Enable Zero Trust Network Access for Industrial Networks with Cisco Secure Equipment Access

Andrew McPhee - IIoT Security Solution Manager
Emmanuel Tychon - IIoT TME

BRKIOT-1005

slido.com #3653386

Let’s start with Slido

kd1hbh

Agenda

- Cyber security mandates for remote access
- Remote Access Technologies and Cyber Security
- Secure Equipment Access
- Q&A

slido

Please download and install the Slido app on all computers you use

What technology do you currently use for remote access to the OT network? Select all that apply.

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

Is your remote access solution dedicated to the OT? Or do you leverage the existing IT implementation?

ⓘ Start presenting to display the poll results on this slide.

Please download and install the Slido app on all computers you use

What are your biggest challenges with your current implementation?

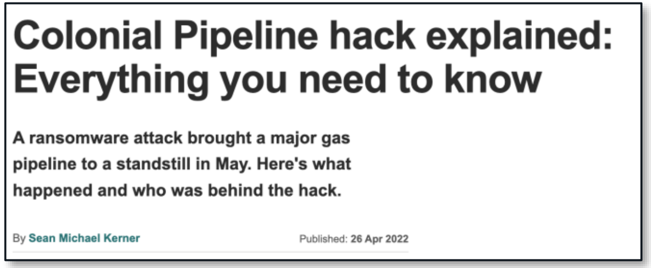
ⓘ Start presenting to display the poll results on this slide.

Is Security really top of mind?

Between 2019 and 2023, attacks causing physical consequences to OT networks are almost doubling every year[1]

Yet, malware free activity (such as identity attacks) represented 75% of detections in 2023 – up from 71% in 2022[2]

VPN with no MFA



Colonial Pipeline hack explained: Everything you need to know

A ransomware attack brought a major gas pipeline to a standstill in May. Here's what happened and who was behind the hack.

By Sean Michael Kerner Published: 26 Apr 2022

[1] Waterfall 2024 Threat Report – OT Cyberattacks with Physical Consequences

[2] Crowdstrike 2024 Global Threat Report

Problems with our existing remote access solutions

Unknown remote access gateways

No visibility into user activity

VPN / Jump servers with full plant access

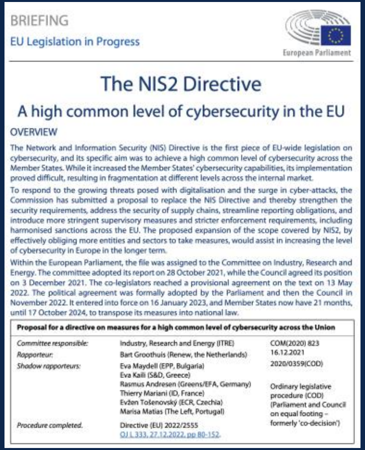
No Multi-Factor Authentication (MFA)

24/7 availability

For many, these are not new problems, and an attacker just needs a single entry to cause damage

Mandates must be implemented to drive change

NIS2



BRIEFING

EU Legislation in Progress

European Parliament

The NIS2 Directive

A high common level of cybersecurity in the EU

OVERVIEW

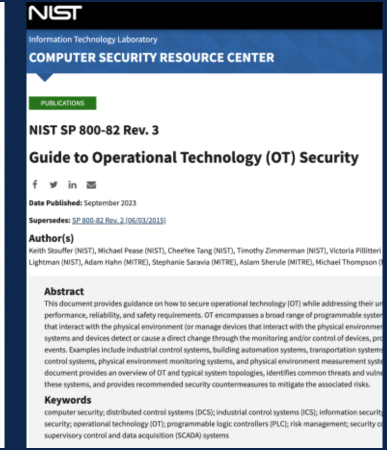
The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Proposal for a directive on measures for a high common level of cybersecurity across the Union		
Committee responsible:	Industry, Research and Energy (ITRE)	COM(2020) 823 16.12.2021
Rapporteur:	Bart Groothuis (Renew, the Netherlands)	
Shadow rapporteurs:	Eva Maydell (EPP, Bulgaria) Eva Kaili (S&D, Greece) Rasmus Andresen (Greens/EFA, Germany) Thierry Mariani (ID, France) Evžen Tošenovský (ECR, Czechia) Marisa Matias (The Left, Portugal)	2020/0359(COD) Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Procedure completed.	Directive (EU) 2022/2555 OJ L 333, 27.12.2022, pp 80-152.	

NIST



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST SP 800-82 Rev. 3

Guide to Operational Technology (OT) Security

Date Published: September 2023

Supersedes: SP 800-82 Rev. 2 (06/03/2015)

Author(s)

Keith Stouffer (NIST), Michael Pease (NIST), CheeYee Tang (NIST), Timothy Zimmerman (NIST), Victoria Pillitteri
Lightman (NIST), Adam Hahn (MITRE), Stephanie Saravia (MITRE), Aslam Sherule (MITRE), Michael Thompson (

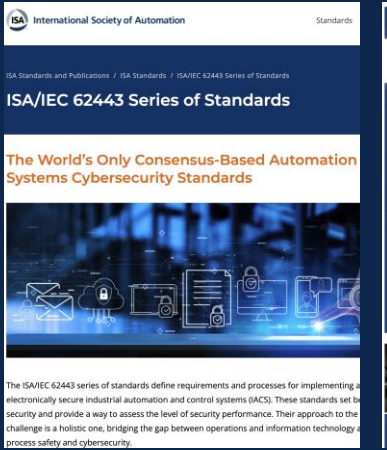
Abstract

This document provides guidance on how to secure operational technology (OT) while addressing their un
performance, reliability, and safety requirements. OT encompasses a broad range of programmable systen
that interact with the physical environment (or manage devices that interact with the physical environmer
systems and devices detect or cause a direct change through the monitoring and/or control of devices, pro
events. Examples include industrial control systems, building automation systems, transportation systems
control systems, physical environment monitoring systems, and physical environment measurement syste
document provides an overview of OT and typical system topologies, identifies common threats and vulne
these systems, and provides recommended security countermeasures to mitigate the associated risks.

Keywords

computer security; distributed control systems (DCS); industrial control systems (ICS); information security
security; operational technology (OT); programmable logic controllers (PLC); risk management; security co
supervisory control and data acquisition (SCADA) systems

ISA/IEC-62443



ISA International Society of Automation

Standards

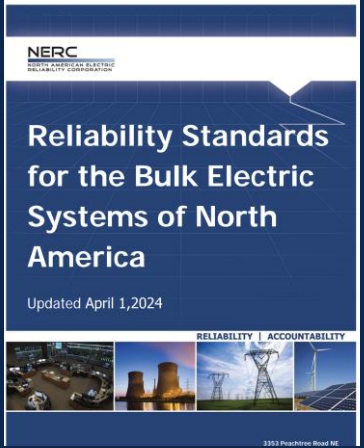
ISA Standards and Publications / ISA Standards / ISA/IEC 62443 Series of Standards

ISA/IEC 62443 Series of Standards

The World's Only Consensus-Based Automation Systems Cybersecurity Standards

The ISA/IEC 62443 series of standards define requirements and processes for implementing a
electronically secure industrial automation and control systems (IACS). These standards set be
security and provide a way to assess the level of security performance. Their approach to the
challenge is a holistic one, bridging the gap between operations and information technology a
process safety and cybersecurity.

NERC CIP



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

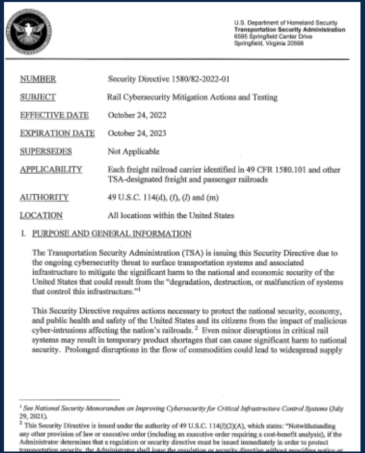
Reliability Standards for the Bulk Electric Systems of North America

Updated April 1,2024

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE

TSA



U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

NUMBER	Security Directive 1580/82-2022-01
SUBJECT	Rail Cybersecurity Mitigation Actions and Testing
EFFECTIVE DATE	October 24, 2022
EXPIRATION DATE	October 24, 2023
SUPERSEDES	Not Applicable
APPLICABILITY	Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads
AUTHORITY	49 U.S.C. 114(d), (f), (*l*) and (m)
LOCATION	All locations within the United States

I. PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this Security Directive due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to mitigate the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure."[1]

This Security Directive requires actions necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation's railroads.[2] Even minor disruptions in critical rail systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply

[1] *See National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021).

[2] This Security Directive is issued under the authority of 49 U.S.C. 114(*l*)(2)(A), which states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or

Mandates must be implemented to drive change

NIS2

*the use of **multi-factor authentication** or continuous authentication solutions*

NIST

MFA is an accepted best practice for remote access to OT applications

ISA/IEC-62443

SR 1.1 RE 2 – MFA for untrusted networks

SR 1.1 RE 3 – MFA for all networks

NERC CIP

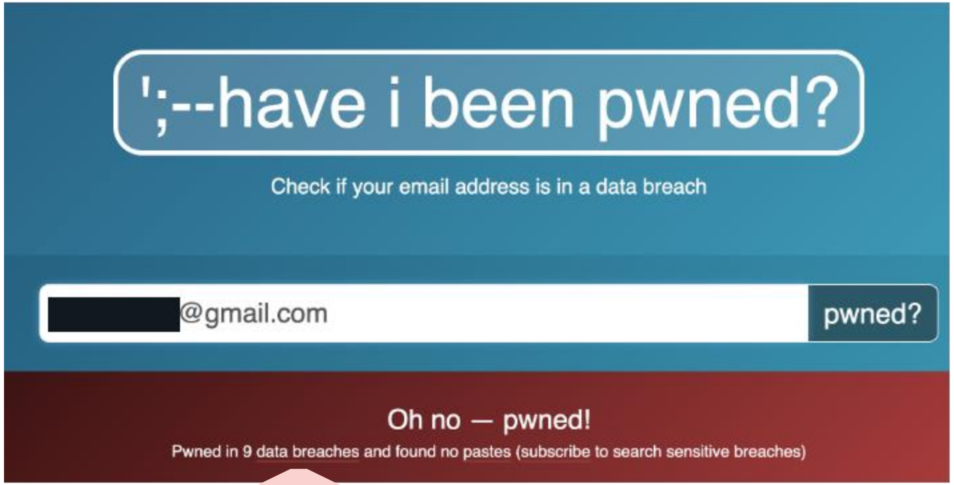
005-7 – Remote Access Management: Require MFA

TSA

MFA, or other logical and physical security controls that supplement password authentication

The Importance of MFA

Have I been Pwned?



';--have i been pwned?

Check if your email address is in a data breach

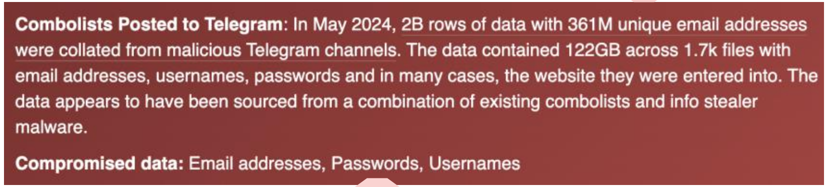
[redacted]@gmail.com

Oh no — pwned!

Pwned in 9 data breaches and found no pastes (subscribe to search sensitive breaches)

9 data breaches

361M unique email addresses



Combolists Posted to Telegram: In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.

Compromised data: Email addresses, Passwords, Usernames

Passwords,

Multi-Factor Authentication (MFA)

Something you **know**

- Password
- PIN
- Email Verification

Something you **have**

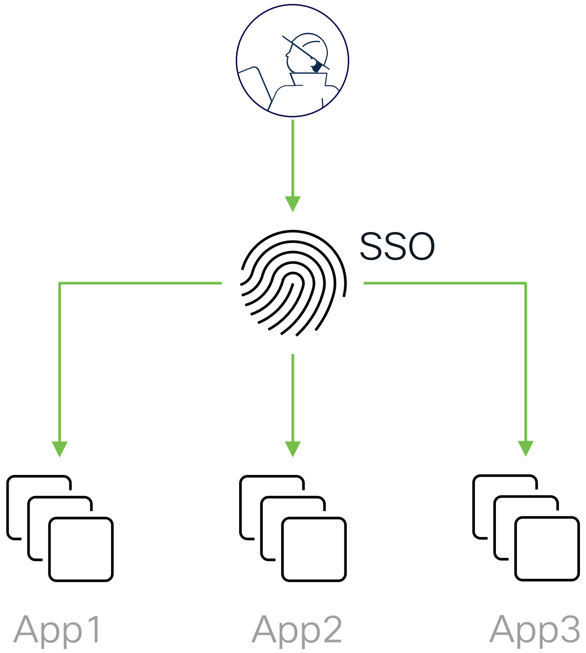
- Mobile
- Yubikey

Something you **are**

- Fingerprint
- Facial Recognition

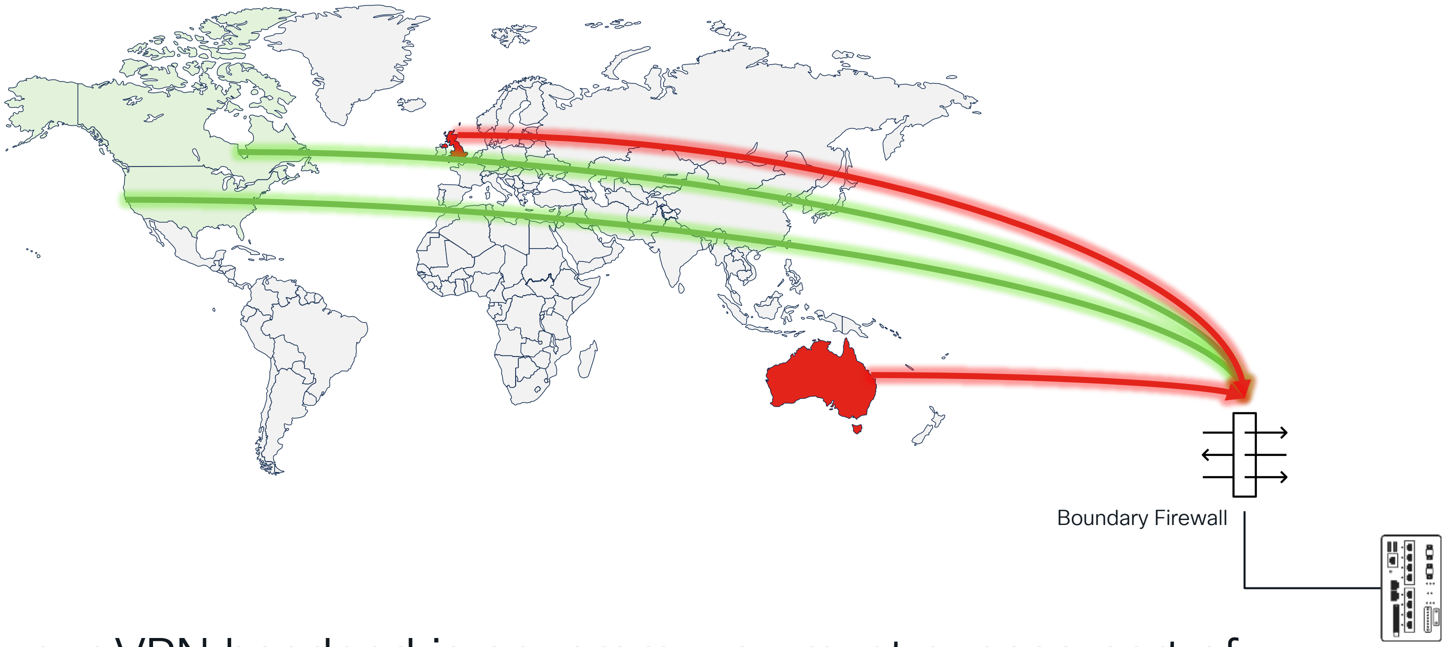
Single Sign-On (SSO)

- One authentication for many applications
- Reduces password sprawl
- Single set of policies across all your applications



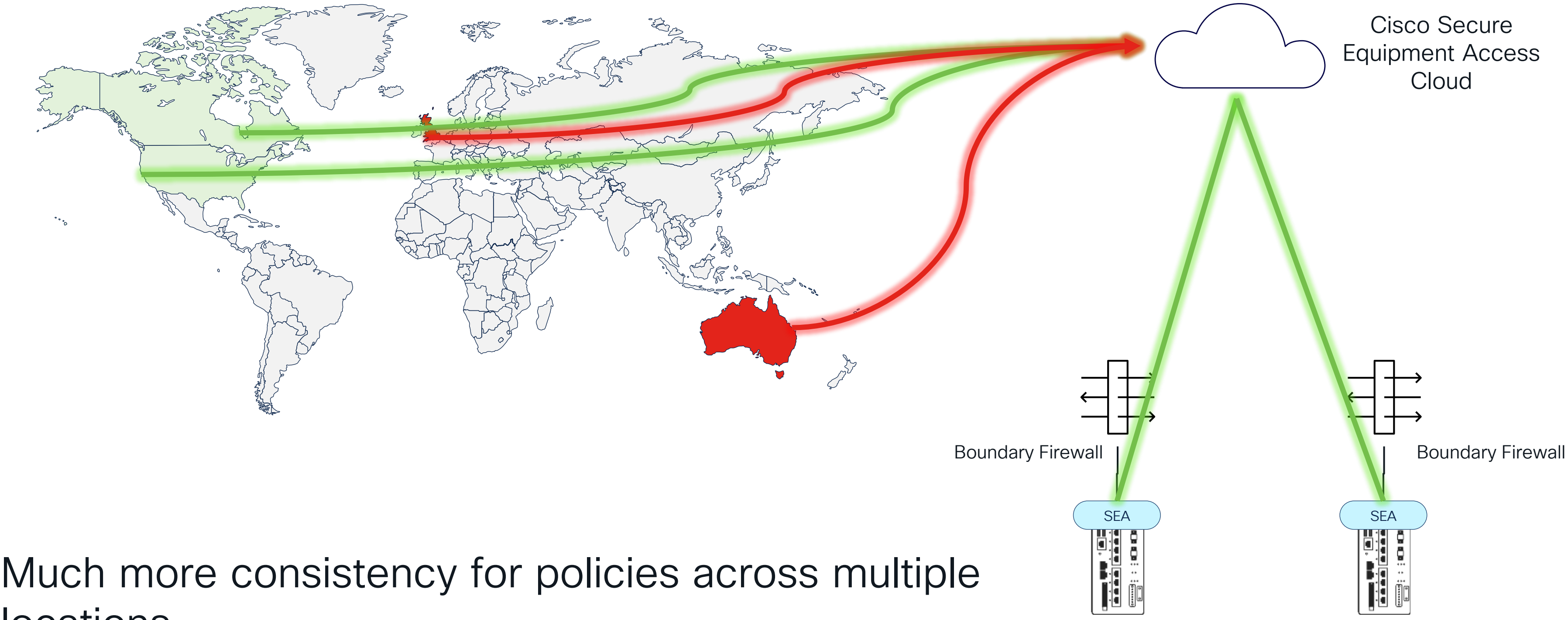
Is cloud based remote access risky?

Remote users come from outside of your network



If your VPN headend is on-prem, you must expose part of your network to the public

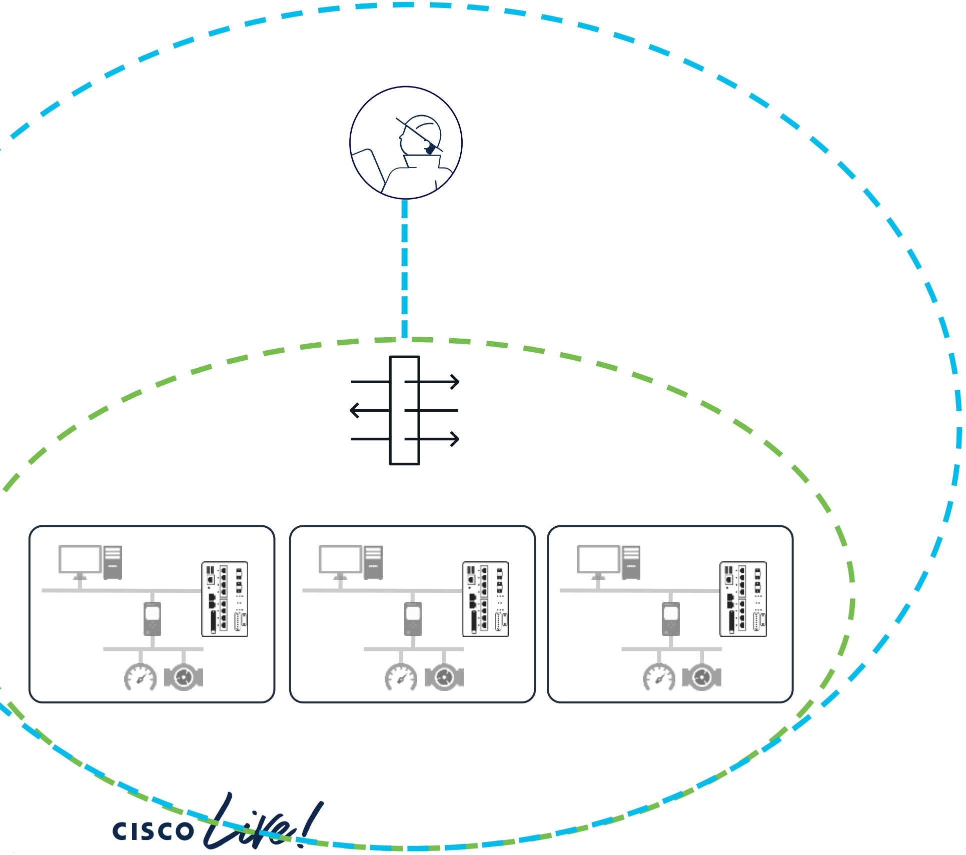
OT Network only needs a single trusted flow through the firewall



Much more consistency for policies across multiple locations

Remote Access Technologies

Virtual Private Network (VPN)



- Extends the network to remote users

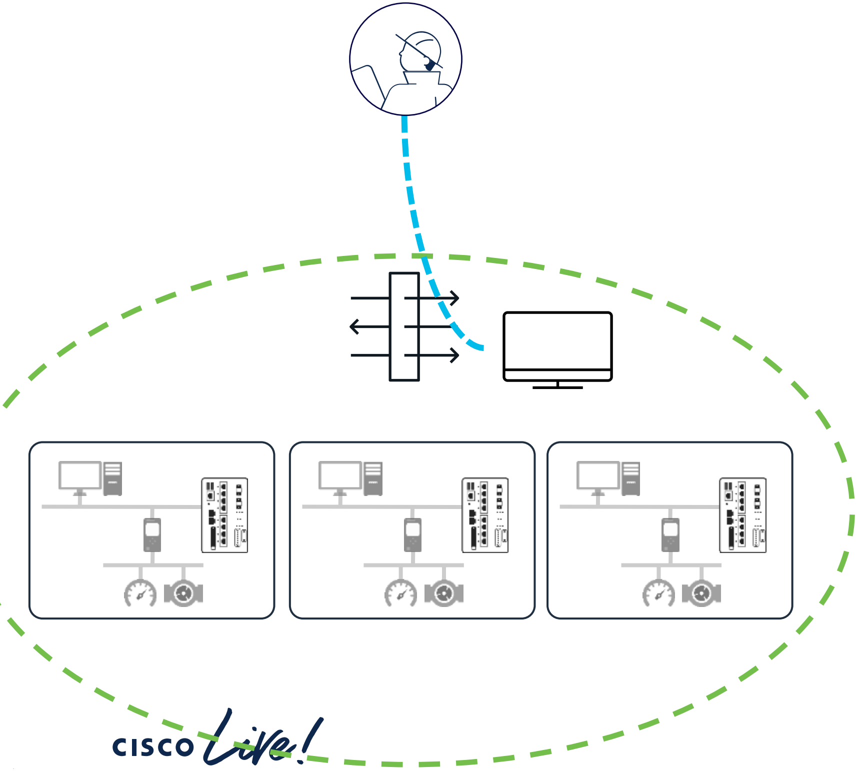
Pros

- Users can use applications hosted natively on their devices
- Minimal friction from end user experience

Cons

- Users have an IP address on your network
- Additional steps for lateral movement and reconnaissance to be prevented
- VPN headend has public IP that will be targeted
- Client can sometimes be a burden
- MFA an additional add-on

Jump Servers



- Users do all their tasks from a trusted device hosted in the network

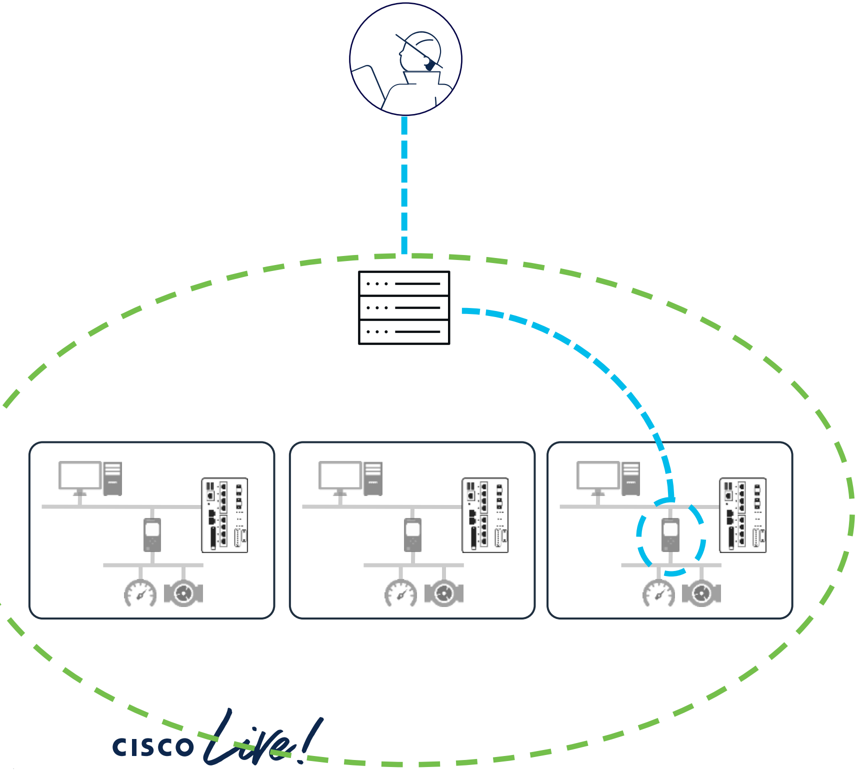
Pros

- Minimize the risk of introducing malware from client device
- Devices can be locked down to only permitted applications
- Jump servers can reside in isolated state until needed

Cons

- Additional overhead often leads to over privileged jump servers
- Must maintain vendor applications
- MFA still not a hard requirement

Shift to Zero Trust Network Access (ZTNA)



- Users have proxied access to specific endpoints / applications

Pros

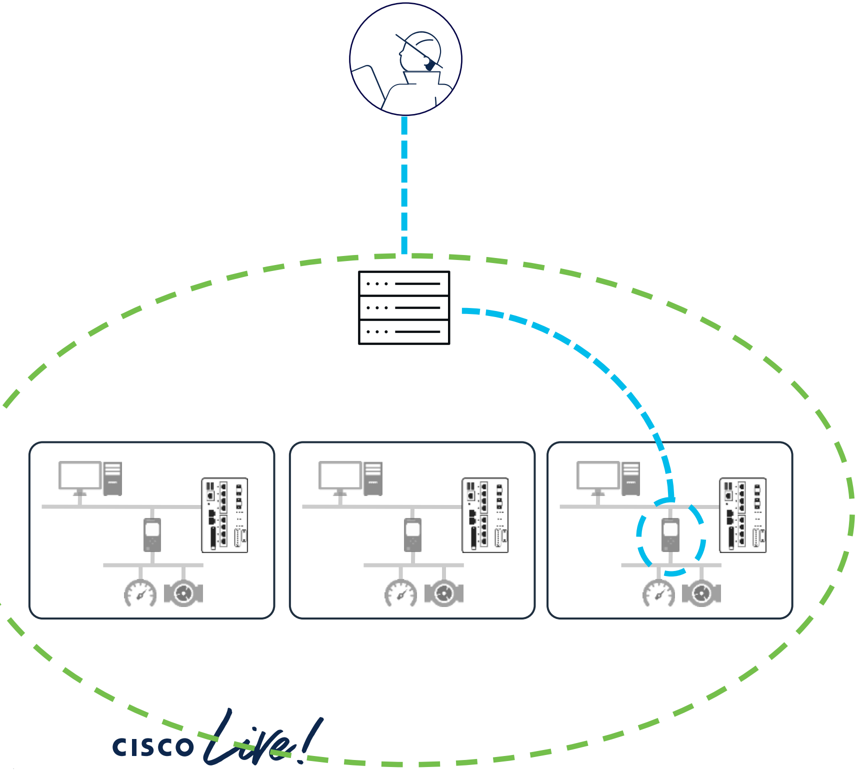
- Users only have access to what they need
- MFA is natively built in
- Clientless connectivity
- ZTNA gateway establishes outbound connection to a trusted cloud*

Cons

- Clientless connectivity does not cover every protocol
- Clients will be needed in some cases

*some solutions can offer ZTNA gateway to be first point of entry

Remote Privileged Access Management (RPAM)



- Very similar to ZTNA, but with extended features

Pros

- Users only have access to what they need
- MFA is natively built in
- Scheduled Access
- Session Monitoring and Recording
- Session Approval flows

Cons

- Clientless connectivity does not cover every protocol
- Clients will be needed in some cases

Cisco Secure Equipment Access

Agenda

- Introduction
- SEA and SEA Plus
- Session Management
- Request and Approvals
- VLAN access
- Installation and Management
- Where is it used?
- Demo

Secure Remote Access for OT

Remote access to OT assets is key for operations

Maintenance

Remote configuration and maintenance by vendors and third-party technicians.

Troubleshooting

Remote experts helping quickly solve issues to maintain production uptime.

Avoiding Truck Rolls

Large sites, distributed operations, limited resources. Remote access helps lower OpEx.

Roadways | Transportation | Renewables | EV chargers | Utilities | Manufacturing | Oil & Gas | Mining | Ports

Operations need remote access to all assets at anytime, for internal and external experts

What do IT and OT users want?

Operational Efficiency

- ✓ Gain instant access to remote assets from anywhere in case of emergencies
- ✓ Be capable of easily creating remote access credentials when needed
- ✓ Be able to use any remote access protocol depending on the need
- ✓ Access to audit trails to understand what changes have been made to an asset

Cybersecurity

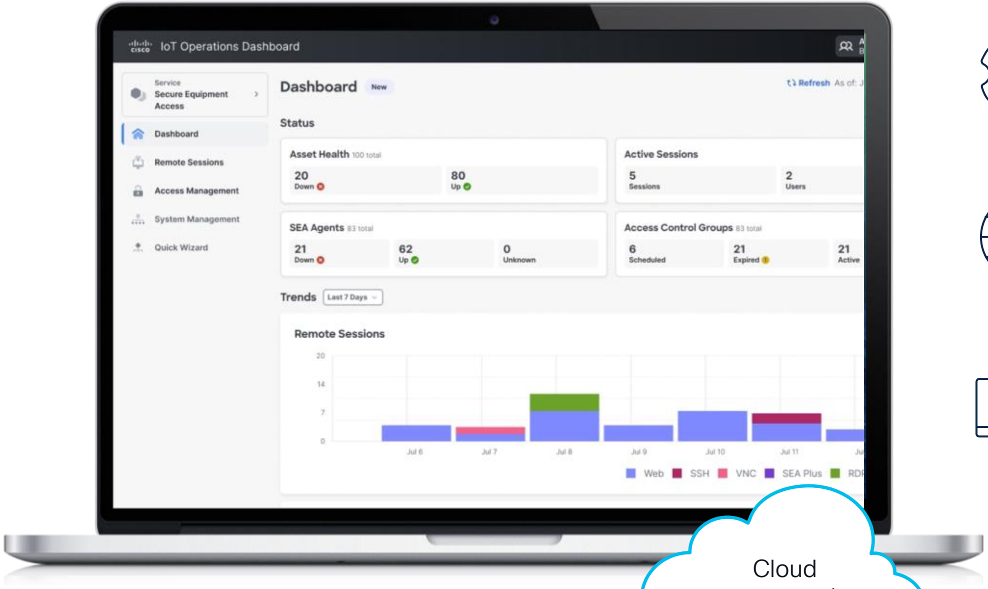
- ✓ Ensure only legitimate users can connect, and never to the entire network
- ✓ Verify remote computers’ posture to avoid malware
- ✓ Simplify architecture to lower costs and avoid complex DMZ/firewall setups
- ✓ Have access to audit trails for regulatory compliance and investigations

Modern industrial operations require both OT agility and IT security

IoT Operations Dashboard

Cisco Secure Equipment Access

Purpose-built for Industrial and OT



Dashboard

Status

Asset Health 100 total
20 Down
80 Up

Active Sessions
5 Sessions
2 Users

SEA Agents 83 total
21 Down
62 Up
0 Unknown

Access Control Groups 83 total
6 Scheduled
21 Expired
21 Active

Trends

Remote Sessions

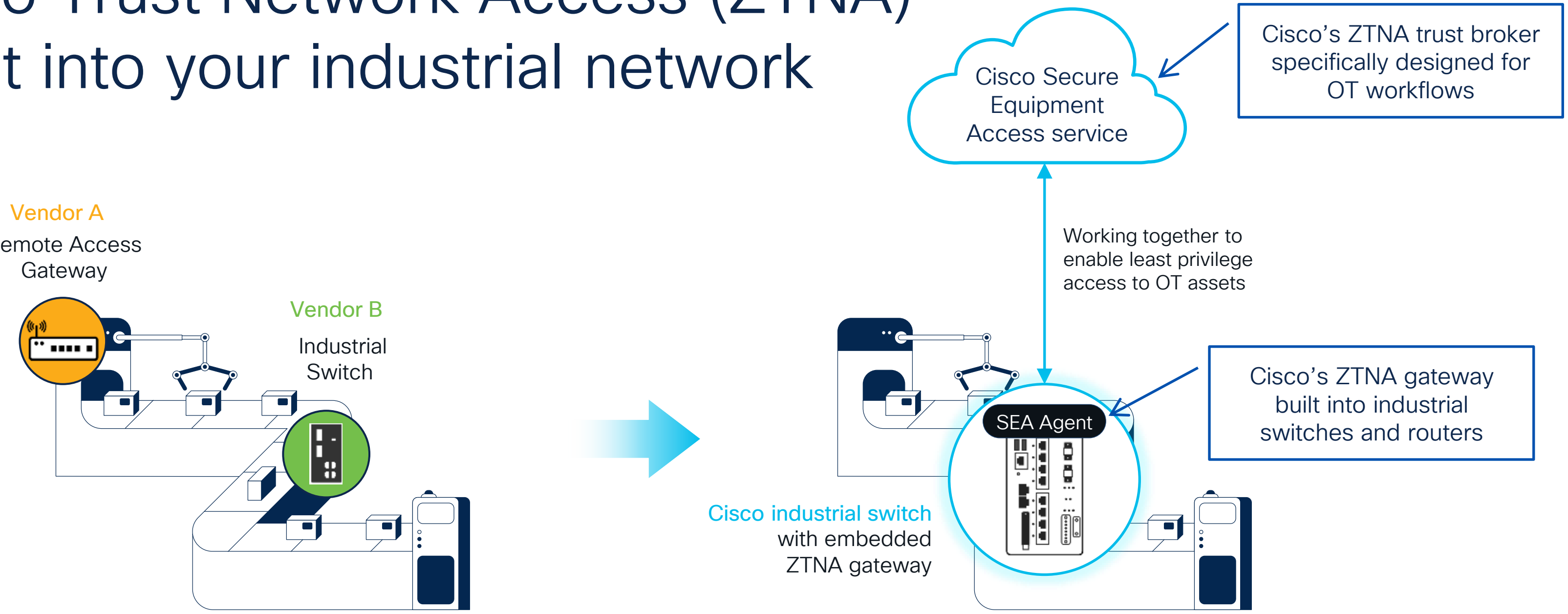
Cloud managed

Centralized cloud enforced policy
Define and enforce ZTNA controls with a cloud-based trust broker

Install and scale with ease
Deploy and monitor network embedded ZTNA gateway agents at scale from the cloud

Access any remote asset the way you want
Connect any OT asset to a Cisco IE switch or IR router and securely access it from anywhere in the world

Zero Trust Network Access (ZTNA) built into your industrial network



Vendor A

Remote Access Gateway

Vendor B

Industrial Switch

Cisco Secure Equipment Access service

Cisco's ZTNA trust broker specifically designed for OT workflows

Working together to enable least privilege access to OT assets

SEA Agent

Cisco's ZTNA gateway built into industrial switches and routers

Cisco industrial switch with embedded ZTNA gateway

Eliminating complexity by converging functionalities as software features on Cisco's industrial network

Platforms that support SEA Agent

SEA Agent is the ZTNA gateway function embedded in network platforms

Industrial Switches

IE3300, IE3400

IE3400H

IE3100

IE9300

Industrial Routers

IR1101

IR1800

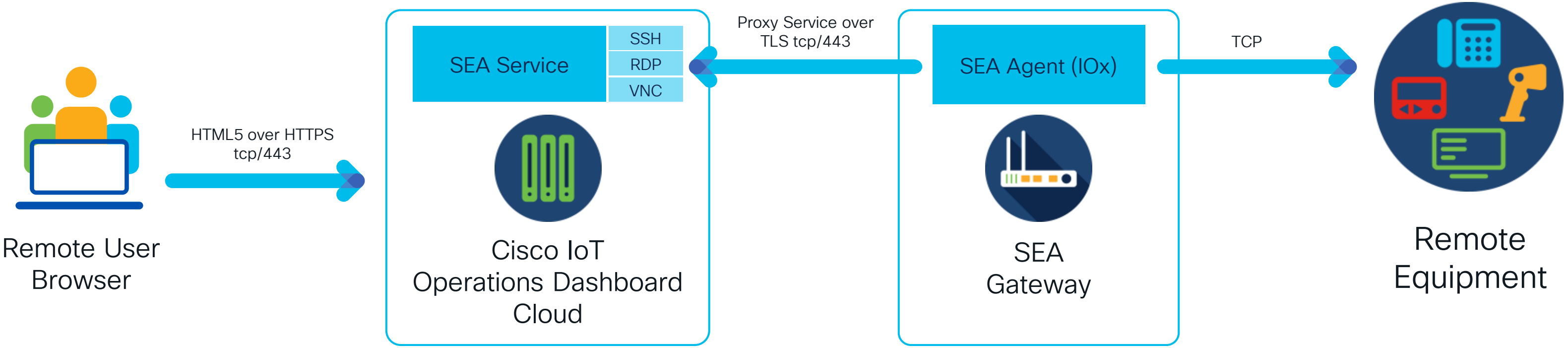
Roadmap

IR8300

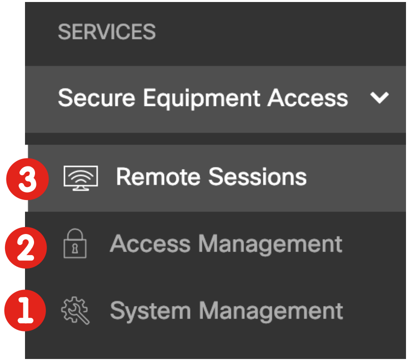
Cisco Secure Equipment Access SEA and SEA Plus

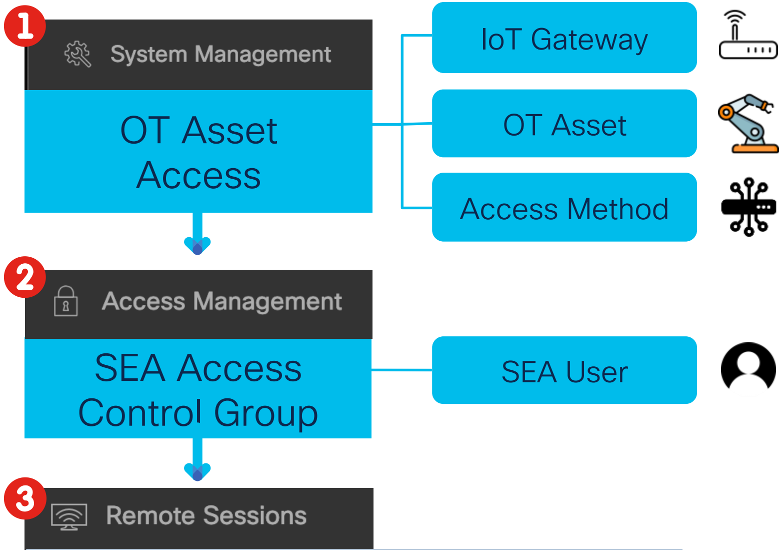
SEA Flow

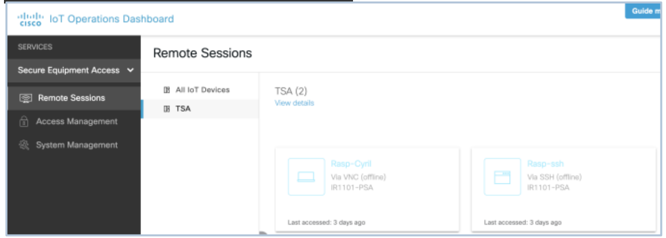
- No installation required: equipment access through browser
- Proxy: SEA Agent on Gateway is a proxy over TLS/443
- Isolation: remote user is never directly connected to remote network



SEA Configuration Overview







Remote Sessions

All IoT Devices
TSA

TSA (2)
View details

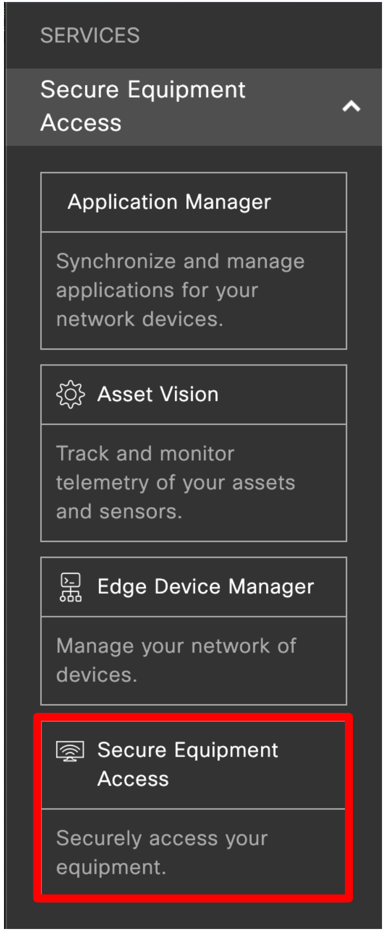
Rasp-Cyril
Via VNC (offline)
IR1101-PSA
Last accessed: 3 days ago

Rasp-ssh
Via SSH (offline)
IR1101-PSA
Last accessed: 3 days ago

How to access SEA Service ?

SEA Configuration

- Login to Cisco IoT Operations Dashboard
  EU cluster https://eu.ciscoiot.com
  US cluster https://us.ciscoiot.com
- On the left panel, in Services, switch to **“Secure Equipment Access”**
- If you don't see Secure Equipment Access, you may need to purchase an additional license. Contact your account team.



SERVICES

Secure Equipment Access

Application Manager

Synchronize and manage applications for your network devices.

Asset Vision

Track and monitor telemetry of your assets and sensors.

Edge Device Manager

Manage your network of devices.

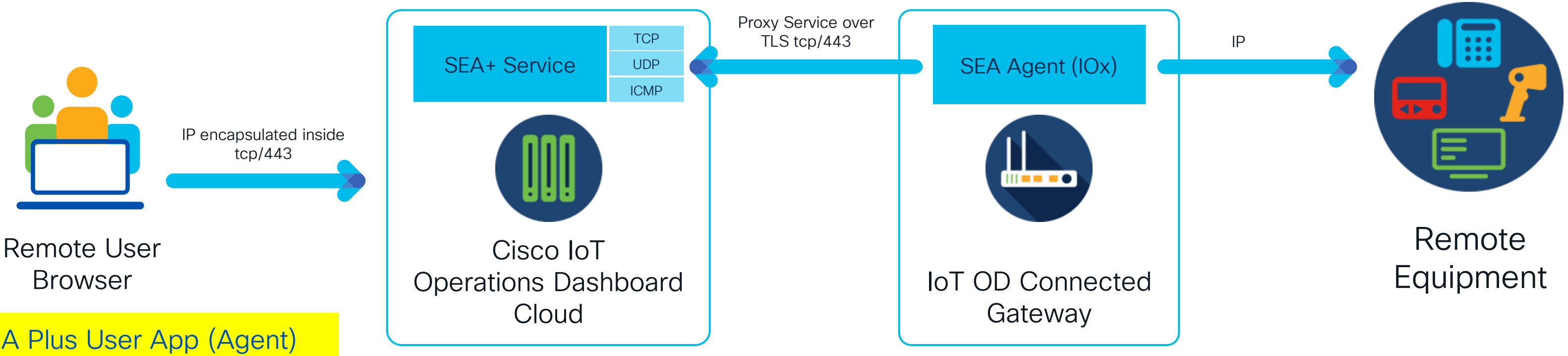
Secure Equipment Access

Securely access your equipment.

This view can be different based on your license

SEA Plus Flow

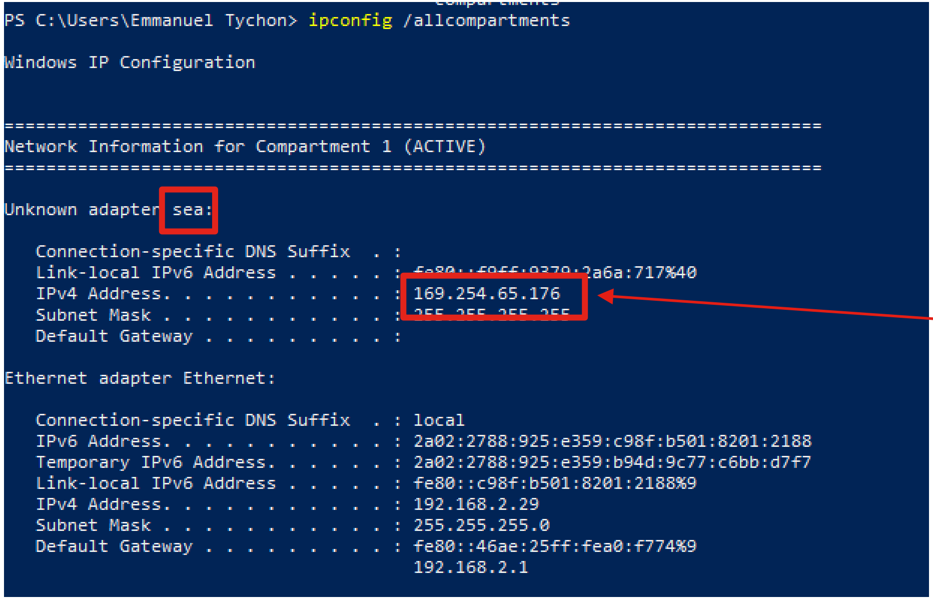
- Agent installation **is required** – creates TUNTAP virtual network device
- TUN devices runs inside SEA TLS/443
- Remote user computer routes changed to use TUN device
- Remote user is **directly connected** to remote network – with ZTNA therefore only allowing what's been explicitly permitted



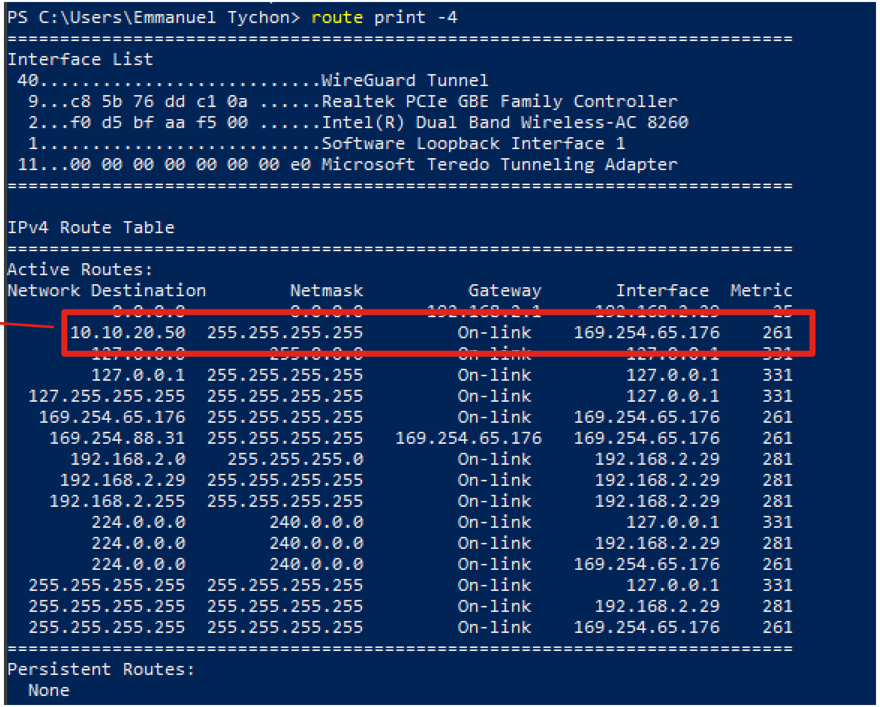
SEA Plus User App (Agent)
(TUN virtual interface)

Filtering happens in all 3 places
1. in Windows SEA Plus app,
2. in Cloud, and
3. in IOx SEA app.

SEA Plus Creates on virtual TUN interface



```
PS C:\Users\Emmanuel Tychon> ipconfig /allcompartments

Windows IP Configuration


==============================================================================
Network Information for Compartment 1 (ACTIVE)
==============================================================================

Unknown adapter sea:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f9ff:9379:2a6a:717%40
   IPv4 Address. . . . . . . . . . . : 169.254.65.176
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : local
   IPv6 Address. . . . . . . . . . . : 2a02:2788:925:e359:c98f:b501:8201:2188
   Temporary IPv6 Address. . . . . . : 2a02:2788:925:e359:b94d:9c77:c6bb:d7f7
   Link-local IPv6 Address . . . . . : fe80::c98f:b501:8201:2188%9
   IPv4 Address. . . . . . . . . . . : 192.168.2.29
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::46ae:25ff:fea0:f774%9
                                       192.168.2.1
```



```
PS C:\Users\Emmanuel Tychon> route print -4
===========================================================================
Interface List
 40...........................WireGuard Tunnel
  9...c8 5b 76 dd c1 0a ......Realtek PCIe GBE Family Controller
  2...f0 d5 bf aa f5 00 ......Intel(R) Dual Band Wireless-AC 8260
  1...........................Software Loopback Interface 1
 11...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.2.1    192.168.2.29     25
      10.10.20.50  255.255.255.255         On-link   169.254.65.176    261
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
   169.254.65.176  255.255.255.255         On-link   169.254.65.176    261
    169.254.88.31  255.255.255.255   169.254.65.176  169.254.65.176    261
      192.168.2.0    255.255.255.0         On-link     192.168.2.29    281
     192.168.2.29  255.255.255.255         On-link     192.168.2.29    281
    192.168.2.255  255.255.255.255         On-link     192.168.2.29    281
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.2.29    281
        224.0.0.0        240.0.0.0         On-link   169.254.65.176    261
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.2.29    281
  255.255.255.255  255.255.255.255         On-link   169.254.65.176    261
===========================================================================
Persistent Routes:
  None
```

SEA vs SEA Plus

- SEA is **easier** to use
- **More secure** with IP isolation
- To be used, when possible, for:
  - SSH
  - VNC
  - RDP
  - Telnet
  - Web

- SEA Plus requires Windows, installation of the SEA Plus User Application, and Windows admin privileges to do so
- SEA Plus is **more flexible**
- Can provide **direct IP connectivity** (ie. to a native client such as Profinet programmer)
- Allows file transfer (ie. with SFTP)

Use both SEA and SEA Plus for different use cases
It always follows the ZTNA principles

SEA Support Matrix

Platform	SEA Support	Recommended Minimum IOS-XE Release
IR8x9	Yes	17.9(3)M8
IR1101	Yes	17.14.1
IR18xx	Yes	17.14.1
IE3400	Yes	17.14.1
IE3300	Yes (4GB of RAM models)	17.14.1
IE31xx	Yes	17.14.1
CAT9K, IE9K	Yes	17.15.1a

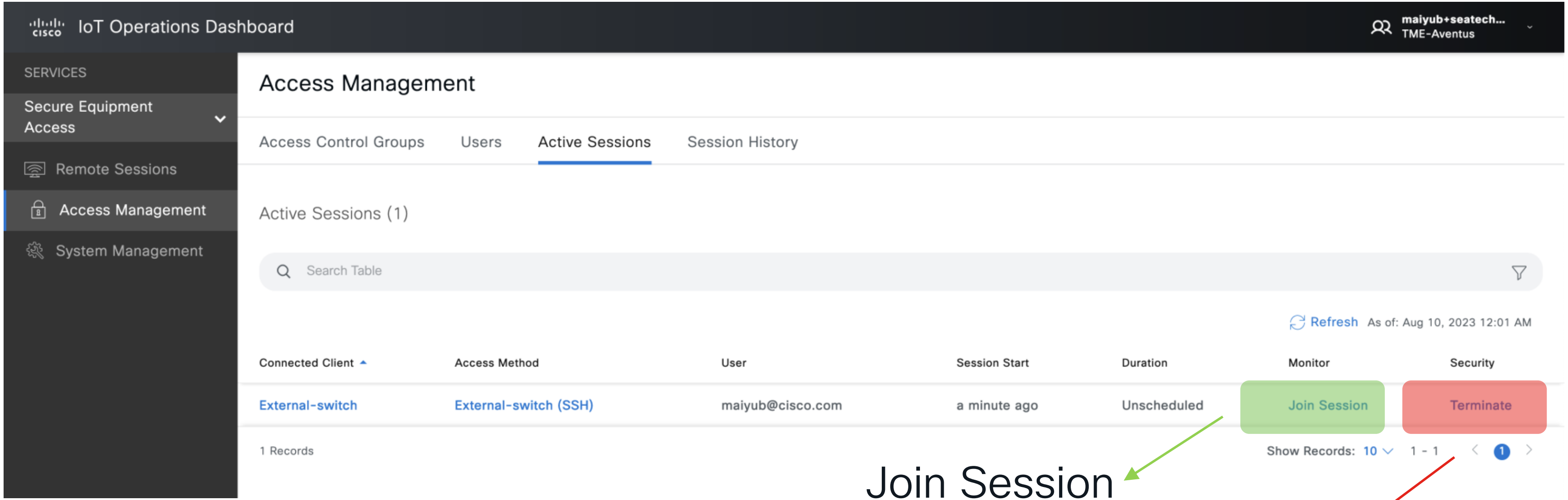
Cisco Secure Equipment Access

Session Management

Features for Session Monitoring

- SEA Admin can:
  - join active sessions to monitor activity in real time (Only for RDP, VNC, SSH and Telnet)
  - immediately terminate an active session
  - see Session History
  - view inline session recordings stored on AWS S3
  - see audit information
- Logs can be seen, but cannot be exported to any Security Information and Event Management (SIEM) system

Accessing and Terminating Sessions



Access Management

Access Control Groups | Users | Active Sessions | Session History

Active Sessions (1)

Search Table

Refresh As of: Aug 10, 2023 12:01 AM

Connected Client	Access Method	User	Session Start	Duration	Monitor	Security
External-switch	External-switch (SSH)	maiyub@cisco.com	a minute ago	Unscheduled	Join Session	Terminate

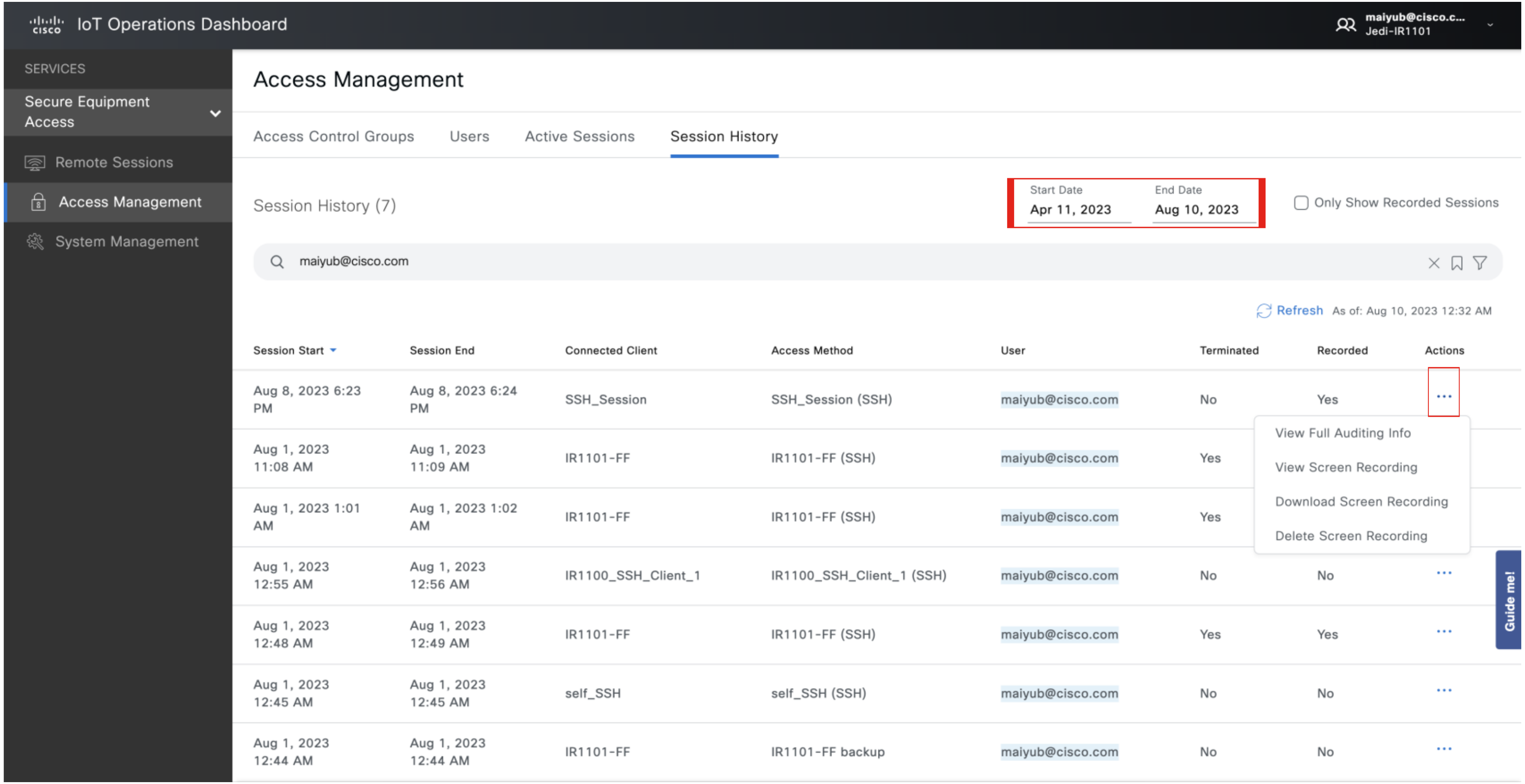
1 Records

Show Records: 10 1 - 1 1

Join Session

Terminate Session

Session History



Access Management

Access Control Groups | Users | Active Sessions | Session History

Session History (7)

Start Date: Apr 11, 2023
End Date: Aug 10, 2023

□ Only Show Recorded Sessions

maiyub@cisco.com

Refresh As of: Aug 10, 2023 12:32 AM

Session Start	Session End	Connected Client	Access Method	User	Terminated	Recorded	Actions
Aug 8, 2023 6:23 PM	Aug 8, 2023 6:24 PM	SSH_Session	SSH_Session (SSH)	maiyub@cisco.com	No	Yes	...
Aug 1, 2023 11:08 AM	Aug 1, 2023 11:09 AM	IR1101-FF	IR1101-FF (SSH)	maiyub@cisco.com	Yes		
Aug 1, 2023 1:01 AM	Aug 1, 2023 1:02 AM	IR1101-FF	IR1101-FF (SSH)	maiyub@cisco.com	Yes		
Aug 1, 2023 12:55 AM	Aug 1, 2023 12:56 AM	IR1100_SSH_Client_1	IR1100_SSH_Client_1 (SSH)	maiyub@cisco.com	No	No	...
Aug 1, 2023 12:48 AM	Aug 1, 2023 12:49 AM	IR1101-FF	IR1101-FF (SSH)	maiyub@cisco.com	Yes	Yes	...
Aug 1, 2023 12:45 AM	Aug 1, 2023 12:45 AM	self_SSH	self_SSH (SSH)	maiyub@cisco.com	No	No	...
Aug 1, 2023 12:44 AM	Aug 1, 2023 12:44 AM	IR1101-FF	IR1101-FF backup	maiyub@cisco.com	No	No	...

Cisco Secure Equipment Access

Session Request and Approval

Remote User Benefits

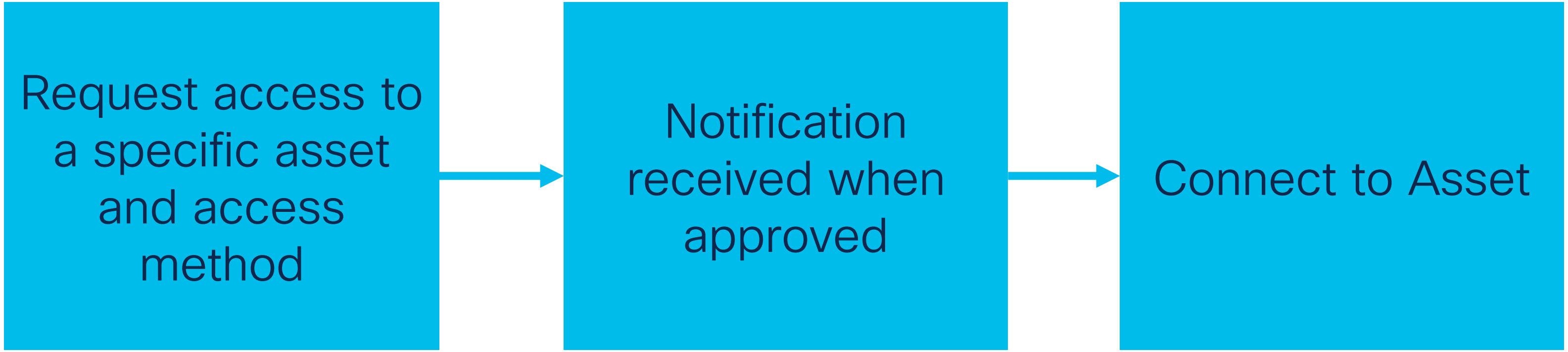
- Can **request access** to a remote asset
- Request is routed to a list of **approvers**
- The approver list can be **unique for each group**
- Once approved – user gets **instant access** for the requested duration

Administrator Benefits

- **No need to pro-actively add users** to group – they request when needed
- Simple **approve / deny / revoke** action to be done by approvers
- Approvers and Administrators can be **separate users**

Simple "Remote User" workflow

- Request, approve, and access:



Request access to a specific asset and access method

Notification received when approved

Connect to Asset

For maximum granularity and security, access is not granted to the whole group, but only to the specific asset(s) and access method(s) that have been requested and approved.

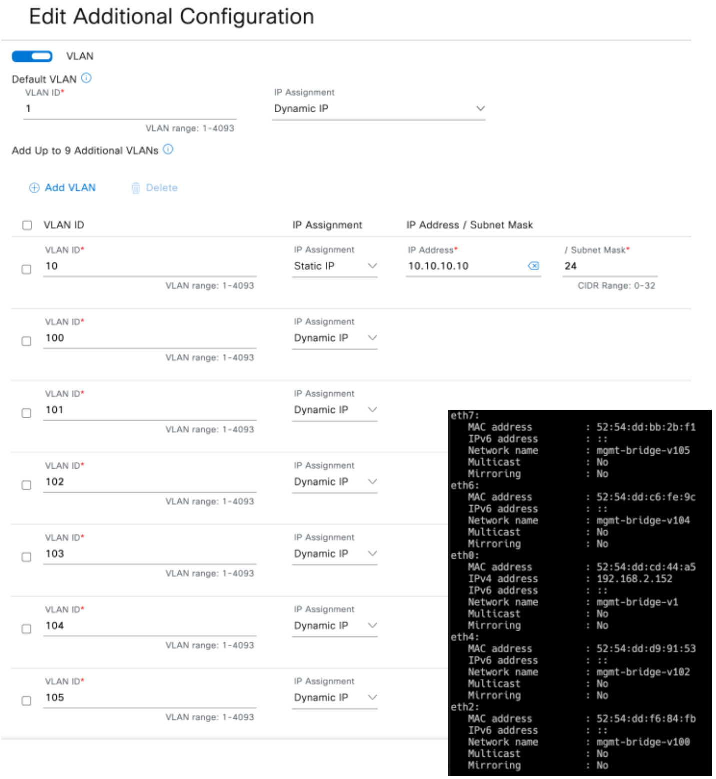
Cisco Secure Equipment Access

VLAN Access

VLAN Access on IE Switches for SEA Agent

- For switches, when installing SEA, you can configure access to up to 9 VLANs.
- For each VLAN you can use a dynamic (DHCP address) or configure a static IP address.
- Multiple interfaces will be created inside IOx, each in their respective assigned VLAN
- No overlapping IP addresses between VLANs
- Note: the IOx port must be in trunking mode, for example:

```
interface AppGigabitEthernet1/1
 switchport trunk native vlan 4094
 switchport mode trunk
```



Edit Additional Configuration

VLAN

Default VLAN ⓘ

VLAN ID*	1
	VLAN range: 1-4093
IP Assignment	Dynamic IP

Add Up to 9 Additional VLANs ⓘ

	VLAN ID	IP Assignment	IP Address / Subnet Mask	
□	VLAN ID* 10 (VLAN range: 1-4093)	Static IP	IP Address* 10.10.10.10	/ Subnet Mask* 24 (CIDR Range: 0-32)
□	VLAN ID* 100 (VLAN range: 1-4093)	Dynamic IP		
□	VLAN ID* 101 (VLAN range: 1-4093)	Dynamic IP		
□	VLAN ID* 102 (VLAN range: 1-4093)	Dynamic IP		
□	VLAN ID* 103 (VLAN range: 1-4093)	Dynamic IP		
□	VLAN ID* 104 (VLAN range: 1-4093)	Dynamic IP		
□	VLAN ID* 105 (VLAN range: 1-4093)	Dynamic IP		

```
eth7:
   MAC address              : 52:54:dd:bb:2b:f1
   IPv6 address             : ::
   Network name             : mgmt-bridge-v105
   Multicast                : No
   Mirroring                : No
eth6:
   MAC address              : 52:54:dd:c6:fe:9c
   IPv6 address             : ::
   Network name             : mgmt-bridge-v104
   Multicast                : No
   Mirroring                : No
eth0:
   MAC address              : 52:54:dd:cd:44:a5
   IPv4 address             : 192.168.2.152
   IPv6 address             : ::
   Network name             : mgmt-bridge-v1
   Multicast                : No
   Mirroring                : No
eth4:
   MAC address              : 52:54:dd:d9:91:53
   IPv6 address             : ::
   Network name             : mgmt-bridge-v102
   Multicast                : No
   Mirroring                : No
eth2:
   MAC address              : 52:54:dd:f6:84:fb
   IPv6 address             : ::
   Network name             : mgmt-bridge-v100
   Multicast                : No
   Mirroring                : No
```

Cisco Secure Equipment Access

SEA Agent Installation

SEA Agent Deployment Model

SEA Agent is an essential part of the solution and it needs to run on the SEA Gateway - switch or router.

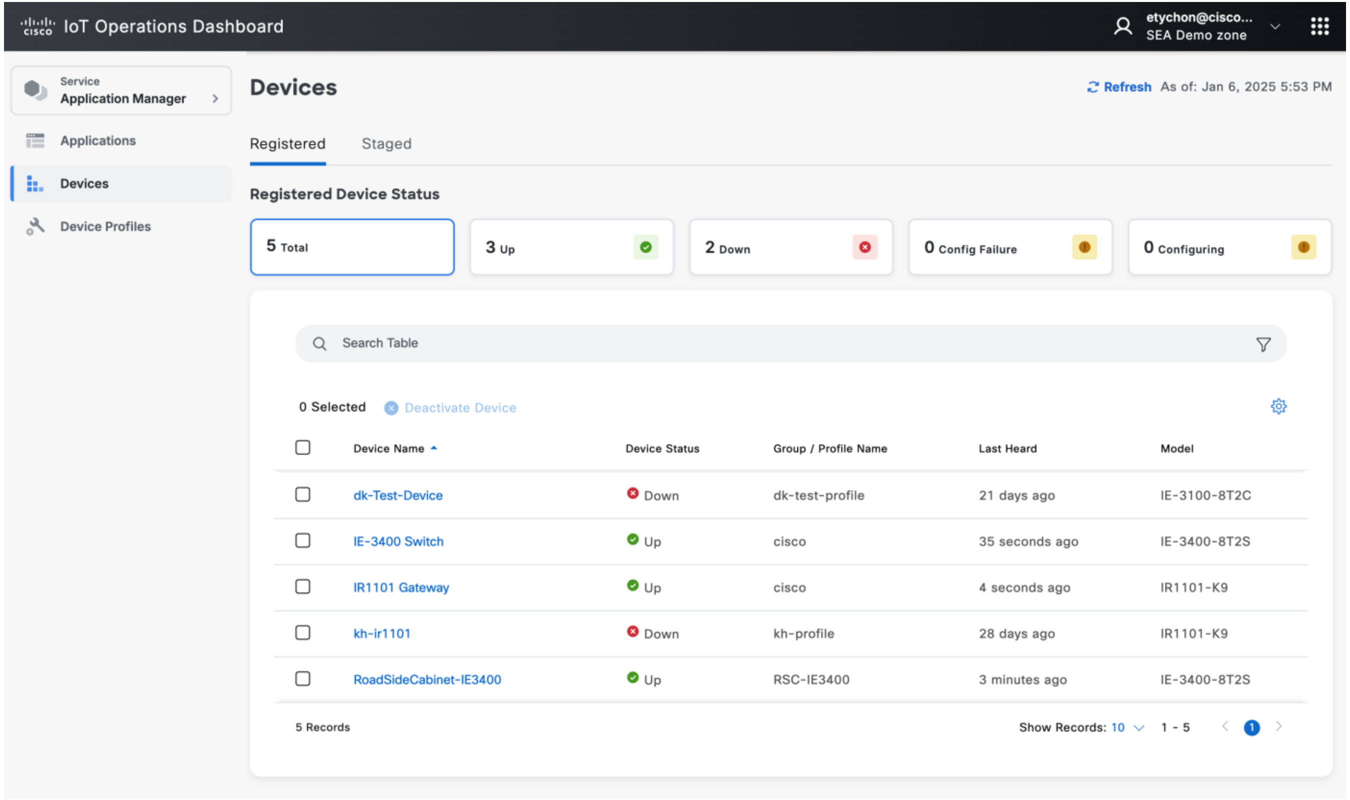
There are four ways for the SEA to be deployed:

1. Through **Cisco IoT Operations Dashboard** ("Application Manager")
2. Through **Cisco Catalyst Center (previously DNA-C)**
3. Through **Cisco Catalyst SD-WAN Manager (previously vManage)**
4. Through IOS-XE **CLI**

Deploying SEA Agent with

Cisco IoT Operations Dashboard

- Add the gateway to "**Application Manager**" service
- Enable the "**Secure Equipment Access**" service.
- SEA Agents is automatically installed and configured. Magic!



Devices

Refresh As of: Jan 6, 2025 5:53 PM

Registered | Staged

Registered Device Status

5 Total | 3 Up | 2 Down | 0 Config Failure | 0 Configuring

Search Table

0 Selected ⊗ Deactivate Device

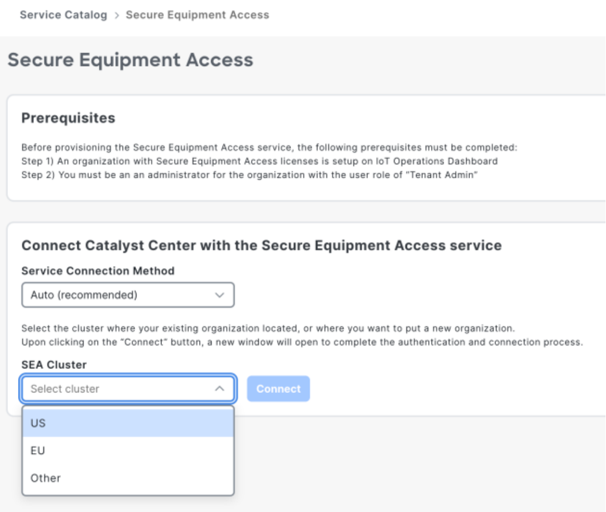
□	Device Name	Device Status	Group / Profile Name	Last Heard	Model
□	dk-Test-Device	Down	dk-test-profile	21 days ago	IE-3100-8T2C
□	IE-3400 Switch	Up	cisco	35 seconds ago	IE-3400-8T2S
□	IR1101 Gateway	Up	cisco	4 seconds ago	IR1101-K9
□	kh-ir1101	Down	kh-profile	28 days ago	IR1101-K9
□	RoadSideCabinet-IE3400	Up	RSC-IE3400	3 minutes ago	IE-3400-8T2S

5 Records

Show Records: 10 1 - 5 1

Deploying SEA Agent with
Cisco Catalyst Center

- SEA can be enabled right from Catalyst Center


Service Catalog > Secure Equipment Access

Secure Equipment Access

Prerequisites

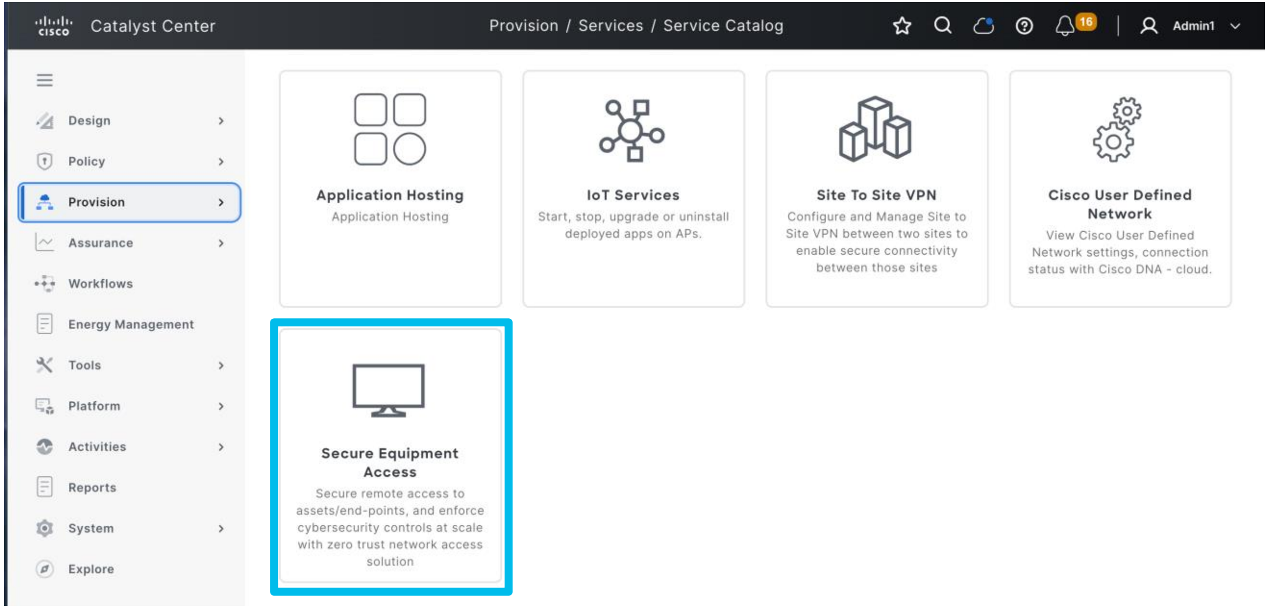
Before provisioning the Secure Equipment Access service, the following prerequisites must be completed:
Step 1) An organization with Secure Equipment Access licenses is setup on IoT Operations Dashboard
Step 2) You must be an an administrator for the organization with the user role of "Tenant Admin"

Connect Catalyst Center with the Secure Equipment Access service

Service Connection Method: Auto (recommended)

Select the cluster where your existing organization located, or where you want to put a new organization.
Upon clicking on the "Connect" button, a new window will open to complete the authentication and connection process.

SEA Cluster: Select cluster



Application Hosting
Application Hosting

IoT Services
Start, stop, upgrade or uninstall deployed apps on APs.

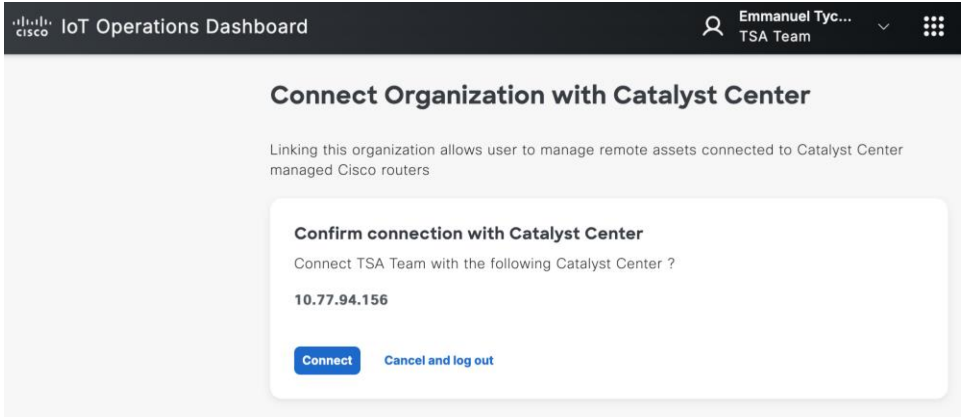
Site To Site VPN
Configure and Manage Site to Site VPN between two sites to enable secure connectivity between those sites

Cisco User Defined Network
View Cisco User Defined Network settings, connection status with Cisco DNA - cloud.

Secure Equipment Access
Secure remote access to assets/end-points, and enforce cybersecurity controls at scale with zero trust network access solution

Deploying SEA Agent with Cisco Catalyst Center

- Automated connection from Catalyst Center to SEA
- Click "Connect" follow the steps, you're done!



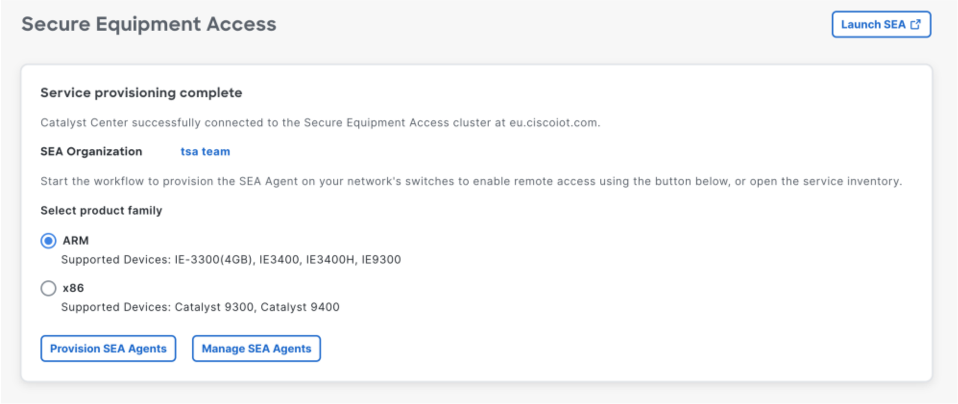
Connect Organization with Catalyst Center

Linking this organization allows user to manage remote assets connected to Catalyst Center managed Cisco routers

Confirm connection with Catalyst Center

Connect TSA Team with the following Catalyst Center ?

10.77.94.156


Secure Equipment Access

Service provisioning complete

Catalyst Center successfully connected to the Secure Equipment Access cluster at eu.ciscoiot.com.

SEA Organization tsa team

Start the workflow to provision the SEA Agent on your network's switches to enable remote access using the button below, or open the service inventory.

Select product family

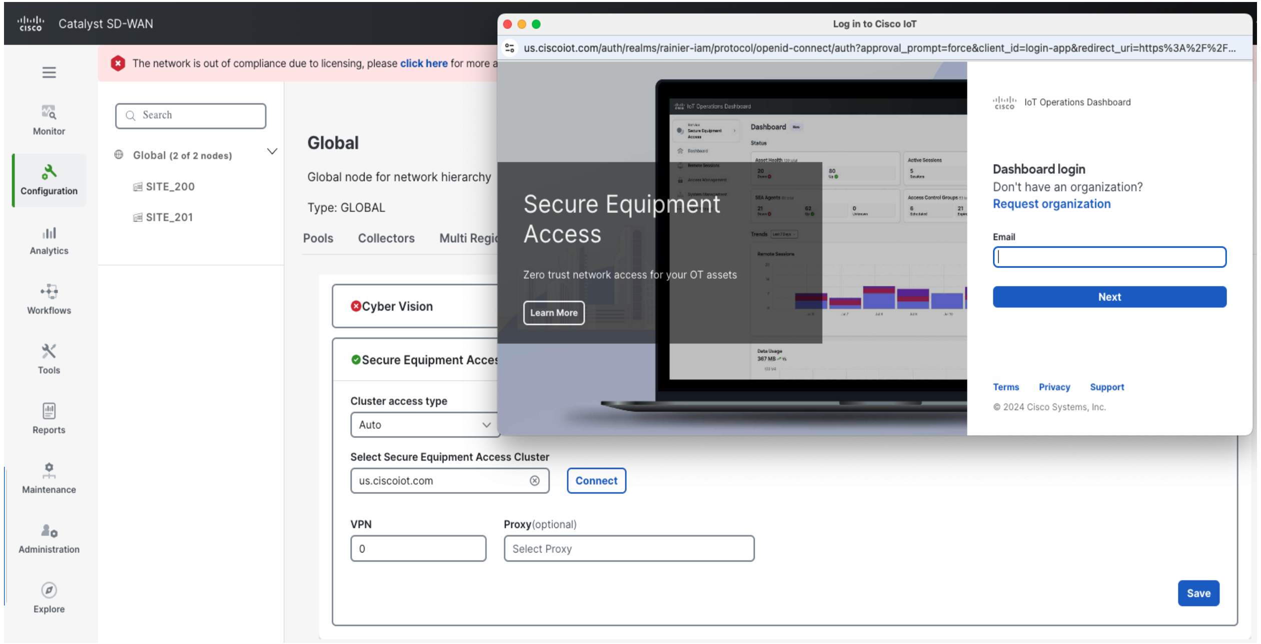
● ARM
Supported Devices: IE-3300(4GB), IE3400, IE3400H, IE9300

○ x86
Supported Devices: Catalyst 9300, Catalyst 9400

New in
SD-WAN 20.16

Deploying SEA Agent with
Cisco Catalyst SD-WAN Manager

- Connects SD-WAN Manager and SEA with one click
- Creates an API-level connection to manage SEA from SD-WAN



The network is out of compliance due to licensing, please click here for more a

Global

Global node for network hierarchy

Type: GLOBAL

Cyber Vision

Secure Equipment Acces

Cluster access type: Auto

Select Secure Equipment Access Cluster: us.ciscoiot.com

VPN: 0

Proxy(optional): Select Proxy

us.ciscoiot.com/auth/realms/rainier-iam/protocol/openid-connect/auth?approval_prompt=force&client_id=login-app&redirect_uri=https%3A%2F%2F...

Secure Equipment Access

Zero trust network access for your OT assets

Dashboard login

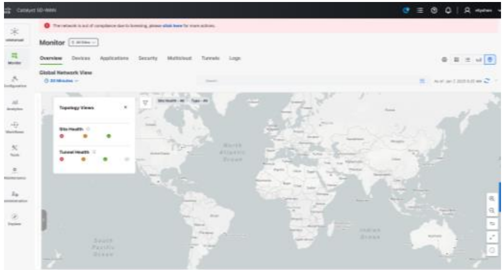
Don't have an organization?
Request organization

Email

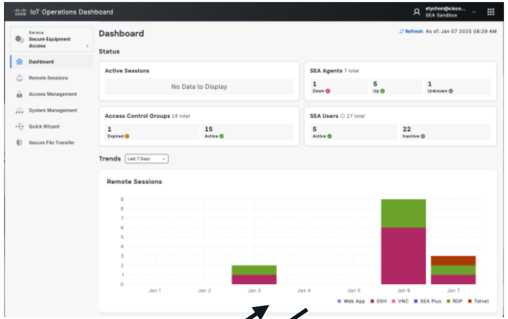
© 2024 Cisco Systems, Inc.

Deploying SEA Agent with
Cisco Catalyst SD-WAN Manager

Cisco Catalyst SD-WAN Manager



Cisco Secure Equipment Access



1

```
Request: Provision App
    Serial: FGL21121G0
    Name: NYC-West-54th-2nd
    Cross Launch URL: https://vmanage01-acme.com/#/app/...
```

2

```
Response:
    On-Boarding Token: App-adfjh64wr4er352jhfw5293959ghse
    Cross Launch URL: https://us.ciscoiot.com/coreshell/devices/...
```

3

```
Request: Deploy App
    Application Config: Config-Blob with OD as SEA download location
    On-Boarding Token: App-adfjh64wr4er352jhfw5293959ghse
```

4

```
4a. Request to download SEA App
4b. Request: Onboard App IOx Agent
    On-Boarding Token: App-adfjh64wr4er352jhfw5293959ghse
```

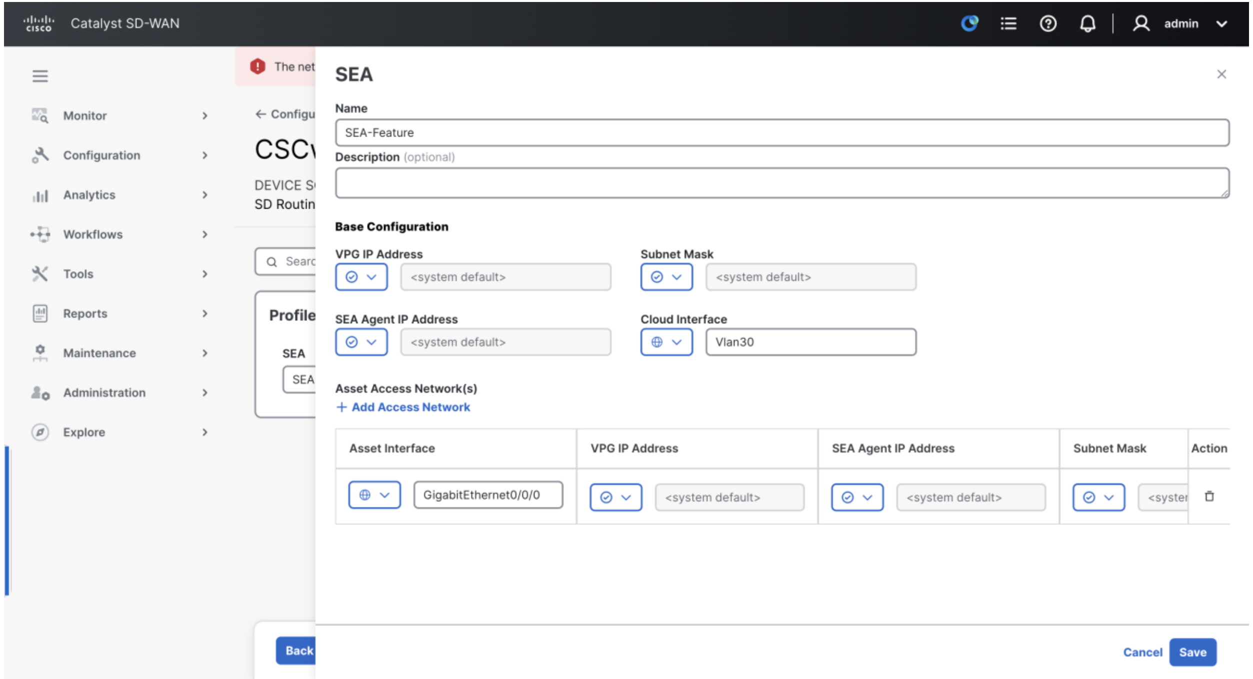
5

```
Request: Update App version
   Content: App Image
```

New in
SD-WAN 20.16

Deploying SEA Agent with Cisco Catalyst SD-WAN Manager

- SEA has a dedicated feature profile in SD-WAN Manager
- Agent is installed and configured by SD-WAN Manager
- SD-WAN and SEA organizations are linked automatically



SEA

Name
SEA-Feature

Description (optional)

Base Configuration

VPG IP Address <system default>	Subnet Mask <system default>
SEA Agent IP Address <system default>	Cloud Interface Vlan30

Asset Access Network(s)

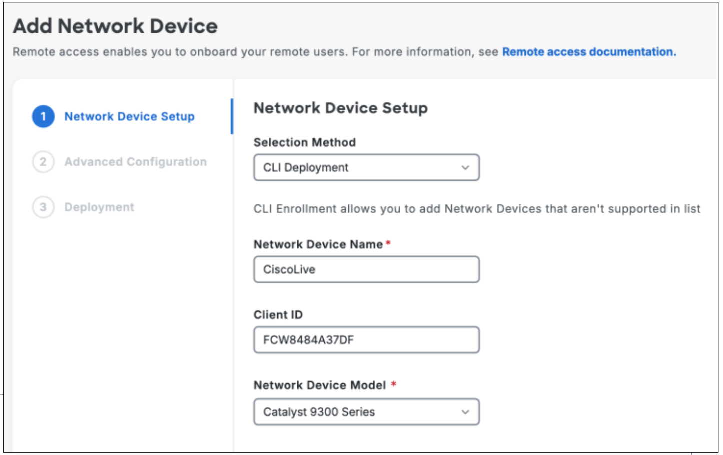
+ Add Access Network

Asset Interface	VPG IP Address	SEA Agent IP Address	Subnet Mask	Action
GigabitEthernet0/0/0	<system default>	<system default>	<syster	🗑

Cancel Save

Deploying SEA Agent with Cisco IOS-XE CLI

- SEA can be enabled with auto-generated configuration
- Cut and paste config on the device.
- Done!



Add Network Device

Remote access enables you to onboard your remote users. For more information, see **Remote access documentation.**

1 Network Device Setup

2 Advanced Configuration

3 Deployment

Network Device Setup

Selection Method: CLI Deployment

CLI Enrollment allows you to add Network Devices that aren't supported in list

Network Device Name *: CiscoLive

Client ID: FCW8484A37DF

Network Device Model *: Catalyst 9300 Series

```
config term
    vlan 4094
    interface AppGigabitEthernet1/0/1
        switchport trunk native vlan 4094
        switchport trunk allowed vlan add 1
        switchport mode trunk
    ! Uncomment the command below to enable app signature verification.
    ! Note that this action may affect other IOX applications on the device.
    ! app-hosting signed-verification
    no app-hosting appid SEA_agent_amd64_linux
    app-hosting appid SEA_agent_amd64_linux
        app-vnic AppGigabitEthernet trunk
            vlan 1 guest-interface 0
        app-resource docker
            prepend-pkg-opts
            run-opts 1 "-e TOKEN=eyJnd9tIn0="
    start
    end
    write mem
    ! The copy command below requires internet connectivity on the device.
    ! Alternatively, download the SEA Agent app and copy to flash manually.
    copy http://apps.eu.ciscoiot.com/seaAgent_amd64_linux_v0.84.tar flash:seaAgent_amd64_linux_v0.84.tar
```

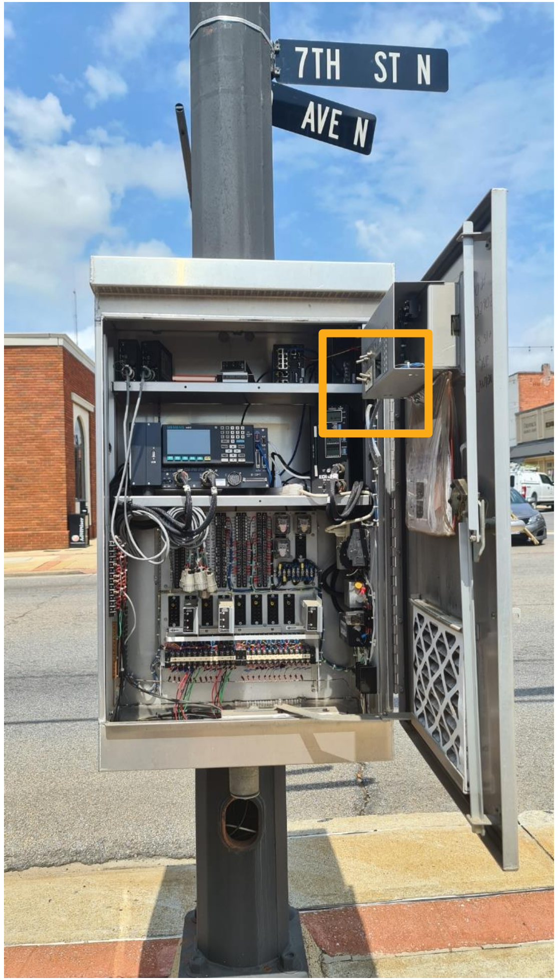
Where is it used?

Blade Manufacturing Plant

- Lots of equipment managed by different vendors
- Need to filter who access what, when
- Need sometimes direct access (ie: for Siemens TIA)
- SEA reduces administration, complexity
- SEA improves time to resolution and satisfaction

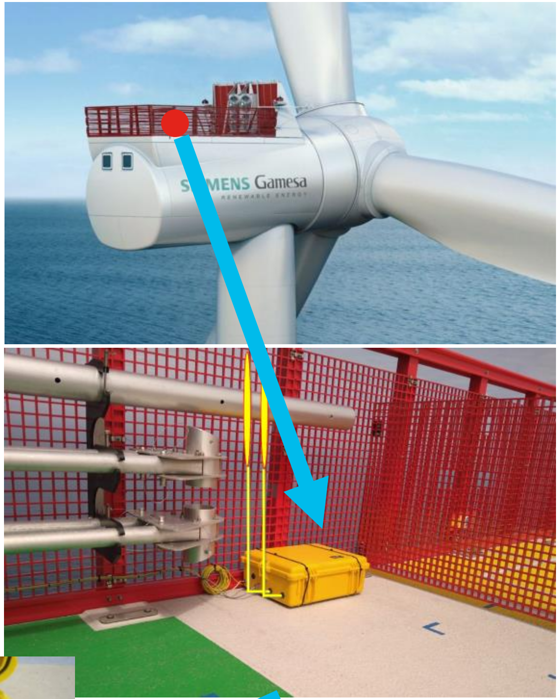
Roadway Intersection

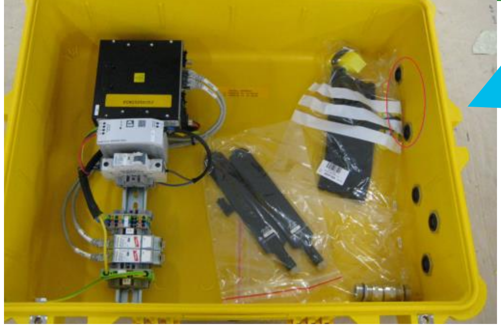
- IE2K in Clanton, AL for traffic controller connectivity.
- Wireless with point-to-point radio
- Radio terminates on an IR1101 with LTE for backhaul



Offshore Wind Turbine

- Using IR1101 with CAT18 LTE
- Installed atop the turbine in a weatherproof case
- Need extended temperature range
- Access to PLCs, HMI, RTU, IED, Relays, Generator, etc... **using OD and SEA** and a local HMI computer (RDP protocol)





Demo

Key takeaways

- Contemporary network access embraces ZTNA, not VPN
- SEA is built with ZTNA in mind, for OT networks
- SEA is embedded in your network – no additional equipment
- SEA is Cloud managed by Cisco – nothing to install

Webex App

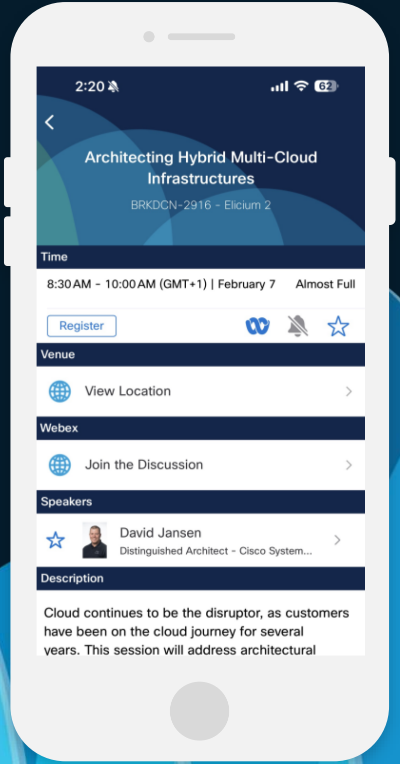
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



2:20

Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Register

Venue

View Location

Webex

Join the Discussion

Speakers

David Jansen

Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

cisco Live!

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'

Content Catalog

Continue your education

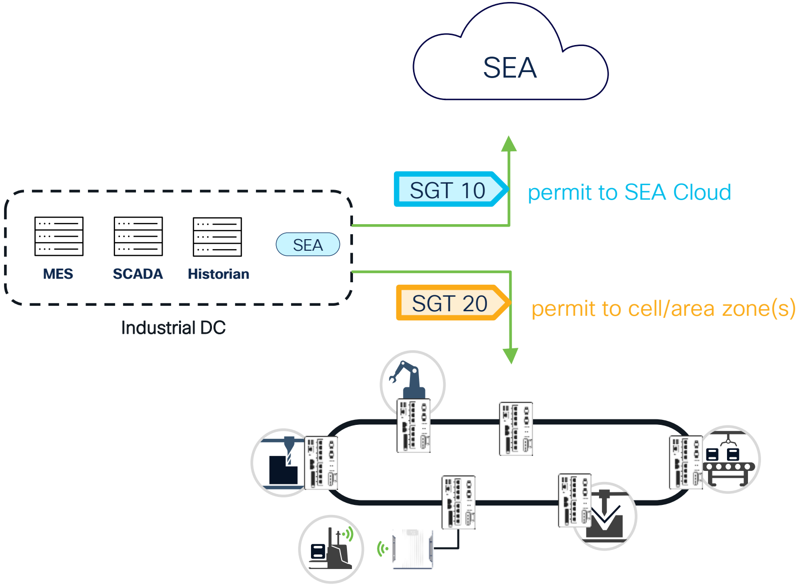
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Thank you

cisco Live!

GO BEYOND

Using SEA in a TrustSec protected network


SEA
SGT 10
permit to SEA Cloud
MES
SCADA
Historian
SEA
Industrial DC
SGT 20
permit to cell/area zone(s)