MayaUPS

SECURITY GUIDE | EN-CA

Security and Deployment Review

Architecture, access, recovery and the review points for a deployment you control

Local data	Credentials and roles	Review material
Configuration, history and audit records stay on infrastructure you control.	Encrypted SNMP profiles, SNMPv3 protection, and viewer, operator and administrator roles.	Security policy, threat model, hardening guidance, review records and a CycloneDX SBOM, ready for your reviewer.

MayaUPS is intended to operate inside a customer-managed environment, close to the UPS equipment it monitors. This guide identifies the product controls and deployment decisions that an IT or security reviewer should examine before production use.

For: IT administrators, security reviewers, infrastructure owners and service providers assessing a MayaUPS deployment.

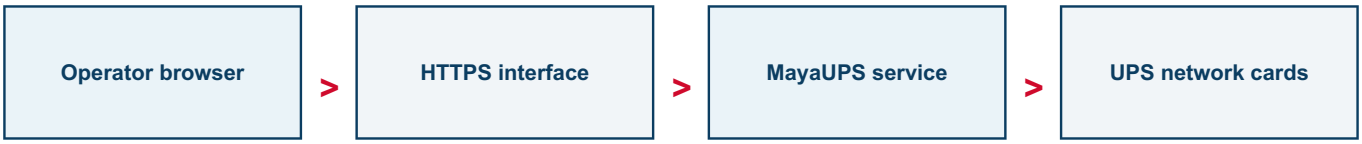
Website launch edition | July 2026 | mayaups.com

Deployment boundary

The MayaUPS service, embedded Web interface and SQLite data store run on customer-controlled Windows or Linux infrastructure. The service communicates with supported network management cards through configured SNMP profiles. Operators connect to the local Web interface according to the customer's network and access design.

A supported UPS connected directly to a host can use the optional agent. Agent communication is authenticated and can use mutual TLS when configured. Remote access, identity integration, firewall policy, certificate management and network segmentation remain customer deployment decisions.

Core trust path



Use a management network and access policy appropriate to the site's risk. Expose only the interfaces and protocols required for the approved design.

Credentials, access and accountability

Control	Product approach
SNMP profiles	Community strings and SNMPv3 credentials are stored in encrypted credential profiles rather than repeated in each device record.
SNMPv3	Authentication and privacy settings can be used with devices that support SNMPv3.
Initial administration	The first administrator establishes the deployment and should replace initial credentials as part of commissioning.
Roles	Viewer, operator and administrator roles separate routine observation, operational changes and administration.
Audit history	Configuration and operational changes are recorded to support review and troubleshooting.

Least-privilege access still depends on role assignment, account lifecycle and network controls operated by the customer.

Availability and recovery controls

Area	Built-in capability
Backup	Scheduled daily backups and rotation protect the local configuration and operating history.
Restore	Restore controls support recovery of a validated backup after a failure or rebuild.
Storage protection	A storage guard monitors available capacity so database growth can be addressed before the host is exhausted.
Service health	Health checks and watchdog behaviour help identify or recover from a stopped or unresponsive service.
Controlled stop	Graceful shutdown and logging preserve useful context when the service or host is stopped.

A backup is not proven until it can be restored. Test the backup location, retention, access and restore procedure within the customer's recovery process.

Material available for review

MayaUPS security documentation gives reviewers more than a feature list. The review material describes the product boundary, known risks and deployment responsibilities.

- Security policy and coordinated vulnerability disclosure process.
- Threat model and product security review records.
- Deployment hardening guidance for Windows, Linux, network access and credentials.
- CycloneDX software bill of materials for distributed components.
- Privacy, accessibility and conformity information for the product.

Deployment review checklist

- Place MayaUPS and UPS management cards on the approved management network and restrict unnecessary access.
- Use SNMPv3 authentication and privacy where the exact equipment supports them; document approved exceptions.
- Replace initial administrator credentials, create named accounts and assign the least role required.
- Configure and validate HTTPS certificates according to the customer's trust and renewal process.
- Protect backup locations, confirm retention and complete a restore test.
- Review email delivery, outbound network paths and any remote access against the site's security policy.
- Run a no-action shutdown test before enabling any device or host control, then repeat it after material changes.
- Review the available security records and SBOM before production approval.

Scope and responsibilities

MayaUPS provides product controls, but it does not determine the customer's network architecture, identity policy, certificate authority, remote access design, operating authority or recovery objectives. Those controls must be selected, documented and tested for the actual environment.

Compatibility and control actions also depend on the exact UPS, network card, firmware and protected host. Review the product documentation and applicable legal terms, then commission the site-specific configuration before production use.

> Base production approval on the available security records, the customer's final architecture and the results of site-specific commissioning.

Continue online

Security and compliance

Privacy

Accessibility

> This guide supports product evaluation. It is not a security certification, penetration-test report or approval of a customer's final architecture.