



Secure Equipment Access Overview

- [Cisco Secure Equipment Access service, on page 1](#)
- [Prerequisites for enabling SEA, on page 1](#)
- [Enabling the SEA service, on page 2](#)

Cisco Secure Equipment Access service

Cisco Secure Equipment Access is a remote access solution that

- provides secure, managed connectivity to industrial IoT devices,
- integrates hybrid-cloud control through Cisco IoT Operations Dashboard, and
- enables customers and partners to perform maintenance on OT assets at remote sites.

The on-premises component runs on supported industrial network devices.

Prerequisites for enabling SEA

You must meet the following prerequisites before enabling SEA on IE switches:

- Ensure you have a valid IoT Operations Dashboard (IoT OD) organization (cloud tenant). If you don't have one, send a request to <mailto:iotod-account-request@cisco.com>.
- Confirm you have SEA System Admin roles in the organization.
- The switch must have an SD card.
- The switch must run Cisco IOS XE version 17.14.1 or later.
- Ensure the switches have an active Internet connection to us.ciscoiot.com or eu.ciscoiot.com, depending on the IoT OD cluster used.

Enabling the SEA service

Summary

The key components or participants involved in the process are:

- Network administrator: Configures and manages the IE switches.
- IE switches: The device that is prepared and configured for enabling SEA service.
- SEA agent: An IOx application that runs on the device.

Workflow

These are the stages for enabling SEA service on your switches:

1. Onboard the required switches to the Cisco IoT Operations Dashboard.
2. Create access control groups and add users and assets to the groups.
3. Configure remote sessions.

Result

The switch is enabled with SEA, allowing secure remote access for operational tasks.