CLAROTY

Data Sheet

CLAROTY SECURE REMOTE ACCESS (SRA)

Simple, Highly Secure Remote Access for OT Environments

The OT Remote Access Challenge

Remote access to OT (operational technology) environments requires balancing the needs of IT security and plant operations. From the IT security perspective, the concern is that OT remote access is high-risk: The use of privileged accounts accessing mission-critical assets from a remote location is an obviously dangerous attack vector.

On the plant operations side, the challenge is that OT staff have unique remote-access needs when compared to typical enterprise requirements. OT staff focus on keeping the plant operational and must make most remote-access decisions, including in emergency situations. However, they tend to lack IT security expertise and therefore require a solution that is operationally simple and tailored to OT workflows.

Key Features & Capabilities

- Purpose-built solution for remote OT administrative access
- Architecture supports highly available access to globally distributed facilities
- Simple, OT-centric console for managing access for administrators and 3rd-party support staff
- Supports all key OT remote access use cases
- Built-in workflows for access approvals and emergency access
- Local audit trail allows rapid troubleshooting

IT Security	Plant Operations
• OT risk management	• Locally allow 3rd party access
• Control priviledged acces	• Simple to operate
• Detect anomalous activity	• Approval and emergency workflows

IT Security & Plant Operations have competing remote access requirements

The OT remote access challenge is exacerbated when plants are distributed and geographically isolated, with limited wide-area network bandwidth. Unfortunately, most enterprise-class remote access solutions are too complex and centralized to support OT remote access.

Claroty SRA - Purpose-Built for OT Remote Access

The Claroty Secure Remote Access (SRA) solution is purpose-built for OT remote access. Available as either physical or virtual appliances, SRA has the following key capabilities:

- **Simplicity:** Unlike enterprise remote access solutions, SRA is designed to be easy for plant staff to configure and operate.
- **Distributed:** SRA supports widely distributed plants and facilities, with both local and centralized administration.
- **OT Aware:** SRA is a tailored solution for OT use cases and workflows.

Simplified Administrative Interface

Secure Remote Access | **OT-Centric Workflows** | **Monitoring & Auditing**

Distributed Architecture

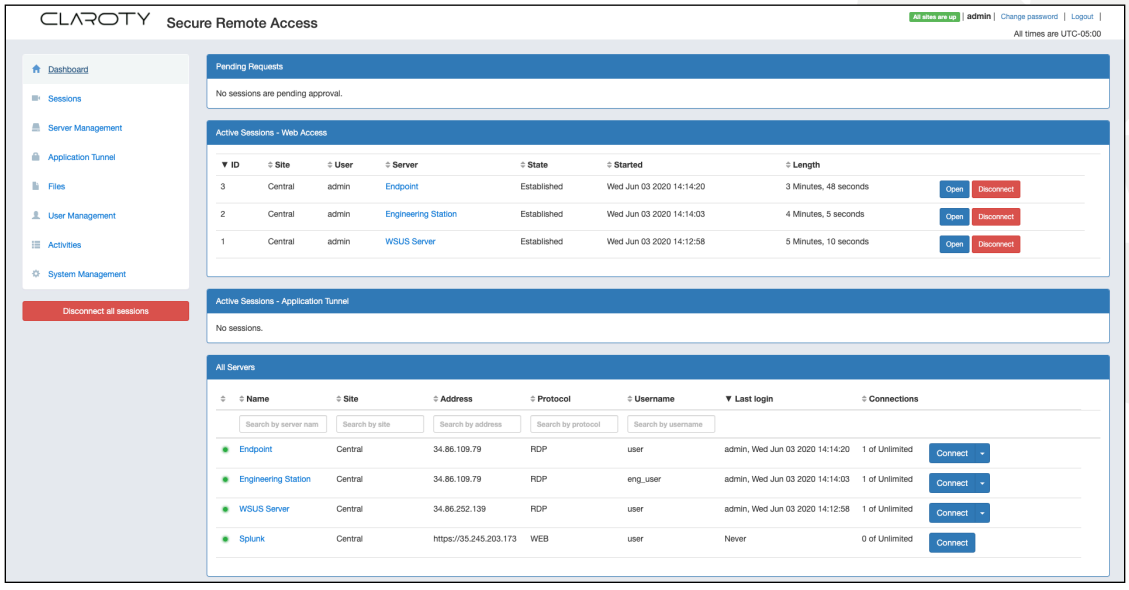
Claroty SRA supports all three use cases typically required for remote or third-party staff to support OT systems:

- **Web:** User accesses OT systems using standard web browser.
- **OT Application:** OT systems accessed using proprietary application on remote client device.
- **File transfer:** Movement of sensitive configuration or documentation files onto PLCs or other OT devices.

SRA leverages a single, highly secure encrypted tunnel for intra-facility communication. This greatly simplifies network firewall configurations, and is consistent with segmentation best practices, for example as required in the Purdue Model.

Simple, OT-Centric Workflows

SRA is designed to be used by on-site OT staff, who are best positioned to authorize remote access to their facilities. The interface is tailored to the needs of OT remote access, lowering training requirements and the likelihood of configuration errors. Its simple user interface supports fast onboarding for remote users (internal or third-party) and the OT systems they need to support.



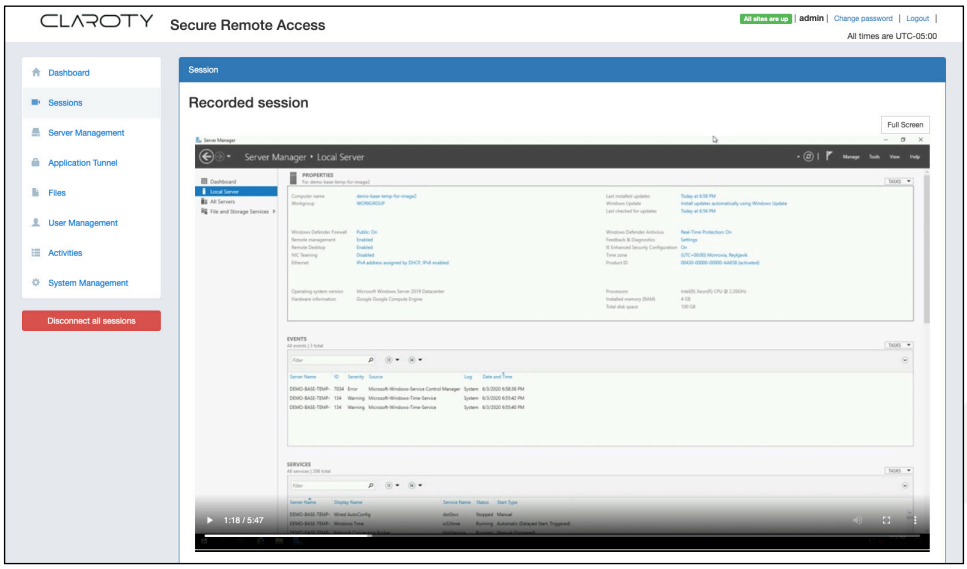
Claroty SRA Dashboard

Comprehensive Monitoring & Auditing

Because OT remote access is so sensitive, it is mandatory to have a strong audit trail of all such activity. SRA provides a complete recording of actions taken over remote access connection. Such monitoring can either be accessed in real time ("over the shoulder") or after the fact. Crucially, the audit trail can be kept locally, where it can be used without delay on-site by the people who need it. This can eliminate issues related to exporting employee activity monitoring beyond national boundaries.

Comprehensive Monitoring & Auditing

SRA complements Claroty's Continuous Threat Detection (CTD) offering to deliver a complete OT security solution. The combined platform delivers the industry's broadest set of OT security controls, including asset discovery and visibility, vulnerability management, threat detection, and segmentation policy. With the Claroty Platform, OT and IT staff can manage risk in their OT environments with minimal training and no disruption to infrastructure and security workflows.



SRA recorded session view gives a full view of all actions taken during a remote session

About Claroty

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

CLAROTY

CONTACT US

contact@claroty.com