Secure Remote Access for Industrial Networks

Design Guide

September 2023

Cisco
Validated
Design

Cisco Systems, Inc. www.cisco.com

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TOCHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED "AS IS."

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTYOF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Introduction

The pandemic normalized remote working. At the end of the pandemic, with a large section of employees still favoring the flexibility offered by remote working, the work model is currently hybrid work. It allows employees, partners, and vendors to work on site as well as at home, co-working spaces, and anywhere in between—wherever and however they work most productively.

This flexibility comes with a cost. Cyberattacks today have become more sophisticated and multipronged. At the same time, the proliferation of user endpoints—both corporate and personal devices, whether managed or unmanaged—has expanded the attack surface, leaving organizations and their end users vulnerable to malware and ransomware attacks.

To combat these security challenges, organizations often purchase new tools to solve specific problems, and may up with more security tools than they can effectively orchestrate or manage. This leads to tool sprawl which can create too many alerts, reduce threat response time, and open security vulnerabilities.

Organizations need a solution that provides trusted hybrid / remote workers, contractors, and vendors with secure access to the organization's network, applications, data, machines, and other services. Access must be granted to specific devices, only when needed, under flexible constraints to meet compliance needs.

Security Landscape

Today, attacks like phishing, ransomware, and advanced persistent threats are common, and no single product can successfully secure your business from these risks. An architectural approach that addresses the full range—from people, to devices, to applications—is needed.

Complexity is one of the main challenges facing security professionals. Technology constantly fragments into new uses, and organizations utilize dozens of products that do not interoperate seamlessly. This multiplies attack surfaces, which in turn complicates defense. Bad actors exploit this weakness to develop advanced threats for more lucrative schemes. The industry desperately needs a resource that simplifies the problem. The solution must be comprehensive, credible, and about more than just products; it needs to focus on the threats to your business.

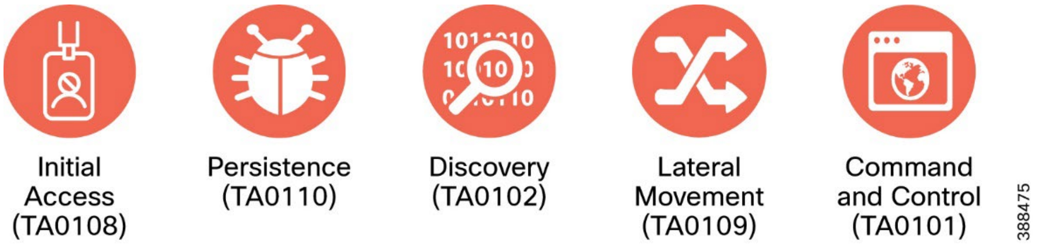
The attack surface of an organization is anyone or anything that can be targeted. Any human, using any device, on any network, accessing any application can be attacked. The attack surface needs to be secured by appropriate capabilities. Each target may be part of a larger overall attack. By identifying a company's business flows which represent the company's attack surface, proper security capabilities can be applied.

Remote access software provides IT/OT teams the ability to maintain remote assets at scale without time-consuming and costly site visits. Industrial equipment – from roadside cameras to robots on the manufacturing floor – frequently requires specialized technical support from their respective manufacturers for upgrades and troubleshooting.

The increasing need for remote connectivity to critical equipment opens the attack surface to remote threat actors. A yearly Verizon Data Breach Investigations Report (DBIR) analyzes thousands of incidents and confirmed breaches from around the world so that security analysts can understand the most exploited vulnerabilities across industries. According to the *2023 DBIR*, over 83% of breaches were from external actors and the top three primary ways in which attackers access an organization are stolen credentials, phishing, and exploitation of vulnerabilities, all of which present themselves in a remote access solution.

There are many great resources to access when learning about the techniques used to infiltrate industrial networks. For example, *MITRE ATT&CK for ICS* is a knowledge base useful for describing the actions an adversary may take when operating within an Industrial Control System (ICS) network. ATT&CK is short for Adversarial Tactics, Techniques, and Common Knowledge. Figure 1 shows relevant attack techniques used to exploit elements that can accessed from a remote location.

Figure 1 Remote Access Attack Techniques used to Exploit Industrial Control System (ICS) networks



Initial Access is described by MITRE ATT&CK as an adversary attempting to penetrate an ICS environment. This is traditionally accomplished by exploiting public facing applications, or the exploitation of remote services. The Colonial Pipeline attack for example, while not an entry into the OT network, was a result of a forgotten Virtual Private Network (VPN) termination point with stolen credentials and no Multi-Factor Authentication (MFA). With many industrial sites using technologies such as VPN and Remote Desktop Protocol (RDP) for remote access services or implementing Industrial IoT (IIoT) gateways for data collection, it is critical that public facing applications are implemented with security top of mind.

After initial access has been gained to the network, adversaries will try to maintain a foothold within the ICS environment. This is known as persistence. This may be achieved using default or stolen system credentials or in advanced scenarios the installation of malicious software to create a new backdoor into the system.

Once a foothold has been gained into the ICS network, the next step an attacker will take is to discover and assess targets in the OT environment. Triton malware is an example of this where a python script was executed in the network to discover Schneider Electric’s Triconex safety controllers. Triconex safety controllers used a proprietary protocol on UDP port 1502, and Triton used this knowledge to scan the network for the devices. If the device existed, the malware could then read the firmware version and use this information in the next phase of an attack.

Lateral Movement refers to the adversary attempting to move through the ICS environment. This could involve jumping to engineering workstations using RDP with weak or default credentials, or in the case of the WannaCry vulnerability, using protocol exploits to hop across machines in the network. Machine builders often provide their own means of remote access built into the machinery; another attack vector that leaves the door open to an Initial Access attack. However, these access methods are commonly unknown to the end customer, and lateral movement becomes easier as these backdoors bypass the upfront security controls an organization may already have in place.

If remote access is not properly secured, an attacker may have the ability to impair process control by manipulating or disabling physical control processes. Adversaries may send unauthorized command messages to instruct control system assets to perform actions outside of their indented functionality if the authorization of a remote user is not correctly implemented.

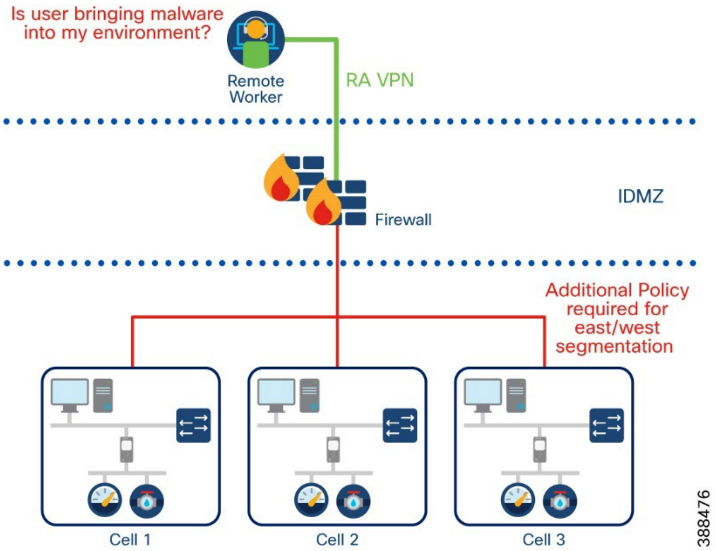
Secure Remote Access Solutions

Remote access solutions come in many forms, and it can often be confusing to understand which one will meet business needs. This design guide explores virtual private networks, the remote desktop protocol, and the evolution towards zero trust network access.

Virtual Private Networks

Virtual private networks, or VPNs, are a way to give remote users an encrypted connection over an Internet network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments. While logging into these networks helps users securely and remotely access work resources and applications, they can be exploited by hackers seeking to steal login credentials.

Figure 2 Using a VPN to connect to the ICS network


Is user bringing malware into my environment?
Remote Worker
RA VPN
Firewall
IDMZ
Additional Policy required for east/west segmentation
Cell 1
Cell 2
Cell 3
388476

VPNs do offer security benefits, but if not configured correctly, can give an adversary unrestricted access to the Operational Technology (OT) network. With what is known about the risk of stolen credentials, using a Multi Factor Authentication (MFA) solution must be used for any remote access solution. However, the additional risk with VPN solutions is the potential for even a legitimate user to unknowingly bring malicious software into the environment. Using a VPN, the network is extended to the remote user, which brings their machine as a remote client to the network. If a device is not scanned before access is given, malicious software could unintentionally be introduced to the OT network.

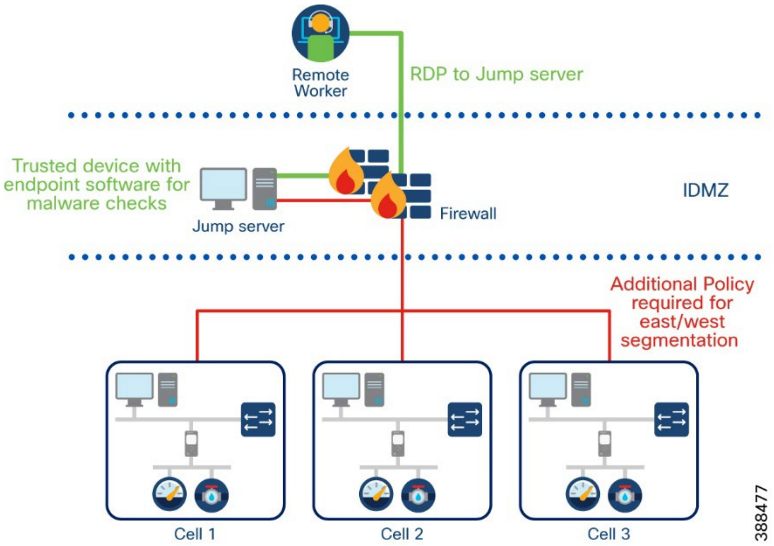
With a VPN solution, additional access control needs to be placed on the user to limit their actions to a pre-determined scope of work. In the case of a vendor who is performing maintenance in a production environment, the vendor needs access to a single machine, during the maintenance window, and should not have the ability to laterally move to any other machine, neither intentionally nor unintentionally.

While all the necessary security checks and controls are possible with a traditional VPN based solution, the operational overhead often leads to lackluster policies and wide-open access policies after remote access has been granted. Additionally, VPN access is commonly maintained by a separate entity in the organization, which causes delays for vendor connectivity and slows down the line of business. As a result, even in the IT world, there has been a shift towards looking for VPN alternatives.

Accessing Jump Servers with the Remote Desktop Protocol

RDP is a protocol that lets you take control of a computer remotely. For example, an employee can access all their engineering workstations, project files and network resources from their home computer using RDP. It is also often used by third party support to remotely access machines that need repair.

Figure 3 Using a Jump Server to connect to the ICS network


Remote Worker
RDP to Jump server
Trusted device with endpoint software for malware checks
Jump server
Firewall
IDMZ
Additional Policy required for east/west segmentation
Cell 1
Cell 2
Cell 3
388477

In OT networks, the server which grants access to the plant remotely is often known as a jump server (or a jump box / jump host). The jump server solves the challenge an OT network can face with malicious software being introduced to the network by a remote device. After a VPN connection is established, policy is placed on the firewall to only allow users to access a set of jump servers that have been assigned to them. All activities performed on the OT network must originate from the jump server, which is a trusted device fully controlled by the networking team.

While jump servers solve one challenge, they do not help solve the challenge of controlling what a user can do once they have access to the jump server. Best practices would leave jump servers in a quarantined state, where they are denied any access to the OT network until called upon. As necessary, security administrators open specific policies to control what a user can and cannot do from that server. Once again, the operational burden can be overwhelming, and, in practice, jump servers expose themselves to the same frailties as the VPN solution.

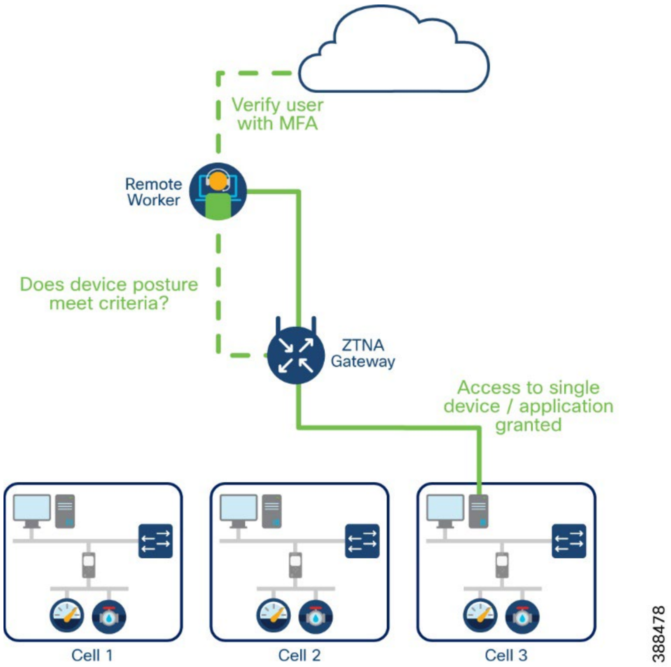
In 2020 hackers harvested and sold as many as 250,000 RDP server credentials in an underground marketplace, xDedic. These credentials gave buyers access to all the data on the servers and the ability to launch future attacks using the servers. Attacks against RDP grew by 768% in 2020, according to ESET.

Unrelated to security, jump servers are assets that will need to be managed, consuming power, and requiring ongoing maintenance. Additionally, if licensed software is needed to perform a task such as the PLC programming software, licensing must be purchased, that software must be maintained, and the cost and complexity increases for the consumer.

Zero Trust Network Access

Zero Trust Network Access (ZTNA) is a security service that verifies users and grants access to specific applications based on identity and context policies. Zero trust can be summed up as "never trust, always verify." Often when users log in to a VPN, they are granted complete access to the entire network. Alternatively, ZTNA solutions connect authorized users directly to applications rather than to the network—and only to those applications they are authorized to access on need-to-know-based policies.

Figure 4 Using ZTNA to connect to a single device on the ICS network


Verify user with MFA
Remote Worker
Does device posture meet criteria?
ZTNA Gateway
Access to single device / application granted
Cell 1
Cell 2
Cell 3
388478

Adoption of zero trust can help address common security challenges in the workforce, such as phishing, malware, credential theft, remote access, and device security. This is done by securing the three primary factors that make up the workforce: users, their devices, and the applications they access.

Verify Users

Ensuring the trust of your users whenever they attempt to access applications remotely is the first step toward secure remote access. The following capabilities aid in mitigating the threat that Initial Access exploits:

- **Multi-Factor Authentication (MFA)** - Authentication based on usernames and passwords alone is unreliable since users may have trouble storing, remembering, and managing them across multiple accounts, and many reuse passwords across services and create passwords that lack complexity. Passwords also offer weak security because of the ease of acquiring them through hacking, phishing, and malware. MFA requires extra means of verification that unauthorized users will not have. Even if a threat actor can impersonate a user with one piece of evidence, they will not be able to provide two or more.

- **Single Sign On (SSO) -** SSO is an authentication process that provides users with one easy and consistent login experience across all applications, eliminating the need to supply user credentials with every application or access request. Using SSO, user experience is streamlined across multiple applications, while security administrators can enforce strict user policies in a centralized location. MFA and user policy can be applied during SSO and eliminate the need to duplicate and maintain authentication policies across multiple applications, such as remote access software.

Device Posture

If users are logging into your company applications with outdated devices, there is a chance they could also be unwittingly spreading malware and using keyloggers to record your keystrokes. Meaning any data you type, including your username or password, can be recorded, and sent to an attacker’s command and control servers. As a result, your company’s data could be at risk if just one out-of-date device logs in, potentially spreading malware throughout your environment. Or worse, spreading ransomware that will keep your files hostage until a ransom is paid to decrypt them.

To protect the OT network from introducing malware to the environment, the remote access solution must have the following capabilities:

- **Device Posture Assessment** - The device posture assessment analyzes the device, assesses its security posture, and reports it to the policy decision management system. Organizations need to enable secure and direct access to business applications for a diverse set of users (remote workers, vendors, and contractors) and their devices that typically reside outside of the control of corporate enterprise mobility management (EMM) and mobile device management (MDM) solutions. Enforcing consistent security policies across managed devices, bring your own devices (BYOD), corporate owned, personally enabled, and third-party (contractor or partner) devices poses a significant challenge. IT security teams often lack insight and an enforcement mechanism when making an access decision on endpoints, particularly among unmanaged devices. This is when device trust is important to establish.

- **Anti-Malware** – Generally, the parameters of advanced malware are to penetrate a system and avoid detection. Once loaded onto a computer system, advanced malware can self-replicate and insert itself into other programs or files, infecting them in the process. Anti-malware protection should be implemented in both the network (to prevent initial infection and detect attempts of spread) and in the endpoint (to prevent endpoint infection and remove unwanted threats). For the purposes of this design guide, this capability represents endpoint anti-malware.

Least Privilege Access Control

Zero trust requires that a user be given access only to the applications they need to do their job — and no more. Application access should be governed by adaptive access policies, created based on the sensitivity of the data in the application. This granularity ensures that access is provided only to users or groups of users who need it, from locations and devices that are trusted. To protect the network from discovery, lateral movement and impairing process control, a remote access solution must provide the following capabilities:

- **Identity Authorization** - Establish trust by verifying user and device identity at every access attempt. Least privilege access should be assigned to every user and device on the network, meaning only the applications, network resources and workload communications that are required should be permitted. Access to the full network should never be granted.
- **Time-based Access –** Remote access should not be an always-on feature. Access should be granted only when needed and restricted to the resources required for a given access attempt. A remote access solution for the OT network should be off by default, and access is granted at time of need, for a specified period before being turned off by the system. If a session expires beyond the allocated window, a new session must be created.

Auditing

Many compliance standards will require that an audit trail be maintained for all activity that occurs from remote networks:

- **Authentication Logs –** Authentication logs show where and how users authenticate, with usernames, location, time, device posture, and access logs.
- **Administration Logs –** Administration logs show the sessions that were created, who created the sessions, and what access control measures were put in place for the end users.
- **Session Monitoring –** Enable an administrative user to supervise a remote session and view in real-time what is happening during the session. For example, when an external technician delivers remote support for an asset, an internal OT operators may want to overlook the actions taken during the remote access session.
- **Session Termination –** The ability for an administrator to terminate an active session that either should never have become active in the first place, or while monitoring a session, the remote user attempts to deviate from their permitted actions.
- **Session Recording –** The ability for remote sessions to be recorded and stored for use in an audit trail. If a breach were to occur, having the ability to watch what remote users did to a system aids incident investigation.
- **Flow Analytics**. Network Detection and Response (NDR) solutions leverage pre-existing infrastructure to offer enterprise-wide, contextual visibility of network traffic. Flow information can be used to conduct forensic analysis to aid in lateral threat movement investigations, ensure ongoing zero trust verification is provided, and modern tools can even detect threats in encrypted traffic.

Secure Equipment Access Design Guidance

To address the secure remote access requirements outlined in the previous section, this Cisco Validated Design (CVD) guide describes the following platforms and software to accomplish a comprehensive and secure remote access for industrial networks design:

- Cisco Secure Equipment Access (hosted by IoT Operations Dashboard)
- Cisco Duo
- Cisco Secure Endpoint

Cisco Secure Equipment Access

Cisco Secure Equipment Access (SEA) and SEA Plus are IoT Operations Dashboard services that enable operations teams to easily connect to remote assets or machines for configuration, monitoring, and troubleshooting. These services provide granular access controls that can easily be managed by an operations administrator, and secure connectivity for authorized users, including internal employees and external workers. The SEA services help organizations to improve efficiency by decreasing the time and cost required for travel to remote sites for equipment maintenance or to respond to an emergency. For example, operations teams can configure equipment such as traffic signal controllers, in-vehicle dispatch systems, cameras, and other systems deployed in the field and connected using Cisco Industrial Routers.

Using SEA, a worker can access a remote asset from anywhere simply by using a browser, without needing to install any additional software on their laptop. The remote equipment can be accessed using either GUI- or CLI-based methods. Supported protocols are HTTP(S), SSH, RDP for Windows-based systems, VNC, and Telnet.

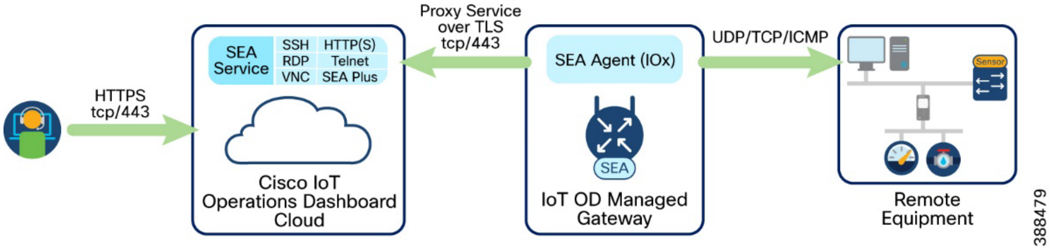
***Note**: Although HTTP and Telnet are not recommended forms of communication due to their use of cleartext, when used under the SEA construct they are wrapped in an encrypted session, and therefore the communication only becomes cleartext at the other end of the proxy (SEA Agent). Precautions still need to be implemented* *between the SEA agent and the target endpoint.*

SEA Plus provides further flexibility by enabling users to configure any type of equipment that supports IP connectivity. With SEA Plus, a direct, secure data connection is created between client software on the user's computer and the remote asset, enabling the user to easily interact with and exchange files with the asset. SEA Plus supports IPv4 TCP, UDP, and ICMP based protocols. The feature provides users with the advanced ability to define specific channels for communications between a user and the remote system and block everything outside.

Cisco SEA Components

SEA comprises a few elements that must be considered when architecting a secure remote access solution.

Figure 5 Components of Cisco SEA



IoT Operations Dashboard

Cisco IoT Operations Dashboard (IoT OD) is a cloud-based dashboard that empowers both operations teams and IT support staff to securely deploy, monitor, and gain insights from networking devices and connected industrial assets at massive scale. At the time of writing this guide, IoT OD supports the following services:

- **Edge Device Manager** - configure, deploy, and monitor supported Cisco Industrial Routers.
- **Secure Equipment Access** - securely connect to remote assets.
- **Cyber Vision** - device visibility and security posture.
- **Edge Intelligence** - enable edge to multi-cloud data orchestration.
- **Asset Vision** - monitor assets and facilities using Cisco industrial sensors.
- **Industrial Wireless** - configure and manage Cisco Industrial Wireless devices.

Note*: The scope of this design guide is remote access using Secure Equipment Access and its relevant integrations. For more information on any other IoT OD services see Cisco IoT Operations Dashboard.*

Secure Equipment Access Agent

IOx is a Cisco-developed end-to-end application framework that provides application hosting capabilities for different application types on Cisco network platforms. The SEA agent is an IOx application that is installed on supported network devices. The SEA agent creates a secure connection (TLS 1.3 over TCP port 443) to the IoT OD cloud and provides a reverse proxy function from the SEA cloud to the devices in an OT network. The SEA agent is supported on the following network devices:

- The **Cisco Catalyst IR1101 Rugged Series (IR1101)** is Cisco's smallest modular industrial router. Built for flexible deployment options via additional expansion modules, it supports multi-path LTE and 5G as well as DSL WAN backhaul connectivity for mission critical IoT initiatives requiring highly secure data delivery and redundant connectivity for fixed location applications. With up to two cellular modems, the IR1101 can concurrently connect to two cellular networks for high reliability or throughput, and/or to wired connections such as fiber or DSL. Additional modules can be added to expand connectivity to serially connected devices using various industry protocols as well as monitor and control connected devices using general purpose I/O.

- The **Cisco Catalyst IR1800 Rugged Series (IR1800)** routers are secure, high-performance, 5G routers in a modular design that support private LTE. The available modularity provides multi-path LTE and/or WAN backhaul for mission critical IoT initiatives requiring highly secure data delivery, edge application execution, and redundant connectivity. With dual 5G modems, the IR1800 can concurrently connect to two cellular networks for high reliability, enhanced data throughputs, load balancing, and differentiated services. Additional modules can be added to expand connectivity with Wi-Fi 6 and edge compute storage.

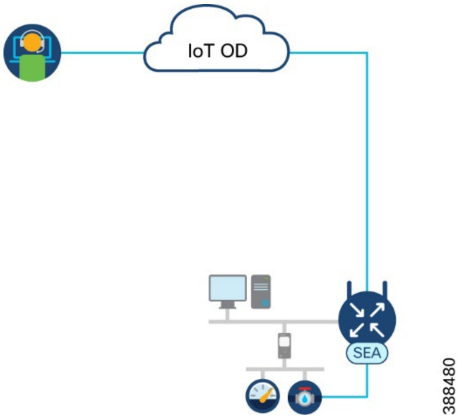
***Note**: In the current version of this CVD, SEA is only supported on network devices that are being managed by Edge Device Manager (EDM) on IoT OD. This will be changed in a future release and subsequent design guidance will be added to an updated version of this guide. Reach out to your Cisco representative for more details.*

Cisco SEA Architecture Guidance

The position that SEA components are placed in the architecture will depend on the architecture that remote access is being granted.

Some use cases, such as distributed assets in a transportation network, will manage industrial routers in IoT OD using a direct connection over a cellular interface.

Figure 6 Connecting the SEA Agent to IoT OD over a cellular channel



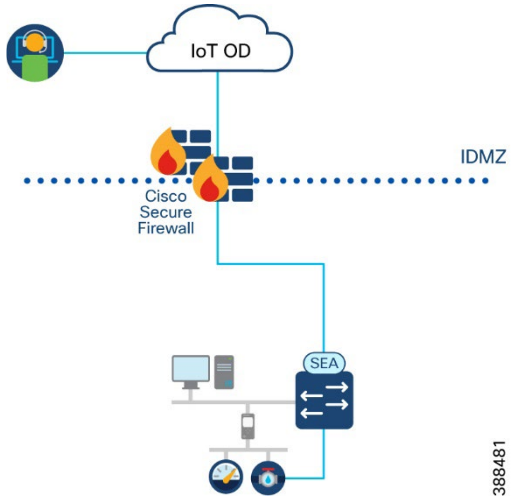
In this architecture, there is no interference between the SEA Agent sitting on the Industrial router and the IoT OD cloud and no additional architectural considerations are required.

Cisco SEA provides benefits to more than just cellular connected devices. Industrial Automation networks, or any network that has a Purdue model structure (OT - IDMZ - IT), typically deploy VPN solutions, accompanied by Jump Servers in the ICS network. When pivoting to a ZTNA solution, a decision needs to be made on where the SEA Agent will be installed.

The SEA Agent requires two connections. On the northside interface, the SEA Agent needs IP connectivity to the IoT OD cloud. On the southside interface, the SEA Agent needs IP accessibility to the target endpoints.

The first architecture option is to place the SEA Agent(s) within the same subnet that the remote targets reside.

Figure 7 Connecting the SEA Agent through IT controlled network



By deploying the SEA Agent within the same subnet as the target devices, the SEA Agent becomes part of the same layer 2 domain and does not require any additional routes or security policies to be placed on the network to reach the target devices. A secure connection is created from the SEA Agent in the process network (for example, a Cell/Area Zone) and sent through IT controlled infrastructure to the IoT OD cloud. The SEA Agent then proxies remote connections into the process network, and additional policy can be put in place on the network device to contain all remote access sessions to the layer 2 domain where the SEA Agent resides.

Note*: At time of writing this guide, the SEA agent supports only a single interface which means the IP address for the SEA agent must have IP accessibility to both the IoT OD cloud and the target devices. When making an architecture decision on where to place the SEA agent, it is important to make a decision that enables this type of support.*

The following TCP/UDP network ports and IP protocols must be opened on the network firewall to allow the edge devices to communicate with Cisco IoT OD.

Table 1 Firewall Rules for IoT OD access

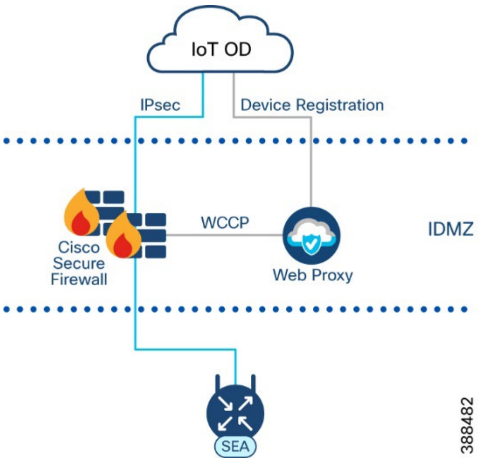
Port	Protocol	Destination	Description
53	UDP	IP (Internet Protocol) of assigned DNS (Domain Name Service) Server	The network device must have access to DNS resolution service
80 **443**	TCP	devicehelper.cisco.com	PnP server used to register the network device with IoT OD
123	UDP	NTP Server	Network Time Protocol (NTP) server for the device
443	TCP	https://us.ciscoiot.com or https://eu.ciscoiot.com	HTTPS connection to access IoT OD and for devices to register via PnP (Plug and Play).
500	UDP	csr0-us2.ciscoiot.com or csr0-eu1.ciscoiot.com	Bidirectional access is required for the Internet Security Association and Key management Protocol (ISAKMP) / Internet Key Exchange (IKE)
4500	UDP	csr0-us2.ciscoiot.com or csr0-eu1.ciscoiot.com	Bidirectional access for IPsec NAT (Network Address Translation) traversal

***Note**: You only need to choose one between EU and US in your firewall rules depending on which cluster is relevant to your deployment.*

***Note**: If you require IP address filters instead of domain name filters see IoT OD Firewall Rules for an up-to-date list of IP addresses for each of the URLs specified in the table above.*

In some instances, your organization may be using a web proxy in the IDMZ to proxy all web connection from the OT network to the cloud.

Figure 1 Connecting SEA Agent to IoT OD via a transparent Web Proxy



Typically, when web proxies are used to secure web connections at an Internet edge, the web proxy is setup in an implicit (transparent) mode, where the web cache communication protocol (WCCP) is used to redirect all web traffic (for example, TCP port 80 and 443) from the edge firewall to a dedicated web proxy before leaving the network. When managing a device in IoT OD, the network device will register with the cloud using a plug-in-play service. The device registration occurs over HTTPS and therefore can be redirected through a web proxy.

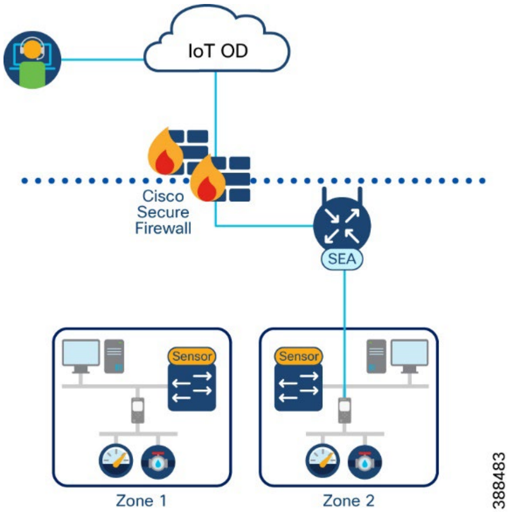
***Note**: In this current version of the design guide, there is no support for using an explicit proxy for network device registration.*

After device registration, the network device establishes an IPsec tunnel with IoT OD, which is not sent through a web proxy. Firewall rules are needed at the IDMZ to allow this communication to occur from each SEA Agent that has been installed in the network.

***Note**: In a future release, Cisco SEA will be moving to a web socket deployment and will no longer require IPsec tunnels to operate. At that time subsequent design guidance will be added to an updated version of this guide. Contact your Cisco representative for more details.*

The last architecture consideration that will be discussed in this guide is the placement of the SEA Agent in the IDMZ.

Figure 2 Placing SEA Agent in the IDMZ



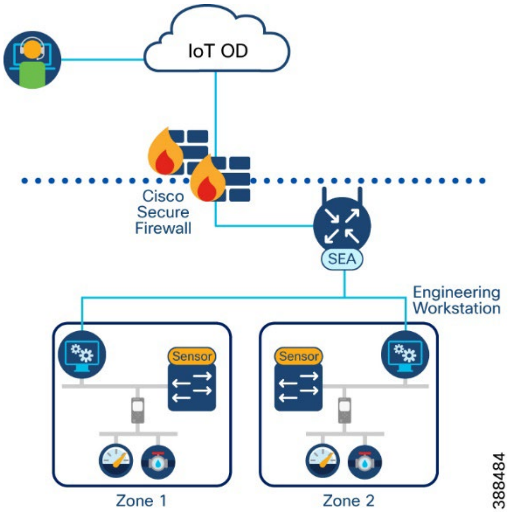
The IDMZ is designed to be the boundary between the IT and the OT network. Services that reside within the IDMZ have interfaces into both parts of the network, which is appropriate for the SEA Agent. The advantage of putting the SEA Agent in the IDMZ is that it tightly aligns with existing mechanisms that may already exist in the network. Nothing in the OT domain should have a direct connection through the IDMZ. The SEA Agent is a security appliance, and because it follows the principles of zero trust, the presence of the agent within the OT network does not pose an additional security risk to the organization.

If the SEA Agent is to be placed in the IDMZ, the IP address of the agent will need IP connectivity to all potential remote access targets in the OT network. The security administrator may need to establish additional policies to ensure that the SEA agent is not blocked by additional firewall policies or switch access control lists.

Note*: If your organization is following the segmentation guide from Cisco's Industrial Security Design Guide, the recommendation is to provide a static SGT (Security Group Tag) assignment to the SEA Agent IP address and to create SGACLs that allow the chosen tag to communicate with all other SGTs in the OT network.*

If the organization is not yet ready to deviate from the traditional remote access solution, there may still be challenges with controlling access to engineering workstations that SEA can help solve.

Figure 3 Using SEA to complement the existing traditional remote access solution



Engineering workstations are placed throughout the ICS network to bring remote vendors down to the cell/area zones to perform remote maintenance of their machines. One of the problems that arises from this is the possibility of an *always on* connection, or the administrative overhead of managing both VPN credentials and RDP access. By placing the SEA agent in the network, the product can be used to control vendor access to engineering workstations and gain all the user authentication, access control, and auditing benefits the SEA solution provides.

Cisco Duo

As discussed previously, a ZTNA solution is broken down into three key components: verifying users, verifying devices, and least privilege access control. While SEA provides an extensive list of capabilities for least privilege access control, Cisco Duo provides both user and device verification.

Duo integrates with SEA in two ways:

- **Single Sign On**: SSO allows users to log in to IoT OD using their corporate account credentials. When a user enters their email ID, they are redirected to your organization Identity Provider (IdP) authentication page. After authentication, they are redirected back to IoT OD and logged in. By integrating Duo with the IdP, all users who log in to IoT OD via SSO will be protected by Duo policy.

- **SEA Plus**: Separately, Duo is natively integrated into SEA for the SEA Plus access method. SEA Plus enables client-based access to the OT network, which requires extra caution to be taken on which devices can be brought into the network.

  Note*: Both methods can be protected by the same Duo administration account but are two separate integrations. The SSO is a function of IoT OD login, while SEA is an application within IoT OD. The Duo integration that is embedded in the SEA user interface does not address user access to IoT OD.*

Cisco Duo Components

Cisco Duo is a cloud-based solution but does comprise of some on-prem elements depending on the use case for your Duo deployment. For this design guide only two components are required:

- Duo Administration Panel
- Duo Device Health Application

Duo Administration Panel

The Duo Administration Panel is a software as a service (SaaS) where a Duo administrator can manage all aspects of a Duo subscription such as enforce policy on protected applications, manage user and their devices or monitor access activity.

An application in Duo is the mechanism to bind Duo protection to one or more of your services. For example, a Duo administrator may add the *Microsoft RDP* application to add MFA to their remote desktop logins or may add the *Microsoft Azure Active Directory* application to add protection to Azure Active Directory logons.

For this design guide, integration is between two cloud services (such as Duo and IoT Operations Dashboard) and therefore no distinctive design considerations are required.

Duo Device Health Application

Duo helps you control access to your applications through the policy system by restricting access when devices do not meet particular security requirements. Users are prompted to download the Duo Device Health app during the first log in attempt to a protected application with the Device Health application policy set to require the app. After installing the Device Health application, Duo blocks access to applications through the Duo browser-based authentication prompt if the device is unhealthy based on the Duo policy definition and informs the user of the reason for denying the authentication.

For more information see *Duo Device Health*.

Validating User Trust with Cisco Duo

Cisco Duo is built on the foundation of zero trust. Duo verifies the identity of users and protects against breaches due to phishing and other password attacks with an advanced MFA solution, verifying trust in multiple ways before granting access.

Multifactor Authentication adds a second layer of trust that your users are who they say they are. After completing primary authentication (usually by entering a username and password), users verify their identity a second time, through a different channel. This reduces the likelihood that someone else can log in, because they would need both the password and their second factor to pose as the original user.

Duo provides flexible authentication options to fit a broad range of users, security profiles, and technical backgrounds such as employees, frequent travelers, contractors, vendors, customers, and partners. For more secure access to high-risk applications, require the use of:

- Easy to use, out-of-band mobile push notifications
- Phishing-proof Universal 2nd Factor security keys
- Biometric-based WebAuthn

Other MFA methods support diverse user login scenarios:

- Phone call-back for users who cannot receive texts
- Mobile one-time passcodes for travelers while offline
- Text message passcodes for users without Internet connectivity
- Temporary bypass codes for users who temporarily cannot use their enrolled devices

With Duo, you can enforce contextual access policies allowing access to your applications with user-, device-, and location-based controls. The context includes several aspects of their login attempt such as where they are located, what role they have in your organization, what type of device, they are using, and so forth. With these policies, you can limit access to only what your users need to do their jobs and add stricter controls for access to more sensitive applications without negatively impacting use workflows.

Validating Device Trust when using the SEA Plus Access Method

Duo verifies the security posture and management status of endpoints before granting access to your applications, and blocks access if the device is unhealthy or does not meet your security requirements.

Before enabling client-based access, Duo can check the security health of all user devices attempting to access your applications. By leveraging the visibility of devices connecting to your applications, you can establish device-based access policies to prevent any risky or untrusted devices from accessing your applications. For access to high-risk applications, you may require a device to be corporate-owned or managed by your organization's IT team.

Duo allows you to establish mobile device trust with or without the use of Mobile Device Management (MDM) software. Users may object to installing MDMs on their personal devices due to privacy concerns, resulting in lower overall adoption and reduced insight into their device security. And sometimes it is outside of your IT team's control to install an agent on the personal devices of third-party provider that may need access to your applications.

Whether or not you have an MDM solution, Duo can allow you to block devices from accessing your applications based on:

- OS, browser, and plug-in versions, and how long they have been out of date
- Status of enabled security features (configured or disabled)
- Full disk encryption
- Mobile device biometrics (face ID/touch ID)
- Screen lock
- Tampered (jailbroken, rooted, or failed Google SafetyNet)

Cisco Secure Endpoint

Cisco Secure Endpoint integrates prevention, detection, threat hunting, and response capabilities in a unified solution leveraging the power of cloud-based analytics. Secure Endpoint will protect your Windows, Mac, Linux, Android, and iOS devices through a public or private cloud deployment.

***Note**: SEA Plus is only supported on Windows (minimum version Windows 10 64-bit).*

Duo and Secure Endpoint work together to provide stronger access security. With Duo and Secure Endpoint, you have the tools in place to establish trust in users' devices connecting to protected applications. Together, they offer the ability to:

- **Prevent:** Duo evaluates risk conditions, device health, and security status on every access attempt. Secure Endpoint strengthens defenses using the best global threat intelligence and automatically blocks known fileless and file-based malware.
- **Detect:** Duo verifies whether the Secure Endpoint agent is running on the user's device before granting application access. Secure Endpoint detects stealthy threats by continuously monitoring file activity, while allowing you to run advanced search on the endpoint.
- **Respond:** Duo automates the response by leveraging telemetry from Secure Endpoint to block access from devices infected with malware. Secure Endpoint rapidly contains the attack by isolating an infected endpoint and accelerating remediation cycles.

The Cisco Secure Endpoint integration verifies endpoint status and blocks access from Duo trusted endpoint client systems that Cisco Secure Endpoint identifies as "compromised". By restricting SEA Plus access to only those devices with a clean Secure Endpoint install, you can gain peace of mind that use cases such as file transfer from remote users to OT devices will not contain hidden malware and cause a breach by an unwitting threat actor.

Cisco Secure Endpoint Capabilities

In the rapidly evolving world of malware, threats are becoming harder and harder to detect. The most advanced 1% of these threats, those that will eventually enter and wreak havoc in your network, could potentially go undetected. However, Secure Endpoint provides comprehensive protection against that 1%. Secure Endpoint prevents breaches, blocks malware at the point of entry, and continuously monitors and analyses file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

Stopping threats at the earliest point in time ensures minimal damage to endpoints and less downtime after a breach. Secure Endpoint employs a robust set of preventative technologies to stop malware, in real-time, protecting endpoints against today's most common attacks as well as emerging cyberthreats.

- **File Reputation:** known malware is quickly and easily quarantined at the point of entry without any processor-intensive scanning.
- **Antivirus:** endpoints benefit from custom signature-based detection, allowing administrators to deliver robust control capabilities and enforce blocklists.
- **Polymorphic malware detection:** Malware actors will often write different variations of the same malware to avoid common detection techniques. Secure Endpoint can detect these variants, or polymorphic malware through loose fingerprinting. Loose fingerprinting will look for similarities between the suspicious file content and the content of known malware families, and convict if there is a substantial match.
- **Machine Learning analysis:** Machine learning capabilities in Secure Endpoint are fed by the comprehensive data set of Cisco Talos to ensure a better, more accurate model. Together, the machine learning in Secure Endpoint can help detect never-before-seen malware at the point of entry.
- **Exploit Prevention:** Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.
- **Script protection:** provides enhanced visibility in Device Trajectory into scripts executing on your endpoints and helps protect against script-based attacks commonly used by malware. Script control provides additional protection by allowing the Exploit Prevention engine to prevent certain DLLs from being loaded by some commonly exploited desktop applications and their child processes.
- **Behavioral protection:** enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve.
- **Device Control:** lets you control the usage of USB mass storage devices and prevent attacks from these devices.

Secure Equipment Access Implementation Guidance

The following section explains how to implement the Secure Remote Access solution described in this design guide.

***Note**: The design guide will provide implementation guidance within the scope of this design guide. For a complete list of IoT OD implementation steps, click here.*

Pre-Requisites

The following deployment steps are pre-requisites for completing the deployment steps described in this guide.

- Set up IoT Operations Dashboard.
- Onboard network devices. *Note: At the time of publishing, the supported devices are the Cisco IR1101 and IR1800 Rugged Routers family.*
- IoT OD Advantage license for these devices to gain access to Secure Equipment Access.

Add Users to IoT OD

IoT Operations Dashboard (OD) provides Roles and Permissions for users. A Role is defined as a collection of one or more Permissions. IoT OD provides two default Roles with a specific set of pre-determined Permissions. The default Roles and accompanying Permissions cannot be changed. The built-in Roles have the following capabilities and privileges:

- **Tenant Admin**: Manage users & sub-tenants (organizations).
- **Device Operator**: Manage and troubleshoot devices.

Within IoT OD, each application then has its own set of roles and permission for their users. For the purposes of this guide, the following built-in SEA roles will be used. A **SEA System Admin** should be created to add SEA Agents to network devices, configure connected clients, and define the access methods to reach those clients. The SEA System admin should also be assigned as a **SEA Access Admin**. An SEA Access admin has permissions to both access remote sessions and manage user permissions to those sessions. **SEA Users** are the end users of the remote access deployment. These users have no configuration privileges, but simply consume the product within the boundaries set by the admins.

To add a user, as a Tenant Admin:

1. Click the organization dropdown menu in the top right of the IoT OD dashboard. Click **Access Control**.
2. Click **Users > Add User.**
3. Enter a **valid email address**.
   - A welcome email with log in and password instructions is sent to this address.
   - If your organization uses SSO (described later in the guide), users receive a confirmation email but are not prompted to enter a password. They will use their corporate credentials to login instead.
4. Select one or more **Roles** to define the user's access permissions.
5. Select **Extend Roles to Sub-tenants** to apply the same toles to any sub-organizations the user can access.
6. Click **Save**.

Create User Groups

User groups are a mechanism in SEA to determine what access methods (discussed in a later section) are available to SEA Users. To create a user group:

1. In IoT OD, navigate to **Secure Equipment Access > Access Management.**
2. In the **Access Control Groups** tab, click **Add Group.**
3. From the **Add Group** screen:
   - Give a meaningful **Name.**
   - (Optional) Provide a **Description.**
   - (Optional) Enable **Schedule Settings** (described later in the implementation guide).

   ***Note**: By default, the **Group Enabled** toggle switch is set to Enabled. When a group is disabled, they will not have access to remote sessions. As an SEA Admin, this option may be used to temporarily disable remote access during a shutdown period without removing all the subsequent policies.*

4. Click **Save**.

Add Users to the User Group

To add a user to the user group:

1. In IoT OD, navigate to **Secure Equipment Access > Access Management.**
2. Click on the **User group** in which users will be added.
3. Under the **Users** tab, click **Add Users.**
4. Select the **users** to add to the group and then click **Save**.

***Note**: Users can be added to multiple user groups. The design implications of this will be discussed in the chapter **Add Access Methods to User Groups**.*

Enable Multi-factor Authentication

***Note**: IoT OD offers MFA access to IoT OD for locally configured users (meaning your Organization's Tenant Admin adds users to your organization and grants roles/permissions to those users). In this scenario, the first factor is username/password, and the second factor is a one-time password via email. The built-in MFA solution to IoT OD is a free value add, and is more secure than no MFA at all, however this design guide recommends using MFA with SSO. For more information on using MFA without SSO click here.*

***Note**: Cisco Duo offers three paid editions to choose from. For MFA and SSO protection, a Duo Essentials license is required. For SEA Plus posture assessment, a Duo Advantage license is required. While Duo has a cost, it offers more capabilities over a one-time password solution, providing more control over the users who access your critical infrastructure. For more details see Duo editions and pricing.*

SSO allows users to log in using their corporate account credentials instead of locally configured credentials in IoT OD. When a user enters their Email ID into IoT OD, IoT OD being the Service Provider (SP), they are redirected to your organization's Identity Provider (IdP) authentication page. After authentication, they are redirected back to the IoT Operations Dashboard (IoT OD) and logged in.

IoT OD can integrate with any SSO provider who uses the Security Assertion Markup Language (SAML) 2.0. SAML is a protocol for authenticating web applications. It simplifies the login experience for users by allowing access to multiple applications with one set of credentials. SAML is the underlying protocol that makes web-based SSO possible and provides a way for users to authenticate themselves when logging into third-party apps. For more information on SAML. See What is SAML?

Cisco Duo is a cloud hosted SAML IdP that adds MFA and access policy enforcement to SSO logons. Duo SSO offers generic connectors with the ability to provide metadata and connect to any app that supports the SAML 2.0 standard. However, Duo is not a primary IdP, so it does not have the ability to check the credentials provided by a user. Duo must integrate with a primary IdP such as Microsoft Active Directory or a SAML IdP for first-factor authentication. Protected cloud applications (for example, IoT OD) redirect users to Duo SSO, authenticate your users using an existing primary authentication source for credential verification, and then prompt for 2FA before permitting access to the application.

For more information on Duo SSO, including the implementation guidance, see Duo Single Sign-On.

To add SSO to IoT OD you must ask your Cisco representative to integrate your account(s) with your corporate identity provider. The Cisco support team will contact you to start the integration process, and you will need the following information:

- SAML metadata for the IdP (for example, metadata for Duo SSO)
- Email domain(s) or email addresses that use SSO

For more information see Enable Single Sign-On.

Add SEA Agent to Network Device

***Note**: The network device must be managed by EDM on IoT OD. This will be changed in a future release and subsequent design guidance will be added to an updated version of this guide. Contact your Cisco representative for more details.*

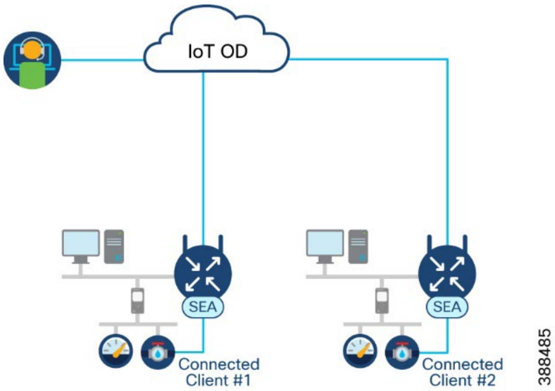
To add the SEA agent to a network device that is managed by EDM:

1. In IoT OD, navigate to **Secure Equipment Access > System Management.**
2. In the **Network Devices** tab, click **Add Network Device.**
3. Select a **network device** from the list or search for it using the **Search** field. Click **Next**.
4. Enter a **network device description**, if needed, and click **Add Network Device** to start the installation of SEA on the device.
5. Click **Next**.
6. Check the SEA Agent state of deployment associated with the network device
    - **SEA Agent** should be changed to **Installed**. If the status does not change to Installed, then go to network device listing and hover over the 3 dots in the Actions column and select **Install SEA Agent**.

Add Connected Clients

Connected clients refer to the endpoint devices that are IP accessible from the SEA Agent. By configuring a connected client on the network device, you are choosing to proxy remote connectivity to that endpoint from the chosen SEA Agent. If more than one SEA Agent exists on the network, make sure to assign the appropriate connected clients to the appropriate SEA Agent.

Figure 4 Multiple SEA Agents installed in the network



To add a connected client to an SEA Agent:

1. In IoT OD, navigate to **Secure Equipment Access > System Management.**
2. In the **Network Devices** tab, click the **Network Device** in which a connected client should be added to open the network device details page.
3. Click **Add Connected Client.**
4. Click the dropdown box under **Selection Method** choose **Manual entry**
5. Add a meaningful **Client Name** and add the **IP Address/Host Name** of the target device. Click **Add**.

***Note**: To remove a connected client from a network device, hover your mouse over the 3 dots (…) in the Actions column and then click **Delete**.*

Add Access Methods

Access methods are the mechanisms by which an SEA user will interact with a connected client. To follow the principles of least privilege access control, a user does not have full access to a device unless specified by an SEA Admin. Access methods control what protocols a user can establish with a connected client. SEA incorporates two groups of access methods:

- **SEA** offers a clientless approach where a user can use a supported web-browser to communicate with remote hosts and applications. Supported protocols are: **SSH**, **RDP**, **VNC**, **HTTP(S)** and **Telnet.**
- **SEA Plus** is a client-based access method where a user installs an SEA Plus client on their local machine to establish a secure communication channel with a remote system. SEA Plus supports **any UDP**, **TCP,** or **ICMP** based protocol and can communicate with a remote host across **any port**.

To add an access method for the SEA Connected Clients:

1. In IoT OD, navigate to **Secure Equipment Access > System Management.**
2. In the **Connected Clients** tab, click the **Connected Client** in which you want to assign access methods to open the connected client details page.
3. Click **Add Access Method.**
4. Click the dropdown link under **Access Method Details** and choose which protocol you would like to add. Depending on the access method was chosen, fill in the appropriate fields.

   ***Note**: For more details on how to customize each access method see: SSH, RDP, VNC, Web App, Telnet, SEA Plus*

5. Click **Add Access Method.**
6. Repeat the process for each access method you wish to assign to the device.

***Note**: SEA Admins have the option to include login credentials for the SSH, RDP, VNC & Telnet access methods. This option enables SEA Users to login to devices remotely without credentials being known to anybody other than the system administrators. It is recommended to use this option to avoid password leak.*

Add Access Methods to User Groups

After access methods have been established, an SEA Admin must determine which user groups have access to these access methods. Distinct groups of users may have access to the same connected clients, but have different privileges provided to them. For an example, a remote technician may be given access to a connected client over a web interface, however, the application administrator may have access to the same connected client over its web interface and an SSH connection or advanced troubleshooting.

To add access methods to user groups:

1. In IoT OD, navigate to **Secure Equipment Access > Access Management.**
2. Click on the **User group** in which a new access method should be added.
3. Under the **Connected Client Access** tab, click **Add Connected Client Access.**
4. Select the **Connected Clients** to add to the group and then click **Save.**

***Note**: A user can have access to one or more groups. It is recommended to create groups based on role. For example, a network administrator may be part of a 'Network Admin' group which has permission to access network devices over SSH and HTTPS. A third-party operator could be part of 'Vendor A' user group which has access to a Programmable Logic Controller (PLC) over the SEA Plus access method. If a user needs access to both sets of resources, rather than create a new user group with extended permissions, it is recommended to add the administrative user as a member to both user groups and then they will have access to both sets of connected clients and their respective access methods.*

Verify SEA Connectivity

1. In IoT OD, navigate to **Secure Equipment Access > Remote Sessions.**
2. For each access method assigned to the logged-in user, a tile will exist. Click any tile to confirm connectivity is successfully enabled.

Scheduling Access for a group

Remote access to an ICS network should not be an *always on* feature. Remote access should be purpose driven, and there should be an outcome with each session that is granted. By leaving the door constantly open, it leaves the systems open to an attack, and while defense-in-depth mechanisms may be put in place to prevent those attacks from succeeding, the absolute best form of defense is to turn off access completely.

When a user group is created in SEA, an admin can schedule a specific time that those users gain access to configured devices. To schedule a specific time to access remote devices:

1. In IoT OD, navigate to **Secure Equipment Access > Access Management.**
2. Click on the **User group** in which a time schedule will be added.
3. Click the **pencil icon** next to **Group Details.**
4. Click the **Schedule Settings** toggle button.
5. Select the **Start** time and **End** time for the SEA session.
6. Click **Save.**

If an SEA user logs in to the dashboard outside of the scheduled hours, they will still see which access methods have been made available to them, but the boxes will be greyed out and unclickable.

SEA Plus

When using SEA Plus to access remote systems, you can employ TCP, UDP, and ICMP (Internet Control Message Protocol) protocols for data transfer across any port. As an SEA Admin you have the option to allow unrestricted access to a connected client (such as, all ports are open to the user) or to restrict access to a defined set of ports (such as, only allow communication over port 502). To create a protocol definition for use in the SEA Plus Access Method:

1. In IoT OD, navigate to **Secure Equipment Access > System Management.**
2. Under the **SEA Plus Protocols** tab select **Add Protocol Definition.**
3. Give a meaningful Name, and then click **Add Protocol**.
4. In the **Network Protocol** dropdown box choose **TCP**, **UDP**, or **ICMP** and the **Port / Port Range** for the desired communication:
    - For example, to enable Modbus communication from a remote device and a connected client, an SEA Admin would choose to open TCP port 502 and assign it to a connected client. This would enable a remote user to access the device with their own client machine over port 502, but communication that falls outside of TCP port 502 would be denied by IoT OD.
5. Click **Add Protocol.**
6. Continue to add protocols under the full protocol definition has been defined.
7. When you are finished, click **Save Protocol Definition.**

To add the SEA Plus access method to a connected client:

1. In IoT OD, navigate to **Secure Equipment Access > System Management.**
2. Select a **Network Device** to open the network device details page.
3. Click on a **Connected Client** to open the associated access methods for that client.
4. Click **Add Access Method**.
5. Select **SEA Plus.**
6. Select either **All** (default) to access all ports on the connected client or **Custom** to add previously created protocol definitions and provide restrictions to the SEA Plus session.
7. (Optional) Click **Advanced Settings**. The advanced settings tab allows you to automatically cross launch additional services when connecting to a client over SEA Plus:
    - **Application Cross Launch URL (Uniform Resource Locator)**: Automatically open a web-based application on the local browser that will be used to interact with the remote client. For example, when a user clicks on a Human Machine Interface (HMI) using the SEA Plus access method, automatically launch the web interface for that HMI.
    - **Application Cross Launch Path**: Automatically launch an executable from the local machine. For example, when a user clicks on the SEA Plus access method for a Rockwell PLC, automatically launch FactoryTalk Studio.
    - **Application Cross Launch Advanced Parameters**: Additional parameters that the cross-launch services will use, such as a password to open the cross-launched application.
8. Provide a meaningful access **Name** and optional **Description.**
9. Click **Add Access Method.**

Posture Check for SEA Plus

As SEA Plus is a client-based remote access technology, it is critical that the client is checked for malware and overall security health before being brought into the network. Remote access use cases covered by this product include firmware upgrades to vendor machinery. You could rely on network checks for malicious files, however, by applying policies directly on the machine, the Cisco solution stops malware at the source, and if any malicious files or activities are present on the machine, the posture check performed by Duo will block access immediately, even if the connection is not related to a file transfer.

To setup the integration to Duo, the SEA system admin must have a Duo Admin account with a unique URL, or the SEA system admin must work with a dedicated Duo administrator for their organization. The integration between Duo and SEA Plus has two steps: creating the SEA Plus application in Duo and then adding the Duo client ID and secret to SEA.

To configure the SEA Plus application in Duo:

1. In the Duo administration dashboard, navigate to **Applications.**
2. In the **Applications** page, select **Web SDK** and click **Protect**. *Note: You can search for Web SDK in the search bar.*
3. In the newly-created Web SDK application page, take note of the **Client ID**, **Client Secret** and **API Host Information.**

Note*: It is recommended to change the name of the Web SDK application to something more meaningful such as 'SEA Plus'. This can be done in the* ***Settings*** *tab at the bottom of the application details page.*

To configure Duo for SEA Plus:

1. In IoT OD, navigate to **Secure Equipment Access > System Management.**
2. Under the **External Integrations** tab, click **Add External Integration.**
3. In the **Integration Type** dropdown menu, choose **Duo.**
4. Provide a meaningful **Name** to the integration and an optional **Description.**
5. Enter the **Client ID**, **Client Secret** and **API Host** from the previous step.
6. Click **Add Integration.**

Note*: SEA Plus only allows one entry of the same integration type, although multiple Duo integrations can be configured simultaneously. One use case for this feature is to introduce a new policy to the SEA Plus users while maintaining the old policy. If there are problems with the new policy, the SEA Admin can revert to the old while troubleshooting occurs. This will ensure posture is always checked, and security checks are not bypassed between policy migrations.*

Cisco Duo Policies

Duo provides the ability for security administrators to define and enforce rules on who can access what applications – under what conditions. After the SEA Plus application has been created in Duo, it is automatically protected by the Duo global policy. The global policy is built-in and cannot be deleted. It always applies to all applications, so it is only modified if there are settings that should be applied across all users and all applications.

Because the scope of the SEA Plus integration is device posture assessment only, you must create a custom policy and assign it to the SEA Plus application in Duo.

Note*: When you view an application in Duo, the global policy settings are shown because these are the settings applied to all applications unless they are superseded by a custom application or group policy.*

To create a custom application policy for SEA Plus:

1. In the Duo administration dashboard, navigate to **Policies**.
2. Scroll down to **Custom Policies** and click **New Policy**.
3. Provide a meaningful **Policy name**.

Note*: This design guide will provide a recommended policy set for SEA Plus protection. The policy can be customized and tailored to the needs of your organization. For a full breakdown of the policies included in Duo see Duo Custom Policies.*

Example policy for SEA Plus:

1. Click **Authentication Policy** and choose **Enforce 2FA**. *Note: Even though we choose Enforce 2FA, we will disable it later in the policy. This setting is to force a user to use Duo, so they are subject to device posture checks.*
2. Click **User location** and choose the countries in which remote access should be enabled (choose **No action** from the dropdown for the selected countries). For **All other countries**, choose **Deny Access**.
3. Click **Device Health Application**. Under **Windows** click **Require users to have the app** and at a minimum require a **firewall** and a **system password**. It is highly recommended to also **block access if an endpoint security agent is not running**. At the time of writing this guide, the following endpoint security agents are supported:
    - Bitdefender Endpoint Security
    - Cisco Secure Endpoint (recommended)
    - Crowdstrike Falcon Sensor
    - CylancePROTECT
    - McAfee Endpoint Security
    - Palo Alto Cortex XDR
    - SentinelOne
    - Sophos AV
    - Symantec Endpoint Protection
    - Trend Micro Apex One
    - VMware Carbon Black Cloud
    - Windows Defender

    ***Note**: If you are interested in using Cisco Secure Endpoint and need design guidance to deploy, see the Cisco Breach Defense Design Guide*.

4. Click **Operating Systems** and uncheck all boxes except for **Allow Windows devices**. SEA Plus is only supported on Windows, so any authentication attempts that are not Windows would be suspicious behavior.

1. Encourage users to update If not up-to-date and when a version becomes out of date or end of life, encourage users to update immediately.
2. Block version if end-of-life.

5. Click **Authorized networks** and in the **Allow access without 2FA from these networks box** enter **0.0.0.0-255.255.255.255**. This covers every network and ensures that nobody undergoes additional 2FA checks. If additional 2FA is required for SEA Plus access, ignore this part of the policy.

    ***Note**: The reason to bypass 2FA is because we are only doing posture checks. 2FA should have already been done during login to IoT OD. If you choose to enforce 2FA in this step, additional configuration is required. To enable 2FA for SEA Plus see Appendix B.*

6. Click **Anonymous networks** and **for users that request access through proxies, Tor, or VPN** choose **Deny Access**. This will ensure users cannot bypass the geo-restrictions provided previously in the policy. ***Note**: SEA Plus client does not work when using VPN as the SEA Plus client is a lightweight VPN client with split tunnel configuration.*
7. Click **Authentication methods** and choose **WebAuthn**, **Duo Push** and **Hardware tokens**. SMS passcodes are not recommended.
8. Click **Save Policy.**

To add the custom application policy to SEA Plus:

1. In the Duo administration dashboard, navigate to **Applications.**

2. Click on the **SEA Plus** application. *Note: If you have not changed the name, it will be called Web SDK.*
3. Click the **Apply a policy to all users** link.
4. Select the newly created SEA Plus policy from the dropdown menu.
5. Click **Apply Policy.**
6. Scroll down the bottom of the page and click **Save.**

Active Session Monitoring and Termination

Cisco SEA gives an SEA system admins or SEA access admin a list of all active remote sessions for their organization. The session list will detail which connected clients are currently being access, who is accessing the session and what access method they are currently using.

Joining a session allows an administrative user to supervise supported session types and view what happens during the session. For example, when an external technician delivers remote support for an asset, an OT person can control the technician's actions and terminate the active session at any moment.

As an SEA Admin, to monitor and terminate active sessions:

1. In IoT OD, navigate to **Secure Equipment Access > Access Management.**
2. Click on the **Active Sessions** tab to get a list of all current remote access sessions.
3. To monitor an active session, click on **Join Session** in the **Monitor** column. This action brings up a real-time view into the user's current activity.
4. To terminate a session, click on **Terminate** in the **Security** column. This action will terminate a user's session immediately.

***Note**: Unless a user's access method has been revoked in by policy, an SEA User will have the ability to click the application again and regain immediate access. Make sure to disable the user's access method privileges if your intent is for permanent termination of the session.*

Audit Logs

Audit logs help meet compliance standards and identify security risks to your organization. Between Cisco SEA, and Cisco Duo, multiple sets of logs are available.

Cisco SEA offers audit logs for both system and user generated administrator logs. For example, you can see what users have been added to the system and which user group they have been assigned to. Additionally, you can see what connected clients have been added to the system and what access methods have been enabled on the machine. To view SEA Audit logs:

1. In IoT OD, click the **organization drop-down menu** in the top-right of the dashboard and click **Audit**.
2. The **Access Control** tab provides insights to user accounts, user groups created by an SEA admin, and system generated events such as feature flags that have been enabled for the organization.
3. The **Secure Equipment Access** tab provides insights into what users are doing in the SEA application. A log is created for activity such as new network device added, new connected client, new access methods, and any deletions that have been made to the system.

SEA audit logs also show remote access connection attempts; however, a more detailed view can be found elsewhere:

1. In IoT OD, navigate to **Secure Equipment Access > Access Management**.
2. Click the **Session History** tab.
3. The session history provides a breakdown of all remote access connections that have been made in the system. The session history page tells the user:
   - When the session started and ended

    - What was the target endpoint for the remote session
    - What access method was used for the connection
    - Who made the connection attempt
    - Was the session terminated by an admin or closed by the user
4. In the **Actions** column, a user can hover over the 3 dots (…) to get a full audit report for every remote access session in SEA Plus.

Cisco Duo offers a wide range of logging to supplement SEA deployments. By navigating to the **Reports** page in the Duo administration dashboard, some of the following logs can be identified:

- **Device Health Deployment:**
    - Duo analyzes what is running on all your user's devices, managed or unmanaged.
    - An analysis of your users' devices, including current device OS, browsers, Flash and Java versions.
    - Security health trends of all devices accessing your remote applications, including which devices are outdated or need to be updated by end users.
    - The latest security events that may result in outdated devices, including a new browser or plugin updated released by a software vendor.
- **Authentication Logs:**
    - Authentication logs show you where and how users authenticate, with metrics such as usernames, location, time, and type of authentication factor.
    - The success or denial of the authentication attempt along with detailed reasoning such as invalid device, no 2FA response, or user disabled.
- **Policy Impact:**
    - The policy impact report shows how policies are impacting users.
    - Get an overview of the major reasons causing authentications to be blocked, or drill down into individual blocked authentications for more details.
    - A users block by policies table shows the top users being blocked, the number of blocked authentications, the reason(s), and the applications(s) they could not access.

Appendix A – Mapping Cisco Secure Remote Access Capabilities to Common Industry Standards

Depending on the industry, or geolocation that your organization resides, there may be a compliance standard that must be met to successfully deploy a remote access solution. How a Cisco remote access solution addresses some of these industry standards can be found below.

NIST 800-82r3

The National Institute of Standards and Technology (NIST) released a special publication labelled **800-82 revision 3** to provide guidance for establishing secure operational technology while addressing the unique performance, reliability, and safety requirements encompassed by the OT. Chapter 6 discusses the application of the cybersecurity framework to OT and outline capabilities to protect remote access connections. The following table outlines how the Cisco remote access solution meets the requirements laid out by NIST.

Table 2 Meeting NIST 800-82r3 remote access requirements with a Cisco solution

NIST Requirement	Cisco Solution
A process should be developed and communicated to the organization for requesting and enabling remote access.	In Cisco SEA, an SEA System Admin must provide access to specific devices on the network which can be further policed by scheduling constraints. An always on connection should not be provided and remote access requests must go through an SEA administrator.
Remote access should be provided only if justified and limited to only what is required to meet the business need.	Remote access with Cisco SEA enables access methods to be specified so that any given user only has access to the protocols and ports that are needed to perform their task. Access privileges are explicit, and not implicit like a traditional VPN solution can be.
Remote access should not circumvent safety or security controls (i.e., a solution should not be put in place that bypasses existing security mechanisms).	While we have the option to provide SEA connectivity over a cellular connection, the communication between the SEA Agent and the IoT OD cloud can traverse an IT owned networking domain so that all connections are known, policed, and

	logged.
Implementing unique username and complex passwords.	IoT OD integrates with external IdPs which can put policy on password creation. More importantly, the use of MFA mitigates the exploitation of weak or stolen passwords. Additionally, when configuring access methods in SEA, the username and password can be provided in the setup, so a remote user never needs to know the password for the device they are accessing. An administrator has effectively entered the password on their behalf.
Removing, disabling, or modifying any default credentials.	This requirement is typically on the onus of the endpoint. However, the point on external IdP integration and MFA still stands for accessing the remote access sessions themselves.
Removing access when no longer required.	Cisco SEA provides the ability to schedule access. Once the scheduled session timeouts, the SEA user no longer has access to the remote machine until given access again.
Monitoring remote activities.	Cisco SEA can monitor, in real-time, active sessions that occur in SEA. At any point the administrator can terminate a session if they see activity that is outside the scope of the agreed remote access activity.
Ensuring operations personnel are aware of planned remote activity in the OT environment.	Cisco SEA provides a list of all active sessions to admin users of SEA.
Initiating the connection from the OT environment.	The SEA Agent which proxy’s communication between the IoT OD cloud and the target devices resides within the OT environment and the

	connection is established by the agent to the cloud.
Labelling remote connection devices so that operations may disconnect quickly in the case of unauthorized use.	A dedicated remote access device, such as the IR1101, can be deployed in the network for the sole purpose of being the remote access gateway if this requirement is to be met literally. Alternatively, SEA can terminate active sessions and disable remote access from ever occurring without unplugging the network device. This would allow you to run the SEA agent within active network infrastructure, but the app can be turned off to disable its features.

ISA/IEC 62443 3-3

The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) worked together to put together a series of standards that address the issue of security for ICS networks known as **ISA/IEC 62443**. The part of the series that discusses the requirements for a remote access solution is part **3-3** where there are a total of seven foundational requirements; identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability. The requirements for a remote access solution exist across many of the seven foundation requirements.

Table 3 Meeting ISA/IEC 62443 remote access requirements with a Cisco solution

ISA/IEC 62443 3-3 Requirement	Cisco Solution
Identification and authentication control	Cisco SEA uses the principles of least privilege when providing remote access to the network. Cisco SEA enables access methods to be specified so that any given user only has access to the protocols and ports that are needed to perform their task. Access privileges are explicit, and not implicit like a traditional VPN solution can be.
Multi-Factor Authentication	IoT OD can integrate with an external IdP which is using MFA for protecting user credentials. The design guide shows the integration

	with Cisco Duo, but any MFA integration to the IdP meets the requirement. Alternatively, SEA provides native MFA through email codes, which is not as secure as app or hardware-based MFA, however, technically meets the requirement.
Authorization enforcement	Not only does Cisco SEA provide granular access control to specific devices in the network, Cisco SEA also provides the ability to schedule access. Once the scheduled session timeouts, the SEA user no longer has access to the remote machine until given access again.
Remote session termination	Cisco SEA can monitor, in real-time, active sessions that occur in SEA. At any point the administrator can terminate a session if they see activity that is outside the scope of the agreed remote access activity.
Auditable events	Between both SEA and Duo, audit logs and reports can be generated to show conformance to compliance standards.
Communication integrity	The Cisco SEA agent communicates to the IoT OD over TLS 1.3 to ensure communication integrity between client and proxy. After data leaves the proxy, it is up to the user to only enable access methods that remain encrypted all the way to the endpoint. Although HTTP and Telnet are not recommended forms of communication due to their use of cleartext, when used under the SEA construct they are wrapped in an encrypted session, and therefore the communication only becomes

	cleartext at the other end of the proxy.
Data confidentiality	Extending upon the capabilities for communication integrity, Cisco SEA Admins have the option to include login credentials for the SSH, RDP, VNC & Telnet access methods. This option enables SEA Users to login to devices remotely without credentials being known to anybody other than the system administrators. It is recommended to use this option to avoid password leak.
Restricted data flow	Remote access with Cisco SEA enables access methods to be specified so that any given user only has access to the protocols and ports that are needed to perform their task. Access privileges are explicit, and not implicit like a traditional VPN solution can be.
Timely response to events	SEA administrators can monitor sessions in real-time and at any point the administrator can terminate an active session if they see activity that is outside the scope of the agreed remote access activity.

NERC CIP-005-7

The focus of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) reporting and audit compliance program is achieving system-level cybersecurity from each utility operator connected to the bulk electric systems (BES) in the United States and adjacent domains. **CIP-005-7**, cybersecurity for the electronic security permitter (ESP), addresses the implementation of remote access to protect BES cyber systems against compromise.

Table 4 Meeting NERC-CIP remote access requirements with a Cisco solution

NERC-CIP Requirement	Cisco Solution
Ensure that interactive remote access is through an intermediate system that is not inside an	The SEA Agent is a proxy solution between the SEA cloud and the remote target. The SEA Agent can be

applicable ESP or ESZ (Electronic Security Zone).	installed in a zone dedicated for intermediate systems and proxy remote connections between remote users and the target device. Alternatively, if the intermediary system of choice is a jump server, the SEA agent can provide all its security capabilities to the connection to the intermediary system, and existing ESP boundary protections can be used between the jump server and the target device.
Protect the confidentiality and integrity of interactive remote access between the client and intermediate system.	The connection between the SEA Agent and IoT OD cloud uses TLS 1.3 and provides the confidentiality and integrity required between the client and intermediate system.
Require MFA to the intermediate system.	IoT OD can integrate with an external IdP which is using MFA for protecting user credentials. The design guide shows the integration with Cisco Duo, but any MFA integration to the IdP meets the requirement. Alternatively, SEA provides native MFA through email codes, which is not as secure as app or hardware-based MFA, however, technically meets the requirement from NERC-CIP.
Have one or more methods for determining active vendor remote access sessions (including interactive remote access and system-to-system remote access).	Cisco SEA can monitor, in real-time, active sessions that occur in SEA. If using a jump-server as the intermediate system in a dedicated zone, Cisco Cyber Vision can be used to monitor activity between the intermediate zone and the ESZ.
Have one or more methods to disable active vendor remote	At any point, an SEA administrator can terminate an active session if

access.	they see activity that is outside the scope of the agreed remote access activity.
Intermediate system may only share CPU, memory, or ESZ or ESP with other intermediate systems.	The SEA agent can be installed in a dedicated zone for intermediate systems.

TSA Security Directive 1580/82-2022-01

The Transportation Security Administration (TSA) issued a security directive (SD) **1580/82-2022-01** due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure. The SD 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.

The cybersecurity measures mandated by the TSA for remote access, and the associated Cisco capabilities, can be found in the table below.

Table 5 Meeting TSA SD 1580/82-2022-01 remote access requirements with a Cisco solution

TSA SD 1580/82-2022-01 Requirement	Cisco Solution
Identification and authentication policies and procedures designed to prevent unauthorized access to critical cyber systems.	IoT OD integrates with external IdPs which can put policy on password creation. More importantly, the use of MFA mitigates the exploitation of weak or stolen passwords.
Multi-Factor Authentication	IoT OD can integrate with an external IdP which is using MFA for protecting user credentials. The design guide shows the integration with Cisco Duo, but any MFA integration to the IdP meets the requirement. Alternatively, SEA provides native MFA through email codes, which is not as secure as app or hardware-based MFA, however, technically meets the requirement.
Policies and procedures to manage access rights based on the principles of least privilege and separation of duties.	Remote access with Cisco SEA enables access methods to be specified so that any given user only has access to the protocols and ports that are needed to perform

	their task. Access privileges are explicit, and not implicit like a traditional VPN solution can be.
Enforcement of standards that limit the availability and use of shared accounts.	While some of the onus for this requirement is on the password management for end devices, Cisco SEA has the option to save passwords for supported access methods, so passwords are never shared to the vendors that have been given access. For example, if a remote user has scheduled access to an HMI over RDP, the network administrator can include the HMI credentials in the SEA configuration so the password is never known by the user who has been given access. Of course, credentials are still needed by the user to log into the SEA cloud, but these credentials can be protected by MFA to verify the identity of a user.
Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.	Cisco SEA provides a mechanism for scheduling remote access over a specified period. Upon expiration, the user no longer has access to the system. If it is deemed that the user needs to extend their session, or be granted access at a future date, an administrator can make that decision and re-instate their privileges for another time period.
Provide documentation to establish compliance.	Between both SEA and Duo, logs and reports can be generated to show conformance to compliance standards.

Appendix B – Duo MFA for SEA Plus

When enabling MFA access for SEA Plus considerations need to be made for the username accessing the application, not just the device. An example policy for SEA Plus with 2FA can be found below.

To create a custom application policy for SEA Plus:

1. In the Duo administration dashboard, navigate to **Policies.**
2. Scroll down to **Custom Policies** and click **New Policy.**
3. Provide a meaningful **Policy name.**

***Note**: This design guide will provide a recommended policy set. The policy can be customized and tailored to the needs of your organization. For a full breakdown of the policies included in Duo see Duo Custom Policies.*

Example policy for SEA Plus:

1. Click **New User policy** and choose **Require enrollment**.
2. Click **Authentication Policy** and choose **Enforce 2FA**.
3. Click **User location** and choose the countries in which remote access should be enabled (choose **No action** from the dropdown for the selected countries). For **All other countries**, choose **Deny Access**.
4. Click **Device Health Application**. Under **Windows** click **Require users to have the app** and at a minimum require a **firewall** and a **system password**. It is highly recommended to also **block access if an endpoint security agent is not running**. At the time of writing this guide, the following endpoint security agents are supported:
    - Bitdefender Endpoint Security
    - Cisco Secure Endpoint (recommended)
    - Crowdstrike Falcon Sensor
    - CylancePROTECT
    - McAfee Endpoint Security
    - Palo Alto Cortex XDR
    - SentinelOne
    - Sophos AV
    - Symantec Endpoint Protection
    - Trend Micro Apex One
    - VMware Carbon Black Cloud
    - Windows Defender

    ***Note**: If you are interested in using Cisco Secure Endpoint and need design guidance to deploy, see the Cisco Breach Defense Design Guide*.

5. Click **Operating Systems** and uncheck all boxes except for **Allow Windows devices**. SEA Plus is only supported on Windows, so any authentication attempts that are not Windows would be suspicious behaviour.
    - Encourage users to update If not up-to-date and when a version becomes out of date or end of life, encourage users to update immediately.
    - Block version if end-of-life.

6. Click **Anonymous networks** and **for users that request access through proxies, Tor, or VPN** choose **Deny Access**. This will ensure users cannot bypass the geo-restrictions provided previously in the policy. *Note: SEA Plus client does not work when using VPN as the SEA Plus client is a lightweight VPN client with split tunnel configuration.*

7. Click **Authentication methods** and choose **WebAuthn**, **Duo Push** and **Hardware tokens**. SMS passcodes are not recommended.
8. Click **Save Policy.**

To add the custom application policy to SEA Plus:

1. In the Duo administration dashboard, navigate to **Applications.**
2. Click on the **SEA Plus** application. *Note: If you have not changed the name, it will be called Web SDK.*
3. Click the **Apply a policy to all users** link.
4. Select the newly created SEA Plus policy from the dropdown menu.
5. Click **Apply Policy.**
6. Scroll down the bottom of the page and click **Save.**

The additional steps beyond policy creation are to create the users who will have access to SEA Plus. When users in SEA click the toggle button for SEA Plus access with a Duo integration enabled, the email address of the user will be sent to Duo during the authentication request. For 2FA to be enabled, this email address must exist in the Duo database.

1. In the Duo administration dashboard, navigate to **Users.**
2. Click **Add User**.
3. Enter the email address of the SEA Plus access user and click **Add User**.
4. Enter the same email address into the **Email** field of the newly created user page.
5. Click **Save Changes**.
6. Click the **Send Enrollment Email** button to pre-emptively enroll a user in Duo. *Note: A user will be met with an enrollment prompt the first time they click SEA Plus with SEA Plus if they have not yet enrolled.*
7. **Repeat for all users in SEA who require SEA Plus access**.

Appendix C – Acronyms

The table below details the acronyms that were used throughout the design guide.

Table 6 Acronyms

BES	Bulk Electric Systems
BYOD	Bring Your Own Device
CVD	Cisco Validated Design
DBIR	Data Breach Investigations Report
EDM	Edge Device Manager
EMM	Enterprise Mobility Management
ESP	Electronic Security Perimeter
ESZ	Electronic Security Zone
HMI	Human Machine Interface
HTTP(S)	Hypertext Transfer Protocol (Secure)
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zone
IdP	Identity Provider
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
IoT	Internet of Things
IR	Industrial Router
ISA	International Society of Automation
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NDR	Network Detection and Response
NERC-CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OD	Operations Dashboard
OT	Operational Technology
PLC	Programmable Logic Controller
RDP	Remote Desktop Protocol
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SEA	Secure Equipment Access
SD	Security Directive
SGT	Security Group Tag
SP	Service Provider
SSH	Secure Service Shell

SSO	Single Sign-On
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSA	Transport Security Administration
UDP	User Datagram Protocol
VNC	Virtual Network Computing
VPN	Virtual Private Network
WCCP	Web Cache Communication Protocol
ZTNA	Zero Trust Network Access