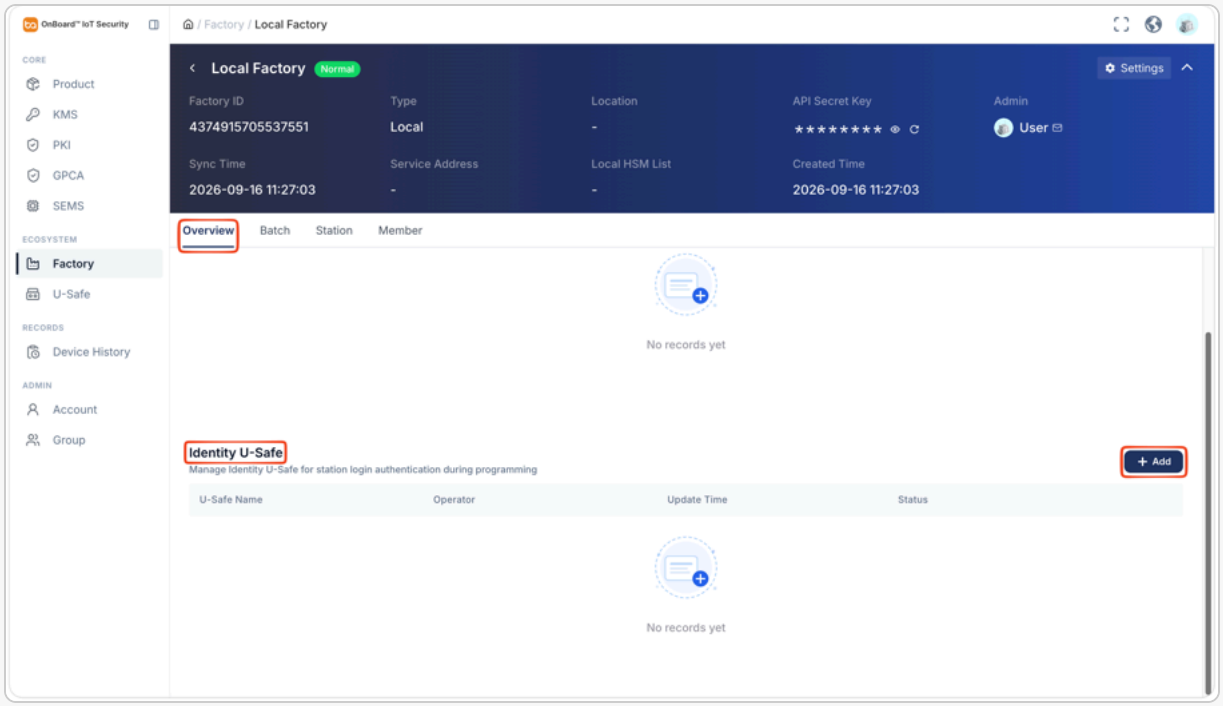


4. In the pop-up window, click **Confirm** to lock or unlock the HSM U-Safe.

Add an Identity U-Safe

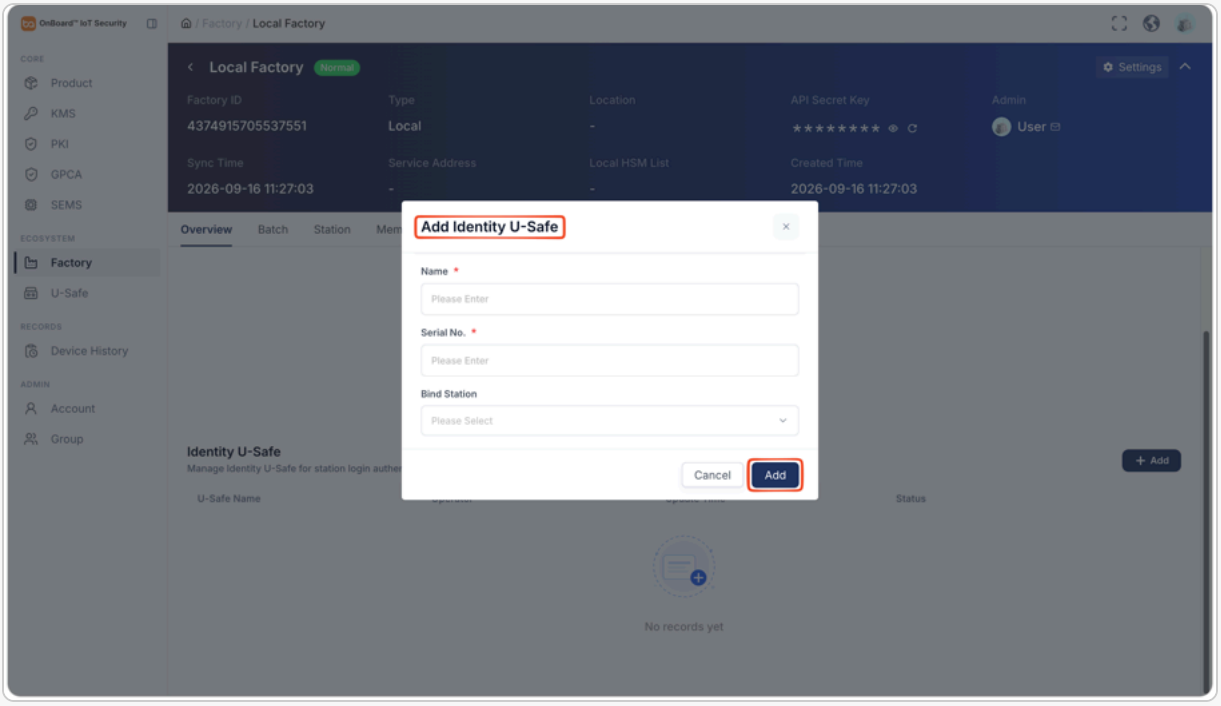
> **TIP**
>
> The purpose of adding an Identity U-Safe is to bind it to the corresponding factory. After binding it to a programming station in OBIS or OnBoard Edge Service, it can be used to sign in to the Programming Station client. Meanwhile, login authentication for the programming station is achieved through the Identity U-Safe management.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, locate the **Identity U-Safe** section and then click **Add**.



4. In the **Add Identity U-Safe** window, enter the **Name** (customizable) and **Serial No.** (which can be found on the device) of the Identity U-Safe you want to bind.

> **TIP**
>
> - If a programming station has already been added, you can select and bind the corresponding programming station.
> - If a programming station hasn't been added yet, you can bind it when adding a programming station.



5. Click **Add** to bind the Identity U-Safe.

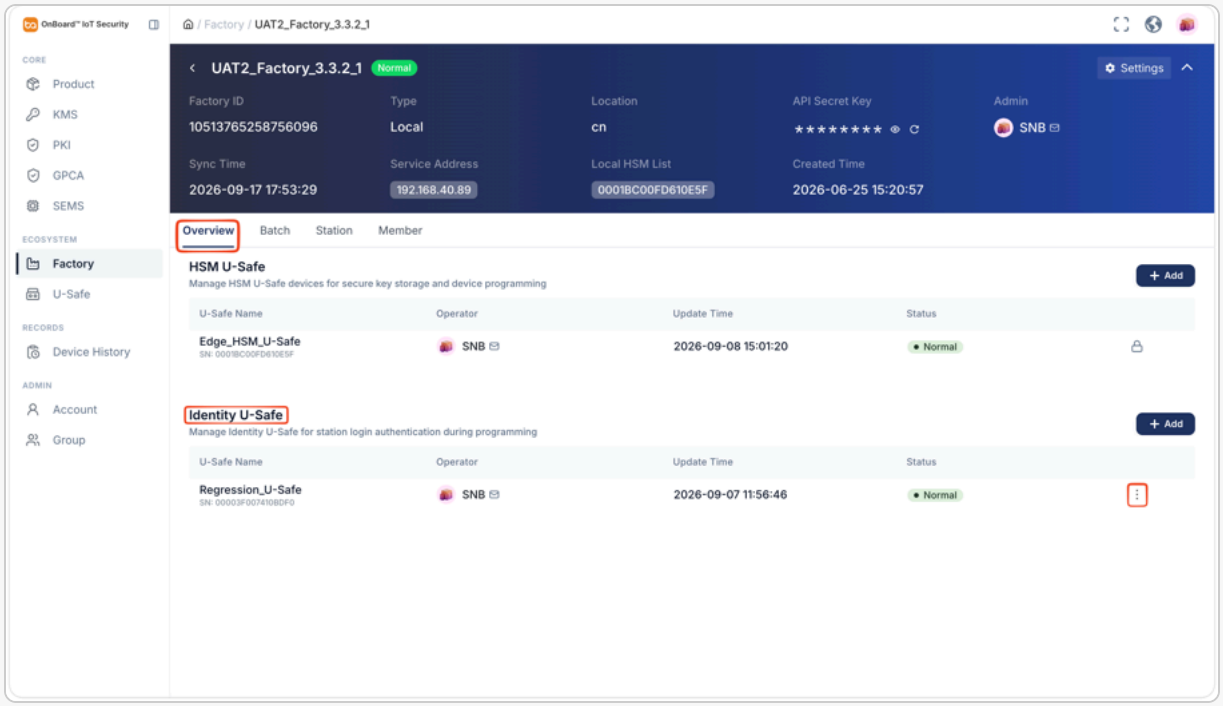
Unbind, lock, or unlock an Identity U-Safe

> **TIP**
>
> Lock the Identity U-Safe to prevent its use and unbinding. Once locked, its status will change to **Locked**.

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, locate the **Identity U-Safe** section, and then click the Options ⋮ icon for the corresponding Identity U-Safe and select **Unbind**, **Lock**, or **Unlock**.



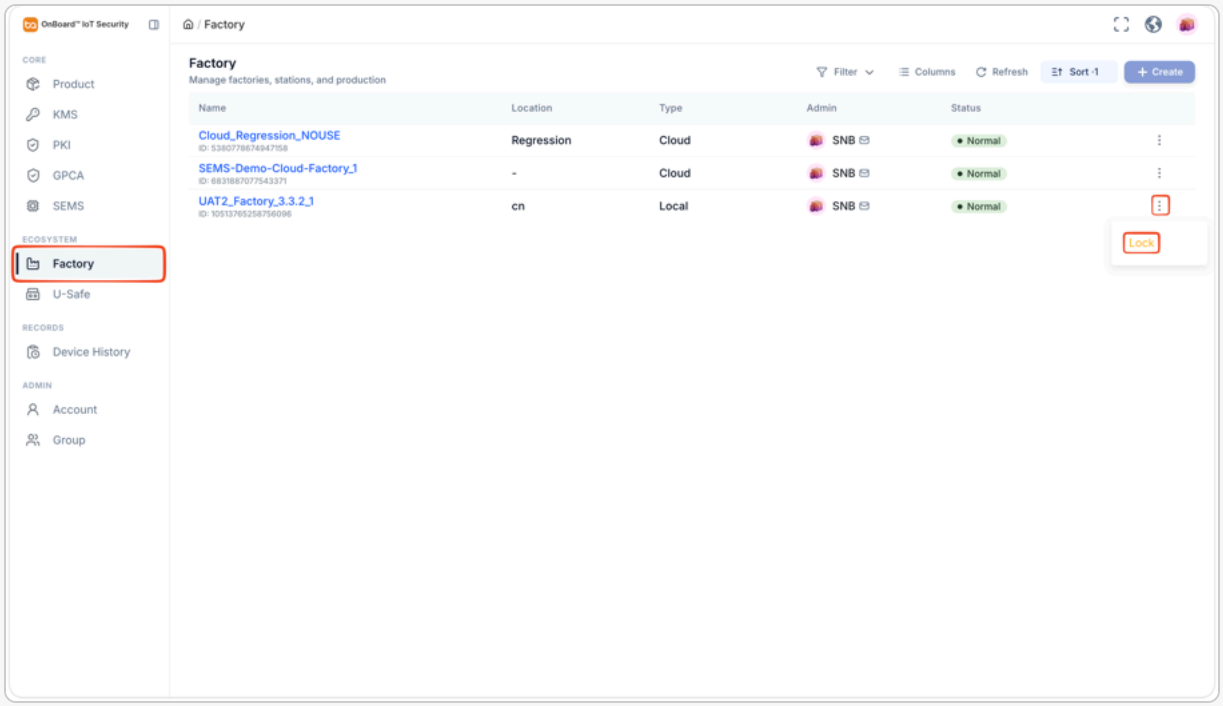
4. In the pop-up window, click **Confirm** to unbind, lock, or unlock the Identity U-Safe.

Lock or unlock a factory

> **TIP**
>
> Lock the factory to prevent its use. Once locked, its status will change to **Locked**.

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then click the Options ⋮ icon for the corresponding factory and select **Lock** or **Unlock** to lock or unlock the factory.



3. In the pop-up window, click **Confirm** to lock or unlock the factory.

Version: v3.4.0 (Latest)

How to configure and manage programming stations in OnBoard™ IoT Security

> **TIP**
>
> You can configure and manage the programming station in OnBoard™ IoT Security (OBIS) or OnBoard Edge Service as needed.

This article will guide you through the following operations in OBIS:

- Create a programming station
- Bind an Identity U-Safe to a programming station
- Unbind an Identity U-Safe from a programming station
- Edit a programming station
- Delete a programming station
- Check the programming station password

Prerequisites

Before getting started, please ensure that:

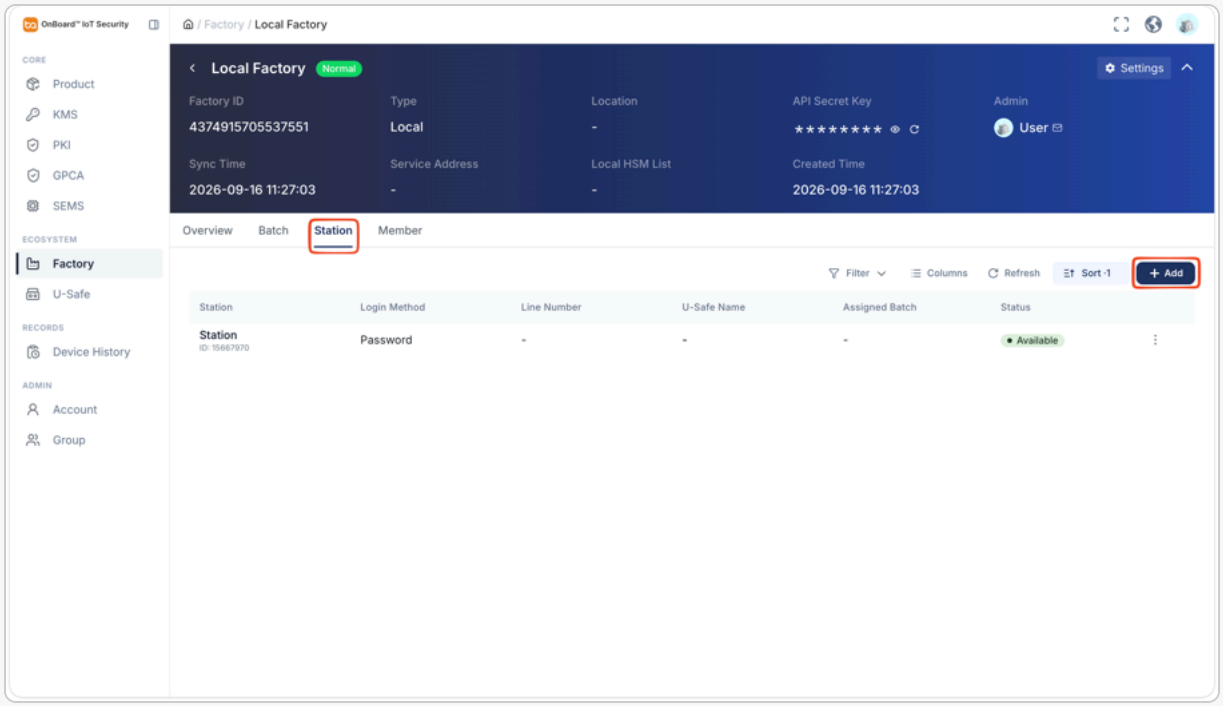
- The factory has already been configured.

- You have factory role permissions as a Factory Admin or Factory Manager.
- You have obtained the Identity U-Safe for identity authentication from Snowball.

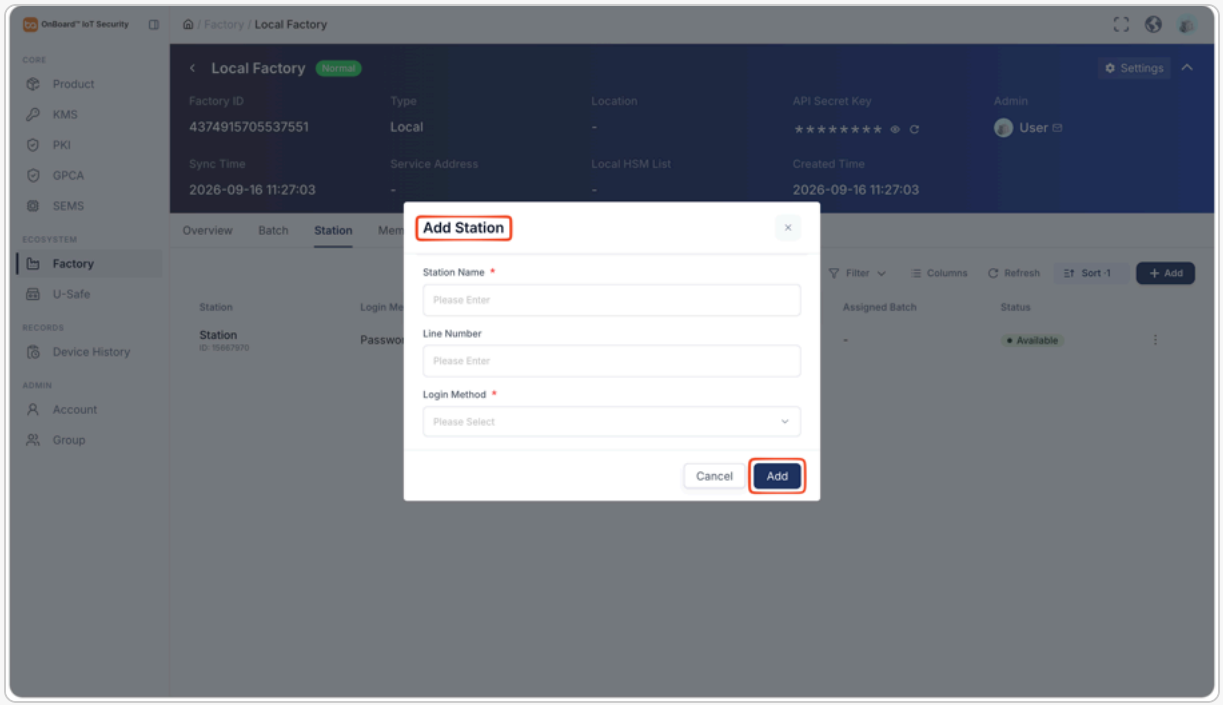
Create a programming station

> **TIP**
>
> After creating a programming station for the factory, you can assign specific programming stations to batches in OnBoard Edge Service as needed. Before programming a device, it is necessary to query and retrieve the corresponding batch information and programming data based on the programming station ID.
>
> Two programming methods are supported:
>
> - Using the Programming Station client
> - Using the OBIS Programming CLI

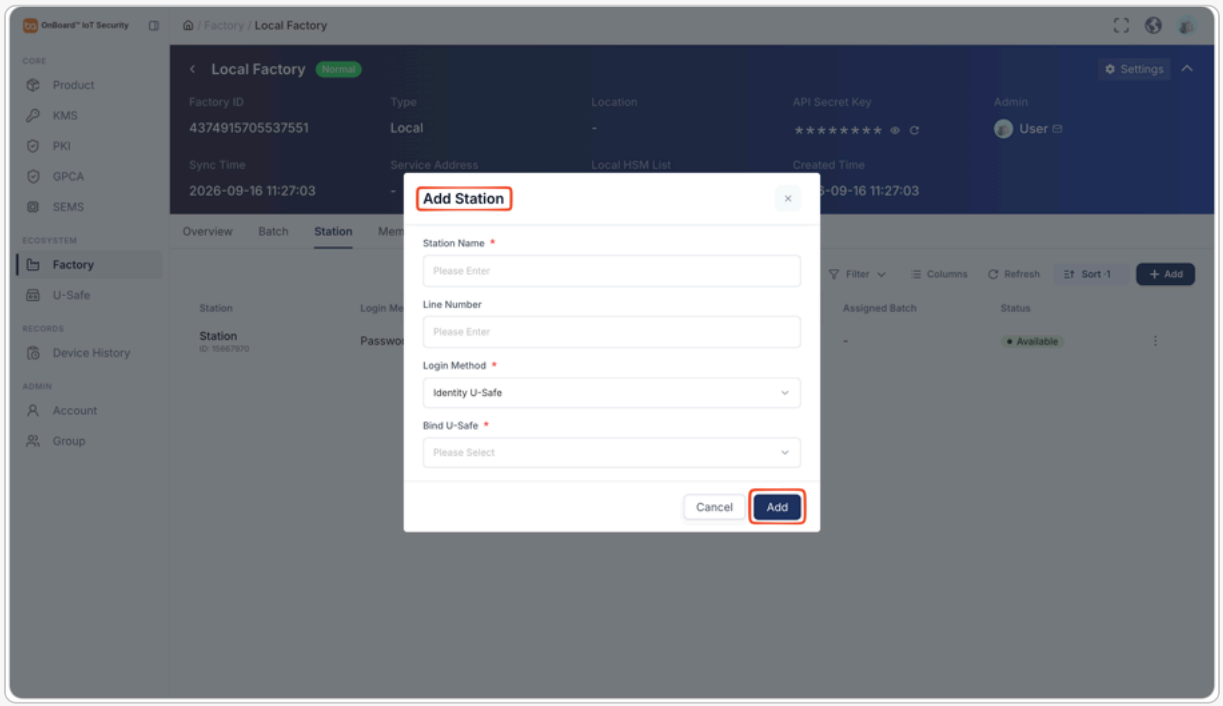
1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Station** tab and then click **Add**.



4. In the **Add Station** window, enter the **Station Name** and **Line Number**, and then select the **Login Method**. The methods include: **No Password**, **Password**, or **Identity U-Safe**.



> **TIP**
>
> If the login method is **Identity U-Safe**, you can select an already added Identity U-Safe from the **Bind U-Safe** drop-down list to bind it.



5. Click **Add** to create the programming station.

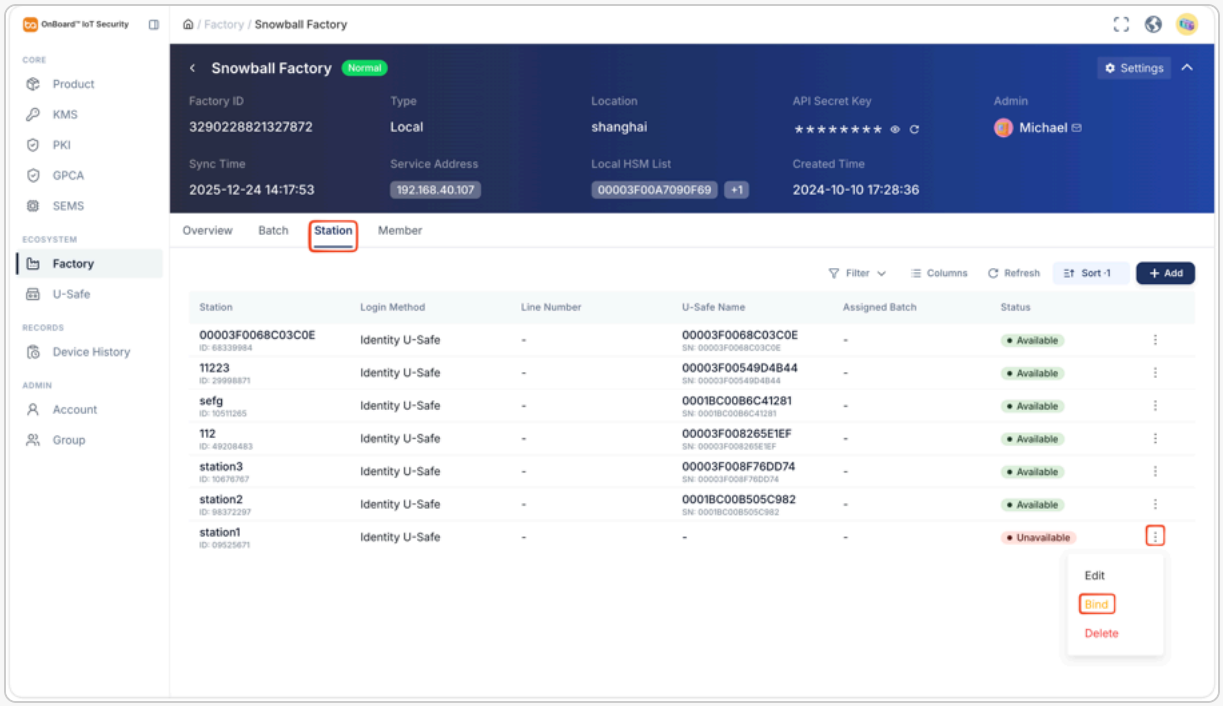
Bind an Identity U-Safe to a programming station

> **TIP**
>
> You can use the Identity U-Safe to sign in to the Programming Station client after binding.

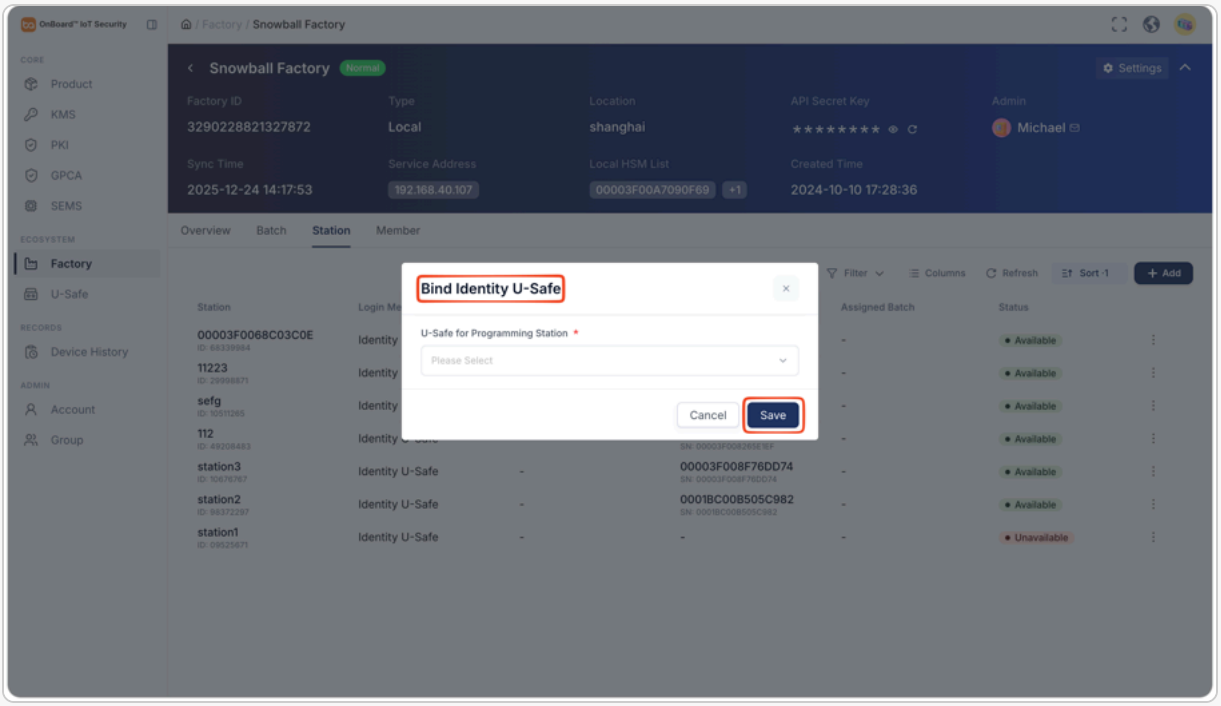
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Bind**.



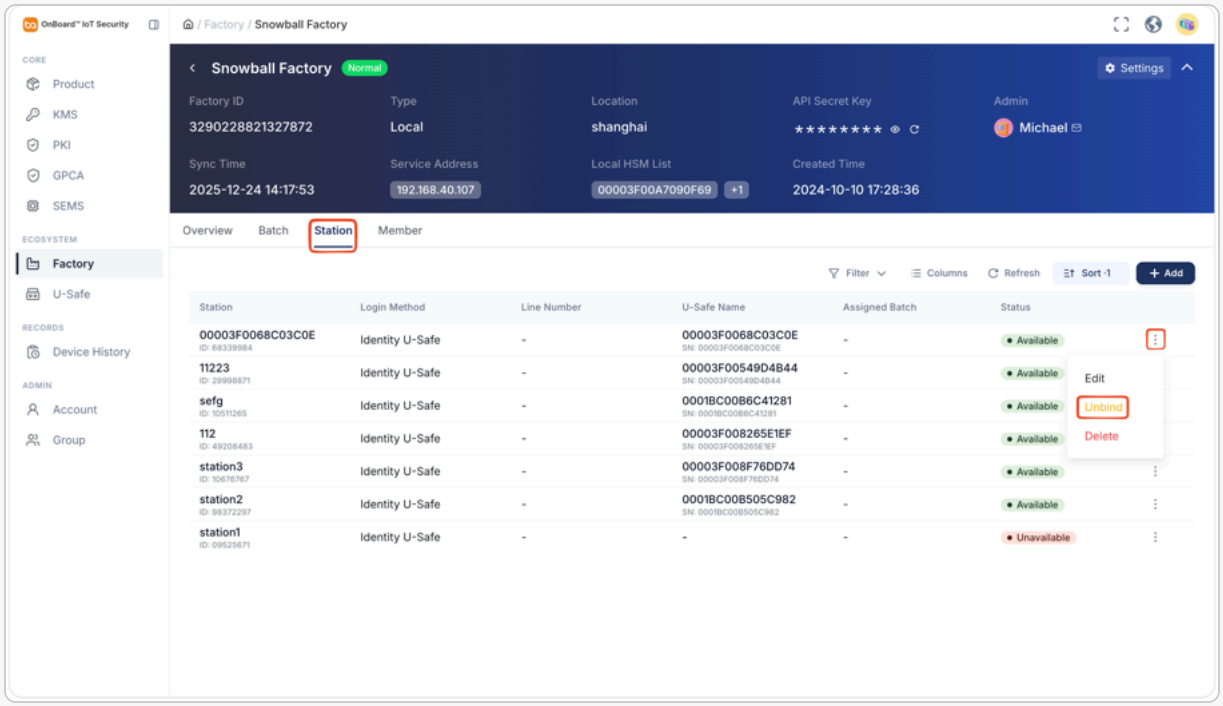
4. In the **Bind Identity U-Safe** window, select the Identity U-Safe you want to bind and then click **Save** to bind it to the programming station.



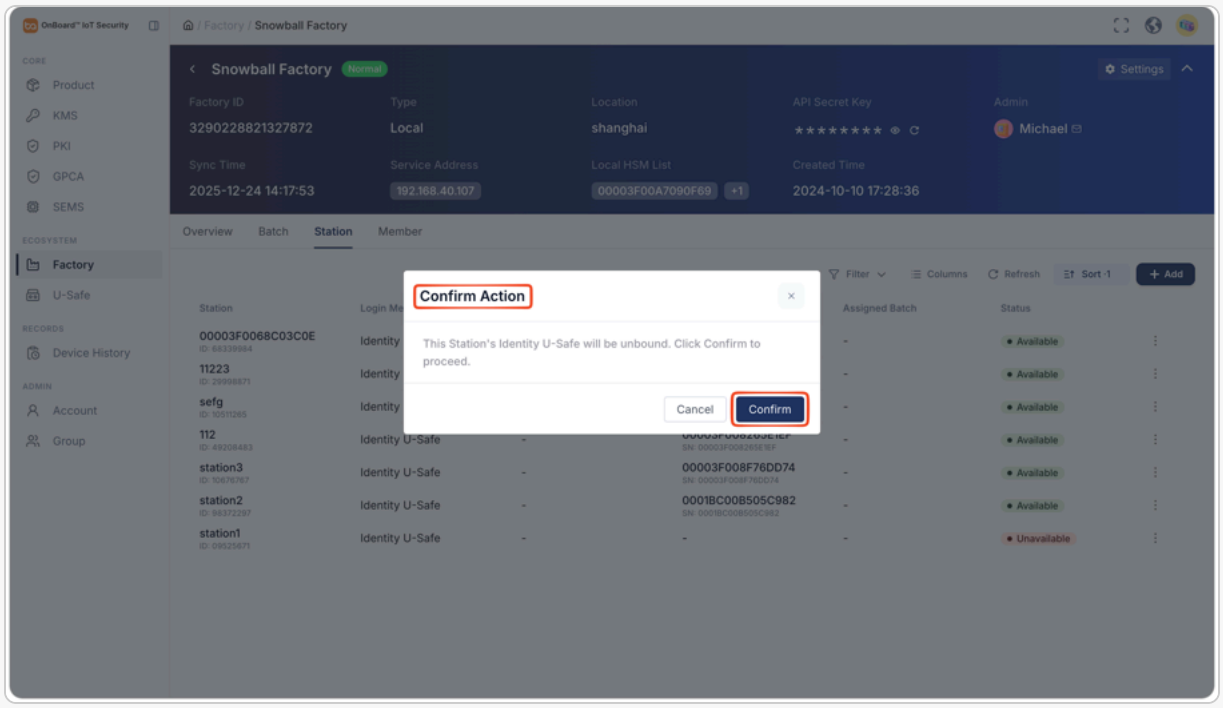
Unbind an Identity U-Safe from a programming station

> **WARNING**
>
> After unbinding, the Identity U-Safe can no longer be used to sign in to the Programming Station client.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Unbind**.



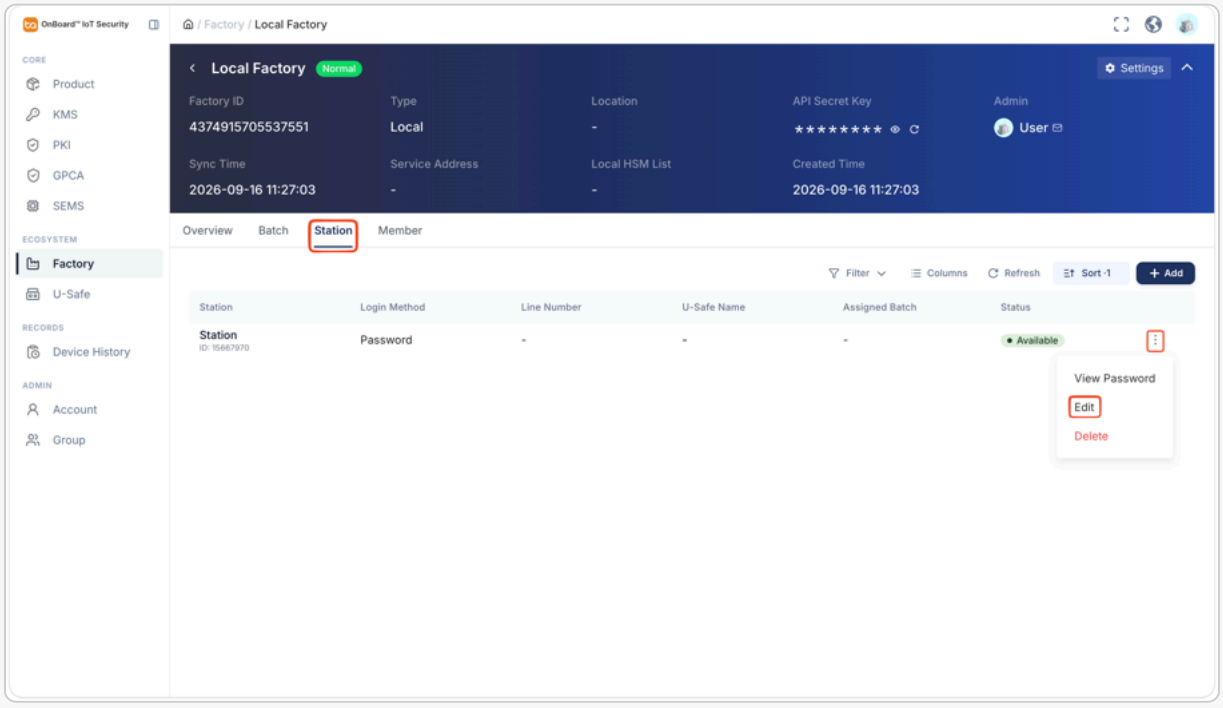
4. In the **Confirm Action** window, click **Confirm** to unbind the Identity U-Safe for the programming station.



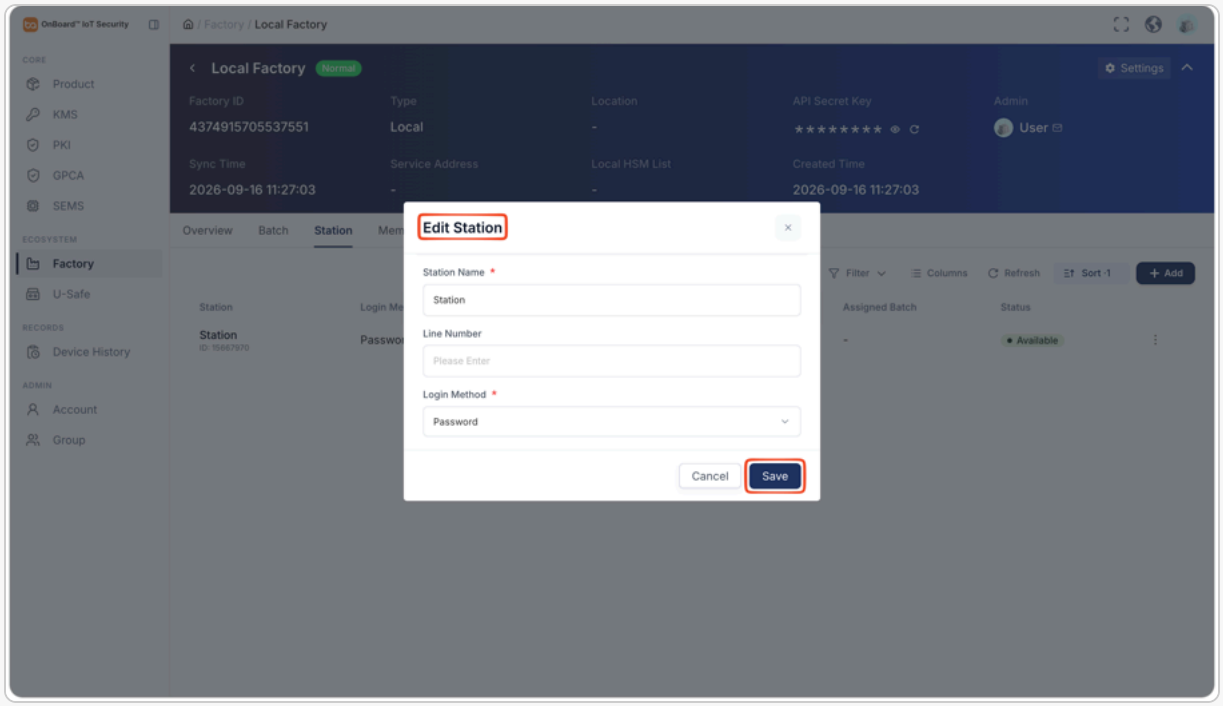
Edit a programming station

> **TIP**
>
> When the programming station status is **Busy**, the **Edit** option is grayed out and unavailable. After unbinding the programming station from the batch, the station status changes to **Available**, and the station can then be edited.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Station** tab and then click the Options ⋮ icon for the corresponding programming station and select **Edit**.



4. In the **Edit Station** window, enter the **Station Name** and **Line Number**, select the **Login Method**, and then click **Save** to edit the programming station.



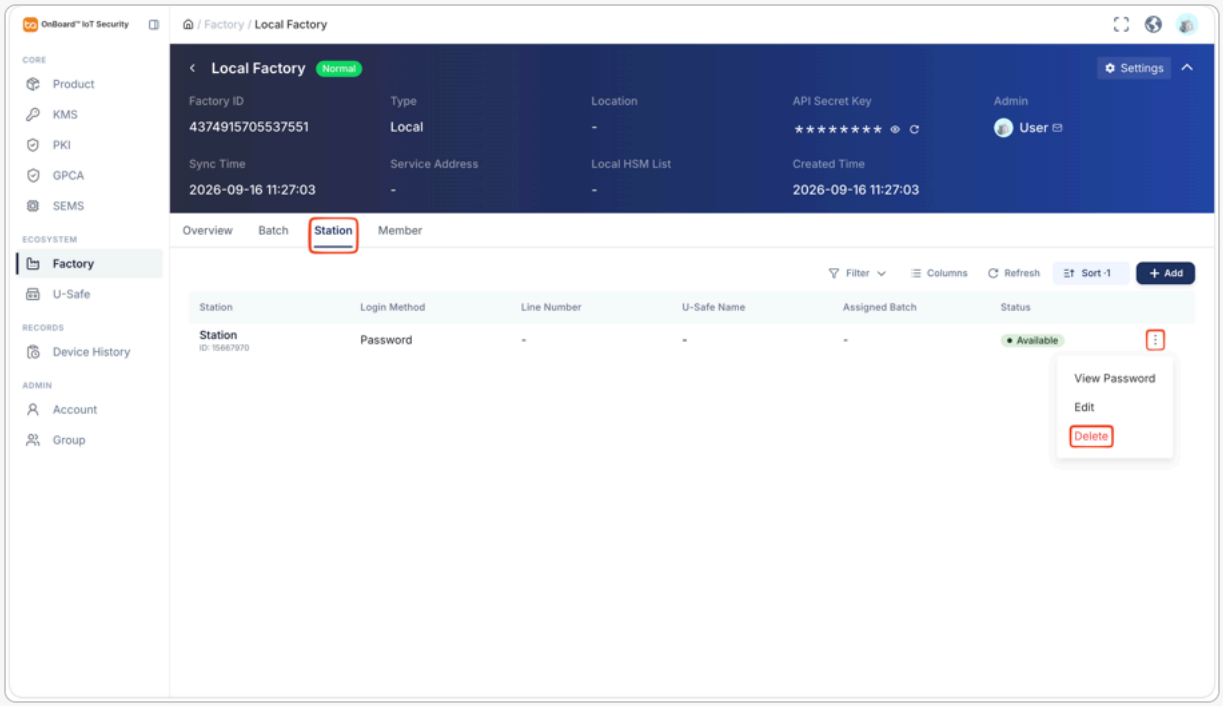
Delete a programming station

> **WARNING**
>
> Deleted programming stations cannot be recovered. Please proceed with caution.

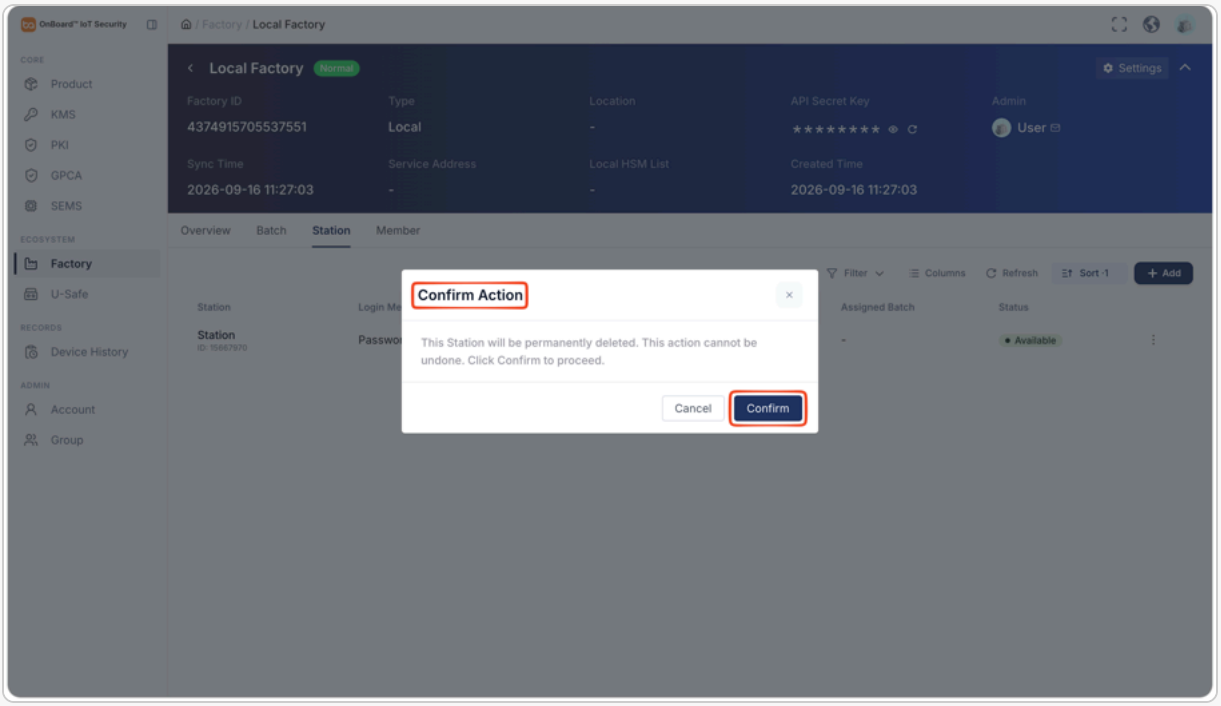
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Delete**.



4. In the **Confirm Action** window, click **Confirm** to delete the programming station.

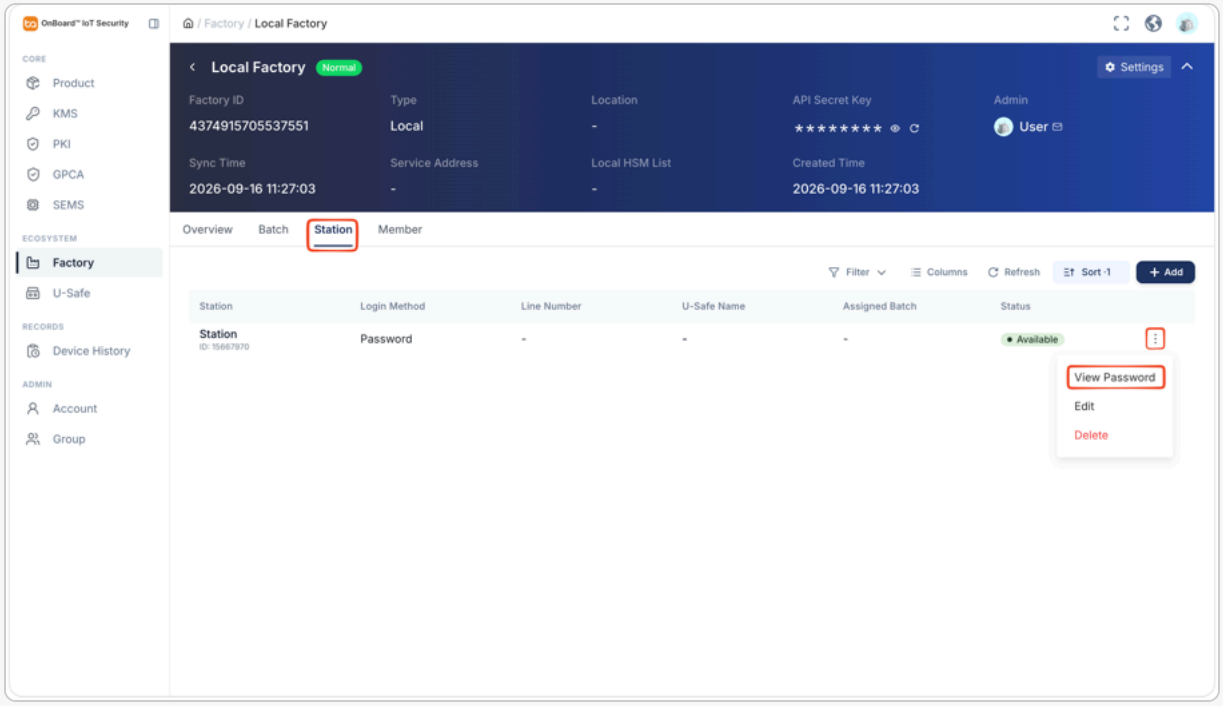


Check the programming station password

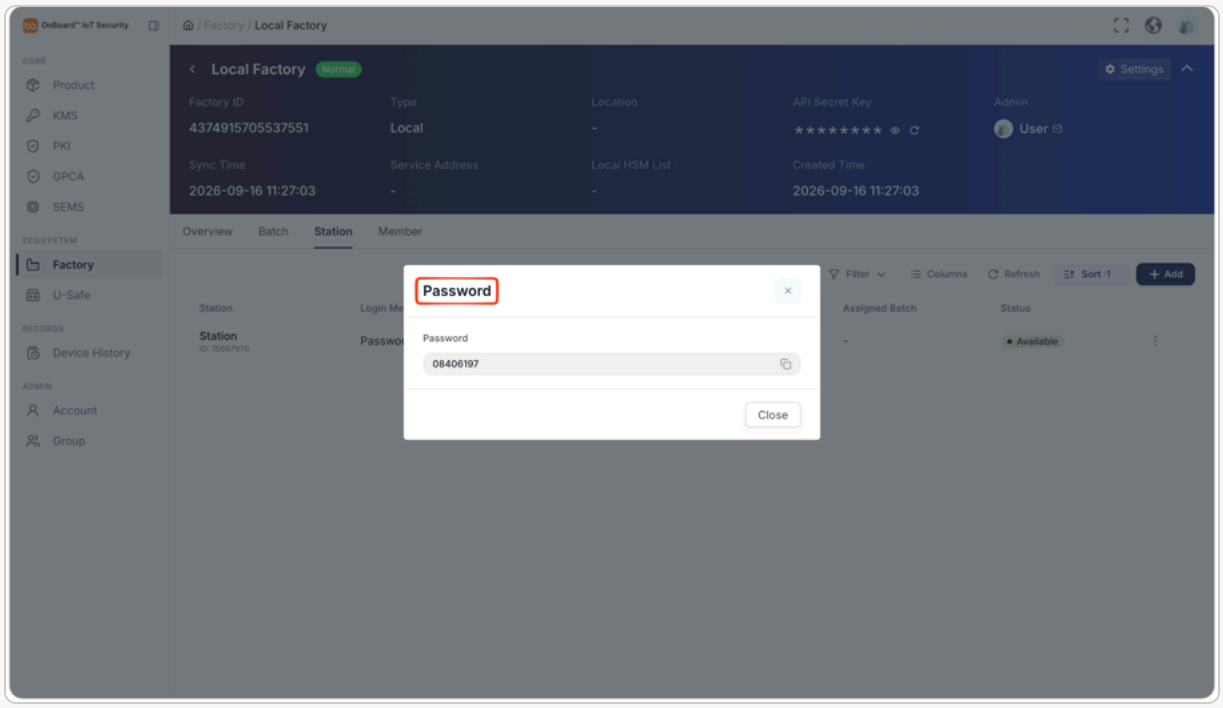
> **TIP**
>
> When the login method for the programming station is **Password**, the system will generate a random password, which can be used to sign in to the Programming Station client. Currently, the randomly generated password can't be changed.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **View Password**.



4. In the **Password** window, you can check and copy the sign-in password for the programming station.



Version: v3.4.0 (Latest)

How to configure and manage factories in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Add a Factory Manager
- Remove a Factory Manager
- Add an Identity U-Safe
- Unbind, lock, or unlock an Identity U-Safe
- Lock or unlock a factory

Prerequisites

Before getting started, please ensure that:

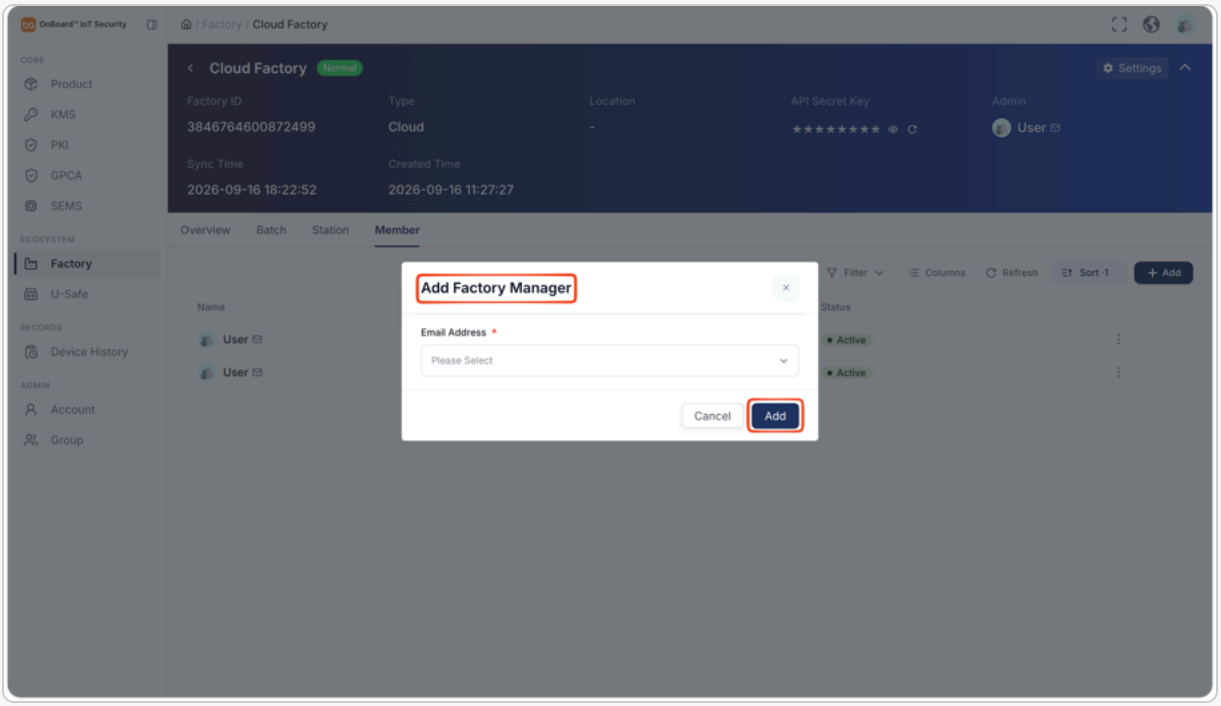
- You have factory role permissions as a Factory Admin or Factory Manager.
- You have obtained the Identity U-Safe required for identity authentication from Snowball.

Add a Factory Manager

> **TIP**
>
> Factory managers can manage and operate factory-related businesses. After a Factory Manager is added, the system automatically generates an initial password and sends it to the corresponding email address. Currently, this randomly generated password can be reset, but custom modification is not yet supported.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. Select the **Member** tab, and then click **Add**. In the **Add Factory Manager** window, select and enter the email address of the new Factory Manager.

   > **TIP**
   >
   > The Factory Manager being added must be an **Active** user within the same tenant.



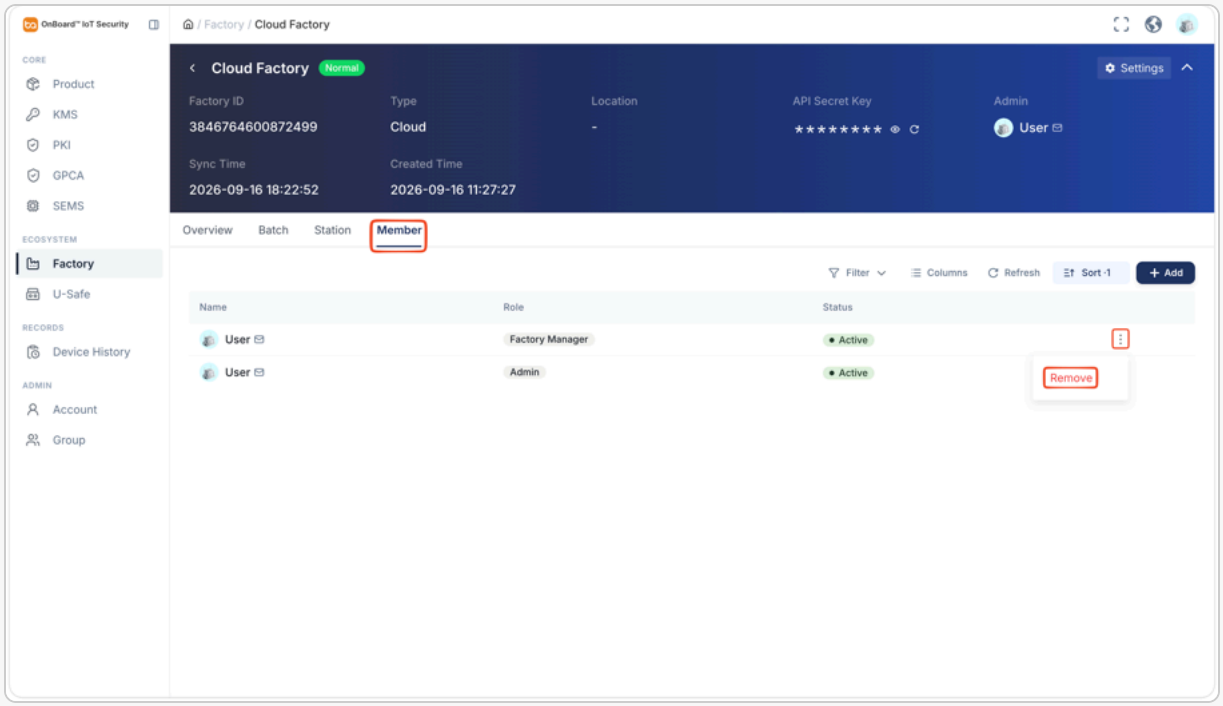
4. Click **Add** to complete adding a Factory Manager.

Remove a Factory Manager

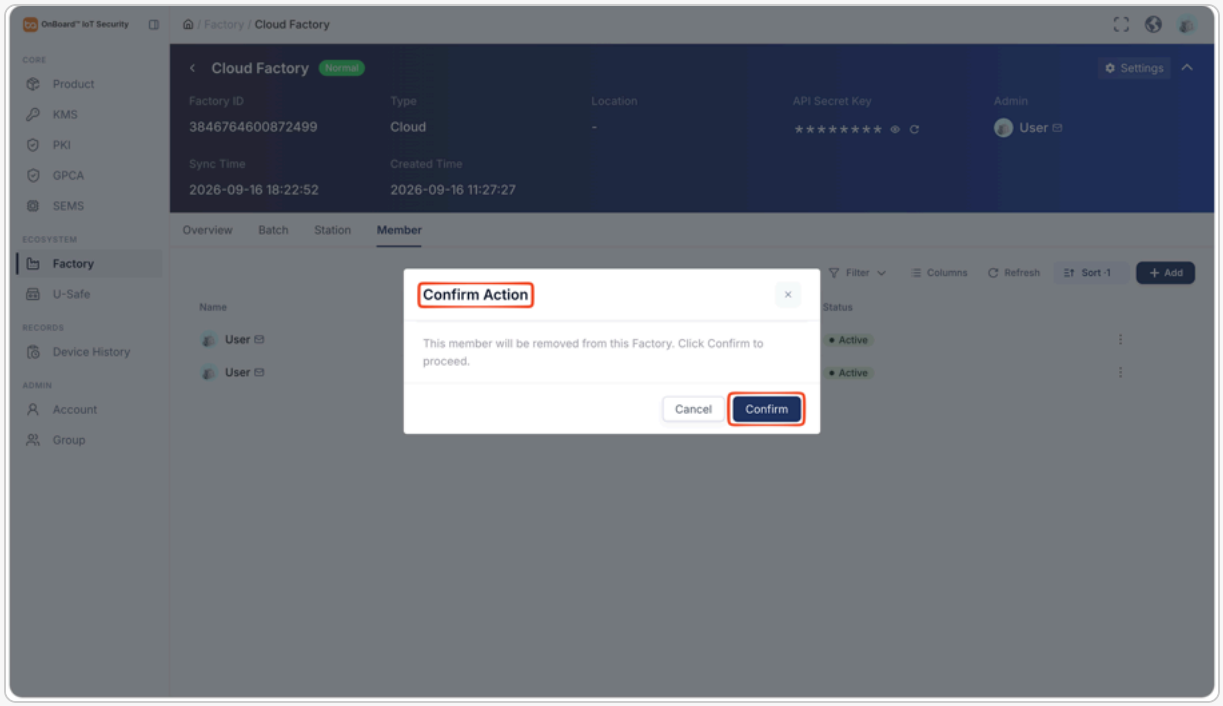
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. Select the **Member** tab, click the Options ⋮ icon for the corresponding Factory Manager and select **Remove**.



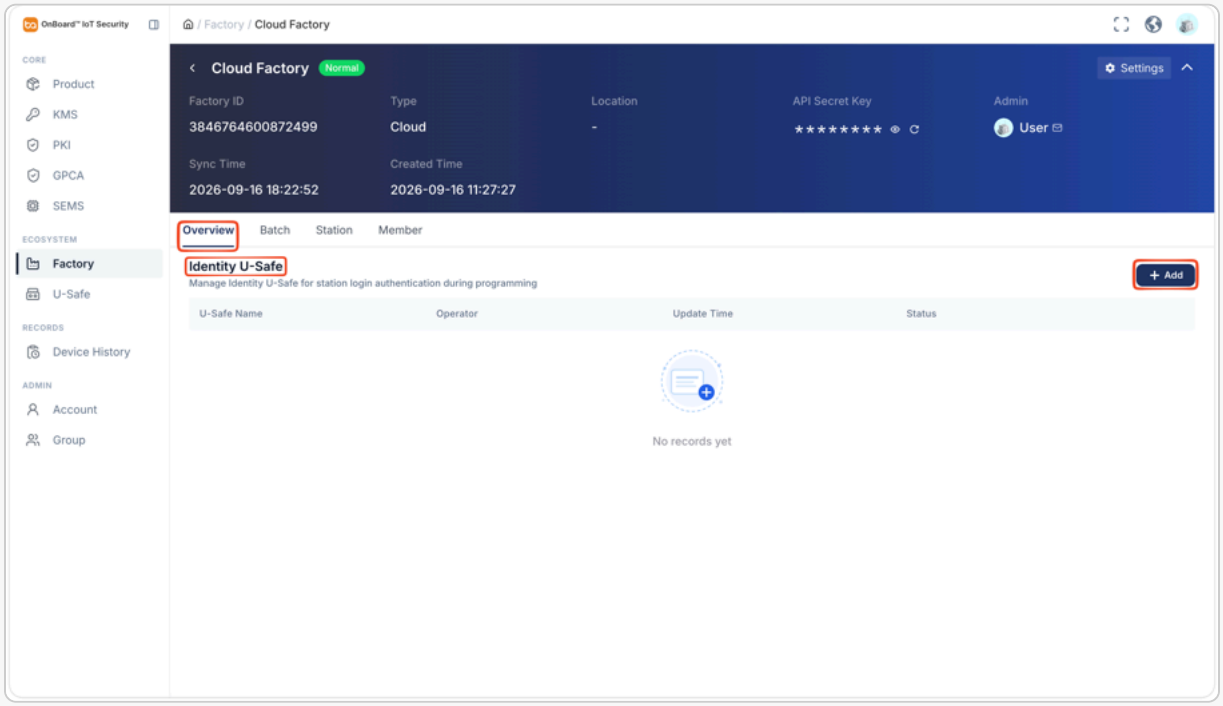
4. In the **Confirm Action** window, click **Confirm** to remove the Factory Manager.



Add an Identity U-Safe

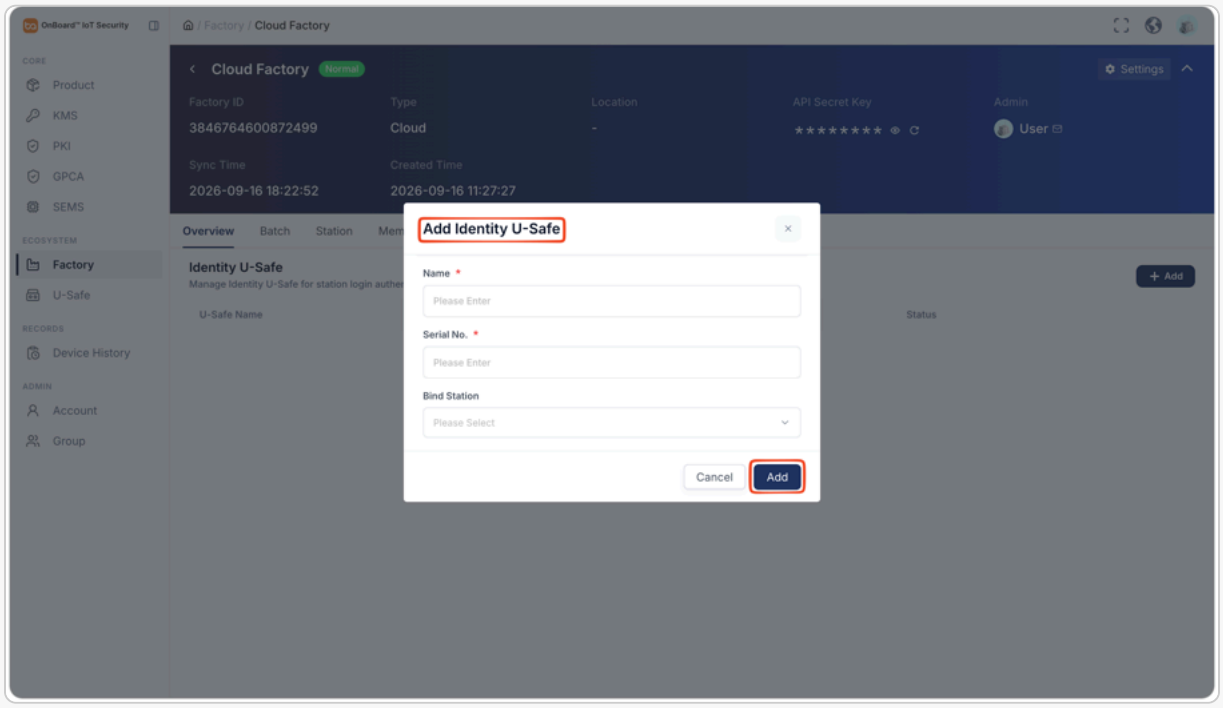
> **TIP**
>
> The purpose of adding an Identity U-Safe is to bind it to the corresponding factory. After binding it to a programming station, it can be used to sign in to the Programming Station client. Meanwhile, login authentication for the programming station is achieved through the Identity U-Safe management.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, locate the **Identity U-Safe** section and then click **Add**.



4. In the **Add Identity U-Safe** window, enter the **Name** (customizable) and **Serial No.** (which can be found on the device) of the Identity U-Safe you want to bind.

> **TIP**
>
> - If a programming station has already been added, you can select and bind the corresponding programming station.
> - If a programming station hasn't been added yet, you can bind it when adding a programming station.

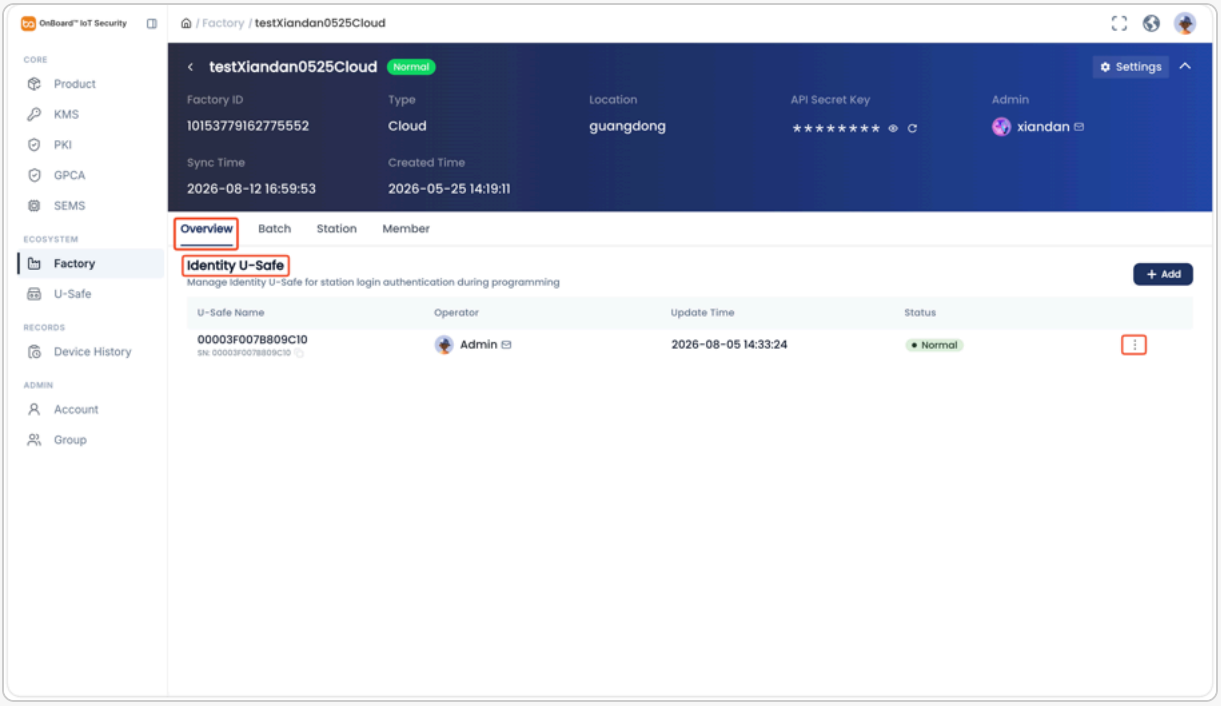


5. Click **Add** to bind the Identity U-Safe.

Unbind, lock, or unlock an Identity U-Safe

> **TIP**
>
> Lock the Identity U-Safe to prevent its use and unbinding. Once locked, its status will change to **Locked**.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, locate the **Identity U-Safe** section, and then click the Options ⋮ icon for the corresponding Identity U-Safe and select **Unbind**, **Lock**, or **Unlock**.



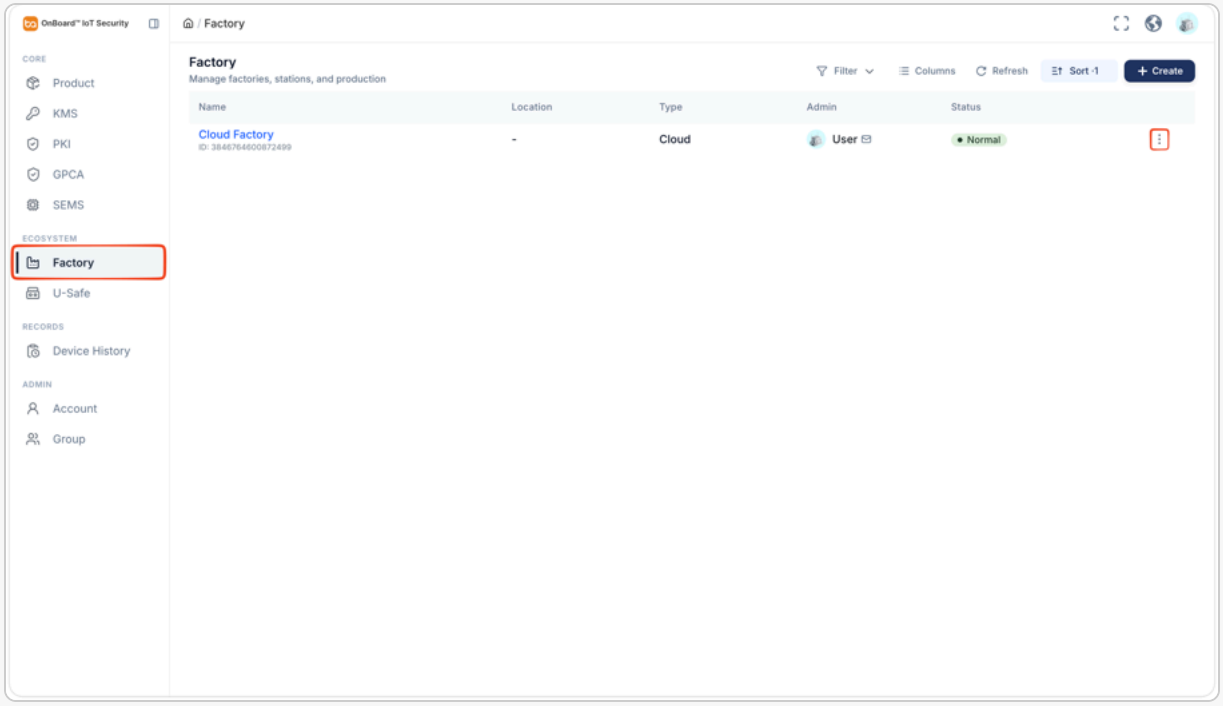
4. In the pop-up window, click **Confirm** to unbind, lock, or unlock the Identity U-Safe.

Lock or unlock a factory

> **TIP**
>
> Lock the factory to prevent its use. Once locked, its status will change to **Locked**.

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then click the Options ⋮ icon for the corresponding factory and select **Lock** or **Unlock**.



3. In the pop-up window, click **Confirm** to lock or unlock the factory.

Version: v3.4.0 (Latest)

How to configure and manage programming stations in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Create a programming station
- Bind an Identity U-Safe to a programming station
- Unbind an Identity U-Safe from a programming station
- Edit a programming station
- Delete a programming station
- Check the programming station password

Prerequisites

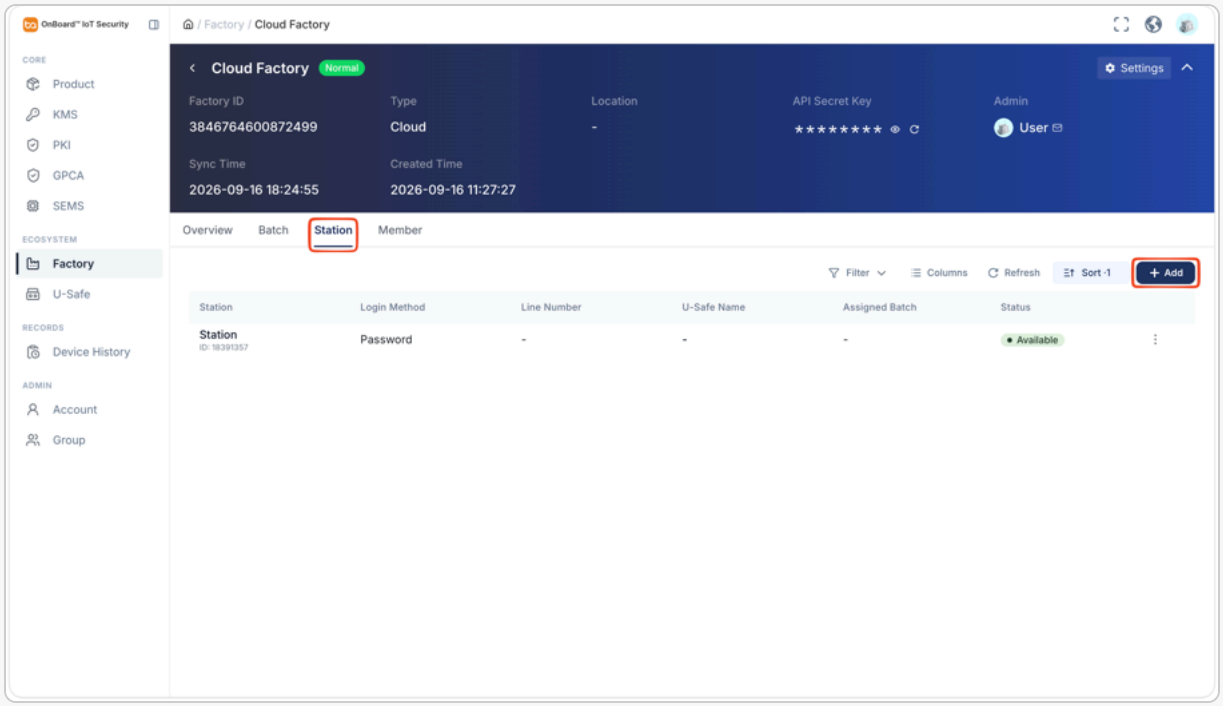
Before getting started, please ensure that:

- The factory has already been configured.
- You have factory role permissions as a Factory Admin or Factory Manager.
- You have obtained the Identity U-Safe for identity authentication from Snowball.

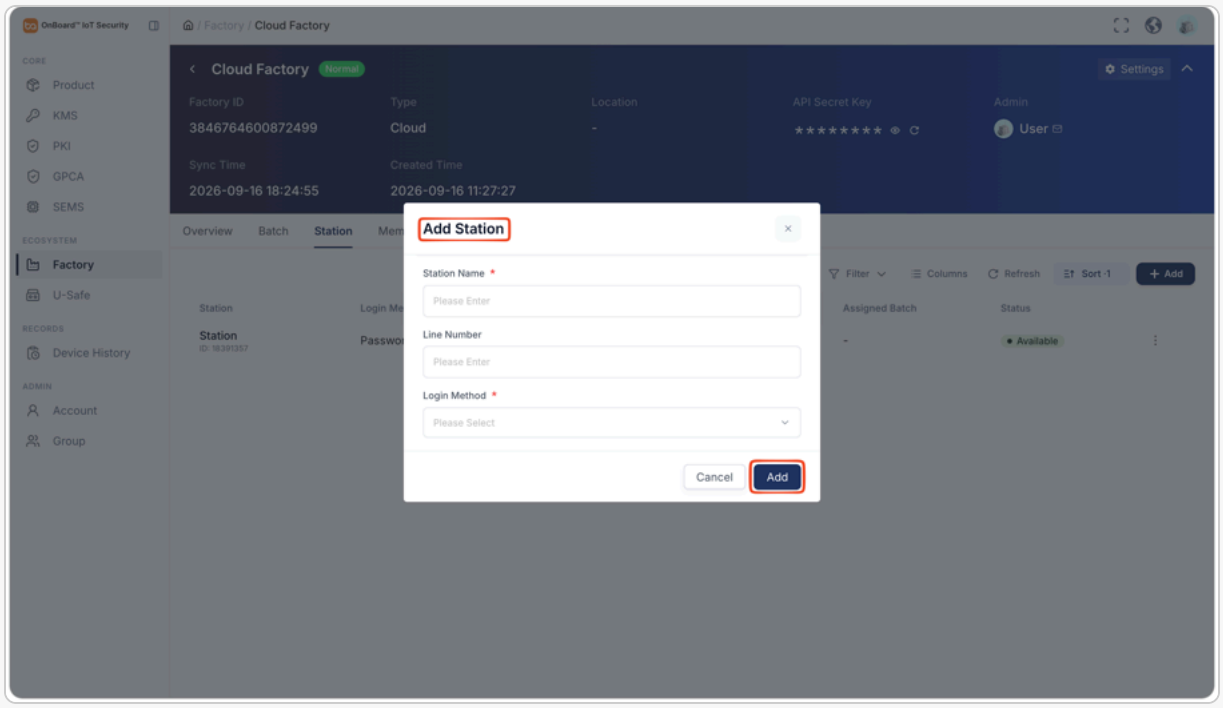
Create a programming station

> **TIP**
>
> After creating a programming station for the factory, you can assign specific programming stations to batches as needed. Before programming a device, it is necessary to query and retrieve the corresponding batch information and programming data based on the programming station ID.
>
> Two programming methods are supported:
>
> - Using the Programming Station client
> - Using the OBIS Programming CLI

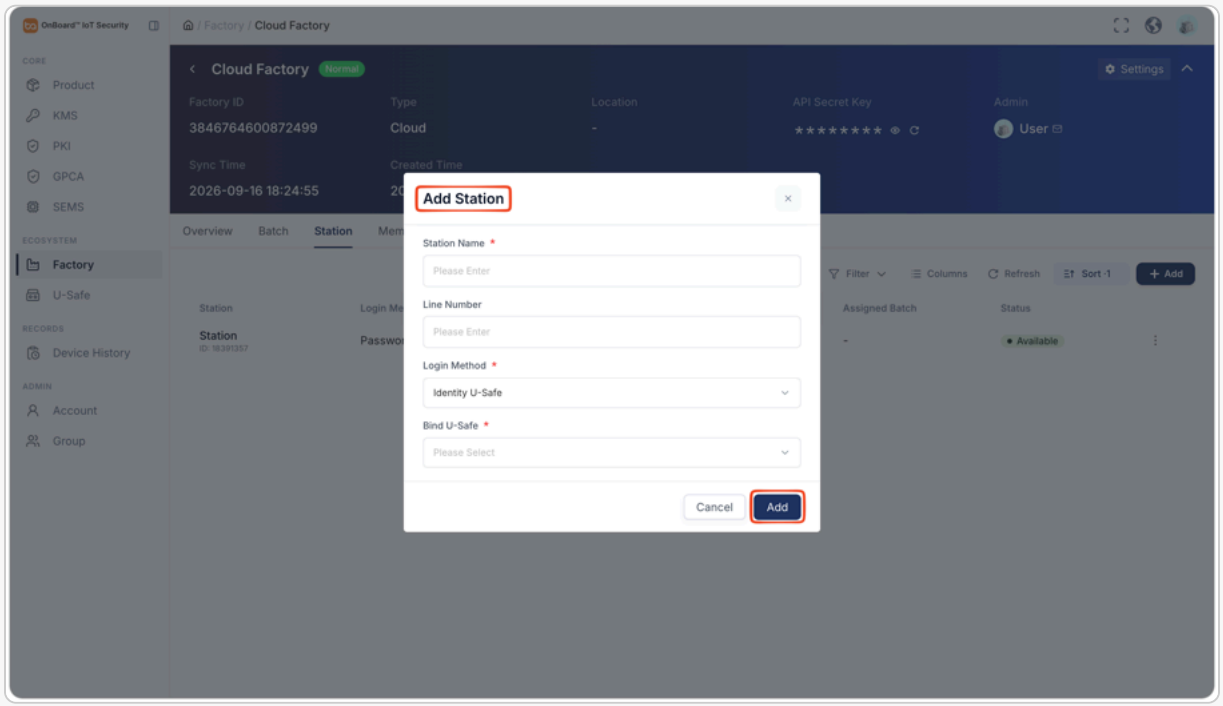
1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Station** tab, and then click **Add**.



4. In the **Add Station** window, enter the **Station Name** and **Line Number**, and then select the **Login Method**. The methods include: **Password** or **Identity U-Safe**.



> **TIP**
>
> If the login method is **Identity U-Safe**, you can select an already added Identity U-Safe from the **Bind U-Safe** drop-down list to bind it.



5. Click **Add** to create the programming station.

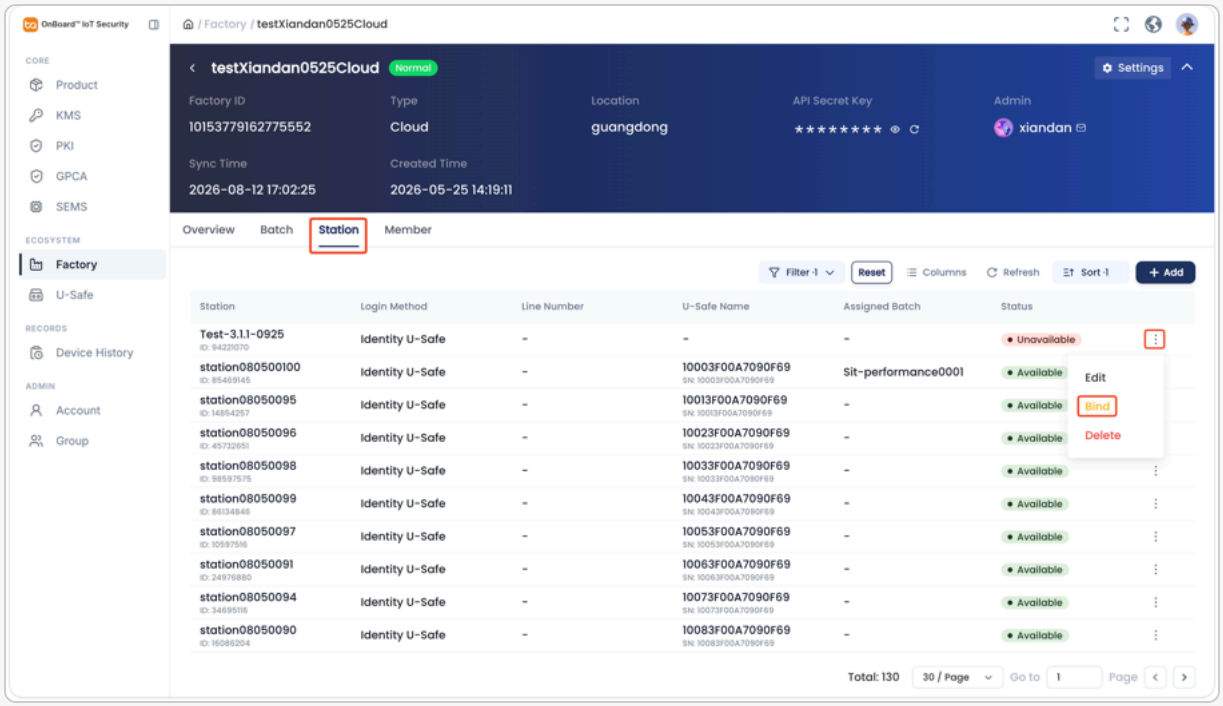
Bind an Identity U-Safe to a programming station

> **TIP**
>
> You can use the Identity U-Safe to sign in to the Programming Station client after binding.

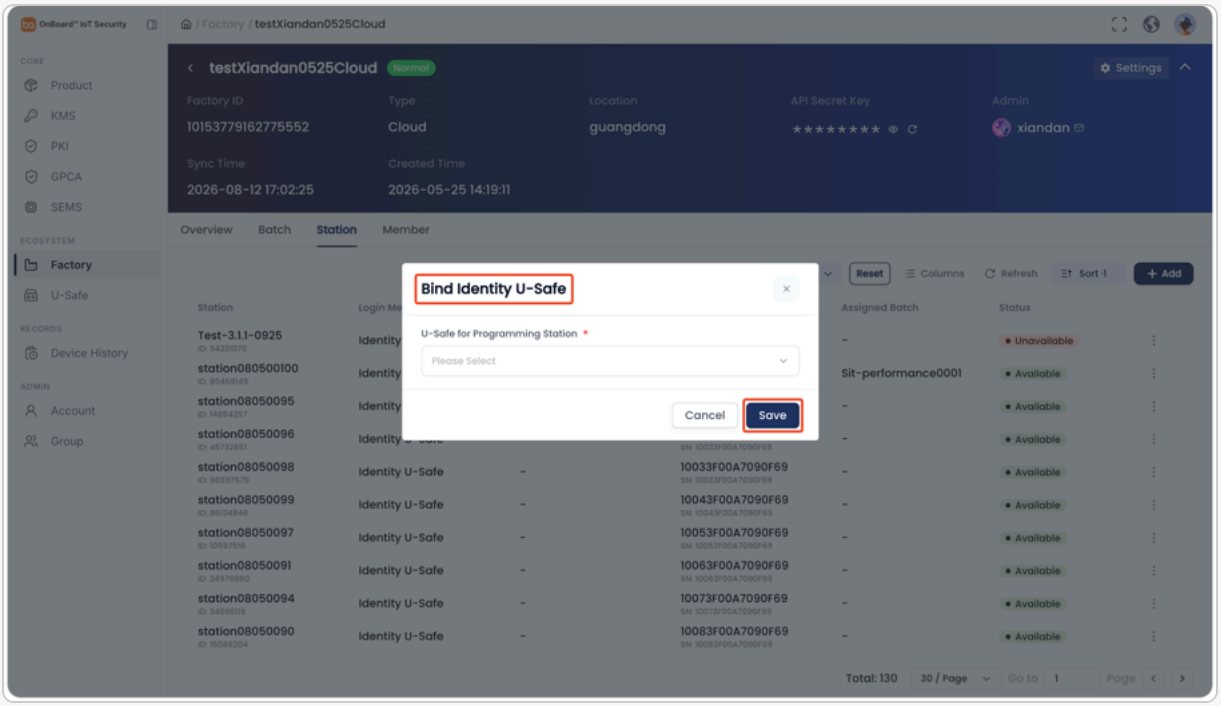
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Bind**.



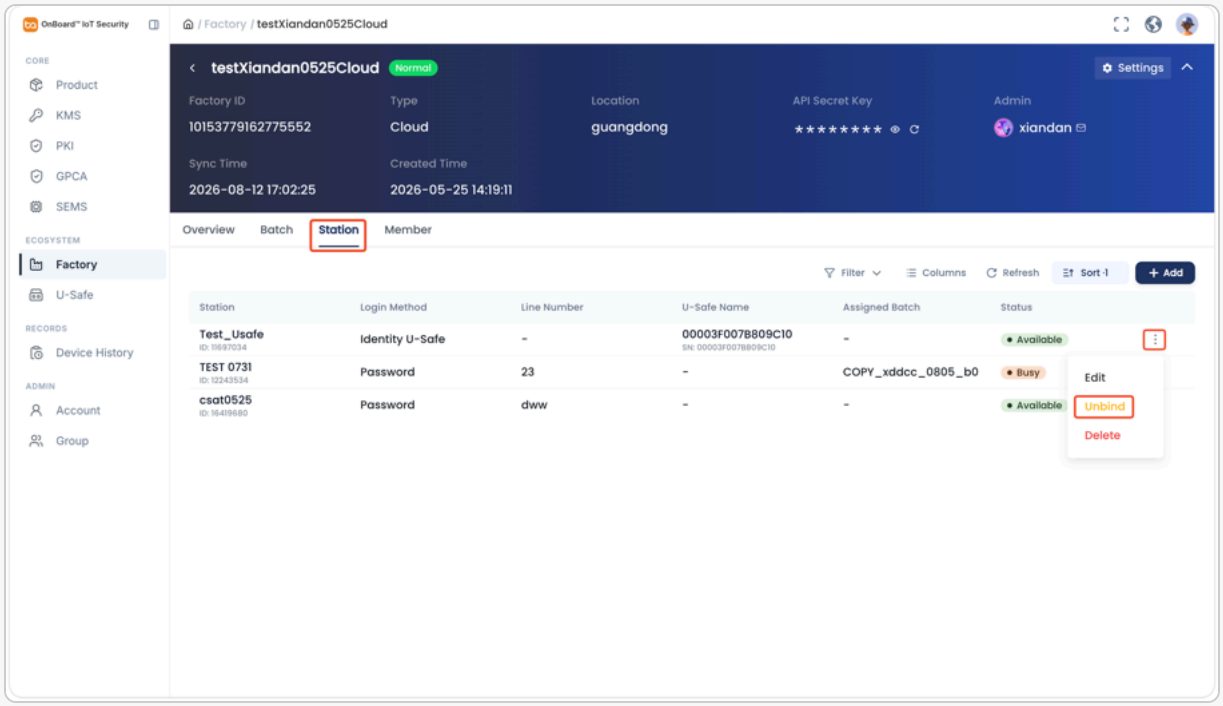
4. In the **Bind Identity U-Safe** window, select the Identity U-Safe you want to bind and then click **Add** to bind it to the programming station.



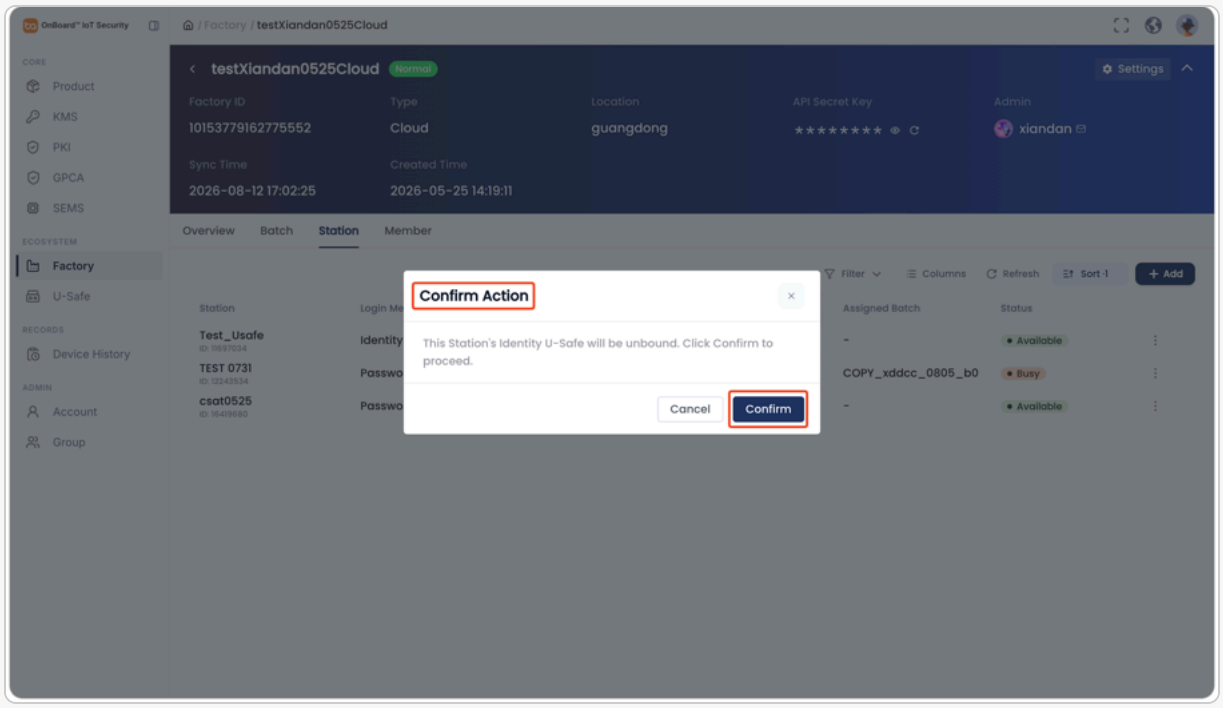
Unbind an Identity U-Safe from a programming station

> **WARNING**
>
> After unbinding, the Identity U-Safe can no longer be used to sign in to the Programming Station client.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Unbind**.



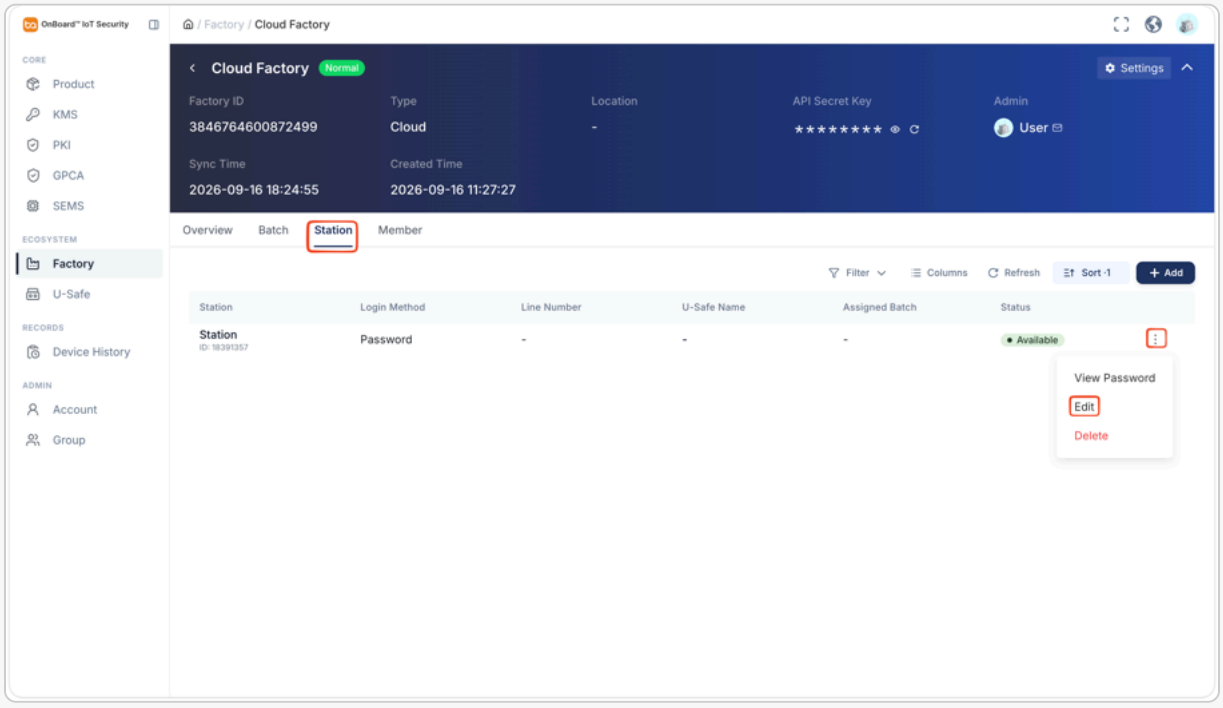
4. In the **Confirm Action** window, click **Confirm** to unbind the Identity U-Safe for the programming station.



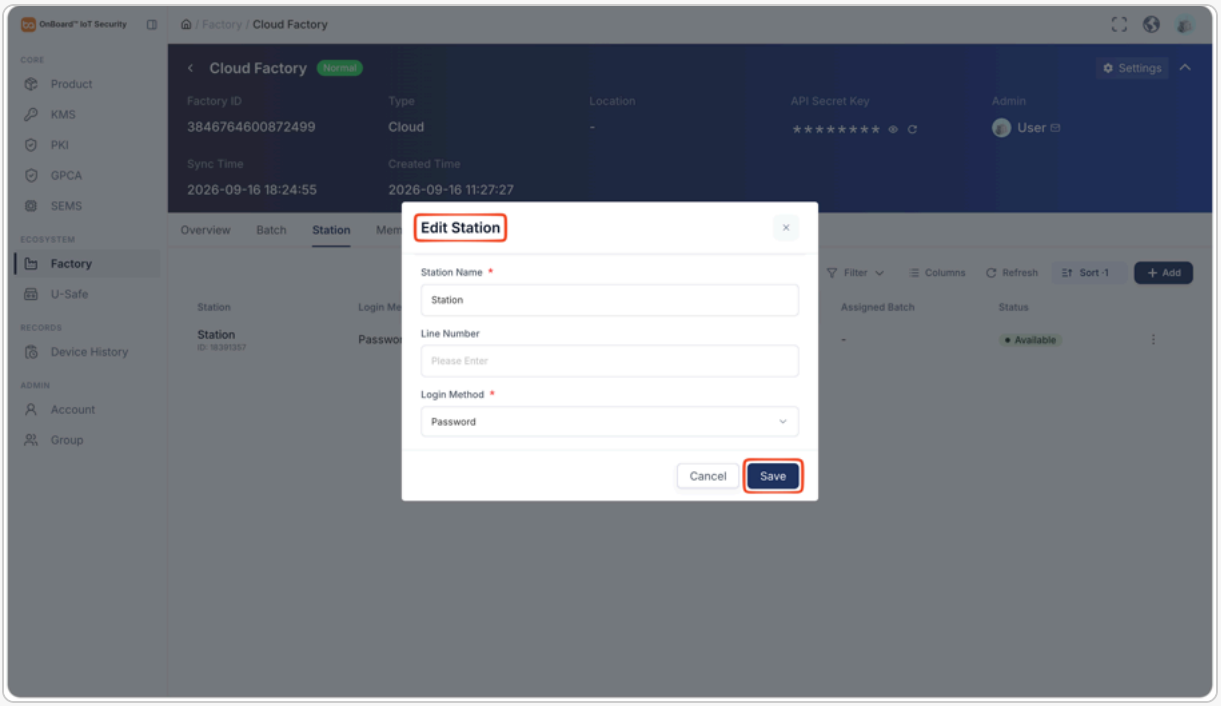
Edit a programming station

> **TIP**
>
> When the programming station status is **Busy**, the **Edit** option is grayed out and unavailable. After unassigning the programming station from the batch, the station status changes to **Available**, and the station can then be edited.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Edit**.



4. In the **Edit Station** window, enter the **Station Name** and **Line Number**, select the **Login Method**, and then click **Save** to edit the programming station.



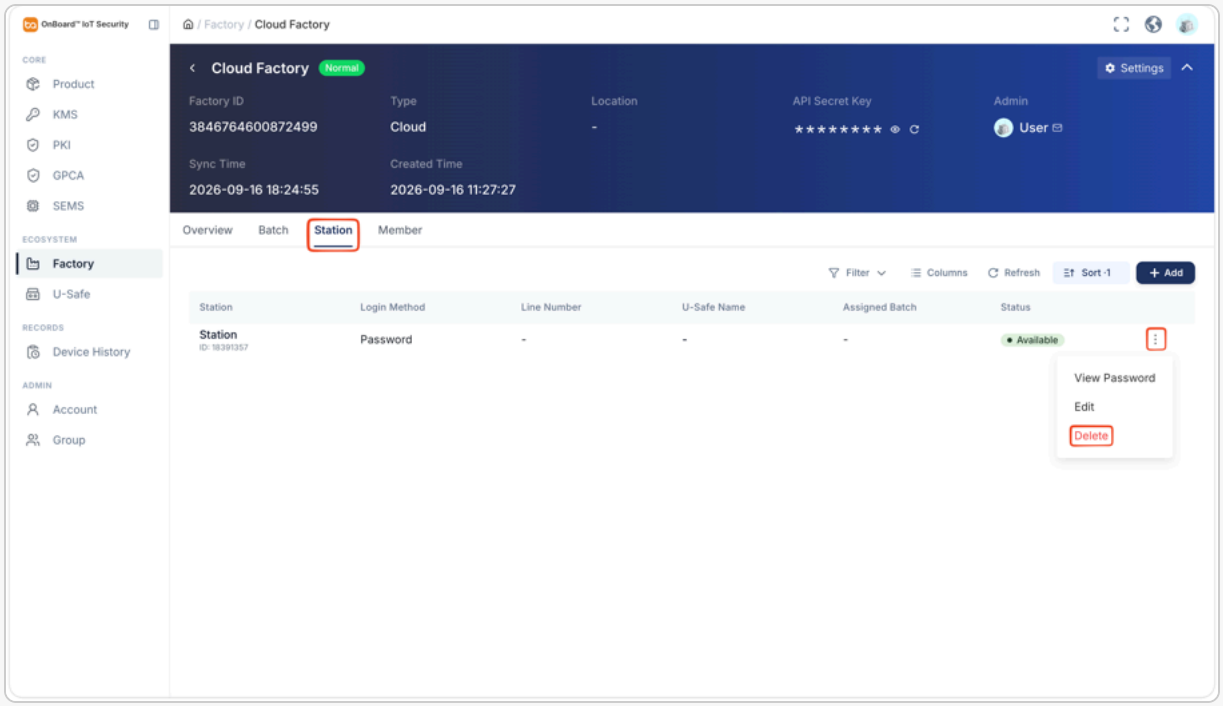
Delete a programming station

> **WARNING**
>
> Deleted programming stations cannot be recovered. Please proceed with caution.

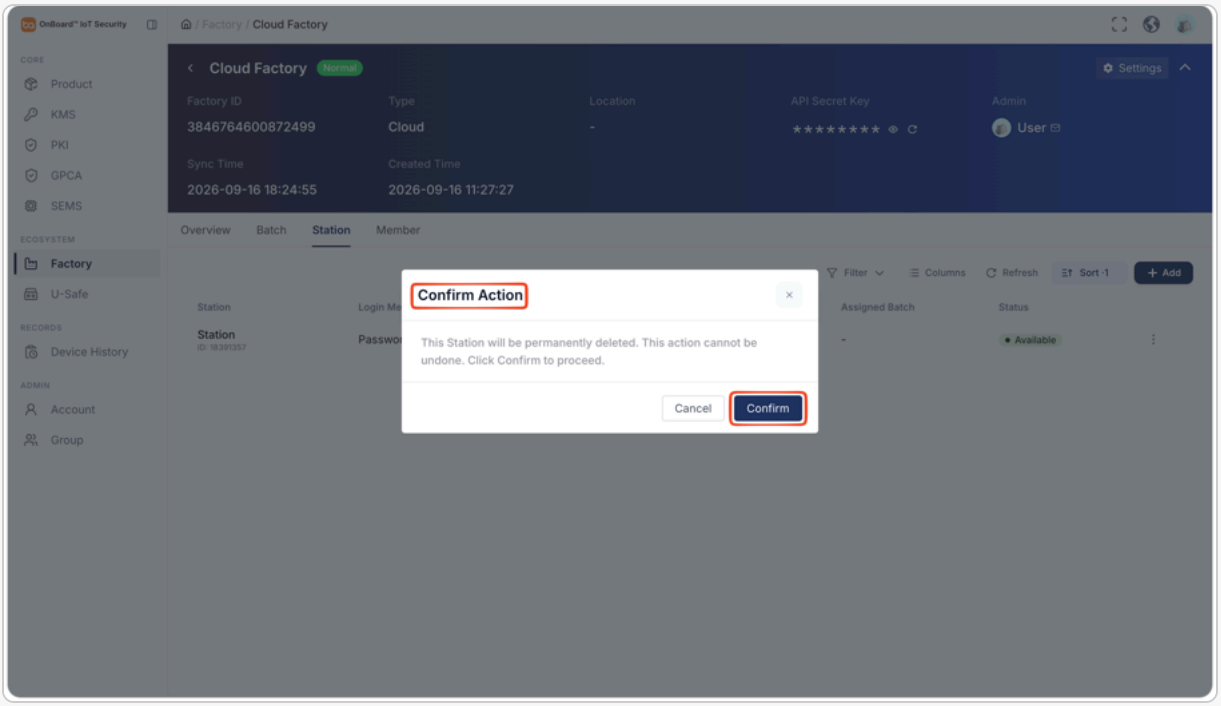
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **Delete**.



4. In the **Confirm Action** window, click **Confirm** to delete the programming station.

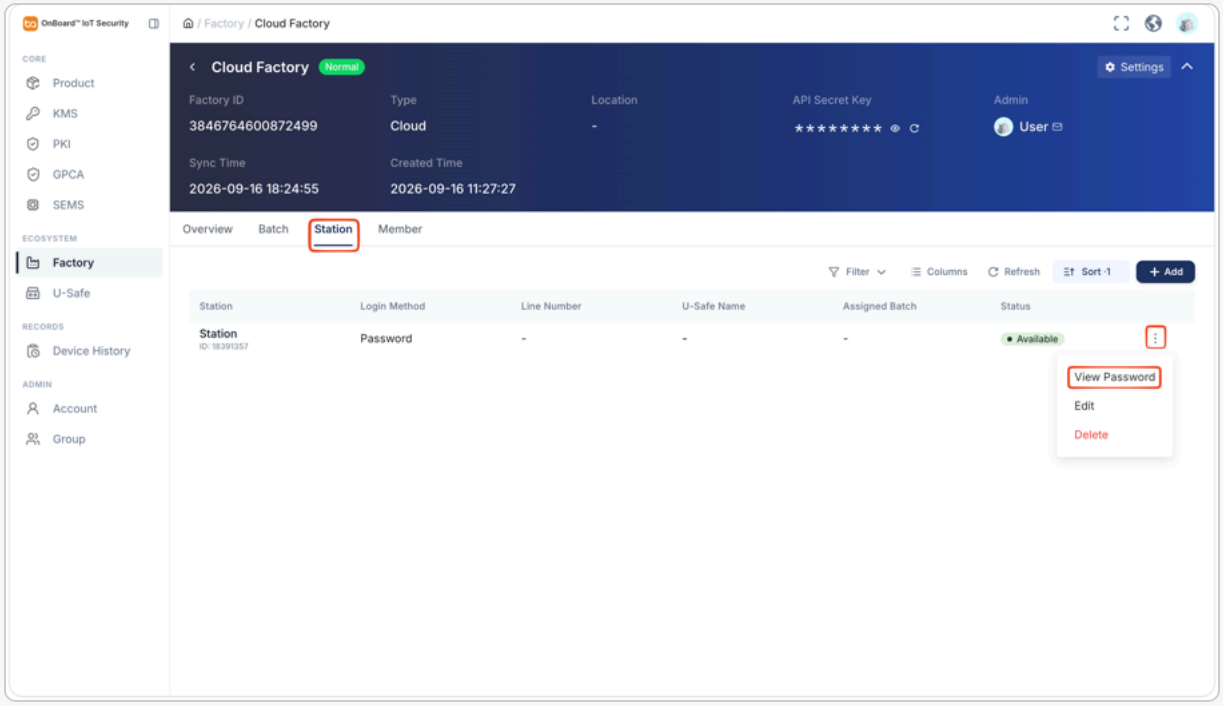


Check the programming station password

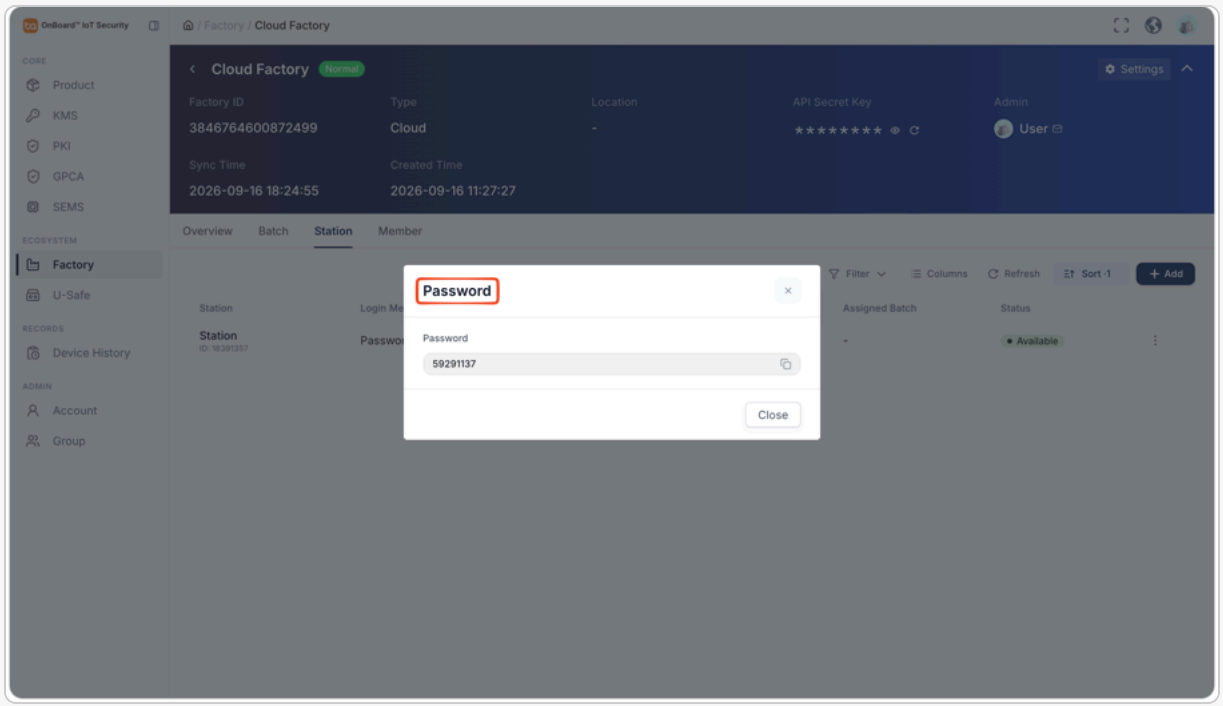
> **TIP**
>
> When the login method for the programming station is **Password**, the system will generate a random password, which can be used to sign in to the Programming Station client. Currently, the randomly generated password can't be changed.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then click the Options ⋮ icon for the corresponding programming station and select **View Password**.



4. In the **Password** window, you can check and copy the sign-in password for the programming station.



Version: v3.4.0 (Latest)

How to manage a batch and assign a programming station in OnBoard Edge Service

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS):

- Check batch status
- Assign a programming station to a batch
- Unassign a programming station from a batch
- Turn off, turn on or delete a batch

Prerequisites

Before getting started, please ensure that:

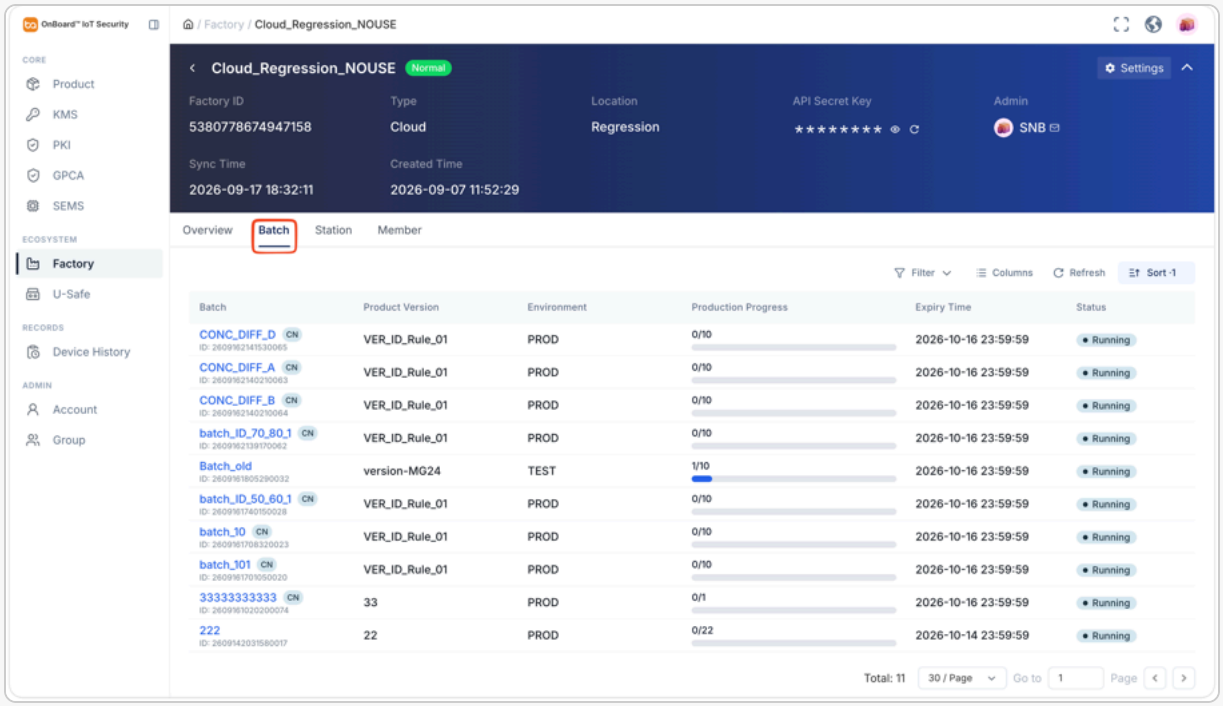
- The factory has already been configured.
- You have factory role permissions as a Factory Admin or Factory Manager.

Check batch status

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Batch** tab, and then you can check the batch status on the **Batch** tab.



Description of batch status:

Status	Can be turned on	Description
Running	-	The default state after creating a batch. You can bind it to a programming station.

Status	Can be turned on	Description
Stopped	Yes	The batch is currently turned off. You can turn it on to bind it to a programming station.
Finished	No	The status after batch programming is completed.
Expired	No	The batch has expired before the programming was completed. **Note**: After a batch expires, most functions related to that batch will no longer operate normally, including programming in the Programming Station client. It is recommended to delete the expired batches.

Assign a programming station to a batch

> **TIP**
>
> A batch can be assigned to multiple programming stations, while a programming station can only program one batch at the same time.

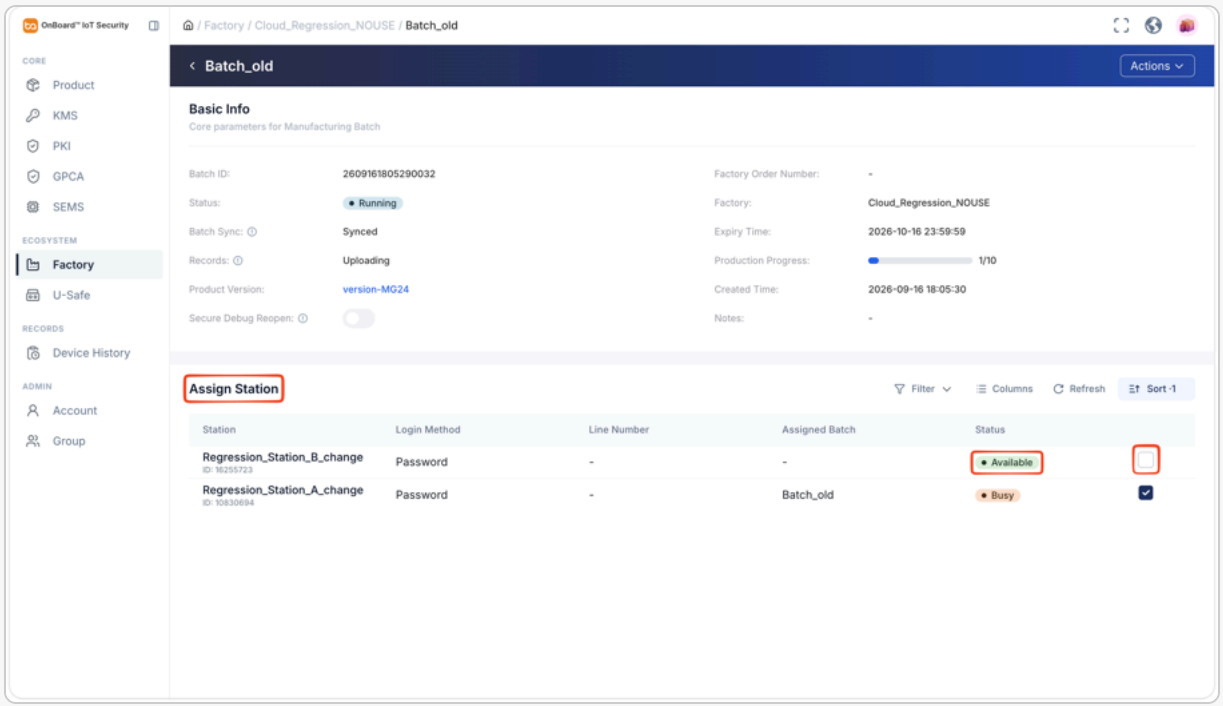
Assign a programming station with the **Available** status to a batch for programming:

1. Sign in to OBIS.

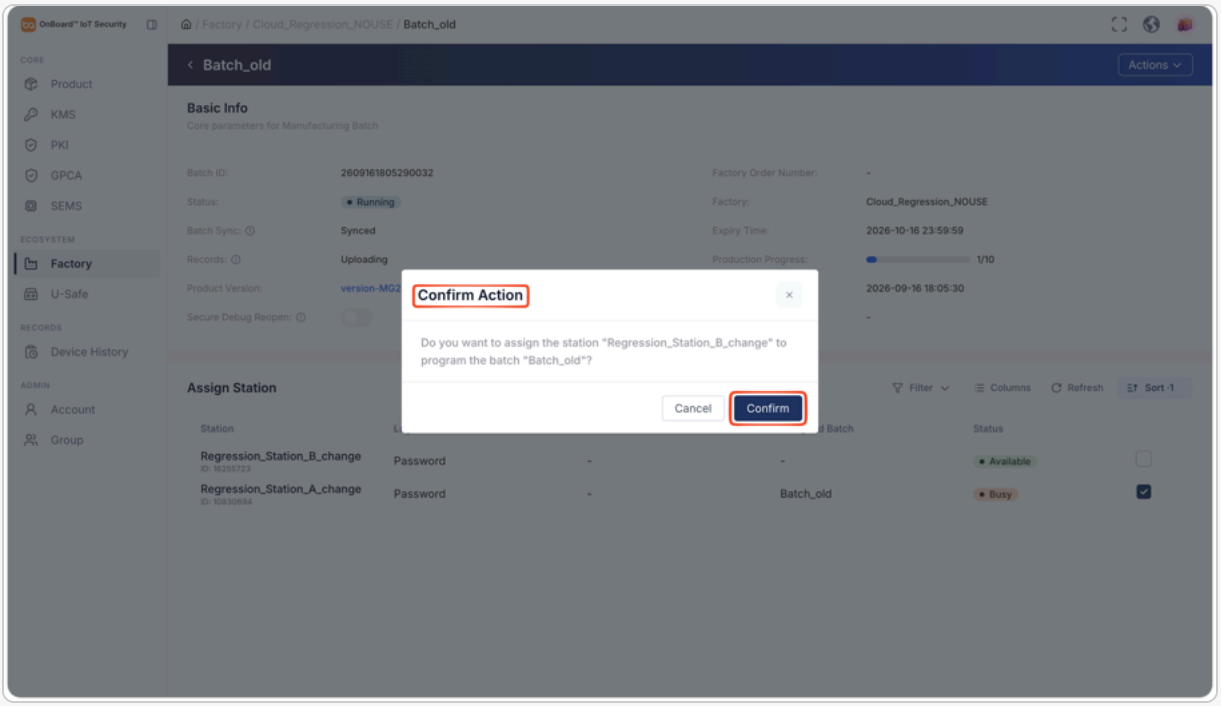
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Batch** tab and click the batch to navigate to the batch page.

4. In the **Assign Station** section of the batch page, confirm that the batch status is **Running**, and then select the programming station with the **Available** status for assignment.



5. In the **Confirm Action** window, click **Confirm** to complete the assignment of the programming station. After the assignment, the programming station status will change to **Busy**.

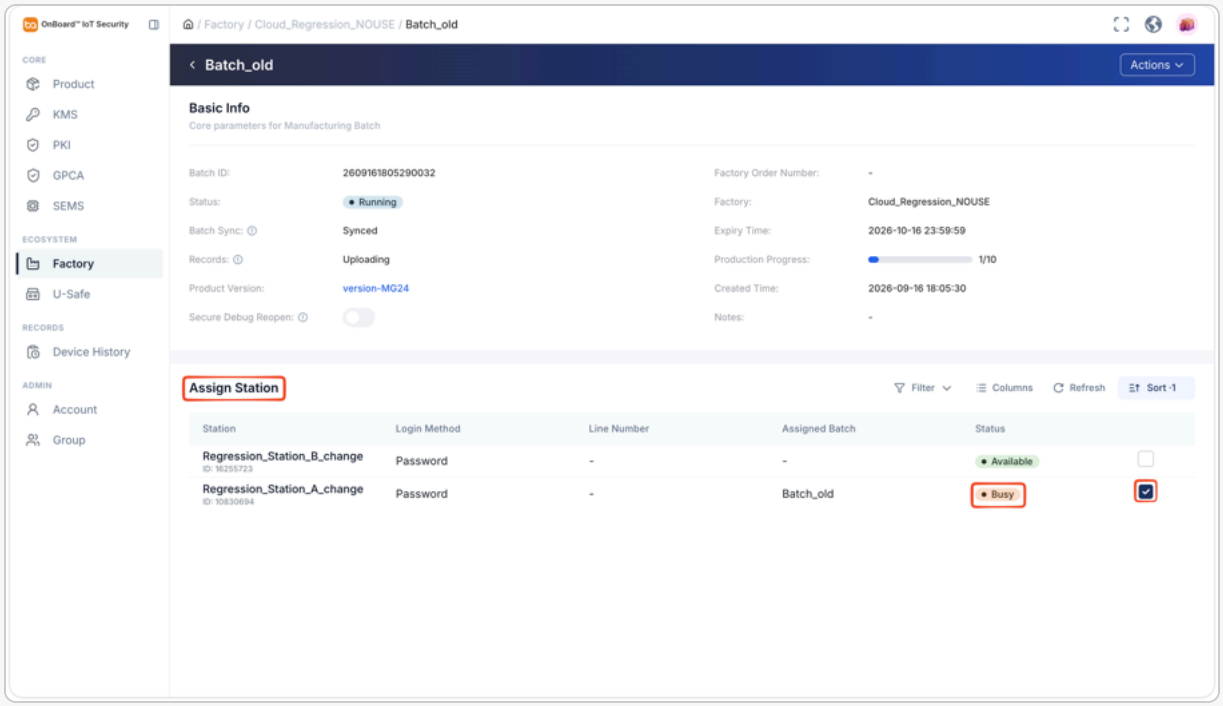


Unassign a programming station from a batch

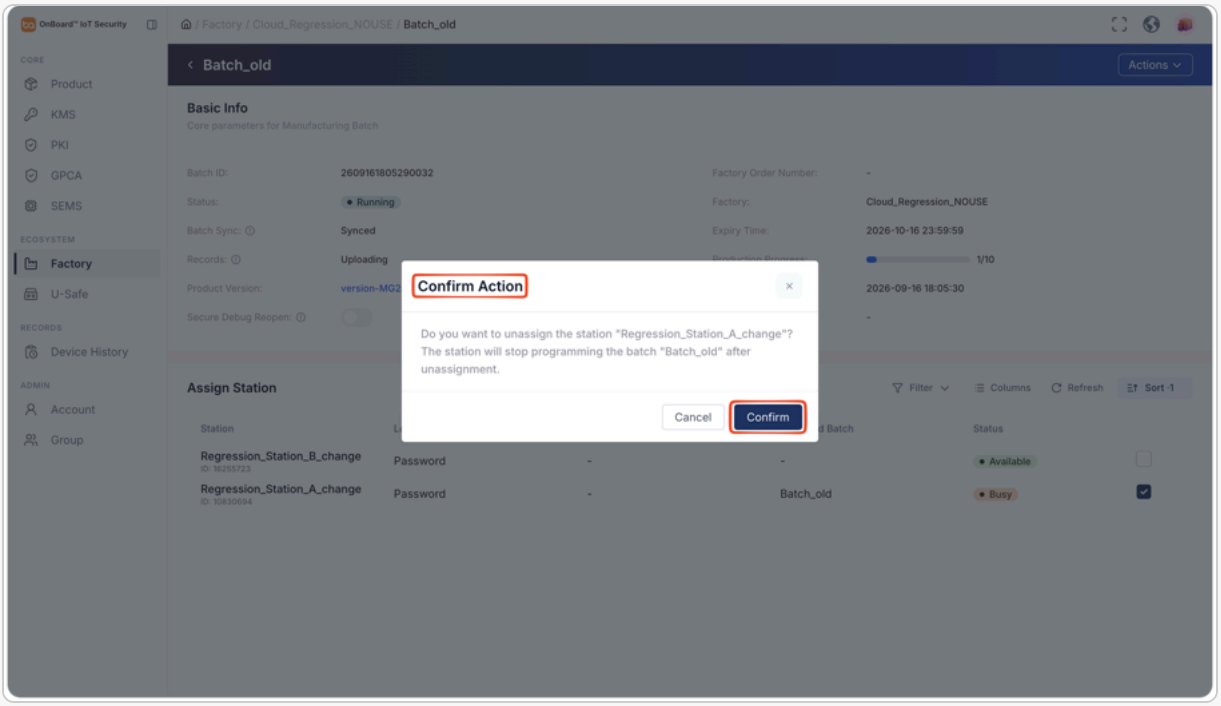
> **WARNING**
>
> After unassignment, the corresponding programming station can no longer be used for programming this batch.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Batch** tab and click the batch to navigate to the batch page.

4. In the **Assign Station** section of the batch page, find the corresponding batch and uncheck the programming station with the **Busy** status.



5. In the **Confirm Action** window, click **Confirm** to complete the unassignment of the programming station. After unassignment, the programming station status will change to **Available**.



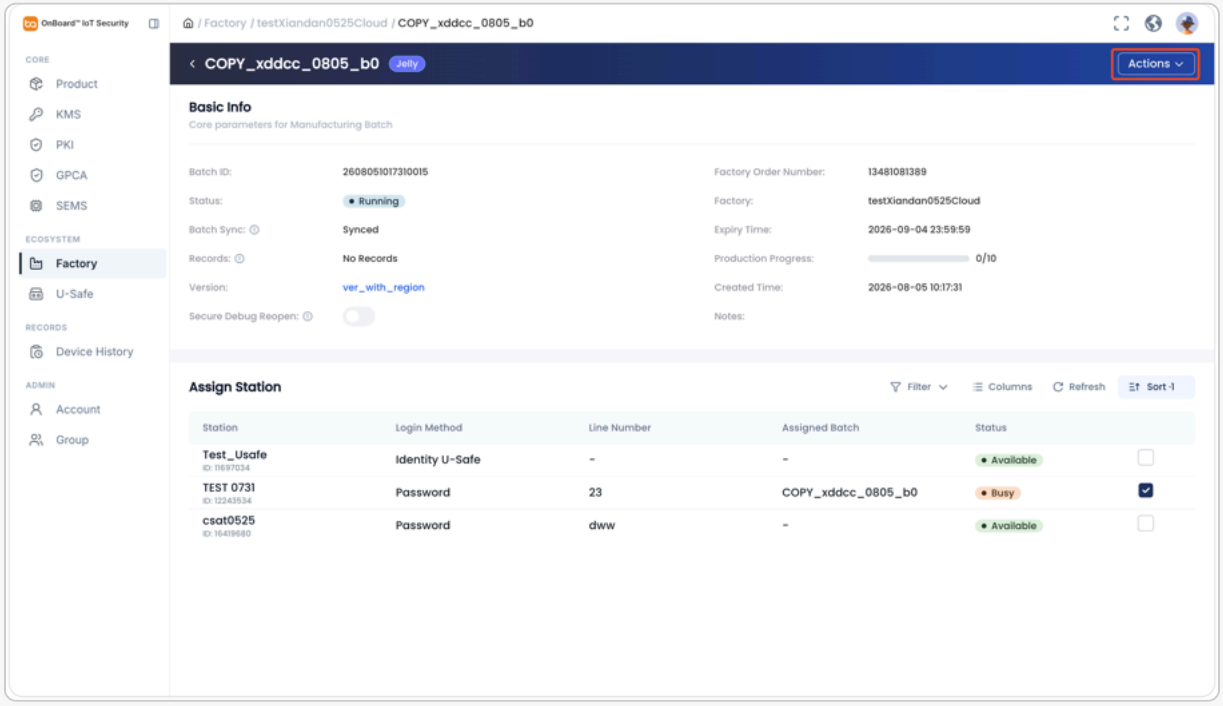
Turn off, turn on or delete a batch

> **INFO**
>
> After a batch is deleted, any programming stations assigned to that batch will be automatically unassigned.

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.
3. On the factory page, select the **Batch** tab and click the batch to navigate to the batch page.
4. On the batch page, click **Actions** and then select **Turn Off**, **Turn On** or **Delete**.

TIP

A batch can only be deleted when it is in a non-running status.



Version: v3.4.0 (Latest)

How to check factories in OnBoard™ IoT Security

This article will guide you on how to check factory information, factory status, programming station information, and batch information in OnBoard™ IoT Security (OBIS).

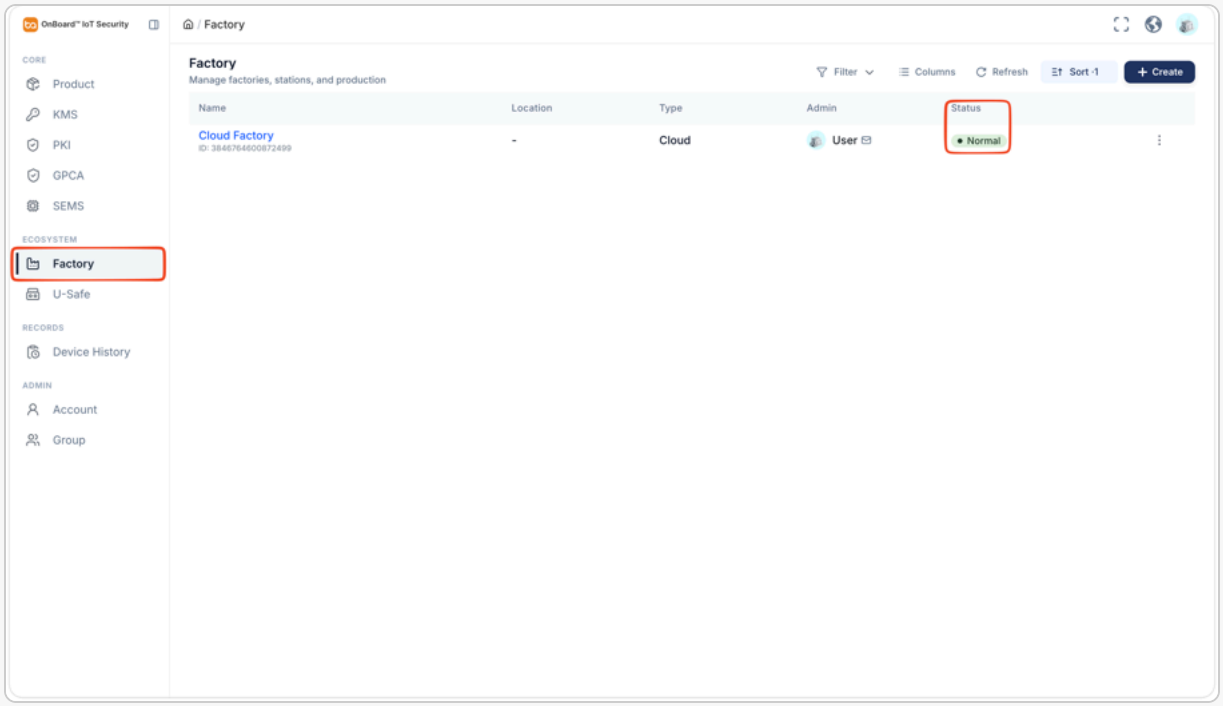
Prerequisites

Before getting started, please ensure that you have factory role permissions as a Factory Admin or Factory Manager.

Check factory status

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **Factory**. On the **Factory** page, the **Status** column will display three statuses: **Normal**, **Locked**, and **Pending**.

> **TIP**
>
> The factory list only displays the factories you are involved in.
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



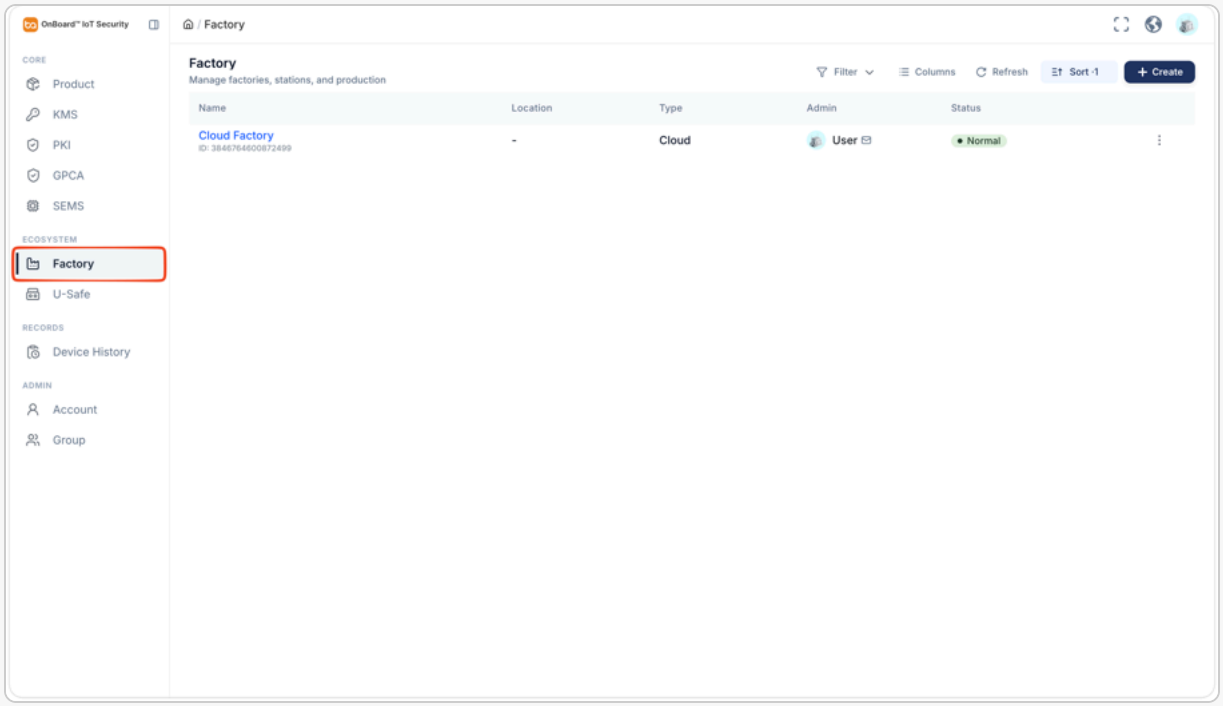
Description of factory status:

Status	Description
Normal	The factory can be selected when creating a batch. ◦ Local factory: Once an HSM U-Safe is added to the local factory, the status will change from **Pending** to **Normal**. ◦ Cloud factory: The initial status of a cloud factory is **Normal**.
Locked	The factory has been locked, and can't be used normally.
Pending	The factory status after the factory creation but without adding an HSM U-Safe, and the factory can't be selected when creating a batch. **Note**: This status applies only to local factories.

Check the factory information

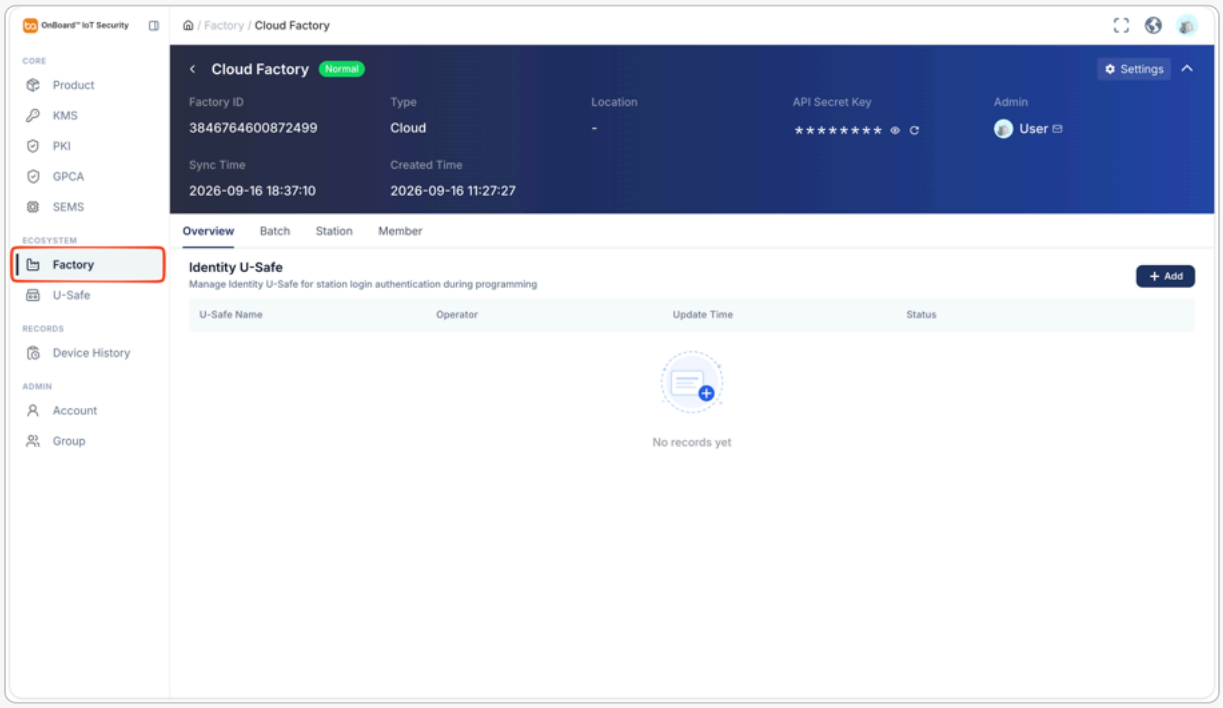
1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then you can check the factory list on the **Factory** page.



3. Select the corresponding factory to navigate to the factory page, and then you can check the factory-related information (such as **Factory ID**, **Type**, and **Location**).

> **TIP**
>
> For a local factory, after contacting Snowball for assistance in deploying OnBoard Edge Service, the corresponding service address can be found in the factory information. This service address will be used to sign in to OnBoard Edge Service and the Programming Station client.



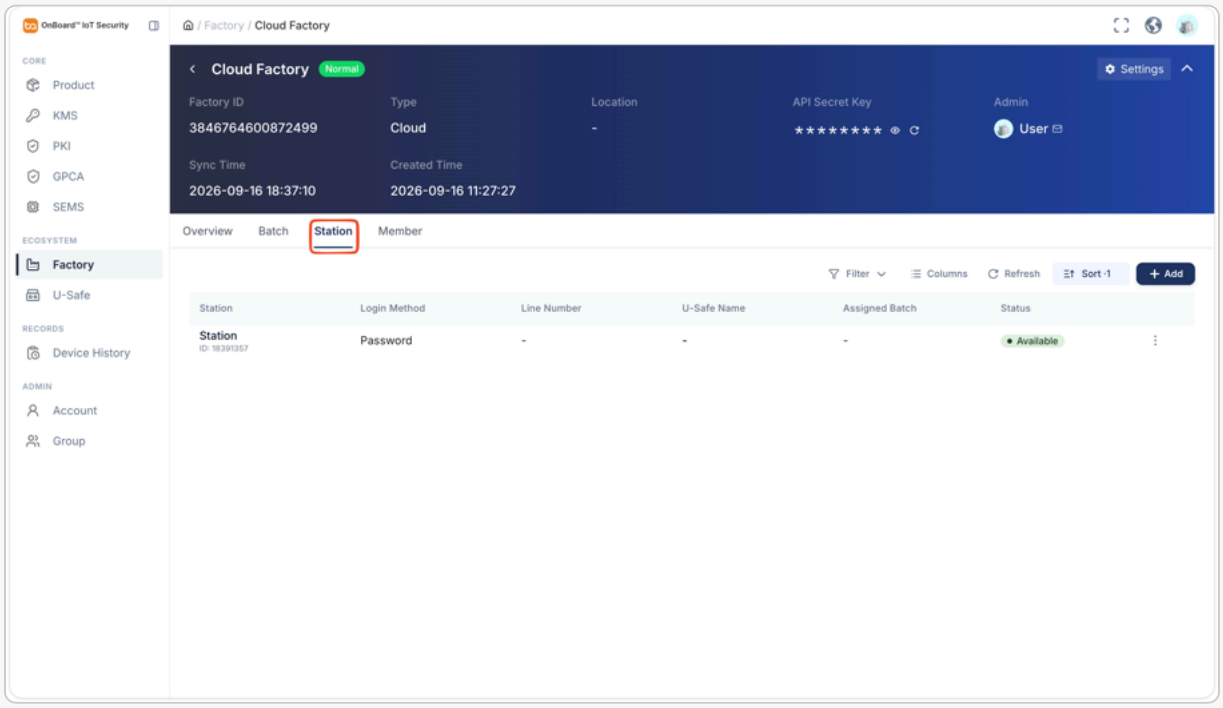
Check the programming station information

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Station** tab, and then you can check the programming station information (such as **Login Method**, **Status**, and **Assigned Batch**).

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Check the batch information

Local factory | Cloud factory

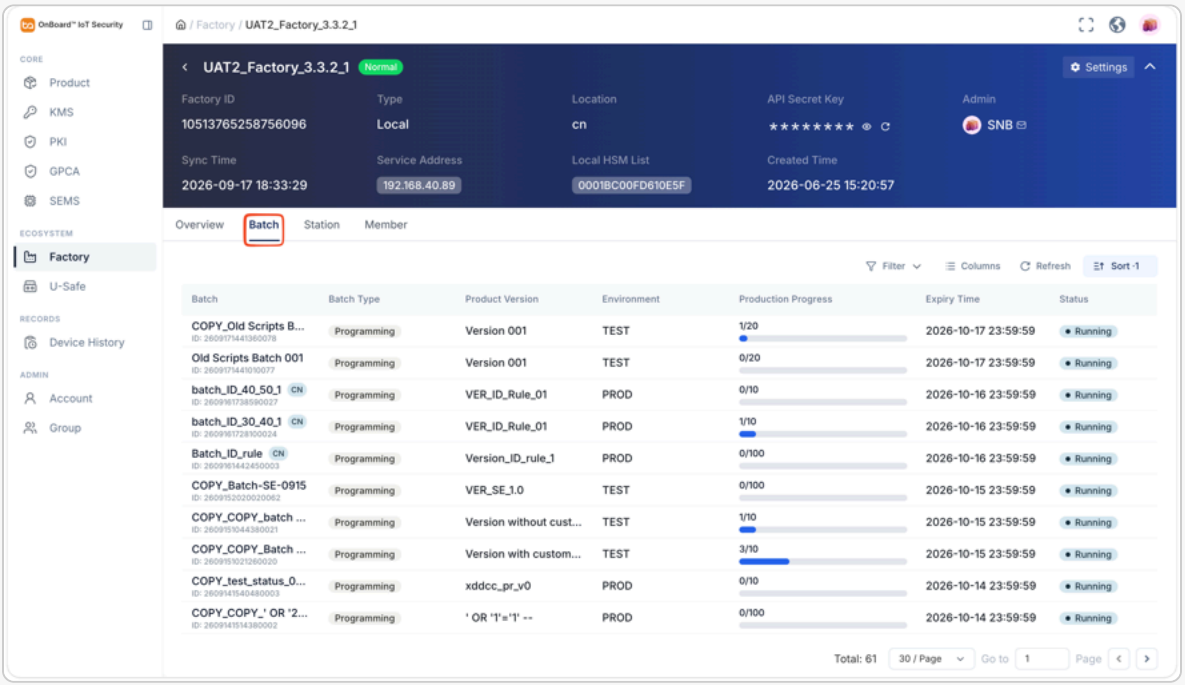
> **TIP**
>
> After selecting the corresponding factory when creating a batch, the **Batch** tab on the factory page will synchronize the batch data.

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Batch** tab, and then you can check the batch information (such as **Batch**, **Product Version**, and **Production Progress**).

   > **TIP**
   >
   > Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



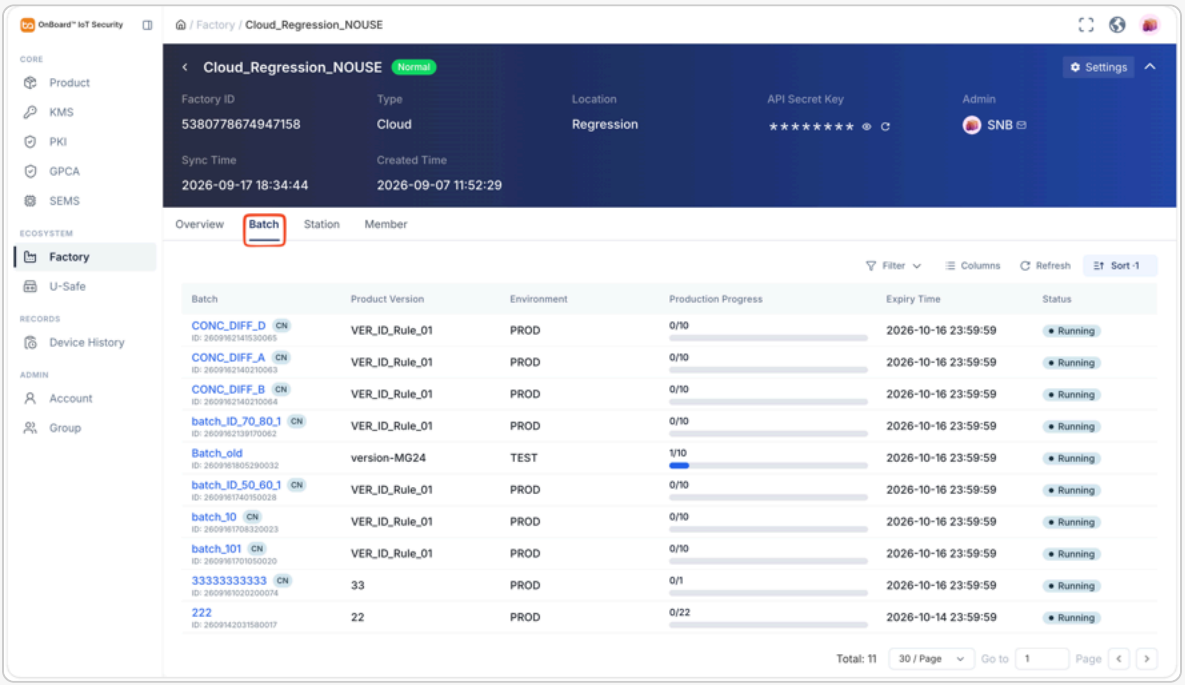
> **TIP**
>
> After selecting the corresponding factory when creating a batch, the **Batch** tab on the factory page will synchronize the batch data.

1. Sign in to OBIS.

2. In the **Ecosystem** section of the left menu, click **Factory**, and then select the corresponding factory to navigate to the factory page.

3. On the factory page, select the **Batch** tab, and then you can check the batch information (such as **Batch**, **Product Version**, and **Production Progress**).

   > **TIP**
   >
   > Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



4. Select the corresponding batch to navigate to the batch page, and then you can check the batch-related information.

Version: v3.4.0 (Latest)

How to check U-Safes in OnBoard™ IoT Security

This article will guide you on how to check the parameters and status of the U-Safe bound to the factory in OnBoard™ IoT Security (OBIS).

Prerequisites

Before getting started, please ensure that:

- The factory has been created and that the HSM U-Safe and Identity U-Safe have been bound.
- You have OBIS role permissions as a System Manager.

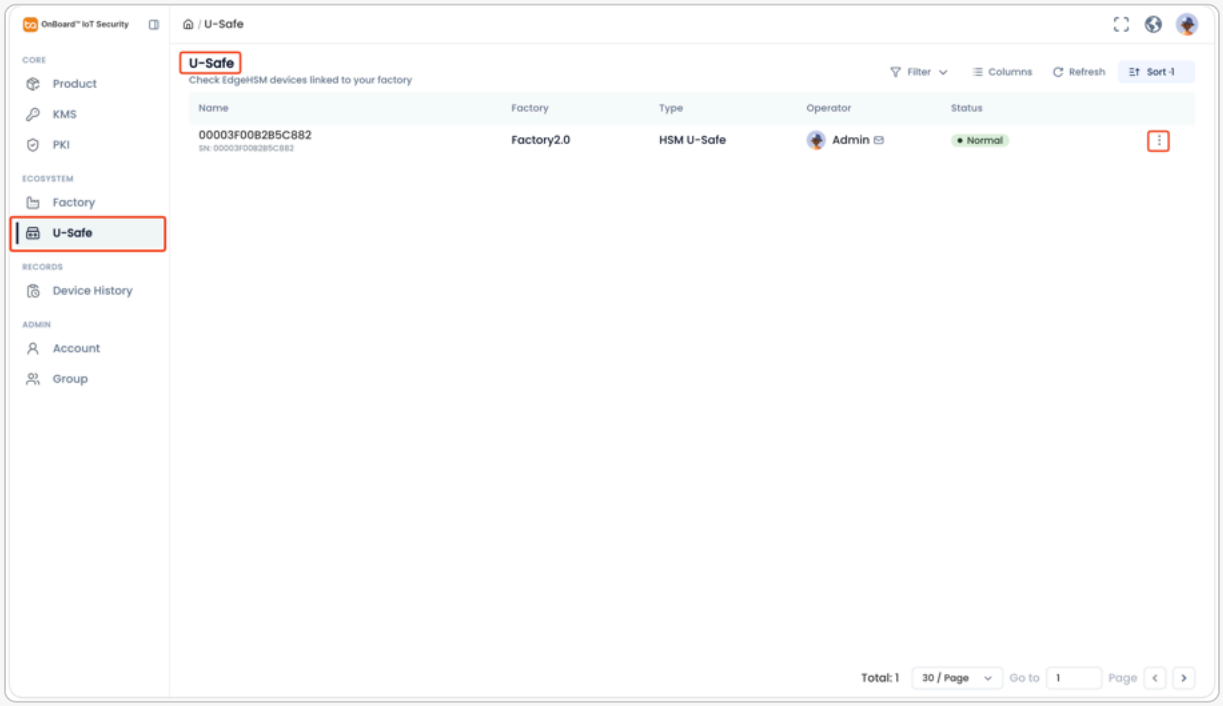
Instructions

1. Sign in to OBIS.
2. In the **Ecosystem** section of the left menu, click **U-Safe**. On the **U-Safe** page, you can check all the U-Safe information bound to factories within the tenant.

TIP

Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.

You can click the Options icon for the corresponding U-Safe and select **Lock** or **Unlock** to lock or unlock the U-Safe.



Description of U-Safe status:

Status	Description
Normal	The U-Safe status after adding the HSM U-Safe and Identity U-Safe during factory configuration, and the U-Safe can be used normally.

Status	Description
Locked	The U-Safe has been locked, and can't be used normally.

Version: v3.4.0 (Latest)

How to check device history in OnBoard™ IoT Security

This article will guide you on how to check the device history records within the tenant in OnBoard™ IoT Security (OBIS).

Prerequisites

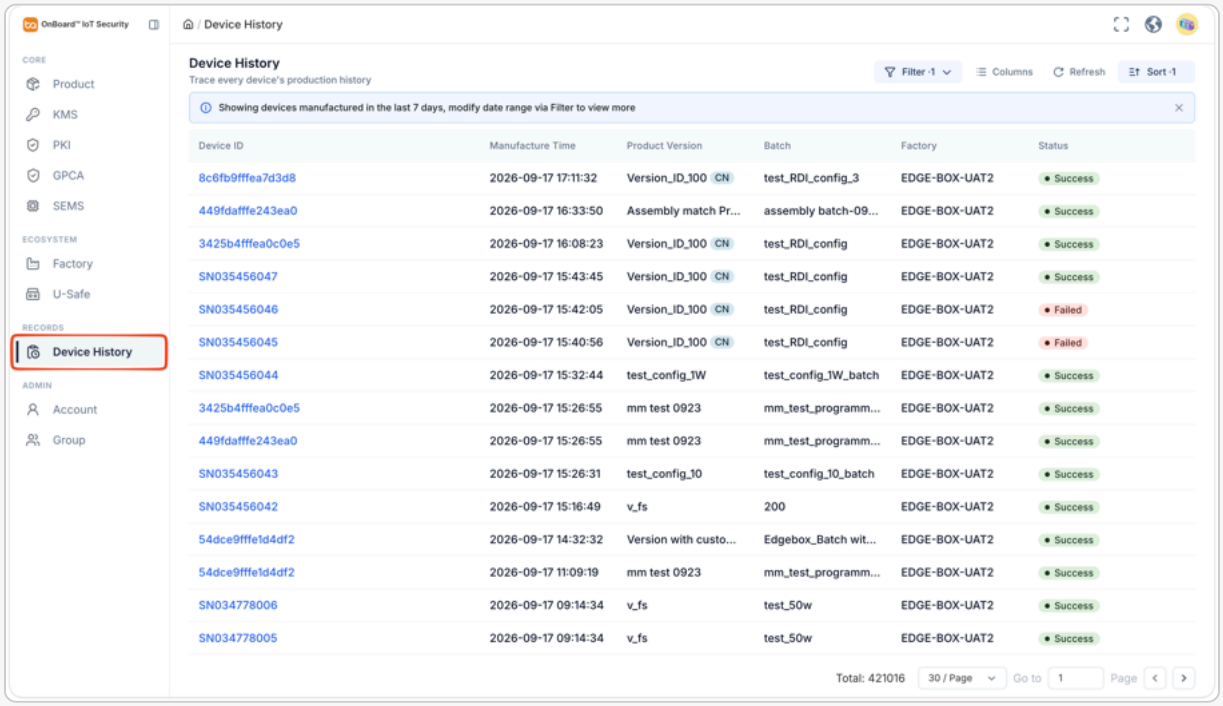
Before getting started, please ensure that:

- The device has already been programmed.
- You have either the product role permissions for the relevant product, or the factory role permissions for the relevant factory.

Instructions

1. Sign in to OBIS.
2. In the **Records** section of the left menu, click **Device History**, and then you can check the device history records on the **Device History** page.

> **TIP**
>
> Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.



Description of device history information:

Information	Description
Device ID	Device identifier.
Manufacture Time	The date and time of device started programming, in the format **YYYY-MM-DD HH:MM:SS**.
Product Version	The version name of the corresponding device.

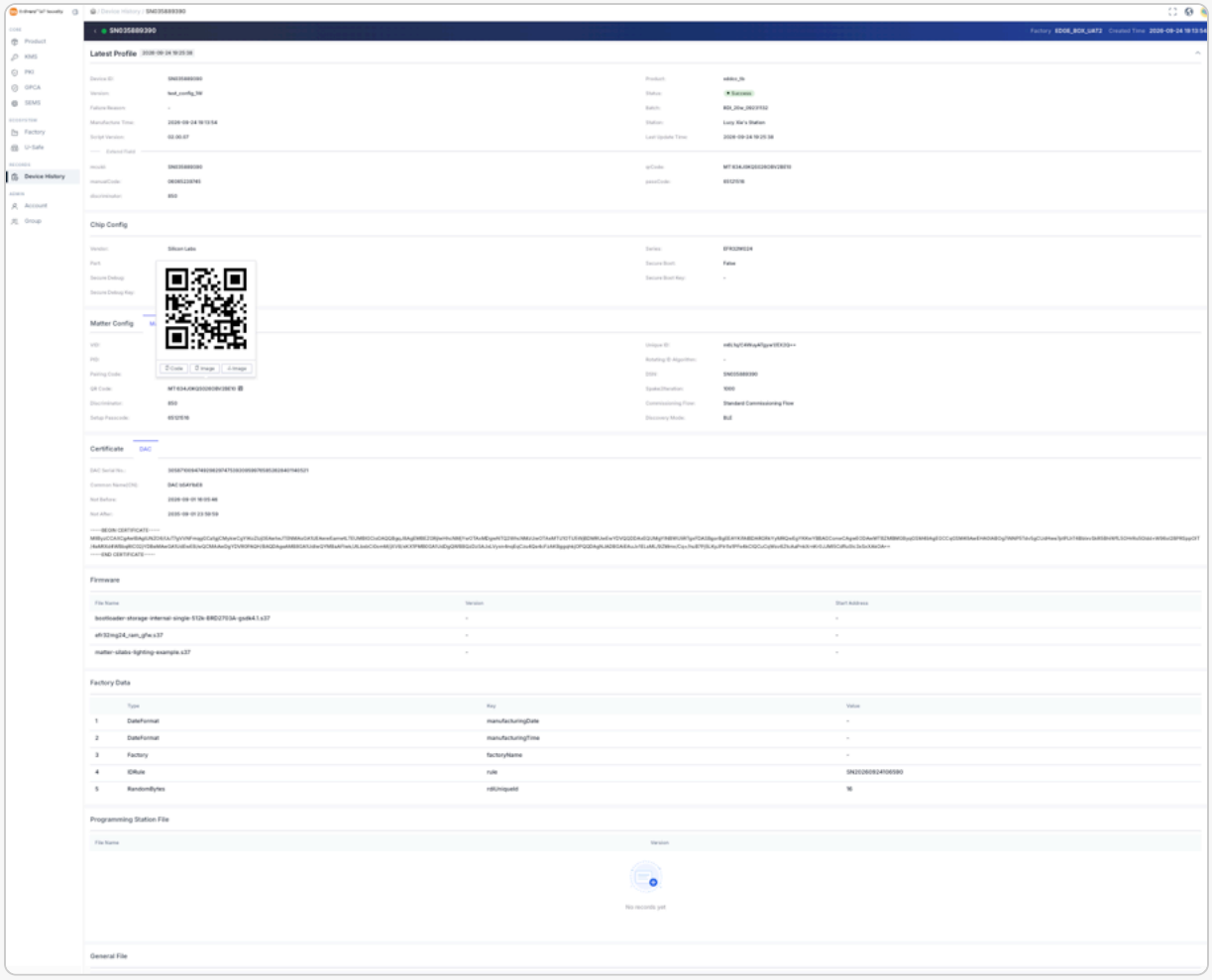
Information	Description
Batch	The batch name of the corresponding device.
Factory	The factory name of the corresponding device.
Station	The station name of the corresponding device.
Status	The status of the device programming result, such as **Success** and **Fail**.

3. Select the corresponding Device ID to navigate to the device page, where you can check the device-related information.

> **TIP**
>
> Hover the mouse over the QR code icon to display the device QR code, which is used for secure and fast commissioning.
>
> - The **Matter Detail** section displays the DAC information (such as **DAC Serial No.**, **Not Before**, and **Not After**). The **DAC Serial No.** can be used to revoke the certification of the corresponding device.
> - The **DAC Certificate** section displays the encoding of the CA certificate. By parsing the encoding of the CA certificate, key certificate attributes such as the issuer information, validity period, and public key can be extracted.

   - System and Extend fields
   - Chip Config
   - Matter Config (Matter Detail and Configuration)

- Certificate (DAC Certificate)
- Firmware
- Factory Data
- Programming Station File
- Attachment File
- General File



Version: v3.4.0 (Latest)

How to create an account in OnBoard™ IoT Security

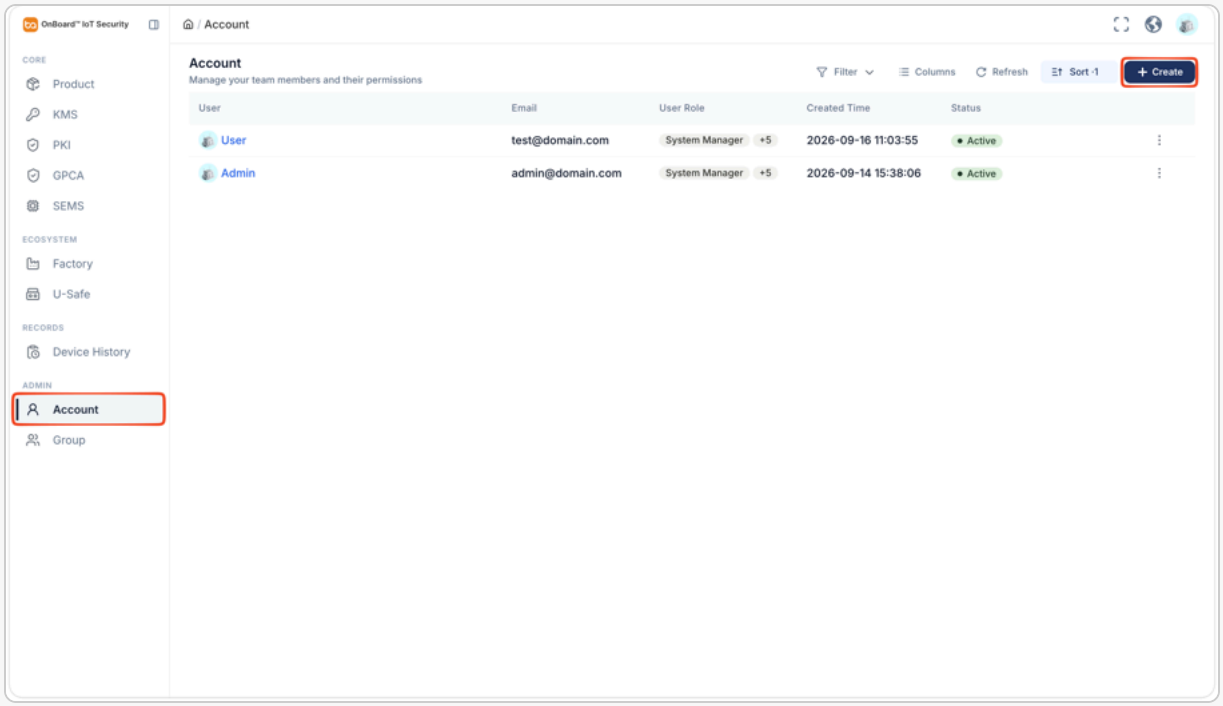
This article will guide you on how to create an account in OnBoard™ IoT Security (OBIS) so that you can add users to access and operate OBIS.

Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager.

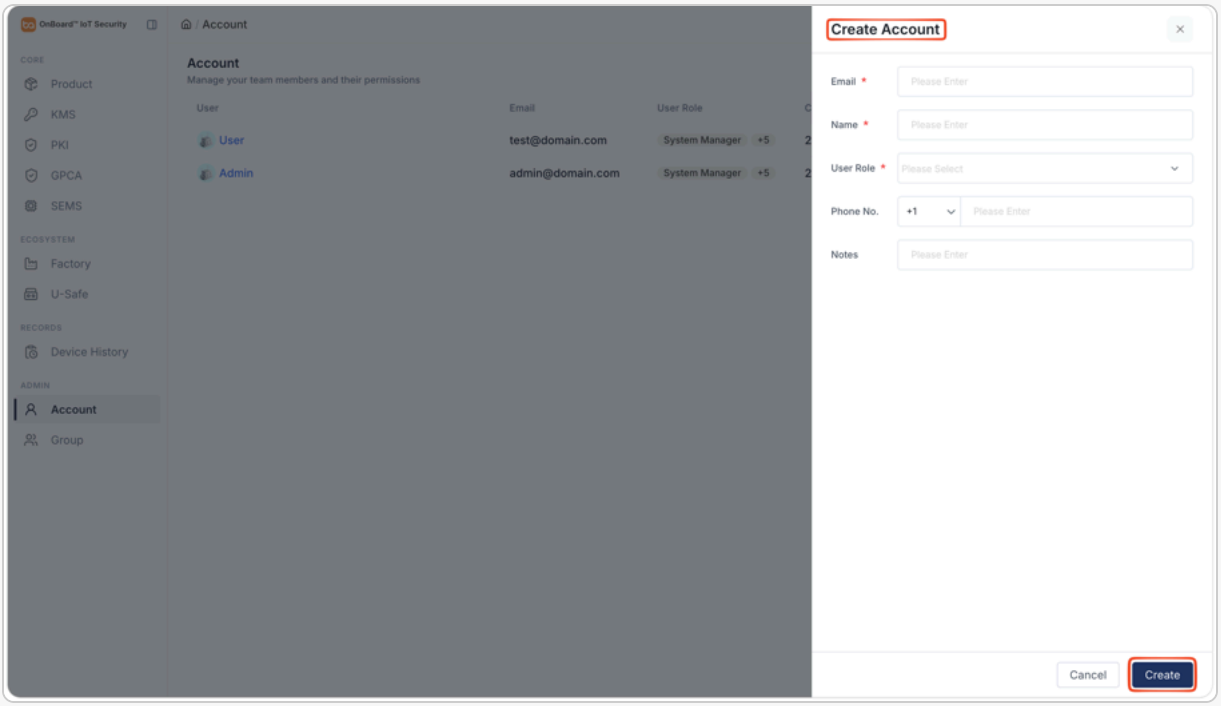
Instructions

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Account**, and then click **Create**.



3. On the **Create Account** panel, enter and select the user-related information.

> **TIP**
>
> For more information, refer to the Role classification and permission description.



Description of user information:

Information	Mandatory	Description
Email	Yes	User email, used to receive notifications and verification information; it must be real, valid, and unique. **Note**: After the account is created, the email can't be changed.
Name	Yes	User name, which does not need to be unique.

Information	Mandatory	Description
User Role	Yes	A user can be assigned multiple roles. User roles determine the user's access and operation permissions. For more information, refer to the Role classification and permission description.
Phone No.	No	Provide an additional contact method besides email for easy communication.
Notes	No	Provide additional information related to the user, such as special requirements and important notes.

4. Click **Create** to complete the account creation.

Version: v3.4.0 (Latest)

How to check accounts in OnBoard™ IoT Security

This article will guide you on how to check account information, AK (Access Key), and SK (Secret Key) in OnBoard™ IoT Security (OBIS).

Prerequisites

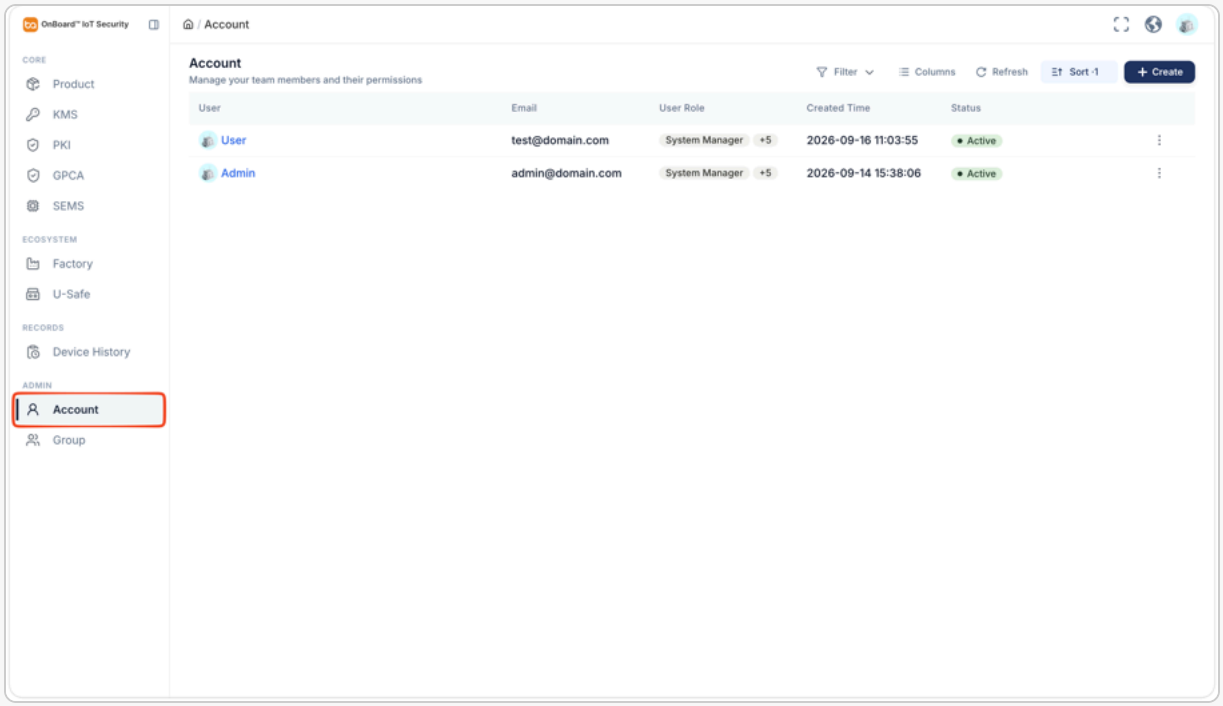
Before getting started, please ensure that you have OBIS role permissions as a System Manager.

Instructions

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Account** to navigate to the **Account** page.

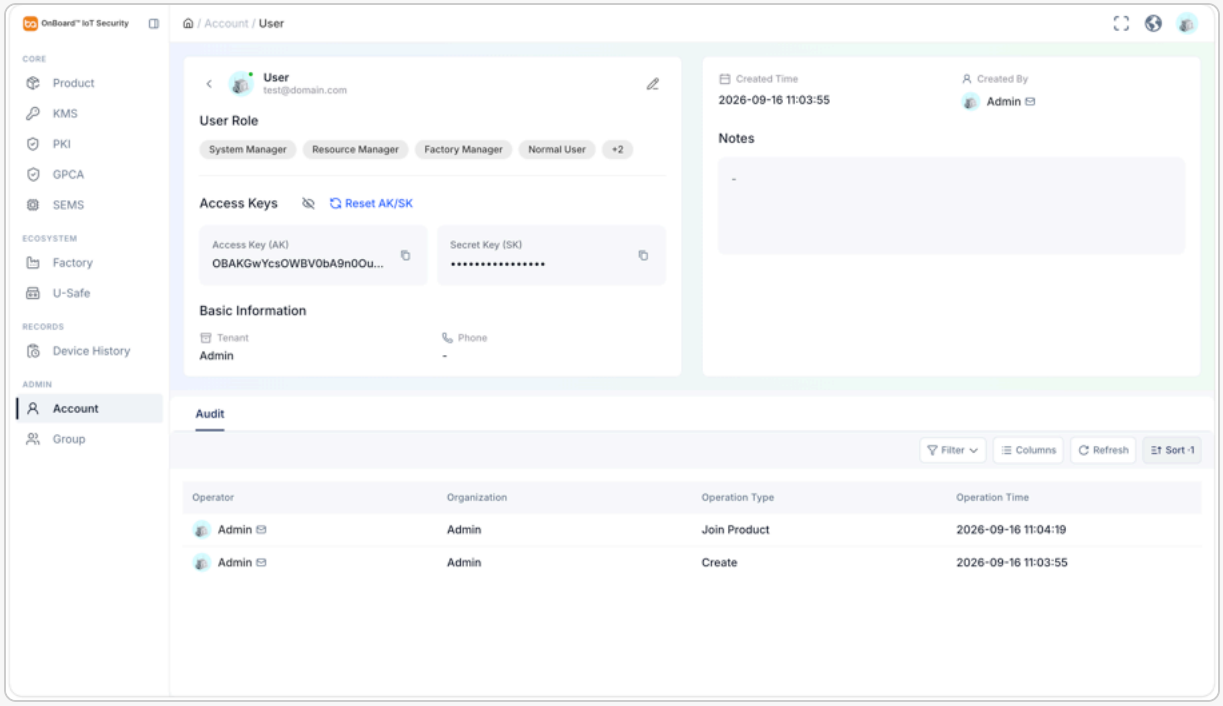
   > **TIP**
   >
   > Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.

3. On the **Account** page, select the corresponding user.



4. On the user page, you can check the account-related information (such as **User Role**, **Basic Information**, and **Audit**).

> **TIP**
>
> In the **Access Keys** section, you can view or reset the AK or SK. AK and SK can be used for authentication and API calls.


OnBoard™ IoT Security
/ Account / User
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
User
test@domain.com
User Role
System Manager
Resource Manager
Factory Manager
Normal User
+2
Access Keys
Reset AK/SK
Access Key (AK)
OBAKGwYcsOWBV0bA9n0Ou...
Secret Key (SK)
••••••••••••••••
Basic Information
Tenant
Admin
Phone
-
Created Time
2026-09-16 11:03:55
Created By
Admin
Notes
-
Audit
Filter
Columns
Refresh
Sort · 1
Operator
Organization
Operation Type
Operation Time
Admin
Admin
Join Product
2026-09-16 11:04:19
Admin
Admin
Create
2026-09-16 11:03:55

Version: v3.4.0 (Latest)

How to manage accounts in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS) to manage user access and permissions for OBIS:

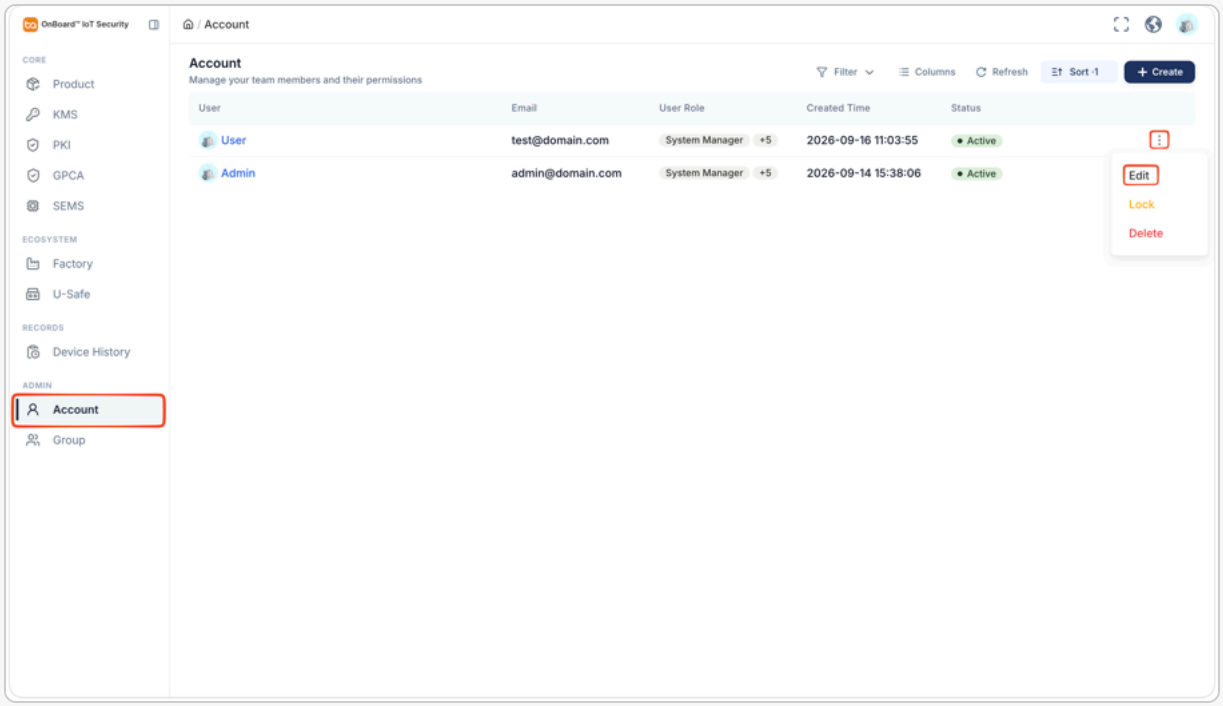
- Edit the information of an account
- Lock or unlock an account
- Delete an account

Prerequisites

Before getting started, please ensure that you have OBIS role permissions as a System Manager.

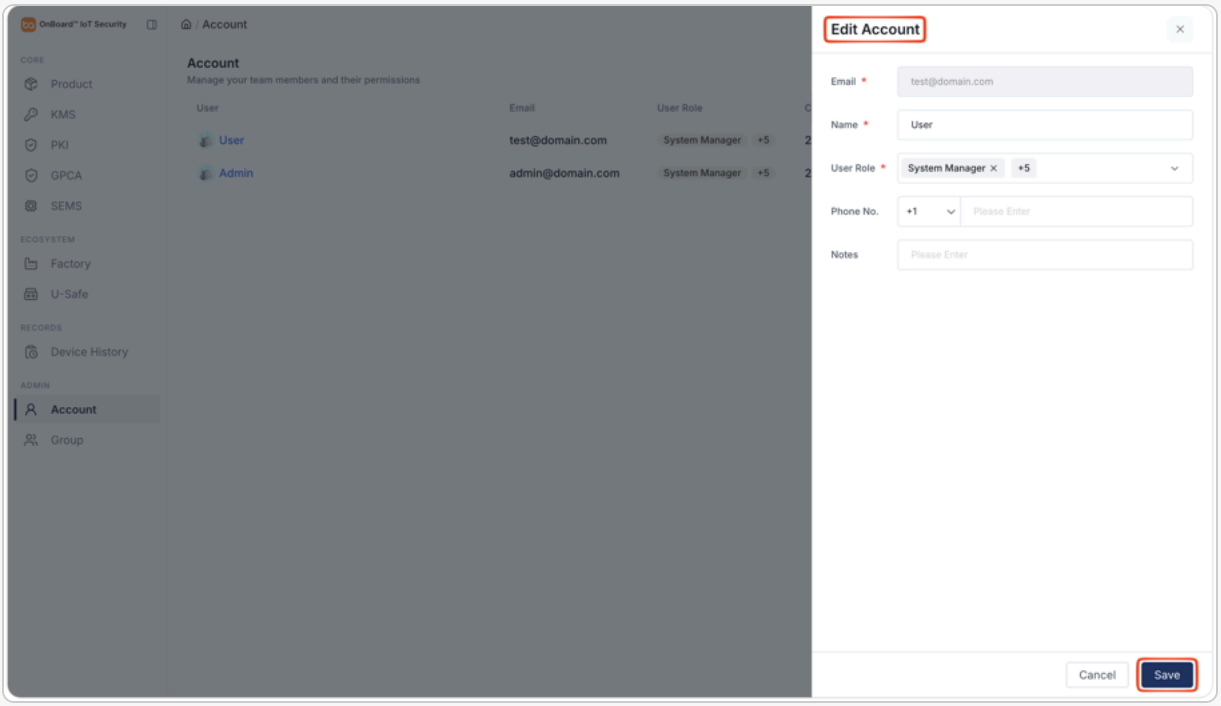
Edit the information of an account

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Account** to navigate to the **Account** page.
3. On the **Account** page, click the Options ⋮ icon for the corresponding account and select **Edit**.



4. On the **Edit Account** panel, change the account information (**Name**, **User Role**, **Phone No.**, and **Notes**), and then click **Save**.

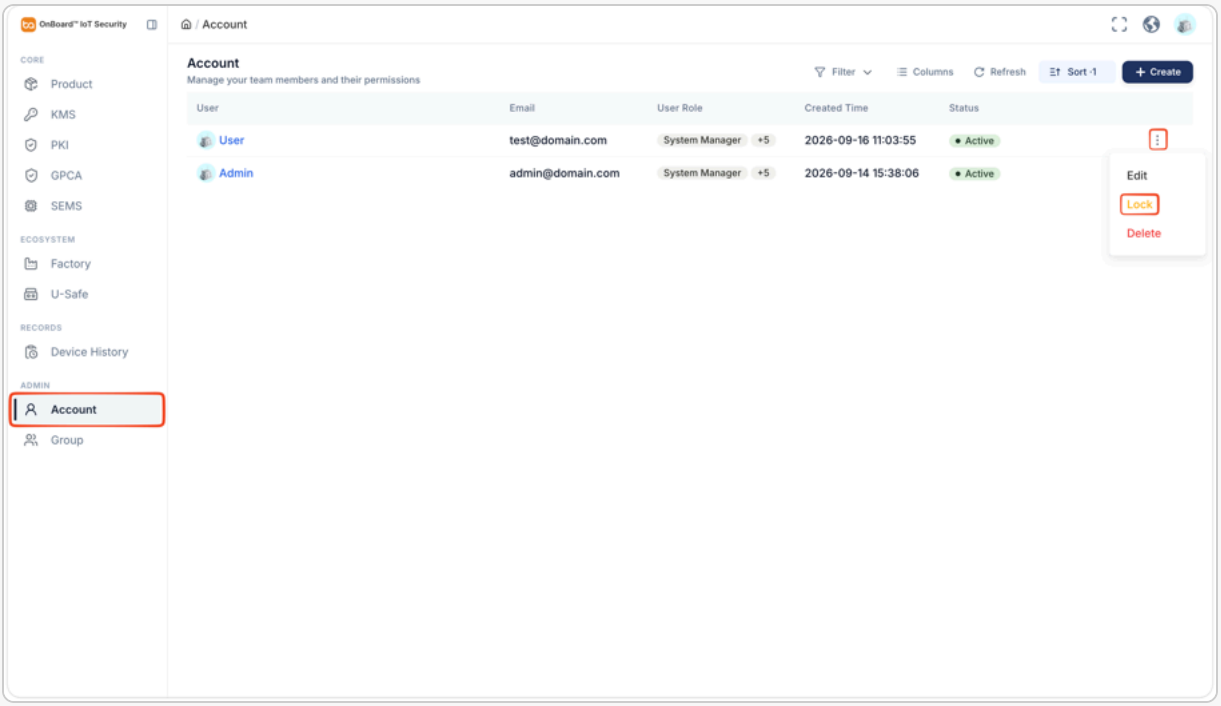
> **TIP**
>
> A user can be assigned multiple roles. User roles determine the user's access and operation permissions. For more information, refer to the Role classification and permission description.



Lock or unlock an account

> **TIP**
>
> Lock the account to prevent its sign-in and use. Once locked, the account status will change to **Disabled**.

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Account** to navigate to the **Account** page.
3. On the **Account** page, click the Options ⋮ icon for the corresponding account and select **Lock** or **Unlock**.

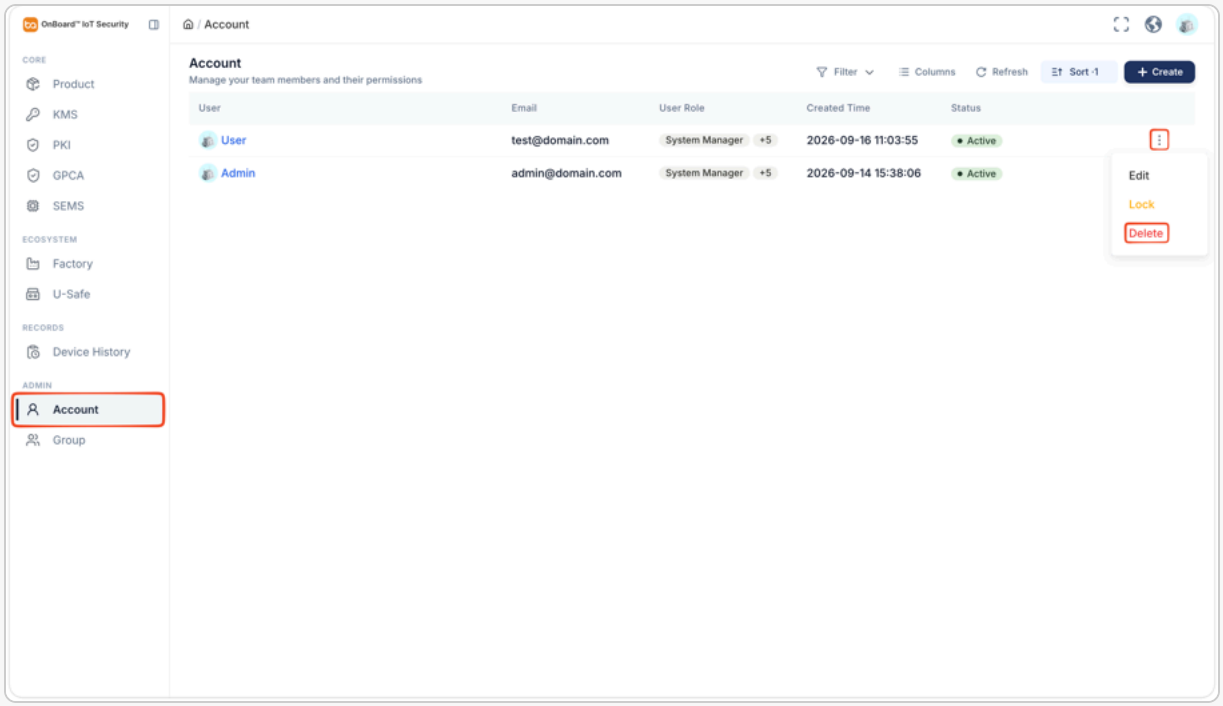


4. In the pop-up window, click **Confirm** to lock or unlock the account.

Delete an account

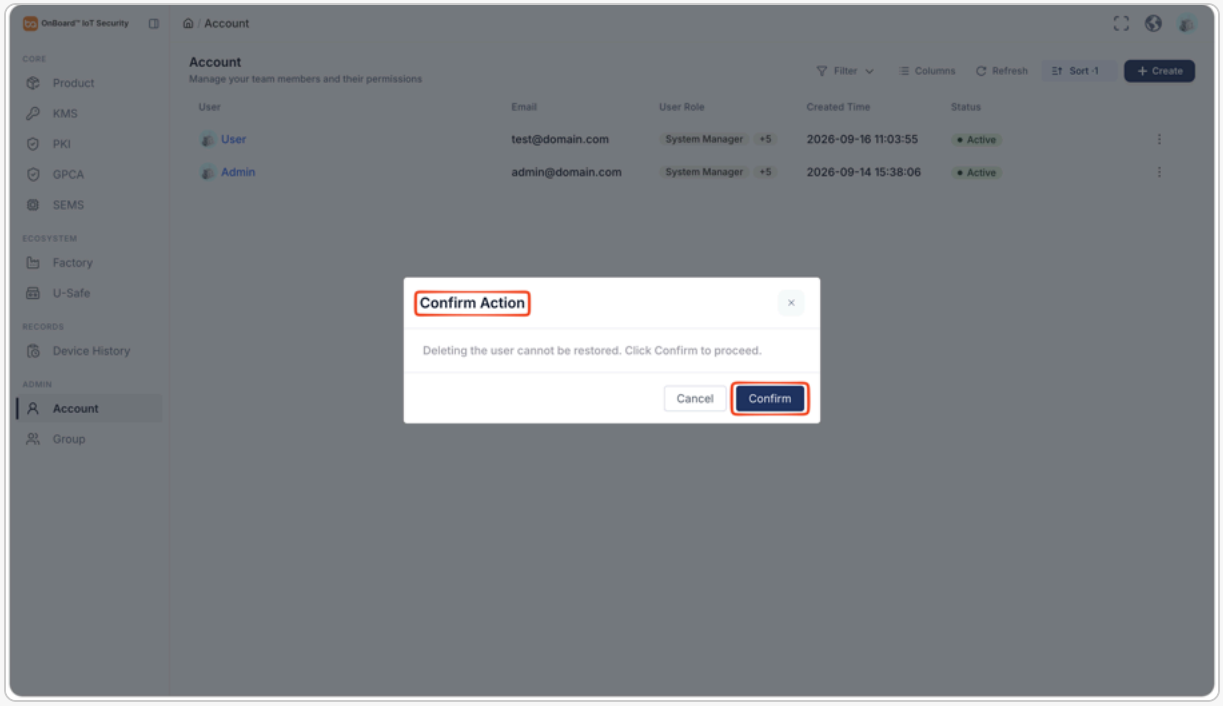
> **WARNING**
>
> Deleted accounts cannot be recovered. Please proceed with caution.

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Account** to navigate to the **Account** page.
3. On the **Account** page, click the Options ⋮ icon for the corresponding account and select **Delete**.



4. In the **Confirm Action** window, click **Confirm** to delete the account.

> **TIP**
>
> If the user has admin rights for some resources, those resources must be transferred to another active user before the account is deleted.


OnBoard™ IoT Security
Account
CORE
Product
KMS
PKI
GPCA
SEMS
ECOSYSTEM
Factory
U-Safe
RECORDS
Device History
ADMIN
Account
Group
Account
Manage your team members and their permissions
Filter
Columns
Refresh
Sort ·1
+ Create
User
Email
User Role
Created Time
Status
User
test@domain.com
System Manager +5
2026-09-16 11:03:55
Active
Admin
admin@domain.com
System Manager +5
2026-09-14 15:38:06
Active
Confirm Action
Deleting the user cannot be restored. Click Confirm to proceed.
Cancel
Confirm

Version: v3.4.0 (Latest)

How to create a group in OnBoard™ IoT Security

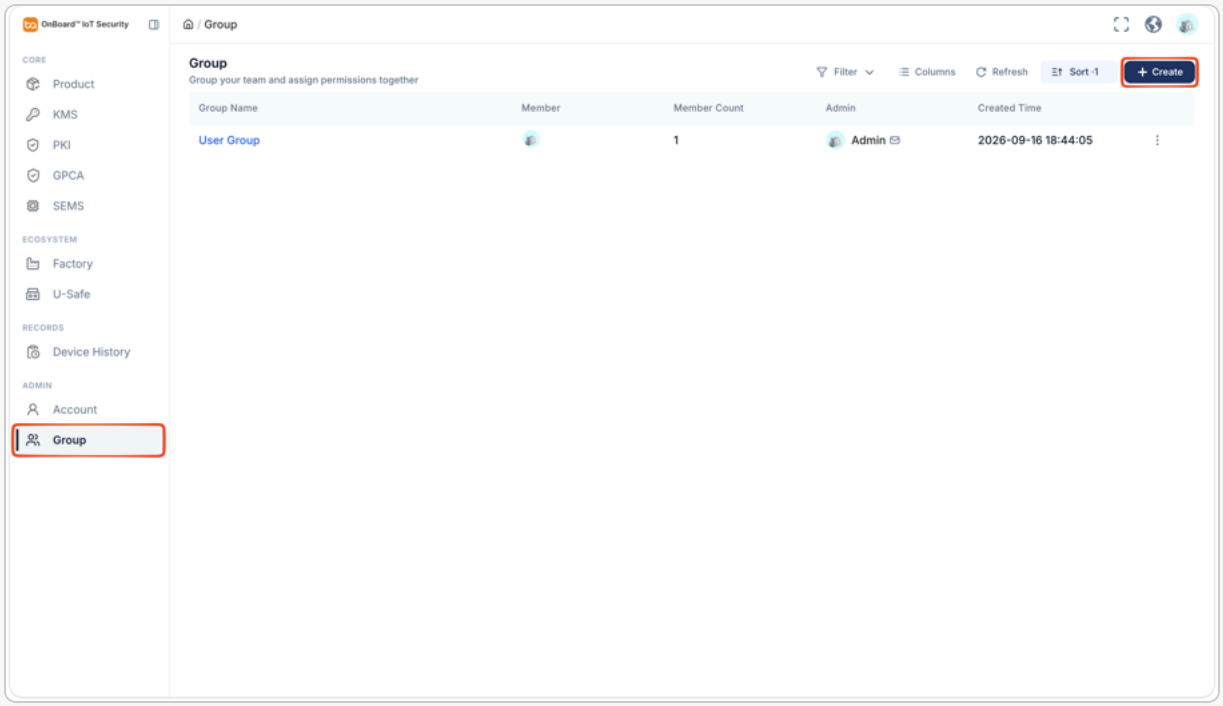
This article will guide you on how to create a user group in OnBoard™ IoT Security (OBIS) for centralized user management.

Prerequisites

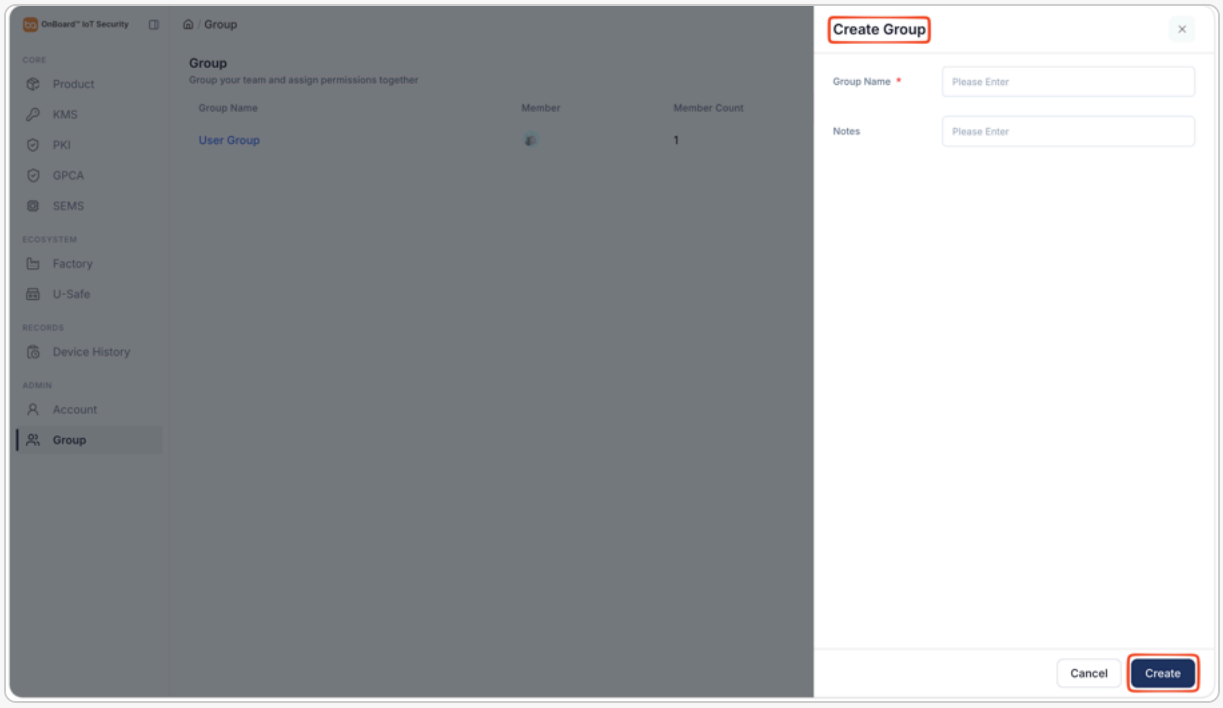
Before getting started, please ensure that you have OBIS role permissions as a System Manager.

Instructions

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group**, and then click **Create**.



3. On the **Create Group** panel, enter the user group related information.



Description of user group information:

Information	Mandatory	Description
Group Name	Yes	The user group name must be unique.
Notes	No	Provide additional information related to the user group, such as special requirements and important notes.

4. Click **Create** to complete the user group creation.

Version: v3.4.0 (Latest)

How to check groups in OnBoard™ IoT Security

This article will guide you on how to check group details in OnBoard™ IoT Security (OBIS).

Prerequisites

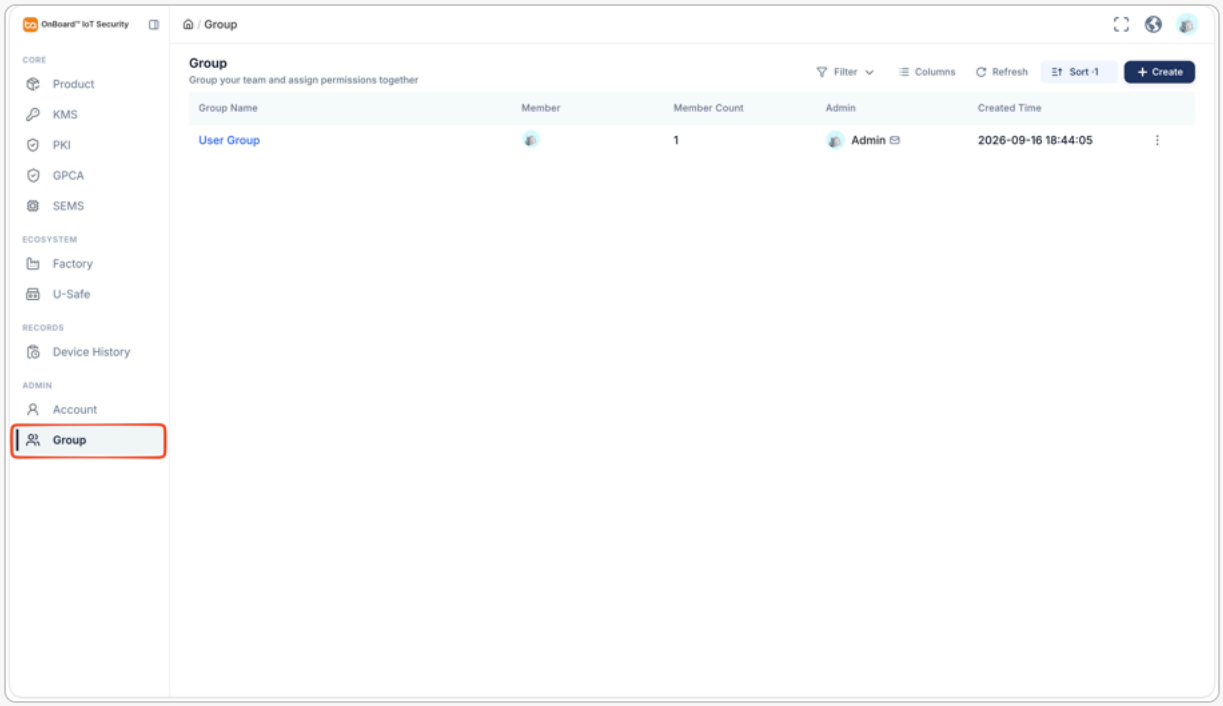
Before getting started, please ensure that you have OBIS role permissions as a System Manager.

Instructions

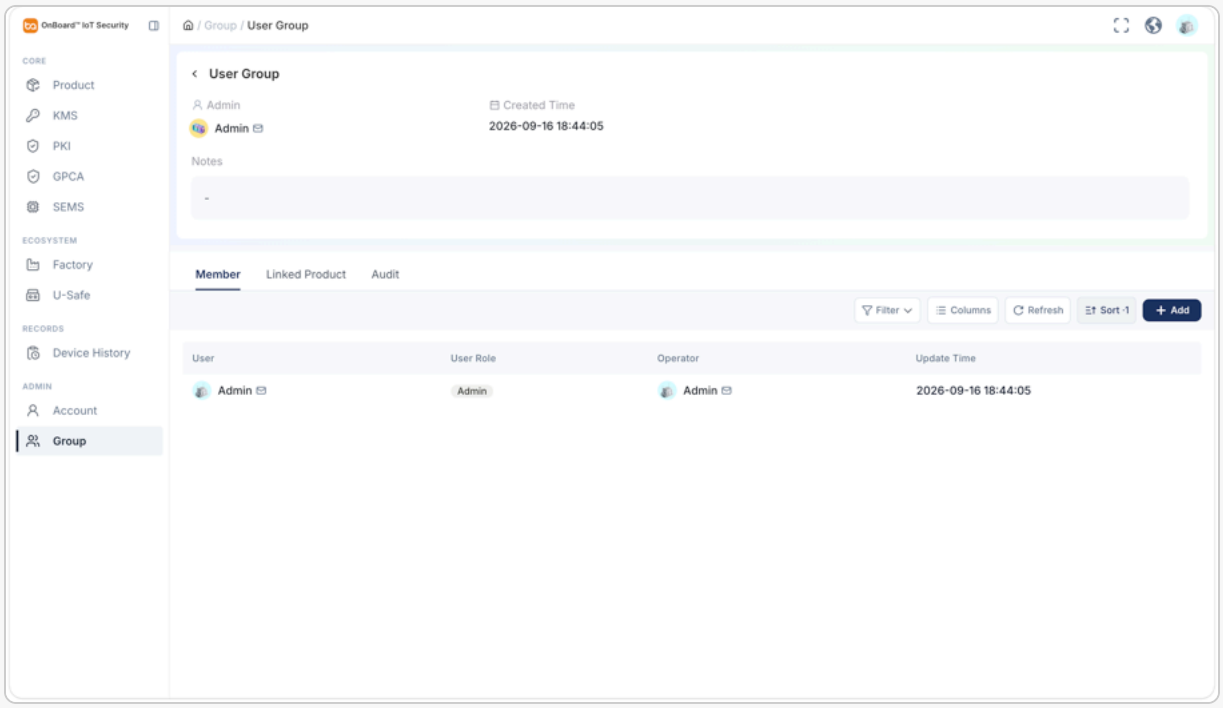
1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group** to navigate to the **Group** page.

   > **TIP**
   >
   > Click the Filter, Sort, Refresh, and Columns Options icons to filter, sort, refresh data, and to customize which columns are shown and how they are ordered.

3. On the **Group** page, select the corresponding group.



4. On the group page, you can check the group related information (such as **Member**, **Linked Product**, and **Audit**).



Version: v3.4.0 (Latest)

How to manage groups in OnBoard™ IoT Security

This article will guide you through the following operations in OnBoard™ IoT Security (OBIS) to manage the access and permissions of user group members for OBIS:

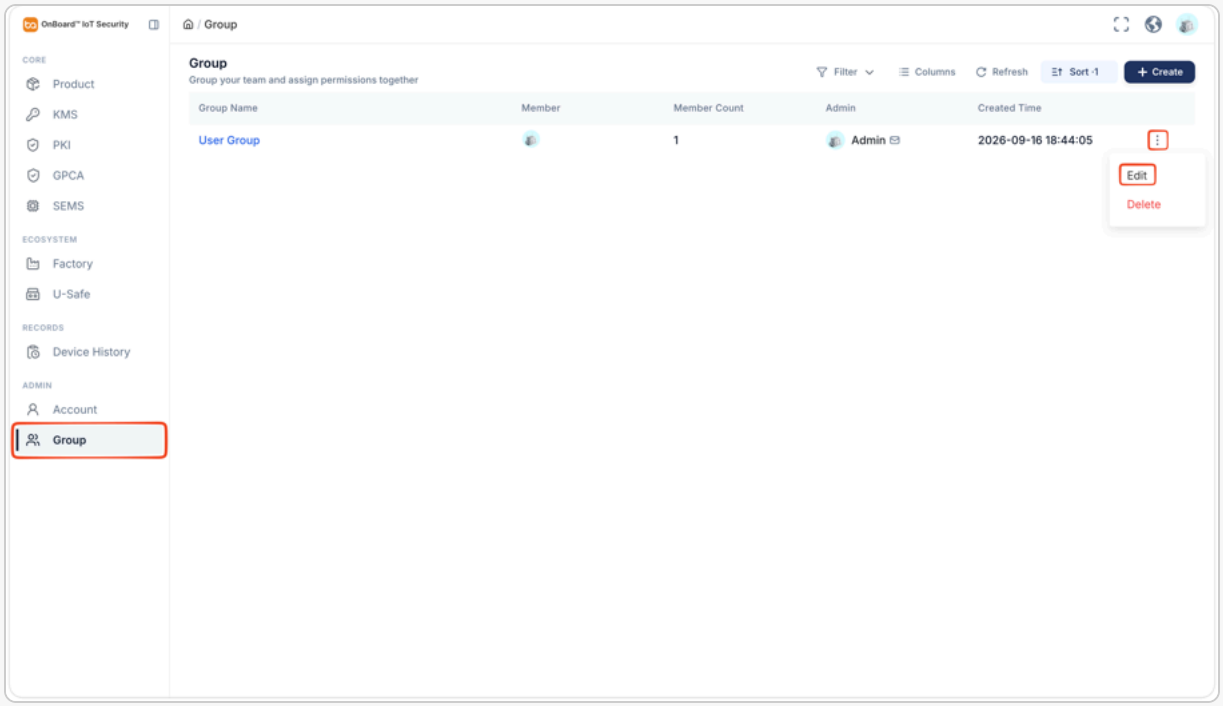
- Edit the information of a user group
- Add a user group member
- Update the user group member role
- Remove a user group member
- Delete a user group

Prerequisites

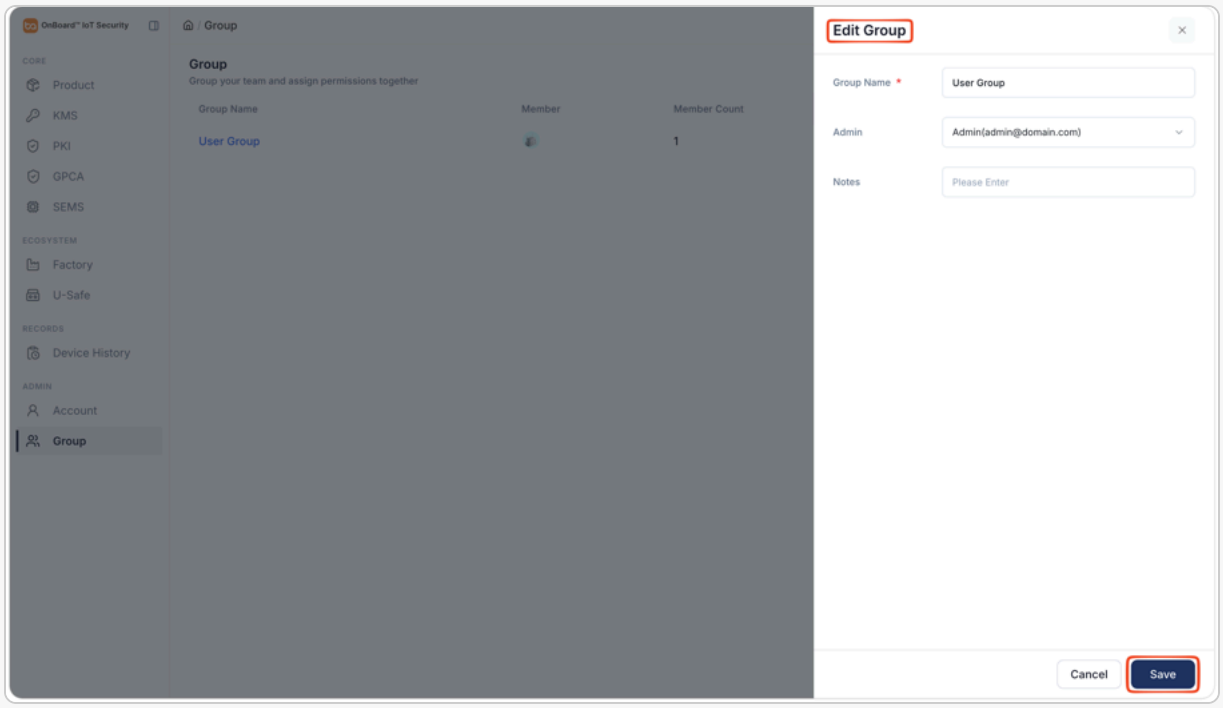
Before getting started, please ensure that you have OBIS role permissions as a System Manager.

Edit the information of a user group

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group** to navigate to the **Group** page.
3. On the **Group** page, select the Options ⋮ icon for the corresponding user group and select **Edit**.

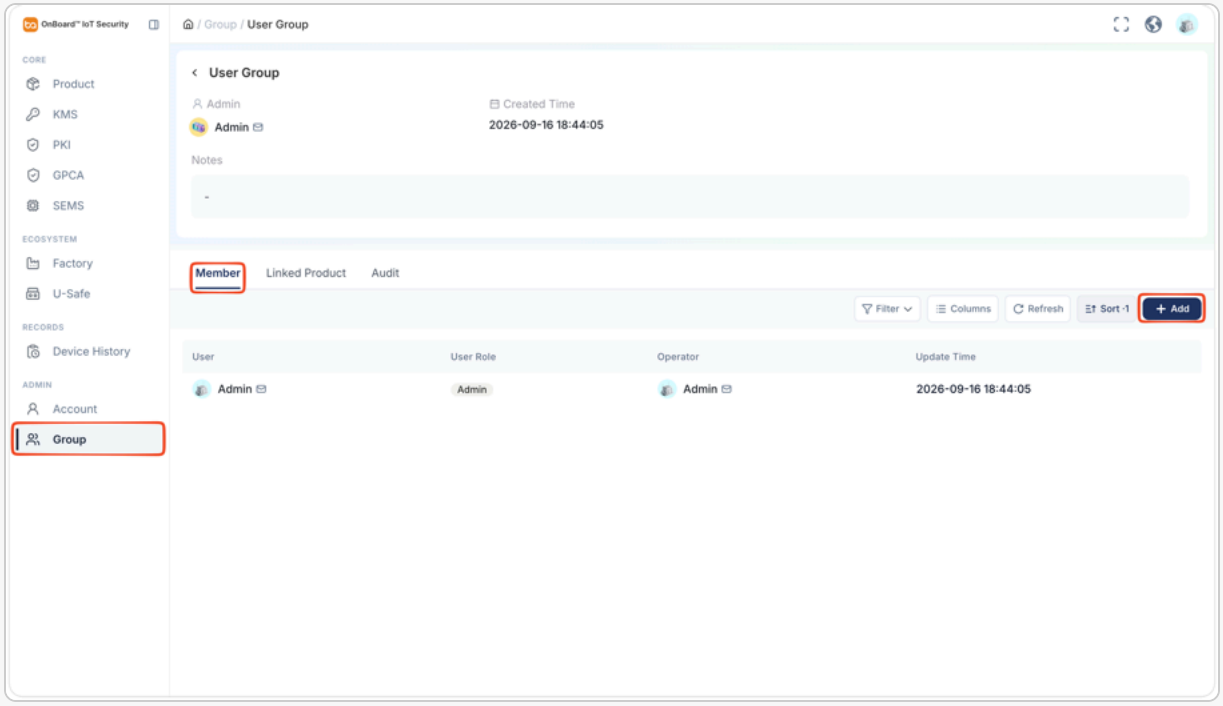


4. On the **Edit Group** panel, change the user group information (**Group Name**, **Admin**, and **Notes**), and then click **Save**.

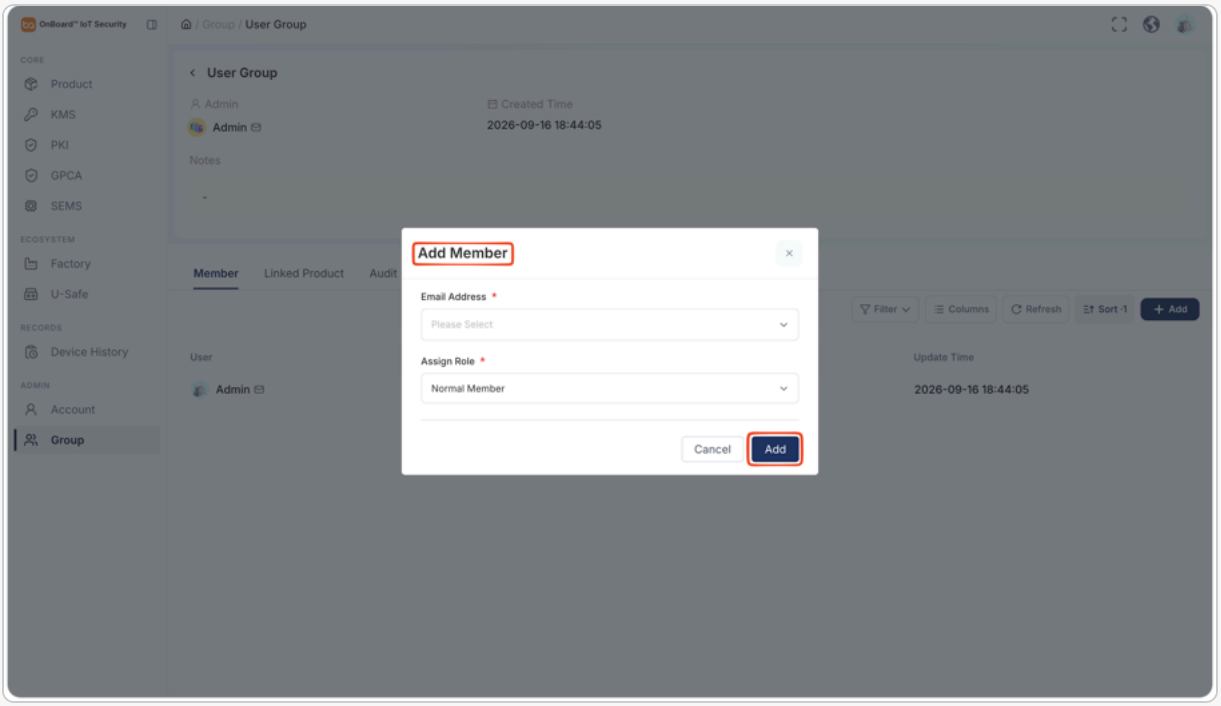


Add a user group member

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group** to navigate to the **Group** page.
3. On the **Group** page, select the corresponding user group.
4. On the group page, click **Add**.

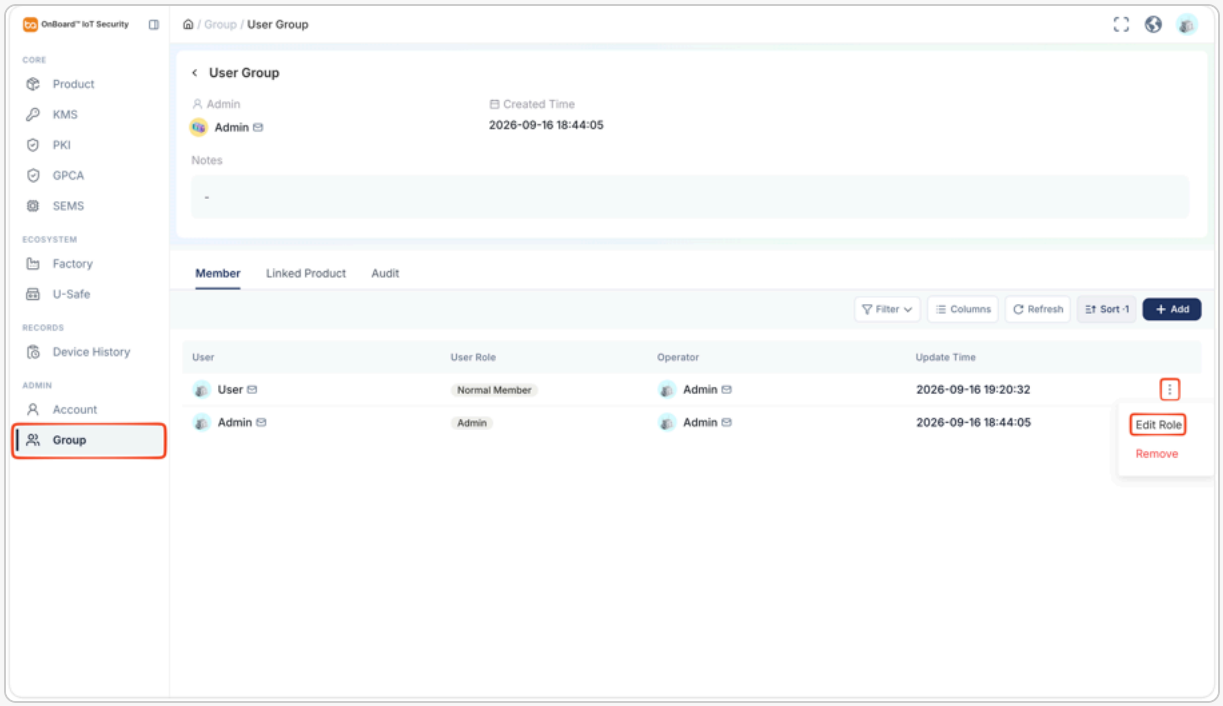


5. In the **Add Member** window, enter the email address and assign the corresponding roles. Then, click **Add** to complete adding the user group member.

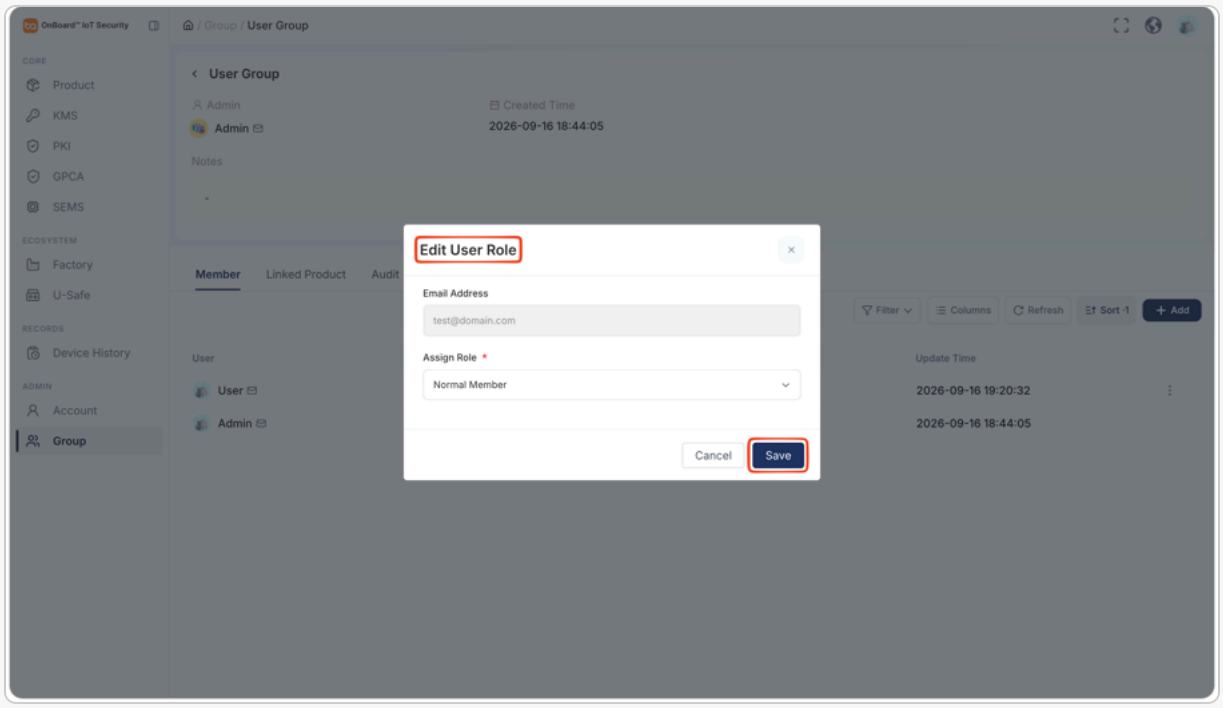


Update a user group member role

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group** to navigate to the **Group** page.
3. On the **Group** page, select the corresponding user group.
4. On the group page, click the Options ⋮ icon for the corresponding member and select **Edit Role**.

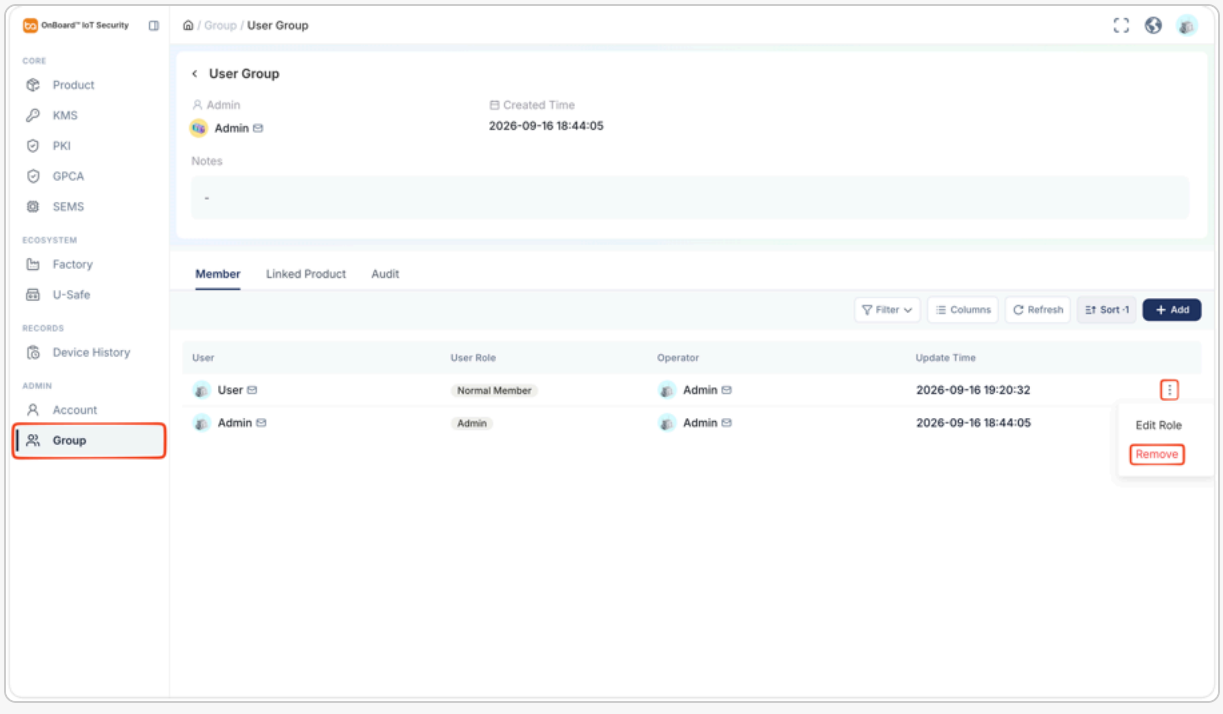


5. In the **Edit User Role** window, select the corresponding roles. Then, click **Save** to update the user group member role.

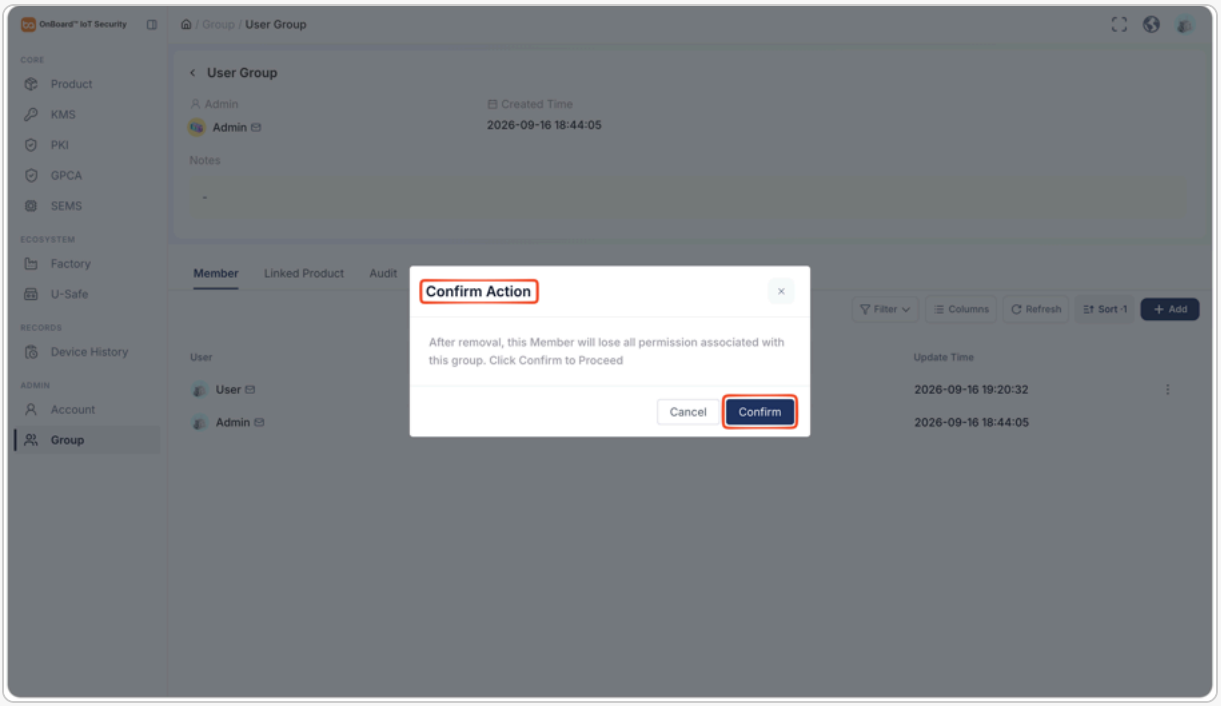


Remove a user group member

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group** to navigate to the **Group** page.
3. On the **Group** page, select the corresponding user group.
4. On the group page, locate the **Group Member** section and then click the Options ⋮ icon for the corresponding member and select **Remove**.



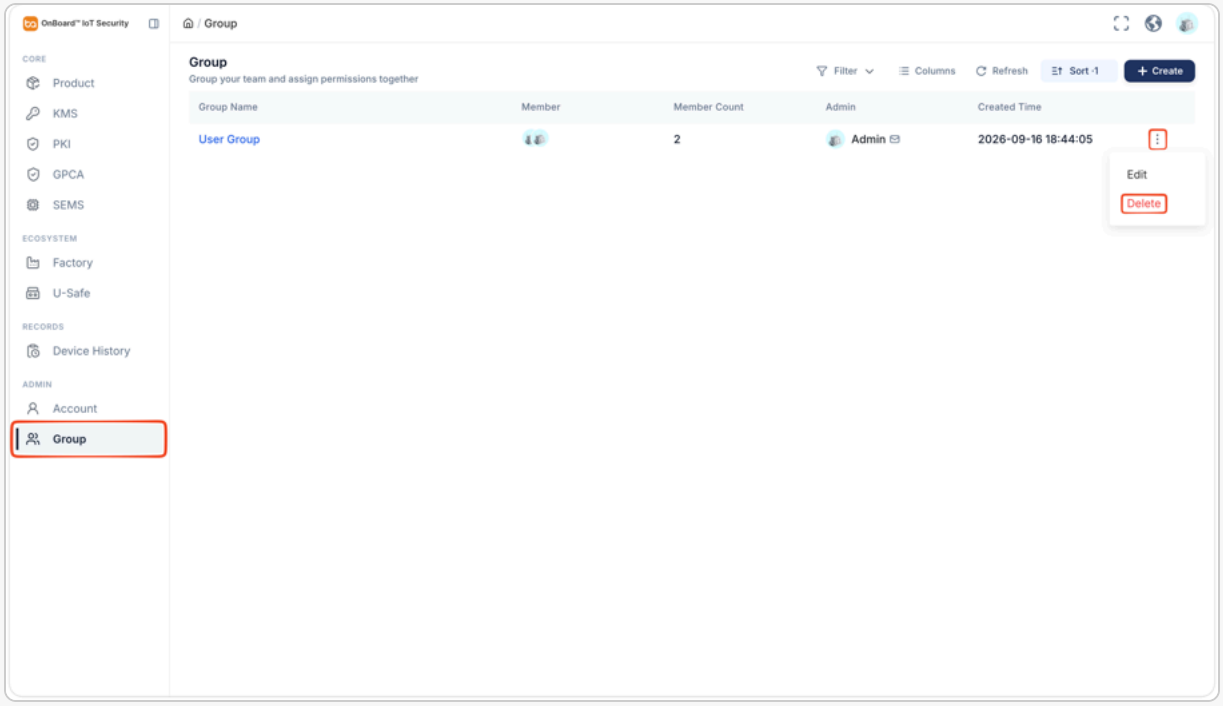
5. After verifying that the information is correct in the pop-up window, click **Confirm** to remove the user group member.



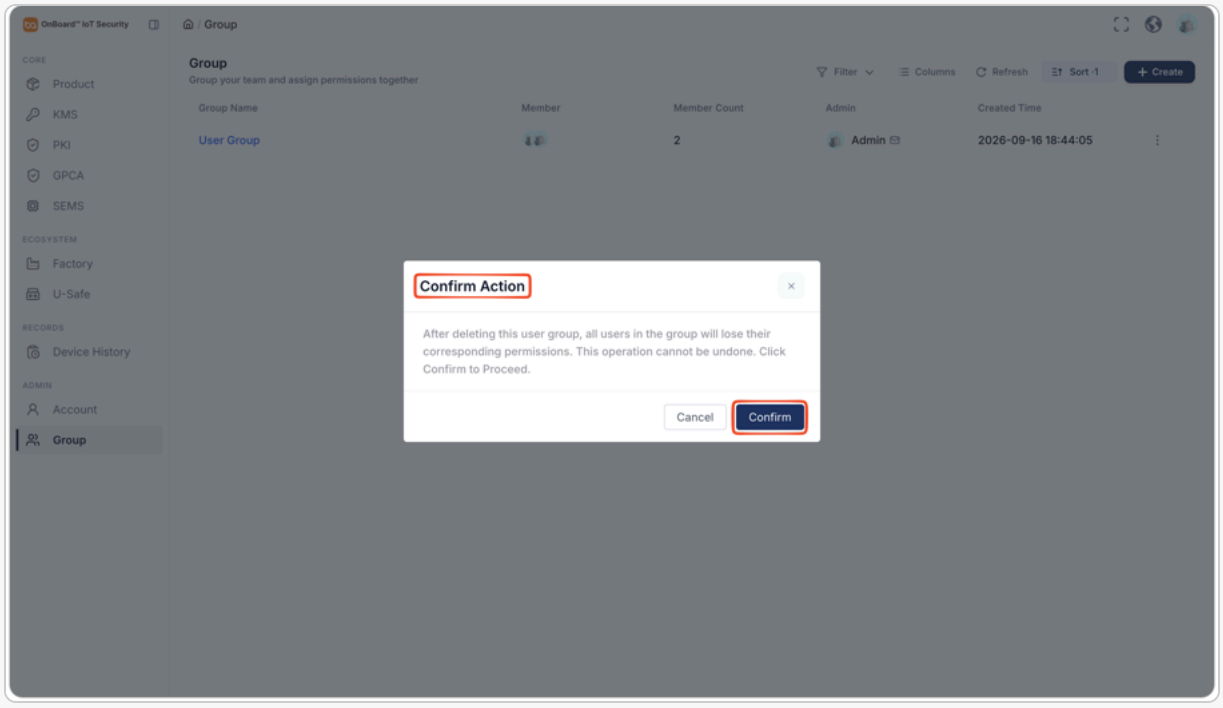
Delete a user group

> **WARNING**
>
> Deleted user groups cannot be recovered. Please proceed with caution.

1. Sign in to OBIS.
2. In the **Admin** section of the left menu, click **Group** to navigate to the **Group** page.
3. On the **Group** page, click the Options ⋮ icon for the corresponding user group and select **Delete**.



4. In the **Confirm Action** window, click **Confirm** to delete the user group.



Version: v3.4.0 (Latest)

Overview of OnBoard Edge Service

> **INFO**
>
> Operations in OnBoard Edge Service are applicable only to local factories, while operations for cloud factories can be performed directly in OnBoard™ IoT Security (OBIS). Please contact Snowball for assistance with the deployment.

OnBoard Edge Service manages Production Batches at the factory level, enforces authorization constraints locally, and enables intranet-connected Programming Stations to perform production execution. It provides an intranet-accessible web portal through which factory managers can monitor production status and perform administrative operations. OnBoard Edge Service provides the following core capabilities:

Production Batch Management

It supports concurrent Production Batch operations from one or more OEMs. Factory managers monitor batch status, allocate batches to Programming Stations, and manage batch lifecycle through the web portal.

Programming Station Management

Factory managers can manage Programming Stations through the web portal, including:

- Create and configure Programming Stations, including secure authentication method for connections to OnBoard Edge Service (Identity U-Safe, password, or no password)
- Allocate batches to Programming Stations from OnBoard Edge Service (alternatively, operators can specify a Batch ID or Production Order ID directly from Programming Station Software)
- Deliver the associated Programming Station Software package to Programming Stations

Production Device Record Management

OnBoard Edge Service generates per-device production records from Programming Stations and submits them to the OBIS cloud platform. It can also interoperate with existing factory systems—such as MES and factory testing systems—to exchange production records. OnBoard Edge Service does not have access to product key materials at any point. All cryptographic key material processing occurs exclusively within the EdgeHSM hardware boundary.

Version: v3.4.0 (Latest)

How to sign in to OnBoard Edge Service

> **INFO**
>
> Operations in OnBoard Edge Service are applicable only to local factories, while operations for cloud factories can be performed directly in OnBoard™ IoT Security (OBIS).

This article will guide you on how to sign in to OnBoard Edge Service using either the "Email + Password" or "Email + Verification code" method.

Prerequisites

Before getting started, please ensure that:

- The factory has been created and configured. For detailed instructions, refer to the steps for creating a factory, configuring a factory, and configuring a programming station.
- You have factory role permissions as a Factory Manager.
- Have contacted Snowball for assistance in deploying of OnBoard Edge Service.
- You have obtained the HSM U-Safe for identity authentication from Snowball, and inserted the corresponding HSM U-Safe (added during factory configuration) into the local factory server.
- Your sign-in device is within the factory service intranet environment.

> **TIP**
>
> The factory server requires at least 1 HSM U-Safe. Inserting multiple HSM U-Safes can improve server performance, and the quantity can be purchased according to the needs of the production line.

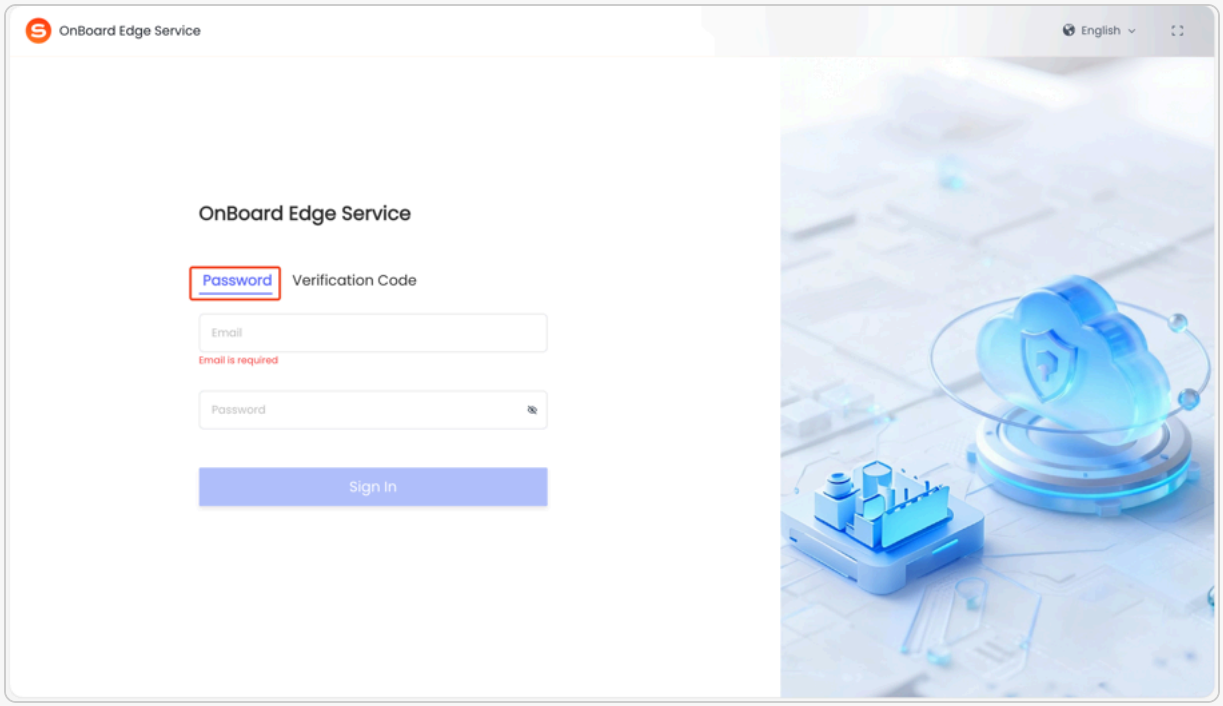
Method one: Password

> **INFO**
>
> - When the Internet is disconnected, OnBoard Edge Service only supports identity verification using the "Email + Password" method.
> - After a Factory Manager is added, the system automatically generates an initial password and sends it to the corresponding email address. Currently, this randomly generated password can be reset, but custom modification is not yet supported.

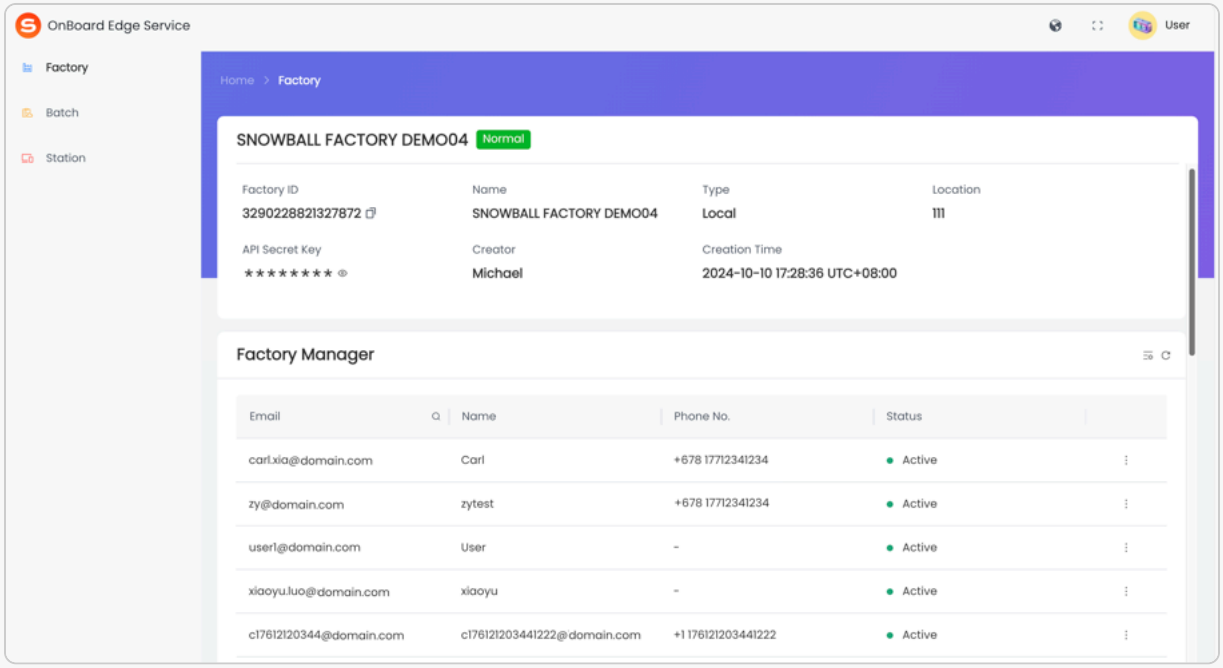
1. Enter the following address in the browser address bar: **http://<Service Address>:32334/login**.

   > **TIP**
   >
   > Replace **<Service Address>** with the actual service IP. For more information, refer to how to check service address.

2. On the OnBoard Edge Service sign-in page, select **Password**, enter your email and password, and then click **Sign In**.



3. After a successful sign-in, the page will navigate to the home page of OnBoard Edge Service.

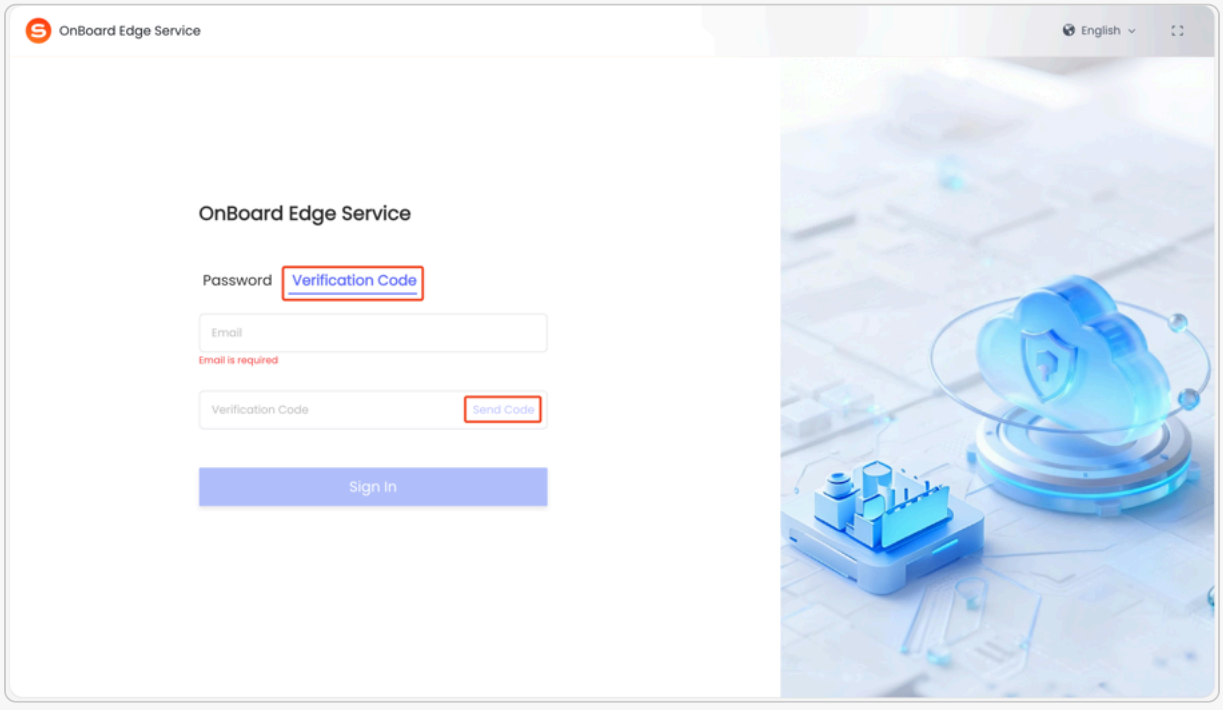


Method two: Verification code

1. Enter the following address in the browser address bar: **http://<Service Address>:32334/login**.

   > **TIP**
   >
   > Replace **<Service Address>** with the actual service IP. For more information, refer to how to check service address.

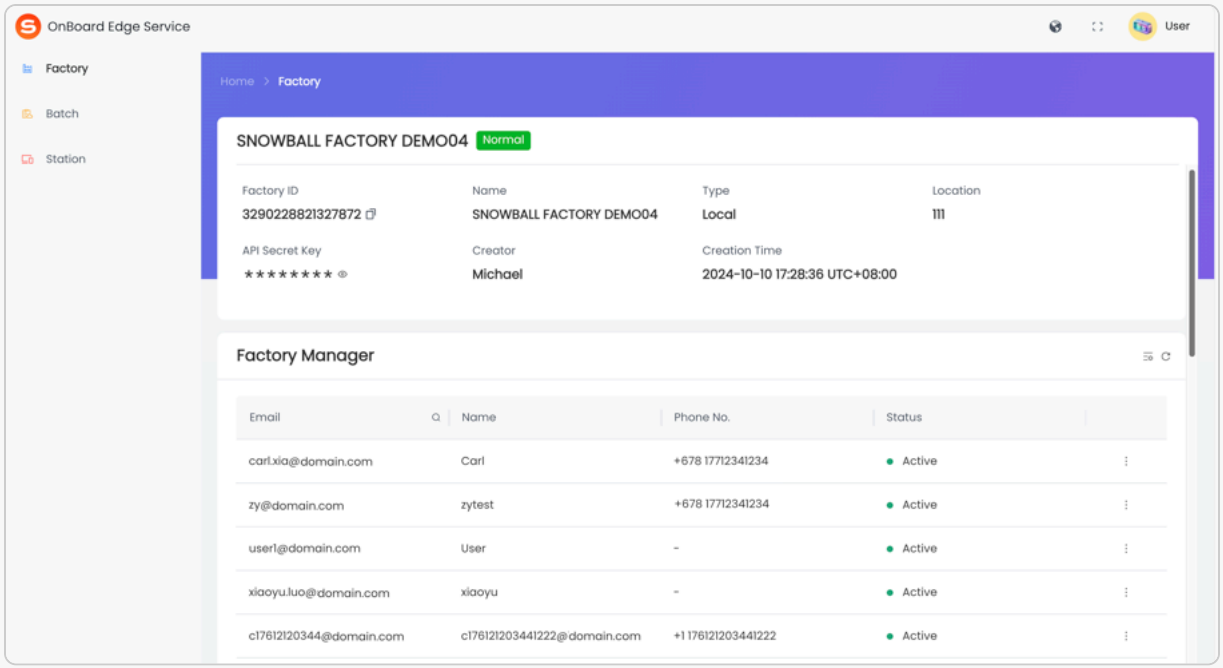
2. On the OnBoard Edge Service sign-in page, select **Verification Code**, enter your email, and then click **Send Code**.



3. Sign in to your email, check the verification email from OBIS which contains a six-digit verification code.

4. On the OBIS sign-in page, enter the six-digit verification code you received in your email, and then click **Sign In**.

5. After a successful sign-in, the page will navigate to the home page of OnBoard Edge Service.



Version: v3.4.0 (Latest)

How to manage factories in OnBoard Edge Service

> **INFO**
>
> Operations in OnBoard Edge Service are applicable only to local factories, while operations for cloud factories can be performed directly in OnBoard™ IoT Security (OBIS).

This article will guide you through the following operations in OnBoard Edge Service:

- Reset the Factory Manager password
- Delete a Factory Manager
- Lock or unlock an HSM U-Safe
- Lock or unlock an Identity U-Safe

Prerequisites

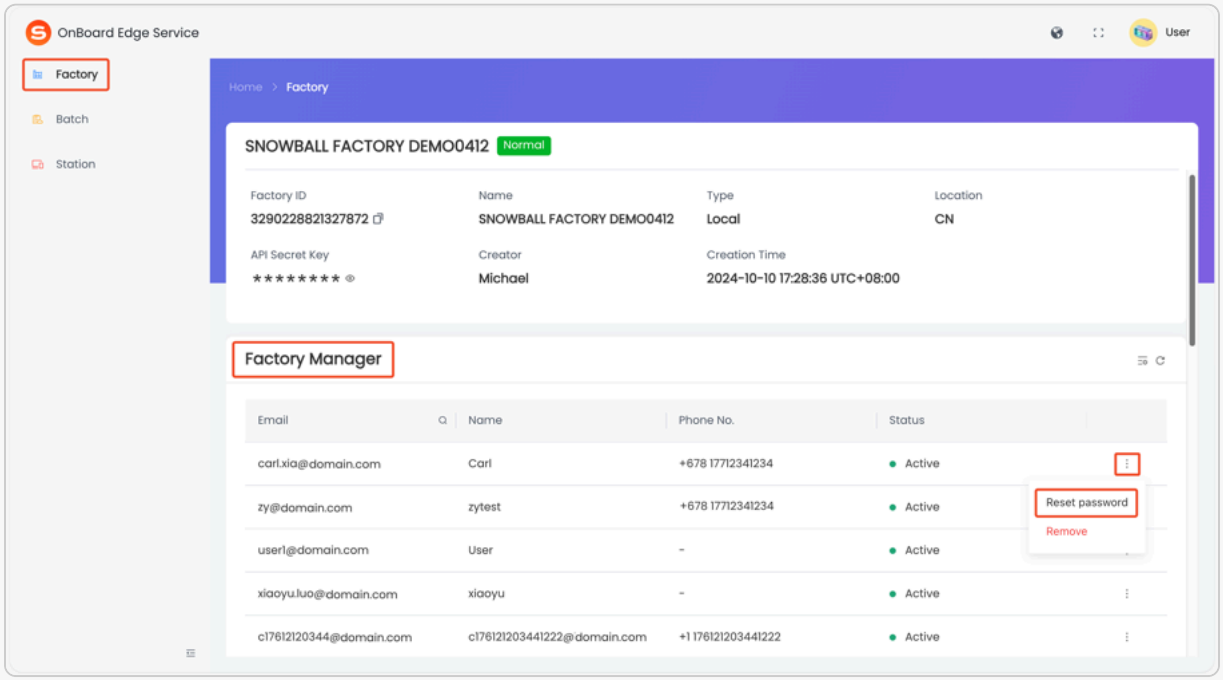
Before getting started, please ensure that you can sign in to OnBoard Edge Service.

Reset the Factory Manager password

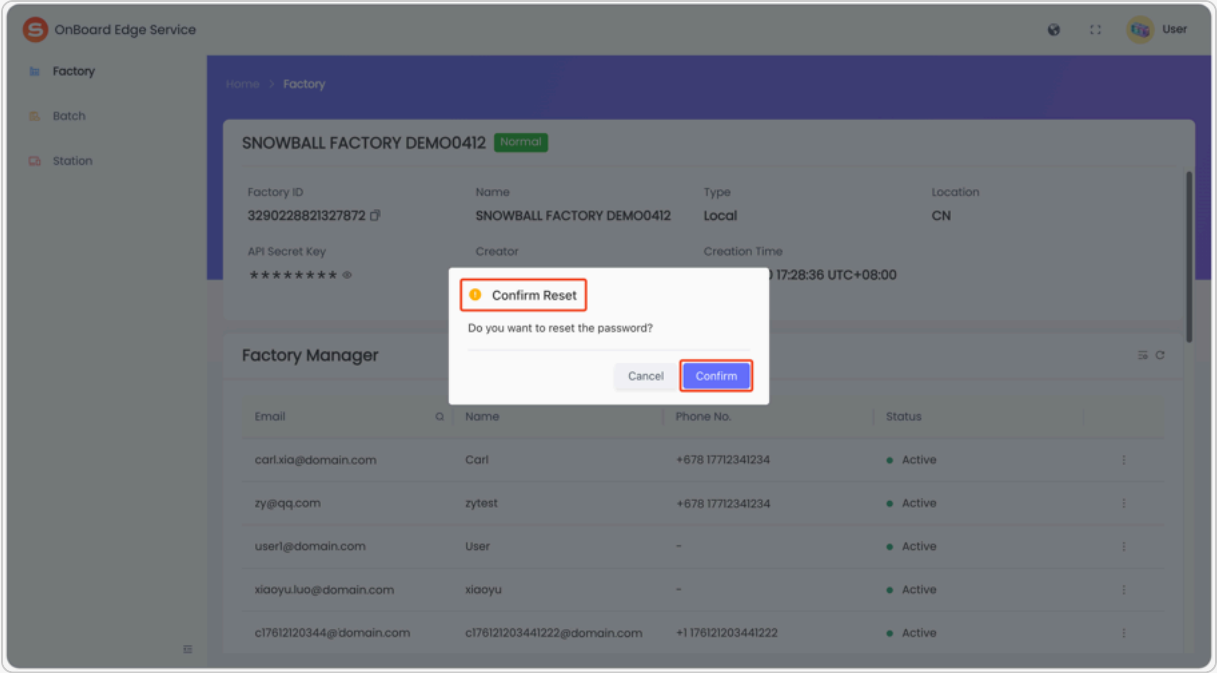
> **TIP**
>
> After the password is reset, the system automatically generates a random password and sends it to the corresponding email address.

1. Sign in to OnBoard Edge Service.

2. In the left menu, click **Factory**. Locate the **Factory Manager** section, and then click the Options ⋮ icon for the corresponding Factory Manager and select **Reset password**.



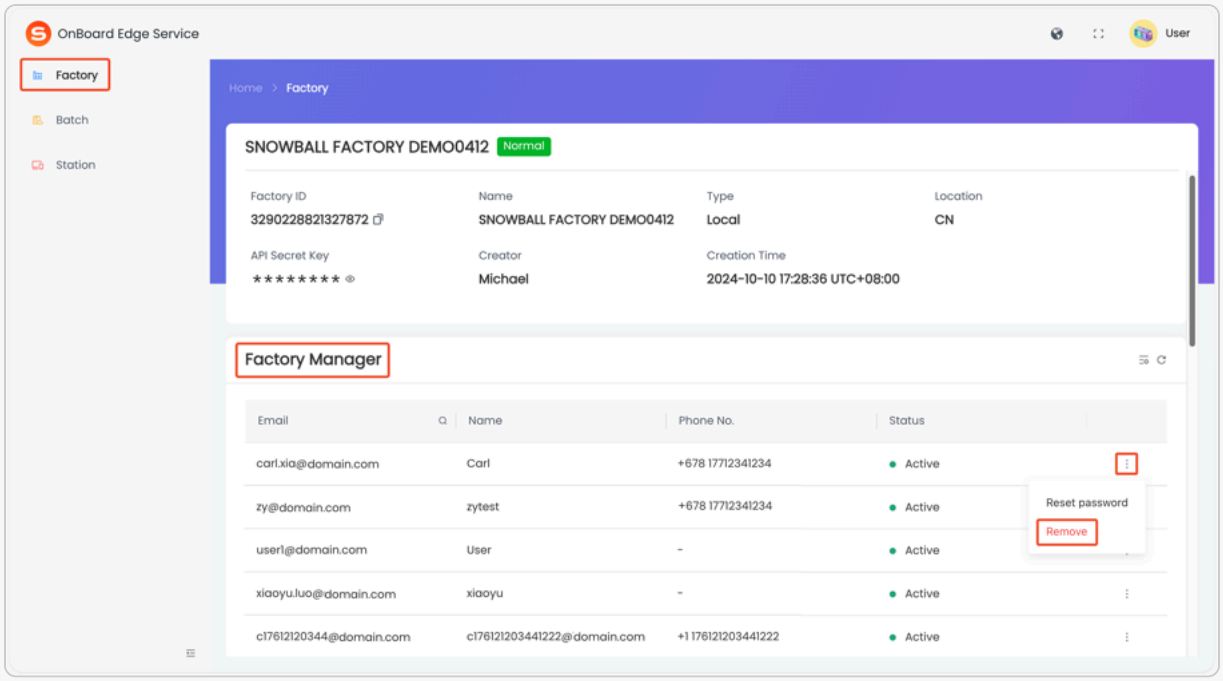
3. In the **Confirm Reset** window, click **Confirm** to reset the password.



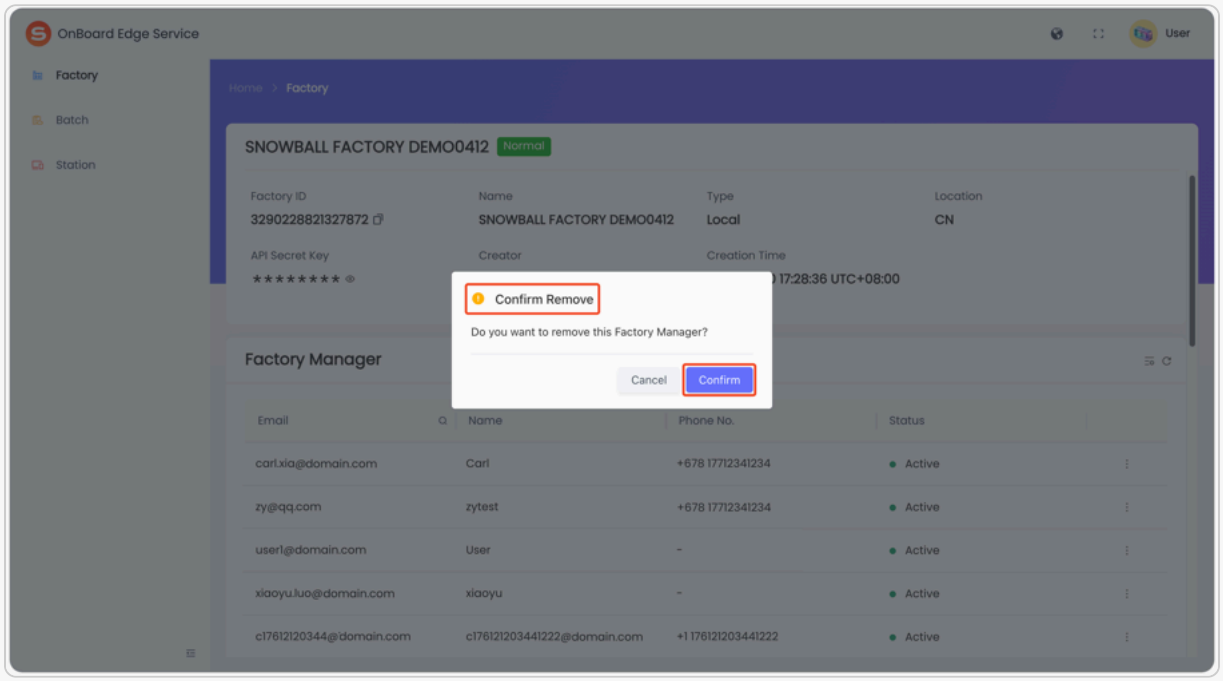
Delete a Factory Manager

1. Sign in to OnBoard Edge Service.

2. In the left menu, click **Factory**. Locate the **Factory Manager** section, and then click the Options ⋮ icon for the corresponding Factory Manager and select **Remove**.



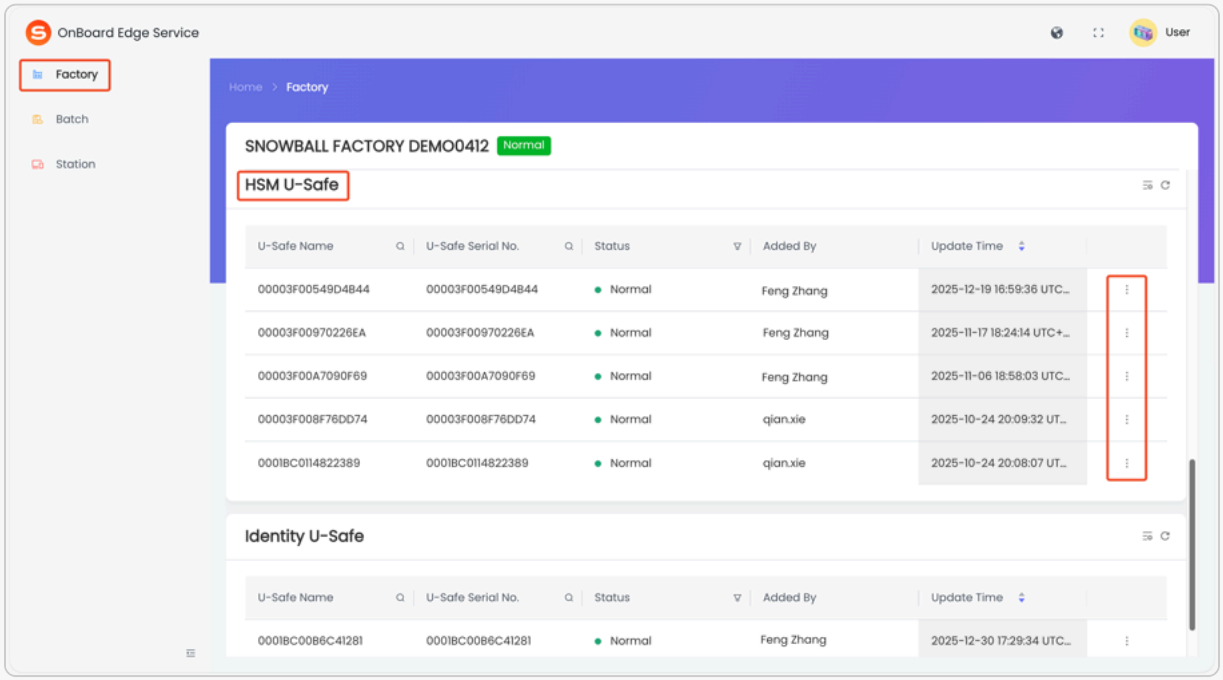
3. In the **Confirm Remove** window, click **Confirm** to delete the Factory Manager.



Lock or unlock an HSM U-Safe

> **TIP**
>
> Lock the HSM U-Safe to prevent its use and unbinding. Once locked, its status will change to **Locked**.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Factory**. Locate the **HSM U-Safe** section, and then click the Options ⋮ icon for the corresponding HSM U-Safe and select **Lock** or **Unlock**.

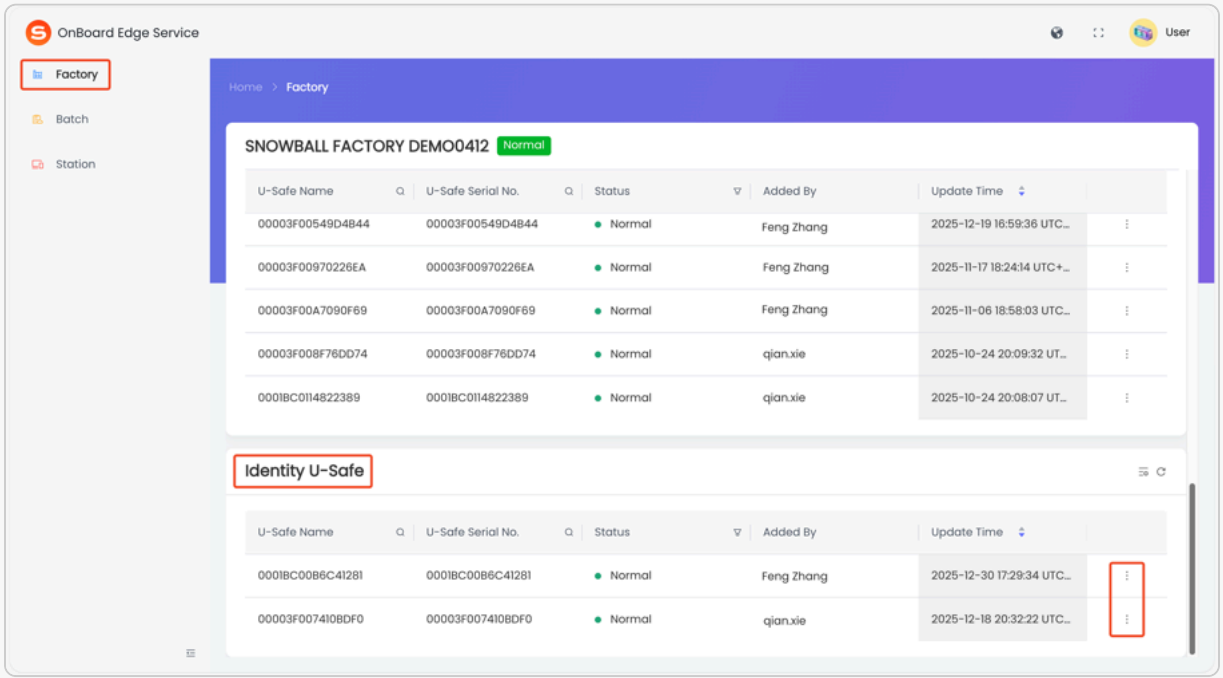


3. In the pop-up window, click **Confirm** to lock or unlock the HSM U-Safe.

Lock or unlock an Identity U-Safe

> **TIP**
>
> Lock the Identity U-Safe to prevent its use and unbinding. Once locked, its status will change to **Locked**.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Factory**. Locate the **Identity U-Safe** section, and then click the Options ⋮ icon for the corresponding Identity U-Safe and select **Lock** or **Unlock**.



3. In the pop-up window, click **Confirm** to lock or unlock the Identity U-Safe.

Version: v3.4.0 (Latest)

How to manage a batch and assign a programming station in OnBoard Edge Service

> **INFO**
>
> Operations in OnBoard Edge Service are applicable only to local factories, while operations for cloud factories can be performed directly in OnBoard™ IoT Security (OBIS).

This article will guide you through the following operations in OnBoard Edge Service:

- Check batches
- Assign a programming station to a batch
- Unassign a programming station from a batch
- Turn off or delete a batch

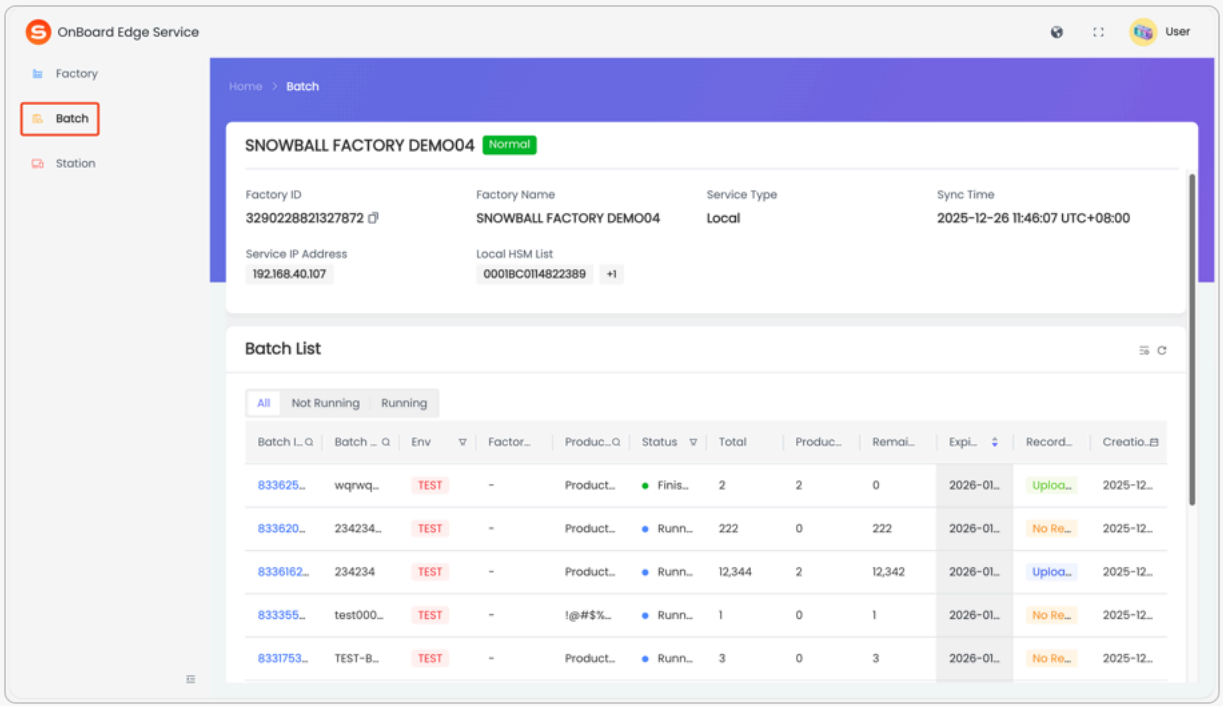
Prerequisites

Before getting started, please ensure that you can sign in to OnBoard Edge Service.

Check batches

1. Sign in to OnBoard Edge Service.

2. In the left menu, click **Batch** to navigate to the **Batch** page.

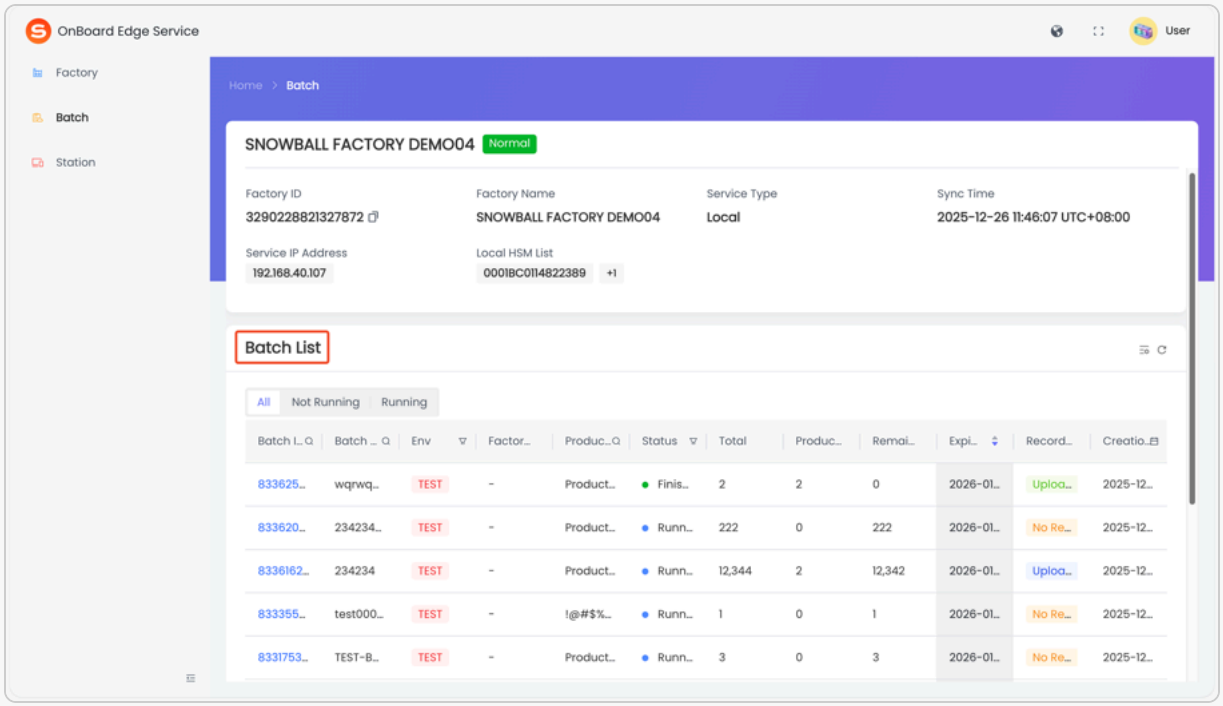


Description of batch status:

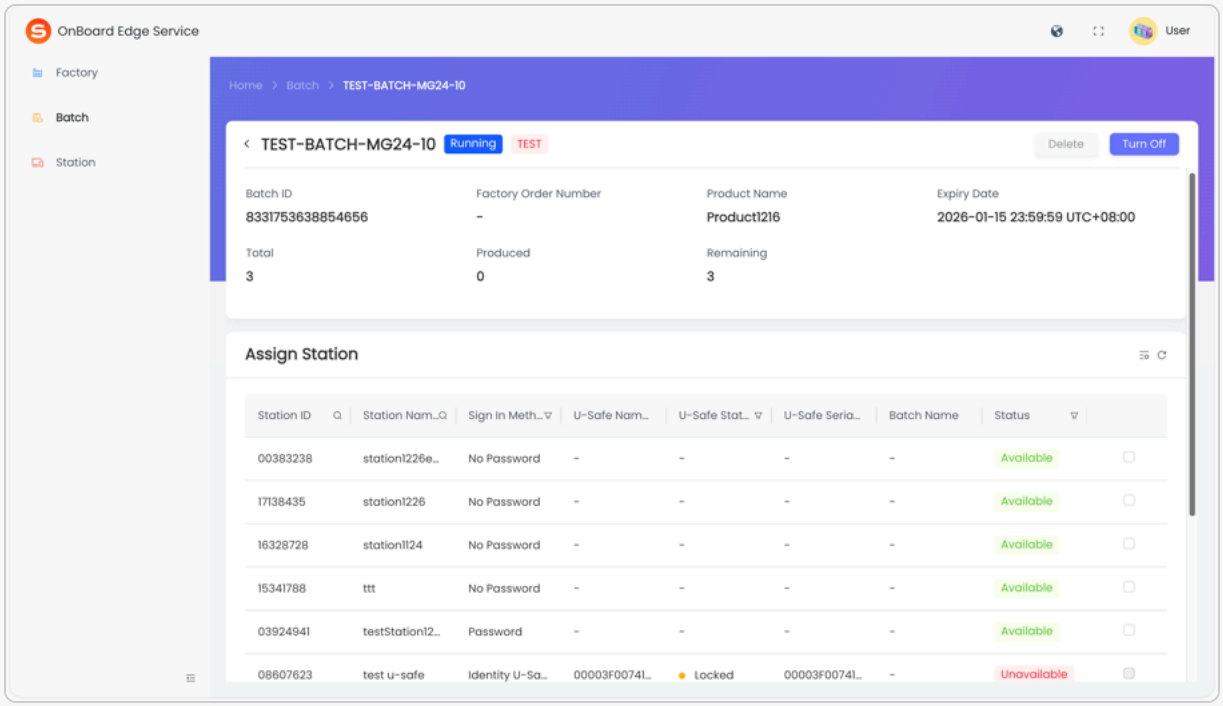
Status	Can be turned on	Description
Running	-	The default state after creating a batch. You can bind it to a programming station.

Status	Can be turned on	Description
Stopped	Yes	The batch is currently turned off. You can turn it on to bind it to a programming station.
Finished	No	The status after batch programming is completed.
Expired	No	The batch has expired before the programming was completed. **Note**: After a batch expires, most functions related to that batch in OnBoard Edge Service will no longer operate normally, including programming in the Programming Station client. It is recommended to delete the expired batches.

1. On the **Batch** page, locate the **Batch List** section, and then select the corresponding batch to navigate to the batch page.



2. On the batch page, you can check the batch-related information.

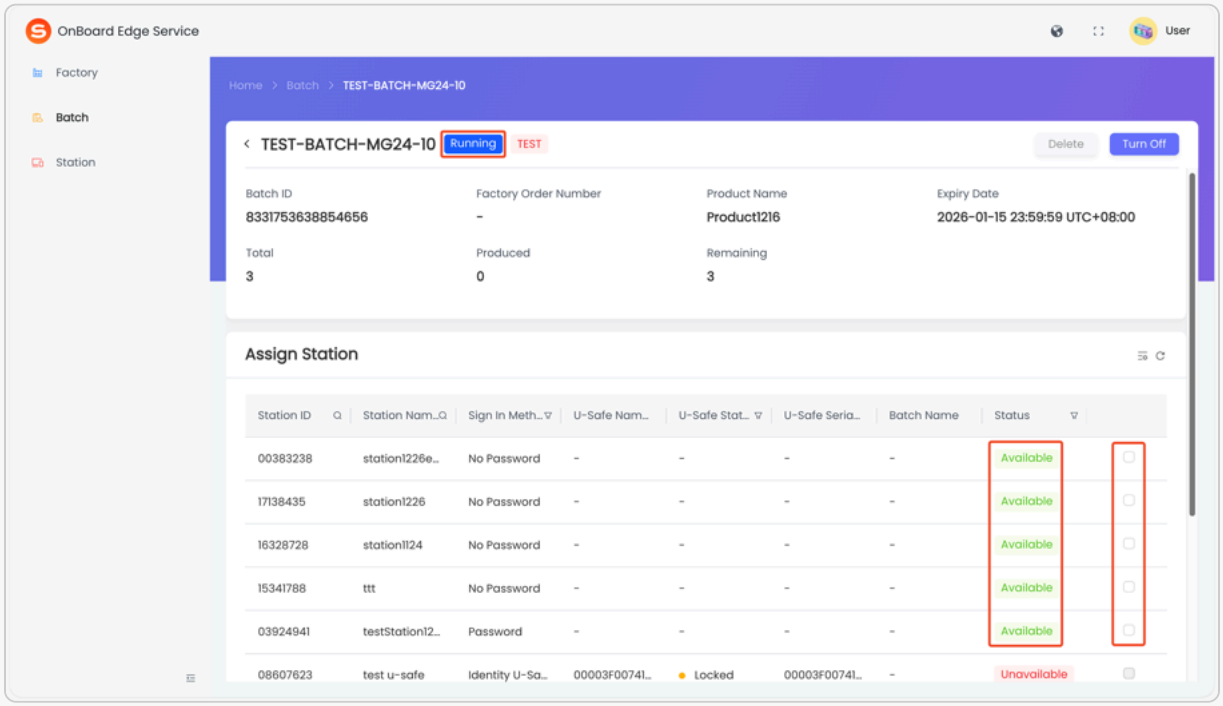


Assign a programming station to a batch

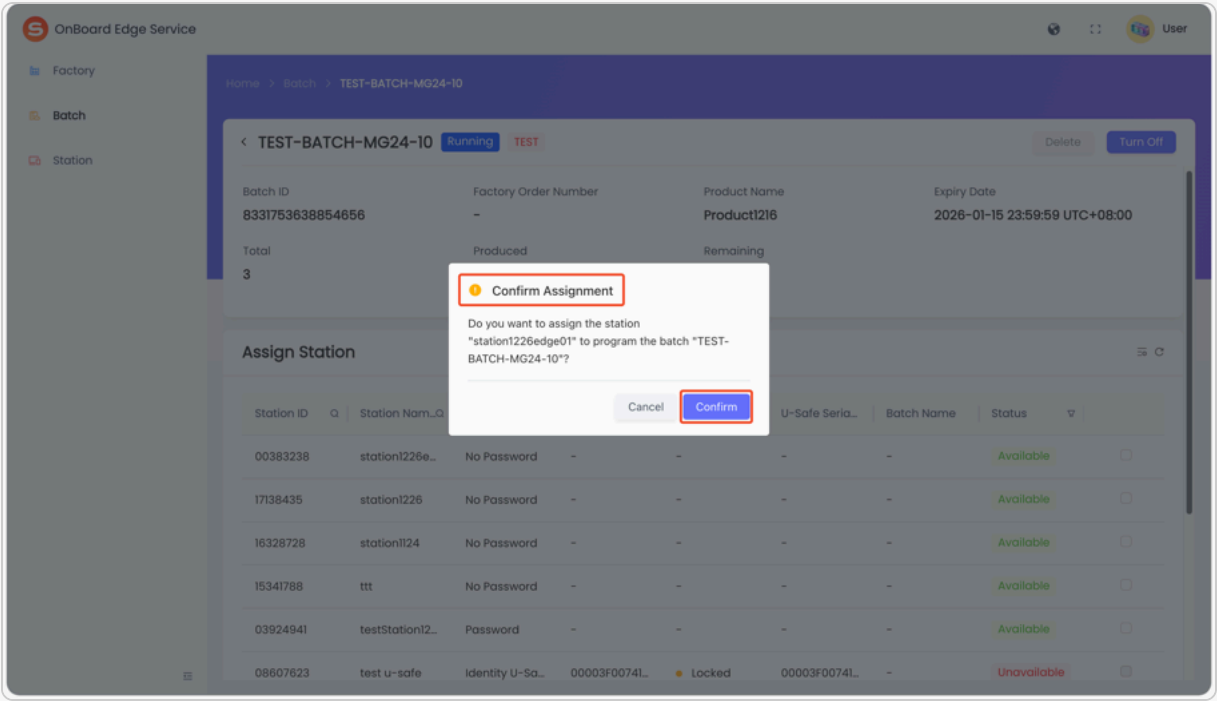
> **TIP**
>
> A batch can be assigned to multiple programming stations, while a programming station can only program one batch at the same time.

Assign a programming station with the **Available** status to a batch for programming:

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Batch**, and then select the corresponding batch to navigate to the batch page.
3. On the batch page, confirm that the batch status is **Running**, and then select the programming station with the **Available** status for assignment.



4. In the **Confirm Assignment** window, click **Confirm** to complete the assignment of the programming station. After the assignment, the programming station status will change to **Busy**.



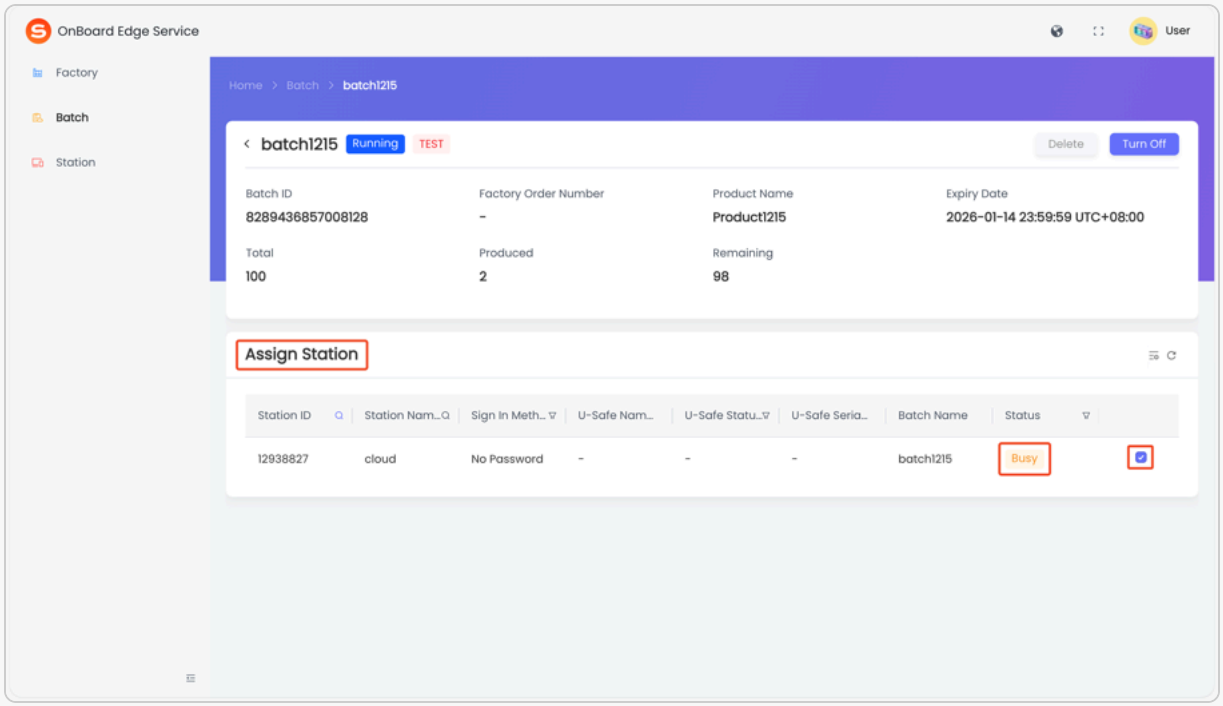
Unassign a programming station from a batch

> **WARNING**
>
> After unassignment, the corresponding programming station can no longer be used for programming this batch.

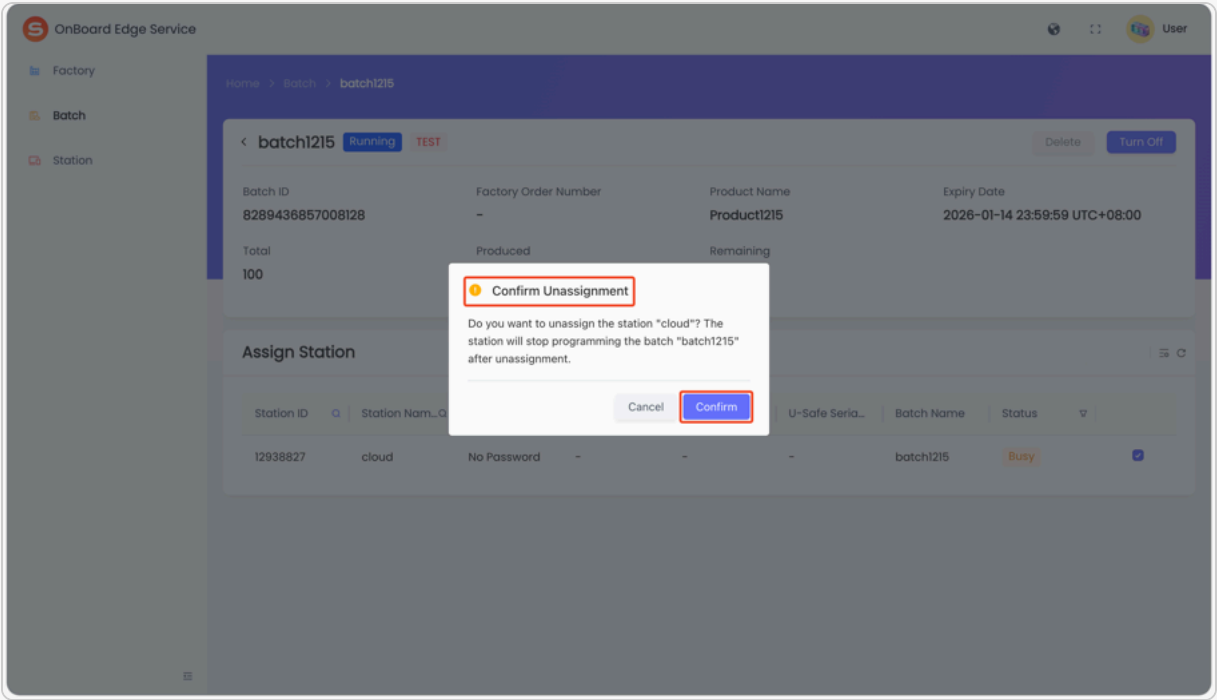
1. Sign in to OnBoard Edge Service.

2. In the left menu, click **Batch**, and then select the corresponding batch to navigate to the batch page.

3. In the **Assign Station** section of the batch page, find the corresponding batch and uncheck the programming station with the **Busy** status.



4. In the **Confirm Unassignment** window, click **Confirm** to complete the unassignment of the programming station. After unassignment, the programming station status will change to **Available**.

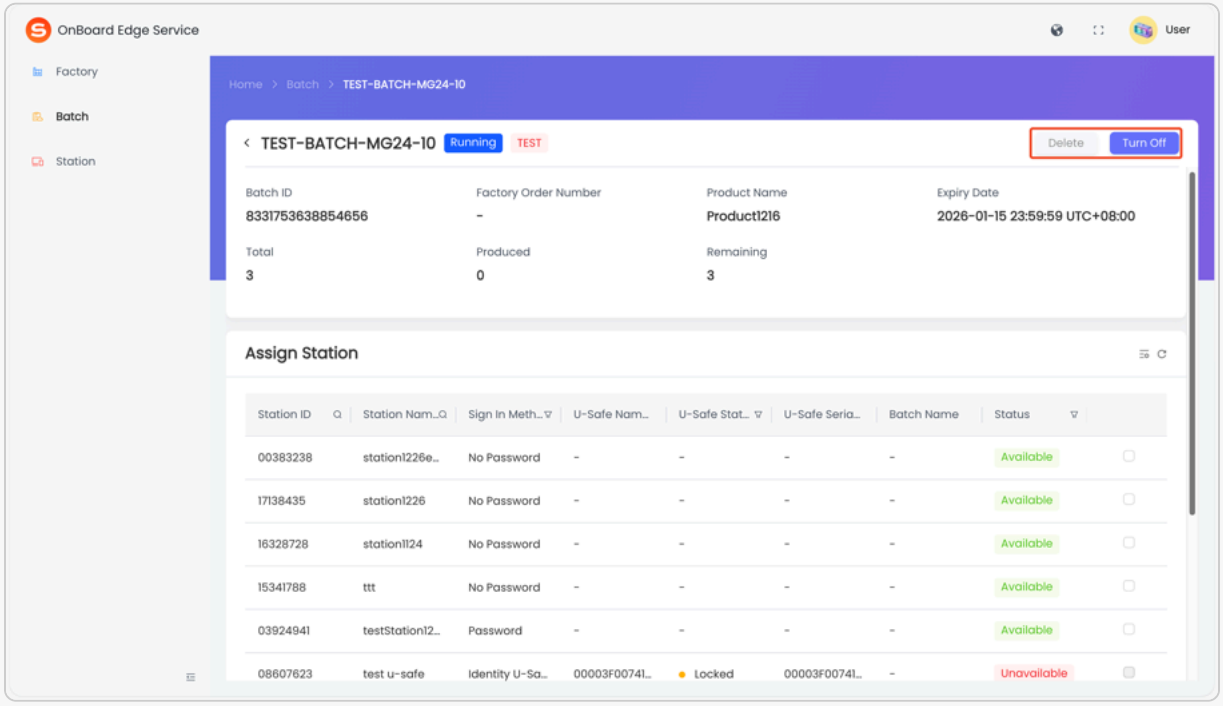


Turn off or delete a batch

> **INFO**
>
> After a batch is deleted, any programming stations assigned to that batch will be automatically unassigned.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Batch**, and then select the corresponding batch to navigate to the batch page.
3. On the batch page, click **Turn Off** or **Delete**.

> **TIP**
>
> If the **Delete** button appears grayed out, it is currently unavailable. Please click **Turn Off** to turn off the batch. Once the batch is in a non-running status, it can be deleted.



Version: v3.4.0 (Latest)

How to configure and manage programming stations in OnBoard Edge Service

> **INFO**
>
> Operations in OnBoard Edge Service are applicable only to local factories, while operations for cloud factories can be performed directly in OnBoard™ IoT Security (OBIS).

> **TIP**
>
> You can configure and manage the programming station in OnBoard Edge Service or OBIS as needed.

This article will guide you through the following operations in OnBoard Edge Service:

- Create a programming station
- Bind an Identity U-Safe to a programming station
- Unbind an Identity U-Safe from a programming station
- Delete a programming station
- Check the programming station information
- Check the programming station password

Prerequisites

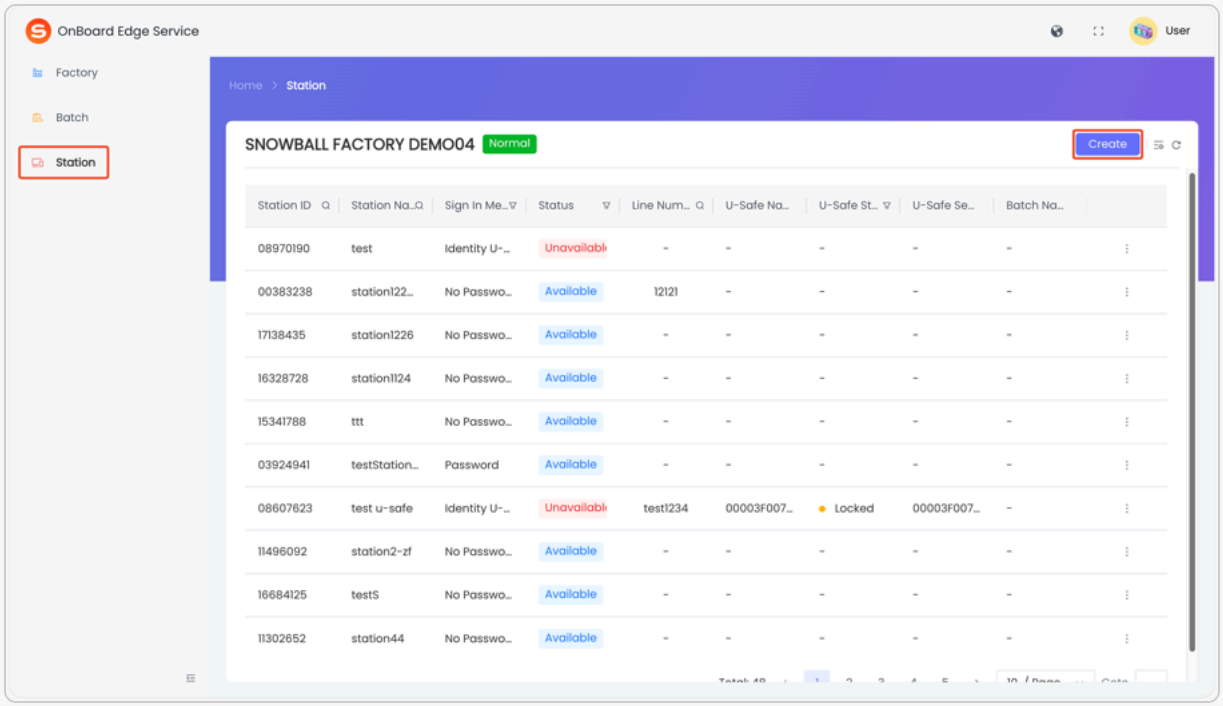
Before getting started, please ensure that:

- You can sign in to OnBoard Edge Service.
- You have obtained the Identity U-Safe for identity authentication from Snowball.

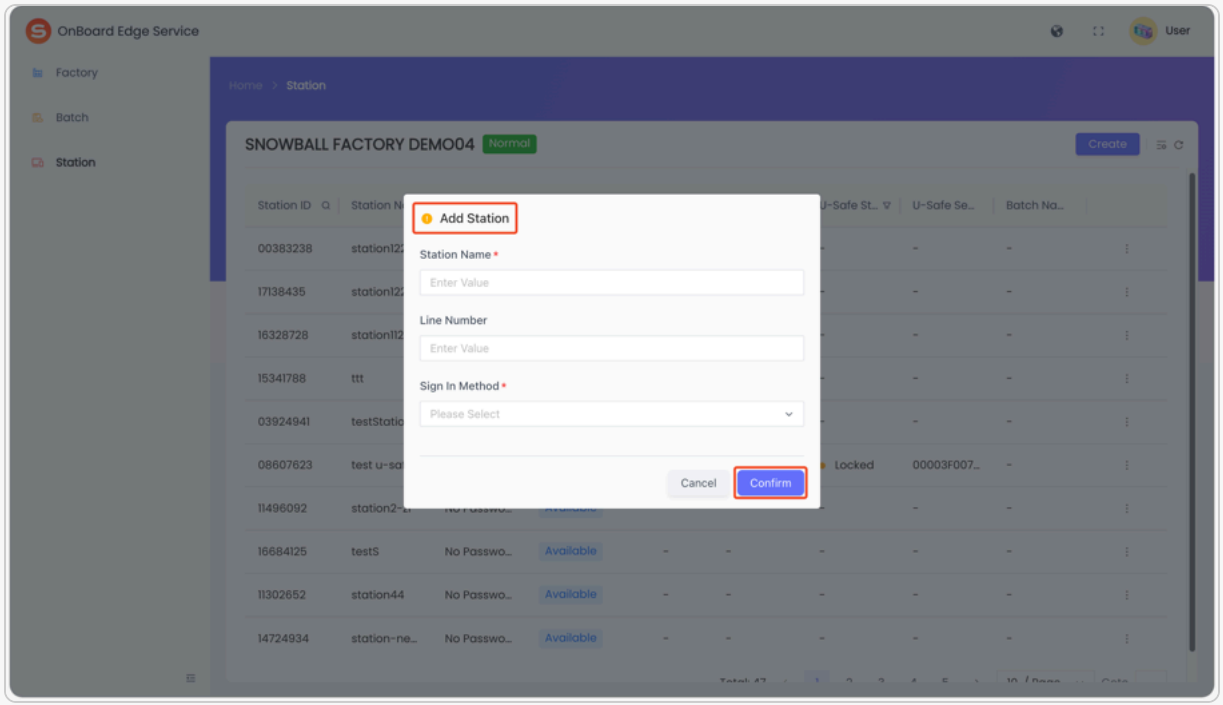
Create a programming station

> **TIP**
>
> After creating a programming station for the factory, you can assign specific programming stations to batches in OnBoard Edge Service as needed. Before programming a device, it is necessary to query and retrieve the corresponding batch information and programming data based on the programming station ID.
>
> Two programming methods are supported:
>
> - Using the Programming Station client
> - Using the OBIS Programming CLI

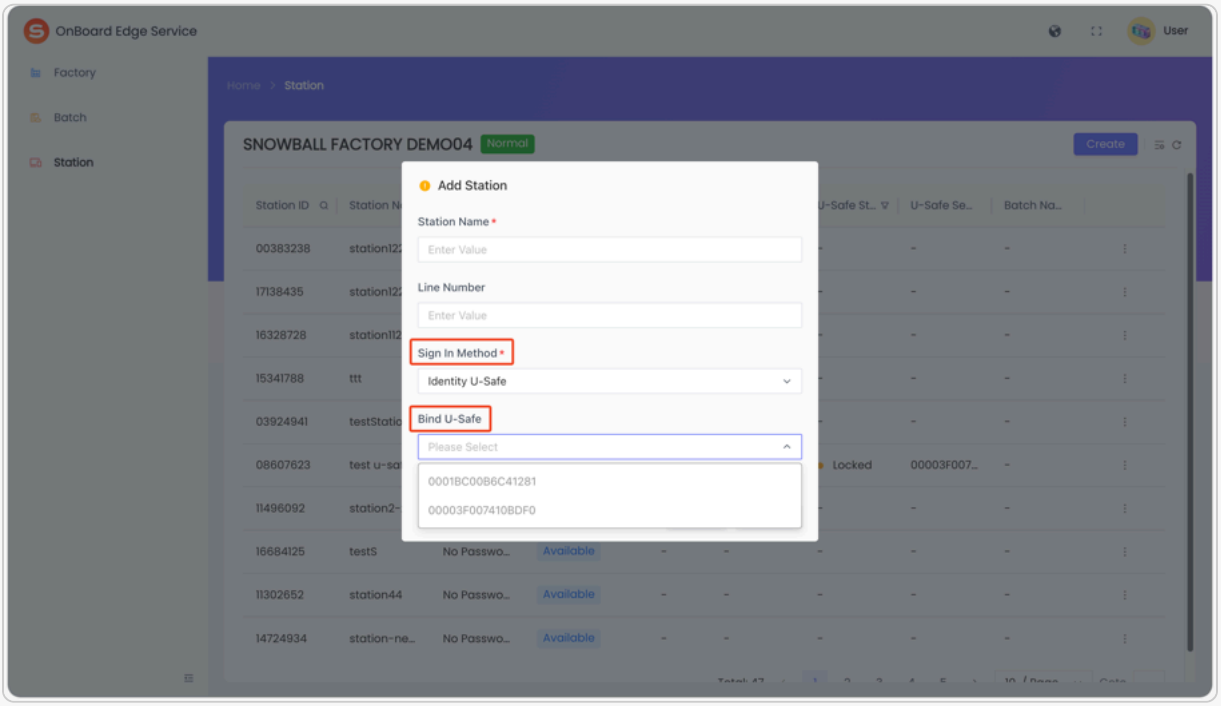
1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Station**, and then click **Create** on the station page.



3. In the **Add** window, enter the **Station Name** and **Line Number**, and then select the **Sign In Method**. The methods include: **No Password**, **Password**, or **Identity U-Safe**.



> **TIP**
>
> If the sign-in method is **Identity U-Safe**, you can select an already added Identity U-Safe from the **Bind U-Safe** drop-down list to bind it, or you can bind it after adding the programming station.

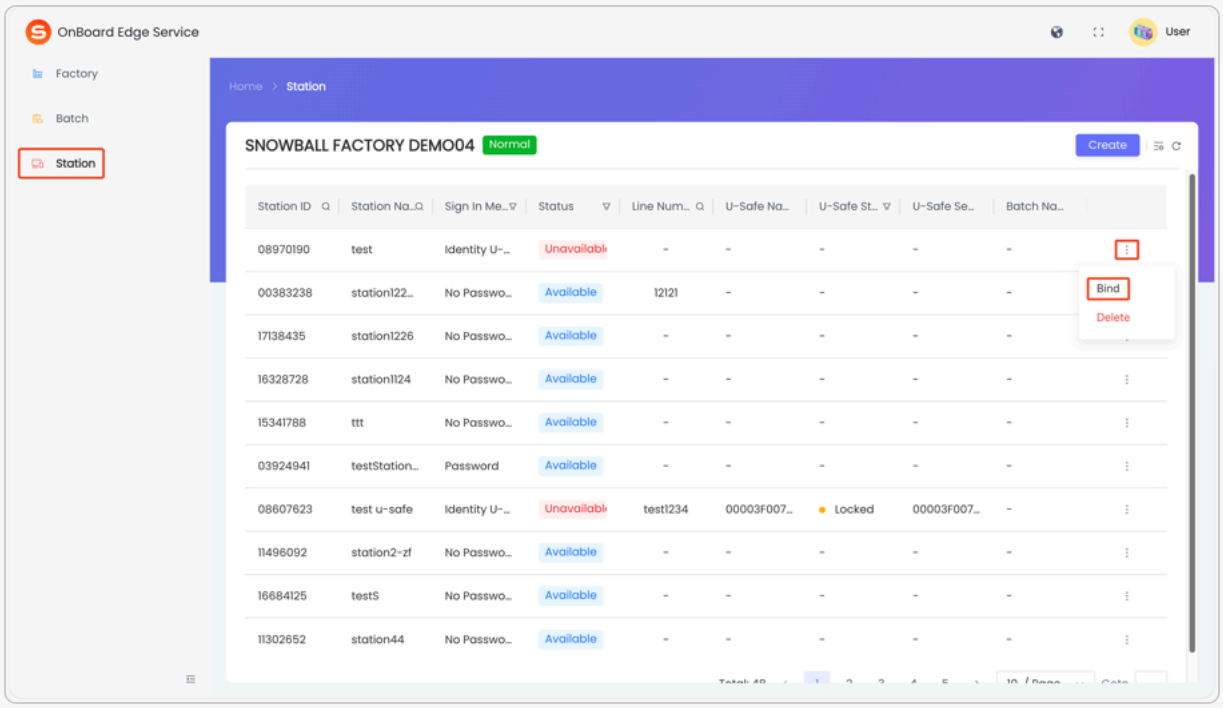


4. Click **Confirm** to create the programming station.

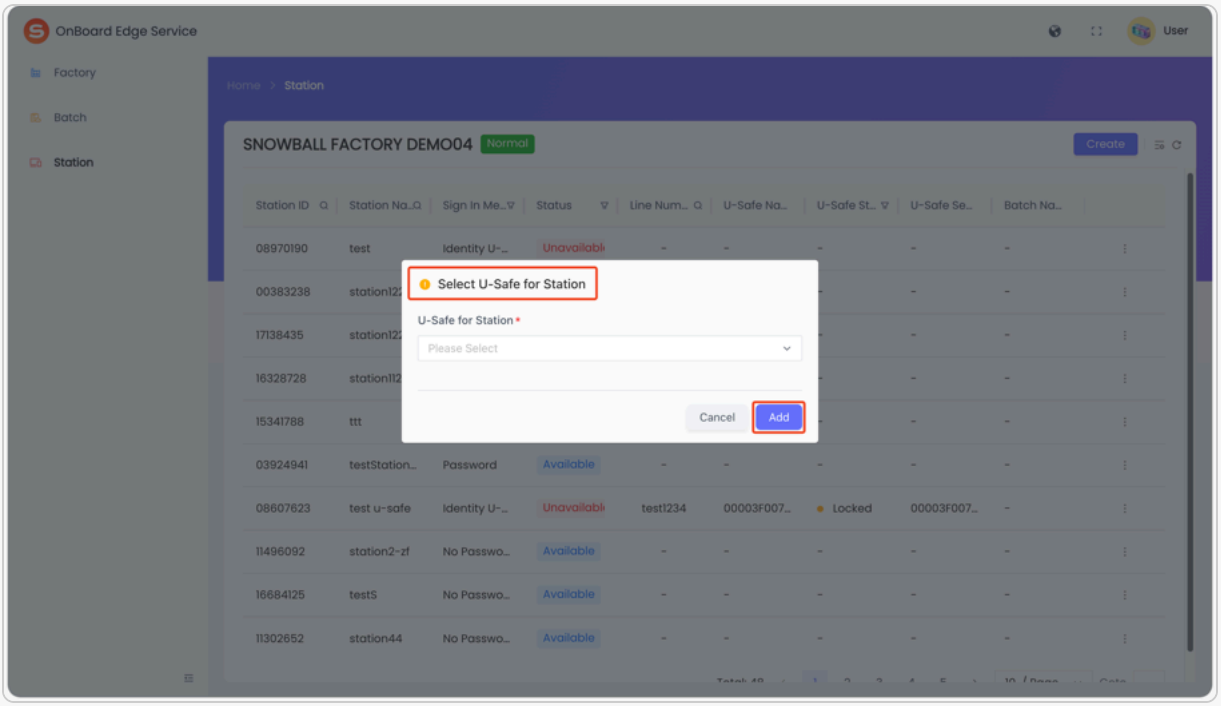
Bind an Identity U-Safe to a programming station

> **TIP**
>
> You can use the Identity U-Safe to sign in to the Programming Station client after binding.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Station**. On the station page, click the Options ⋮ icon for the corresponding programming station and select **Bind**.



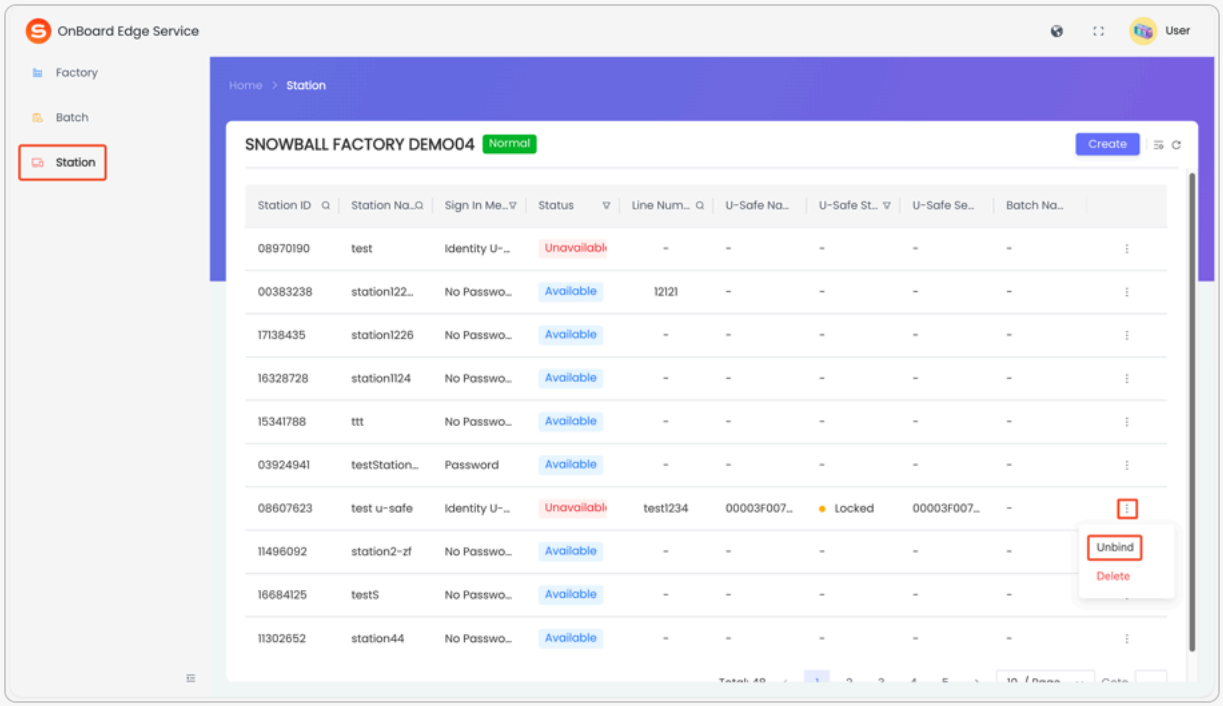
3. In the **Select U-Safe for Station** window, select the Identity U-Safe you want to bind and then click **Add** to bind it to the programming station.



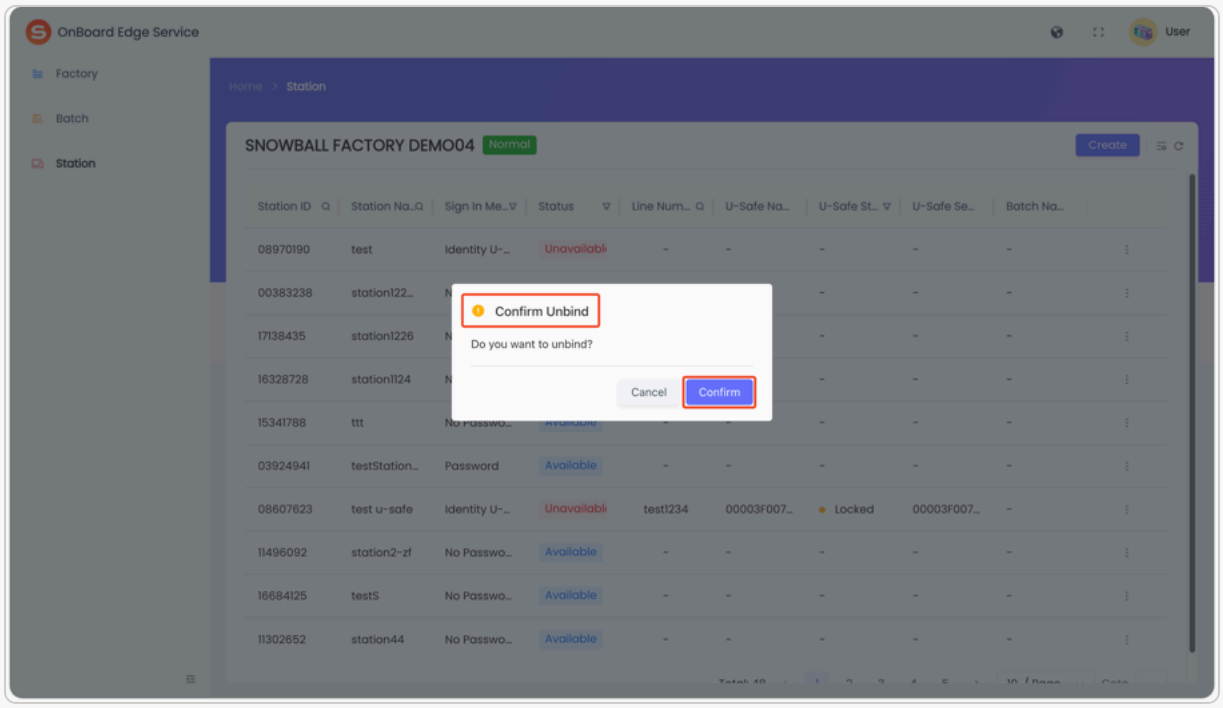
Unbind an Identity U-Safe from a programming station

> **WARNING**
>
> After unbinding, the Identity U-Safe can no longer be used to sign in to the Programming Station client.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Station**. On the station page, click the Options ⋮ icon for the corresponding programming station and click **Unbind**.



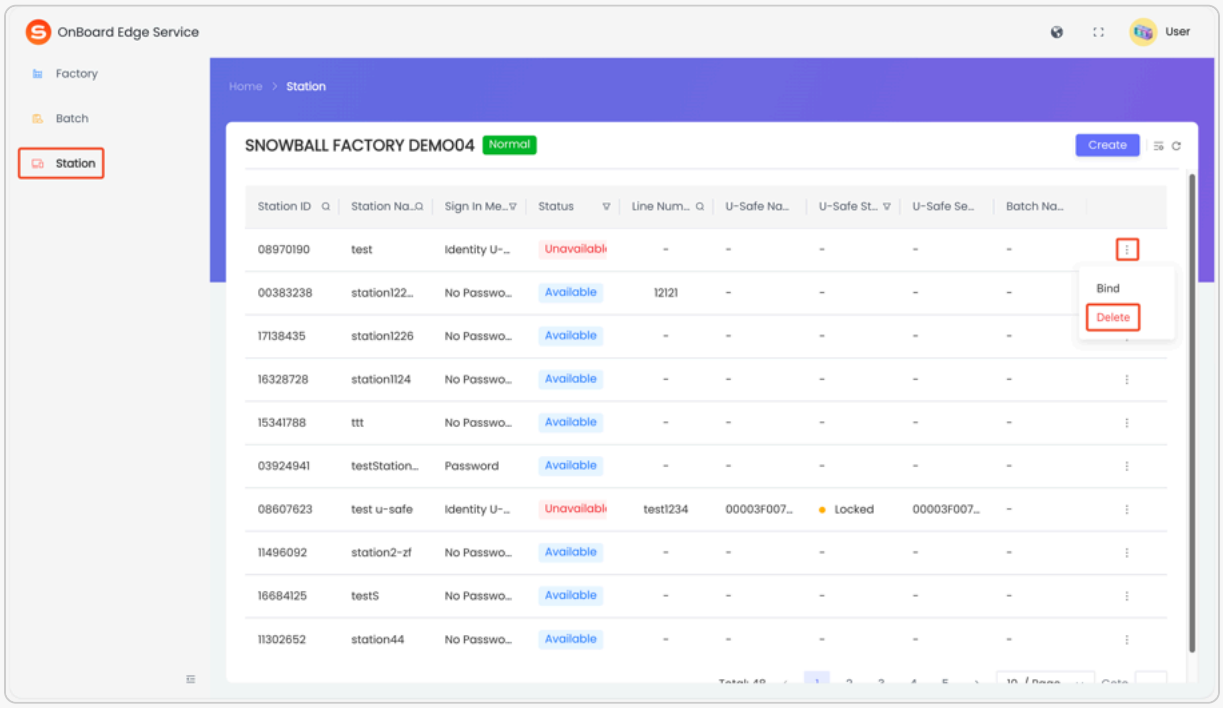
3. In the **Confirm Unbind** window, click **Confirm** to unbind the Identity U-Safe for the programming station.



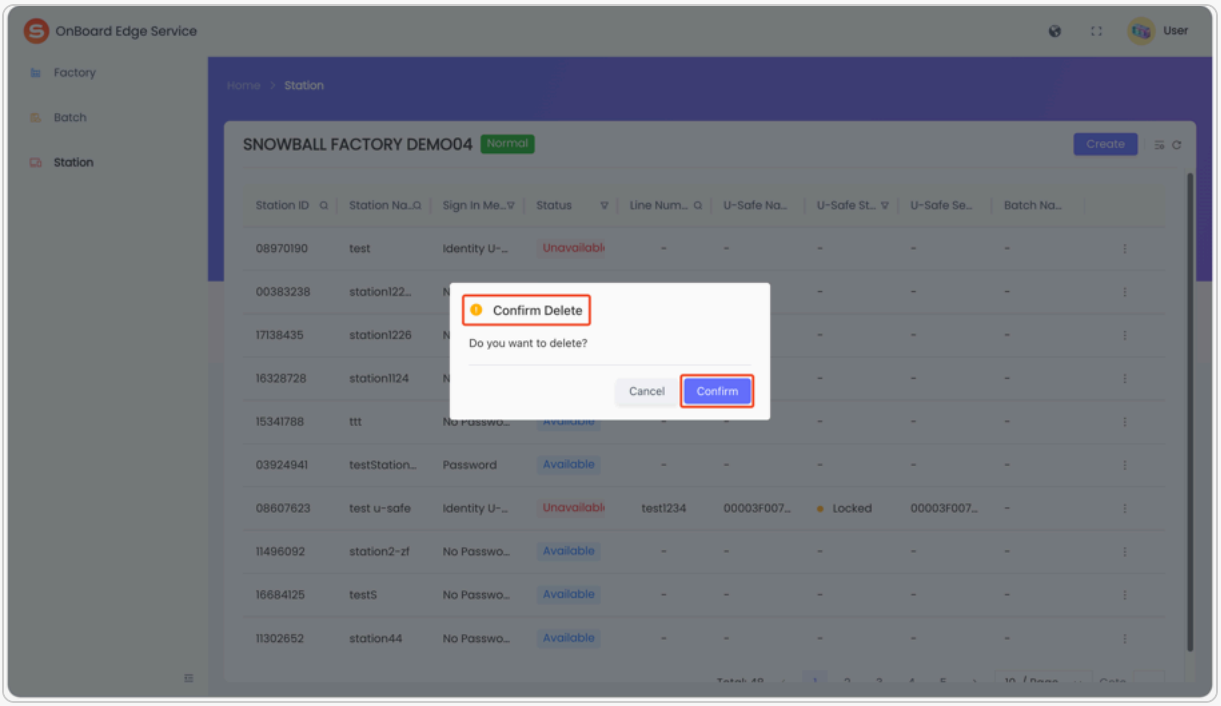
Delete a programming station

> **WARNING**
>
> Deleted programming stations cannot be recovered. Please proceed with caution.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Station**. On the station page, click the Options ⋮ icon for the corresponding programming station and select **Delete**.



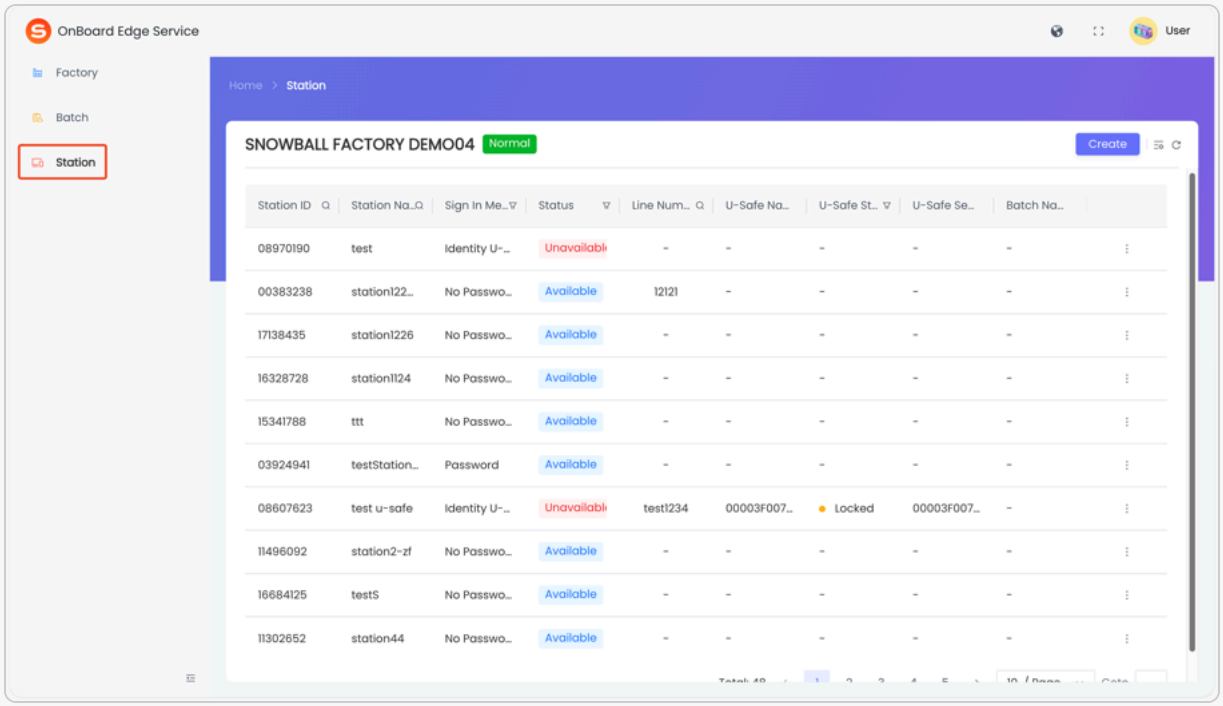
3. In the **Confirm Delete** window, click **Confirm** to delete the programming station.



Check the programming station information

1. Sign in to OnBoard Edge Service.

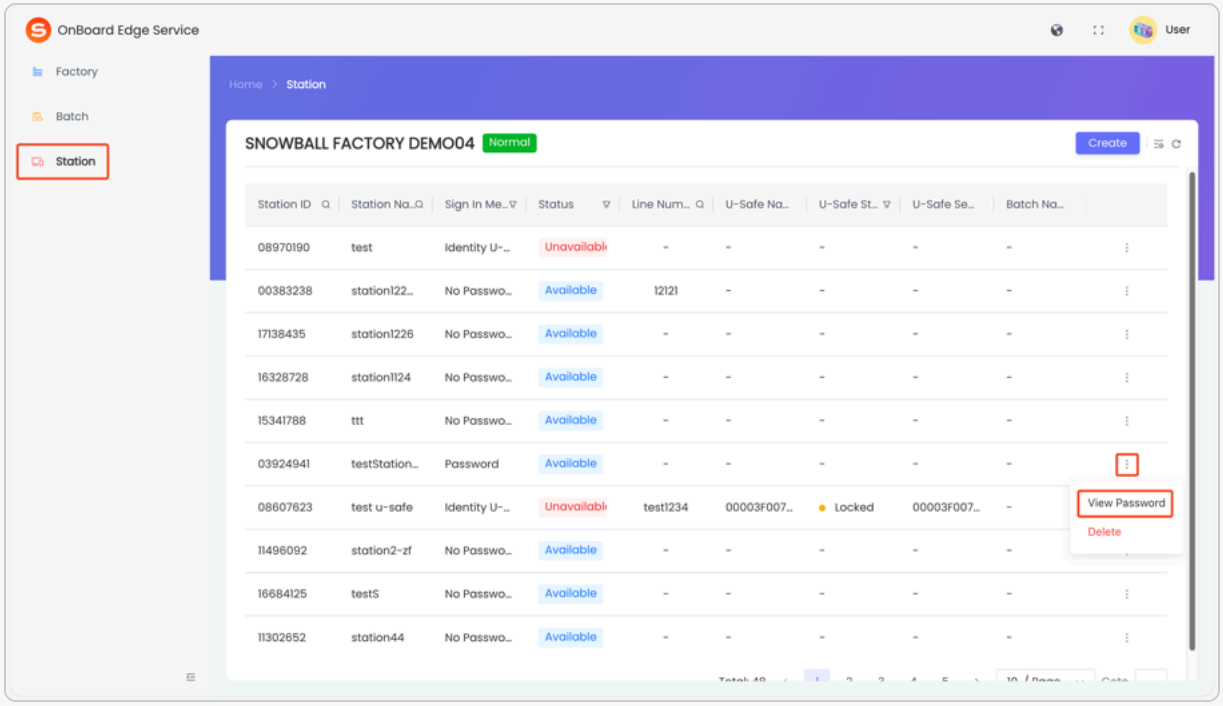
2. In the left menu, click **Station**. On the station page, you can check the programming station information (such as **Station ID**, **Station Name**, and **Sign In Method**).



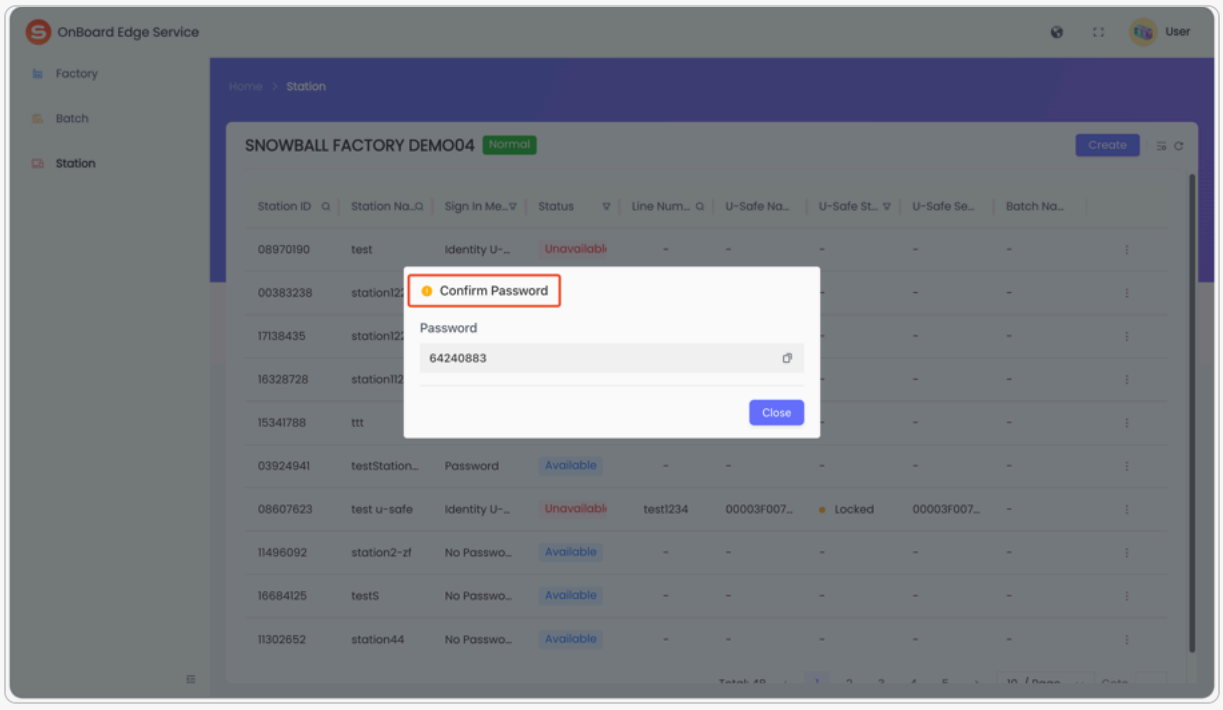
Check the programming station password

> **TIP**
>
> When the sign-in method for the programming station is **Password**, the system will generate a random password, which can be used to sign in to the Programming Station client. Currently, the randomly generated password can't be changed.

1. Sign in to OnBoard Edge Service.
2. In the left menu, click **Station**. On the station page, click the Options ⋮ icon for the corresponding programming station and select **View Password**.



3. In the **Confirm Password** window, you can check and copy the sign-in password for the programming station.



Version: v3.4.0 (Latest)

Overview of Programming Station

> **INFO**
>
> Currently, the Programming Station client is available only on Windows.

The Programming Station is the last-mile execution endpoint where devices are physically programmed and provisioned. Programming Station Software is the tooling software used to connect to the devices to be programmed and execute various chip programming tasks. As a key part of the chip programming process that directly interfaces with the operator, it offers a clean and user-friendly operating environment, allowing operators to complete all chip programming tasks easily without in-depth knowledge of complex underlying technologies.

Programming Station Software wraps and governs existing chip vendor and programmer vendor tooling through a layered component architecture, enabling flexibility across different chips and product requirements, as summarized in the following table:

Component	Provider	Role
Programming Station Application	OBIS	User interface for programming engineers • Execute an assigned Production Batch, or manually enter either a Production Batch identifier or a Production Order identifier to download the associated Programming Station Software package, which combines the Execution Process Control Scripts CLI and Chip Adaptation CLI tools • Configure channel settings and USB port-to-channel mapping
Execution Process Control Scripts CLI	OEM	OEM-developed scripts, orchestrate programming and provisioning flows
Chip Adaptation CLI	Chip vendor	Chip vendor provided tooling software, supports chip-specific programming and provisioning interfaces
Programmer CLI	Programmer vendor	(If applicable) Programmer vendor provided drivers and tools (e.g., J-Link), interfaces directly with physical programming hardware

This layered architecture allows OBIS to support a wide range of chip platforms and programmer hardware while maintaining a consistent, centralized governance model for all provisioning operations.

Version: v3.4.0 (Latest)

How to install Programming Station

> **INFO**
>
> Currently, the Programming Station client is available only on Windows.

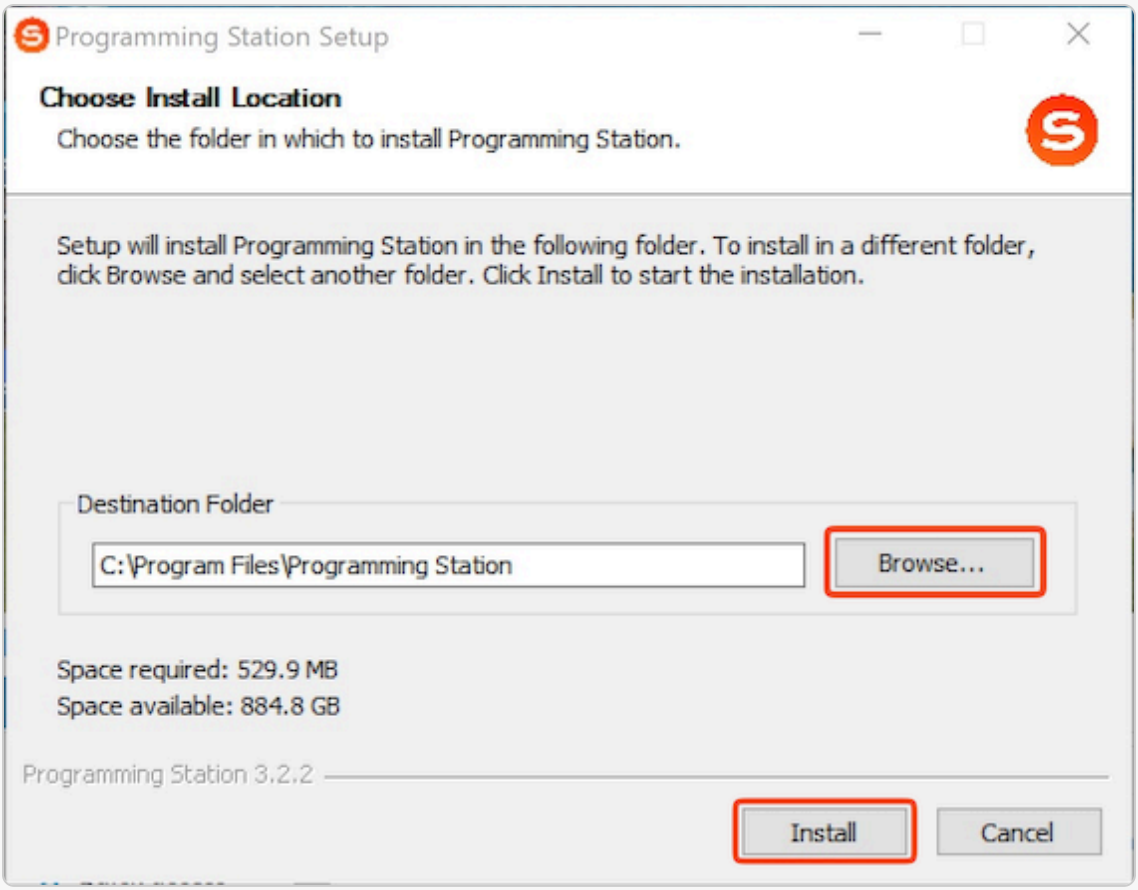
This article will guide you on how to install the Programming Station client.

Prerequisites

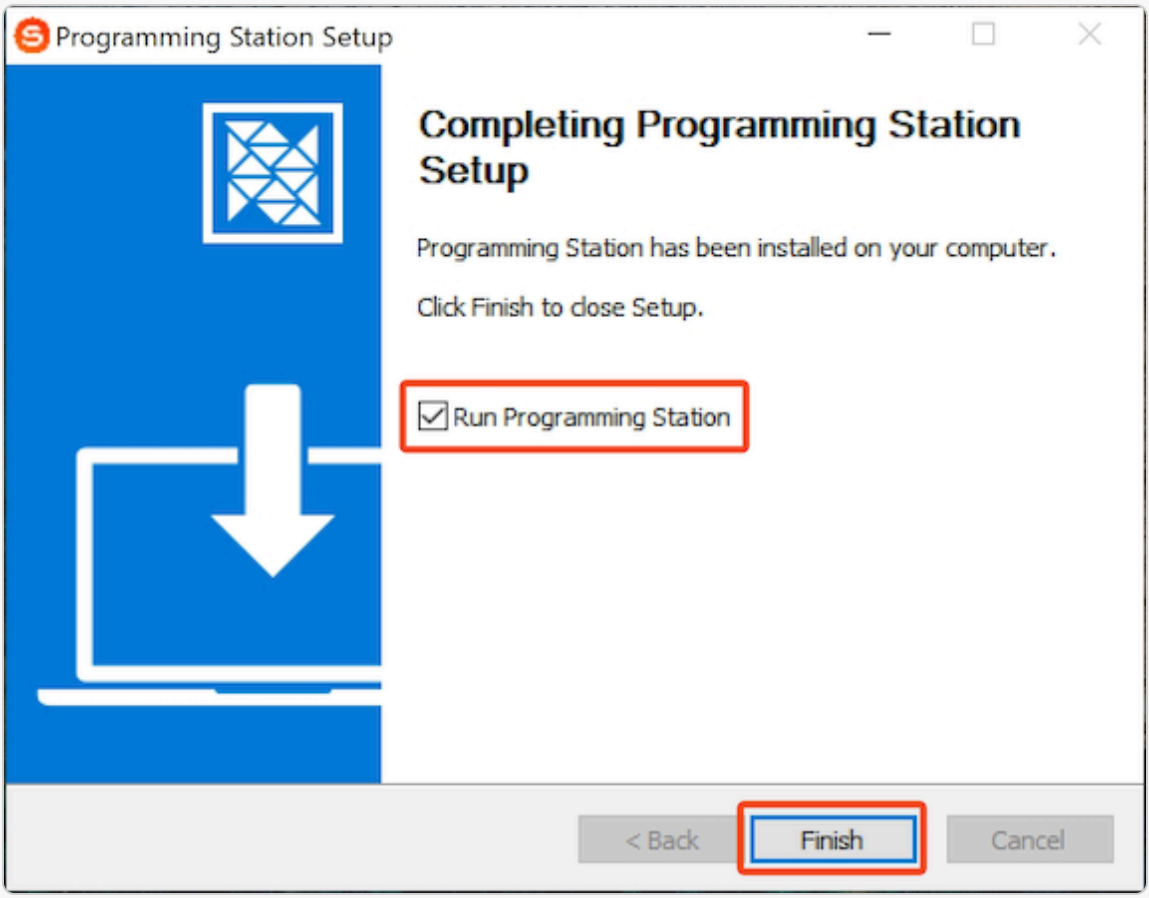
Before getting started, please ensure that you have obtained the installation package for the Programming Station client from Snowball.

Instructions

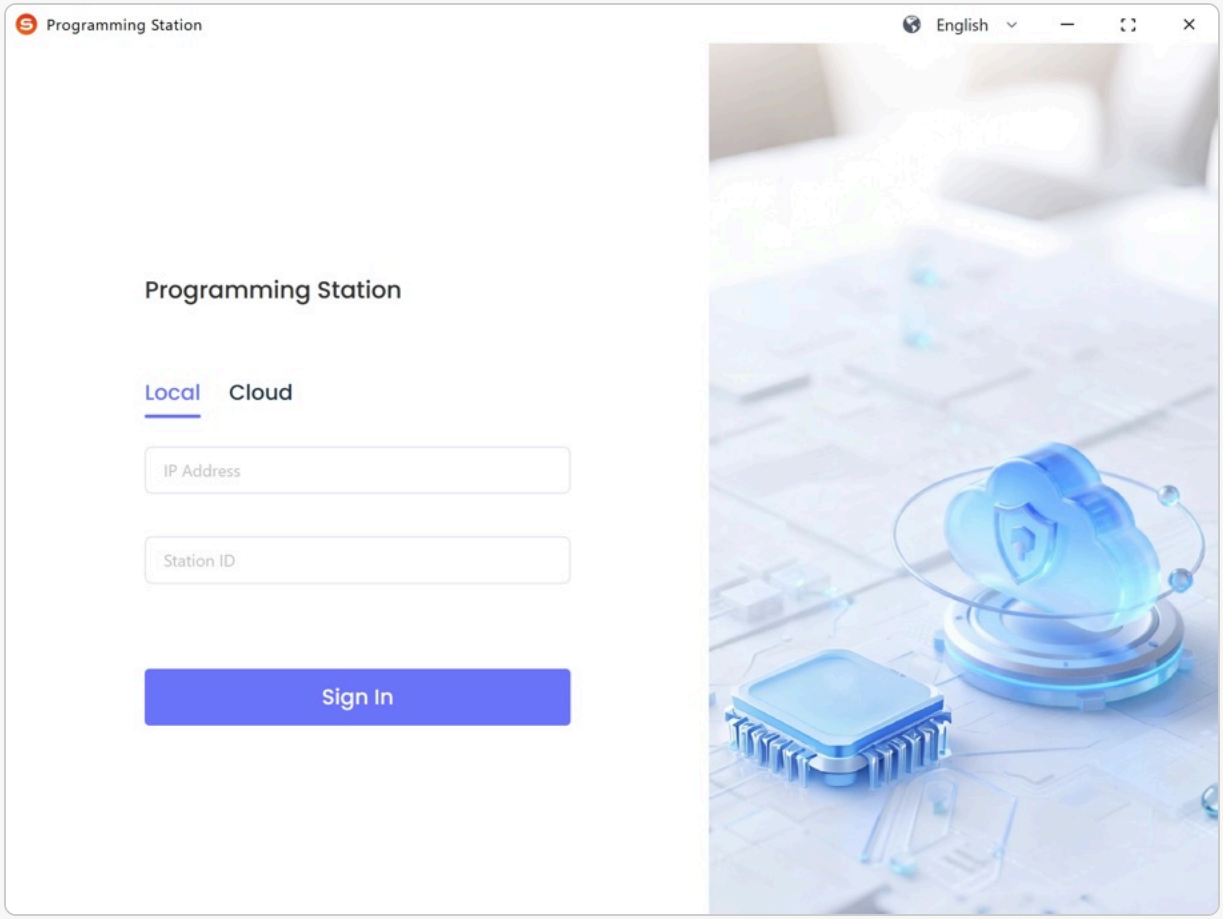
1. Run the installation package of the Programming Station client to start the installation.
2. In the **Choose Install Location** window, click **Browse** to specify an installation location (or use the default path) for the client, and then click **Install**.



3. In the pop-up window, select the **Run Programming Station** check box as needed, and then click **Finish**.



4. If the **Run Programming Station** check box is selected, the Programming Station client will start automatically.


Programming Station
English
Programming Station
Local
Cloud
IP Address
Station ID
Sign In

Version: v3.4.0 (Latest)

How to sign in to Programming Station

> **INFO**
>
> Currently, the Programming Station client is available only on Windows.

This article will guide you on how to sign in to the Programming Station client using either the "No Password", "Password", or "Identity U-Safe" method.

Prerequisites

Before getting started, please ensure that:

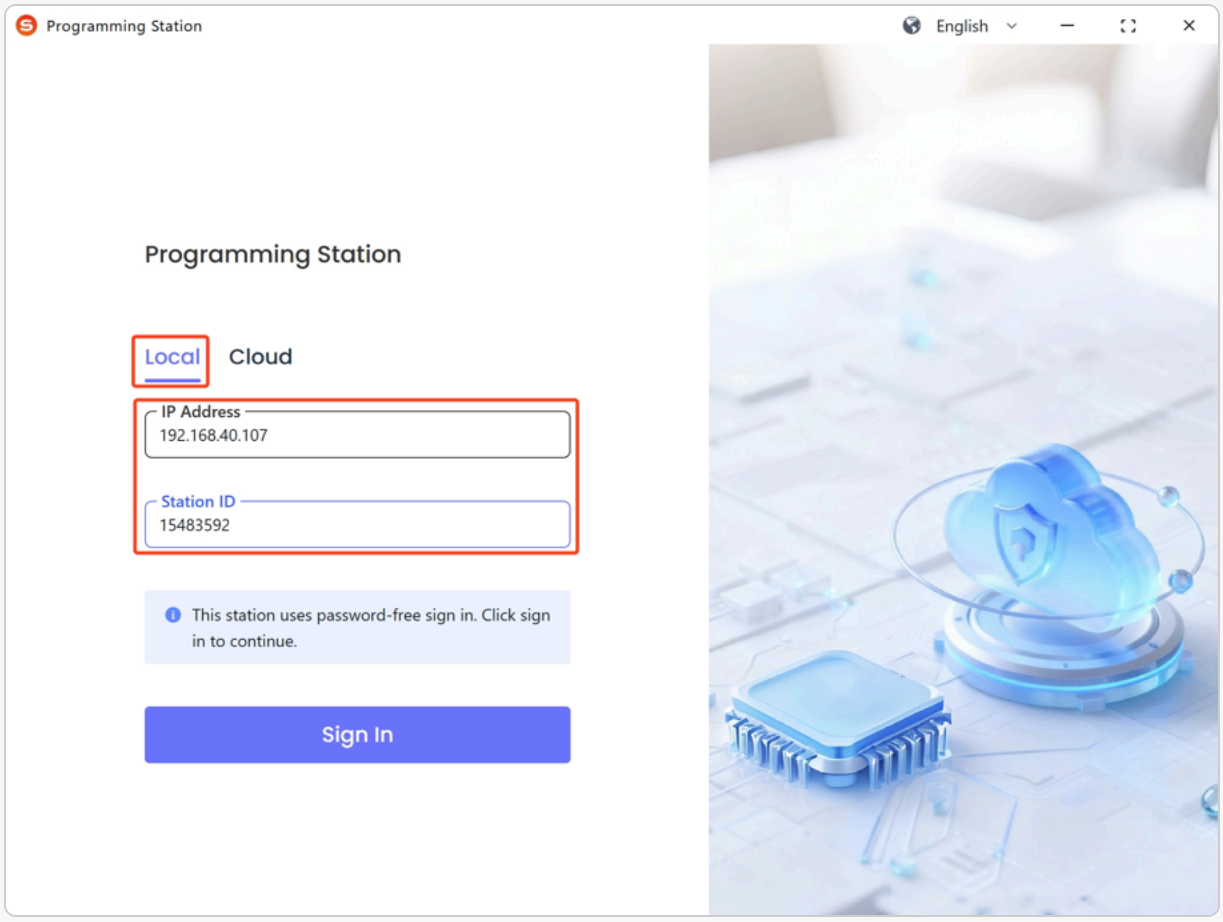
- A programming station has been added in OnBoard™ IoT Security (OBIS) (local factory & cloud factory) or OnBoard Edge Service.
- The Programming Station client has been installed.

Local factory

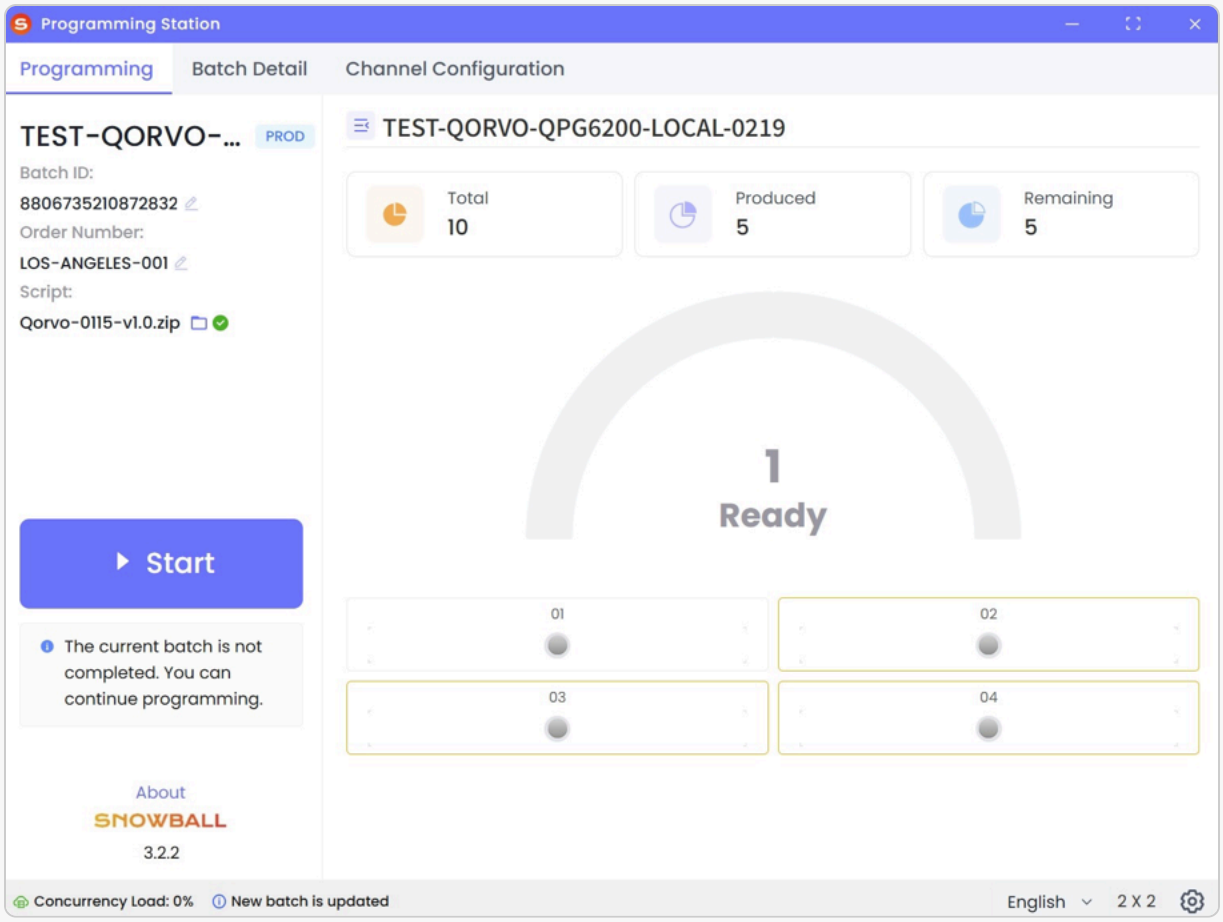
> **TIP**
>
> Please ensure that you have contacted Snowball for assistance with the deployment of OnBoard Edge Service, and that your sign-in device is within the factory service intranet environment.

Method one: No Password

1. Start the Programming Station client, and then select **Local**.
2. Enter the IP address (for example, 192.168.0.1) in the **IP Address** field. For more information, refer to how to check service address.



3. Enter the corresponding programming station ID and then click **Sign In**. Once signed in, the page will navigate to the main window of the Programming Station client.

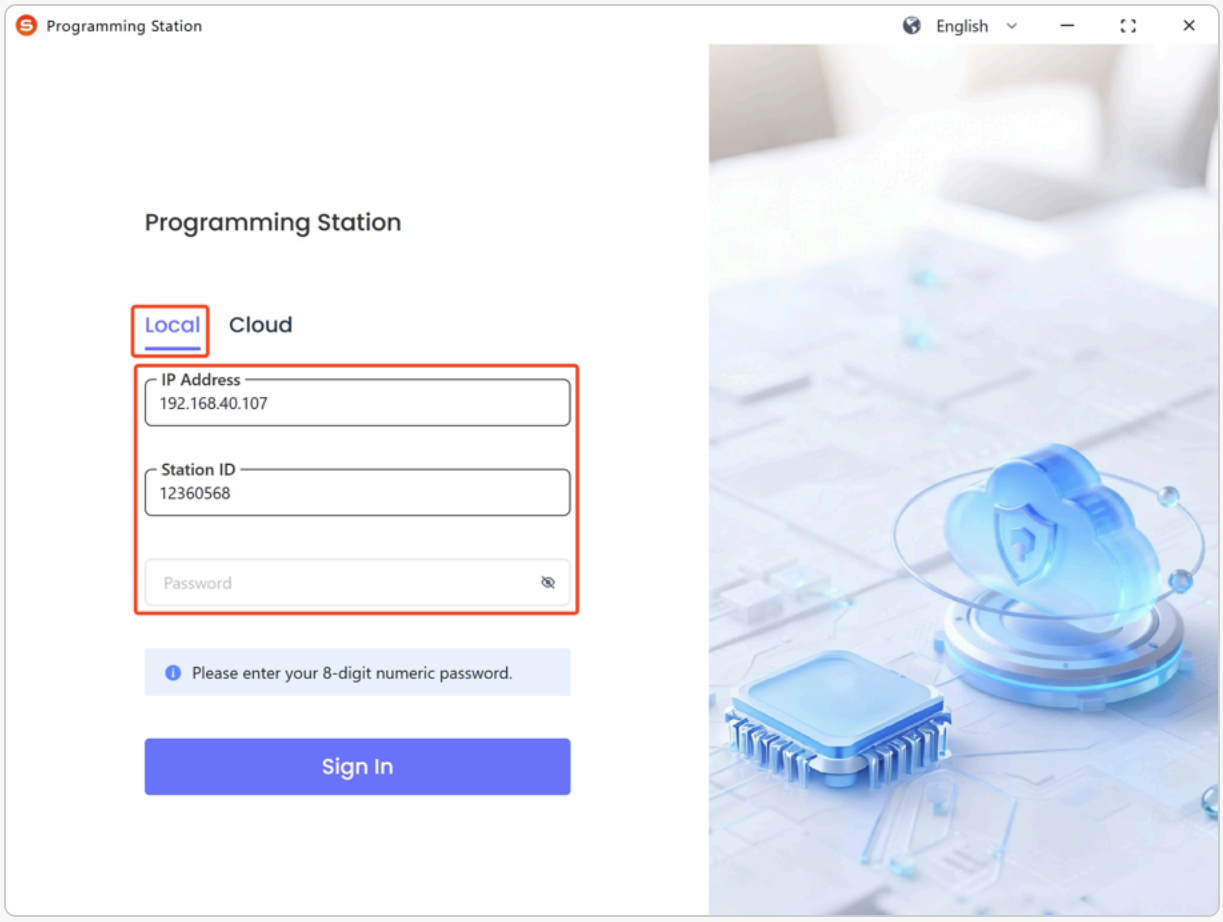


Method two: Password

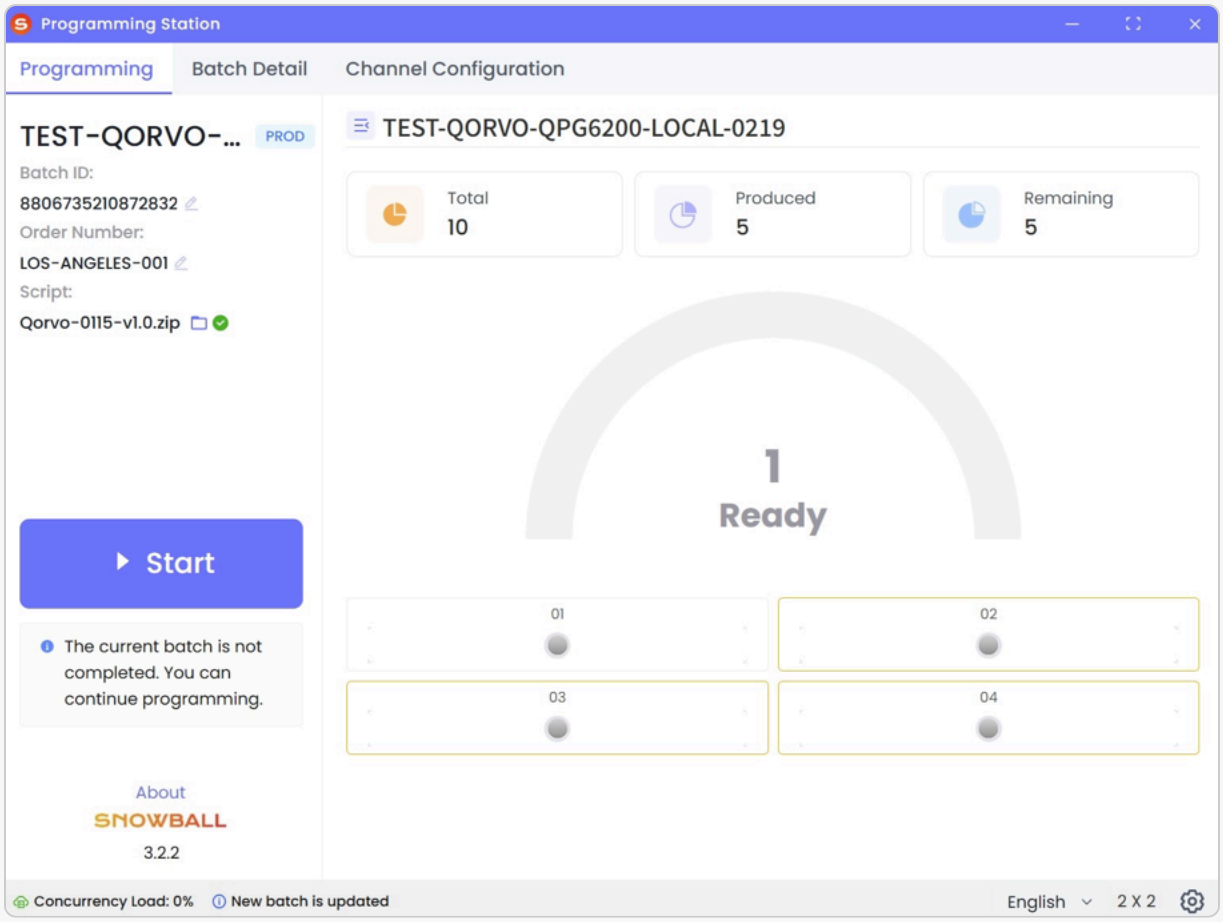
> **TIP**
>
> The initial sign-in password is randomly generated by the system after a programming station is added to the factory. You can check the sign-in password in OBIS or OnBoard Edge Service. Currently, the randomly generated password can't be changed.

1. Start the Programming Station client, and then select **Local**.

2. Enter the IP address (for example, 192.168.0.1) in the **IP Address** field. For more information, refer to how to check service address.



3. Enter the corresponding programming station ID and password, and then click **Sign In**. Once signed in, the page will navigate to the main window of the Programming Station client.

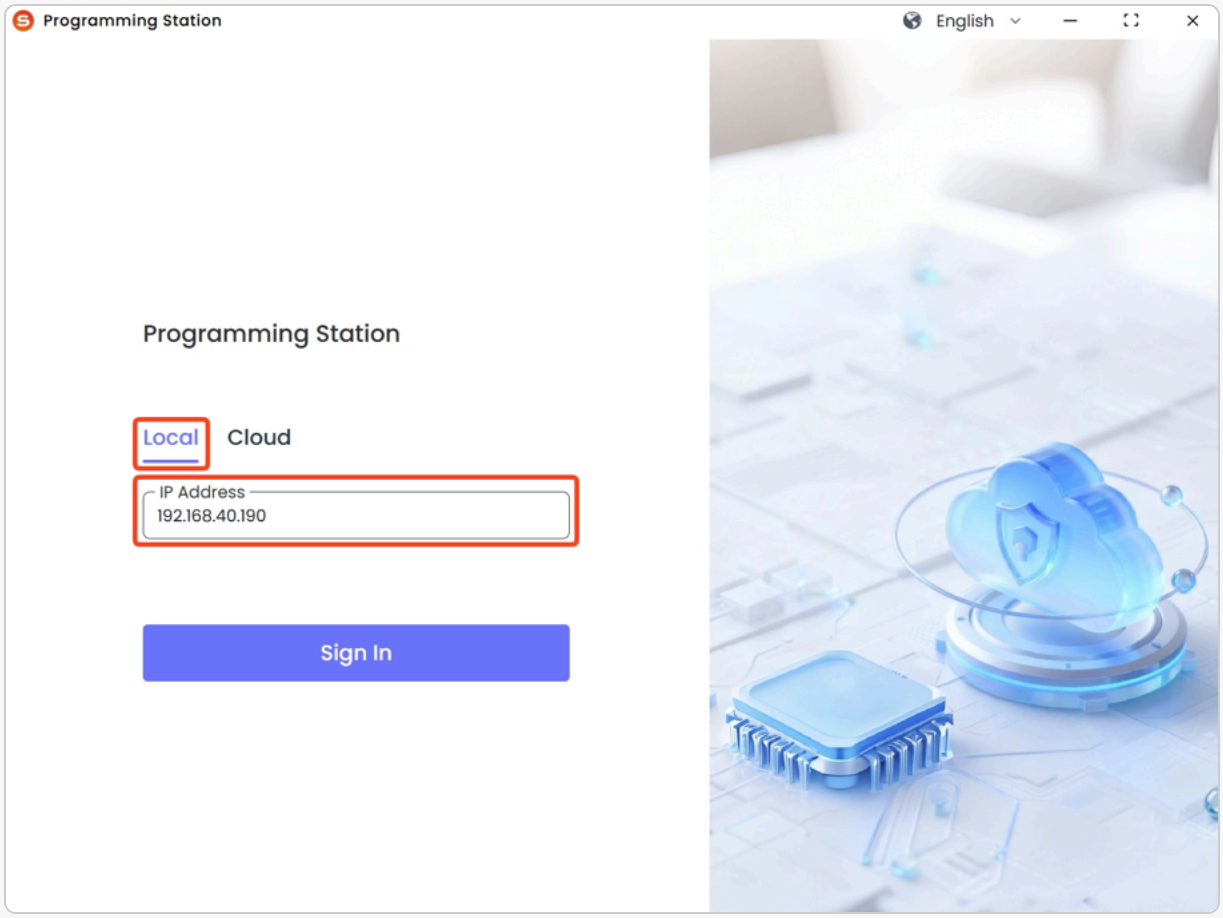


Method three: Identity U-Safe

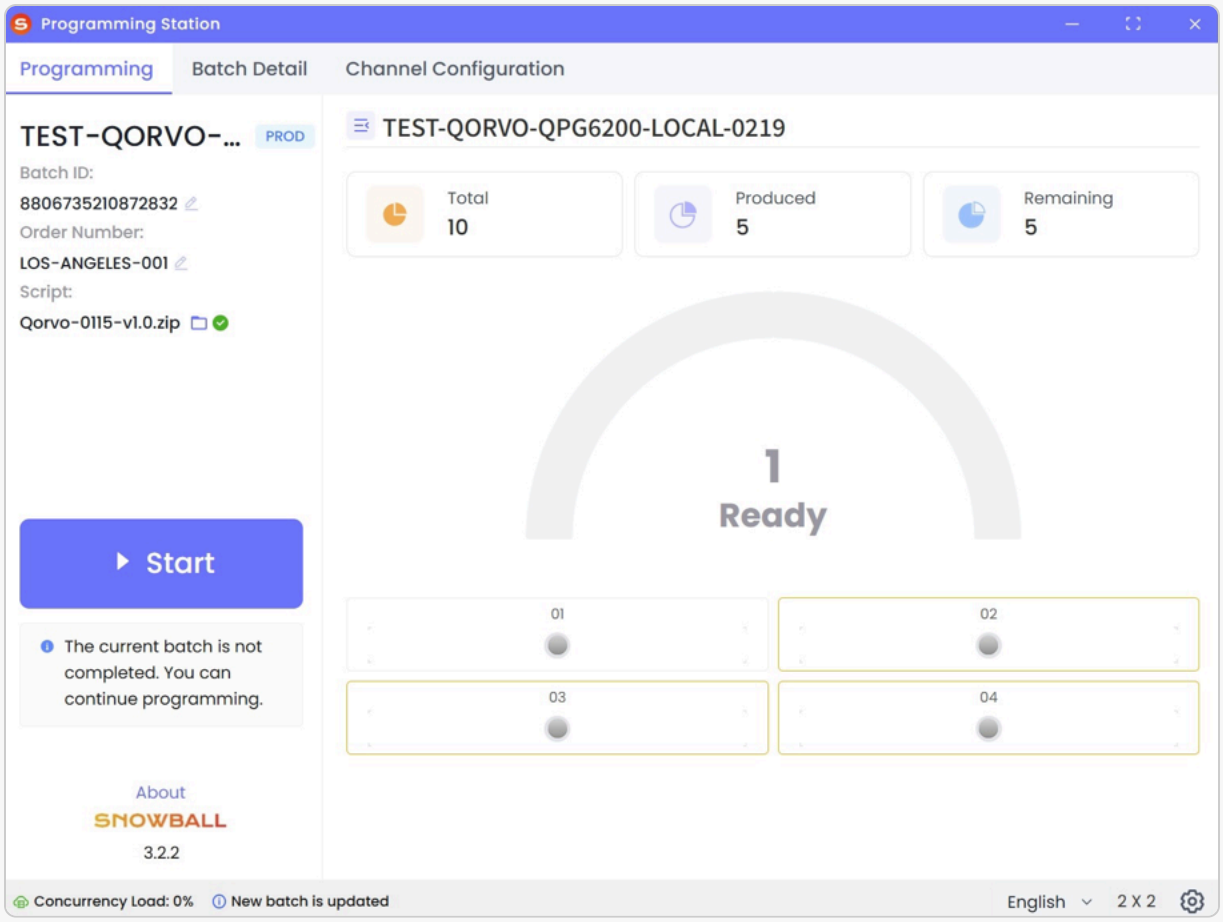
> **INFO**
>
> When signing in using the Identity U-Safe method, you need to obtain the Identity U-Safe used for identity authentication from Snowball, and insert the corresponding Identity U-Safe (added during factory configuration) into the device that has installed the Programming Station client. After insertion, if the Identify U-Safe is already bound to the programming station, the client will recognize the station ID.
>
> Only one Identify U-Safe can be inserted at a time; otherwise, sign-in will fail.

1. Start the Programming Station client, then select **Local** and insert the Identity U-Safe.

2. Enter the IP address (for example, 192.168.0.1) in the **IP Address** field. For more information, refer to how to check service address.



3. Click **Sign In**. Once signed in, the page will navigate to the main window of the Programming Station client.

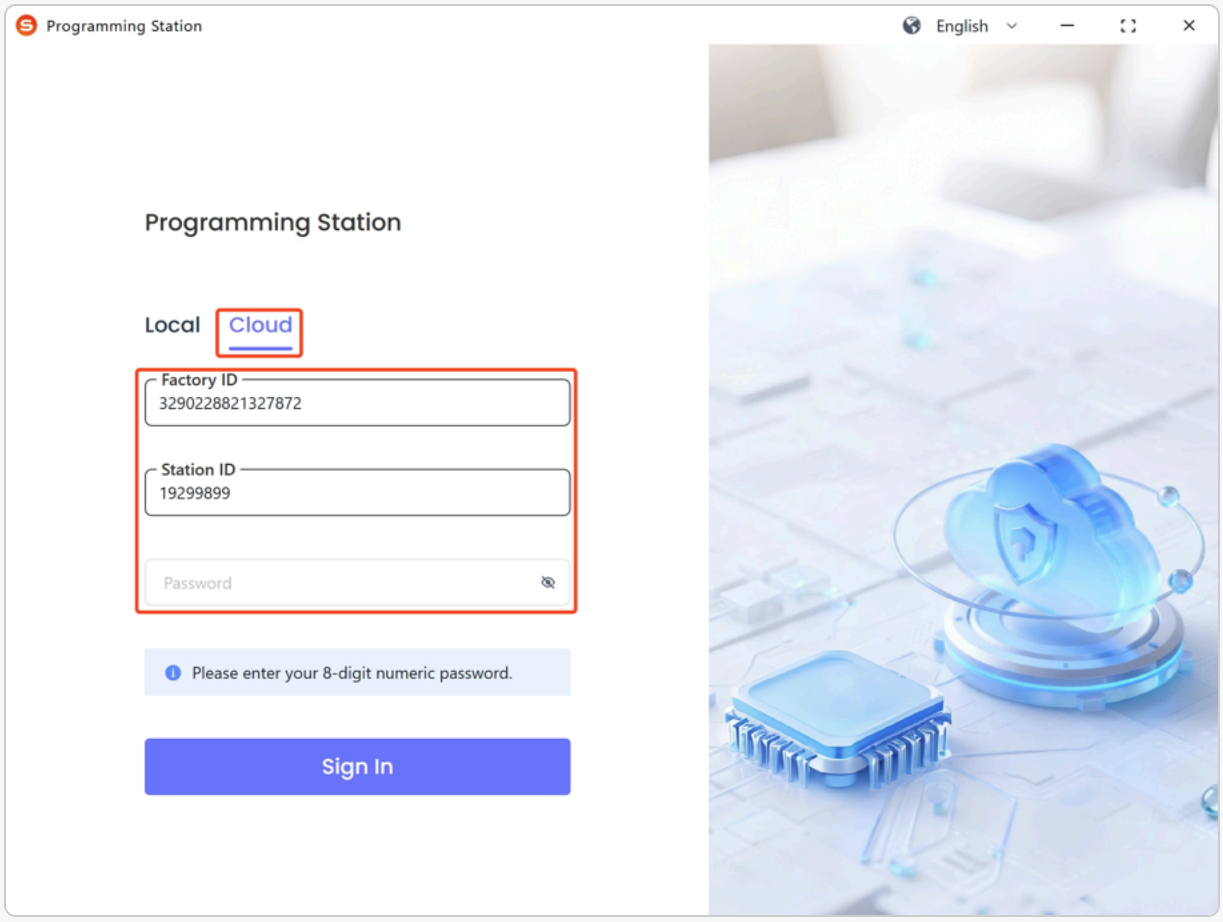


Cloud factory

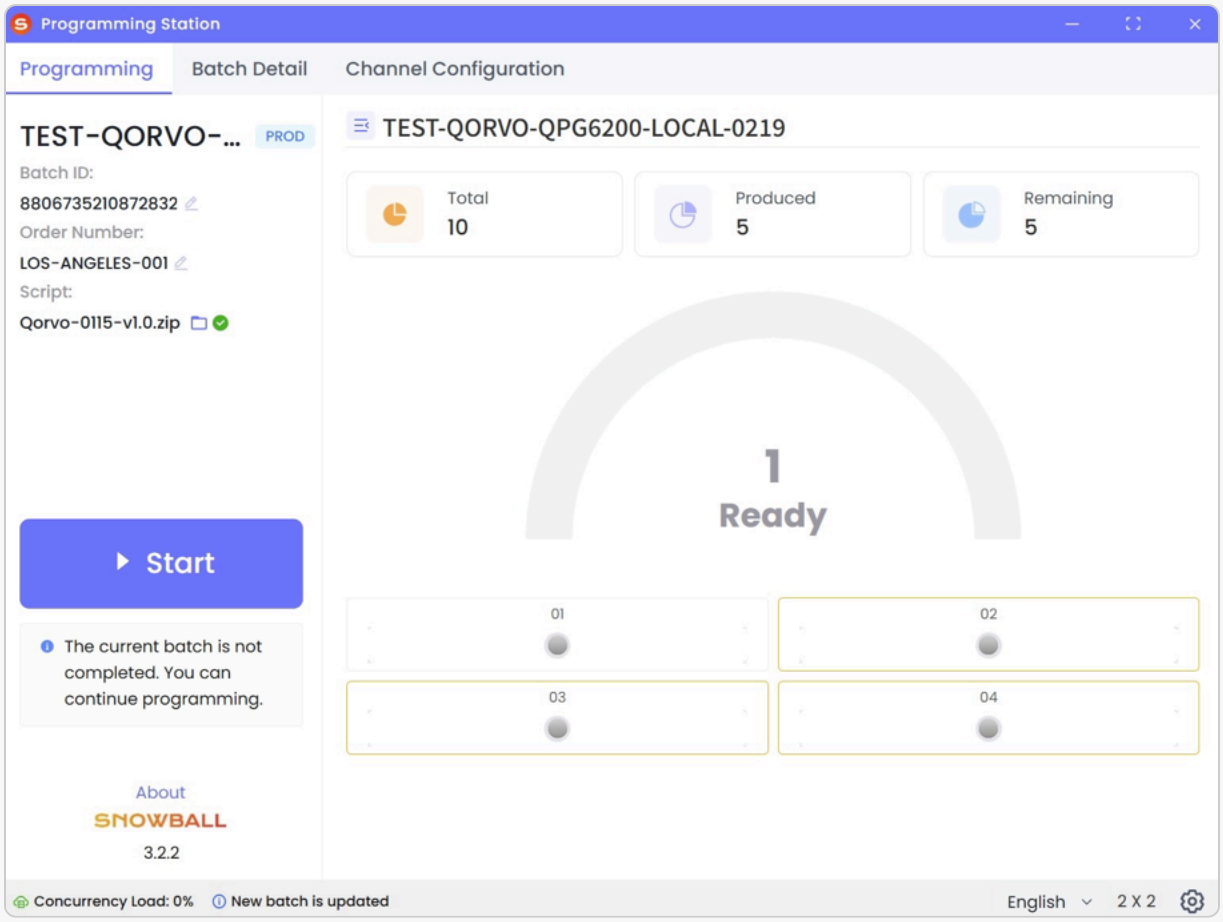
Method one: Password

> **TIP**
>
> The initial sign-in password is randomly generated by the system after a programming station is added to the factory. You can check the sign-in password in OBIS. Currently, the randomly generated password can't be changed.

1. Start the Programming Station client, select **Cloud**, and then enter the corresponding factory ID.



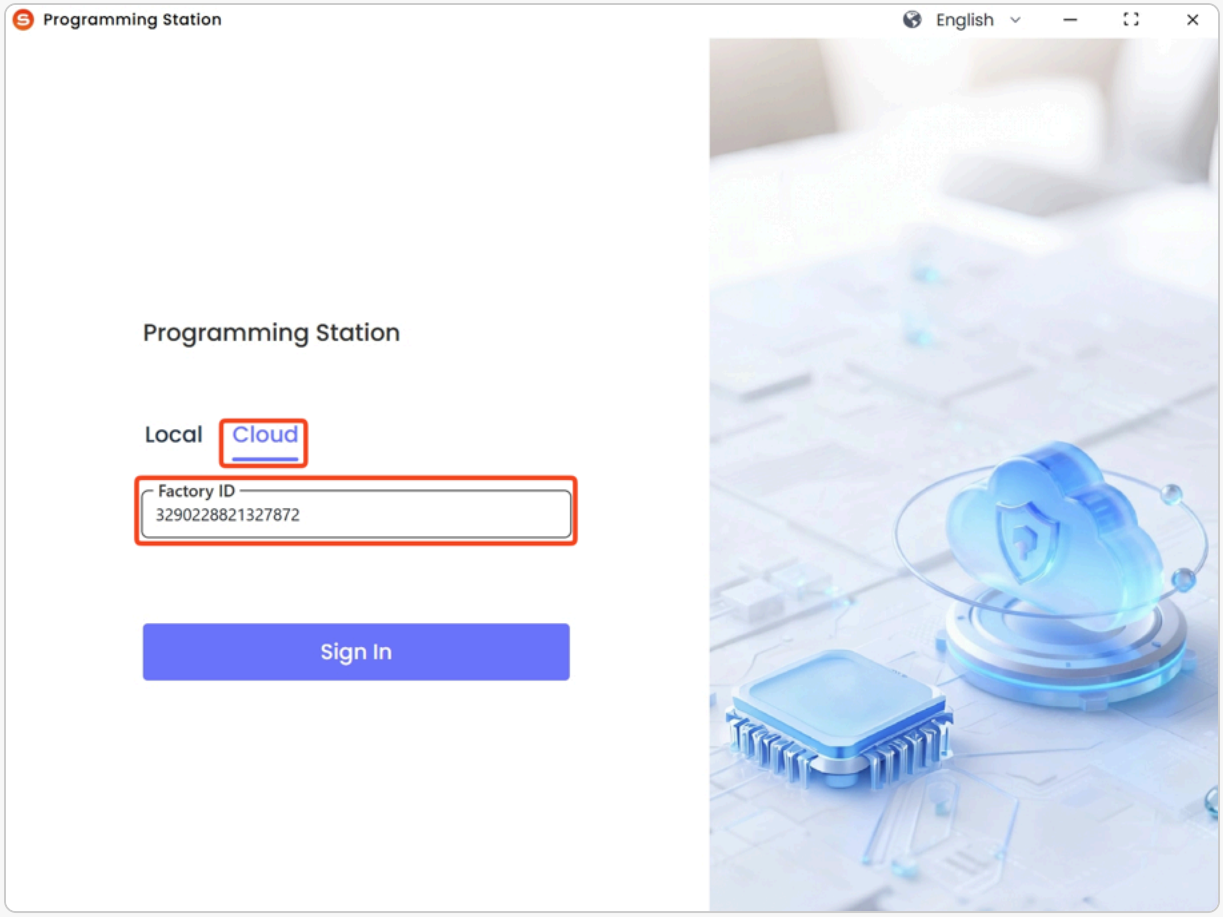
2. Enter the corresponding programming station ID and password, and then click **Sign In**. Once signed in, the page will navigate to the main window of the Programming Station client.



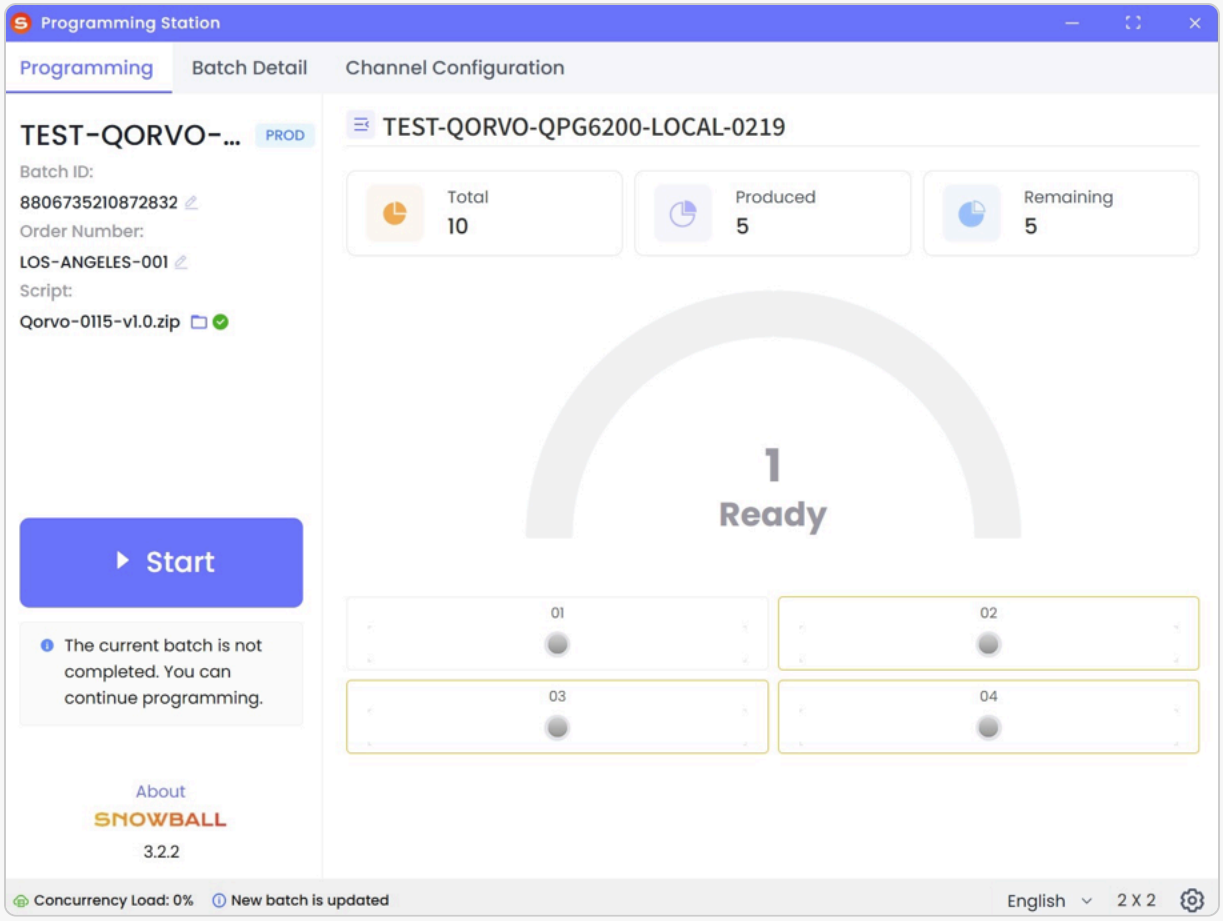
Method two: Identity U-Safe

> **INFO**
>
> When signing in using the Identity U-Safe method, you need to obtain the Identity U-Safe used for identity authentication from Snowball, and insert the corresponding Identity U-Safe (added during factory configuration) into the device that has installed the Programming Station client. After insertion, if the Identify U-Safe is already bound to the programming station, the client will recognize the station ID.
>
> Only one Identify U-Safe can be inserted at a time; otherwise, sign-in will fail.

1. Start the Programming Station client, select **Cloud**, then enter the corresponding factory ID and insert the Identity U-Safe.



2. Click **Sign In**. Once signed in, the page will navigate to the main window of the Programming Station client.


Programming Station
Programming
Batch Detail
Channel Configuration
TEST-QORVO-...
PROD
Batch ID:
8806735210872832
Order Number:
LOS-ANGELES-001
Script:
Qorvo-0115-v1.0.zip
TEST-QORVO-QPG6200-LOCAL-0219
Total
10
Produced
5
Remaining
5
1
Ready
Start
01
02
03
04
The current batch is not completed. You can continue programming.
About
SNOWBALL
3.2.2
Concurrency Load: 0%
New batch is updated
English
2 X 2

Version: v3.4.0 (Latest)

How to execute device programming in Programming Station

> **INFO**
>
> Currently, the Programming Station client is available only on Windows.

This article will guide you on how to use the Programming Station client to execute device programming.

Prerequisites

Before getting started, please ensure that you can sign in to the Programming Station client.

Instructions

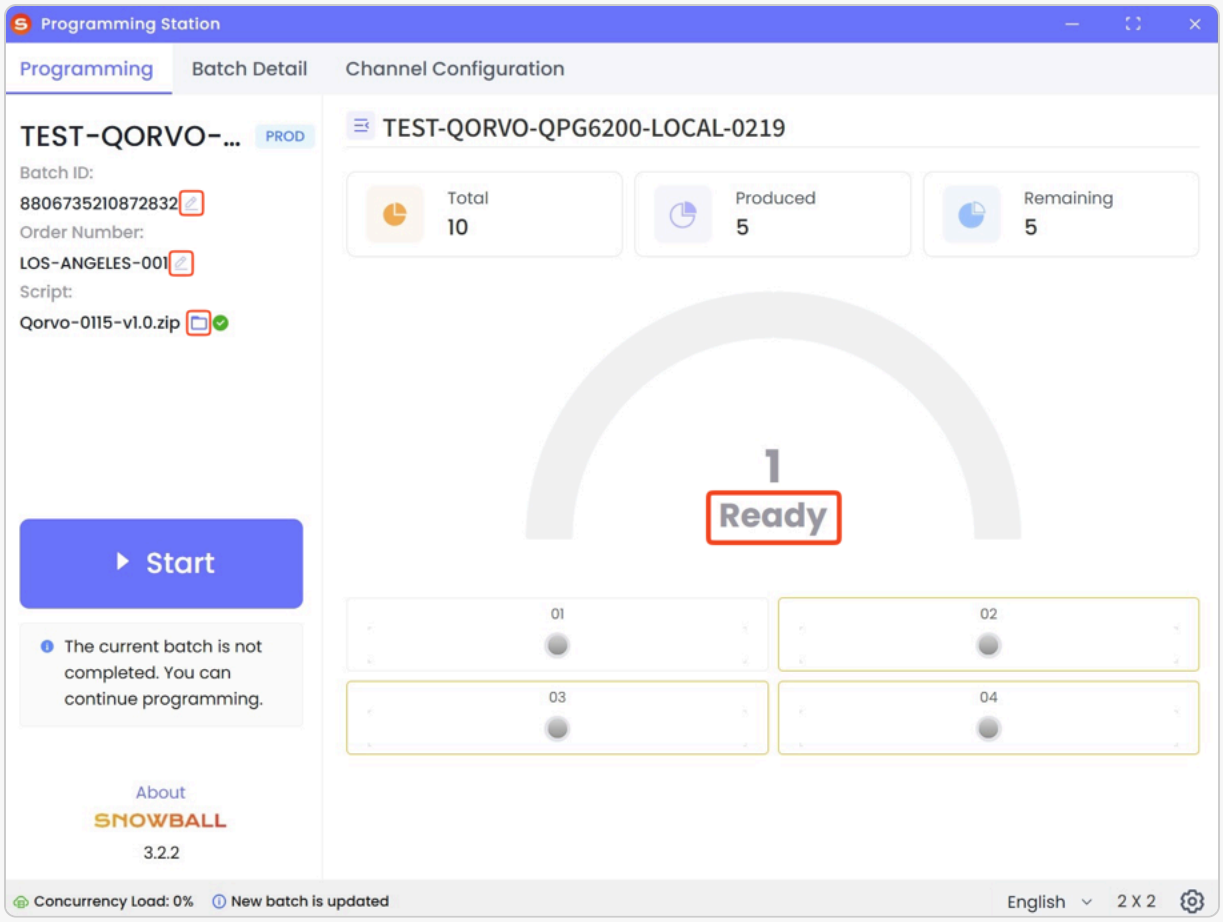
1. Sign in to the Programming Station client, and then verify that the device status is **Ready**.

TIP

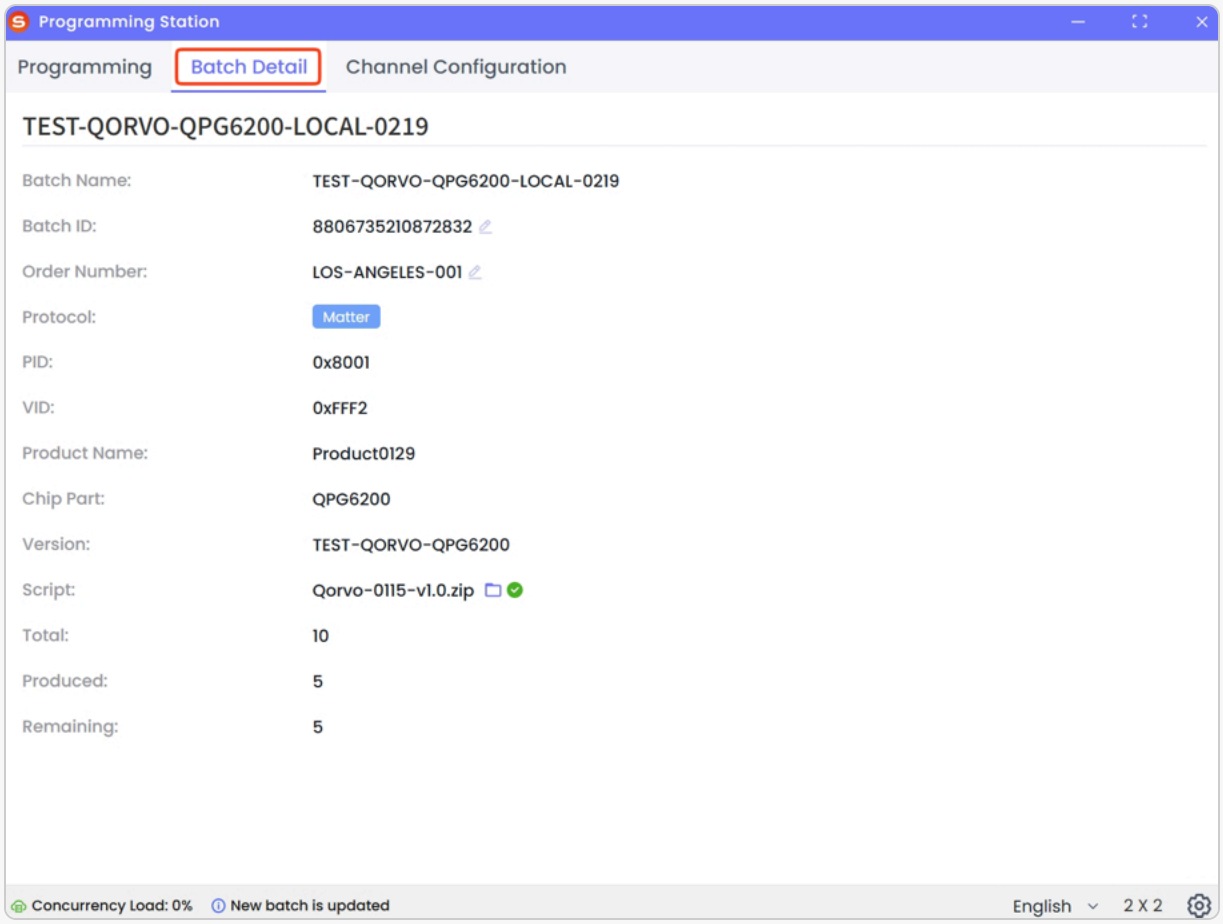
If the programming script is not selected when creating a batch, or if you want to select a different programming script, you can click the Folder icon to select the required programming script (any script format is supported, and the maximum supported file size is 512 MB). Additionally, you can click the Settings icon in the bottom-right corner and select **Script Download Path** to customize the default script download path.

If the programming station is not yet assigned to a batch:

- Click the Edit icon to the right of the **Batch ID** area, then enter the batch ID to retrieve the corresponding batch information.
- Click the Edit icon to the right of the **Order Number** area, enter the order number, and then select the associated batch name to retrieve the corresponding batch information.



2. On the **Batch Detail** tab, you can check batch-related information (such as **Protocol**, **VID**, and **PID**).



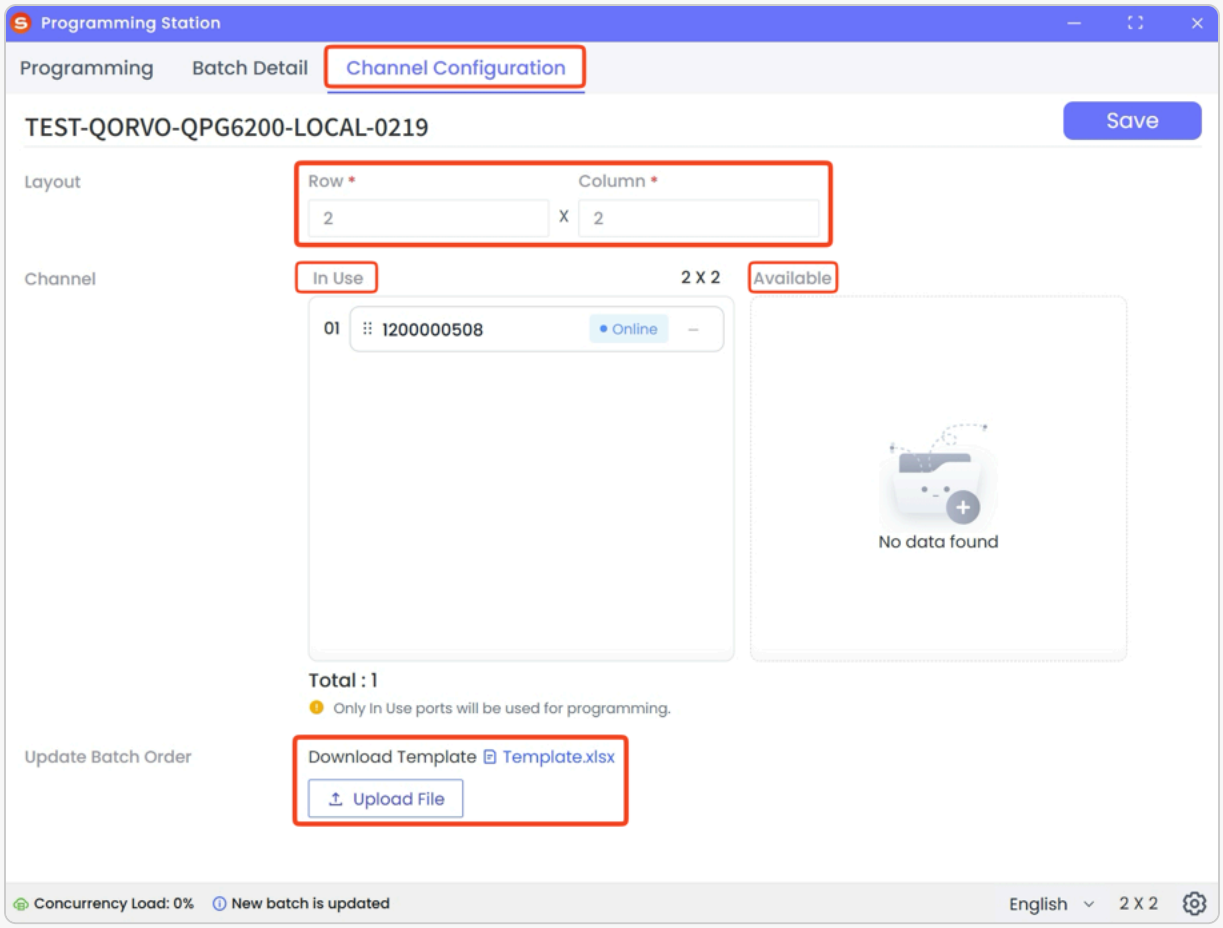
3. In the main window, select the **Channel Configuration** tab and then set the number of programmer connections in the **Layout** area as needed.

TIP

The number of connections determines how many devices can be programmed simultaneously. The system currently supports a number of connections based on the product of rows and columns in the layout area, which must satisfy the following conditions:

- Both rows and columns must be integers.
- Rows × Columns ≤ 24.
- Neither rows nor columns may exceed 16.
- If the number of rows exceeds 4, the number of columns can only be 1 or 2.

Ports can be dragged and reordered between the **In Use** and **Available** ports, or you can update the order by downloading and modifying the Excel template (**Template.xlsx**) and then uploading it. Changes take effect after uploading.



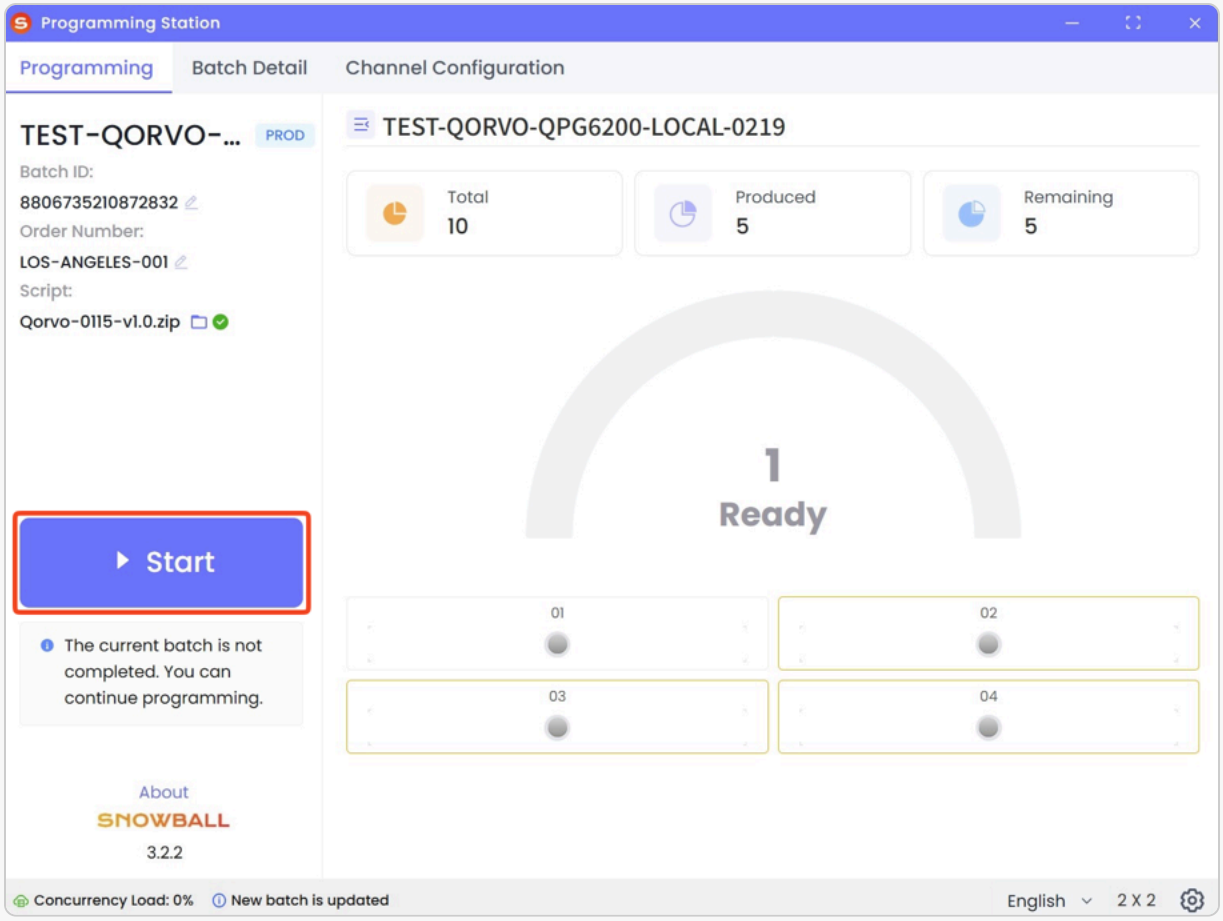
4. After verifying that the information is correct, click **Start** in the main window to execute device programming.

TIP

The **Concurrency Load** displayed in the bottom-left corner of the client indicates the server load when multiple programming stations are simultaneously programming:

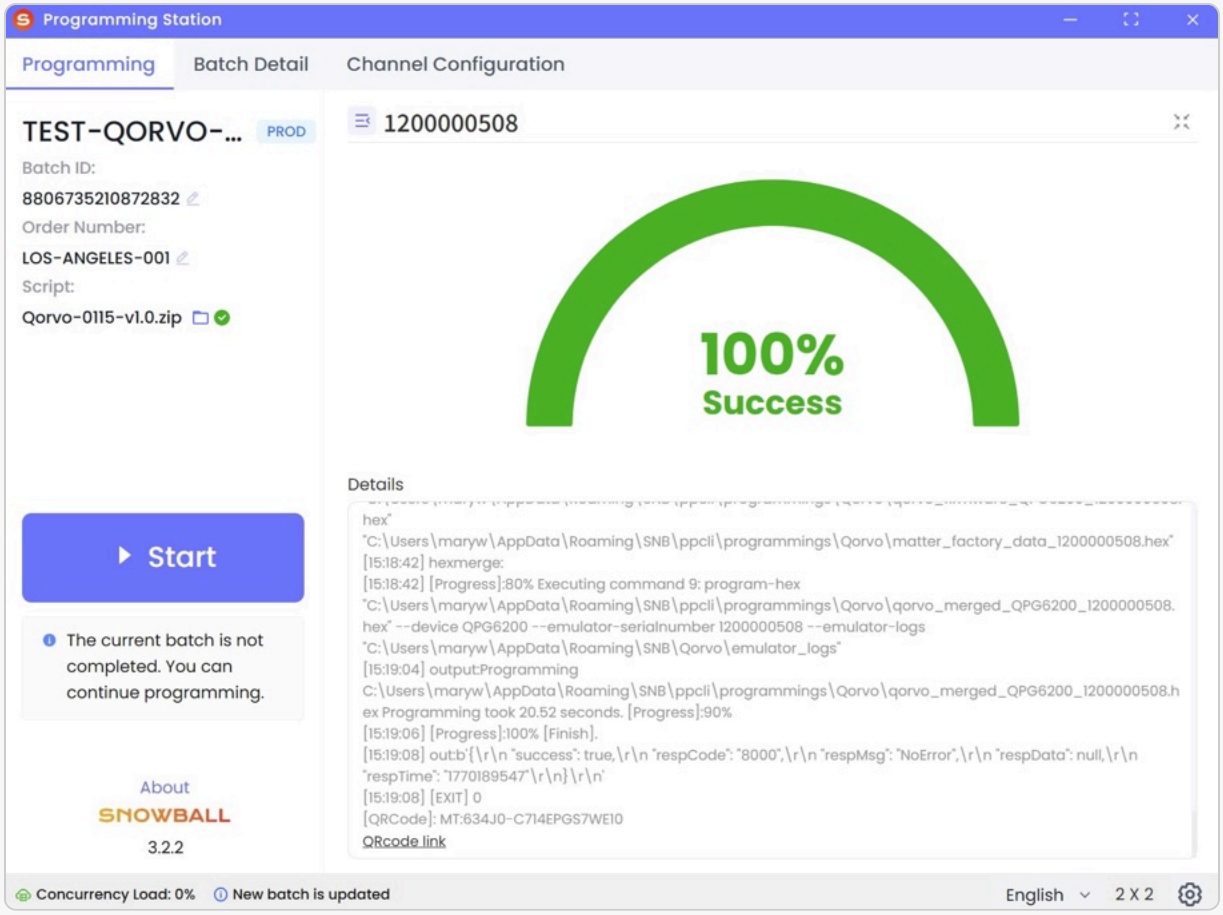
- Load ≥ 90%:
  - Message: "Concurrency limit nearly reached. Please contact the factory administrator to check the server".
  - You can continue programming.
- Load = 100%:
  - Message: "Concurrency limit reached. Please contact the factory administrator to check the server".
  - You can continue programming.

During programming, switching to the **Channel Configuration** tab is not allowed.



5. After programming is completed, click the corresponding port to check the device programming details.

> **TIP**
>
> You can also check the device profile and related log information in OnBoard™ IoT Security (OBIS).


Programming Station
Programming
Batch Detail
Channel Configuration
TEST-QORVO-...
PROD
Batch ID:
8806735210872832
Order Number:
LOS-ANGELES-001
Script:
Qorvo-0115-v1.0.zip
1200000508
100%
Success
Details
hex"
"C:\Users\maryw\AppData\Roaming\SNB\ppcli\programmings\Qorvo\matter_factory_data_1200000508.hex"
[15:18:42] hexmerge:
[15:18:42] [Progress]:80% Executing command 9: program-hex
"C:\Users\maryw\AppData\Roaming\SNB\ppcli\programmings\Qorvo\qorvo_merged_QPG6200_1200000508.hex" --device QPG6200 --emulator-serialnumber 1200000508 --emulator-logs
"C:\Users\maryw\AppData\Roaming\SNB\Qorvo\emulator_logs"
[15:19:04] output:Programming
C:\Users\maryw\AppData\Roaming\SNB\ppcli\programmings\Qorvo\qorvo_merged_QPG6200_1200000508.hex Programming took 20.52 seconds. [Progress]:90%
[15:19:06] [Progress]:100% [Finish].
[15:19:08] out:b'{\r\n "success": true,\r\n "respCode": "8000",\r\n "respMsg": "NoError",\r\n "respData": null,\r\n "respTime": "1770189547"\r\n}\r\n'
[15:19:08] [EXIT] 0
[QRCode]: MT:634J0-C714EPGS7WE10
QRcode link
Start
The current batch is not completed. You can continue programming.
About
SNOWBALL
3.2.2
Concurrency Load: 0%
New batch is updated
English
2 X 2

Version: v3.4.0 (Latest)

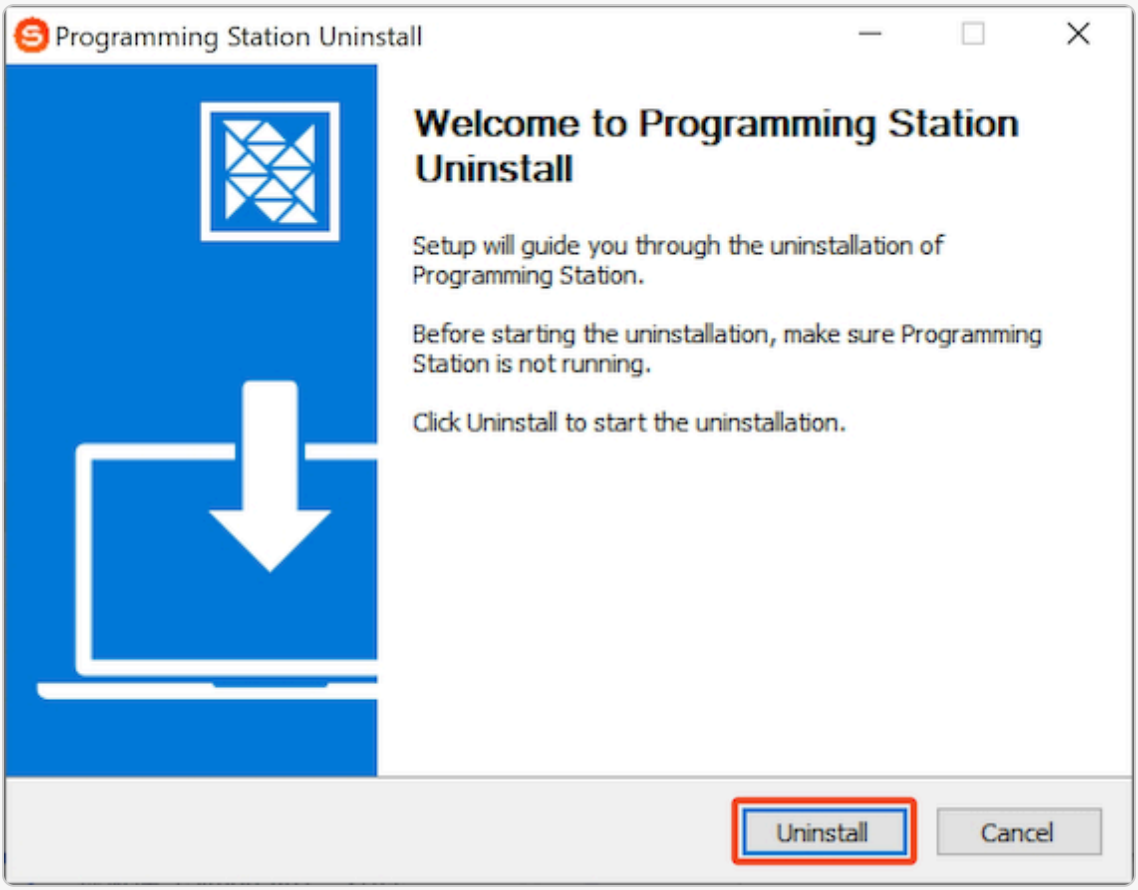
How to uninstall Programming Station

> **INFO**
>
> Currently, the Programming Station client is available only on Windows.

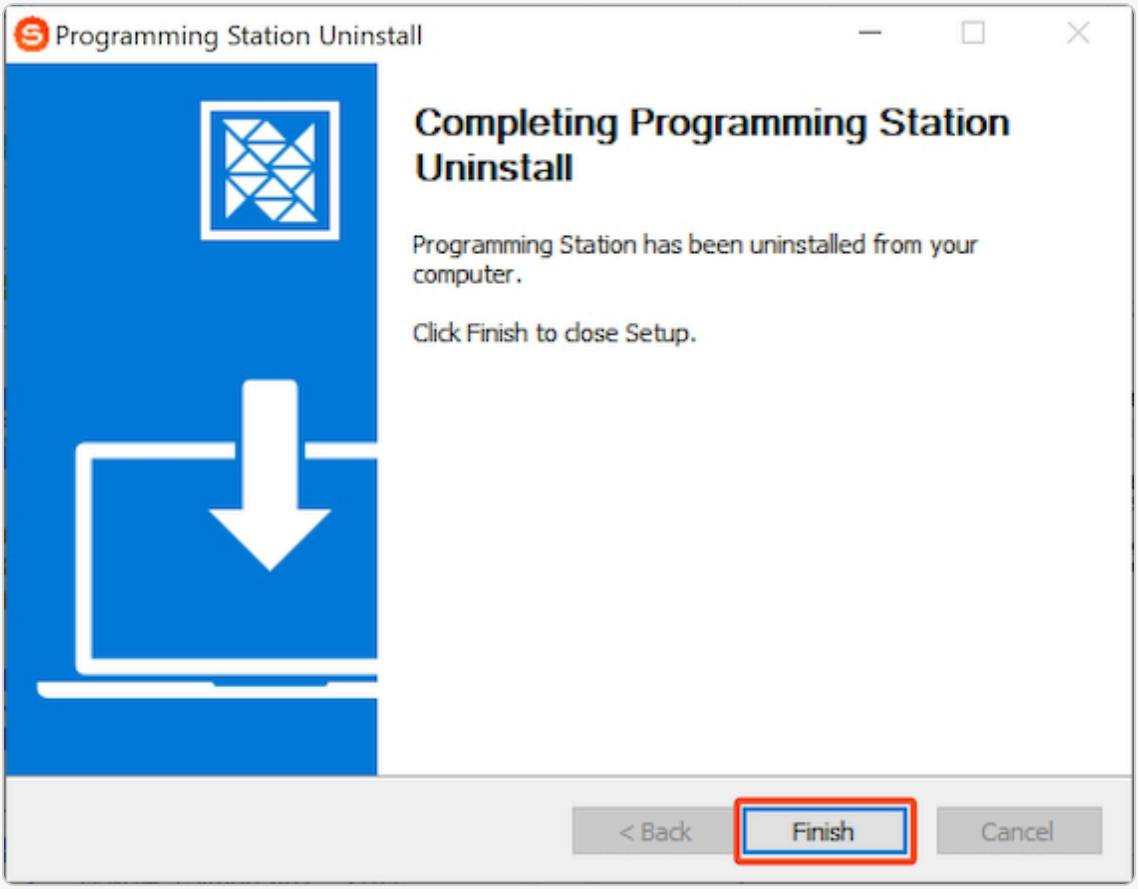
This article will guide you on how to uninstall the Programming Station client.

Instructions

1. Right-click the client icon on the desktop or the Start menu, and then click **Open file location**.
2. In the installation location, find the file named **Uninstall Programming Station** and double-click to run it.
3. In the pop-up window, click **Uninstall** to start the uninstallation.



4. After the client is uninstalled, click **Finish** to complete the uninstallation.


Programming Station Uninstall
Completing Programming Station Uninstall
Programming Station has been uninstalled from your computer.
Click Finish to close Setup.
< Back
Finish
Cancel

Version: v3.4.0 (Latest)

Factory Edge Service API - v1.5

1. Revision Record

Version	Modified Date	Notes
v1.0	2025/03/26	Initial release
v1.1	2025/12/17	Added "Query Device Details" API, which can be used to retrieve programming status
v1.2	2025/12/22	• Updated the required parameter validation and parameter descriptions of the "Query Device Details" API (Supports using the Matter QR code as a query condition to retrieve device information) • Added API exception status code definitions • Added an error code list
v1.3	2026/01/26	• Deprecated "Query Device Data" and "Update Device Info" APIs • Added "Update Devices Profile" API
v1.4	2026/09/10	Added the "Upload Device Production Data" API.
v1.5	2026/10/16	• Updated the "Query Device Details", "Update Devices Profile", and "Upload Device Production Data" APIs. • Added "Query Device Information", "Recover Matter QR Code", "Upload Device Test File", "Connection Heartbeat", "Query Login Options", "Query Programming Station Login Method", "U-Safe Pre-login", "Programming Station Login", "Programming Station Logout", "Query Batches by Order Number", "Assign Programming Station Batch", "Query Programming Station Batch Information", "Get Dynamic Programming Data", "Get Batch Metadata", "Get Full Programming Data" (compatibility API), "Submit Intermediate Programming Request Data", "Report Programming Result", "SE APDU Stepwise Programming", "Get Programming Script URL", "Download File", "Upload Device Event Logs", "Generate Matter Verifier", "Generate Matter Onboarding Payload", and "Generate Matter Unique ID" APIs. • Added compatibility notes for the deprecated "Query Device Data" and "Update Device Info" APIs. • vAdded common call conventions and error code descriptions.

2. Overview

Factory Edge Service API supports Programming Station login, production batch management, device programming, production data upload, device data queries, and device profile updates. These APIs use HTTP for data transmission, and all requests and responses are encoded in UTF-8.

This document describes the API conventions and common request headers, and provides request parameters, response parameters, and call examples for each API.

3. Common Request Headers

These APIs use the following keys (all lowercase):

Key	Mandatory	Description
content-type	Yes	Content type, unless otherwise specified, should always be `application/json;charset=utf-8`
x-snbps-factory-id	No	Factory ID
x-snbps-timestamp	No	Request time. For example, 2021-09-17T16:47:05.132+0800
x-snbps-lang	No	Language code, default is English: en-US, supports Simplified Chinese: zh-CN
x-snbps-request-id	No	Request `traceID`

3.1 API Call Conventions and Authentication

3.1.1 Service Address and Request Format

The service prefix is `{BASE_URL}/api/iot-factory-edge-service`. `{BASE_URL}` is the actual Edge address, including protocol, IP address or domain name, and port; it must not already include the service prefix. Paths below are relative to this prefix. JSON requests use UTF-8 encoding. Pass GET parameters in the URL query string; the client generates the boundary for `multipart` file uploads.

3.1.2 Programming Station Session and API Validation

After a Programming Station (PS) calls `/login`, retrieve the session token from `respData.token` and send it in the `x-snbps-session` header of subsequent requests. The station session token is distinct from a programming `traceId` or `uuid`. `x-snbps-request-id` is only for request tracing and cannot replace the business `traceId`.

The session lifetime is deployment-dependent and is refreshed when a protected API is called.

`UkeyPermissionFilter` enforces session validation for the following APIs:

```
/assignBatch
/queryPPCBatchInfo
/v1/queryBatchByOrderNumber
/getPPData
/getProgrammingData
/uploadRequestData
/programmingResult
/executeApdu
/v1/eventLog/upload
/v1/matter/onboarding-payloads/recover
/v1/device/information/query
/v1/testFile/upload
/v1/deviceData/upload
```

If validation data is missing or invalid, the service returns `HTTP 200` with business code `8050`.

3.1.3 Platform Authentication and Factory Context

Platform authentication is controlled separately by deployment configuration. In the current repository, `application.yml` does not exempt the following API paths from platform authentication:

- `/v1/device/detail`
- `/v1/updateDevicesProfile`
- `/v1/deviceData/upload`
- `/executeApdu`
- `/v1/eventLog/upload`
- `/v1/queryBatchByOrderNumber`
- The three `/generate*` API paths

When platform authentication is enabled in the target environment, these calls also require `x-snbps-auth-token`. Check the target environment's authentication configuration before integration testing; a valid station session token alone does not establish that all authentication requirements are met.

`x-snbps-factory-id` carries common factory information. The current factory context is primarily resolved from platform login information or a valid station session; this header alone cannot switch factories.

3.2 Unified Response and Error Handling

Factory Edge Service API generally uses a unified JSON response format, with the following fields:

Field	Type	Mandatory / condition	Description
success	boolean	Response	`true` indicates business success.
respCode	string	Response	`8000` indicates success; see the appendix for other business error codes.
respMsg	string	Response	Status description, affected by the selected language.
respData	object / array / null	Response	Business data for the API; usually `null` when no data is returned or the business operation fails.
respTime	integer (int64)	Response	Unix timestamp in seconds, not a string.

3.2.1 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": null,
  "respTime": 1792108800
}
```

3.2.2 Error Handling

Business exceptions (`ClientApiException`) and expired station sessions are returned with HTTP 200. Callers must check `success` and `respCode` rather than relying on the HTTP status alone.

Parameter binding errors, Bean Validation failures, platform authentication failures, and gateway errors are not guaranteed to return HTTP 200. Handle the actual HTTP status and response content.

3.2.3 Special Responses

On success, `/download` returns a file stream directly rather than the unified JSON format.

4. API Index (29 APIs)

This section lists the current 29 Factory Edge Service APIs, including method, relative path, purpose, and caller identity requirements. See API Call Conventions and Authentication for authentication rules.

No.	Request Method	Relative Path	API Name	Caller Identity
5.1	POST	/v1/device/detail	Query Device Details	Platform authentication depends on deployment configuration.
5.2	POST	/v1/updateDevicesProfile	Update Devices Profile	Platform authentication depends on deployment configuration.
5.3	POST	/v1/deviceData/upload	Upload Device Production Data	Station session; see common conventions for platform authentication.
5.4	POST	/v1/device/information/query	Query Device Information	Station session; see common conventions for platform authentication.
5.5	POST	/v1/matter/onboarding-payloads/recover	Recover Matter QR Code	Station session; see common conventions for platform authentication.
5.6	POST	/v1/testFile/upload	Upload Device Test File	Station session; see common conventions for platform authentication.
5.7	GET	/heartBeat	Connection Heartbeat	Before login / initialization.
5.8	GET	/queryLoginOptions	Query Login Options	Before login / initialization.
5.9	POST	/queryLoginType	Query Programming Station Login Method	Before login / initialization.
5.10	GET	/preLogin	U-Safe Pre-login	Before login / initialization.
5.11	POST	/login	Programming Station Login	Before login / initialization.
5.12	POST	/logout	Programming Station Logout	Provide station context as required.

No.	Request Method	Relative Path	API Name	Caller Identity
5.13	GET	/v1/ queryBatchByOrderNumber	Query Batches by Order Number	Station session; see common conventions for platform authentication.
5.14	POST	/assignBatch	Assign Programming Station Batch	Station session; see common conventions for platform authentication.
5.15	GET	/queryPPCBatchInfo	Query Programming Station Batch Information	Station session; see common conventions for platform authentication.
5.16	GET	/getProgrammingData	Get Dynamic Programming Data	Station session; see common conventions for platform authentication.
5.17	GET	/getMetadata	Get Batch Metadata	Provide station context as required.
5.18	GET	/getPPData	Get Full Programming Data (Compatibility API)	Station session; see common conventions for platform authentication.
5.19	POST	/uploadRequestData	Submit Intermediate Programming Request Data	Station session; see common cdeploymentns for platform authentication.
5.20	POST	/programmingResult	Report Programming Result	Station session; see common conventions for platform authentication.
5.21	POST	/executeApdu	Execute SE APDU Stepwise Programming	Station session; see common conventions for platform authentication.
5.22	POST	/getScriptFile	Get Programming Script URL	Provide station context as required.
5.23	GET	/download	Download File	Provide station context as required.
5.24	POST	/v1/eventLog/upload	Upload Device Event Logs	Station session; see common conventions for platform authentication.
5.25	POST	/generateVerifier	Generate Matter Verifier	Platform authentication depends on deployment configuration.
5.26	POST	/generateOnboardingData	Generate Matter Onboarding Payload	Platform authentication depends on deployment configuration.
5.27	POST	/generateUniqueId	Generate Matter Unique ID	Platform authentication depends on deployment configuration.
5.28	POST	/queryDeviceData	Query Device Data (Deprecated)	Provide station context as required.
5.29	POST	/updateDeviceInfo	Update Device Info (Deprecated)	Provide station context as required.

4.1 API Scope

This index covers the 29 external routes currently registered by `ProgrammingStationController` and `ExternalSystemController`. It excludes administration controllers, the debugging `TestController`, and the entirely commented-out `UsbKeyController`.

`/v1/testData/upload` remains in some filter or authentication exclusion configurations, but no current controller registers it. Upload device production data through `/v1/deviceData/upload`.

5. API List

5.1 Query Device Details

Query device profiles using locator and filter conditions combined with AND logic, and return the groups or fields specified by `queryKeys`. If no local record matches, query historical data and then cloud data. If multiple results refer to different products or `deviceId` values, return error code `8102`. If multiple records belong to the same product and device, return the most recent by production time.

5.1.1 Request Method

`POST`

5.1.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/device/detail

5.1.3 Request Body

The request `body` contains the following parameters:

> **TIP**
> At least one non-empty value is required among `chipUid`, `bleMac`, `serialNumber`, `matterQrcode`, and `matterManualCode` in `deviceLocator`. Other parameters are auxiliary query conditions. All conditions are combined using AND logic. Provide sufficiently precise parameters to identify the target device. `queryKeys` only selects returned data groups or fields; it does not participate in device matching.

Name	Type	Mandatory	Description
deviceLocator	object	Yes	Used to retrieve basic device information. When `deviceLocator` is selected as a query condition, at least one of the following parameters must be provided: `chipUid`, `bleMac`, `serialNumber`, `matterQrcode`, or `matterManualCode`
├──chipUid	string	No	`mcuId` in the programmed device chip
├──bleMac	string	No	Bluetooth MAC address of the chip
├──serialNumber	string	No	Device serial number assigned during programming
├──matterQrcode	string	No	Matter commissioning QR code
├──matterManualCode	string	No	Matter manual commissioning code

Name	Type	Mandatory	Description
filters	object	No	Auxiliary filter conditions used to improve device identification accuracy
├──productionTimeStart	string	No	Device programming production start time. Date format: 2025-12-16T12:02:58+08:00
├──productionTimeEnd	string	No	Device programming production completion time. Date format: 2025-12-17T12:02:58+08:00
├──batchId	string	No	Production batch number
matter	object	No	Matter-related device parameters. Providing this parameter helps improve query accuracy
├──pid	string	No	Matter PID. Including this parameter helps improve device query accuracy
├──vid	string	No	Matter VID. Including this parameter helps improve device query accuracy
customParams	object	No	Custom filter parameters. For details, refer to the description of customParams parameter.
queryKeys	string[]	Recommended	Pass a string array naming groups (such as `matterData`) or fields (such as `chipData.chipUid`). If a local device profile matches but `queryKeys` is omitted or empty, the API returns an empty object `{}` rather than all fields by default. See the queryKeys V2 list for supported keys.

Description of customParams Parameter

This API accepts custom query conditions in customParams for more flexible filtering. To query fields uploaded for a business use case, add the field names and expected values to this object as key-value pairs.

Parameter structure

- Type: JSON object (key-value collection).
- Key: The extension field name to match (for example, `"customData"`).
- Value: The expected value for this field (for example, `"customDataValue"`).

Example

```
{"customData1": "customDataValue1", "customData2": "customDataValue2"}
```

This example indicates querying device records where the reported data customData1 equals "customDataValue1" and customData2 equals "customDataValue2".

Name	Type	Mandatory	Description
key	string	Yes	Used to query the basic key values in the device profile information. The available keys are either system-generated or a set of custom keys uploaded during the programming process
value	string	Yes	Each key corresponds to the value of the query parameter

5.1.4 Response Parameters

> **TIP**
> The following table shows the data returned when querying all `queryKeys`. In practice, querying only the required keys can help improve API performance.

Name	Type	Description
respCode	string	`8000` indicates success; any other value indicates an error. Detailed error information can be found in `respMsg`
respMsg	string	Response messages, such as `NoError` or `DataNotFound`
respData	object	Query result data
├──matterData	object	Matter data related
├──iterations	string	Iteration count
├──commissioningFlows	string	Commissioning flow
├──discoverableMode	string	Device discoverable mode
├──vid	string	Vendor ID
├──pid	string	Product ID
├──discriminator	string	Discriminator
├──enableRotatingDeviceId	string	Enable rotating device identifier
├──manualCode	string	Manual pairing code
├──passcode	string	Pairing code
├──qrcode	string	Matter commissioning QR code
├──salt	string	Salt
├──saltLength	string	Salt length
├──uniqueid	string	Unique device identifier
├──verifier	string	Password verifier
├──serialNumber	string	Matter device programming serial number
├──dacCertMd5	string	DAC certificate MD5
├──cdFileMd5	string	CD file MD5

Name	Type	Description
├──cdFileName	string	CD file name
├──paiCertMd5	string	PAI certificate MD5
├──factoryData	object	Factory data configuration related
├──vendorName	string	Vendor name
├──hardwareVersion	string	Hardware version
├──hardwareVersionString	string	Hardware version string
├──partNumber	string	Part number
├──productUrl	string	Product URL
├──productLabel	string	Product label
├──productName	string	Product name
├──startAddress	string	Start address
├──programmingData	object	Device programming results related
├──programmingStatus	string	Device programming status • Success: `success` • Failure: `failure` • Pending: `pending`
├──programmingLog	string	Programming log
├──programmingTime	string	Programming time
├──chipData	object	Chip data related
├──chipUid	string	mucId in the programmed device chip
├──bleMac	string	Bluetooth MAC address of the chip
├──firmwareData	object[]	Firmware related
├──fwName	string	Firmware name
├──fwMd5	string	Firmware MD5
├──customData	object	Custom data reported by the customer during production

5.1.5 Request Example

```
{
  "deviceLocator": {
    "chipUid": "f9e203b4cf3ce6323637364250 55f321",
    "bleMac": "f9:e2:03:b4:cf:3c:e6:32",
    "serialNumber": "8360224622727172372"
  },
  "filters": {
    "productionTimeStart": "2025-12-16T12:02:58+08:00",
    "batchId": "7603594830282752"
  },
  "matter": {
    "pid": "8001",
    "vid": "FFF2"
  },
  "customParams": {
    "customData1": "nPK3DqGQQwdE3fYxaofURw==",
    "customData2": "1"
  },
  "queryKeys": [
    "matterData.vid",
    "matterData.pid",
    "matterData.manualCode",
    "matterData.passcode",
    "matterData.qrcode",
    "matterData.salt",
    "matterData.uniqueid",
    "matterData.verifier",
    "matterData.serialNumber",
    "matterData.dacCertMd5",
    "matterData.paiCertMd5",
    "factoryData.vendorName",
    "factoryData.hardwareVersion",
    "factoryData.hardwareVersionString",
    "factoryData.partNumber",
    "factoryData.productUrl",
    "factoryData.productLabel",
    "factoryData.productName",
    "programmingData.programmingStatus",
    "chipData.chipUid",
    "chipData.bleMac",
    "firmwareData.fwName",
    "firmwareData.fwMd5"
  ]
}
```

5.1.6 Response Example

Note: This response example shows all result data. In practice, use `queryKeys` to retrieve only the required data.

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "matterData": {
      "vid": "FFF2",
      "pid": "8001",
```

5.1.7 Current Implementation Notes

- **Supported data groups**: `matterData`、`factoryData`、`programmingData`、`chipData`、`firmwareData`、`customData`、`seData`。
- **Field return rules**: `seData` can be returned only as a whole group; specifying `seData.xxx` does not filter its subfields. Unknown groups in `queryKeys` add no data. If a requested field is empty or has not been stored, its value may be empty.
- **Programming data**: `programmingData.programmingStatus` supports `success`, `failure`, and `pending`. The current local data construction logic does not populate `programmingLog` with actual log content; do not rely on it for programming logs.
- **Authentication**: `UkeyPermissionFilter` does not enforce station session validation for this API. See API Call Conventions and Authentication for platform authentication requirements.

5.2 Update Devices Profile

After a factory modifies device programming data, it can use this API to synchronize the updates to OBIS for centralized management.

5.2.1 Request Method

`POST`

5.2.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/updateDevicesProfile

5.2.3 Request Body

The request `body` contains the following parameters:

Name	Type	Mandatory	Description
deviceLocator	object	Yes	Used to retrieve basic device information. When `deviceLocator` is selected as a query condition, at least one of the following parameters must be provided: `chipUid`, `bleMac`, `serialNumber`, `matterQrcode`, or `matterManualCode`
├──chipUid	string	No	`mcuId` in the programmed device chip
├──bleMac	string	No	Bluetooth MAC address of the chip
├──serialNumber	string	No	Device serial number assigned during programming
├──matterQrcode	string	No	Matter commissioning QR code
├──matterManualCode	string	No	Matter manual commissioning code
filters	object	No	Auxiliary filter conditions used to improve device identification accuracy
├──productionTimeStart	string	No	Device programming production start time. Date format: 2025-12-16T12:02:58+08:00
├──productionTimeEnd	string	No	Device programming production completion time. Date format: 2025-12-17T12:02:58+08:00
├──batchId	string	No	Production batch number

Name	Type	Mandatory	Description
matter	object	No	Matter-related device parameters. Providing this parameter helps improve query accuracy
├──pid	string	No	Matter PID. Including this parameter helps improve device query accuracy
├──vid	string	No	Matter VID. Including this parameter helps improve device query accuracy
customParams	object	No	Custom filter parameters. For details, refer to the description of customParams parameter.
updateParams	object[]	No	Pass updates as an array. Each item contains `type`, `key`, and `value`, all `strings`. An empty array does not update fields. See the updateParams description for supported keys and operations.

Description of updateParams Parameter

This API accepts system-supported keys in updateParams to modify specified fields in a device record. Provide the field name, target value, and operation type (type) together as an array.

Parameter structure

- Type: JSON array.
- When type is `add`, a new field record corresponding to the key will be created; if the key already exists, its field value will be updated.
- Some device data supports deletion. When type is `delete`, the field record corresponding to the key will be deleted.
- For details about the keys supported by this parameter, refer to the updatable keys list (updateDevicesProfile).

Example

```
[
    {
        "type": "add",
        "key": "qrcode",
        "value": "MT:XXX-S0XXXX"
    },
    {
        "type": "delete",
        "key": "factoryData.productURL"
    },
    {
        "type": "add",
        "key": "factoryData.qqbb",
        "value": "abcd"
    },
    {
        "type": "add",
        "key": "firmwareData.bootloader-xxx-1.1.s37",
        "value": "00000001"
    }
]
```

The above example indicates:

1. Add the `qrcode` field and set its value to MT:XXX-S0XXXX; if the field already exists in the device, the existing value will be

overwritten.

2. Delete the `productURL` field from `factoryData` of the device.
3. Add the `qqbb` field to `factoryData` of the corresponding device and set its value to `abcd`.
4. Add the firmware bootloader-xxx-1.1.s37 to the firmware list of the device and set its `startAddress` to `00000001`. If a firmware with the same name already exists in the device, update its start address to this value.

5.2.4 Response Parameters

Name	Type	Description
respCode	string	`8000` indicates success; any other value indicates an error. Detailed error information can be found in `respMsg`
success	bool	`True` indicates success
respMsg	string	Response messages, such as `NoError` or `DataNotFound`

5.2.5 Request Example

```
{
  "deviceLocator": {
    "chipUid": "f9e203b4cf3ce632363736425055f321"
  },
  "filters": {
    "productionTimeStart": "2025-12-16T12:02:58+08:00",
    "batchId": "7603594830282752"
  },
  "matter": {
    "pid": "8001",
    "vid": "FFF2"
  },
  "customParams": {
    "customData1": "nPK3DqGQQwdE3fYxaofURw=="
  },
  "updateParams": [
    {
      "type": "add",
      "key": "qrcode",
      "value": "MT:XXX-S0XXXX"
    },
    {
      "type": "delete",
      "key": "factoryData.productURL",
      "value": ""
    },
    {
      "type": "add",
      "key": "factoryData.qqbb",
      "value": "abcd"
    },
    {
      "type": "add",
      "key": "firmwareData.bootloader-xxx.s37",
      "value": "00000000"
    }
  ]
}
```

5.2.6 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respTime": 1765768529
}
```

5.2.7 Operation Rules and Limits

The following requirements apply to fields in `updateParams`:

Field	Type	Mandatory / condition	Description
updateParams[].type	string	By operation	`add` creates or overwrites; `delete` applies only to collection fields that support deletion.
updateParams[].key	string	Yes	A system key or collection prefix listed in Appendix 3.
updateParams[].value	string	For add	Only strings are accepted. Date and integer text must meet the target field format requirements.

Device Location and Update Scope

The device location rules for `deviceLocator`, `filters`, `matter`, and `customParams` are the same as for Query Device Details. Updates affect local device profiles only; they do not query historical or cloud data.

Field Value Rules

- The environment value supports only `test` and `prod`.
- `programmingStatus` supports `Complete`, `Failed`, and `Unreported`. Other values are currently treated as incomplete.

Field Update and Deletion Rules

- **Deletable fields**: `factoryData.*`, `firmwareData.*`, `otherFile.*`, `attachment.*`, and `programmingScript`.
- **Fields that cannot be deleted**: scalar keys and `extend.*` are currently assigned directly from `value`; `delete` is not supported.
- Unknown fields: unknown `keys` are currently skipped and do not necessarily produce a parameter error.

Other Processing Rules

- If `updateParams` is an empty array, no fields are updated, but the service still attempts to read the target device profile and metadata.
- After an update, the record is marked as awaiting synchronization. Receiving the HTTP response does not mean cloud synchronization is complete.

5.3 Upload Device Production Data

Factories can use this API to upload programming, test, and assembly data generated during device production and maintain the corresponding production record by `traceId`. At the end of programming, the API reuses the `programmingResult` processing logic. Test and assembly data are synchronized by a subsequent asynchronous flow.

5.3.1 Request Method

`POST`

5.3.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/deviceData/upload

5.3.3 Request Body

The `Content-Type` for this API is `application/json`. In addition to the common request headers, provide the following header:

Field	Mandatory	Description
x-snbps-session	Yes	Station session `token` returned by `/login`.

5.3.4 Request Body

The request `body` contains the following parameters:

Name	Type	Mandatory / condition	Description
traceId	string	By scenario	Production record trace ID; `uuid` is an accepted alias. In the programming scenario, use the `uuid` returned by `/getProgrammingData`. If omitted, a new record may be created. A supplied value must refer to an existing production record or file task; otherwise the API returns `8006`.
scenarioType	string	Required for test or custom scenarios	Production scenario name, for example `RF-Test`. The `assembly` batch uses assembly, and an existing programming session uses `programming`. Other scenarios return `8069` if this field is absent.
deviceId	string	Required for test or assembly integration	Device MCU ID. If omitted, `deviceRecord.deviceId` is used.
batchId	string	Required for assembly integration	Production batch ID. Only a numeric string is treated as an ID. Assembly is identified by batch type, not by `scenarioType=assembly` alone.
deviceProfileId	string	No	Existing device profile ID; it must correspond to `deviceId`. If omitted, the service matches an existing profile by device ID.
stationId	string	No	Programming Station code. If omitted, the station in the current session is used. It need not be numeric.
factoryId	string	No	Factory ID. For new records, only a numeric string takes effect; otherwise the factory from the current session is used.
deviceSn	string	No	Device serial number.

Name	Type	Mandatory / condition	Description
result	boolean	Recommended for programming	Programming result: `true` for success, `false` for failure. If omitted at the end of programming, it is treated as failure.
failureReason	string	No	Failure reason, stored in the production record.
timestamp	string	No	This API does not use this field to set the production record time; the server generates the creation time.
status	string	No	Custom status. Programming and assembly may generate and overwrite it from the system result; other nonempty values are stored in `customStatus`.
deviceRecord	object	Per scenario integration contract	Device production data; `deviceProfile` is an accepted alias. See deviceRecord parameters for its fields.

5.3.5 deviceRecord Parameters

`deviceRecord` contains data produced by the device at the current production stage.

Name	Type	Required / Condition	Description
deviceId	string	Conditionally required	Device MCU ID; used when top-level `deviceId` in the request body is empty.
firmwareVersion	string	As needed for programming	Firmware version
seid	string	As needed for SE programming	SEID; use lowercase for the field name.
cplc	string	As needed for SE programming	CPLC data
matterData	map	As needed for Matter programming	Matter data actually programmed.
factoryData	map	No	Factory Data actually programmed. Field names must be nonempty and values must be strings.
customData	map	No	Custom data, up to 50 fields. Field names must be nonempty and no longer than 64 characters, and values must be strings; otherwise `8002` is returned. This upload replaces all existing `customData`.

Name	Type	Required / Condition	Description
testData	map	Required for test / assembly integration	Test data; also accepts the legacy field name `diagnosticData`. Values may be text or lists of file references. Fields with the same name are appended when both values are lists; otherwise the new value overwrites the old one.

5.3.6 Scenario Handling Rules

Parameter requirements and handling rules for different production scenarios are as follows:

Scenario	traceId and Batch	Data and Status
Programming	Use the existing programming session `traceId`, usually from `/getProgrammingData`.	Provide `deviceRecord` based on the actual programmed content and explicitly pass `result`. At completion, the API reuses `/programmingResult` handling. Merely setting `scenarioType=programming` does not create a complete programming flow.
Test / Custom	The first upload may omit `traceId`; later uploads use the `traceId` returned in the response. `scenarioType` is required.	Provide `deviceId` and `deviceRecord.testData` as specified by the integration contract. If a matching device profile exists, it is associated; otherwise only a production record may be created and `deviceProfileId` is `null`.
Assembly	`batchId` identifies the assembly batch. `traceId` may come from `/getProgrammingData` or a file task; a new record can also be created if the first upload omits it.	Provide `deviceId` and `deviceRecord.testData`. The scenario is fixed to `assembly`. `testData.result` affects result status and output counts. The current implementation deduplicates successful assembly records for the same device in the same batch.

Parameter Length and Format Limits

Database field length limits are as follows:

Field	Maximum Length
traceId	64 characters
deviceId	128 characters
deviceSn	64 characters
failureReason	1024 characters
status / scenarioType	64 characters

These length limits do not mean that the API automatically validates every request field. ID values must fall within the Java `Long` range. Overlong fields, invalid number formats, or violations of database constraints may cause data persistence to fail. Numeric strings must also satisfy the applicable length and value limits.

Other Handling Rules

- **Programming data**: The integration contract requires at least one of `deviceRecord.firmwareVersion`, `deviceRecord.seid`, `deviceRecord.cplc`, or `deviceRecord.matterData`, but the current API does not enforce this requirement.
- **Test and assembly data**: Upload test data in `deviceRecord.testData`. A top-level `customData` field in the request body is not recognized as `deviceRecord.customData`.

5.3.7 Request Example

Programming Scenario

Use the `uuid` returned by `/getProgrammingData` as `traceId`, and submit the programming result and device data.

```
{
  "traceId": "<uuid returned by getProgrammingData>",
  "deviceId": "DEVICE-001",
  "result": true,
  "deviceRecord": {
    "firmwareVersion": "1.2.3",
    "matterData": {
      "qrcode": "<actual commissioning payload>"
    },
    "customData": {
      "mac": "AA:BB:CC:DD:EE:FF"
    }
  }
}
```

Test Scenario

The first test report may omit `traceId`. Specify the test scenario through `scenarioType` and submit the test data in `testData`.

```
{
  "scenarioType": "RF-Test",
  "deviceId": "DEVICE-001",
  "status": "success",
  "deviceRecord": {
    "testData": {
      "voltage": "3.3",
      "result": "success"
    },
    "customData": {
      "fixture": "A01"
    }
  }
}
```

Assembly Scenario

Use `batchId` to specify the assembly batch. The first report may omit `traceId`.

```
{
  "batchId": "<actual assembly batch ID>",
  "deviceId": "DEVICE-001",
  "deviceRecord": {
    "testData": {
```

5.3.8 Associate Files with Production

To associate a test file, first upload it with `POST /v1/testFile/upload` and save the returned `traceId`. Then call this API with the same `traceId` and reference the file through `fileName` in `testData`.

If an existing production record has a `traceId`, you may pass it when uploading the file. `fileTraceId` is an internal association field and need not be added to the top level of this API request.

Request example:

```
{
  "traceId": "<traceId returned by testFile/upload>",
  "scenarioType": "RF-Test",
  "deviceId": "DEVICE-001",
  "deviceRecord": {
    "testData": {
      "report": [
        {
          "fileName": "report.txt"
        }
      ]
    }
  }
}
```

5.3.9 Response Parameters

This API uses the standard JSON response format. See "Standard Response and Error Handling" for common response fields. `respData` contains the following fields:

Field	Type	Description
traceId	string	Trace ID ultimately used by the server. Pass it unchanged on subsequent uploads.
deviceProfileId	integer (int64) / null	Associated device profile ID; `null` if none is associated.
programmingRecordId	integer (int64)	Device production record ID

5.3.10 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "traceId": "example-trace-id",
    "deviceProfileId": 200,
    "programmingRecordId": 11
  },
  "respTime": 1792108800
}
```

5.3.11 Main Error Codes

Error Code	Description
8002	Custom field does not meet requirements.
8006	`traceId` is not associated with an existing production record or file task.
8007	Data persistence failed.
8032	Batch does not exist.
8037	Device profile creation failed.
8050	Programming Station session expired.
8069	`scenarioType` is missing for a test or custom scenario.

5.3.12 HTTP Call Example and Subsequent Uploads

The following `curl` example uploads test data for the first time. `BASE_URL` contains only the scheme, host, and port, for example `http://edge-host:8005`. `SESSION` is the session token returned by `/login` for the Programming Station. If platform authentication is enabled in the target environment, also supply the `x-snbps-auth-token header`.

```
curl -X POST "$BASE_URL/api/iot-factory-edge-service/v1/deviceData/upload" \
  -H "Content-Type: application/json;charset=utf-8" \
  -H "x-snbps-session: $SESSION" \
  -d '{
    "scenarioType": "RF-Test",
    "deviceId": "DEVICE-001",
    "status": "success",
    "deviceRecord": {
      "testData": {"voltage": "3.3", "result": "success"},
      "customData": {"fixture": "A01"}
    }
  }'
```

Subsequent Upload Rules and Notes

- **Trace ID**: After the first successful upload, save `respData.traceId` from the response. Pass that value at the top level of subsequent uploads to the same production record, and continue to supply `scenarioType`. Independent tests must not reuse an existing `traceId`.
- **Identifiers**: `x-snbps-request-id` is only for request tracing and cannot replace the business `traceId`. Passing a `traceId` that does not exist and is not associated with a file task returns `8006`.
- **Test data**: Under the same `traceId`, list fields with the same name in `testData` are appended. Repeated requests may create duplicate attachment references.
- **Custom data**: Each upload replaces all existing `customData`. On a subsequent upload, include every custom field you need to retain.
- **Repeated requests**: After a network timeout, do not assume that the previous request did not run or that repeated uploads are fully idempotent.

5.4 Query Device Information

This API queries general information, Matter data, and specified custom data in the local device profile. Unlike `/v1/device/detail`, it cannot select returned fields through `queryKeys`.

5.4.1 Request Method

`POST`

5.4.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/device/information/query

5.4.3 Request Headers

In addition to the common request headers, this API requires the following header:

Field	Required	Description
x-snbps-session	Yes	Programming Station session `token` returned by `/login`.

5.4.4 Request Body

The request `body` contains the following parameters. Supply at least one nonempty device identifier.

Field	Type	Required / Condition	Description
deviceId	string	At least one required	Exact match against `deviceId` in the device profile; maximum 128 characters.
chipId	string	At least one required	Exact match against `chipUid` in the device profile; maximum 128 characters.
uniqueId	string	At least one required	Match `uniqueId`, `uniqueid`, or the corresponding `snake_case` fields in Matter data; maximum 128 characters.

5.4.5 Notes

- **Query conditions**: Multiple nonempty device identifiers are combined with AND; all conditions must match.
- **Query scope**: Only local device profiles are queried, not the historical database or cloud. If no record matches, the API returns `8101`.
- **Query result**: If multiple records match, the first result is returned. This does not guarantee identifier uniqueness or that the returned device was programmed successfully.
- **Programming status**: `provisionStatus` currently always returns `Success` and cannot, by itself, establish the device's actual programming status.

5.4.6 Request Example

```
{
  "deviceId": "DEVICE-001"
}
```

5.4.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following data objects:

Field	Type	Description
generalData	object	Device identity, programming information, and product version information.
matterData	object / null	Matter certificate and commissioning data; may be `null` for non-Matter devices.
customData	object	Device serial number, business identifier, MAC address, and test and calibration data.

Fields without recorded values may be empty.

5.4.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "generalData": {
      "deviceId": "DEVICE-001",
      "provisionStatus": "Success",
      "provisionTime": "2026-10-16T02:00:00Z",
      "sourceProgramingBatchId": "10",
      "provisionFactoryId": "20",
      "provisionStationId": "30",
      "productId": "40",
      "productName": "sample product",
      "productVersionId": "50",
      "productVersionName": "1.0"
    },
    "matterData": null,
    "customData": {
      "serialNumber": "SN-001",
      "customId": "CUSTOM-001",
      "macAddress": "AA:BB:CC:DD:EE:FF",
      "factoryTestData": null,
      "calibrationParams": null
    }
  },
  "respTime": 1792108800
}
```

5.4.9 Response Field Descriptions

generalData: General information

> **TIP**
>
> `sourceProgramingBatchId` is the actual response field name; retain the original "`Programing`" spelling.

Field	Type	Description
deviceId	string	Device ID

Field	Type	Description
provisionStatus	string	Programming status; currently always returns `Success`.
provisionTime	string	Programming time in UTC ISO 8601 format.
sourceProgramingBatchId	string	Source programming batch ID
provisionFactoryId	string	Programming factory ID
provisionStationId	string	Programming Station ID; corresponds to the station primary key in the device profile.
productId	string	Product ID
productName	string	Product name
productVersionId	string	Product version ID
productVersionName	string	Product version name

matterData: Matter data

Field	Type	Description
dacCert	string	DAC certificate in its stored Base64 DER or PEM format.
paiCert	string	PAI certificate in its stored Base64 DER or PEM format.
certDeclaration	string	Certification Declaration (CD), Base64 encoded.
discriminator	integer	Matter Discriminator as a decimal number.
spake2plterationCount	integer	SPAKE2+ iteration count.
passcode	string	Matter commissioning passcode.
manualPairingCode	string	Matter manual pairing code.
setupPayload	string	Matter commissioning payload.
spake2pVerifier	string	SPAKE2+ verifier; retain the stored value.
spake2pSalt	string	SPAKE2+ salt; retain the stored value.

customData: Custom data

> **TIP**
> Before returning `factoryTestData` and `calibrationParams`, the API recursively removes defined credential fields and does not return the device private key.

Field	Type	Description
serialNumber	string	Device serial number
customId	string	Business identifier
macAddress	string	MAC address
factoryTestData	JSON	Factory test data
calibrationParams	JSON	Device calibration parameters

5.4.10 Main Error Codes

Error Code	Description
8002	All query parameters are empty.
8007	Stored data could not be parsed.
8050	Authentication failed.
8101	No matching device found.

See the appendix for other error codes.

5.5 Recover Matter QR Code

During assembly, this API uses the input programming batch associated with the assembly batch, Matter VID, PID, Discriminator, and the Rotating Device Identifier (RDI) in BLE advertising to find a successfully programmed local device profile and recover its Matter onboarding data.

5.5.1 Request Method

`POST`

5.5.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/matter/onboarding-payloads/recover

5.5.3 Request Body

In addition to the common request headers, this API requires the following header:

Parameter	Required	Description
x-snbps-session	Yes	Programming Station session `token` returned by `/login`.

5.5.4 Request Body

The request `body` contains the following parameters:

Field	Type	Required	Description
batchId	string	Yes	Assembly batch ID. It must be associated with an input programming batch, have `RUNNING` status, and not be expired.
matterProductId	string	Yes	Matter PID as a hexadecimal string without a `0x` prefix. Do not use `productId` or `pid` as the field name.
matterVendorId	string	Yes	Matter VID as a hexadecimal string without a `0x` prefix. Do not use `vendorId` or `vid` as the field name.
discriminator	string	Yes	Hexadecimal string whose parsed value is in the range `0x000–0xFFF`, for example `0F00`. Do not pass a decimal string.
rotatingDeviceIdentifier	string	Yes	RDI from BLE advertising: 18 bytes (36 hexadecimal characters), without a `0x` prefix. Use the actual advertised value.

5.5.5 Notes

- **Query scope**: Only successfully programmed local device profiles in the input programming batch associated with the assembly batch are queried. The API does not look up RDI in the cloud.
- **Device matching**: The device is matched using VID, PID, Discriminator, and RDI. An RDI mismatch or no matching device returns `8101`.
- **Data format**: VID and PID are matched against their text values in the database. Use the same format as the batch data.

5.5.6 Request Example

```
{
  "batchId": "<assembly batch ID>",
  "matterProductId": "8001",
  "matterVendorId": "FFF2",
  "discriminator": "0F00",
  "rotatingDeviceIdentifier": "<actual 36-character hexadecimal BLE advertising RDI>"
}
```

5.5.7 Response Parameters

This API uses the standard JSON response format. The current implementation returns the following four fields in `respData`, rather than only `setupPayload`:

Field	Type	Description
setupPayload	string	Matter QR-code commissioning payload.
deviceId	string	Device ID
deviceProfileId	integer	Device profile ID
manualCode	string	Matter manual onboarding code. The field name is `manualCode`, not `manualPairingCode`.

5.5.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "setupPayload": "<actual QR code payload>",
    "deviceId": "DEVICE-001",
    "deviceProfileId": 200,
    "manualCode": "<actual manual pairing code>"
  },
  "respTime": 1792108800
}
```

5.5.9 Main Error Codes

Error Code	Description
8002	Invalid Discriminator parameter.
8009	Batch has expired.
8010	Batch is not in RUNNING status.
8032	Assembly batch or its association does not exist.
8050	Authentication failed.
8101	No matching device found.

See the appendix for other error codes.

5.6 Upload Device Test File

This API uploads device test files. After receiving a file, it saves the file locally and creates an asynchronous upload task. The HTTP response only confirms receipt and local processing; it does not mean the file has reached cloud storage.

5.6.1 Request Method

`POST`

5.6.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/testFile/upload

5.6.3 Request Body

This API uses `multipart/form-data` as its Content-Type. In addition to the common request headers, supply the following header:

Parameter	Required	Description
x-snbps-session	Yes	Programming Station session `token` returned by `/login`.

5.6.4 Request Body

This API uploads files through multipart/form-data with the following parameters:

Field	Type	Required	Description
traceId	string (form field)	No	Existing script trace ID, if available; generated automatically if omitted. Pass the returned traceId unchanged to the production data upload API.
files	file[] (multipart parts)	Yes	List of files to upload; include at least one nonempty file. Repeat the files field to upload multiple files in one request. File names must not include a path, must not be `.` or `..`, and must be unique within the request.

5.6.5 Notes

- **File handling**: After receiving a file, the API saves it locally, then creates an asynchronous upload task.
- **Task tracking**: Pass an existing `traceId` if available; otherwise the API generates one. Pass the returned `traceId` unchanged to subsequent production data uploads.
- **Upload status**: A successful HTTP request does not mean the file has reached cloud storage. Errors during the background upload may not appear in the initial HTTP response.
- **File size limits**: File size is limited by the deployment's `multipart` configuration. `application.yml` defaults to 2 GB per file and 4 GB per request; the `dev` configuration sets 200 MB and 250 MB, respectively. Environment variables or external configuration may override the actual limits.

5.6.6 Request Example

```
curl -X POST "$BASE_URL/api/iot-factory-edge-service/v1/testFile/upload" \
  -H "x-snbps-session: $SESSION" \
  -F "files=@./report.txt" \
  -F "files=@./photo.png"
```

5.6.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
traceId	string	File task trace ID.
fileCount	integer	Number of files received in this request.
status	integer	Asynchronous file upload task status: `1` pending sync; `2` uploading; `3` successful; `4` awaiting retry; `5` failed; `6` local file cleaned up.

5.6.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
```

5.6.9 Main Error Codes

Error Code	Description
8057	Invalid upload parameters.
8058	File list or file name does not meet requirements.
8059	Local file storage failed.
8060	Failed to save the file upload task.
8061	Background cloud storage upload failed.
8051	Insufficient storage space or concurrent processing capacity.

Errors during asynchronous background upload may not appear in the initial HTTP response. See the appendix for other error codes.

5.7 Connection Heartbeat

The programming client uses this API to check connectivity to the Edge service.

5.7.1 Request Method

`GET`

5.7.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/heartBeat

5.7.3 Request Parameters

This is an initialization API. It does not require a Programming Station session token in advance and has no request parameters.

5.7.4 Notes

The client may call this API periodically as needed. A successful heartbeat only means the Edge HTTP service is reachable; it does not establish that other business services are healthy.

5.7.5 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/heartBeat
```

5.7.6 Response Parameters

This API uses the standard JSON response format. On success, `respData` is `null`.

5.7.7 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": null,
```

5.8 Query Login Options

For compatibility with older clients, this API queries whether a U-Safe and a production password are required for the batch assigned to the Programming Station.

5.8.1 Request Method

`GET`

5.8.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/queryLoginOptions

5.8.3 Request Parameters

This is an initialization API and does not require a Programming Station session token in advance. Pass the following fields as query parameters:

Field	Type	Required / Condition	Description
usafeSN	string	Provide at least one of usafeSN or stationId.	Legacy U-Safe serial number.
stationId	string	Provide at least one of usafeSN or stationId.	Programming Station code; takes precedence when supplied.

5.8.4 Notes

- **Query conditions**: The Programming Station and its assigned batch must exist.
- **Compatibility**: This API supports older clients. In the newer login flow, call `/queryLoginType` first to determine the Programming Station login method.

5.8.5 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/queryLoginOptions?stationId=STATION-001
```

5.8.6 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
requireUsafe	boolean	Whether U-Safe is required; currently always `true`.
requirePassword	boolean	Whether a production password is required, as determined by the assigned batch setting.

5.8.7 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "requireUsafe": true,
```

5.8.8 Main Error Codes

Error Code	Description
8007	Programming Station or assigned batch not found.

See the appendix for other error codes.

5.9 Query Programming Station Login Method

This API queries the login method for a specified Programming Station and supports reporting client information for compatibility.

5.9.1 Request Method

`POST`

5.9.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/queryLoginType

5.9.3 Request Body

This is an initialization API and does not require a Programming Station session token in advance. The request `body` contains the following parameters:

Field	Type	Required / Condition	Description
factoryId	integer (int64)	Required for cloud factories	In cloud mode, verifies that the specified factory exists and is a cloud factory.
stationId	string	Yes	Programming Station code
clientPcMessage	string	No	JSON object string containing client information. Deprecated since 3.3.2; new clients should report it through `/login`.

5.9.4 Notes

Cloud factory login supports only password or Identity U-Safe authentication.

5.9.5 Request Example

```
{
  "factoryId": 20,
  "stationId": "STATION-001"
}
```

5.9.6 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
loginType	integer	Login method: `1` passwordless; `2` password; `3` Identity U-Safe.

5.9.7 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "loginType": 2
  },
  "respTime": 1792108800
}
```

5.9.8 Main Error Codes

Error Code	Description
8016	Programming Station does not exist.
8036	Invalid cloud factory ID.

See the appendix for other error codes.

5.10 U-Safe Pre-login

This API performs the first step of U-Safe mutual authentication and returns the server certificate, challenge, and signature.

5.10.1 Request Method

`GET`

5.10.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/preLogin

5.10.3 Request Parameters

This is an initialization API and does not require a Programming Station session token in advance. Pass the following fields as query parameters:

Field	Type	Required / Condition	Description
usafeSN	string	Yes	Identity U-Safe serial number.
nonce	string	Yes	Client-generated random challenge.
type	integer	No	Compatibility parameter; the current method does not use its value.
factoryId	integer (int64)	Pass by factory in cloud mode	Used to match the factory scope in cloud mode.

5.10.4 Notes

- **Scope**: This API is for U-Safe mutual authentication, not direct password login.
- **Signature handling**: `sign` in the response is the server signature and cannot be used directly as the client login signature. The client should verify the server's identity, sign `challenge` according to the existing U-Safe authentication protocol, then call `/login`.

5.10.5 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/
preLogin?usafeSN=USAFE-001&nonce=%3C%E5%AE%A2%E6%88%B7%E7%AB%AF%E9%9A%8F%E6%9C%BA%E6%95%B0%3E&factoryId=20
```

5.10.6 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
cert	string	Server authentication certificate.
challenge	string	Server challenge data for the client to sign.
sign	string	Server signature for the client to verify server identity.

5.10.7 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "cert": "<authentication certificate>",
    "challenge": "<server challenge>",
    "sign": "<server signature>"
  },
  "respTime": 1792108800
}
```

5.10.8 Main Error Codes

Error Code	Description
8020	U-Safe does not exist.
8031	U-Safe is unavailable.
8024 / 8026	Authentication or signature verification failed.

See the appendix for other error codes.

5.11 Programming Station Login

This API authenticates the Programming Station and obtains a station session token. After a successful login, the programming client passes the returned `token` in the `x-snbps-session` header on subsequent requests requiring a station session.

5.11.1 Request Method

`POST`

5.11.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/login

5.11.3 Request Body

This is an initialization API and does not require a Programming Station session token in advance. The request `body` contains the following parameters:

Field	Type	Required / Condition	Description
stationId	string	Required for new login flow	When nonempty, authenticates the Programming Station; when omitted, uses the legacy U-Safe authentication flow.
factoryId	integer (int64)	Required for cloud factories	Factory ID
password	string	Required when loginType=2	Password encrypted with the existing RSA public key; do not pass plaintext.
usafeSN	string	Required for loginType=3 or legacy flow	Identity U-Safe serial number; must match the Programming Station.
sign	string	Required for U-Safe authentication	Client signature over the challenge returned by `/preLogin`.
usafeCert	string	No	Compatibility field; not directly used by the current controller branch.
clientPcMessage	string	No	JSON object string containing client information.

5.11.4 Notes

- **Login method**: Follow the authentication flow corresponding to the method returned by `/queryLoginType`.
- **Passwordless login**: `NO_PASSWORD` (`loginType=1`) does not require a password.
- **Password login**: `PASSWORD` (`loginType=2`) requires an RSA-encrypted password.
- **U-Safe login**: `IDENTITY_USAFE` (`loginType=3`) requires a prior `/preLogin` call and a client signature.
- **Session token**: The returned `token` authenticates the Programming Station session and must not be confused with a business operation's `uuid` or `traceId`.

5.11.5 Request Example

```
{
  "factoryId": 20,
  "stationId": "STATION-001",
  "password": "<RSA-encrypted password>",
  "clientPcMessage": "{\"hostname\":\"PS-01\"}"
}
```

5.11.6 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
stationId	string	Programming Station code
token	string	Programming Station session token
factoryId	integer (int64)	Factory ID
partnerCode	string	Tenant code

5.11.7 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "stationId": "STATION-001",
    "token": "<station session token>",
    "factoryId": 20,
    "partnerCode": "<tenant code>"
  },
  "respTime": 1792108800
}
```

5.11.8 Main Error Codes

Error Code	Description
8012	Programming Station already logged in
8014	Incorrect password
8016	Programming Station does not exist
8017	Unsupported login method
8020 / 8021	U-Safe does not exist or does not match
8036	Invalid cloud factory ID

See the appendix for other error codes.

5.12 Programming Station Logout

This API removes the current Programming Station session from the cache to log the station out.

5.12.1 Request Method

`POST`

5.12.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/logout

5.12.3 Request Body

This API should include the following header to identify the current Programming Station and factory context:

Parameter	Required / Condition	Description
x-snbps-session	Required for an effective logout.	Programming Station session `token` returned by `/login`

5.12.4 Request Parameters

This API requires no request parameters.

5.12.5 Notes

- **Session identification**: A valid `x-snbps-session` is required to identify and clear the corresponding Programming Station session.
- **Validation**: This API is not on the mandatory `UkeyPermissionFilter` validation path, but a valid session token is still required to log out effectively.
- **Logout result**: If the Programming Station context cannot be identified, do not assume that the specified station session was cleared.

5.12.6 Request Example

```
curl -X POST "$BASE_URL/api/iot-factory-edge-service/logout" \
  -H "x-snbps-session: $SESSION"
```

5.12.7 Response Parameters

This API uses the standard JSON response format; `respData` is `null`.

5.12.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": null,
  "respTime": 1792108800
}
```

5.13 Query Batches by Order Number

This API queries running batches for a specified order number in the current factory.

5.13.1 Request Method

`GET`

5.13.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/queryBatchByOrderNumber

5.13.3 Request Body

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.13.4 Request Parameters

This API accepts the following query parameter:

Field	Type	Mandatory	Description
orderNumber	string	Yes	Factory order number; it cannot be empty or whitespace only

5.13.5 Notes

- **Query scope**: Only batches in `RUNNING` status for the specified order number in the current factory are queried.
- **Batch assignment**: This API only queries batches; it does not automatically assign the returned batch to the current Programming Station.

5.13.6 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/v1/queryBatchByOrderNumber?orderNumber=ORDER-001
```

5.13.7 Response Parameters

This API uses the standard JSON response format. `respData` is an array of batch information, or an empty array `[]` if no batch matches. Each object contains:

Field	Type	Description
batchId	integer (int64)	Batch ID
batchName	string	Batch name

5.13.8 Response Example


```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": [
    {
      "batchId": 10,
      "batchName": "BATCH-001"
    }
  ],
  "respTime": 1792108800
}
```


5.13.9 Main Error Codes

Error code	Description
8039	Order number is empty
8050	Authentication failed

See the appendix for other error codes.

5.14 Assign Programming Station Batch

This API assigns a specified batch to the currently logged-in Programming Station and synchronizes the station–batch association.

5.14.1 Request Method

`POST`

5.14.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/assignBatch

5.14.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.14.4 Request Body

The request `body` contains:

Field	Type	Mandatory	Description
batchId	integer (int64)	Yes	Batch ID to assign. It must belong to the current factory, be unexpired, and be running.

5.14.5 Notes

- **Batch requirements**: Only an unexpired, running batch in the current factory can be assigned.
- **Assignment restriction**: A Programming Station already assigned through Edge management cannot be reassigned through this API if overriding the association is prohibited.
- **Repeated assignment**: Assigning the same batch to a station already assigned to it returns `8011`.

5.14.6 Request Example

```
{
  "batchId": 10
}
```

5.14.7 Response Parameters

This API uses the standard JSON response format. `respData.batchInfo.batches` is an array of batch details with the same structure as the batch details returned by `/queryPPCBatchInfo`.

5.14.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchInfo": {
      "batches": [
        {
          "batchId": "10",
          "batchName": "BATCH-001",
          "programmingType": "SE",
          "bindType": 2
        }
      ]
    }
  },
  "respTime": 1792108800
}
```

5.14.9 Main Error Codes

Error code	Description
8009	Batch has expired
8010	Batch is closed
8011	Programming Station is already assigned to this batch
8013	Data parsing failed
8016	Programming Station does not exist
8032	Batch does not exist

Error code	Description
8035	Conflict with an assignment made in Edge management
8050	Authentication failed

See the appendix for other error codes.

5.15 Query Programming Station Batch Information

This API queries the batches associated with a Programming Station, programming scripts, and server load information.

5.15.1 Request Method

`GET`

5.15.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/queryPPCBatchInfo

5.15.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.15.4 Request Parameters

This API accepts the following query parameters:

Field	Type	Mandatory	Description
usafeSN	string	No	For legacy U-Safe Programming Station queries
batchId	integer (int64)	No	When positive, queries the specified running batch. If neither parameter is provided, queries by the station in the current session.

5.15.5 Notes

- **Query and assignment**: This API only queries batch information; it does not perform `/assignBatch`.
- **Programming type**: `programmingType` distinguishes programming types such as `MCU`, `SE`, and S`E_MCU`. Use the value in the actual batch.
- **Enum values**: Follow the `ProgrammingType` enum and the actual API response. `MATTER` and `SE_MATTER` in older comments must not be used directly as request enum values.

5.15.6 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/queryPPCBatchInfo
```

5.15.7 Response Parameters

This API uses the standard JSON response format and mainly returns the station's associated batches and server load information.

Field	Type	Description
usafeSN	string	U-Safe serial number
batchInfo.batches	array	Array of batches associated with the Programming Station; may be empty if no batch is available
serverLoadInfo.pressureLevel	integer	Server load level
serverLoadInfo.pressurePercentage	number	Server load percentage

5.15.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchInfo": {
      "batches": [
        {
          "batchId": "10",
          "batchName": "BATCH-001",
          "total": 100,
          "produced": 10,
          "toBeProduced": 90,
          "programmingType": "SE",
          "scriptName": "burn-1.0",
          "scriptMd5": "<md5>",
          "scriptUrl": "<script download URL>"
        }
      ]
    },
    "serverLoadInfo": {
      "pressureLevel": 1,
      "pressurePercentage": 10.0
    }
  },
  "respTime": 1792108800
}
```

5.15.9 Batch Detail Fields

Each object in `batchInfo.batches` contains batch, chip, programming script, and production progress information, including:

Field	Type	Description
batchId	string	Batch ID
batchName	string	Batch name

Field	Type	Description
chips	object[]	Chip information array; `chipPart`, `chipVendor`, and `objectid` are strings
env	string	Environment information
extData	string	Extended data
mark	string	Batch marker
notes	string	Batch notes
orderNo	string	Order number
produced	integer	Quantity produced
toBeProduced	integer	Quantity remaining
total	integer	Total batch quantity
productName	string	Product name
version	string	Product version
region	string	Region
secureDebugReopen	integer	Secure debug switch
supportProtocols	string[]	Supported protocol list
scriptName	string	Programming script name
scriptMd5	string	Programming script MD5 digest
scriptUrl	string	Programming script download URL
vid	string	Matter VID
pid	string	Matter PID
bindType	integer	Assignment method: 1, Edge management; 2, manual client assignment
programmingType	string	Programming type, such as `MCU`, `SE`, or `SE_MCU`; choose the programming flow from the actual response value

5.15.10 Main Error Codes

Error code	Description
8013	Data parsing failed
8015	Programming Station has no assigned batch

Error code	Description
8016	Programming Station does not exist
8050	Authentication failed

See the appendix for other error codes.

5.16 Get Dynamic Programming Data

This API generates device programming data for the batch assigned to the current Programming Station and creates a production record for this programming operation.

5.16.1 Request Method

`GET`

5.16.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/getProgrammingData

5.16.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.16.4 Request Parameters

This API accepts the following query parameters:

Field	Type	Mandatory / condition	Description
uuid	string	No	Trace ID for a single programming operation. If omitted, `getProgrammingData` generates one; retain and reuse it in later calls.
ppcliVersion	string	No	Client script version
usafeSN	string	Legacy flow compatibility	Since 3.1.1, no longer a primary parameter in the new flow. Station information takes precedence when a session station exists.
chipIndex	integer	No	No longer used since 3.1.1.

5.16.5 Notes

- **Programming trace**: Omit `uuid` on the initial call. After obtaining the returned `uuid`, retain and reuse it in subsequent `/uploadRequestData`, `/executeApdu`, or programming result requests.
- **SE programming**: In an SE-only scenario, a programming record is created even if the returned `bundles` array is empty.
- **File download**: Use the `downloadUrl` in the actual response for large files.

- **Sensitive material**: Sensitive production material is not sent as plaintext in a `bundle`.

5.16.6 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/getProgrammingData?ppcliVersion=1.0.0
```

5.16.7 Response Parameters

This API uses the standard JSON response format. `respData` is a batch Bundle object containing:

Field	Type	Description
batchId	string	Batch ID
batchName	string	Batch name
uuid	string	Trace ID for this programming operation
bundles	object[]	Data entries for this programming operation; may be an empty array in an SE-only scenario

5.16.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchId": "10",
    "batchName": "BATCH-001",
    "uuid": "example-programming-trace",
    "bundles": []
  },
  "respTime": 1792108800
}
```

5.16.9 Main Error Codes

Error code	Description
8013	Bundle data parsing failed
8030	No available Programming Station batch
8050	Authentication failed

See the appendix for other error codes.

5.17 Get Batch Metadata

This API returns complete batch metadata and download URLs for firmware and other files so the client can prepare device programming.

5.17.1 Request Method

`GET`

5.17.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/getMetadata

5.17.3 Request Headers

The following header is recommended to resolve the current Programming Station and factory context:

Parameter	Mandatory / condition	Description
x-snbps-session	Recommended	Programming Station session `token` from `/login`

This API is not on the mandatory `UkeyPermissionFilter` validation path.

5.17.4 Request Parameters

This API accepts the following query parameters:

Field	Type	Mandatory / condition	Description
uuid	string	No	Trace ID for a single programming operation. If omitted, a later `getProgrammingData` call may generate one; retain it for later calls.
ppcliVersion	string	No	Client script version
usafeSN	string	Legacy flow compatibility	Since 3.1.1, no longer a primary parameter in the new flow. Station information takes precedence when a session station exists.
chipIndex	integer	No	No longer used since 3.1.1.

5.17.5 Notes

- **Metadata retrieval**: Returns the complete batch Bundle, performs the necessary metadata processing, and removes specified key material.
- **Production record**: This API does not replace `/getProgrammingData` in creating a programming record. The `uuid` in its response does not prove that a new production session was created.
- **Programming Station context**: A valid `x-snbps-session` can be used to resolve the current Programming Station.

5.17.6 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/getMetadata?usafeSN=USAFE-001
```

5.17.7 Response Parameters

This API uses the standard JSON response format. `respData` is a batch Bundle object containing:

Field	Type	Description
batchId	string	Batch ID
batchName	string	Batch name

Field	Type	Description
uuid	1string	Programming trace ID in the response; does not prove that a production record was created
bundles	object[]	Complete batch data entries

5.17.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchId": "10",
    "batchName": "BATCH-001",
    "uuid": "example-programming-trace",
    "bundles": []
  },
  "respTime": 1792108800
}
```

The empty `bundles` array in the example illustrates the response structure only; it does not mean every batch returns an empty array.

5.17.9 Main Error Codes

Error code	Description
8013	Data parsing failed
8030	No available Programming Station batch

See the appendix for other error codes.

5.18 Get Full Programming Data (Compatibility API)

This is the legacy API for retrieving a complete Bundle. Its service method is marked `@Deprecated`. New clients should use `/getMetadata` and `/getProgrammingData`.

5.18.1 Request Method

`GET`

5.18.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/getPPData

5.18.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.18.4 Request Parameters

This API accepts the following query parameters:

Field	Type	Mandatory / condition	Description
uuid	string	No	Trace ID for a single programming operation. In the new flow, `getProgrammingData` generates one if omitted; retain it for later calls.
ppcliVersion	string	No	Client script version
usafeSN	string	Legacy flow compatibility	Since 3.1.1, no longer a primary parameter in the new flow. Station information takes precedence when a session station exists.
chipIndex	integer	No	No longer used since 3.1.1.

5.18.5 Notes

- **Batch query**: This API identifies the batch by `usafeSN`, generates a new `uuid`, and returns the processed complete programming data.
- **No available batch**: The response may be `null` if no usable batch is found.
- **Compatibility**: This API supports legacy clients. New clients should use `/getMetadata` and `/getProgrammingData`.

5.18.6 Request Example

```
GET {BASE_URL}/api/iot-factory-edge-service/getPPData?usafeSN=USAFE-001
```

5.18.7 Response Parameters

This API uses the standard JSON response format. `respData` is a batch Bundle object containing:

Field	Type	Description
batchId	string	Batch ID
batchName	string	Batch name
uuid	string	Programming trace ID returned in this response
bundles	object[]	Processed complete programming data entries

5.18.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchId": "10",
    "batchName": "BATCH-001",
```

The empty `bundles` array in the example illustrates the response structure and is not the actual content for every batch. In an SE-only scenario, `/getProgrammingData` may return an empty `bundles` array.

5.18.9 Common Bundle Structure

Each Bundle object in the `bundles` array contains:

Field	Type	Description
type	string	Bundle type
section	string	Section to which the Bundle belongs
ownerId	string	Associated object ID
authToken	string	Authentication token
authCert	string	Authentication certificate
authSign	string	Authentication signature
items	object[]	List of Bundle data entries

Each entry in the `items` array contains:

Field	Type	Description
itemId	string	Entry ID
key	string	Entry key
objectId	string	Object ID
parentId	string	Parent object ID
fieldType	string	Field type
attribute	JSON object	Entry attributes; structure depends on field type

Bundle fields and content may differ by batch. Clients should follow the actual server response and download URLs; do not treat the empty `bundles` example as actual data for every batch.

5.18.10 Main Error Codes

Error code	Description
8050	Authentication failed

Other exceptional behavior of this legacy API depends on the old flow. See the appendix for specific error codes.

5.19 Submit Intermediate Programming Request Data

This API reports chip execution results for batch Bundle entries and lets the corresponding processor generate the next stage of programming data.

5.19.1 Request Method

`POST`

5.19.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/uploadRequestData

5.19.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.19.4 Request Body

The request `body` contains:

Field	Type	Mandatory / condition	Description
batchId	string	Yes	Batch ID in the current factory
uuid	string	Required by business rules	Programming trace ID returned by `/getProgrammingData`; IDRule number allocation requires a valid, stable `traceId`
bundles	object[]	As needed	Reported Bundle data; if empty, the current implementation returns `respData=null`
bundles[].type	string	Per template	Bundle type
bundles[].section	string	Per template	Section to which the Bundle belongs
bundles[].deviceId	string	Recommended for IDRule	Stable device identifier. If omitted, the service attempts to resolve it from the record for `uuid`. Do not change it after initial number allocation.
bundles[].items	object[]	Required for a nonempty Bundle	List of Bundle entries; empty `items` or `null` entries are not allowed
bundles[].items[].key	string	Yes	Nonempty entry key
bundles[].items[].response	object[]	Per item protocol	List of results from the previous step; fields are defined by `fieldType` and the corresponding processor protocol

5.19.5 Notes

- **Purpose**: This API submits intermediate programming data; it does not report the final programming result.
- **Data structure**: Populate `items[].key` and `response` according to the actual batch template and processor protocol. Do not use the placeholders in the example directly.
- **Device identifier**: In an IDRule scenario, reuse a stable device identifier for the same device. Do not change `deviceId` in later programming steps after the first number allocation.
- **Empty data**: If `bundles` is empty, the current implementation returns `respData=null`.

5.19.6 Request Example

```
{
  "batchId": "10",
  "uuid": "<uuid returned by getProgrammingData>",
  "bundles": [
    {
      "section": "<template section>",
      "deviceId": "DEVICE-001",
      "items": [
        {
          "key": "<template item key>",
          "response": [
            {
              "<protocol field>": "<actual execution result>"
            }
          ]
        }
      ]
    }
  ]
}
```

5.19.7 Response Parameters

This API uses the standard JSON response format. `respData` contains:

Field	Type	Description
batchId	string	Batch ID
batchName	string	Batch name
uuid	string	Programming trace ID for this operation
bundles	object[]	Next-stage programming data entries generated by the corresponding processor

5.19.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchId": "10",
```

5.19.9 Main Error Codes

Error code	Description
8002	Invalid request parameters
8003	Data processing failed
8032	Batch does not exist
8040–8046	Certificate or key agreement error
8065	Invalid IDRule rule
8066	Number range exhausted
8067	State conflict
8068	Stable device identifier is missing
8050	Authentication failed

See the appendix for other error codes.

5.20 Report Programming Result

This API closes an existing device programming record and creates or updates the device profile, while remaining compatible with legacy clients.

5.20.1 Request Method

`POST`

5.20.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/programmingResult

5.20.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.20.4 Request Body

The request `body` contains:

Field	Type	Mandatory / condition	Description
uuid	string	Yes (integration contract)	traceId of an existing programming record
batchId	integer (int64)	Recommended	Used as additional context when the programming record lacks batch information
result	boolean	Explicitly recommended	`true` means success; `false` or `null` is treated as failure
failureReason	string	No	Reason for programming failure
deviceProfile	object	No	Actual CPS programming data. Fields are described under `deviceRecord` in the Production Data Upload API, including `deviceId`, `firmwareVersion`, `seid`, `cplc`, `matterData`, `factoryData`, and `customData`.
changeKeys	object	No	Compatibility field. Accepts `null`, an empty string, or a JSON object; other types return `8002`. The current programming result flow does not use this field further.

5.20.5 Notes

- **Record handling**: If the programming record does not exist or the current factory batch cannot be identified, the current method skips device profile creation and returns normally.
- **Duplicate report**: A repeated report with the same status, or a report for a record already in success status, is not processed again.
- **Result confirmation**: `respCode="8000"` does not necessarily mean a new device profile was created. Confirm through a device query API.
- **Custom data**: `customData` values must be strings and may contain at most 50 entries.
- **Compatibility**: The newer unified production data upload flow can report programming results through `/v1/deviceData/upload`.

5.20.6 Request Example

```
{
  "uuid": "<current programming uuid>",
  "batchId": 10,
  "result": true,
  "deviceProfile": {
    "deviceId": "DEVICE-001",
    "firmwareVersion": "1.2.3",
    "customData": {
      "fixture": "A01"
    }
  }
}
```

5.20.7 Response Parameters

This API uses the standard JSON response format. On success, `respData` is `null`.

5.20.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": null,
  "respTime": 1792108800
}
```

5.20.9 Main Error Codes

Error code	Description
8002	Invalid request parameters
8007	Data processing or storage error
8037	Device profile creation failed
8050	Authentication failed

See the appendix for other error codes.

5.21 SE APDU Stepwise Programming

This API performs stepwise APDU programming of an SE device. The client executes the APDU commands returned by the server in order and submits their results to obtain the next commands. A `nextStep` value of `EOF` means the programming flow is complete.

5.21.1 Request Method

`POST`

5.21.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/executeApdu

5.21.3 Request Headers

In addition to the common request headers, this API requires the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Programming Station session `token` from `/login`

5.21.4 Request Body

The request `body` contains:

Field	Type	Mandatory / condition	Description
batchId	string	Yes	SE configuration batch ID in the current factory. It cannot be omitted in reliance on the station assignment alone.
cplc	string	Provide for SE integration	CPLC protocol value of the SE device, usually 84 characters, used for the SE device record
seId	string	Provide for SE integration	SE identifier. The field name is case-sensitive: use `seId`.
nfcUid	string	For power keys	Protocol hex value of the device physical identifier; `nfcId` is accepted as an input alias. It must remain identical on initial and subsequent steps.
programmingTraceId	string	Optional for BOF; required for other steps	Programming trace ID; `uuid` is accepted as an input alias. In an `SE_MCU` flow, reuse the Matter session `traceId`. The response returns only `programmingTraceId`.
currentStep	string	Yes	Use BOF on the initial call. On subsequent calls, use `nextStep` from the previous response unchanged; do not construct a step cursor.
commandResults	object	Required for subsequent steps	Previous APDU execution result. Omit for BOF. For subsequent steps, `succeed` must be `true` and `results` must correspond to the previous commands.
commandResults.succeed	boolean	Required for subsequent steps	Whether the previous step succeeded. `false` stops the flow and returns `8053`.
commandResults.results	object[]	For subsequent steps, follow the previous response	List of APDU execution results. Each entry contains `index` (integer) and `command`, `checker`, and `result` (strings). `index` must numerically match the string sequence number of the previous command.

5.21.5 Notes

- **Initial call**: Start programming with `currentStep="BOF"` and save `programmingTraceId` from the response for later steps.
- **Command execution**: The client must execute APDU commands in the order of `commands` and submit the actual results of the previous batch in the next request.
- **Step control**: Use the previous response's `nextStep` unchanged in the next request. Do not parse or modify the server step cursor. Stop at `EOF`; do not submit `EOF` again.
- **Session recovery**: `8054` means the current session cannot continue. Restart from `BOF`; do not automatically replay earlier APDU commands.
- **Session lifetime**: The current SE session lifetime is defined by a server configuration constant.
- **Power key**: `nfcUid` (or its input alias `nfcId`) must stay the same on the initial and subsequent steps. Do not use `seId` as the NFC UID.

5.21.6 Request Example

Use `BOF` on the initial call:

```
{
  "batchId": "10",
  "cplc": "<device CPLC>",
  "seId": "<device SEID>",
  "currentStep": "BOF"
}
```

5.21.7 Response Parameters

This API uses the standard JSON response format. `respData` contains:

Field	Type	Description
nextStep	string	Next server step cursor; EOF means the flow is complete
programmingTraceId	string	Trace ID of this SE programming operation
commands	object[]	List of APDU commands to execute in this step
commands[].index	string	APDU command sequence number
commands[].checker	string	APDU response checker
commands[].command	string	APDU hex command to execute

5.21.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "nextStep": "<server step cursor>",
    "programmingTraceId": "example-programming-trace",
    "commands": [
      {
        "index": "1",
        "checker": "<server-provided checker>",
        "command": "<server-provided APDU hex>"
      }
    ]
  },
  "respTime": 1792108800
}
```

5.21.9 APDU Subsequent-Step Request Example

After executing the previous batch of APDU commands, the client submits the results using `programmingTraceId` and `nextStep` returned by the server.

```
{
  "batchId": "10",
  "programmingTraceId": "<programmingTraceId from previous response>",
  "currentStep": "<nextStep from previous response>",
  "cplc": "<same device CPLC>",
  "seId": "<same device SEID>",
  "commandResults": {
    "succeed": true,
    "results": [
      {
        "index": 1,
        "command": "<original command>",
        "checker": "<original checker>",
        "result": "<actual card response hex>"
      }
    ]
  }
}
```

For a power key, include the same `nfcUid` (or input alias `nfcId`) in the initial request and every subsequent request. Do not download the raw production key file separately to the client. Edge prepares the relevant production material and returns it through the APDU commands for the current step. After successful programming reaches `EOF`, use the existing production count and device profile handling flow. If command execution on the card clearly failed, do not report `commandResults.succeed` as `true`.

5.21.10 Power Key Device Binding Rules

- **Device identifiers**: The current power key flow requires both `nfcUid` (input alias `nfcId` is supported) and `seId`.
- **Data format**: Pass both identifiers as even-length hexadecimal strings as required by the device protocol. The current allocation endpoint requires non-empty values of at most 64 characters and converts them to uppercase.
- **Alias usage**: Do not submit `nfcUid` and `nfcId` with different values. Keep the same nfcUid and device identity in the initial call and every continuation request.
- **Material binding**: Production materials are stored against the device binding of factory, batch, NFC UID, and SEID. Even if a device changes `traceId` or resends `BOF`, previously bound materials are reused first.
- **Binding conflict**: If an NFC UID or SEID is already bound but the other device identifier differs, the API returns `8073`.
- **Material exhaustion**: If no production materials are available, the API returns `8072`.
- **Historical data**: If a batch still has an allocation state from legacy Redis or production records that has not been migrated, the API may also return `8073`. Resending BOF does not allocate new materials.

5.21.11 Main Error Codes

Error code	Description
8006	Batch or programming record is missing
8047	SE configuration is missing
8048	Data parsing failed
8049	CPLC-related error
8052	Step execution result does not match
8053	Previous step failed

Error code	Description
8054	Session cannot continue; restart required
8055	APDU processing failed
8056	Configuration decryption failed
8070–8074	Production data, material allocation, or configuration error
8050	Authentication failed

See the appendix for other error codes.

5.22 Get Programming Script URL

This API obtains the programming script download URL for a specified batch.

5.22.1 Request Method

`POST`

5.22.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/getScriptFile

5.22.3 Request Headers

Provide the following request header to resolve the current station and factory context:

Parameter	Mandatory	Description
x-snbps-session	Recommended	Station session `token` returned by `/login`

This API is not on the mandatory validation path list of `UkeyPermissionFilter`.

5.22.4 Request Body

The request `body` contains the following parameters:

Field	Type	Mandatory / condition	Description
batchId	integer (int64)	Required when querying by batch	Batch ID
productId	integer (int64)	No	Compatibility parameter for product-based queries
chipPart	string	As needed	Chip model
chipVendor	string	As needed	Chip vendor

5.22.5 Notes

- **Download URL**: The client should download the programming script from the `fileUrl` returned by the API.
- **Script verification**: An HTTP success response does not mean the client has completed local script download and verification.

5.22.6 Request Example

```
{
  "batchId": 10
}
```

5.22.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following field:

Field	Type	Description
fileUrl	string	Programming script download URL returned by the server

5.22.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
  "fileUrl": "<server-generated script download URL>"
  },
  "respTime": 1792108800
}
```

5.22.9 Main Error Codes

Error code	Description
8022	Failed to get the programming script

See the appendix for other error codes.

5.23 Download File

This API downloads a file by its local file record ID.

5.23.1 Request Method

`GET`

5.23.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/download

5.23.3 Request Headers

Calls requiring factory context should provide the following request header:

Parameter	Mandatory / condition	Description
x-snbps-session	When factory context is required	Valid station session `token` returned by `/login`

5.23.4 Request Parameters

Pass the following fields as query parameters:

Field	Type	Mandatory	Description
fileId	integer (int64)	Yes	Local file record ID
fileName	string	No	Download filename requested by the client

5.23.5 Notes

- **Response format**: On success, the API returns a binary file stream with download headers such as `Content-Disposition`. It does not use the standard `ClientR` JSON response structure.
- **Download URL**: The client can use the full download URL returned by `/getScriptFile` or `/getMetadata` rather than building it manually.
- **Session requirement**: Provide a valid `x-snbps-session` when factory context is required.

5.23.6 Request Example

```
curl -L "$BASE_URL/api/iot-factory-edge-service/download?fileId=100&fileName=burn.zip" \
  -H "x-snbps-session: $SESSION" \
  -o burn.zip
```

5.23.7 Response Parameters

On success, the API returns a binary file stream, not JSON `respData`.

5.23.8 Main Error Codes

Error code	Description
8022	File record does not exist
8023	File download failed

See the appendix for other error codes.

5.24 Upload Device Event Logs

This API receives event logs produced during device programming, filters them by configured priority, and reports them through MQTT. If sending fails, it saves a compensation record.

5.24.1 Request Method

`POST`

5.24.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/v1/eventLog/upload

5.24.3 Request Headers

In addition to the common request headers, provide the following header:

Parameter	Mandatory	Description
x-snbps-session	Yes	Station session `token` returned by `/login`

5.24.4 Request Body

The request `body` contains the following parameters:

Field	Type	Mandatory / condition	Description
programmingTraceId	string	Yes (non-null)	Programming trace ID; `uuid` is also accepted as an input alias
events	object[]	Yes (non-null)	Event log list; an empty array may be ignored
events[].eventName	string	Recommended	Event name
events[].timestamp	string	Recommended	Client event time in the format defined by the event protocol
events[].source	string	Recommended	Event source
events[].priority	string	Recommended	Event priority as a numeric string from 1 to 5; larger values mean higher priority. Empty or invalid values are filtered out.
events[].status	string	Recommended	Event status: `success` or `failure`
events[].content	string	No	Log content; the current implementation truncates it after 256 characters.

5.24.5 Notes

- **Event filtering**: The server filters events by the configured priority threshold. Events below the threshold or with invalid priority are not reported further.
- **Log synchronization**: A successful HTTP request means only that the API received and processed the request; it does not mean every event has been synchronized to the cloud.
- **Failure compensation**: If MQTT sending fails, the server saves a compensation record.

5.24.6 Request Example

```
{
  "programmingTraceId": "<current programming traceId>",
  "events": [
    {
      "eventName": "ProgrammingFinished",
      "timestamp": "2026-10-16T10:00:00+08:00",
      "source": "PS",
      "priority": "5",
      "status": "success",
      "content": "Burn completed"
```

5.24.7 Response Parameters

This API uses the standard JSON response format. On success, `respData` is `null`.

5.24.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": null,
  "respTime": 1792108800
}
```

5.24.9 Main Error Codes

Error code	Description
8050	Authentication failed

Request parameter binding or validation may also produce errors. See the appendix for other error codes.

5.25 Generate Matter Verifier

This API calls the Matter SDK to generate a Matter passcode, Salt, and Verifier.

5.25.1 Request Method

`POST`

5.25.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/generateVerifier

5.25.3 Request Headers

The current `application.yml` does not exclude this API from platform authentication. If platform authentication is enabled in the deployment, provide the following header:

Parameter	Mandatory / condition	Description
x-snbps-auth-token	When platform authentication is enabled	Platform authentication token, distinct from the station session token `x-snbps-session`

5.25.4 Request Parameters

This API requires no request parameters.

5.25.5 Notes

- **Generation parameters**: The current implementation fixes `saltLen` at 32 bytes and `iterations` at 1000. They cannot be overridden in the request body.
- **Runtime dependency**: The corresponding native Matter SDK must be deployed on the server.
- **Status interpretation**: The outer `respCode` and `respData.status` have different meanings. The former indicates the API business

response status; the latter is the status returned by the Matter SDK.

- **Example data**: Numeric values in the response example illustrate field types only.

5.25.6 Request Example

```
POST {BASE_URL}/api/iot-factory-edge-service/generateVerifier
```

5.25.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
status	integer	Status code returned by the Matter SDK
passcode	integer	Matter passcode
salt	string	Base64-encoded Salt
verifier	string	Base64-encoded Verifier

5.25.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "status": 0,
    "passcode": 20202021,
    "salt": "<Base64 salt>",
    "verifier": "<Base64 verifier>"
  },
  "respTime": 1792108800
}
```

5.26 Generate Matter Onboarding Payload

This API calls the Matter SDK with specified Matter parameters to generate a QR code onboarding payload and manual pairing code.

5.26.1 Request Method

`POST`

5.26.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/generateOnboardingData

5.26.3 Request Headers

The current `application.yml` does not exclude this API from platform authentication. If platform authentication is enabled in the deployment, provide the following header:

Parameter	Mandatory / condition	Description
x-snbps-auth-token	When platform authentication is enabled	Platform authentication token, distinct from the station session token `x-snbps-session`

5.26.4 Request Parameters

The API accepts the following query or form parameters, not a JSON request body.

Field	Type	Mandatory	Description
vid	integer	Yes	Matter Vendor ID (VID) as a decimal integer, unlike the hexadecimal text used by the Matter payload recovery API
pid	integer	Yes	Matter Product ID (PID) as a decimal integer
passcode	integer	Yes	Matter passcode
commissioningFlow	integer	Yes	Matter SDK commissioning flow parameter
discoveryMode	integer	Yes	Matter SDK device discovery mode parameter

5.26.5 Notes

- **Parameter transport**: Although this API uses `POST`, all five parameters are bound with `@RequestParam`. Pass them through URL query or form parameters, not a JSON request body.
- **Parameter validation**: The underlying Matter SDK determines the valid range for each parameter.
- **VID/PID format**: This API uses decimal integers, unlike the hexadecimal strings used by `/v1/matter/onboarding-payloads/recover`.

5.26.6 Request Example

```
POST {BASE_URL}/api/iot-factory-edge-service/
generateOnboardingData?vid=65522&pid=32769&passcode=20202021&commissioningFlow=0&discoveryMode=2
```

5.26.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
status	integer	Status code returned by the Matter SDK
discriminator	integer	Matter onboarding `Discriminator`
qrcode	string	Matter QR code onboarding payload
manualcode	string	Matter manual pairing code; note that the field name `manualcode` is all lowercase

5.26.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "status": 0,
    "discriminator": 3840,
    "qrcode": "<SDK-generated QR code payload>",
    "manualcode": "<SDK-generated manual pairing code>"
  },
  "respTime": 1792108800
}
```

5.27 Generate Matter Unique ID

This API calls the Matter SDK to generate a Matter Unique ID.

5.27.1 Request Method

`POST`

5.27.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/generateUniqueId

5.27.3 Request Headers

The current `application.yml` does not exclude this API from platform authentication. If platform authentication is enabled in the deployment, provide the following header:

Parameter	Mandatory / condition	Description
x-snbps-auth-token	When platform authentication is enabled	Platform authentication token, distinct from the station session token `x-snbps-session`

5.27.4 Request Parameters

This API requires no request parameters or request body.

5.27.5 Notes

- **Generation**: The Matter SDK generates the Unique ID; the client supplies no generation parameters.
- **Status interpretation**: A successful Matter SDK status is usually `0`, while the outer API business success code is `8000`. They have different meanings.

5.27.6 Request Example

```
POST {BASE_URL}/api/iot-factory-edge-service/generateUniqueId
```

5.27.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
status	integer	Status code returned by the Matter SDK
result	string	Base64-encoded Unique ID

5.27.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "status": 0,
    "result": "<Base64 uniqueId>"
  },
  "respTime": 1792108800
}
```

5.28 Query Device Data (Legacy API, Deprecated)

This API supports device data queries by legacy clients. New clients should use `/v1/device/detail`, or `/v1/device/information/query` for station query scenarios.

5.28.1 Request Method

`POST`

5.28.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/queryDeviceData

5.28.3 Request Body

Provide the following request header to resolve the current station and factory context:

Parameter	Mandatory / condition	Description
x-snbps-session	Recommended	Station session `token` returned by `/login`

This API is not on the mandatory validation path list of `UkeyPermissionFilter`.

5.28.4 Request Body

The request `body` contains the following parameters:

Field	Type	Mandatory / condition	Description
batchId	string	Yes	Batch ID
paramKey	string	Yes	Key identifying the parameter group
paramField	string	Yes	Field to locate

Field	Type	Mandatory / condition	Description
paramValue	string	Yes	Field value identifying the device
queryKeys	string[]	Yes	See the queryable keys list (queryKeys V1) for supported keys.

5.28.5 Notes

- **Compatibility**: This API was declared deprecated in the v1.3 document and remains only for legacy clients.
- **Query source**: If the batch was deleted, a file cannot be read, or no local device profile matches, the API may query historical records or cloud data.
- **Query parameters**: `queryKeys` must follow the legacy Bundle query protocol. Do not use field definitions from the newer QueryKeys V2 directly.

5.28.6 Request Example

```
{
  "batchId": "10",
  "paramKey": "<legacy protocol key>",
  "paramField": "<legacy protocol field>",
  "paramValue": "<actual value>",
  "queryKeys": [
    "<legacy query key>"
  ]
}
```

5.28.7 Response Parameters

This API uses the standard JSON response format. `respData` contains the following fields:

Field	Type	Description
batchId	string	Batch ID
paramKey	string	Parameter Key used by the query
paramField	string	Field used by the query
paramValue	string	Field value used by the query
data	map<string,map<string,object>>	Device information in the legacy data structure

5.28.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {
    "batchId": "10",
    "paramKey": "<legacy protocol key>",
    "paramField": "<legacy protocol field>",
    "paramValue": "<actual value>",
```

5.28.9 Main Error Codes

Error code	Description
8006	Batch does not exist
8003	Legacy device information query failed

See the appendix for other error codes.

5.29 Update Device Information (Legacy API, Deprecated)

This API supports updates using the legacy device data model. New clients should use `/v1/updateDevicesProfile`.

5.29.1 Request Method

`POST`

5.29.2 Request URL

{BASE_URL}/api/iot-factory-edge-service/updateDeviceInfo

5.29.3 Request Headers

Provide the following request header to resolve the current station and factory context:

Parameter	Mandatory / condition	Description
x-snbps-session	Recommended	Station session `token` returned by `/login`

This API is not on the mandatory validation path list of `UkeyPermissionFilter`.

5.29.4 Request Body

The request `body` contains the following parameters:

Field	Type	Mandatory / condition	Description
batchId	integer (int64)	Yes	Batch ID; note that this differs from the string type used by the legacy query API
paramKey	string	Yes	Key identifying the parameter group
paramField	string	Yes	Field to locate
paramValue	string	Yes	Field value identifying the device
data	map<string,map<string,string>>	Yes	Device data to update

5.29.5 Notes

- **Compatibility**: This API uses the legacy device data model. New clients should use `/v1/updateDevicesProfile`.

- **Batch handling**: If the specified batch does not exist, the current service returns directly, while the controller may still return the `data` from the request.
- **Update confirmation**: `respCode="8000"` and an echoed `data` value do not prove that data was persisted. Do not infer a successful device information update solely from the API response.

5.29.6 Request Example

```
{
  "batchId": 10,
  "paramKey": "<legacy protocol key>",
  "paramField": "<legacy protocol field>",
  "paramValue": "<actual value>",
  "data": {}
}
```

5.29.7 Response Parameters

This API uses the standard JSON response format. `respData` is the `data` object from the request, of type `map<string, map<string, string>>`. It only echoes request data; it does not represent a fresh read of persisted state.

5.29.8 Response Example

```
{
  "success": true,
  "respCode": "8000",
  "respMsg": "NoError",
  "respData": {},
  "respTime": 1792108800
}
```

6. Appendix

6.1 Appendix One: Queryable Keys (queryKeys V2)

Data item	Key
Matter commissioning: PBKDF iterations (1000)	matterData.iterations
Matter commissioning: salt length (32 bytes)	matterData.saltLength
Matter commissioning flow type (0 = standard flow)	matterData.commissioningFlows
Device discovery mode	matterData.discoverableMode
Matter Vendor ID	matterData.vid
Matter Product ID	matterData.pid
Discriminator	matterData.discriminator
Matter commissioning: rotating device ID enabled (true = enabled)	matterData.enableRotatingDeviceId

Data item	Key
Matter manual pairing code	matterData.manualCode
Matter passcode	matterData.passcode
Matter onboarding QR code	matterData.qrcode
Matter salt used by the password derivation algorithm	matterData.salt
Matter device Unique ID (Base64 encoded)	matterData.uniqueid
Matter Verifier	matterData.verifier
Matter programming device serial number	matterData.serialNumber
Matter DAC certificate MD5	matterData.dacCertMd5
Matter PAI certificate MD5	matterData.paiCertMd5
Matter CD filename	matterData.cdFileName
Matter CD file MD5	matterData.cdFileMd5
Factory data; see the OBIS product configuration UI	factoryData.vendorName
Factory data; see the OBIS product configuration UI	factoryData.hardwareVersion
Factory data; see the OBIS product configuration UI	factoryData.hardwareVersionString
Factory data; see the OBIS product configuration UI	factoryData.partNumber
Factory data; see the OBIS product configuration UI	factoryData.productUrl
Factory data; see the OBIS product configuration UI	factoryData.productLabel
Factory data; see the OBIS product configuration UI	factoryData.productName
Factory data; see the OBIS product configuration UI	factoryData.startAddress
Programming status	programmingData.programmingStatus
Programming log	programmingData.programmingLog
Programming time	programmingData.programmingTime
MCU ID in the programmed chip	chipData.chipUid
Chip Bluetooth MAC address	chipData.bleMac

Data item	Key
Firmware name (returns firmware list)	firmwareData.fwName
Firmware MD5 (returns firmware list)	firmwareData.fwMd5
Custom field	customData.<custom field>

6.1.1 Additional Query Keys

> **TIP**
> This API follows `queryKeys V2` naming. Matter data uses `matterData.manualCode`, `matterData.qrcode`, and `matterData.uniqueid`, which differ from `manualPairingCode` and `setupPayload` in the "Query Device Information" API; do not mix them.

Data item	Key	Description
SE data	seData	Returns the complete SE data object in the device profile
Query entire group	matterData / factoryData / programmingData / chipData / firmwareData / customData	A group name without a dot queries its supported fields; the exact response depends on the current implementation.

6.2 Appendix Two: Error Code List

The following table lists client business error codes used by the APIs and their descriptions.

- Each API uses only a subset of these codes. See the corresponding API description for causes and handling.
- Parameter validation, platform authentication, and framework processing may produce other error codes not listed here.
- An SDK status of 0 has a different meaning from `respCode="8000"` in the standard API response; do not confuse them.

respCode	Enum name	Description
8000	NO_ERROR	Operation succeeded (NoError)
8001	REQUEST_FAILED	Request failed (RequestFailed)
8002	PARAM_ERROR	Invalid parameter (ParamError)
8003	METHOD_ERROR	Invalid method (MethodError)
8004	AUTH_ERROR	Authentication failed (AuthError)
8005	USAFE_TYPE_ERROR	Invalid U-Safe type (USafeTypeError)
8006	DATA_NOT_FOUND	Data not found (DataNotFound)

respCode	Enum name	Description
8007	DATA_ERROR	Invalid data (DataError)
8008	NOT_ALLOWED	Operation not allowed (NotAllowed)
8009	BATCH_EXPIRED_ERROR	Batch expired
8010	BATCH_STATUS_CLOSED	Batch closed
8011	STATION_BATCH_HAS_BIND	Batch already assigned to this station
8012	STATION_HAS_LOGIN	Station already logged in (StationHasLogin)
8013	BATCH_BUNDLE_PARSE_ERROR	Failed to parse the Bundle file generated for the batch
8014	STATION_PASSWORD_ERROR	Incorrect station password (StationPasswordError)
8015	STATION_NOT_BIND_BATCH	Station has no assigned batch
8016	STATION_NOT_EXIST	Station does not exist
8017	UNKNOWN_LOGIN_TYPE	Unknown login type
8018	FACTORY_NOT_EXIST	Factory does not exist
8019	FACTORY_STATUS_LOCKED	Factory is locked
8020	USAFE_NOT_FOUNT	U-Safe not found
8021	STATION_USAFE_NOT_MATCH	U-Safe does not match station ID
8022	FETCH_BURN_SCRIPT_ERROR	Failed to get programming script
8023	DOWNLOAD_BURN_SCRIPT_ERROR	Failed to download programming script
8024	PRELOGIN_AUTH_ERROR	Pre-login authentication failed
8025	HSM_CERT_SYNC_REQUIRED	HSM authentication certificate not found. Edit factory HSM information in the cloud to trigger certificate synchronization.
8026	SIGN_VERIFY_ERROR	Signature verification failed
8027	BATCH_HAS_DONE	Batch completed
8028	BATCH_FILE_NOT_EXIST	Operation failed: product batch file does not exist
8029	BATCH_IMPORT_FAILED	Failed to import batch
8030	PS_BURN_STATION_RECORDING_FINISHED	U-Safe SN has completed programming or is not assigned to a batch
8031	USAFE_UNAVAILABLE	U-Safe unavailable

respCode	Enum name	Description
8032	BATCH_NOT_FOUND	Batch not found
8033	BATCH_DOWNLOAD_STATUS_NOT_WAIT	Batch download status is not pending
8034	DEVICES_PROGRAMMER_DATA_UPLOAD_ERROR	Failed to upload device adapter data
8035	STATION_HAS_EDGE_BIND	Station already assigned a batch from the Edge Service
8036	CLOUD_FACTORY_ID_ERROR	Invalid cloud factory ID
8037	DEVICE_PROFILE_GENERATE_ERROR	Failed to generate device profile
8038	UNSUPPORTED_CERTIFICATE_FORMAT	Unsupported certificate format
8039	ORDER_NUMBER_CANNOT_BE_EMPTY	Order number must not be empty
8040	CERT_CHAIN_VERIFY_FAILED	Silicon Labs certificate chain verification failed
8041	PUBKEY_SIGNATURE_VERIFY_FAILED	Chip temporary public key signature verification failed
8042	ECDH_KEY_AGREEMENT_FAILED	ECDH key agreement failed
8043	SESSION_KEY_NOT_FOUND	Session key does not exist or has expired
8044	KEY_WRAP_FAILED	Key encapsulation failed
8045	DAC_PUBKEY_SIGNATURE_VERIFY_FAILED	DAC public key signature verification failed
8046	BUNDLE_PUBLIC_KEY_NOT_FOUND	Bundle public key material for the specified keyCode not found
8047	SE_PROFILE_NOT_FOUND	SE Profile for the batch not found
8048	SE_PROFILE_PARSE_ERROR	Failed to parse SE Profile
8049	CPLC_INVALID	Invalid CPLC; length must be 84
8050	PERMISSION_CHECK_DENY	Authorization verification failed; obtain verification permission again
8051	SERVER_PERFORMANCE_LIMIT	Concurrency limit reached; ask the factory administrator to check the server
8052	APDU_SESSION_INVALID	Invalid executeApdu session: command result for the current step does not match the expected result
8053	APDU_STEP_FAILED	Previous APDU execution failed
8054	APDU_RESTART_REQUIRED	APDU session invalid or expired; restart programming for this device
8055	APDU_PROCESS_FAILED	Failed to process APDU Profile step

respCode	Enum name	Description
8056	SE_PROFILE_DECRYPT_ERROR	Failed to decrypt SE Profile
8057	TEST_FILE_PARAM_ERROR	Invalid test file upload parameters
8058	TEST_FILE_MANIFEST_ERROR	Invalid test file manifest
8059	TEST_FILE_STORAGE_ERROR	Failed to save test file locally
8060	TEST_FILE_TASK_ERROR	Failed to save test file upload task
8061	TEST_FILE_UPLOAD_ERROR	Failed to upload test file to cloud storage
8064	TEST_DATA_TASK_ERROR	Failed to save test data report task
8065	ID_RULE_INVALID	Invalid ID Rule description
8066	ID_RULE_RANGE_EXHAUSTED	ID Rule allocation range exhausted
8067	ID_RULE_CONFLICT	ID Rule status conflicts with batch description
8068	ID_RULE_DEVICE_KEY_REQUIRED	A stable device identifier is required to parse the ID Rule
8069	SCENARIO_TYPE_NOT_BE_NULL	scenarioType must not be empty
8070	DATA_INVALID	Invalid production data
8071	KEY_DECRYPT_FAILED	Failed to decrypt batch protection key
8072	DATA_EXHAUSTED	Production data exhausted
8073	ASSIGNMENT_CONFLICT	Production data allocation conflicts with batch or device
8074	PROFILE_INVALID	Programming requires a PERSONALIZE operation and corresponding Applet selection information
8101	DEVICE_NOT_FOUND	Device not found; check query parameters
8102	MULTI_DEVICES_FOUND	Multiple devices matched; add filters
8103	QUERY_CONDITION_REQUIRED	Specify at least one valid query condition in deviceLocator

6.3 Appendix Three: Updatable Keys (updateDevicesProfile)

Keys supported by the Update Devices Profile API:

Data item	Key	Value description
Device extension field	extend.<extension field key>	Supported extension fields: vid, pid, chipId, qrcode, pairingCode
env	environment	test / prod

Data item	Key	Value description
Production time	manufactureTime	• string • Time format: 2020-11-11T01:11:11+08:00
Version name	productVersion	string
Batch name	productBatch	string
Factory name	factory	string
Programming station name	programmingStation	string
Programming status	programmingStatus	Complete / Failed / Unreported
DAC certificate serial number	dacSerialNo	string
DAC certificate commonName	dacCommonName	string
DAC certificate VID	dacVid	string
DAC certificate PID	dacPid	string
Subject key identifier	subjectKeyIdentifier	string
Authority key identifier	authorityKeyIdentifier	string
DAC effective date	notBefore	• string • Time format: 2020-11-11T01:11:11+08:00
DAC expiration date	notAfter	• string • Time format: 2020-11-11T01:11:11+08:00
Pairing code	pairingCode	string
QR code	qrcode	string
DAC expiration time (date, time, and time zone)	expiryDate	• string • Time format: 2020-11-11T01:11:11+08:00
Remaining days of DAC validity	leftDays	string
Issued DAC certificate	certificate	string
Field in factoryData	factoryData.<key name>	• string • Supports deletion of the corresponding key in factory data.

Data item	Key	Value description
Script filename	programmingScript	• string • Supports deletion of the script file with this name. Only one script file may exist; uploading a new script filename overwrites the prior file record.
Firmware	firmwareData.<firmware name>	• The startAddress of the named firmware may be updated. • Deletion of the named firmware is supported.
otherFiles	otherFile.<filename>	• The key of the named file in otherFile may be updated. • Deletion of the named file is supported.
attachmentFiles	attachment.<filename>	• The key of the named attachment may be updated. • Deletion of the named file is supported.

6.4 Appendix Four: Queryable Keys (queryKeys V1)

> **TIP**
> - If a data item is not configured for the product, the API returns an empty value for it.
> - The digit `1` in the key `fw1.fileName` denotes the first firmware file.

Data item	Key
CD file MD5	cdFile.md5
CD filename	cdFile.fileName
Commissioning flow	matterCommissioningParameter.commissioningFlows
DAC MD5	dacTemplate.md5
Discovery mode	matterCommissioningParameter.discoverableMode
Discriminator	matterCommissioningParameter.discriminator
EnableRotatingDeviceId	matterCommissioningParameter.enableRotatingDeviceId
hardwareVersion	hardwareVersion
hardwareVersionString	hardwareVersionString
mcuId	mcuId
PAI MD5	paiCert.md5
partNumber	partNumber
PID	pid
productLabel	productLabel

Data item	Key
productUrl	productUrl
salt	matterCommissioningParameter.salt
softwareVersion	softwareVersion
softwareVersionString	softwareVersionString
SPAKE2+Iterations	matterCommissioningParameter.iterations
UniqueID	matterCommissioningParameter.uniqueId
vendorName	vendorName
verifier	matterCommissioningParameter.verifier
VID	vid
QR code	matterCommissioningParameter.qrcode
Firmware filename	fw1.fileName
Device programming result	programmingStatus
Manual pairing code	matterCommissioningParameter.manualCode
Original passcode	matterCommissioningParameter.passcode

6.5 Typical Business Call Flows

This section gives typical API call sequences for station programming, testing, and assembly. See each API description for its request parameters, response structure, and handling rules.

6.5.1 Station Programming

After login, batch query, and assignment, the station obtains programming data, programs the device, and reports the result. A typical call flow is:

```
queryLoginType
    ↓
 preLogin (as needed)
    ↓
 login
    ↓
 queryPPCBatchInfo / queryBatchByOrderNumber
    ↓
 assignBatch (as needed)
    ↓
 getMetadata
    ↓
 getProgrammingData
    ↓
 uploadRequestData (as required by programming items)
```

For SE programming, also observe the following rules:

- SE-only scenario: A production record may be created at the BOF stage.
- Mixed SE_MCU programming: Reuse the same `traceId` from the MCU or Matter programming stage, then execute SE programming operations through `executeApdu` until EOF.

6.5.2 Testing and Assembly

Testing and assembly data is reported through `/v1/deviceData/upload`. To associate a test file, upload the file first, then submit the related production data. A typical call flow is:

```
login
   ↓
 testFile/upload (as needed)
   ↓
 deviceData/upload
```

When calling these APIs, note:

- **Testing**: For the first upload without attachments, `traceId` may be omitted, but `scenarioType` is required. Use the `traceId` returned by the API for subsequent uploads.
- **File association**: To attach a test file, first upload it through `/v1/testFile/upload`, then use the returned `traceId` in `/v1/deviceData/upload`.
- **Assembly**: Use the `batchId` of the actual assembly batch and report the execution result through `deviceRecord.testData`.result.

Depending on the business flow, a scan may first call `/v1/matter/onboarding-payloads/recover` to recover Matter onboarding data. Use `/v1/device/information/query` when detailed device information is needed.

Version: v3.4.0 (Latest)

OnBoard™ IoT Security FW Signing and Pushing CLI - v1.0.0

1. Revision Record

Version	Modified Date	Notes
v1.0.0	2025/02/17	Initial release

2. Overview

OnBoard™ IoT Security (OBIS) FW Signing and Pushing CLI is a command-line tool built specifically for OBIS, dedicated to firmware signing and pushing. It integrates several core functions, including key configuration based on the PKI (Public Key Infrastructure) certificate signing, KMS (Key Management System) firmware signing, public key export, and firmware pushing to OBIS.

This article introduces the common commands of the OBIS FW Signing and Pushing CLI and provides parameter descriptions and usage examples to help you efficiently complete firmware signing and pushing operations.

3. Syntax

`snb [command] [subcommand] [parameters]`

4. Command List

4.1 Key Configuration Command

Used to set the Access Key and Secret Key.

4.1.1 Command

`config`

4.1.2 Parameters

Parameters	Type	Mandatory	Description
`--accessKey`	string	Yes	Set the Access Key, which can be viewed in the user page in OBIS.
`--secretKey`	string	Yes	Set the Secret Key, which can be viewed in the user page in OBIS.

4.1.3 Example

```
snb config --accessKey <AK> --secretKey <SK>
```

4.2 Firmware Signing Command

Used to perform a signing operation on input data with the specified key pair.

4.2.1 Command

`kms`

4.2.2 Subcommand

`sign`

4.2.3 Parameters

Parameters	Type	Mandatory	Description
`--algorithm`	string	Yes	Configure the signing algorithm, currently supporting `ecdsa_sha_256`.
`--keyId`	string	Yes	Specify the key ID to use for the signing operation.
`--inputFile`	string	No	Specify the target file to be signed.
`--inputData`	string	No	Input the data to be signed, in hexadecimal string format.

Parameters	Type	Mandatory	Description
`--inputHash`	string	No	Input the pre-hashed data to be signed, in hexadecimal string format.
`--outputFile`	string	No	Specify the output file for the signature result, in the **.der** format. Defaults to standard output (stdout).
`--resourcePackageId`	string	No	Specify the resource package ID for the product. This parameter is required when accessing the product keys.

TIP

- At least one of the parameters (`inputFile`, `inputData`, or `inputHash`) must be provided.
- When outputting to standard output (stdout), the signature result in the **.der** format is represented as a hexadecimal string.

4.2.4 Example

```
snb kms sign --algorithm ecdsa_sha_256 --keyId <keyID> --
inputFile ./firmware.bin --outputFile ./signedResult.der
```

4.3 Public Key Export Command

Used to export the public key of a specified key pair.

4.3.1 Command

`kms`

4.3.2 Subcommand

`exportPubKey`

4.3.3 Parameters

Parameters	Type	Mandatory	Description
`--keyId`	string	Yes	Specify the key ID to export.
`--outputFormat`	string	Yes	Specify the output format for the exported key, options are `PEM` or `DER`. Default is `DER`.
`--outputFile`	string	Yes	Specify the output file for the exported key. Defaults to standard output (stdout).
`--resourcePackageId`	string	No	Specify the resource package ID for the product. This parameter is required when the Access Key used belongs to a personal account.

> **TIP**
>
> When outputting to standard output (stdout), the signature result in the **.der** format is represented as a hexadecimal string.

4.3.4 Example

```
snb kms exportPubKey --keyId <keyID> --outputFormat PEM --
outputFile pubKey.pem
```

4.4 Certificate Signing Command (such as Matter DAC)

Used to sign a certificate signing request (CSR) file using the specified certificate template.

4.4.1 Command

`pki`

4.4.2 Sub-command

`sign`

4.4.3 Parameters

Parameters	Type	Mandatory	Description
`--inputFormat`	string	Yes	Specify the input format (`PEM` or `DER`). Default is `PEM`.

Parameters	Type	Mandatory	Description
`--certTemplateId`	string	Yes	Specify the certificate (such as Matter DAC) template ID.
`--outputFormat`	string	Yes	Specify the output file format(`PEM` or `DER`). Default is `DER`.
`--csrFile`	string	No	Specify the path of the CSR file.
`--csrContent`	string	No	Provide the content of the CSR file.
`--outputFile`	string	No	Specify the output filename. Defaults to standard output (stdout).

TIP

- At least one of the parameters (`csrFile` or `csrContent`) must be provided.
- When outputting to standard output (stdout), the signature result in the **.der** format is represented as a hexadecimal string.

4.4.4 Example

```
snb pki sign --csrFile ./csr.der --inputFormat DER --
certTemplateId 1F118749-EEB1-11EF-A430-B8CEF6C25058
```

4.5 Firmware Push Command

Used to push the signed firmware file to OBIS.

4.5.1 Command

`obis`

4.5.2 Subcommand

`push`

4.5.3 Parameters

Parameters	Type	Mandatory	Description
`--file`	string	Yes	Specify the file to be pushed to OBIS.
`--fileType`	string	Yes	Specify the type of the file being pushed: `Application` (default), `Bootloader`, or `Others`.
`--resourcePackageId`	string	Yes	Specify the resource package ID under the target product in OBIS.
`--env`	string	Yes	Specify the target environment for pushing: `TEST` or `PROD`.
`--startAddress`	string	No	Specify the firmware programming start address, in hexadecimal format starting with `0x`.

Parameters	Type	Mandatory	Description
`--version`	string	No	Set the firmware file version, with a maximum length of 16 characters. Allowed characters include text, numbers (0-9), letters (a-z, A-Z), dot (.), underscore (_), and hyphen (-).

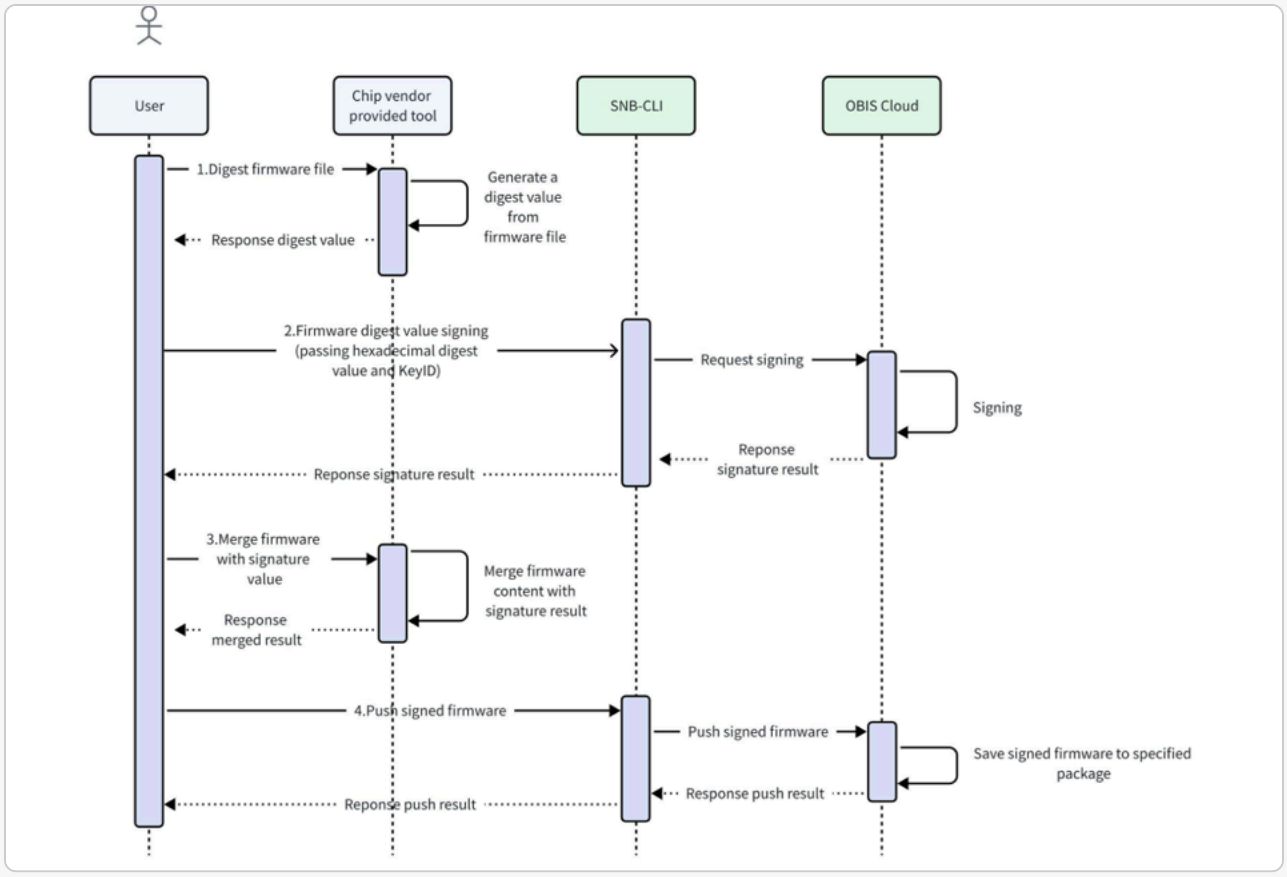
TIP

- When the file being pushed is in the **.bin** format, the `startAddress` parameter is required.
- The combination of `version`, `env`, and `file` must be unique and can't be duplicated.

4.5.4 Example

```
snb obis push --file ./lighting.s37 --fileType Application --
resourcePackageId <id> --env TEST --version 1.0.0
```

5. Execution Flow Example



Version: v3.4.0 (Latest)

OnBoard™ IoT Security Programming CLI - v3.0.5

1. Revision Record

Version	Modified Date	Notes
v1.0.0	2025/05/12	Initial release
v3.0.0	2026/01/22	Added the following nine commands: • Log out of Edge Service • Query Login Type • Query Batch List • Assign Batch • Push Programming Events • Extract Programming Script • View Log Configuration • Start Log Collection • Stop Log Collection Deleted the following three commands: • Query Identity U-Safe Information • Query Tool Version • Download Tool Update Package Updated the following two commands: • Added the `--stationId` parameter for the "Log in to Edge Service" command • Added the `scriptUrl` field to the output of the "Query Batch Information" command
v3.0.1	2026/03/13	The `--stationId` parameter in the "Log in to Edge Service" command is now optional instead of mandatory
v3.0.2	2026/03/17	In the Query Programming Script command section, add instructions for downloading the programming script, and update the corresponding command example
v3.0.3	2026/06/02	• Added the Download Large Firmware command • Added the `--stationVersion` parameter for the "Log in to Edge Service" command
v3.0.4	2026/09/19	• Added PPCLI (Programming Process Control CLI) and the dedicated Telink programming interface, with UI (Programming Station client) integration guidance • Added the complete call flow from login, batch and programming script preparation through device programming • Added process startup, output reading, result determination, and error handling guidance for programming • Updated related command parameters and programming flow descriptions

Version	Modified Date	Notes
v3.0.5	2026/09/22	Added the Execute Batch APDU Operation command, including parameters, call examples, HTTP mapping, response, and exit code descriptions

2. Overview

OnBoard™ IoT Security (OBIS) Programming CLI is a command-line tool built specifically for OBIS, dedicated to supporting the device programming process. It offers a comprehensive set of features: you can use it to log in to the Edge Service, query Identity U-Safe list, retrieve and upload batch data, upload programming results, and query or download programming scripts.

This article introduces common OBIS Programming CLI commands, with parameter descriptions and usage examples to help you perform device programming and related operations. It also explains how the UI (Programming Station client) starts device programming through PPCLI (Programming Process Control CLI) or a dedicated programming interface, and covers the full call flow from login, batch and programming script preparation through device programming and result handling.

3. OBIS Programming CLI Syntax

`obiscli [command] [subcommand] [parameters]`

> **INFO**
>
> Strings containing spaces in command-line arguments must be enclosed in double quotes `"`; otherwise, the command may fail to parse.
>
> - Correct Example: `--chipVendor="Test Labs"`
> - Error Example: `--chipVendor=Test Labs`

4. OBIS Programming CLI Commands

4.1 Query Tool Help

Used to query the usage instructions of the command-line tool and the list of available parameters.

4.1.1 Parameter

`--help`

4.1.2 Example

```
obiscli.exe --help
positional arguments:
                OBIS CLI Tool Command
    login       Login to OBIS Local Service.
    logout      logout to OBIS Local Service.
    usafe       OBIS usafe commands.
    batch       OBIS batch commands.
    script      OBIS batch commands.
    obisexe     OBIS commands.
    logCollect  OBIS batch commands.
    addPath     add sys Path.

options:
```

4.2 Log in to Edge Service

Used to log in to the Edge Service.

4.2.1 Command

`login`

4.2.2 Parameters

Parameters	Type	Mandatory	Description
`--ip`	string	Yes	Programming Station client IP, default value: 127.0.0.1
`--port`	string	Yes	Programming Station client port, default value: 32333
`--stationId`	string	No	Programming Station ID
`--stationVersion`	string	No	Version of the Programming Station client
`--factorytype`	string	No	Factory type, default value: local
`--password`	string	No	Login password, required only when password-based login is enabled
`--usafesn`	string	No	U-Safe serial number

4.2.3 Example

```
# no-password login:
obiscli login --ip=192.168.40.100 --port=32333 --stationId 81045379
# u-safe login:
obiscli login --ip=192.168.40.100 --port=32333 --usafesn=00003F00AB013668 --stationId 81045379
# password login:
obiscli login --ip=192.168.40.100 --port=32333 --password=12345678 --stationId 81045379
or
obiscli login --ip=192.168.40.100 --port=32333 --password=12345678
output:
{
    "stationid": "94221070",
    "token": "b69a9fe7-9df4-4bdc-819e-9b84a7bc0b23",
    "tokenexpire": "unlimited"
}
```

4.3 Log out of Edge Service

Used to log out of the Edge Service.

4.3.1 Command

`logout`

4.3.2 Example

```
# Logout
obiscli logout
```

4.4 Query Login Type

Used to query the login type for the Edge Service.

4.4.1 Command

`login`

4.4.2 Subcommand

`queryType`

4.4.3 Parameters

Parameters	Type	Mandatory	Description
`--ip`	string	Yes	Programming Station client IP, default value: 127.0.0.1
`--port`	string	Yes	Programming Station client port, default value: 32333
`--stationId`	string	Yes	Programming Station ID

4.4.4 Example

```
obiscli login queryType --ip=192.168.40.205 --port=32333 --stationId=97123586

output◈◈1 No password, 2 Password, 3 U-safe◈
{
    "loginType": 3
}
```

4.5 Query Login Options

Used to query the specific login options for the Edge Service.

4.5.1 Command

`login`

4.5.2 Subcommand

`queryoptions`

4.5.3 Parameters

Parameters	Type	Mandatory	Description
`--ip`	string	Yes	Programming Station client IP, default value: 127.0.0.1
`--port`	string	Yes	Programming Station client port, default value: 32333
`--usafesn`	string	Yes	U-Safe serial number
`--factoryType`	string	No	Factory type, default value: local
`--stationId`	string	No	Programming Station ID

4.5.4 Example

```
obiscli login queryoptions --factoryType=local --ip=192.168.40.100 --port=32333 --usafesn=00003F00AB013668
```

4.6 Query Identity U-Safe List

Used to list the Identity U-Safes inserted in the local device.

4.6.1 Command

`usafe`

4.6.2 Subcommand

`list`

4.6.3 Example

```
obiscli usafe list
output⏎
{
    "usafelist": [
        {
            "usafesn": "0001BC00B86DA2BB"
        }
    ]
}
```

4.7 Query Batch Information

Used to query information about the batch corresponding to the devices to be programmed.

4.7.1 Command

`batch`

4.7.2 Subcommand

`query`

4.7.3 Example

```
obiscli batch query

output⏎
{
    "batches": [
        {
            "batchId": "7346273795440640",
            "batchName": "UI-jason-0925",
            "chips": [
                {
                    "chipPart": "QPG6200",
                    "chipVendor": "Qorvo",
                    "objectid": "4bb81efb504248fe813c83a4ed4602ac"
                }
            ],
            "env": "test",
            "extData": "VID : 0xFFF2  PID : 0x8001",
```

4.8 Query Batch List

Used to query the batch list associated with a factory order number.

4.8.1 Command

`batch`

4.8.2 Subcommand

`queryList`

4.8.3 Parameter

Parameter	Type	Mandatory	Description
`--orderNumber`	string	Yes	Order number

4.8.4 Example

```
obiscli batch queryList --orderNumber "LDS-19990101-1030BTC"

output
[
    {
        "batchId": "8725582734950400",
        "batchName": "Test-Order-5"
    }
]
```

4.9 Assign Batch

Used to bind the batch to the programming station.

4.9.1 Command

`batch`

4.9.2 Subcommand

`assign`

4.9.3 Parameter

Parameter	Type	Mandatory	Description
`--batchId`	string	Yes	Batch ID

4.9.4 Example

```
obiscli batch assign --batchId 7176076344164352

output
{
    "batches": [
        {
```

4.10 Query Batch Full Data

Used to query the complete data to be programmed into a device. This command is typically called by PPCLI or a vendor programming script; the UI does not need to call it directly.

4.10.1 Command

`batch`

4.10.2 Subcommand

`getfulldata`

4.10.3 Example

```
obiscli batch getfulldata
```

4.11 Query Batch Fixed Data

Used to query fixed data to be programmed into a device. This command is typically called by PPCLI or a vendor programming script; the UI does not need to call it directly.

4.11.1 Command

`batch`

4.11.2 Subcommand

`getFixData`

4.11.3 Example

```
obiscli batch getFixData
```

4.12 Query Batch Changed Data

Used to query changing data to be programmed into a device. This command is typically called by PPCLI or a vendor programming script; the UI does not need to call it directly.

4.12.1 Command

`batch`

4.12.2 Subcommand

`getChangingData`

4.12.3 Example

```
obiscli batch getChangingData

output
{
    "batchId": "7115488079380480",
    "batchName": "V1.8.5 Dual Button 0906 MP",
    "bundles": [
```

4.13 Push Batch Data

Used to push data to the Edge Service. This command is typically called by PPCLI or a vendor programming script; the UI does not need to call it directly.

4.13.1 Command

`batch`

4.13.2 Subcommand

`putdata`

4.13.3 Parameters

Parameters	Type	Mandatory	Description
`--batchId`	string	Yes	Batch ID
`--chipVendor`	string	Yes	Chip vendor name, for example: Silicon Labs
`--chipPart`	string	Yes	Chip part
`--data`	json	Yes	Push data
`--uuid`	string	Yes	Universally unique identifier

4.13.4 Example

```
obiscli batch putdata --uuid=24a1c3da-459a-429b-a717-29989f926d43 --batchId=4808741360762880 --chipVendor="Silicon Labs" --chipPart=EFR
[{\"items\": [{\"key\": \"dacTemplate\", \"response\": [{\"csr\":
\"MIHmMIGNAgEAMCsxKTAnBgNVBAMMIERBQyA1SFNmblpxVSBNdmlkOjE0NDEgTXBpZDowMTIzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEXeJ5k1UtgF7YJDRm37XvHu47m
FNF1JjcucbEgaIR+KAAMAoGCCqGSM49BAMCA0gAMEUCIQDeR2rM9FOdCg1GTJyAOpQR2FtARVwIw3nEjXv9t7mg6wIgBcvUbH1G8NAlB/I7rOY48b/Fgnf5UkEOMx/7eekcU0k=
```

4.14 Execute Batch APDU Operation

Used to execute an APDU (Application Protocol Data Unit) operation through the platform service in programming flows that require APDU interaction. This command is typically called by PPCLI or a vendor programming script; the UI does not need to call it directly.

4.14.1 Command

`batch`

4.14.2 Subcommand

`executeApdu`

4.14.3 Parameters

Parameter	Type	Mandatory	Description
`--batchId`	string	Yes	Current programming batch ID. It must match the batch to which this device data belongs.

Parameter	Type	Mandatory	Description
`--uuid`	string	Yes	`uuid` of this device data or programming record. Use the identifier obtained in the current programming flow; do not substitute the adapter `serialno`.
`--data`	string	No	Additional request fields as a JSON object. After parsing, they are merged into the top level of the request body. Examples include `programmingTraceId` and command response data required by the server protocol. Follow the actual server protocol for field names, types, and which stages require them.

TIP

- `--batchId` and `--uuid` are not marked required by the current argument parser, but the command does not fill them in from the assigned batch or data cache. Supply valid `batchId` and `uuid` values. If omitted, their request values are `null`; final business validation is performed by the server.
- Log in first and obtain identifiers for the current batch and device data. OBIS Programming CLI reads the service address and session token from local configuration; do not pass login parameters again.
- `--data` must be a valid JSON object, not a file path, plain string, or array. The current implementation merges its fields directly into the top level of the request body, without adding a `data` layer. Duplicate fields overwrite existing values, so do not repeat `batchId` or `uuid` in `--data`.
- This command does not support `--chipVendor`, `--chipPart`, or `--serialno`.
- Whether `executeApdu` must be called more than once, how to submit the previous command response, and how to determine when the APDU flow is complete depend on the server protocol.

4.14.4 Examples

Without additional request fields:

```
obiscli batch executeApdu --batchId="<BATCH_ID>" --uuid="<UUID>"
```

When programmingTraceId is required, add other business fields according to the server protocol:

```
obiscli batch executeApdu --batchId="<BATCH_ID>" --uuid="<UUID>" --
data="{\"programmingTraceId\":\"<PROGRAMMING_TRACE_ID>\"}"
```

The two examples show alternative argument forms; they do not mean the command must be run twice in succession. Follow the actual server protocol for the use of `--data` and the business fields it contains.

The `\"` escaping in `--data` above applies to the Windows `cmd.exe` example. When an application invokes the process API, pass the JSON string directly in the argument array, without additional shell quotes or escaping.

4.14.5 HTTP Mapping

OBIS Programming CLI sends `executeApdu` requests to the following endpoint:

Item	Description
Method	`POST`
Path	`/api/iot-factory-edge-service/executeApdu`
Content-Type	`application/json`
Session	`x-snbps-session` uses the current login token

Item	Description
Request ID	`x-snbps-request-id` is generated automatically by OBIS Programming CLI
Timestamp	`x-snbps-timestamp` is generated automatically by OBIS Programming CLI

Local mode uses the saved IP and port. Cloud mode uses the saved host and automatically includes `factoryId` when configured.

For example, a command containing `programmingTraceId` produces this request body:

```
{
  "uuid": "<UUID>",
  "batchId": "<BATCH_ID>",
  "programmingTraceId": "<PROGRAMMING_TRACE_ID>"
}
```

4.14.6 Response and Exit Codes

After parsing the HTTP response, OBIS Programming CLI formats `respData` itself as JSON and exits with code `0` when `respCode` is the string `"8000"` and `respData` is not `null`.

The CLI does not also output the outer `respCode` and `respMsg`. The server defines the business structure of respData; the current CLI does not prescribe fixed fields.

Exit code	Description
`0`	This interface call succeeded. The calling script must still process the response according to the business protocol; this does not establish that the full device programming flow is complete.
`1`	`--data` is not valid JSON text.
`45`	The HTTP client call failed. The CLI outputs `executeApdu failed: Network error`
`46`	`respData` is missing or `null` in a successful response. The current implementation does not return this error solely for an empty object `{}` or empty array `[]`.
Integer converted from the server `respCode`	When `respCode` is not `"8000"`, the CLI outputs `respMsg` and exits with the corresponding business error code.
`200`	An uncaught exception occurs, for example when the response cannot be parsed or a business error code cannot be converted to an integer.

After the APDU step, PPCLI or the vendor programming script continues the original programming flow and reports the final programming result with batch `putresult`. `executeApdu` does not replace batch `putresult`.

4.15 Push Programming Results

Used to push programming results to the Edge Service. This command is typically called by PPCLI or a vendor programming script; the UI does not need to call it directly.

4.15.1 Command

`batch`

4.15.2 Subcommand

`putresult`

4.15.3 Parameters

Parameters	Type	Mandatory	Description
`--batchId`	string	Yes	Batch ID
`--changeKeys`	string	Yes	If service data is not used, enter the key. Supported keys are defined in the list of queryKeys V2
`--result`	string	Yes	Programming results
`--uuid`	string	Yes	Universally unique identifier

4.15.4 Example

```
obiscli batch putresult --batchId=4808741360762880 --uuid=24a1c3da-459a-429b-a717-29989f926d43 --result=success --
changeKeys=''
```

4.16 Push Programming Events

Used to push programming events to the Edge Service.

4.16.1 Command

`batch`

4.16.2 Subcommand

`uploadEvent`

4.16.3 Parameters

Parameters	Type	Mandatory	Description
`--batchId`	string	Yes	Batch ID
`--uuid`	string	Yes	Unique device identifier
`--event`	string	No	Programming events

4.16.4 Example

```
obiscli batch uploadEvent --batchId=4808741360762880 --uuid=24a1c3da-459a-429b-a717-29989f926d43 --event
"{\"uuid\":\"24a1c3da-459a-429b-a717-29989f926d43\", \"events\": [{\"eventName\": \"Generate Trace ID\",
\"timestamp\": \"2026-01-09T09:46:02.672Z\", \"source\": \"script\", \"priority\": \"1\", \"status\": \"success\",
\"content\": \"\"}, {\"eventName\": \"Fetch Batch Dynamic Data\", \"timestamp\": \"2026-01-09T09:46:04.538Z\",
\"source\": \"script\", \"priority\": \"1\", \"status\": \"success\", \"content\": \"\"}, {\"eventName\": \"Fetch
Device ID\", \"timestamp\": \"2026-01-09T09:46:07.340Z\", \"source\": \"script\", \"priority\": \"1\", \"status\":
\"success\", \"content\": \"\"}, {\"eventName\": \"Fetch CSR\", \"timestamp\": \"2026-01-09T09:46:27.433Z\",
\"source\": \"script\", \"priority\": \"1\", \"status\": \"success\", \"content\": \"\"}, {\"eventName\": \"Program
Factory Data\", \"timestamp\": \"2026-01-09T09:46:33.631Z\", \"source\": \"script\", \"priority\": \"1\", \"status\":
\"success\", \"content\": \"\"}, {\"eventName\": \"Report Programming Result\", \"timestamp\":
```

4.17 Query Programming Script

> **TIP**
>
> It is recommended to directly use the Query Batch Information command (`batch query`) to obtain the batch information for the devices to be programmed, retrieve the script download link, and then execute the Download Programming Script command (`script download`) to perform the download.

Used to check whether a programming script exists for the batch to be programmed.

4.17.1 Command

`script`

4.17.2 Subcommand

`query`

4.17.3 Parameters

Parameters	Type	Mandatory	Description
`--batchId`	string	Yes	Batch ID
`--chipPart`	string	No	Chip part
`--chipVendor`	string	No	Chip vendor name, for example: Silicon Labs
`--productId`	string	No	Product ID

4.17.4 Example

> **TIP**
>
> When `scriptExist` is `false`, the script should be downloaded by executing the Download Programming Script command (`script download`); if `true`, downloading is not required.

```
obiscli script query --batchId=4808741360762880 --chipVendor="Silicon Labs" --chipPart=EFR32MG24B210F1536IM48
output:
{
    "scriptExist": bool,
    "path": ...
}
```

4.18 Download Programming Script

Used to download the programming script.

4.18.1 Command

`script`

4.18.2 Subcommand

`download`

4.18.3 Parameters

Parameters	Type	Mandatory	Description
`--url`	string	Yes	Download link for the programming script
`--extractFolder`	string	No	Extraction path after downloading the programming script
`--savePath`	string	No	Save path after downloading the programming script

4.18.4 Example

```
obiscli script download --url="http://192.168.40.171:8005/api/iot-factory-edge-service/
download?fileId=1866310684527935298&fileName=0d232bf966e516f4bf2a75e1880e59ee.zip" --
savePath="C:\\Users\\Administrator\\AppData\\Roaming\\SNB\\chipVendorCmd" --
extractFolder="C:\\Users\\Administrator\\AppData\\Roaming\\SNB\\chipVendorCmd"
```

4.19 Extract Programming Script

Used to extract the programming script.

4.19.1 Command

`script`

4.19.2 Subcommand

`extract`

4.19.3 Parameters

Parameters	Type	Mandatory	Description
`--extractFolder`	string	No	Extraction path of the file
`--zipFile`	string	No	Path of the compressed file, must be in the **.zip** format

4.19.4 Example

```
obiscli script extract --zipFile="C:\\Users\\Administrator\\AppData\\Roaming\\SNB\\chipVendorCmd\\Silicon Labs.zip"
--extractFolder="C:\\Users\\Administrator\\AppData\\Roaming\\SNB\\chipVendorCmd"
```

4.20 Log Configuration

Used to configure parameters related to log collection.

4.20.1 Command

`logCollect`

4.20.2 Subcommand

`config`

4.20.3 Parameters

Parameters	Type	Mandatory	Description
`--logLevel`	string	No	Log level control
`--collectLogPath`	string	No	Directory for storing log files, default: **C:\Users\<User Name>\AppData\SNB**
`--collectLogSuffix`	string	No	Suffix for log files, default: `.log`
`--mqttIp`	string	No	IP of the MQTT Broker (server)
`--mqttPassword`	string	No	Password for connecting to the MQTT Broker user
`--mqttPort`	string	No	Port number of the MQTT Broker
`--mqttUser`	string	No	User name for connecting to the MQTT Broker

4.20.4 Example

```
obiscli logCollect config --logLevel=INFO
```

4.21 View Log Configuration

Used to view parameters related to log collection.

4.21.1 Command

`logCollect`

4.21.2 Subcommand

`showConfig`

4.21.3 Example

```
obiscli logCollect showConfig
output
{
  "DEFAULT": {
    "log_level": "INFO",
    "log_file_path": "C:\\Users\\Administrator\\AppData\\Roaming\\iot-log-collecter\\collecter.log",
    "log_rotation": "2 hour",
    "log_retention": "1 days",
    "send_times_save_status": "1",
    "collect_log_path": "C:\\Users\\Administrator\\AppData\\Roaming\\SNB",
    "collect_log_suffix": "[\".log\"]",
    "send_log_mode": "1",
    "source_type": "\"PS\" # ps:programming station  es:edge service"
  },
  "MQTT": {
    "broker": "192.168.40.144",
    "port": "32222",
    "user": "snowball",
    "password": "vX4hR9tV7iE8pO9d",
    "connect_crt": "",
    "connect_key": "",
```

4.22 Start Log Collection

Used to start log collection.

4.22.1 Command

`logCollect`

4.22.2 Subcommand

`start`

4.22.3 Example

```
obiscli logCollect start
output◈
iot-log-collect.exe run successfully.
```

4.23 Stop Log Collection

Used to stop log collection.

4.23.1 Command

`logCollect`

4.23.2 Subcommand

`stop`

4.23.3 Example

```
obiscli logCollect stop
output◈
iot-log-collecter.exe stop successfully.
```

4.24 Download Large Firmware

Used to download large firmware files.

4.24.1 Command

`downloadFw`

4.24.2 Parameters

Parameters	Type	Mandatory	Description
`--url`	string	Yes	Download link for the large firmware file
`--savePath`	string	No	Save path after downloading the large firmware file

4.24.3 Example

```
obiscli downloadFw --url <URL> --savePath <Path>
```

5. PPCLI Programming Interface

5.1 Overview

PPCLI (Programming Process Control CLI) controls the device programming flow. To integrate device programming, the UI (Programming Station client) first uses OBIS Programming CLI to log in, assign a batch, and prepare the programming script. It then uses the PPCLI entry point supplied with the programming script package to list adapters and start device programming.

PPCLI or the vendor programming script uses OBIS Programming CLI to retrieve batch data, request certificates, perform APDU interactions when needed, and report programming results. The UI generally does not need to call those interfaces directly.

5.2 Python PPCLI

This applies when the programming script package includes `ppcli.py` and its Python runtime. `ppcli.py` is the PPCLI entry point; `process.py` contains the vendor programming implementation that it calls. The UI should start programming through `ppcli.py` rather than executing `process.py` directly. Follow the package documentation for the actual entry point.

5.2.1 Prerequisites

Before calling Python PPCLI, ensure that:

- You have logged in to the Edge Service and assigned the current batch;
- The programming script package matches the current batch and chip model, has been downloaded and prepared, and contains all required dependencies;
- The child process working directory (`cwd`) is the actual entry directory containing `ppcli.py`, rather than the ZIP download directory or UI installation directory. Relative paths are resolved from this directory;
- The current process and its child processes can find the correct `obiscli.exe` version through `PATH` and use the same Windows user and configuration environment as the earlier OBIS Programming CLI calls, so they share the login session and current batch assignment. Using an absolute OBIS CLI path only in the UI does not ensure that PPCLI can find `obiscli.exe` internally;
- The adapter driver is installed and connected, and the target device is powered on;
- Parameters such as `--type`, `--speed`, chip vendor, and chip model match the actual programming script package.

5.2.2 List Adapters

Used to list currently available programmers.

5.2.2.1 Command

`adapter`

5.2.2.2 Subcommand

`list`

5.2.2.3 Parameters

Parameter	Type	Mandatory	Description
`--chipVendor`	string	Yes	Chip vendor name recognized by the delivered package, usually from batch `chips[].chipVendor`. Map it according to the package contract if needed; do not assume that case and spaces are interchangeable.
`--type`	string	Yes	Adapter type. Use the value specified by the programming script package.

5.2.2.4 Example

> **TIP**
> `--type=1` is the value used in this example. Use the value specified by the actual programming script package.

```
".\python-3.12.9-embed-amd64\python.exe" ".\ppcli.py" adapter list --chipVendor="<CHIP_VENDOR>" --type=1
Output
{
  "adapterList": [
    {
      "serialno": "<SERIALNO>"
    }
  ]
}
```

After a successful query, select the target adapter from `adapterList` and pass its `serialno` unchanged to the `program` command. Treat `serialno` as a string. Preserve leading zeros, for example `0008`. Do not start device programming if `adapterList` is empty. Treat missing required fields or an unparseable response as an adapter query failure. An exit code of `0` alone does not establish that an adapter is available.

5.2.3 Start Programming

Used to start device programming with the selected adapter.

5.2.3.1 Command

`program`

5.2.3.2 Parameters

Parameter	Mandatory	Type	Description
`--serialno`	string	Yes	Adapter or channel selector returned by `adapter list` in this package. Preserve the original string; do not substitute `batchId`, `stationId`, chip UID, or `uuid`.
`--type`	string	Yes	Use the value required by the package, consistent with `adapter list`. The package defines the meaning of `1` in this example.
`--chipVendor`	string	No	Vendor of the chip selected for the current batch. The UI should pass it; map it from configuration if the package uses a vendor alias.
`--chipPart`	string	No	Chip model selected for the current batch, usually from `chips[].chipPart`. The UI should pass it.
`--speed`	string	No	Programming communication speed; `115200` is an example. The package defines its units, valid range, and default. Do not interpret it universally as a UART baud rate or debug clock.
`--extInfo`	string	No	Vendor extension parameters. Pass them only when the package explicitly defines them; otherwise omit them. Do not pass arbitrary batch JSON.

5.2.3.3 Example

In the Python PPCLI version reviewed, `--serialno` and `--type` are required; the other parameters above are syntactically optional. Because the vendor implementation may depend on chip vendor and model, the UI should also pass `--chipVendor` and `--chipPart`. The `program` command does not need `batchId`; the preceding `obiscli batch assign` command binds the current batch.

```
".\python-3.12.9-embed-amd64\python.exe" ".\ppcli.py" program --chipVendor="<CHIP_VENDOR>" --chipPart="<CHIP_PART>"
--serialno="<SERIALNO>" --speed=115200 --type=1
```

> **TIP**
>
> Use `--chipVendor`, `--chipPart`, and `--type` values defined by the actual Python PPCLI package. Do not copy `TELINK` or `telinkevk` from the dedicated Telink interface example.

If the programming script package explicitly requires vendor extension parameters, add `--extInfo="<EXT_INFO>"`.

5.2.4 Check Parameters

Use these commands to check the parameters supported by the actual Python PPCLI package:

```
".\python-3.12.9-embed-amd64\python.exe" ".\ppcli.py" adapter list --help
".\python-3.12.9-embed-amd64\python.exe" ".\ppcli.py" program --help
```

> **TIP**
>
> `--help` only displays command and parameter definitions; it does not program a device.

5.2.5 Internal PPCLI Calls

This section describes the calls between PPCLI and OBIS Programming CLI after device programming starts. The UI prepares the runtime, selects an adapter, starts `program`, and handles its output. PPCLI then follows the current batch and chip configuration to perform the programming flow, including:

1. Calling `obiscli batch getChangingData` to retrieve changing data and the programming identifier for the current device;
2. When fixed data is not cached, calling `obiscli batch getFixData` to retrieve and cache it, then combining it with the changing data;
3. Calling the vendor programming logic in `process.py` to access the device and perform certificate and Factory Data processing, firmware writing, and verification according to the chip and batch configuration;
4. Using `obiscli batch putdata` to exchange data with the Edge Service when required during programming, for example to submit a CSR and obtain a DAC; using `obiscli batch executeApdu` for APDU programming steps when APDU interaction is required;
5. After programming, reporting `success` or `failure` through `obiscli batch putresult`. Reporting may be impossible if preliminary data retrieval fails, a valid `uuid` or `batchId` is unavailable, or the flow stops unexpectedly.

The UI does not need to retrieve changing device data, request a DAC, or report the same programming result again. PPCLI or the programming script performs these operations.

5.3 Dedicated Telink Programming Interface

Some Telink programming script packages use a dedicated executable to list adapters and start device programming directly. The UI should select the programming entry point supplied by the actual package. Python PPCLI and the dedicated Telink executable are alternative integration methods; use one of them. If Python PPCLI already calls the Telink programming tool internally, the UI should call only the outer PPCLI to avoid starting programming twice for the same device.

5.3.1 List Adapters

Used to list available adapters through the dedicated Telink programming executable.

5.3.1.1 Command

`adapter`

5.3.1.2 Subcommand

`list`

5.3.1.3 Parameters

Parameter	Type	Mandatory	Description
`--chipVendor`	string	Yes	Chip vendor identifier. This example uses `TELINK`; do not substitute the vendor name used by Python PPCLI without checking the package.
`--type`	string	Yes	Adapter type. This example uses `telinkevk`; do not mix it with `--type=1` from the Python PPCLI example.

5.3.1.4 Example

```
".\Cmd\_download\_tool.exe" adapter list --chipVendor="TELINK" --type=telinkevk
```

The path above refers to `_tool.exe` in the `_download` subdirectory of `Cmd`; it does not refer to a single file named `Cmd_download_tool.exe`.

Use the executable path in the delivered programming script package. For example, if the executable is in the package root, use:

```
".\Cmd_download_tool.exe" adapter list --chipVendor="TELINK" --type=telinkevk
```

Packages may have different directory structures. The UI should determine the executable path and working directory from package configuration, without hard-coding a fixed path or guessing a substitute when the target file is absent.

5.3.2 Start Programming

Used to start device programming with the selected Telink adapter.

5.3.2.1 Command

program

5.3.2.2 Parameters

Parameter	Type	Mandatory	Description
`--serialno`	string	Yes	Target adapter device ID returned by `adapter list` of the same dedicated Telink executable. Preserve the original string.

5.3.2.3 Example

```
".\Cmd\_download\_tool.exe" program --serialno="<SERIALNO>"
```

If the delivered executable is in the package root, use:

```
".\Cmd_download_tool.exe" program --serialno="<SERIALNO>"
```

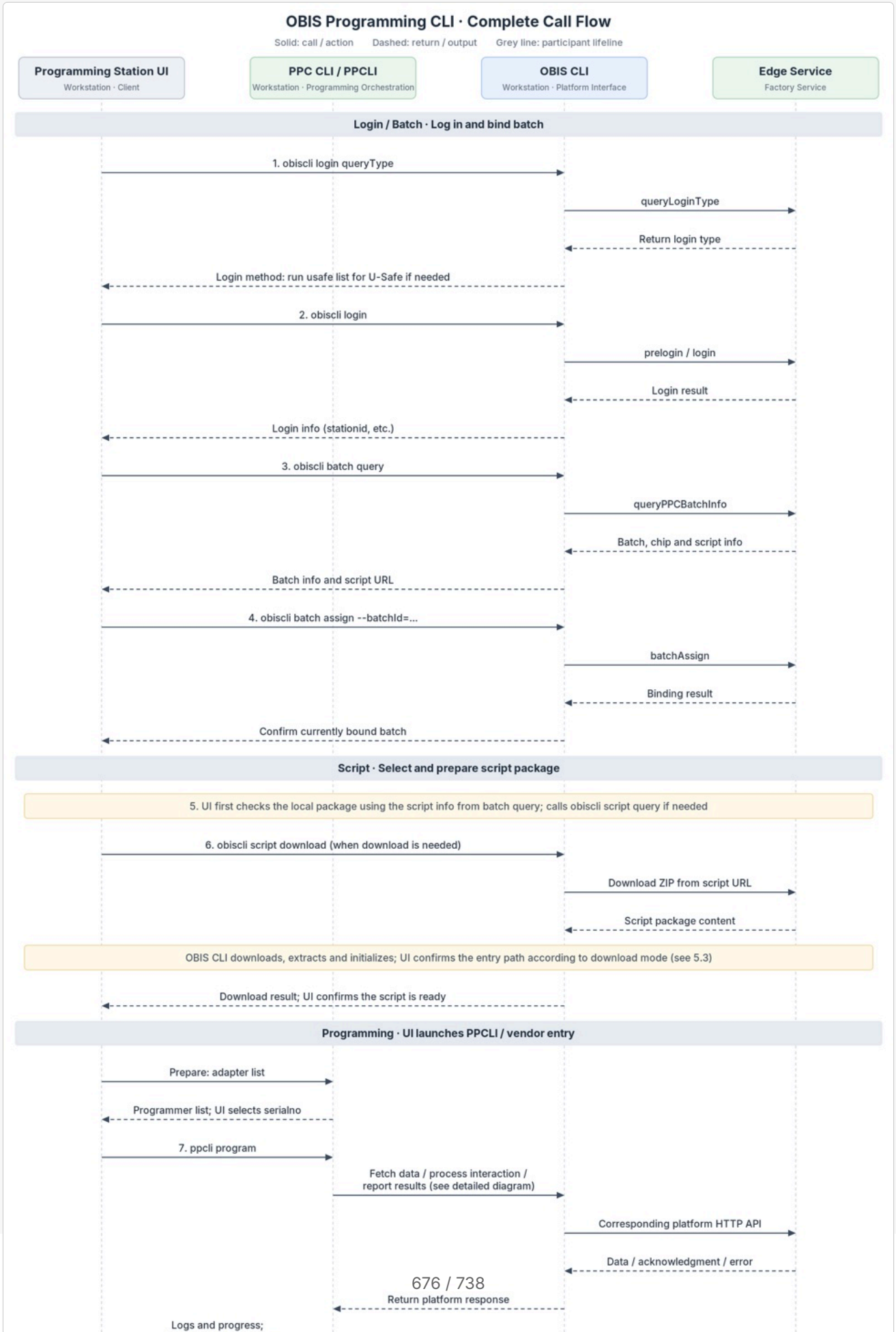
The `program` command of the dedicated Telink interface does not use the `--chipVendor`, `--chipPart`, `--speed`, or `--type` parameters shown for Python PPCLI. Do not append them to the Telink command. Follow the actual Telink package documentation for other programming settings.

The response, progress format, timeout, and exit codes of the dedicated Telink interface depend on the delivered package version.

6. Device Programming Execution Flow

6.1 Overall Call Flow

This section describes the overall UI flow from Edge Service login and batch and programming script preparation through device programming with PPCLI.


OBIS Programming CLI · Complete Call Flow
Solid: call / action
Dashed: return / output
Grey line: participant lifeline
Programming Station UI
Workstation · Client
PPC CLI / PPCLI
Workstation · Programming Orchestration
OBIS CLI
Workstation · Platform Interface
Edge Service
Factory Service
Login / Batch · Log in and bind batch
1. obiscli login queryType
queryLoginType
Return login type
Login method: run usafe list for U-Safe if needed
2. obiscli login
prelogin / login
Login result
Login info (stationid, etc.)
3. obiscli batch query
queryPPCBatchInfo
Batch, chip and script info
Batch info and script URL
4. obiscli batch assign --batchId=...
batchAssign
Binding result
Confirm currently bound batch
Script · Select and prepare script package
5. UI first checks the local package using the script info from batch query; calls obiscli script query if needed
6. obiscli script download (when download is needed)
Download ZIP from script URL
Script package content
OBIS CLI downloads, extracts and initializes; UI confirms the entry path according to download mode (see 5.3)
Download result; UI confirms the script is ready
Programming · UI launches PPCLI / vendor entry
Prepare: adapter list
Programmer list; UI selects serialno
7. ppcli program
Fetch data / process interaction /
report results (see detailed diagram)
Corresponding platform HTTP API
Data / acknowledgment / error
Return platform response
Logs and progress;

Stage	Caller → Receiver	Command / action	Prerequisite for next action
1	UI → OBIS CLI	`login queryType`; run `usafe list` if needed for U-Safe login	Obtain the login type and required identity information.
2	UI → OBIS CLI	`login`	Login succeeds; save the `stationid` required by the client.
3	UI → OBIS CLI	`batch query`; or `batch queryList` for an order	Obtain full batch information and identify `batchId`, chip, and programming script. A list containing only IDs cannot replace full batch information.
4	UI → OBIS CLI	`batch assign`	Batch assignment succeeds; subsequent programming uses the current assigned batch.
5	UI	Prefer script URL, name, and version or digest from `batch query`; run `script query` if needed.	Decide whether to reuse a matching local package or download it again.
6	UI → OBIS CLI	`script download`	Download, extract, and initialize the package; locate its actual entry directory. Skip download if a prepared package is already cached.
7 (prepare)	UI → PPCLI / package entry	`adapter list`	List available adapters successfully and select the target `serialno`.
7	UI → PPCLI / package entry	`program`	Read programming output in real time, wait for process completion, and handle success, failure, or a result reporting error.
Finish	UI → OBIS CLI	Run `batch query` to refresh batch statistics if needed; run `logout` at session end.	End the login session after programming and result reporting have finished on all channels.

Step 5 should use the programming script information returned by `batch query` first. The UI need not always call `script query`; call it only if the flow requires more information. Batch responses may have an outer wrapper that varies by version. Parse the actual OBIS Programming CLI output rather than assuming its JSON structure from a raw HTTP response.

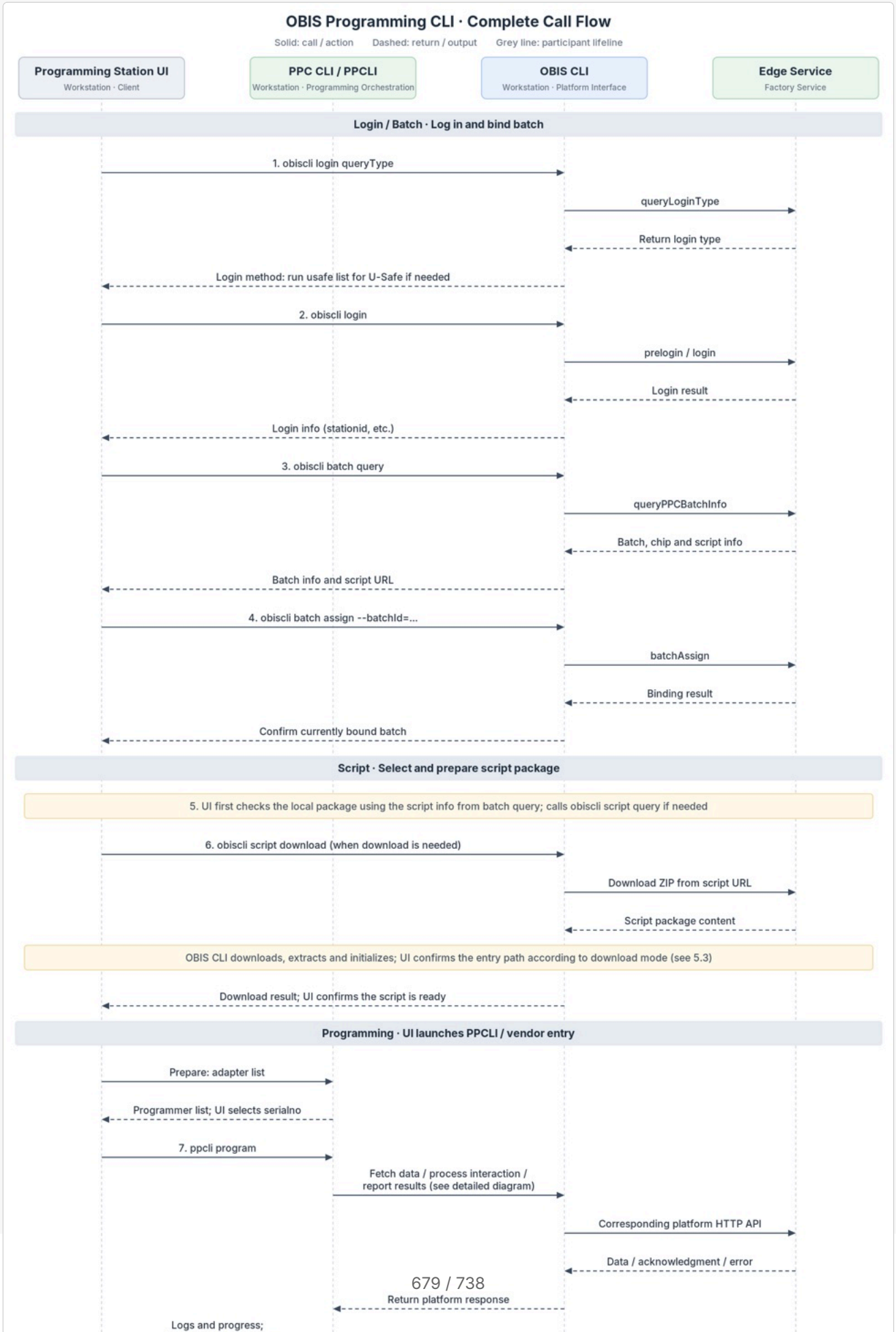
6.2 Programming Stage Call Flow

This section describes stage 7 of the overall flow, including how the UI starts programming, retrieves programming data, programs the device, and reports the result.

TIP

- getChangingData and getFixData are OBIS Programming CLI commands for changing and fixed device data. Their HTTP endpoints are getProgrammingData and getMetadata, respectively; do not confuse CLI command names with HTTP endpoint names.
- If fixed data is cached, getFixData may be skipped.
- The chip and batch configuration determine device erase, Device ID retrieval, CSR/DAC processing, Factory Data writing, firmware programming, reset, and other steps.
- Non-Matter devices or flows without device-generated CSRs may not include CSR/DAC processing.
- putdata exchanges data and requests/responses during programming, for example CSR/DAC requests; its HTTP endpoint is uploadRequestData.
- putresult reports the final programming result; its HTTP endpoint is programmingResult. putdata and putresult have different purposes and are not interchangeable.

The diagram shows a typical Python PPCLI flow. The internal flow of the dedicated Telink interface depends on the delivered version.


OBIS Programming CLI · Complete Call Flow
Solid: call / action
Dashed: return / output
Grey line: participant lifeline
Programming Station UI
Workstation · Client
PPC CLI / PPCLI
Workstation · Programming Orchestration
OBIS CLI
Workstation · Platform Interface
Edge Service
Factory Service
Login / Batch · Log in and bind batch
1. obiscli login queryType
queryLoginType
Return login type
Login method: run usafe list for U-Safe if needed
2. obiscli login
prelogin / login
Login result
Login info (stationid, etc.)
3. obiscli batch query
queryPPCBatchInfo
Batch, chip and script info
Batch info and script URL
4. obiscli batch assign --batchId=...
batchAssign
Binding result
Confirm currently bound batch
Script · Select and prepare script package
5. UI first checks the local package using the script info from batch query; calls obiscli script query if needed
6. obiscli script download (when download is needed)
Download ZIP from script URL
Script package content
OBIS CLI downloads, extracts and initializes; UI confirms the entry path according to download mode (see 5.3)
Download result; UI confirms the script is ready
Programming · UI launches PPCLI / vendor entry
Prepare: adapter list
Programmer list; UI selects serialno
7. ppcli program
Fetch data / process interaction /
report results (see detailed diagram)
Corresponding platform HTTP API
Data / acknowledgment / error
Return platform response
Logs and progress;

6.3 Complete Command Example

This example shows the basic command sequence from Edge Service login through device programming. It uses Python PPCLI and Windows `cmd.exe` syntax. Set actual parameters according to the site, batch, and programming script package. Confirm that each step succeeds before proceeding. Python PPCLI and the dedicated Telink interface are alternative entry points; select the one provided by the package.

```
REM 1. Query login type; run obiscli usafe list if needed for U-Safe login
obiscli login queryType --ip="<EDGE_IP>" --port=32333
f
REM 2. Log in using the type returned by queryType; this example uses passwordless login
REM For password login add --password="<PASSWORD>"; for U-Safe login add --usafesn="<USAFE_SN>"
obiscli login --ip="<EDGE_IP>" --port=32333 --stationVersion="<UI_VERSION>"

REM 3. Query batch information including batchId, chips, and scriptUrl
obiscli batch query

REM 4. Assign the current batch
obiscli batch assign --batchId="<BATCH_ID>"

REM 5. Get scriptUrl from the batch response; check for a matching prepared local package

REM 6. Download when no usable local package exists
obiscli script download --url="<SCRIPT_URL>"

REM Locate the actual entry directory from the download result and change directory
cd /d "<SCRIPT_ENTRY_DIRECTORY>"

REM 7 (prepare). List adapters and select SERIALNO
".\python-3.12.9-embed-amd64\python.exe" ".\ppcli.py" adapter list --chipVendor="<CHIP_VENDOR>" --type=1

REM 7. Start device programming
".\python-3.12.9-embed-amd64\python.exe" ".\ppcli.py" program --chipVendor="<CHIP_VENDOR>" --chipPart="<CHIP_PART>"
--serialno="<SERIALNO>" --speed=115200 --type=1

REM Check the exit code after program completes; the UI should read the child exit code directly rather than rely on
this echo
echo %ERRORLEVEL%

REM Refresh batch statistics if needed
obiscli batch query

REM Log out after programming and result reporting finish on all channels
obiscli logout
```

When using the dedicated Telink interface, replace only the stage 7 adapter query and programming commands:

```
REM 7 (prepare). List Telink adapters and select SERIALNO
".\Cmd\_download\_tool.exe" adapter list --chipVendor="TELINK" --type=telinkevk

REM 7. Start device programming
".\Cmd\_download\_tool.exe" program --serialno="<SERIALNO>"
```

The login, batch assignment, and programming script preparation flow remains the same. Use the executable path and working directory from the delivered Telink package.

6.4 Programming Script Download and Entry Directory

This section explains how the UI locates the actual programming entry point after downloading the script.

When only `--url` is passed, `script download` uses the default cache directory. The `scriptExist` and path values in its response indicate whether the script already exists and where it is located.

If both `--savePath` and `--extractFolder` are specified, the UI should not assume the command output contains the actual entry path. Locate the entry point from the chosen extraction directory and package structure, and verify that the entry executable and dependencies exist.

`--savePath` specifies the downloaded file directory. A programming script ZIP can contain one or more nested directories, so the download directory may differ from the actual programming entry directory.

Before starting, perform the initialization and dependency checks required by the package.

6.5 UI Process and Result Handling

This section describes process startup, output reading, and result handling when the UI calls PPCLI or a dedicated Telink programming executable.

Item	Integration requirement
Process startup	Set `executable` (path), `args[]` (arguments), and `cwd` (working directory) separately. Prefer an absolute executable path and `shell=false` to start the target process directly. Argument values in `args[]` need no extra shell quoting.
Parameter sources	Chip vendor and model come from the selected batch; `serialno` comes from `adapter list` of the selected programming entry point. Determine type, speed, and entry path from package configuration.
Output reading	Read `stdout` and `stderr` continuously and asynchronously until the process exits and output reading completes, so an unconsumed stream cannot block the process. Python PPCLI usually uses UTF-8; check the actual output encoding of older EXE versions.
Adapter output	Parse the complete `adapter list` response as defined by the package. Handle an empty list, missing fields, unexpected output, and nonzero exit codes. Parse multiline JSON as a complete response, not as separate JSON on each line.
Programming output	Programming output may contain logs and events; do not parse all `stdout` as a single JSON object. The Python PPCLI version reviewed may emit `[Progress]:<value>%` or `[Finish].` for progress or completion and `{"errMsg":"..."}` on failure. Other packages may use different formats.
Success criteria	Wait for normal process termination, then evaluate the exit code and final result defined by the package. Reaching 100% progress or emitting `[Finish].` indicates progress or flow completion only; do not release the channel early or treat either alone as proof that the platform received the result.
Result reporting	Check whether a `putresult` reporting failure affects the script's final status. If not, verify the platform record separately. A change in batch statistics alone does not prove that a particular `uuid` was reported successfully.
Failure, timeout, or cancellation	Retain serialno, package version, exit code, `stdout`, `stderr`, and any `uuid` obtained. Never mark a timed-out or terminated process successful. Before retrying, check device state and the previous result to avoid obtaining duplicate programming data or certificates.
Concurrency	One active programming task corresponds to one `serialno`. Actual concurrency depends on the package, driver, and service. While tasks share an OBIS login session, do not switch the current batch, log out, or replace the package in use.

6.5.1 UI Process Invocation Example

This example shows how the UI organizes process arguments when starting Python PPCLI. It does not define new CLI parameters or a fixed interface format:

- `executable`: path to the Python executable;
- `args`: commands and arguments passed to Python PPCLI;
- `cwd`: actual entry directory of the programming script;
- `shell`: `false` in this example, so the target process starts directly without running the full command through a shell.

```
{
  "executable": "<ENTRY_DIRECTORY>\\python-3.12.9-embed-amd64\\python.exe",
  "args": [
    "<ENTRY_DIRECTORY>\\ppcli.py",
    "program",
    "--chipVendor=<CHIP_VENDOR>",
    "--chipPart=<CHIP_PART>",
    "--serialno=<SERIALNO>",
    "--speed=115200",
    "--type=1"
  ],
  "cwd": "<ENTRY_DIRECTORY>",
  "shell": false
}
```

6.6 Integration Verification

This section lists key scenarios to verify after integrating the programming interface into the UI.

Verification item	Verification scope
Normal flow	Verify login, batch query and assignment, script preparation, adapter query, single-device programming, process exit status, platform record confirmation, and logout.
Parameters and paths	Verify directories and chip vendor names containing spaces, preservation of leading zeros in `serialno`, and correct executable, working directory, and `type` mapping.
Device errors	Verify that the UI ends tasks correctly and retains errors when no device is present, a device is unplugged, `serialno` is wrong, or a device is busy.
Platform errors	Verify that device data retrieval, certificate request, and result reporting failures are distinguished and that reaching 100% progress alone is not treated as success.
Multiple devices	Verify that cached and freshly downloaded packages both start; `serialno` and `uuid` stay separate across channels; and the shared batch and login session remain unchanged during programming.

Version: v3.4.0 (Latest)

Glossary in OnBoard™ IoT Security

B

BYOK (Bring Your Own Key)

A key management model in which the customer retains ownership and control over cryptographic key generation, while importing or delegating keys to an external platform for managed use.

C

CLI (Command-Line Interface)

A text-based interface for interacting with software systems through typed commands, commonly used for automation, scripting, and integration with development and production workflows.

CSR (Certificate Signing Request)

A cryptographic request generated by a device or secure environment containing a public key and identity information, used to request a digital certificate from a Certificate Authority (CA).

D

Device Identity

The cryptographic identity assigned to a device during provisioning, typically represented by a unique key pair and corresponding certificate.

Digital Assets

Product-related artifacts used during device production and provisioning, including firmware, cryptographic keys, certificates, and configurations.

E

EdgeHSM

A hardware-protected cryptographic execution device deployed at factory sites, designed to perform security-sensitive operations locally under externally issued authorization.

Edge Service

The Edge Service of OnBoard™ IoT Security provides on-site production management capabilities for factories. It is typically deployed on on-premises servers along the production line, where it caches, processes, and stores batch data and device data. It also provides cryptographic services through the Edge HSM.

G

GPCA

A dedicated certificate service for GlobalPlatform SCP11c, providing certificate and trust chain management, secure private key operations, authorization for signing and key derivation, as well as cross-organizational permission collaboration capabilities.

H

HSM (Hardware Security Module)

A tamper-resistant hardware device designed to securely generate, store, and use cryptographic keys.

HSM U-Safe

A hardware security token used for authentication when logging in to OnBoard Edge Service.

I

Identity U-Safe

A hardware security token used for authentication when logging in to the Programming Station client.

K

KMS (Key Management System)

A system for managing the full lifecycle of cryptographic keys, including generation, storage, distribution, rotation, revocation, and destruction.

M

MES (Manufacturing Execution System)

A factory-side system used to manage, monitor, and control manufacturing operations, including production scheduling, process tracking, and quality control.

O

OBIS

OnBoard™ IoT Security, a security service platform built by Snowball for IoT scenarios. It is a security control plane that governs how product digital assets may be used across the device manufacturing lifecycle.

OBIS CLI

OnBoard™ IoT Security CLI establishes a secure channel with the Local Service using authentication provided by U-Safe for PPC, and retrieves the corresponding device data from the Local Service for use by upper-layer applications.

OBIS Edge Web Portal

The portal website of OBIS Edge, through which factory managers can manage on-site operations for factories visually.

OBIS Programming Station software

The controlled, last-mile software environment installed on a factory Programming Station where devices are physically connected, programmed, and initialized.

OBIS Web Portal

The portal website of OnBoard™ IoT Security. Users can perform product-related operations and management through this website, such as product management, factory management, user management, key management, and certificate management.

ODM (Original Design Manufacturer)

A manufacturer that provides end-to-end product design and manufacturing services on behalf of an OEM. ODMs typically develop products based on their own reference designs or platforms, customized to OEM specifications, with the final product shipped under the OEM's brand.

OEM (Original Equipment Manufacturer)

The entity that designs, owns, and markets a product under its own brand. The OEM bears ultimate responsibility for product specifications, quality, and regulatory compliance, even when some or all manufacturing activities are delegated to external partners.

OIDC (OpenID Connect)

An identity layer built on top of the OAuth 2.0 protocol, used for authentication and single sign-on (SSO). OBIS supports OIDC-based integration with enterprise identity and access management systems.

P

PKI (Public Key Infrastructure)

A framework of technologies, policies, and procedures for managing digital certificates and public-private key pairs, enabling secure authentication, encryption, and digital signing.

PPC (Programming Process Control) CLI

Programming Process Control Command Line Interface, a command-line tool used for executing programming process control tasks.

Production Order

A production order (also referred to as a Work Order or Manufacturing Order depending on the system) is a directive created in the OEM's SAP, ERP, or MES platform that authorizes and tracks the manufacturing of a specific quantity of products.

Programming CLI

Programming Command Line Interface, a command-line tool used for executing device programming.

Programming Station client

The factory programming client used on production lines to perform chip programming operations.

S

Secure Provisioning

The end-to-end process of securely initializing a device with its identity, cryptographic materials, firmware, configurations, and security settings required for authenticated operation and lifecycle management.

SEMS

A configuration management service for Secure Element (SE), offering SE profile lifecycle management, secure channel configuration, secure encapsulation of SCP11c scripts, permission coordination, and production integration capabilities.

SnowBall

Shanghai Snowball Digital Intelligence Technology Co., Ltd., referred to as Snowball. A technology company with deep expertise in secure device provisioning and cryptographic infrastructure.

SSO (Single Sign-On)

An authentication mechanism that lets users access multiple systems using a single set of credentials.

Version: v3.4.0 (Latest)

FAQs in OnBoard™ IoT Security

This article lists the issues that you may encounter when using OnBoard™ IoT Security (OBIS) and provides corresponding solutions.

Account & Sign-in

How to self-register for an OBIS account?

When your organization has enabled the self-registration feature, click **Sign Up** on the OBIS sign-in page. After completing the registration, you can sign in to OBIS by using the verification code method.

Why can't I self-register for an OBIS account?

If you see the message "Your organization has not enabled self-registration. Please contact your admin", please contact the System Manager to confirm whether the self-registration feature has been enabled for your organization.

Why can't I sign in to OBIS through a verification code?

- If you see the message "The email address does not exist. Please check and try again", please contact the System Manager to confirm whether an OBIS account has been created for your email address.
- If you see the message "This account has been disabled. If you have any questions, please contact the administrator", please contact the System Manager to check your account status. Only accounts with the **Active** status can sign in to OBIS. For more information, refer to Manage accounts.

Why can't I sign in to OBIS through SSO?

- If you see the message "Your organization has not enabled SSO", please contact the System Manager to check if SSO has been enabled for your organization.
- If you see the message "SSO service is currently unavailable. Please try again later", please contact the System Manager to check if there are any issues with the SSO service of your organization.
- If you see the message "Your organization does not allow automatic account creation via SSO. Please contact your admin", please contact the System Manager to check if the automatic account creation via SSO feature has been enabled for your organization.

User & Role

Can a user be assigned multiple roles, and can these assignments be updated?

- The System Manager can assign multiple OBIS roles to a user and modify these assignments afterward. For more information, refer to Manage accounts.
- The Product Owner and Product Manager can assign multiple product roles to a user and modify these assignments afterward. For more information, refer to Manage members.

Can users and user groups from other tenants be added to a product team?

Users from other tenants can be added, but user groups can't be added across tenants. Only users with the **Active** status can be added.

For example, a Product Manager from Tenant A can add a user from Tenant B to their product team. For more information, refer to Manage members.

Why do I see the message "Cannot be invited. Please check the address and try again" when adding a user to a product team?

Please check whether the user already has an OBIS account. Only OBIS users can be invited to join a product team. Contact the System Manager to create an account for the user before attempting to add them.

Product

Why are some products not displayed in the product list?

The product list only displays the products you are involved in. Please check whether you are a member of the product team for the specific product. If not, contact the Product Owner or Product Manager of the product to invite you to the team and assign a role. Once added, you will receive an email containing a link, which you can use to access the product details.

Why is the product status shown as Draft?

After a product is created, its initial status is **Draft**. Once a version is created, the product status will change to **Released**. For more information, refer to the description of product status.

Which chips are currently supported by OBIS?

For the detailed list, refer to the currently supported chip settings. Additional chip vendors, series, and parts will be added in the future based on demand.

What does "Mandatory" mean when configuring Factory Data for a product?

If the checkbox in the **Mandatory** column for a Factory Data item is selected, members are required to enter a value for that Factory Data when creating a version.

Why can't some product assets be selected when creating a version or batch?

When creating a version or batch, you can only select product assets that are not deactivated. For more information, refer to Deactivate or activate a product asset.

How can I check the QR code after a device is programmed?

After the device has been programmed, you can select the corresponding device on the Device tab for the product and then check the QR code on the device page.

Why is the programmed device information for some batches not displayed on the Device tab?

The **Device** tab only displays devices programmed by factories within the current tenant. Batches programmed in other tenants are not displayed.

Version

Why is the Create button grayed out on the Version tab?

If the **Create** button on the **Version** tab appears grayed out, it is currently unavailable. Please check whether all required assets for your product have been configured. Once everything is properly configured, the **Create** button will be enabled automatically.

Why am I unable to delete a version?

Before deleting a version, please ensure that:

- The version isn't in the **Pending for approval** status (versions in **Pending for approval** can't be deleted).
- This version isn't associated with any batches (once a version has been used to create batches, it can't be deleted).

Batch

Why is the Create button grayed out on the Batch tab?

If the **Create** button on the **Batch** tab appears grayed out, it is currently unavailable. Please check whether a version has been created. After a version is created, the **Create** button will be enabled automatically.

Why are some versions can't be selected when creating a batch?

When creating a batch, only versions with the **Approved** status can be selected. If manual approval is enabled for the product, versions created in the PROD environment will require manual approval (approve or reject) by the Product Owner or Product Manager.

- Once the version is approved, the version status changes to **Approved** and it can be used to create a batch.
- Once the version is rejected, the version status changes to **Rejected**, and the version needs to be updated and resubmitted for approval.

Factory

Why are some factories not displayed in the factory list?

The factory list only displays the factories you are involved in. Please check whether you are the Factory Admin or Factory Manager for the specific factory. If not, contact the Factory Admin or Factory Manager of the factory to invite you to the factory. Once added, you will receive an email containing the credentials to log in to the Factory Service.

Why are some factories grayed out and can't be selected when creating a batch?

When creating a batch, only factories with the **Normal** status can be selected. After a local factory is created, its initial status is **Pending**. The status will change from **Pending** to **Normal** after adding HSM U-Safe to the local factory. For more information, refer to the description of factory status.

Why am I unable to unbind the Identity U-Safe?

An Identity U-Safe can't be unbound if it is locked. For more information, refer to unbinding, locking, or unlocking Identity U-Safe.

Why can't I edit the programming station?

When the programming station status is **Busy**, the **Edit** option is grayed out and unavailable. After unbinding the programming station from the batch in OBIS or OnBoard Edge Service, the station status changes to **Available**, and the station can then be edited.

Certificate

Why can't I check the certificate verification services?

The **Verification Services** tab is displayed only for system-generated intermediate certificates (PAI, Manufacturer, Model, and Sub Cert certificates).

SE Profile

Why can't I edit an SE Profile?

You can configure the SE Profile only when it is in the **Draft** state. Once an SE Profile is published, it becomes permanently locked, and none of its fields can be modified. For more information, refer to Configure and publish an SE Profile.

Why can't I publish an SE Profile?

Before publishing an SE Profile, please ensure that:

- The SE Profile is in the **Draft** state, and you have the necessary permissions to publish it.
- The ISDs for both the initial profile and the Post-Provision Profile have been configured.
- All keys and GPCA objects referenced by any node are in the **Active** state.
- The SCP (SCP03 or SCP11c) for all security domains has been configured.

For more information, refer to Publish the SE Profile.

OnBoard Edge Service & Programming Station

How can I check the service address used by the local factory for logging in to OnBoard Edge Service and the Programming Station client?

After contacting Snowball for assistance in deploying OnBoard Edge Service, the corresponding service address can be found in the factory information.

Why am I unable to sign in to OnBoard Edge Service?

Please check whether the prerequisites for logging in to OnBoard Edge Service have been met.

How can I check the password for logging in to the Programming Station client?

The initial sign-in password is randomly generated by the system after a programming station is added to the factory. You can check the sign-in password in OBIS (local factory & cloud factory) or OnBoard Edge Service (local factory). Currently, the randomly generated password can't be changed.

Version: v3.4.0 (Latest)

Release Notes

This article provides an overview of the release dates, key feature updates, and related documentation for OnBoard™ IoT Security (OBIS), covering versions up to **v3.4.0**. For CLI and API version updates and changes, refer to the revision records in the corresponding documentation.

2026 Release Versions

v3.4.0 (September 10, 2026)

Version **v3.4.0** introduces updates to the Product, Records, KMS, PKI, GPCA, and SEMS features. In addition, the UI has been updated and optimized to enhance usability and user experience.

Feature Categories	Key Updates	Description	Related Documents
Product	Added SE Profile asset type	Supports configuring SE Profiles and checking the SE Profiles associated with a product, including their reference relationships and statistical data, making it easier to understand the security module configurations relevant to that product.	Product: • Configure a product • Manage products • Create a version • Create a batch
	Adjusted file download permissions	Files added during the configuration of **Firmware**, **Matter Config**, **Factory Data**, **General File**, **Programming Script**, and **SE Profile** are restricted for download only to users within the same tenant. This prevents files from being transferred across tenant boundaries during cross-tenant collaboration.	

Feature Categories	Key Updates	Description	Related Documents
	Unified **General File** asset management	Merged **Attachment File** into the **General File** asset, providing a single entry point for certificate configuration and management, simplifying workflows and improving consistency.General files can be selected as needed when creating versions and batches.	
	Added batch limit notifications	When creating a batch, if the number of unexpired batches at a factory exceeds 200, the system will display a notification regarding the batch limit, helping users manage and clear out batch resources.	
Record	Enhanced device records	Improved the device record list by optimizing field visibility and presentation, providing a more complete view of historical information and making it easier to review and trace device lifecycle records.	• Product - Check programmed devices • Record - Check device history
KMS	Enhanced the key creation workflow	Improved the key creation workflow by standardizing key attribute configuration and identity management, enhancing configuration accuracy and management efficiency.	KMS: • Create a key • Manage keys
	Optimized key name isolation across different environments	The same key name can be used independently in the TEST and PROD environments, making it easier to manage key assets across testing and production environments.	

Feature Categories	Key Updates	Description	Related Documents
	Added the **Revoke** option for keys	Supports key revocation to stop the key's service capabilities and prevent further use.	
PKI	Enhanced the certificate creation workflow	Improved the certificate creation workflow by standardizing certificate attribute configuration and identity management, enhancing configuration accuracy and management efficiency.	PKI: • Create a certificate • Check certificates • Manage certificates
	Optimized the verification service feature	The **Verification Service** tab is displayed only for intermediate certificates generated by the system, clarifying the scope to which the verification service applies.	
	Added **Lock** and **Unlock** options	Certificates can now be locked or unlocked. Once a certificate is locked, it can't be referenced by new configurations; existing references remain unaffected.	
GPCA	Added GP CA management	Added GP CA list and detail pages, with support for managing SD, OCE, and mixed certificate chains.	GPCA: • Create a GlobalPlatform certificate • Check GlobalPlatform certificates • Manage GlobalPlatform certificates
	Support for GP CA creation and offline signing	Enables the creation of a GP CA, offline signing, and import of signing results, facilitating a complete offline certificate issuance process.	

Feature Categories	Key Updates	Description	Related Documents
	Added GP CA lifecycle management	Supports state operations such as locking, unlocking, revoking, and destroying, and provides a standardized process for confirming these actions and specifying the reasons for them.	
	Added input validation for GP CA	Supports input validation during the creation and import of certificates, with automatic cleanup of input data such as certificates and CSRs.	
SEMS	Added SE Profile management	Supports the creation, cloning, editing, publishing, and viewing of SE Profile details, with the SE Profile structure and configuration content displayed via a content tree.	SEMS: • Create an SE Profile • Configure and publish an SE Profile • Check SE Profiles • Manage SE Profiles • Manage SCP11c scripts
	Added SCP11c script support	SCP11c scripts can now be configured in SE Profiles.	

v3.3.0 (August 19, 2026)

Version **v3.3.0** introduces updates to the Product, Records, Member, Key, Certificate, Factory, and User Group features. In addition, the UI has been comprehensively updated and optimized to enhance usability and user experience.

Feature Categories	Key Updates	Description	Related Documents
Product	Added the environment switching feature	Supports switching between **PROD** and **TEST** environments from the top of the product page. The PROD environment is selected by default.	Product: • Create a product • Configure a product • Check products • Manage products • Create a version • Check versions • Manage versions • Check logs • Manage members
	Updated the product overview page	The overview page now includes assets, production version, and manufacturing batch sections, improving asset traceability, factory authorization management, and version consistency verification.	
	Improved product settings navigation	Relocated the product settings entry from a tab to the upper-right corner of the product page, enabling quicker access to settings from any product page.	
	Unified **Certificates** and **Programming Station Software Package** asset management	• Merged **Custom certificate configuration** and **Google certificate configuration** into the **Certificates** asset category, providing a single entry point for certificate configuration and management, simplifying workflows and improving consistency. • Consolidated **Programming Script** and **Attachment File** into the **Programming Station Software Package** asset category, enabling centralized management of programming scripts and related files to ensure production configuration consistency and streamline operations.	

Feature Categories	Key Updates	Description	Related Documents
	Added the **Assets** tab	Added a new **Assets** tab to centralize product asset management, providing a unified interface for configuring and managing **Chip Config**, **Keys**, **Certificates**, **Firmware**, **Matter Config**, **Factory Data**, **General File**, and **Programming Station Software Package**.	
	Updated file upload limits	Increased the maximum file upload size to 512 MB. The adjustment applies to firmware files, programming scripts, attachment files, and general files.	
	Support for deactivating or activating product assets	Product assets can now be activated or deactivated to control whether they are available for selection when creating versions or batches.	
	Enhanced archived product management in the product list	Improved the filtering experience for archived products by integrating archive status into the unified filter options, replacing the separate "Show Archived/Unarchived Data" control and providing a more consistent and efficient filtering experience.	
	Enhanced the version page	Unified the entry points and workflows for version approval, rejection, and deletion, providing a more consistent user experience.	
	Added the **Audit** tab	With the **Audit** tab, you can view all members' activity records, including the operator, organization, operation type, and operation time, making it easier to track product changes and stay informed about team activity.	

Feature Categories	Key Updates	Description	Related Documents
	Added the **Member** tab	Introduced a dedicated **Member** tab, moving member management out of product settings to provide quicker access and a more streamlined member management experience.	
Records	Enhanced device records	Improved the device record list by optimizing field visibility and presentation, providing a more complete view of historical information and making it easier to review and trace device lifecycle records.	• Product - Check programmed devices • Record - Check device history
KMS	Enhanced the key creation workflow	Improved the key creation workflow by standardizing key attribute configuration and identity management, enhancing configuration accuracy and management efficiency.	KMS: • Create a key • Check keys • Manage keys
	Added the usage count feature	Added a **Usage** tab for keys, allowing users to view key usage across users and products. This improves key information visibility and enhances asset management transparency and usage tracking.	
	Added key download limits	Only keys in a **Normal** status can be downloaded. In addition, each user is limited to 10 downloads per key per hour, further strengthening key security and access control.	

Feature Categories	Key Updates	Description	Related Documents
PKI	Enhanced certificate list sorting	Active certificates are now displayed first in the certificate list, improving visibility and simplifying certificate management.	PKI: • Create a certificate • Check certificates • Manage certificates
	Enhanced the certificate creation workflow	Improved the certificate creation workflow by standardizing certificate attribute configuration and identity management, enhancing configuration accuracy and management efficiency.	
	Enhanced Certificate Validity Period Validation	Supports configuring certificate validity periods beyond the expiration date of the inherited certificate. Risk notifications are displayed to help users identify potential certificate chain validation failures, client trust issues, and audit risks.	
	Added the usage count feature	Added a **Usage** tab for certificates, allowing users to view certificate usage across users and products. This enhances certificate visibility and improves asset management transparency and usage tracking.	
	Added the verification service feature	Added a **Verification Service** tab for certificates, enabling users to verify certificate revocation status, retrieve issuer certificates to build a complete trust chain, and troubleshoot certificate validation failures.	
	Added the end entity certificate feature	Added an **End Entity Certificate** tab, allowing users to view all end-entity certificates issued from a certificate template and gain visibility into the template's actual issuance activity.	

Feature Categories	Key Updates	Description	Related Documents
	Added the **Download** option	Added the ability to download certificate files for deployment and configuration across clients, servers, and other systems.	
Factory	Improved factory settings navigation	Relocated the factory settings entry from a tab to the upper-right corner of the factory page, enabling quicker access to settings from any factory page.	Factory: • Local Factory - Configure and manage programming stations • Cloud Factory - Configure and manage programming stations
	Added the feature to edit programming stations	Programming stations can now be edited after creation, enabling updates to station names and login methods while improving operational flexibility.	
	Other Updates	Added the Factory Admin role.	
User Group	Added the **Linked Product** tab	On the **Linked Product** tab of a user group, you can view the products associated with the current user group, making it easier to understand the relationships between the user group and products.	User Group - Check groups
Programming Station	Updated script file upload limits	Increased the maximum script file upload size to 512 MB.	Programming Station - Execute device programming

v3.2.2 (February 9, 2026)

Version **v3.2.2** introduces updates to the Product, Factory, Certificate, Records, and Programming Station features.

Feature Categories	Key Updates	Description	Related Documents
Product	Adjusted and optimized the batch page	• The batch status, batch synchronization status, and programming data synchronization status are displayed in different colors based on their respective values • Batches can be searched using the following conditions: **Batch ID**, **Batch Name**, **Version Name**, **Environment**, **Creation Time**, **Batch Status**, **Batch Sync**, and **Records**	Product - Check batches

Feature Categories	Key Updates	Description	Related Documents
Factory	Adjusted and optimized the Factory Manager permission configuration	Only the Factory Manager can access the details page of their respective factory and perform factory configurations	Factory: • Manage factories and programming stations: ◦ Local factory: ▪ Configure and manage factories ▪ Configure and manage programming stations ◦ Cloud factory: ▪ Configure and manage factories ▪ Configure and manage programming stations ▪ Manage batches and assign programming stations • Check factories

Feature Categories	Key Updates	Description	Related Documents

Certificate	Supports selecting the platform's pre-built Google Cast template, and allows adding custom certificates or Google certificates when creating a version	• When creating a certificate, you can directly select the platform's pre-built Google Cast template, and the corresponding configuration will be automatically applied based on the Google Cast certificate level (Root / Manufacturer / Model / Device)
		• Custom certificates allow configuration of **Extended Key Usage**
		• The product supports adding non-Matter certificate configurations, allowing non-Matter certificates to be added when creating a version, so factories can produce devices that support other protocols
		• The certificate chain details page now includes a new feature to display
			• Product:
			  ◦ Configure a product
			  ◦ Create a version
			• PKI - Create a certificate

Feature Categories	Key Updates	Description	Related Documents
		newly added certificate templates, with the certificate list clearly indicating whether a certificate contains a private key	

Feature Categories	Key Updates	Description	Related Documents
Records	Added device profile and log recording features, retained programmed data, improved filtering and search, and updated log viewing permissions	• Optimized device profile: Captures critical device information during production, including chip configuration, Matter configuration, DAC programmed, factory data, firmware version, and programming scripts • Custom extended fields for basic device information: Supports user-defined fields in addition to system-defined ones, enabling fuzzy searches. Currently supported fields include **VID**, **PID**, **Chip UID**, **QR Code**, and **Pairing Code** • Added programming logs: Records all key events and results during device programming, along with environment information, making tracking and troubleshooting	• Product - Check programmed devices • Records - Check device history

Feature Categories	Key Updates	Description	Related Documents
		easier • Enhanced access control: Only users with product role permissions or the Factory Manager of the corresponding factory can check device records, ensuring data security	

Feature Categories	Key Updates	Description	Related Documents
Programming Station	• Optimized UI layout to support the new port configuration • Added a batch details viewing function, allowing you to retrieve the corresponding batch information by order number • Supports automatic recognition of the programmer station ID bound to Identity U-Safe, with no manual input required during sign-in	• Optimized Programming Station client UI: Displays overall programming progress and supports double-clicking a port to view its detailed programming status • Multi-port programming support: Enables simultaneous programming across 1 to 24 ports, with customizable port layouts for greater operational flexibility • Optimized batch information query: Supports retrieving batches by order number and allows viewing detailed batch information directly within the Programming Station client for easier tracking and management • Station ID Auto-Detection: Once the Identity U-Safe is inserted, the client	Programming Station: • Installation • Sign-in • Execute device programming

Feature Categories	Key Updates	Description	Related Documents
		automatically detects the bound station ID, requiring no manual input during sign-in	

v3.2.1 (January 15, 2026)

Version **v3.2.1** introduces updates to the Registration and Sign-in, User Group, Product, Version, Batch, Factory, KMS, OnBoard Edge Service, and Programming Station features.

Feature Categories	Key Updates	Description	Related Documents
Registration and Sign-in	Added **Sign in with SSO** and **Self-Registration** features	• Sign in with SSO: Sign in to OBIS directly using your company's IdP account, without needing to remember a separate OBIS account • Self-Registration: Register with your company email address and automatically receive a default role, enabling quick access to your organization's tenant	Registration and Sign-in

Feature Categories	Key Updates	Description	Related Documents

User Group	Added the **User Group** menu	• User group management: Enables unified user management by organizing users into groups
		• Product permission assignment: Allows user groups to be added directly to a product, granting product access to all group members at once
			• Product - Manage members
			• User:
			  ◦ Group:
			  ▪ Create a group
			  ▪ Check groups
			  ▪ Manage groups

Feature Categories	Key Updates	Description	Related Documents

Product	• Splits the key and certificate resource package
	• Supports downloading product resource files
	• Added product archiving feature
	• Removed the Mark field when creating a product
		Split the key and certificate resource package:
		• You need to add all certificates and keys used by the product to the corresponding resource packages in advance
		• The product's Resource Manager allows you to select the required certificates or keys from the resource packages within configuration items (such as Matter Config and Chip Config)
		
		Download product resource files:
		• Product members can download uploaded files
		• Downloads are supported on the resource configuration
			• Quick Start
			• Product:
			  ◦ Create a product
			  ◦ Configure a product
			  ◦ Manage products

Feature Categories	Key Updates	Description	Related Documents
		page, including Firmware, CD files in Matter Config, files in Factory Data, Programming Scripts, Attachment Files, and Other Files Product archiving feature: • Inactive products can be archived or unarchived, with their status clearly displayed in the product list. Archived or unarchived products can be quickly filtered • Archived products can't be edited (including information modification, resource configuration, version or batch creation, etc.), but programming of already created batches remains	

Feature Categories	Key Updates	Description	Related Documents
		unaffected Remove the Mark field from the product: • The Mark field is no longer required when creating a product and will no longer appear on the product page • For existing products, the Mark field will automatically be appended to the product name	

Feature Categories	Key Updates	Description	Related Documents

Version	Supports tab switching, long names, mass production marking, and multi-select firmware addition	• Tab switching: When creating a version, you can switch tabs to check other product information
		• Version name: Supports a length of 128 characters
		• Mass production mark: You can mark a version as **Mass Production**. This mark will then appear in the batch list
		• Firmware addition optimization:
		  ◦ Clicking **Add** displays a firmware list, supporting searching by filename or version
		  ◦ Supports multi-selection for adding firmware, improving operational efficiency
			Product - Create a version

Feature Categories	Key Updates	Description	Related Documents
Batch	• Supports tab switching, long names, and display of version mass-production information; simplifies factory selection and enables automatic script matching • Enhances batch and data synchronization status management, with a resynchronization feature	Batch optimization: • Tab switching: When creating a batch, you can switch tabs to check other product information • Batch name: Supports a length of 128 characters • Version information display: Displays whether a selected version is in mass production and its configuration region • Simplified factory selection: Only the factory needs to be selected; selecting a Factory Manager is no longer required • Automatic script matching: Automatically matches the programming script based on the chip	Product: • Create a batch • Check batches

Feature Categories	Key Updates	Description	Related Documents
		configured for the selected version Batch status optimization: • Batch status: Indicates the complete lifecycle of a batch, including **Generating**, **Generated**, **Generate Failed**, **Running**, **Completed**, **Stopped**, and **Expired** • Batch synchronization status: Indicates the status of batch data synchronization to the factory, including **Waiting**, **Syncing**, **Sync Failed**, **Synced**, and **Deleted** • Programming data synchronization status: Indicates the data synchronization status of batch programming,	

Feature Categories	Key Updates	Description	Related Documents
		including **No Records**, **Uploading**, and **Uploaded** • Resynchronization feature: For batches that fail to synchronize (batch status is **Generate Failed** or batch synchronization status is **Sync Failed**), click **Resync** in the batch list to resend the batch to the factory	

Feature Categories	Key Updates	Description	Related Documents
Factory	Supports creating cloud factories	• Cloud factory creation: Enables creating cloud factories in OBIS, including programming stations that support password or Identity U-Safe login • Cloud factory management: Allows management of cloud factory batches and programming station assignment in OBIS, including starting and stopping batches	Factory: • Create a factory • Manage factories and programming stations: Cloud factory: ▪ Configure and manage factories ▪ Configure and manage programming stations ▪ Manage batches and assign programming stations • Check factories

Feature Categories	Key Updates	Description	Related Documents
KMS	Added **Complete**, **Download**, and **Archive** options	• Key creation: Select **Complete** to proceed with key creation • Key download: Supports downloading the public key for asymmetric keys • Key archiving: Allows archiving of inactive keys. Active keys are displayed first, while archived keys are hidden by default for easier daily management	KMS - Manage keys

Feature Categories	Key Updates	Description	Related Documents
OnBoard Edge Service	• Added **Factory**, **Batch**, and **Station** menus • Supports multiple HSM U-Safes programming	• Factory management: Supports factory management within OnBoard Edge Service, including batch management, programming station assignment, and programming station configuration • Multiple HSM U-Safes programming: The Edge-Service server can accommodate multiple HSM U-Safes, enhancing programming performance and concurrency	OnBoard Edge Service: • Sign-in • Manage factories • Manage batches and assign programming stations • Configure and manage programming stations

Feature Categories	Key Updates	Description	Related Documents
Programming Station	• Added new login methods for cloud factories • Supports switching programming scripts and custom download paths • Added display and alerts for programming concurrent load	• Cloud factory sign-in: Allows sign-in using password or Identity U-Safe • Local programming script management: Supports switching programming scripts and customizing the script download path • Programming concurrent load alerts: ◦ The client displays real-time concurrent load in the bottom-left corner ◦ When the load ≥ 90%, a warning is displayed; at 100% load, a high-load alert appears, facilitating operation and	Programming Station: • Sign-in • Execute device programming

Feature Categories	Key Updates	Description	Related Documents
		monitoring	

Version: v3.4.0 (Latest)

How to configure SSO for Microsoft work accounts in OnBoard™ IoT Security

> **TIP**
>
> The Single Sign-On (SSO) feature in OnBoard™ IoT Security (OBIS) allows users to sign in with their company email through the Enterprise Identity Provider (IdP). OBIS will automatically create an account for them and assign default role permissions.

This article will guide you on how to configure and enable the Sign in with SSO feature in OBIS for Microsoft work accounts. Once enabled, users can sign in to OBIS using their work accounts and passwords.

Prerequisites

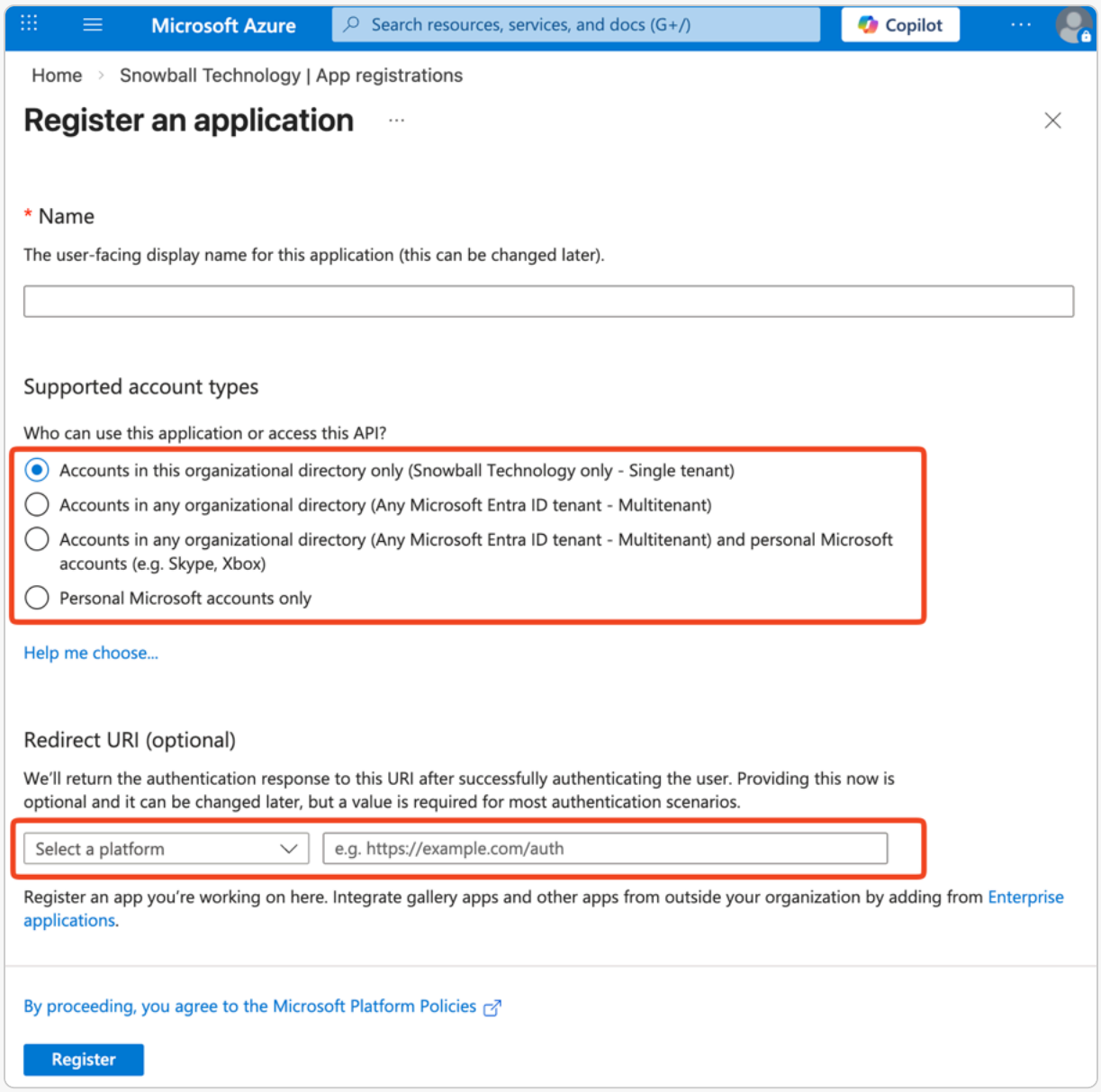
Before getting started, please ensure that you have obtained the Redirect URL required to configure SSO from Snowball.

Instructions

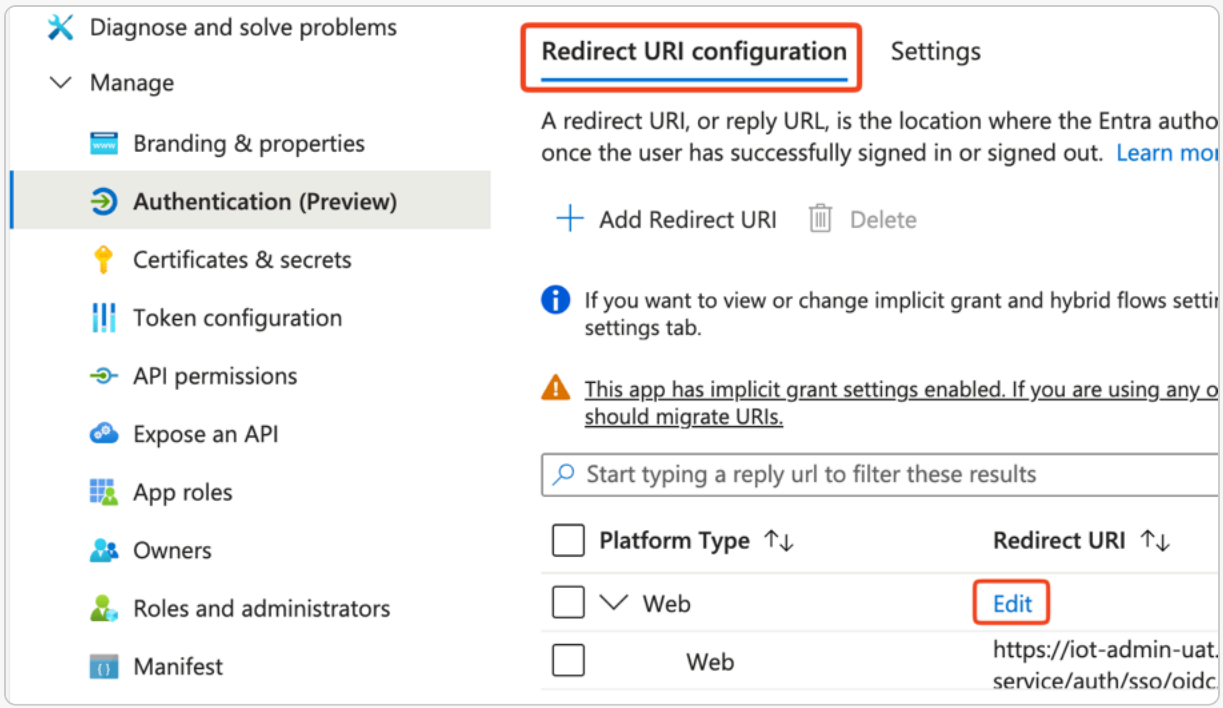
1. Sign in to the Microsoft Azure portal.
2. In the search box at the top, search for and select **Microsoft Entra ID**.

3. In the left menu, click **Manage** > **App registrations** > **New registration**. On the **Register an application** page, enter the application name and then select the **Supported account types**.

4. In the **Redirect URI** section, select **Web** as the platform, enter the Redirect URL obtained from Snowball, and then click **Register**.

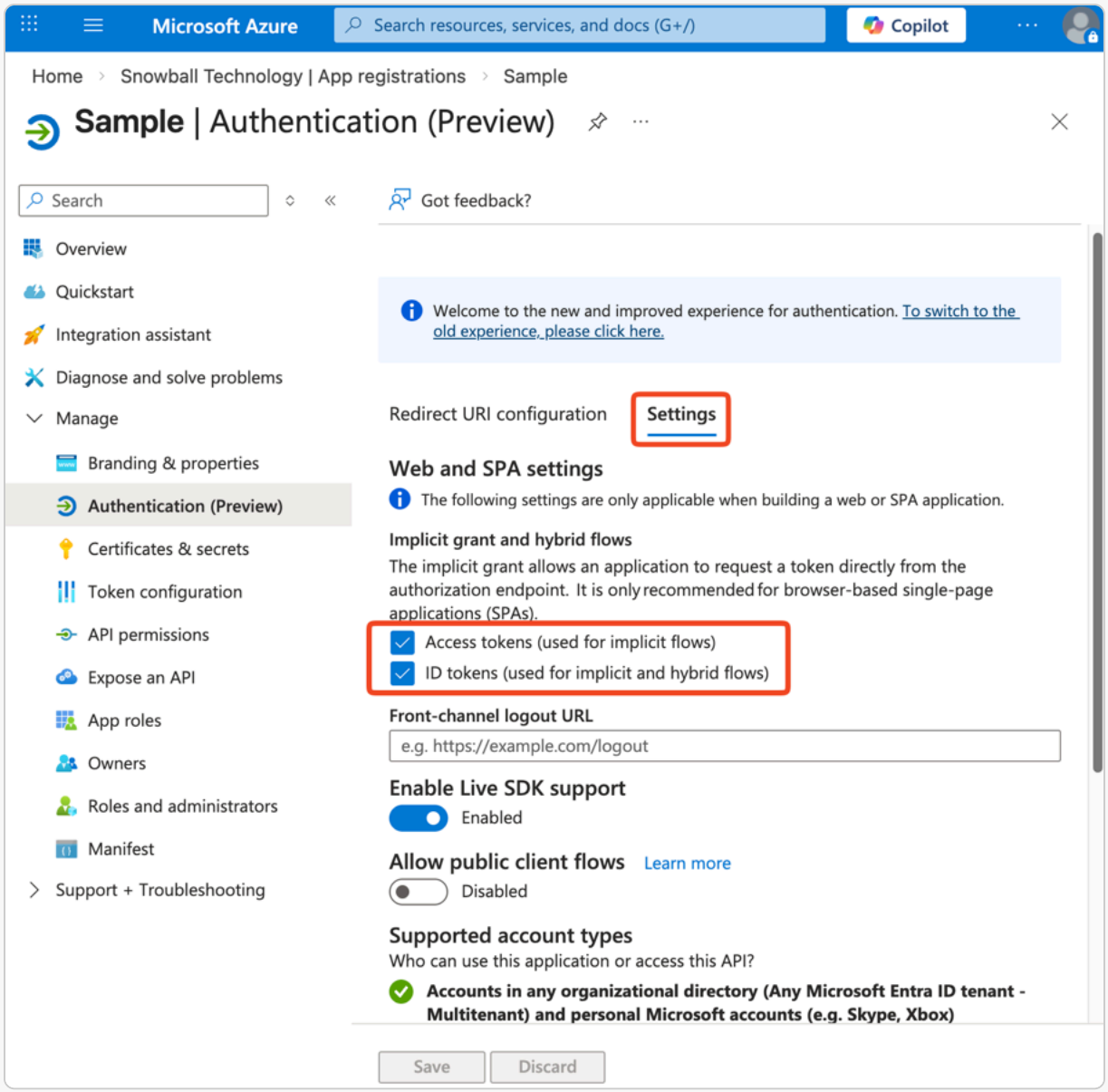


If you need to change the Redirect URI later, click **Manage** > **Authentication (Preview)** in the left menu of the application, and then make the edit on the **Redirect URI configuration** tab.



5. In the left menu of the application, click **Manage** > **Authentication (Preview)** > **Settings**, and then select the **Access tokens (used for implicit flows)** and **ID tokens (used for implicit and hybrid flows)** checkboxes.

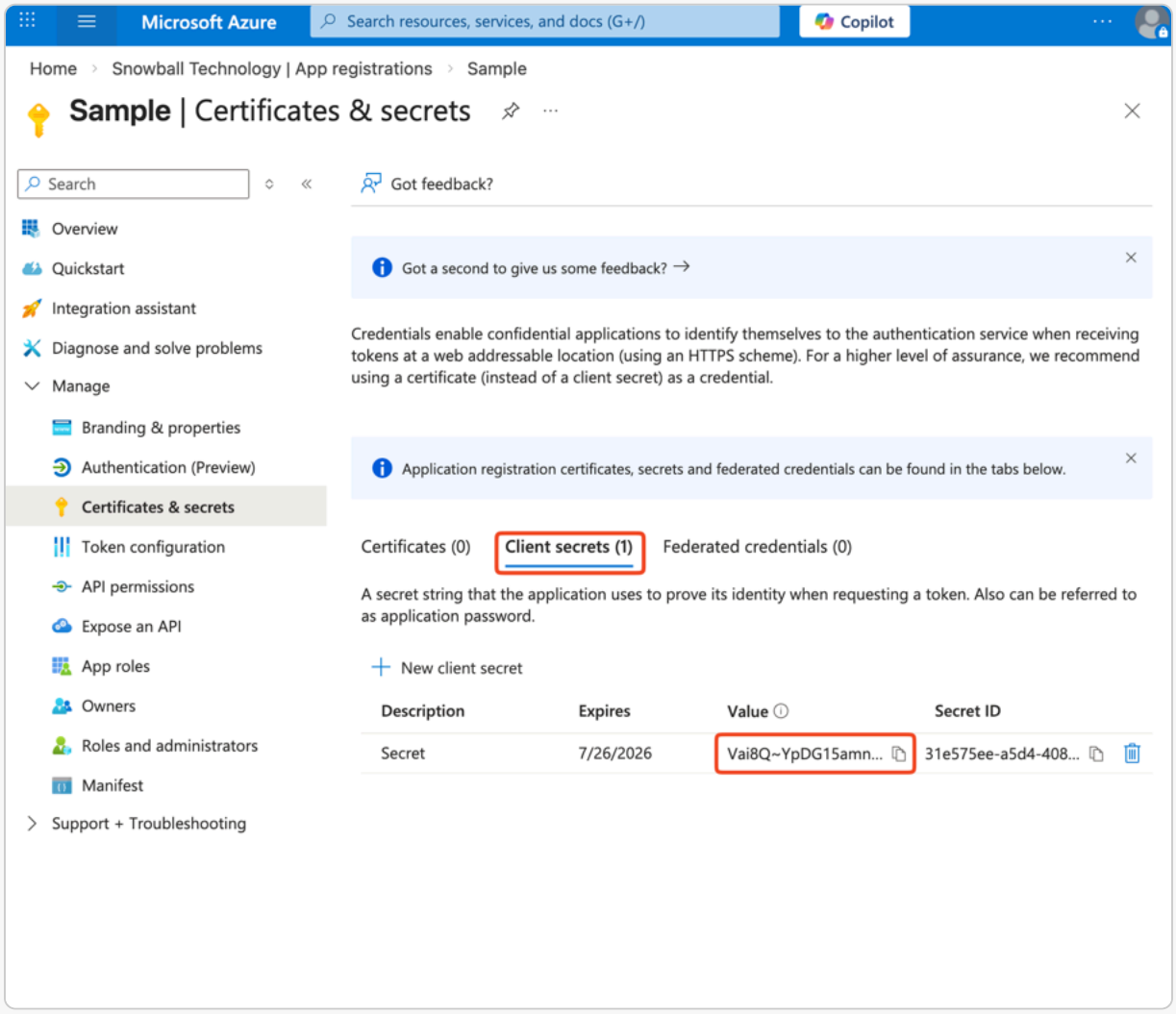
> **TIP**
>
> The Access token is used to call the API for retrieving user information, while the ID token is used for parameter validation during the SSO sign-in process.



6. In the left menu of the application, click **Manage** > **Certificates & secrets** > **Client secrets** > **New client secret**. On the **Add a client secret** panel, enter the client secret description, select the expiration date, and then click **Add**.

7. Record the client secret value. This secret value is never displayed again after you leave this page.

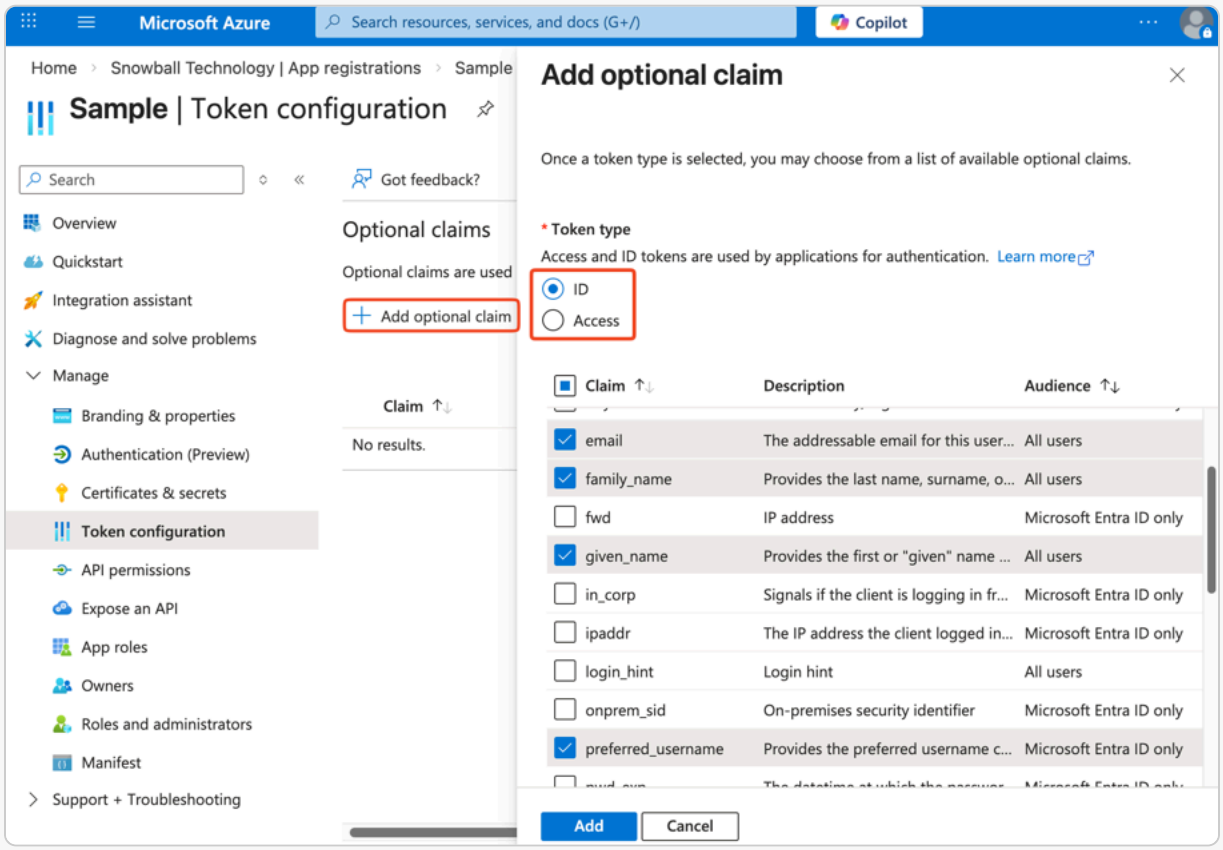
> **TIP**
>
> The client secret of the currently authorized application is used to verify application information through callbacks, ensuring that the source of the authorization request is trusted.



8. In the left menu of the application, click **Manage** > **Token configuration** > **Add optional claim**, then configure and add the ID token and access token separately.

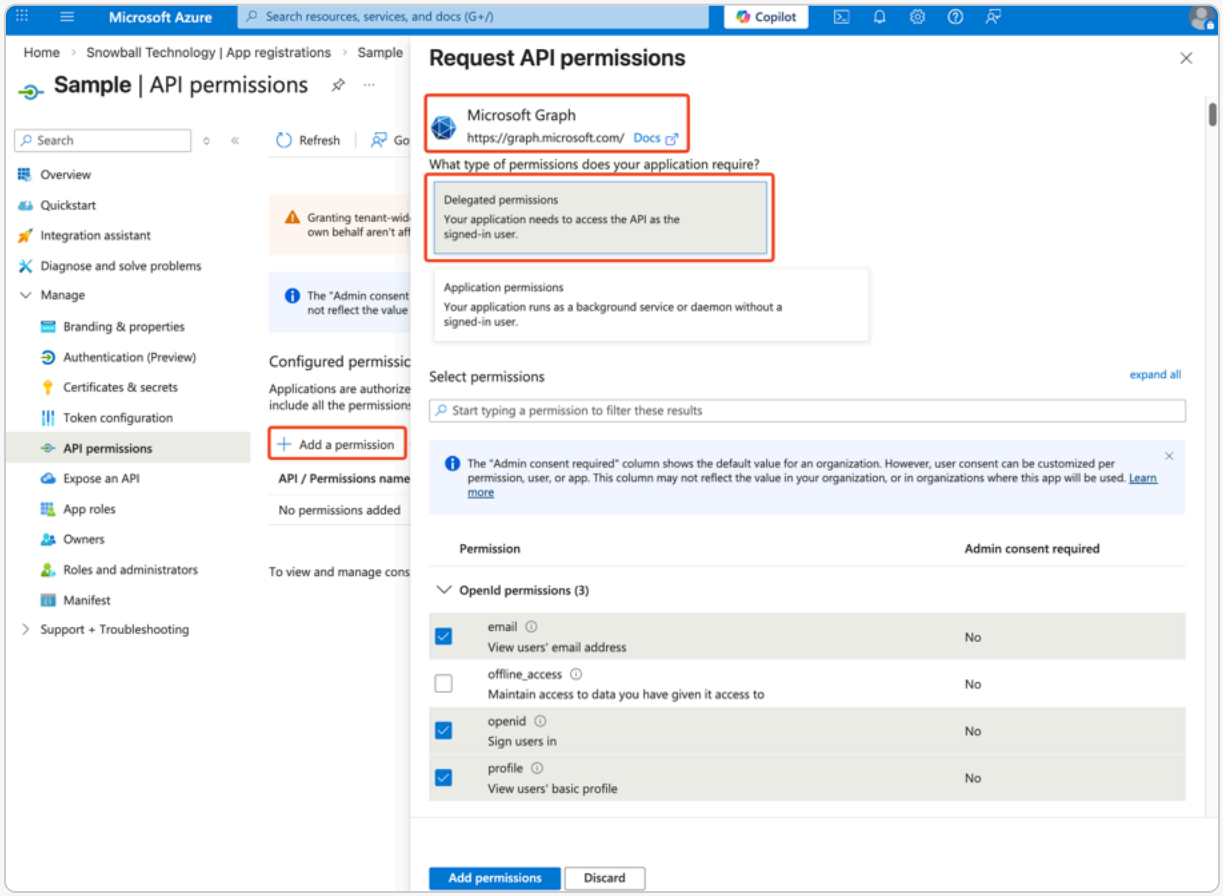
> **TIP**
>
> The optional claims correspond to the information returned by Microsoft to the platform during the authentication callback.

- Select **ID** as the **Token type**, and then select **email**, **family_name**, **given_name**, and **preferred_username**
- Select **Access** as the **Token type**, and then select **email**, **family_name**, **given_name**, and **preferred_username**



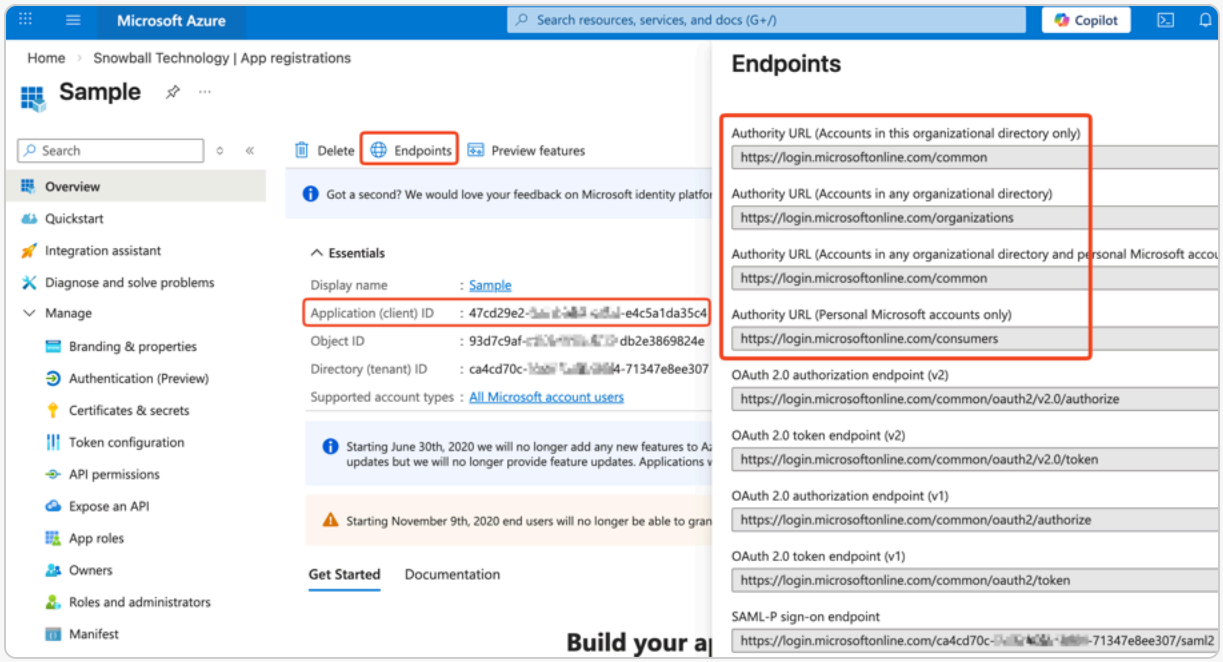
9. In the left menu of the application, click **Manage** > **API permissions** > **Add a permission**. On the **Request API permissions** panel, select **Microsoft Graph** > **Delegated permissions**. In the **OpenId permissions** section, select the corresponding permissions (it is recommended to select **email**, **openid**, and **profile**), and then click **Add permissions**.

> **TIP**
>
> The API permissions configured here correspond to the scope settings in OBIS for SSO.



10. Once the application configuration is complete, please provide the following information to Snowball, so that we can enable the **Sign in with SSO** feature for your tenant in OBIS.

    - **Email Domain**: The email domain of your Microsoft work account
    - **Issuer**: On the **Overview** page of the application, click **Endpoints**, and then copy the relevant **Authority URL**
    - **Client ID**: On the **Overview** page of the application, copy the **Application (client) ID**
    - **Client Key**: The client secret recorded in step 7



Make Security Simple

上海雪球数智科技有限公司

Shanghai Snowball Digital Intelligence Technology Co., Ltd

www.snowballtech.com

info@snowballtech.com

Floor 19, Building T2, Yuqiao Smart Bay, 968 Yuqiao Road, Pudong New Area, Shanghai

Visit Website

www.snowballtech.com

© 2026 Shanghai Snowball Digital Intelligence Technology Co., Ltd. All rights reserved.

This document is for reference only and does not constitute any warranty, express or implied.

To cite or use this document, please contact Shanghai Snowball Digital Intelligence Technology Co., Ltd. for authorization.