MayaUPS

GUIDE DE SÉCURITÉ | FR-CA

Revue de sécurité et de déploiement

Architecture, accès, reprise et points d'examen pour un déploiement que vous contrôlez

Données locales	Identifiants et rôles	Documents d'examen
La configuration, l'historique et l'audit restent dans l'infrastructure que vous contrôlez.	Profils SNMP chiffrés, protection SNMPv3 et rôles de consultation, d'exploitation et d'administration.	Politique de sécurité, modèle de menace, guide de renforcement, dossiers de revue et nomenclature CycloneDX, prêts pour votre examen.

MayaUPS est conçu pour fonctionner dans un environnement géré par le client, près des onduleurs surveillés. Ce guide présente les contrôles du produit et les décisions de déploiement qu'une équipe des technologies de l'information ou de la sécurité devrait examiner avant l'utilisation en production.

Public visé : administrateurs des technologies de l'information, responsables de la sécurité, propriétaires d'infrastructure et fournisseurs de services qui évaluent un déploiement MayaUPS.

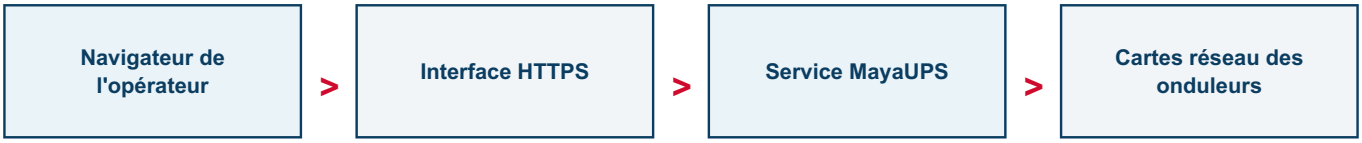
Édition de lancement du site Web | Juillet 2026 | mayaups.com

Périmètre du déploiement

Le service MayaUPS, l'interface Web intégrée et la base de données SQLite fonctionnent dans l'infrastructure Windows ou Linux contrôlée par le client. Le service communique avec les cartes de gestion réseau prises en charge au moyen de profils SNMP configurés. Les opérateurs accèdent à l'interface Web locale selon la conception du réseau et des accès du client.

Un onduleur pris en charge et relié directement à un ordinateur hôte peut utiliser l'agent facultatif. Les communications de l'agent sont authentifiées et peuvent utiliser l'authentification TLS mutuelle lorsqu'elle est configurée. L'accès à distance, l'intégration des identités, les règles de pare-feu, les certificats et la segmentation du réseau demeurent des décisions du client.

Chaîne de confiance principale



Utilisez un réseau de gestion et une politique d'accès adaptés au risque du site. Rendez accessibles uniquement les interfaces et les protocoles nécessaires à la conception approuvée.

Identifiants, accès et traçabilité

Contrôle	Approche du produit
Profils SNMP	Les communautés et les identifiants SNMPv3 sont conservés dans des profils chiffrés plutôt que répétés dans chaque dossier d'appareil.
SNMPv3	L'authentification et le chiffrement peuvent être utilisés avec les appareils qui prennent en charge SNMPv3.
Administration initiale	Le premier administrateur établit le déploiement et doit remplacer les identifiants initiaux pendant la mise en service.
Rôles	Les rôles de consultation, d'exploitation et d'administration séparent l'observation courante, les changements d'exploitation et l'administration.
Historique d'audit	Les changements de configuration et d'exploitation sont consignés pour faciliter l'examen et le diagnostic.

Le principe du moindre privilège dépend aussi de l'attribution des rôles, du cycle de vie des comptes et des contrôles réseau administrés par le client.

Disponibilité et reprise

Domaine	Fonction intégrée
Sauvegarde	Des sauvegardes quotidiennes planifiées et leur rotation protègent la configuration locale et l'historique d'exploitation.
Restauration	Les fonctions de restauration permettent de récupérer une sauvegarde validée après une défaillance ou une reconstruction.
Protection du stockage	Un contrôle surveille l'espace disponible afin que la croissance de la base puisse être traitée avant de saturer l'hôte.
État du service	Les contrôles d'état et la surveillance du service facilitent la détection ou le rétablissement d'un service arrêté ou sans réponse.
Arrêt contrôlé	L'arrêt ordonné et la journalisation conservent le contexte utile lorsque le service ou l'hôte est arrêté.

Une sauvegarde n'est confirmée qu'après une restauration réussie. Vérifiez l'emplacement, la conservation, les accès et la procédure de restauration dans le processus de reprise du client.

Documents pour l'examen

La documentation de sécurité MayaUPS donne aux responsables de l'examen plus qu'une liste de fonctions. Elle décrit le périmètre du produit, les risques connus et les responsabilités de déploiement.

- Politique de sécurité et processus coordonné de divulgation des vulnérabilités.
- Modèle de menace et dossiers de revue de sécurité du produit.
- Guide de renforcement pour Windows, Linux, les accès réseau et les identifiants.
- Nomenclature logicielle CycloneDX des composants distribués.
- Documentation sur la protection des renseignements personnels, l'accessibilité et la conformité.

Liste de vérification du déploiement

- Placer MayaUPS et les cartes de gestion des onduleurs dans le réseau de gestion approuvé et limiter les accès inutiles.
- Utiliser l'authentification et le chiffrement SNMPv3 lorsque l'appareil exact les prend en charge, et documenter les exceptions approuvées.
- Remplacer les identifiants initiaux, créer des comptes nominatifs et attribuer le rôle minimal requis.
- Configurer et valider les certificats HTTPS selon le processus de confiance et de renouvellement du client.
- Protéger les emplacements de sauvegarde, confirmer la conservation et effectuer un essai de restauration.
- Examiner la livraison des courriels, les communications sortantes et tout accès à distance selon la politique de sécurité du site.
- Effectuer un essai d'arrêt sans action avant d'autoriser une commande, puis le répéter après une modification importante.
- Examiner les dossiers de sécurité et la nomenclature logicielle avant l'approbation de production.

Portée et responsabilités

MayaUPS fournit des contrôles de produit, mais ne détermine pas l'architecture réseau, la politique d'identité, l'autorité de certification, l'accès à distance, l'autorité d'exploitation ni les objectifs de reprise du client. Ces contrôles doivent être choisis, documentés et vérifiés dans l'environnement réel.

La compatibilité et les commandes dépendent également de l'onduleur, de la carte réseau, du micrologiciel et de l'ordinateur hôte protégé. Examinez la documentation du produit et les modalités juridiques applicables, puis mettez en service la configuration propre au site.

Fondez l'approbation de production sur les dossiers de sécurité disponibles, l'architecture finale du client et les résultats de la mise en service propre au site.

Poursuivre en ligne

Sécurité et conformité

Protection des renseignements personnels

Accessibilité

Ce guide facilite l'évaluation du produit. Il ne constitue pas une certification de sécurité, un rapport d'essai d'intrusion ni une approbation de l'architecture finale du client.