Secure Remote Access w/Audit

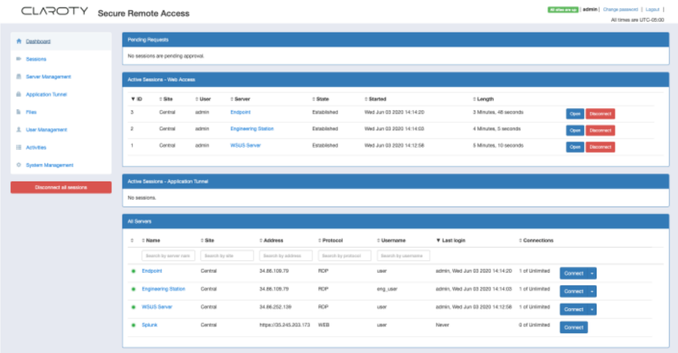
The Industrial Remote Access Challenge

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. Traditional enterprise remote access tools do not address these challenges.

Remote Access Built For the Industrial Environment

Here are some of the key features and 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



All times are UTC-05:00

Pending Requests

No sessions are pending approval.

Active Sessions - Web Access

▼ ID	⇕ Site	⇕ User	⇕ Server	⇕ State	⇕ Started	⇕ Length	
3	Central	admin	Endpoint	Established	Wed Jun 03 2020 14:14:20	3 Minutes, 48 seconds	Open Disconnect
2	Central	admin	Engineering Station	Established	Wed Jun 03 2020 14:14:03	4 Minutes, 5 seconds	Open Disconnect
1	Central	admin	WSUS Server	Established	Wed Jun 03 2020 14:12:58	5 Minutes, 10 seconds	Open Disconnect

Active Sessions - Application Tunnel

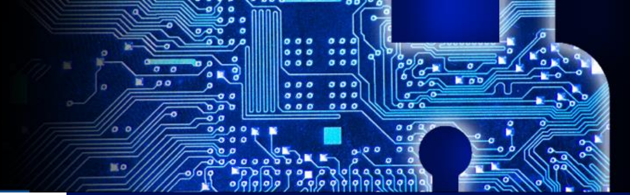
No sessions.

All Servers

⇕	⇕ Name	⇕ Site	⇕ Address	⇕ Protocol	⇕ Username	▼ Last login	⇕ Connections	
	Search by server nam	Search by site	Search by address	Search by protocol	Search by username			
●	Endpoint	Central	34.86.109.79	RDP	user	admin, Wed Jun 03 2020 14:14:20	1 of Unlimited	Connect ▾
●	Engineering Station	Central	34.86.109.79	RDP	eng_user	admin, Wed Jun 03 2020 14:14:03	1 of Unlimited	Connect ▾
●	WSUS Server	Central	34.86.252.139	RDP	user	admin, Wed Jun 03 2020 14:12:58	1 of Unlimited	Connect ▾
●	Splunk	Central	https://35.245.203.173	WEB	user	Never	0 of Unlimited	Connect

Secure Remote Access is designed to minimize the risk remote users, including employees and contractors introduce to industrial networks. The system provides a single, managed interface through which all remote users connect and authenticate prior to performing software upgrades, periodic maintenance and other system support activities.

It's complicated…but we've figured it out



Platform Highlights:

Proactive Access Control – Through granular user and asset policies governing which assets authorized users can see and access, when they can log into each asset and the authentication-level required for access.

Password Vaulting – Securely store user and asset credentials. Eliminate shared passwords schemes, easily manage password changes and avoid risks from valid passwords of non-active users.

Workflow Controls and Real-Time Monitoring – Using manual access requests and permission controls.

"Over-the-Shoulder" - Real-time video visibility into all remote user activity by operator or administrator.

Red Button - Ability to terminate ongoing sessions as they are happening in real-time.

Activity Reports – Filtered by user, asset or session and providing video recordings of all remote sessions.

Platform Benefits:

Monitor - SRA enables system administrators continuously monitor and audit privileged users, sessions, and assets, including which ICS devices are being accessed, by which user, and the total number of users who have access to each asset.

Secure - If a contradiction between the stated remote access purpose and the actual activity occurs, system administrators can immediately terminate the remote session, preventing network disruption, and improving overall cyber resiliency.

Audit - Following the remote session, system administrators and auditors can playback a full video recording of each session, as well correlate specific reports filtered by user, asset or session to facilitate retrospective auditing.

About Velta Technology

- Over 100 years of combined OT/ IT Industrial, Enterprise & C-suite experience
- Laser-focused on the industrial and manufacturing space
- Platform agnostic while having relationships with world-class partners across technologies & environments
- Proprietary Velta Technology Standards, Platforms & Methodologies
- Specialized Digital Safety / Cybersecurity Training program
- First to the market with Digital Safety as a Service
- Unique capabilities to put all the pieces together for a solution of value
- Qualified to exist on the production floor and in cyberspace - safely