ABB Ability™ Secure Remote Access designed for OT/ICS

Purpose-built to protect and streamline OT system remote maintenance, ABB Ability™ Secure Remote Access (ABB Ability™ SRA) delivers good engineering experience, efficient tooling, easy access control, end to end security, and real-time auditing to ensure safe and efficient remote service management.

As digital transformation accelerates automation, and Industry 4.0 technologies are driving significant improvements in operational efficiency for industrial organizations.

Yet, traditional remote access tools often fall short in delivering the robust control, visibility, and security required to safeguard critical industrial operations.

A secure remote access needs to facilitate encrypted end-to-end communication, allowing engineers, technicians, and operators to monitor, diagnose, and manage OT and industrial control systems (ICS) with ease while providing full control for asset owners.

Key Challenges

Over-Permissioned Access

Organizations that operate OT environments face real and persistent obstacles when it comes to securing critical systems against unauthorized access.

Inadequacy of IT-centric Solution

There is a fundamental mismatches with system design, priority, and protocol requirements of OT and IT-centric remote access solution.

Cumbersome Login Procedure

Consistent administration policies are needed to manage multiple remote access with separate credentials for each network and/or device, creating a burden for end-users, IT, and security teams.

Vulnerabilities within Legacy Systems

Non-connected legacy devices lack automatic updates and real-time monitoring, making them vulnerable to security risks like tampering and overlooked vulnerabilities.

Enhance Security, Simplify Access, and Optimize Operations

SECURITY

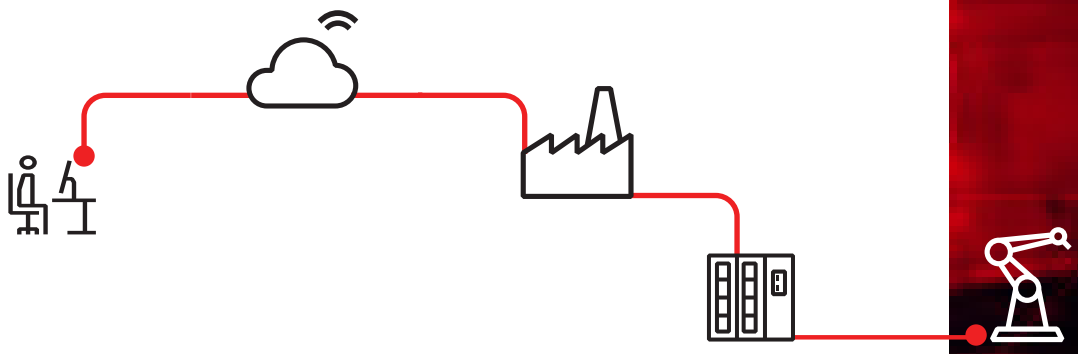
- End-to-end encrypted remote connection, safeguarding data from unauthorized access while providing secure and seamless connectivity for industrial operations.
- Facilitate robust network segmentation by securely connecting OT devices with ICS software repositories, ensuring safe and regular updates.
- Enabling target devices to seamlessly authenticate users and ensure only authorized access to OT device and ICS environment.

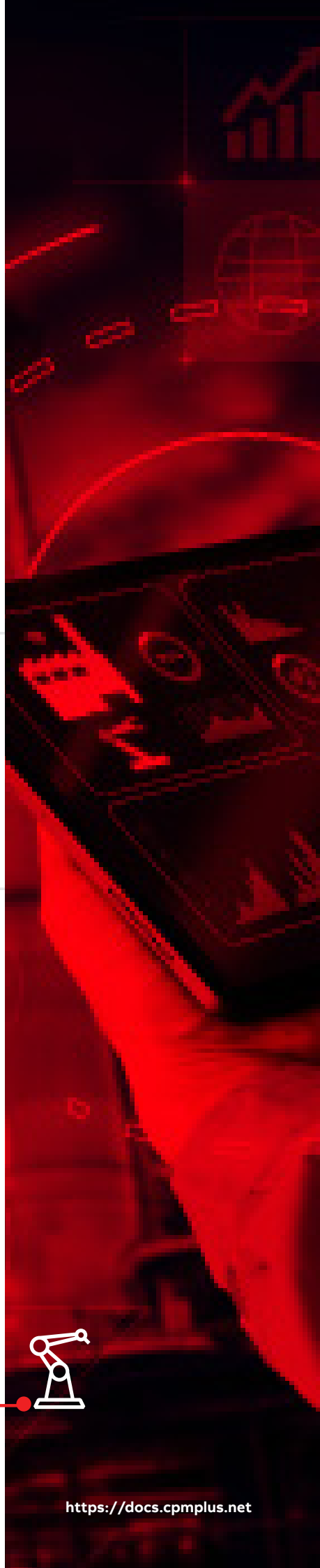
CONTROL

- Effortlessly bypass firewalls and proxies with secure connectivity, requiring only outbound HTTPS (443) on client and target systems.
- Empower asset owners with full control through a comprehensive dashboard, enabling them to manage remote access, set schedules, and enhance security effortlessly.
- Maintain OT devices and ICS audit logs to track user actions and optionally report them to a central SIEM (Security Information and Event Monitoring) system.

EFFICIENCY

- Efficient access control with SSO via OAuth2, allowing users to authenticate seamlessly across multiple targets without the complexity of managing separate accounts or passwords.
- Equip users with full-featured, native tools designed for optimal performance, allowing user to experience the power of robust, high-performance applications built for efficiency and reliability.
- The user-friendly interface enhances navigation to the target resource,allowing users to complete tasks more efficiently.





Designed to meet the unique requirements of complex operational technology (OT) and industrial control systems (ICS) environments ABB Ability™ Secure Remote Access (ABB Ability™ SRA) unlock seamless and secure remote access.

KEY FEATURES: -

Effortless Firewall & Proxy Bypass – Requires only outbound HTTPS (443) on clients and targets, ensuring smooth access through secure gateways.

Single Sign-On (SSO) – OAuth2-based authentication eliminates the need for managing separate accounts and passwords for every target.

Native Tooling Support – Utilize fully-featured native applications instead of limited browser-based versions, with support for custom applications.

Multi-Hop Connectivity – Access target devices securely, even without direct internet access, by routing through multiple intermediate nodes.

True End-to-End Encryption – Prevents eavesdropping or tampering, ensuring uncompromised security, even if gateways or intermediate nodes are compromised.

Smart Network Redirection – Redirect access to other devices within the same network while maintaining encryption integrity.

Patented Tunneled OAuth2 Authentication – Both gateway and target nodes authenticate users, even without internet access, ensuring secure verification at every step.

1/3 reported being victims of a ransomware attack

54% of cyber attack impacted discrete or process industries

75% of cyber threats pose a direct risk to operational safety

73% allow third parties to access the OT environment