CISCO
SECURE

Data sheet
Cisco public

Cisco Secure Equipment Access

February 2024

Contents

Cisco® Secure Equipment Access empowers operations teams to easily connect to remote Operational Technology (OT) assets for configuration, maintenance, and troubleshooting. It is a hybrid-cloud service that runs in Cisco industrial network equipment to enable a Zero-Trust Network Access (ZTNA) architecture in operational environments, such as manufacturing, public transportation, roadways infrastructure, renewable energy production sites, oil and gas, water utilities, EV chargers, and more.

Product overview

Remote access is key for operations teams, maintenance contractors, and machine builders to manage and troubleshoot OT assets without time-consuming and costly site visits. Zero-Trust Network Access (ZTNA) solutions are gaining increased momentum as an alternative to unmanaged cellular gateways or always-on VPNs to help organizations to deploy secure remote access and reduce cyber risks.

With Secure Equipment Access (SEA), Cisco is bringing all the benefits of ZTNA to operational spaces. Remote users connect to a cloud portal where they are authenticated and offered access only to the devices you choose, using only the protocols you specify, and only on the day and time you allow. It starts with a default deny posture and adaptively offers the appropriate trust required at the time. Assets are hidden from discovery, and lateral movement is made impossible.

The Cisco SEA portal acts as a ZTNA trust broker, enforcing policies based on identity and context and working in conjunction with the SEA app running in Cisco industrial switches and routers, turning your industrial network equipment into ZTNA gateways responsible for establishing communication with the OT asset.

Embedding the ZTNA gateway function into Cisco industrial switches and routers makes it easy to gain remote access to all assets, even those sitting behind Network Address Translation (NAT) boundaries, and simplifies deployment at scale. There is no dedicated hardware to source, install, and manage. No complex industrial DMZ (iDMZ) firewall rules to configure. Enabling remote access is just a software feature to activate in your Cisco industrial network equipment.

Features and benefits

Table 1. Features and benefits

Feature	Benefit
Remote access designed for OT workflows	• Enable machine builders, Industrial Control System (ICS) vendors, maintenance contractors, and the operations teams themselves to access remote operational assets for configuration, maintenance, or troubleshooting. • Empower operations administrators to easily create credentials for vendor connectivity and avoid delays that could impact operational agility or production uptime.
Least-privilege access control	• Never grant access to the entire network to anyone. Remote access is denied by default. Administrators must define policies based on identities and contexts: – **Identities:** Verify user and device identities at every access attempt to help ensure that access is granted only to users you trust, from devices that comply with your policies, and only to assets they need. – **Schedules:** Prevent remote users from connecting at any time. Grant access only at time of need and for a specified period by configuring day and time schedules for each asset and each user. – **Access methods:** Deny remote operators the ability to use any protocols other than the ones you selected (Secure Shell [SSH], Remote Desktop Protocol [RDP], Virtual Network Computing [VNC], HTTP(S), Telnet, or any UDP, TCP or ICMP-based application). • Make policies easy to manage at scale by creating access groups that combine user identities, remote assets, schedules, and access methods.
Secure authentication	• Address the risk of stolen credentials by enforcing Multifactor Authentication (MFA). • Streamline the user experience and enforce strict user policies from a centralized location by using your Identity Provider (IDP) to enable Single Sign-On (SSO) with Security Assertion Markup Language (SAML) 2.0 integration.

Feature	Benefit
Device posture check	· Assess the remote user's security posture with Cisco Duo when a remote user requires full IP access to an asset. · Grant access only to remote computers that comply with your security policies, such as having an up-to-date operating system or malware protection software installed and enabled.
Full control over remote access sessions	· Session monitoring: Have a list of all active remote access sessions and the ability to join a session to view what a remote user is doing in real time, for control or training purposes. · Session termination: Give administrators the ability to terminate an active session that should never have become active in the first place or in which the remote user deviates from permitted actions. · Session recording: Turn inline session recording on and store sessions for use in an audit trail. When needed, go back in time and watch what remote users did to a system to aid incident investigation.
Remote access dashboard	· Easily monitor your remote access infrastructure in a single view highlighting key data points such as number of sessions, session types, data usage, asset health, and more.
Guided configuration	· Flow-based user interface helps first-time users or non-IT personnel easily configure remote access and achieve their goals. Advanced users also have access to advanced menus.
Cloud-based ZTNA broker	· Get secure remote access up and running quickly across all your sites. There are no complex servers to install, configure, and maintain. Cisco SEA is a Software-as-a-Service (SaaS) solution that can reach all connected assets throughout your distributed infrastructure and will grow with your needs. · Reduce the attack surface. The point of entry to your network is a moving target for hackers. · Empower operations administrators to easily configure remote access using a single portal for all sites.
ZTNA gateway built into Cisco industrial switches and routers	· Make it simple to deploy secure remote access at scale. Cisco SEA removes the need for sourcing, installing, and managing dedicated ZTNA gateway hardware on every site. · Reach more assets, even those sitting behind NAT boundaries. A switch or router in the same subnet now also provides zero-trust remote access to these assets, whatever your NAT strategy. · Enforce complete isolation. The same switch or router can also enforce microsegmentation policies to prevent lateral movements if the asset is used as a jump host. · Reduce the attack surface. You don't need to expose your IP addresses to jump servers in the iDMZ. · Stop struggling with complex firewall and iDMZ setups. The Cisco ZTNA gateway establishes an outbound connection to the Cisco ZTNA trust broker to create a secure and controlled communication path to all OT assets you want to provide remote access to.
Clientless and agent-based ZTNA	· Clientless: Users just need a web browser to access remote OT assets using RDP, VNC, HTTP(S), SSH, or Telnet. · Agent-based (SEA Plus): Cisco SEA establishes a secure IP communication channel between the user's computer and the OT asset, so any desktop application can be used for advanced tasks, such as file transfer or Programmable Logic Controller (PLC) programming using native applications.
Role-Based Access Control (RBAC)	· Easily delegate remote access management without compromising security. Administrators can use RBAC to restrict what users can configure when creating remote access policies. · Create custom user roles for your specific needs or choose between the three predefined roles.
Audit and compliance information	· Meet compliance requirements and help run investigations with audit logs for both system-generated and user-generated events, such as who added new users or new assets to the systems and how remote users authenticate, with usernames, time, device posture, and access logs. · Detailed session logs are available via the user interface or can be exported as CSV files to populate your reports or meet your compliance processes.
Programmability for process automation	· The Cisco SEA APIs are available in a Swagger user interface to simplify development of custom automations for customers and partners willing to implement a programmatic approach to secure remote access.

Platform support

Cisco Secure Equipment Access is built on a unique architecture consisting of multiple ZTNA gateways running in your Cisco industrial switches or routers to establish a secure and controlled communication path between the cloud-based ZTNA broker and the remote OT asset. The SEA ZTNA broker supports an unlimited number of ZTNA gateways.

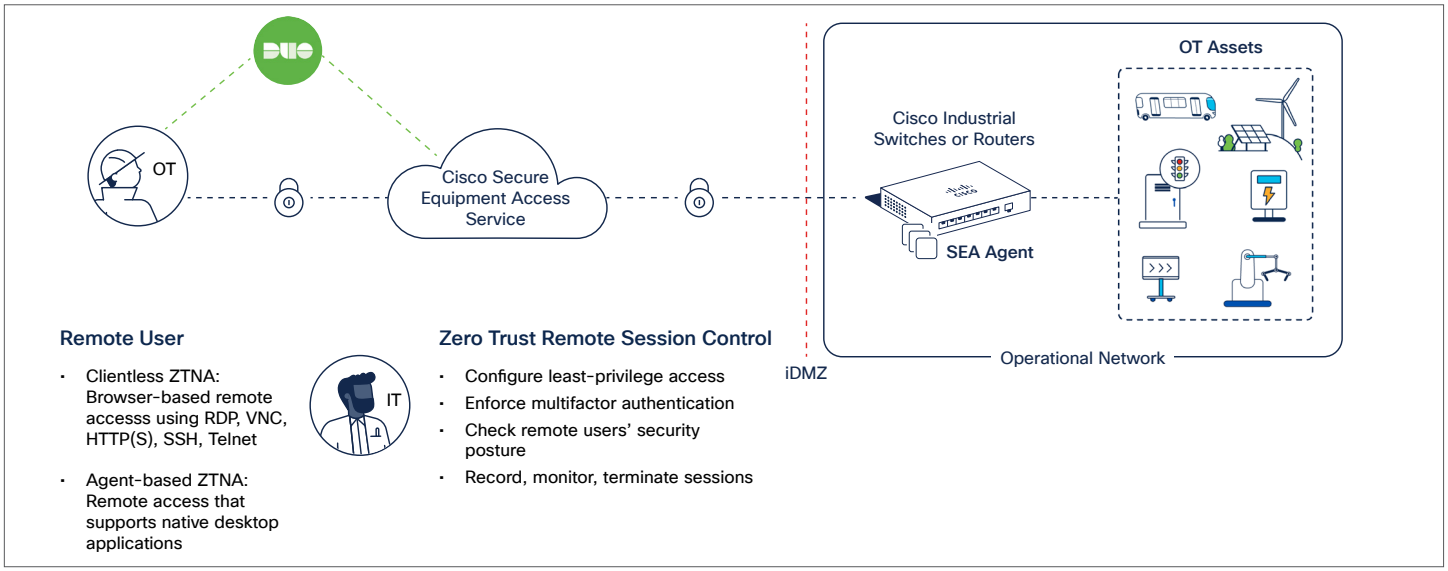

Figure 1. Cisco Secure Equipment Access's ZTNA architecture

The ZTNA gateway function is enabled by the Cisco SEA agent, a Cisco IOx app running in a dedicated CPU core in the network equipment without impact on routing or switching performance or other features. The Cisco SEA agent is supported on the platforms listed in the table below.

Table 2. Platforms hosting the Cisco SEA agent

Product type	Platforms supported
Industrial switches	Cisco Catalyst® IE3300 Rugged Series switches (models with 4 GB RAM only) Cisco Catalyst IE3400 Rugged Series switches Cisco Catalyst IE3400 Heavy Duty Series switches Cisco Catalyst IE3100 Rugged Series switches
Industrial routers	Cisco Catalyst IR1100 Rugged Series routers Cisco Catalyst IR1800 Rugged Series routers

Cisco SEA ZTNA gateway hardware specifications

Please refer to the associated data sheets for hardware specifications:

- Cisco Catalyst IE3300 Rugged Series switches
- Cisco Catalyst IE3400 Rugged Series switches
- Cisco Catalyst IE3400 Heavy Duty Series switches
- Cisco Catalyst IE3100 Rugged Series switches
- Cisco Catalyst IR1100 Rugged Series routers
- Cisco Catalyst IR1800 Rugged Series routers

Table 3. Cisco SEA platform specifications

Platforms	Maximum number of concurrent remote access sessions	Minimum version of Cisco IOS	Recommended version of Cisco IOS
Cisco Catalyst IE3300 Rugged Series switches	10	17.12.01	17.13.01
Cisco Catalyst IE3400 Rugged Series switches	10	17.12.01	17.13.01
Cisco Catalyst IE3400 Heavy Duty Series switches	10	17.12.01	17.13.01
Cisco Catalyst IE3100 Rugged Series switches	5	17.12.01	17.13.01
Cisco Catalyst IR1100 Rugged Series routers	10	17.04.01	17.13.01a
Cisco Catalyst IR1800 Rugged Series routers	10	17.11.01	17.13.01a

Note: Provided a maximum number of concurrent sessions applicable for cases when the SEA Agent is the only installed application on the device. Available uplink bandwidth should be considered carefully when using multiple concurrent SEA sessions.

Licensing

Cisco Secure Equipment Access is licensed using a recurring subscription model based on the number of OT assets or endpoints that can be accessed and is available in 1-, 3-, 5-, and 7-year terms. Each SEA license comes with 1Gbps/month/endpoint to access remote assets. Licenses and traffic allowance within an organization are considered as a pool in the cloud. Such a pool can be used through any distribution model across all target sites and OT assets. Licensing is available in two tiers–Essentials and Advantage–that provide different levels of capabilities to meet your particular requirements. The product uses Cisco Smart Licensing. The SEA license includes the SEA cloud portal and an unlimited number of SEA agents to enable deployment of an unlimited number of ZTNA gateways.

Table 4. Licensing tiers

Licensing tier	
Essentials	**Advantage**
• All access methods: – Clientless ZTNA (RDP, VNC, HTTP/S, SSH, Telnet) – Agent-based ZTNA (SEA Plus) • Just-in-time access (scheduled access) • Access control groups • Platform-level security controls (SSO, MFA, RBAC)	Includes Essentials features, plus: • Active sessions monitoring • Session supervision (session join) • Session termination • Inline session recording (AWS S3 account required for storage) • Host security posture check via Cisco Duo for additional security when using the SEA Plus access method (Duo account required)

Secure Equipment Access licenses come with Basic software support. More details on all available software support levels can be found here.

Ordering information

Cisco Secure Equipment Access is available to order today. Please visit the Cisco Ordering homepage for more information.

Table 5. Cisco SEA product IDs

Product ID	Product description
SEA-LICENSE	ATO Product ID
SEA-E	Cisco Secure Equipment Access **Essentials** License for OT Asset
SEA-A	Cisco Secure Equipment Access **Advantage** License for OT Asset

Warranty

Please refer to the respective data sheets for the hardware platforms running the Cisco SEA agent for warranty information.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environmental Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environmental Sustainability" section of the CSR Report) are provided in the following table.

Table 6. Links to specific environmental sustainability topics

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco and partner services

Services for planning, deploying, and support

Services provided by Cisco and our certified partners are available to help you through the design, deployment, and operational phases of your Cisco SEA project. Whether you need some expert advice, support throughout the entire project, or something in between, we, together with our partners, have the experts and expertise to help you be successful. For more information, visit https://www.cisco.com/go/services.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation, and stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

Document history

New or revised topic	Described in	Date
Document creation		October 16, 2023
New features and support for new platforms	Table 1, 2, and 3	January 2024