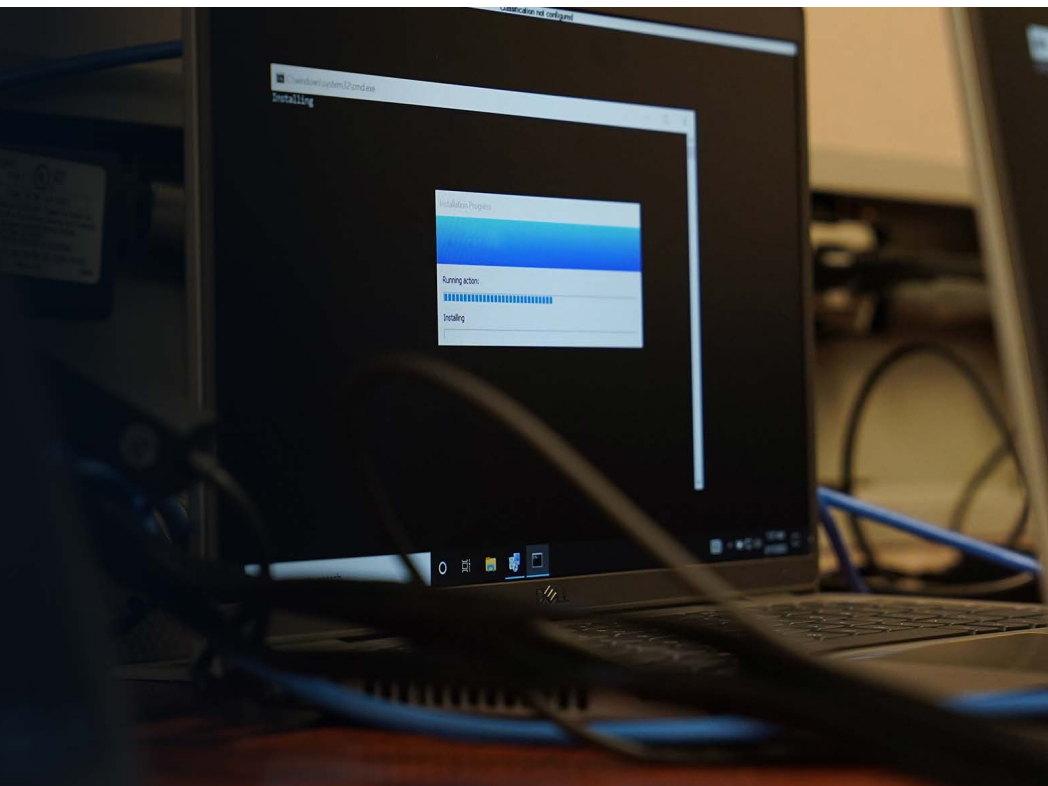


Archon Manager

CSfC over-the-air enterprise management



For more information about Archon Gateway and the Archon Suite of secure network computing solutions, visit caci.com/archon

Personnel working in remote field locations on critical missions may find it difficult to return to depot, which makes it challenging when updates or certificate renewals need to be pushed to their devices.

Additionally, devices used in disconnected, denied, intermittent, or limited bandwidth (DDIL) environments present additional security risk should they be lost with the potential of information falling into the wrong hands.

Archon Manager makes it easy to update or patch end-user devices and Archon SideArm, the internal retransmission device. It simplifies certificate management, renewals, or revocation, anytime, anywhere. Plus, it allows lost devices to be wiped remotely.



CACI

The Archon Manager difference

AUTOMATED UPDATES

Automate required renewal dates to stay compliant and relieve administrative burden.

INSTANT DEVICE PROTECTION

Immediately wipe compromised laptops if lost.

REAL-TIME SECURITY PATCH INSTALLATION

Install security patches in real time instead of having to wait for personnel to return their devices.

CONTINUAL UPDATES

Deliver uninterrupted updates to devices, even when personnel are in DDIL environments.

OVER-THE-AIR UPDATES

Updates the Archon software, certificates, and the Internal Retransmission Device over the air so clients do not need to be returned to depot.

FEATURES

- Architecture management and monitoring: When integrated with Archon Gateway and combined with Archon Director, Archon technologies provide Architecture management and monitoring for all Archon CSfC infrastructure components and endpoint devices.
- Simplified CSfC compliance: Archon Manager automates National Security Agency (NSA) rekeying requirements for end-user device certificates, wherever the Archon client is located. Assets in the field don't need to be brought back to a depot for updates, which makes it easier to stay compliant and mission ready.
- Pre-shared key automation: Archon Manager automates installation and auditing of quantum-resistant pre-shared keys on inner VPN gateways and end-user devices, reducing the risks of keys being compromised and end users' administrative burden to deploy quantum resistance. Archon Manager also automates the pre-shared key cycling required every 180 days.

Archon Manager allows end users to securely manage inventory, patches, updates, and configurations, including certificates for dual VPN tunnels, and quantum resistance pre-shared keys on the inner tunnel all through over-the-air updates.

About the Archon Suite

Empower your end-users to securely work from anywhere at any scale. From next-generation devices to hardware and data services, the Archon® Suite of CSfC capabilities make securing your edge simple, fast and efficient.