Unité de distribution électrique en rack Vertiv™ PowerIT

Guide d’installation et d’utilisation

Série M et série D évolutives et non évolutives
(équipées du firmware 6.3.x)

Les informations contenues dans ce document sont susceptibles d’être modifiées sans préavis et peuvent ne pas convenir à toutes les applications. Bien que toutes les précautions aient été prises pour garantir l’exactitude et l’exhaustivité de ce document, Vertiv n’assume aucune responsabilité et décline toute responsabilité pour les dommages résultant de l’utilisation de ces informations ou pour toute erreur ou omission.

Reportez-vous aux réglementations locales et aux codes du bâtiment relatifs à l’application, à l’installation et au fonctionnement de ce produit. L’ingénieur-conseil, l’installateur et/ou l’utilisateur final est responsable du respect de toutes les lois et réglementations applicables relatives à l’application, à l’installation et au fonctionnement de ce produit.

Les produits couverts par ce manuel d’instructions sont fabriqués et/ou vendus par Vertiv. Ce document est la propriété de Vertiv et contient des informations confidentielles et exclusives appartenant à Vertiv. Toute copie, utilisation ou divulgation sans l’autorisation écrite de Vertiv est strictement interdite.

Les noms des sociétés et des produits sont des marques de commerce ou des marques déposées des sociétés respectives. Toute question concernant l’utilisation des noms de marque de commerce doit être adressée au fabricant d’origine.

Site de l’assistance technique

En cas de problème lors de l’installation ou de l’utilisation de votre produit, consultez la section pertinente de ce manuel et essayez de résoudre le problème en suivant les procédures décrites.

Rendez-vous sur le site https://www.vertiv.com/en-us/support/ pour obtenir une assistance supplémentaire.

TABLE DES MATIÈRES

Page laissée vierge intentionnellement

1 Consignes de sécurité importantes

Conformité réglementaire

Les produits Vertiv sont réglementés en matière de sécurité, d'émissions et d'impact environnemental par les agences et politiques suivantes.

Underwriters Laboratories (UL)

Les normes UL permettent d'évaluer les produits, de tester les composants, les matériaux, les systèmes et les performances, et d'évaluer les produits écologiquement durables, les énergies renouvelables, les produits alimentaires et à base d'eau, les systèmes de recyclage et d'autres technologies novatrices.

Les normes UL spécifiques à cet équipement sont indiquées sur la plaque signalétique du dispositif.

CE

Le marquage CE d'un produit signifie que le produit est conforme aux exigences européennes (UE) applicables en matière de santé, de sécurité et de protection de l'environnement, notamment la législation et les directives de l'UE relatives aux produits. La marque CE est requise pour les produits proposés à la vente dans l'Espace économique européen (EEE).

Les réglementations, directives et normes spécifiques applicables à chaque produit sont spécifiées dans la déclaration de conformité.

FCC (Federal Communications Commission)

La FCC (Federal Communications Commission) réglemente les communications internationales et entre les États par radio, télévision, satellite, câble et filaires dans les 50 États, le district de Columbia et les territoires américains. Agence gouvernementale américaine indépendante supervisée par le Congrès américain, la FCC est la principale autorité des États-Unis en matière de lois, de réglementations et d'innovation technologique dans le secteur des communications.

Les normes FCC spécifiques à cet équipement sont les suivantes :

- Ce dispositif de classe A est conforme à la partie 15 du règlement de la FCC.
- Son utilisation est soumise aux deux conditions suivantes :
  - Ce dispositif ne doit pas créer d'interférences néfastes.
  - Ce dispositif doit accepter toute interférence reçue, y compris celles pouvant provoquer un fonctionnement non souhaité.
- Cet appareil numérique de la classe A est conforme à la norme ICES-003 du Canada.
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

AVERTISSEMENT ! Toute modification apportée à l'unité sans l'approbation expresse du responsable de la conformité peut entraîner l'annulation des droits de l'utilisateur à utiliser cet équipement.

REMARQUE : veuillez consulter la page *http://www.Vertiv.com/ComplianceRegulatoryInfo* pour obtenir des informations importantes sur la sécurité avant l'installation.

Page laissée vierge intentionnellement

2 Présentation

L'unité de distribution électrique en rack (rPDU) Vertiv™ PowerIT offre aux responsables de datacenters des solutions d'alimentation flexibles, modulables en fonction de l'évolution des besoins. D'une distribution de base à une surveillance avancée et une commutation de prises complexe, la rPDU PowerIT s'adapte à vos exigences actuelles et futures.

Pour permettre une telle mis à niveau, les ingénieurs de Vertiv ont intégré un dispositif de surveillance interchangeable (IMD) à la conception robuste de la rPDU. Étant donnée la longue durée de vie utile des PDU, l'IMD permet aux entreprises d'adopter de nouvelles technologies de surveillance, sans avoir à remplacer l'unité toute entière. L'installation de l'IMD remplaçable à chaud s'effectue simplement en quelques étapes, garantissant ainsi que les mises à niveau sont effectuées sans perturber l'alimentation des serveurs critiques.

2.1 Exigences environnementales

Les limites environnementales de fonctionnement relatives à la température, à l'humidité et à l'altitude sont définies dans les tableaux suivants.

Tableau 2.1 Limites de température

Description	Minimum	Maximum
En fonctionnement	0 °C (32 °F)	60 °C (140 °F)
Stockage	-40 °C (-40 °F)	70 °C (158 °F)

Tableau 2.2 Limites d'humidité

Description	Minimum	Maximum
En fonctionnement	5 %	95 % (hors condensation)
Stockage	5 %	95 % (hors condensation)

REMARQUE : si la rPDU Vertiv PowerIT n'est pas installée immédiatement, elle doit être conservée dans son emballage d'origine dans une pièce propre, à l'abri de toute humidité excessive et à l'écart de toute source de chaleur.

Tableau 2.3 Limites d'altitude

Description	Minimum	Maximum
En fonctionnement	0 m (0 ft)	3 050 m (10 000 ft)
Stockage	0 m (0 ft)	15 240 m (50 000 ft)

2.2 Caractéristiques électriques

Les caractéristiques et performances des produits électriques sont définies au Tableau 2.4 ci-dessous. Veuillez également consulter la plaque signalétique du produit pour connaître les limites de classification supplémentaires.

Tableau 2.4 Valeurs nominales des prises

Type	Valeurs nominales
Combinaison C13/C19	250 V c.a., 16 A (UL et CSA 16 A, 250 V c.a.) avec cordon C20 250 V c.a., 10 A (UL et CSA 12 A, 250 V c.a.) avec cordon C14
Prise allemande (Schuko)	250 V c.a., 16 A
IEC-60320 C13	250 V c.a., 10 A (UL et CSA 12 A, 250 V c.a.)
IEC-60320 C19	250 V c.a., 16 A (UL et CSA 16 A, 250 V c.a.)
IEC309 PS6	230 V c.a., 16 A
IEC309 PS56	230/400 V c.a., 32 A
NEMA 5-15R ou L5-15R	125 V c.a., 12 A
NEMA 6-15R ou L6-15R	250 V c.a., 12 A
NEMA 5-20R ou L5-20R	125 V c.a., 16 A
NEMA 6-20R ou L6-20R	250 V c.a., 16 A
NEMA L5-30R	125 V c.a., 24 A
NEMA L6-30R	250 V c.a., 24 A
NEMA L7-15R	277 V c.a., 12 A
NEMA L7-20R	277 V c.a., 16 A
Saf-D-Grid	277 V c.a., 16 A
Verrouillage U-Lock CEI-60320 C13	250 V c.a., 10 A (UL et CSA 12 A, 250 V c.a.)
Verrouillage U-Lock CEI-60320 C19	250 V c.a., 16 A (UL et CSA 16 A, 250 V c.a.)
Prise du Royaume-Uni BS1363	250 V c.a., 13 A

2.3 Mise en réseau

Les exigences de communication du produit sont définies dans les sections suivantes.

2.3.1 Ethernet

La vitesse de la liaison Ethernet pour ce produit est la suivante : 10/100/1 000 Mo ; duplex intégral.

2.3.2 Protocoles

Ce produit prend en charge les protocoles de communication suivants : ARP, IPv4, IPv6, ICMP, ICMPv6, NDP, TCP, UDP, RSTP, STP, DNS, HTTP, HTTPS (TLSv1.3), SMTP, SMTPS, Modbus TCP/IP, DHCP, SNMP (V1/V2c/V3), LDAP, TACACS+, RADIUS, NTP, SSH, RS232 et Syslog.

2.3.3 Interfaces utilisateur

Ce produit prend en charge les interfaces utilisateur suivantes : SNMP, interface utilisateur graphique Web JSON, API JSON et interface de ligne de commande utilisant SSH ou série (RS232).

Page laissée vierge intentionnellement

3 Installation

Installez la rPDU Vertiv™ PowerIT à l'aide des images présentées à la section Montage sur la page suivante.

REMARQUE : veuillez consulter la page http://www.Vertiv.com/ComplianceRegulatoryInfo pour obtenir des informations importantes sur la sécurité avant l'installation

Pour installer l'unité :

1. Portez tous les équipements de protection individuelle (EPI) requis. Il est préférable que les opérations de levage et d'installation d'unités lourdes soient effectuées par deux personnes.
2. Pour les unités horizontales, fixez les supports de montage avec le matériel fourni et serrez les attaches à 7 po/lb. Pour les unités verticales, installez les boutons de montage sans outils fournis à l'arrière de l'unité et serrez les attaches à 13,5 po/lb. À l'aide du matériel approprié, fixez l'unité au rack. Le cas échéant, l'équipement doit être monté dans le rack de sorte à maintenir une circulation d'air suffisante pour garantir un fonctionnement en toute sécurité et à ne pas bloquer les orifices de ventilation.
3. Branchez la rPDU Vertiv™ PowerIT sur une prise de circuit de dérivation de taille adéquate et correctement protégée.

ATTENTION : Risque de chute d'objets étrangers dans le corps de la rPDU. Peut provoquer des dommages matériels. Lors de l'accès au compartiment de câblage durant l'installation, assurez-vous qu'aucun corps étranger, tel que des débris, ne tombe dans le corps de la rPDU. Lors de l'installation, en cas de chute dans la rPDU d'objets étrangers qui ne peuvent pas être récupérés, NE METTEZ PAS la rPDU SOUS TENSION. Renvoyez la rPDU à Vertiv pour réparation.

   Pour les unités triphasées en étoile, vérifiez toujours qu'une connexion neutre correcte est présente au niveau de la prise du circuit de dérivation de l'installation du bâtiment pour les unités raccordées par cordon ou au niveau de la borne de câblage d'entrée pour les unités câblées. En cas de connexion neutre ouverte, la rPDU et l'équipement raccordé peuvent être endommagés.

4. Branchez les dispositifs qui doivent être alimentés par la rPDU Vertiv™ PowerIT.
5. Activez chaque dispositif connecté à la rPDU Vertiv™ PowerIT.

REMARQUE : une mise sous tension séquentielle est recommandée pour éviter tout courant d'appel élevé.

3.1 Montage

Les supports en option sont vendus séparément.

Figure 3.1 Supports pleine longueur

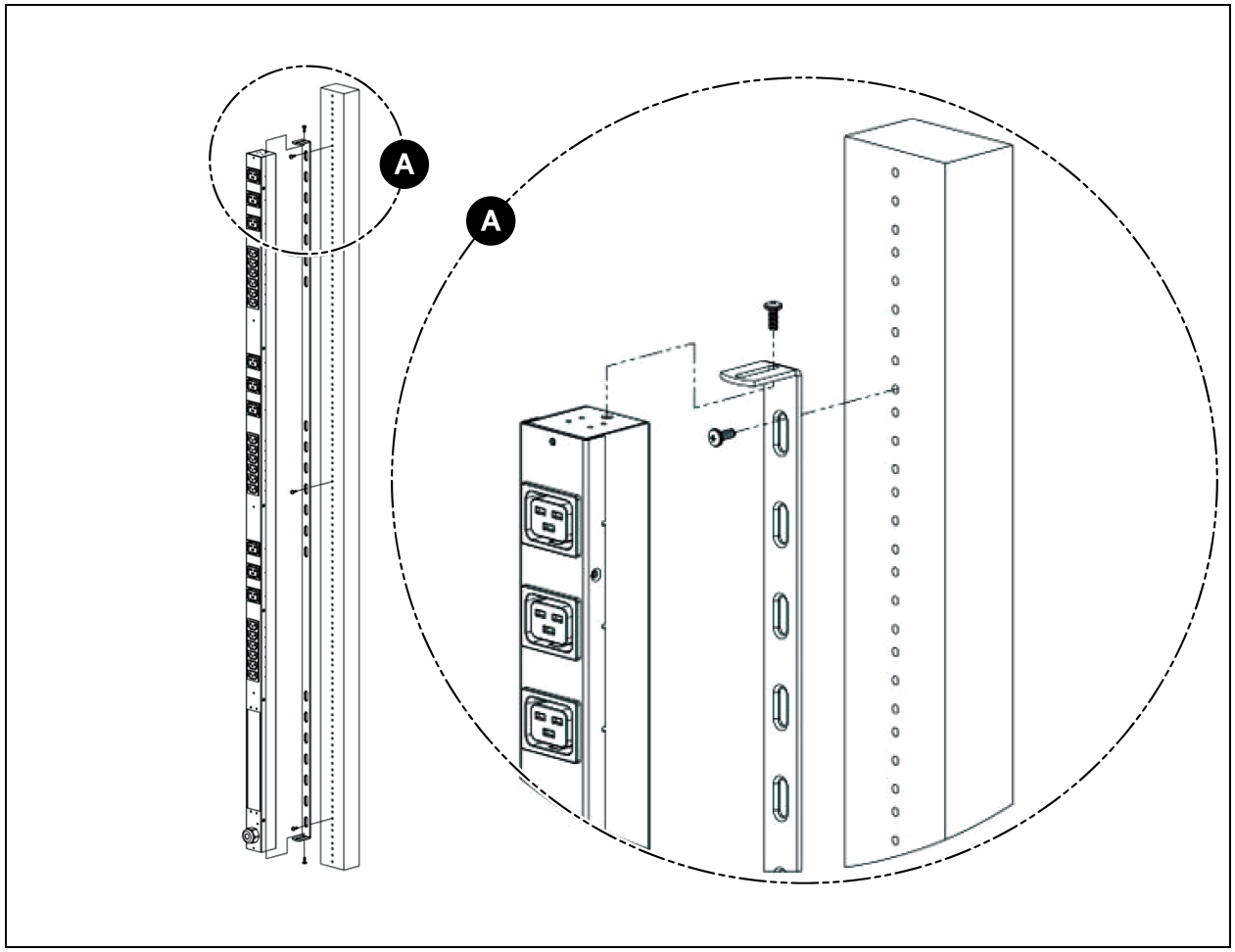


Figure 3.2 Supports Mini L

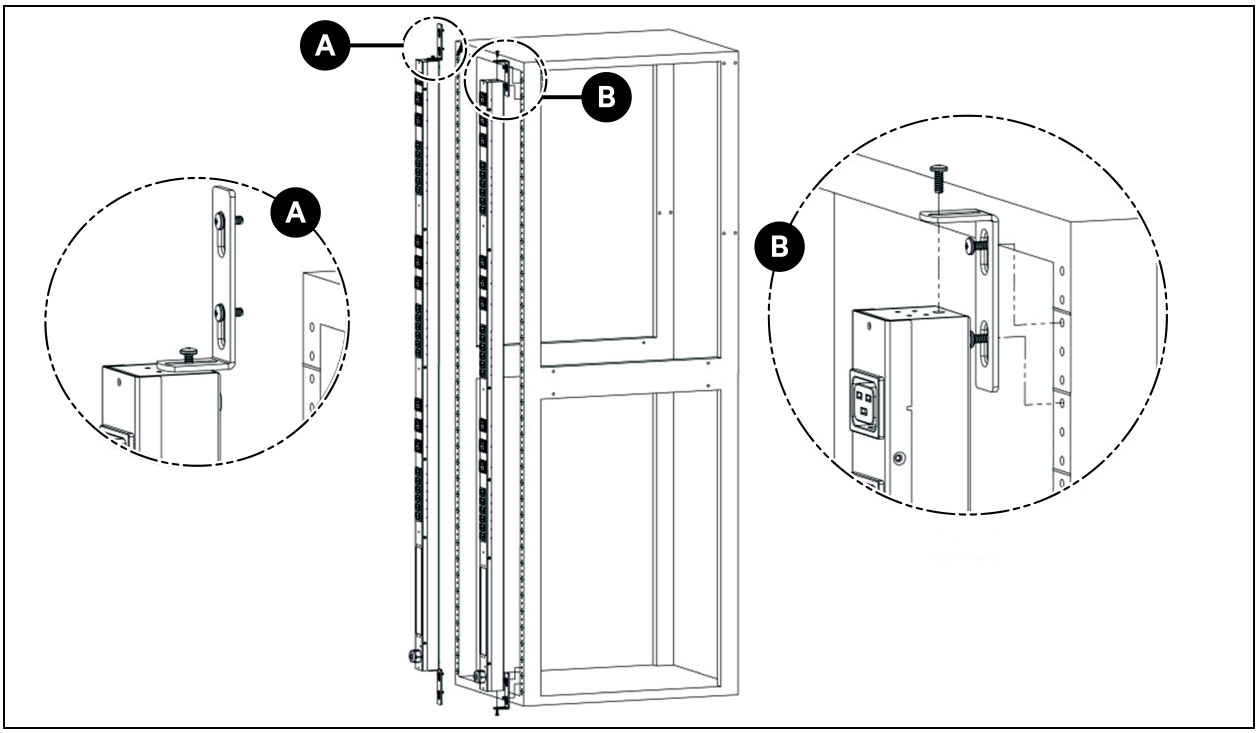


Figure 3.3 Supports d'extension verticaux

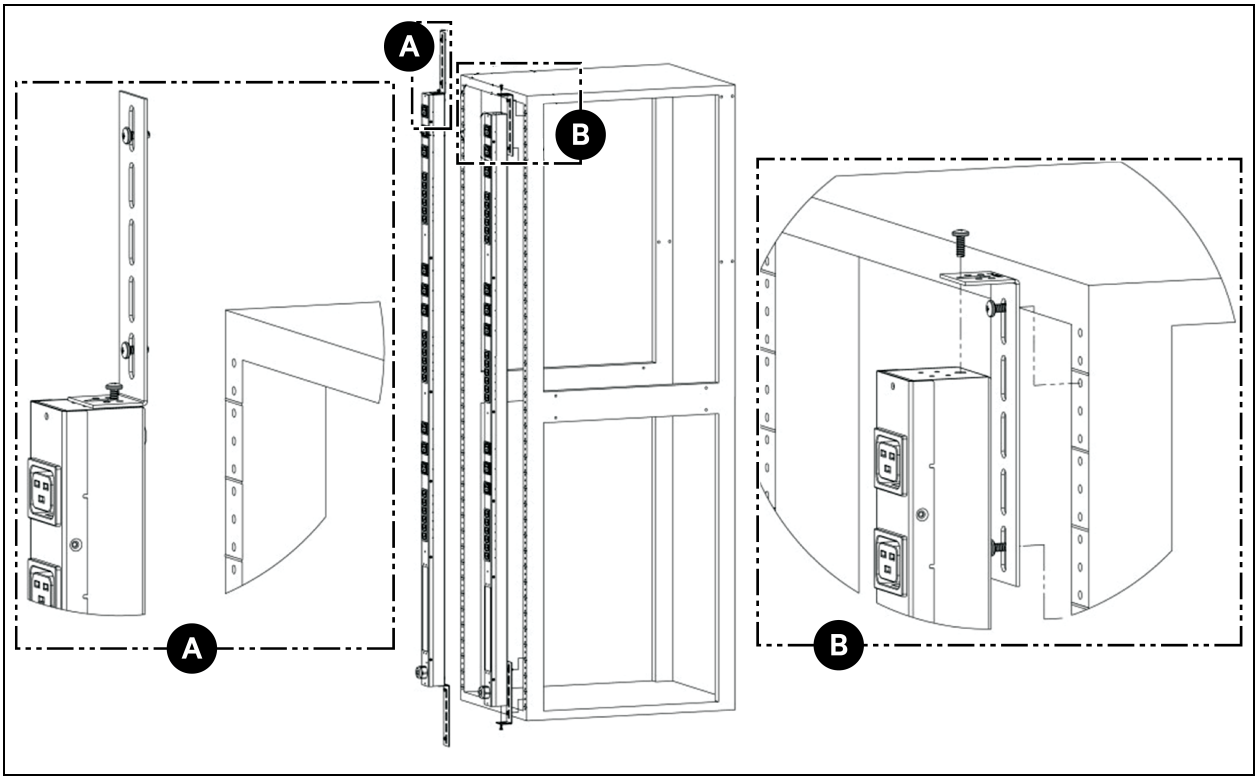


Figure 3.4 Matériel de montage sans outil

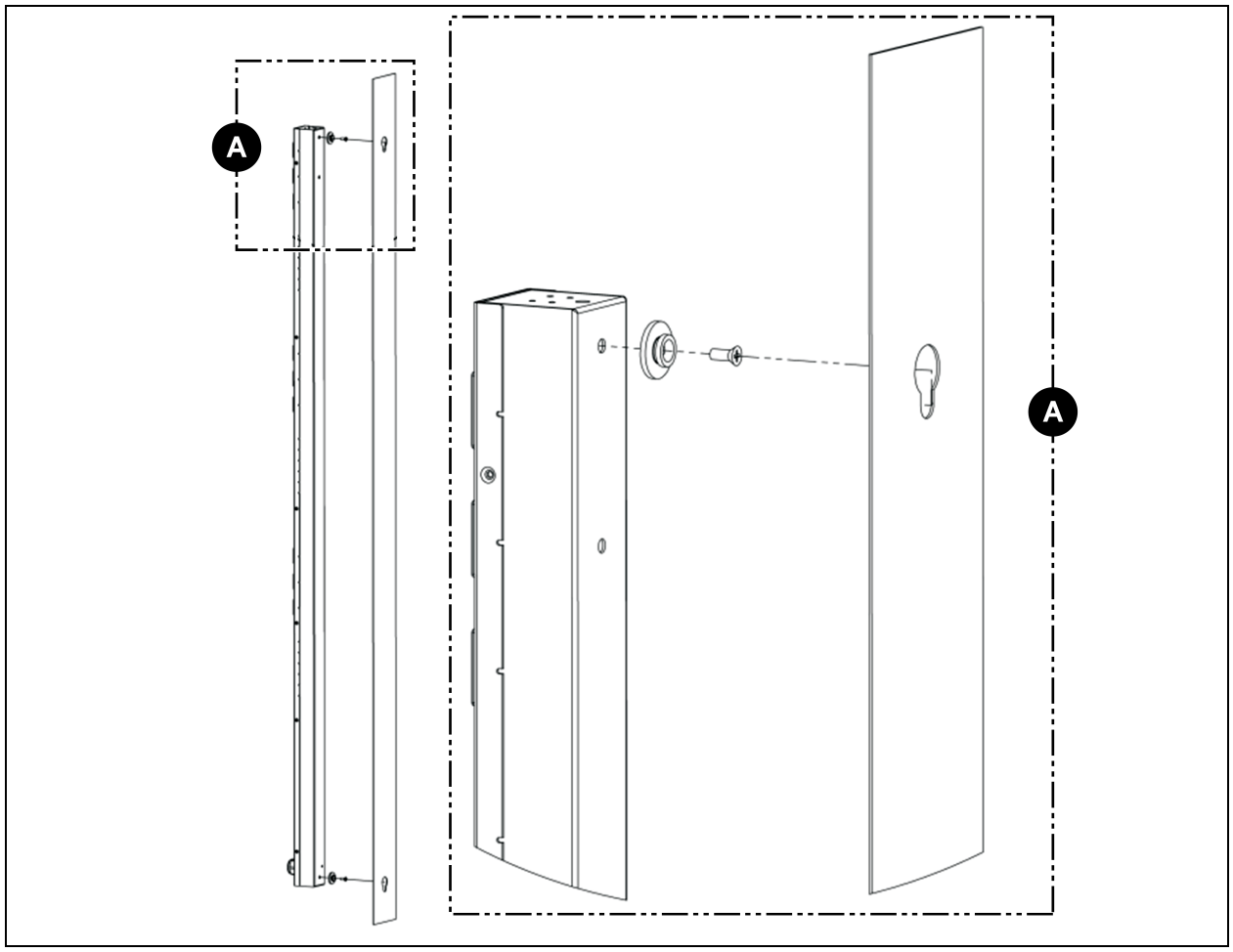
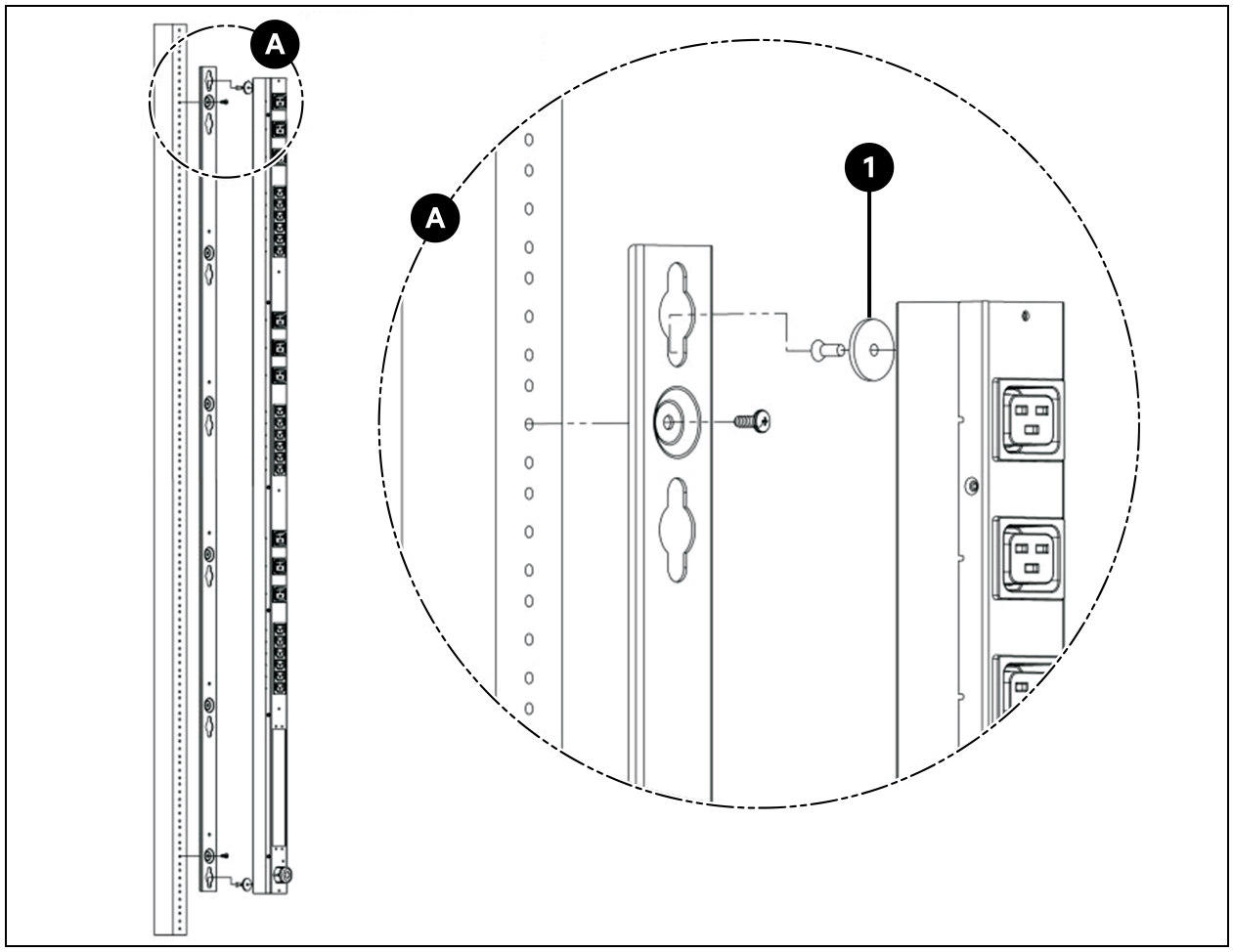


Figure 3.5 Supports pleine longueur sans outil



Élément	Description
1	Rondelle à épaulement sans outil

Figure 3.6 Supports pour deux unités à montage latéral simple

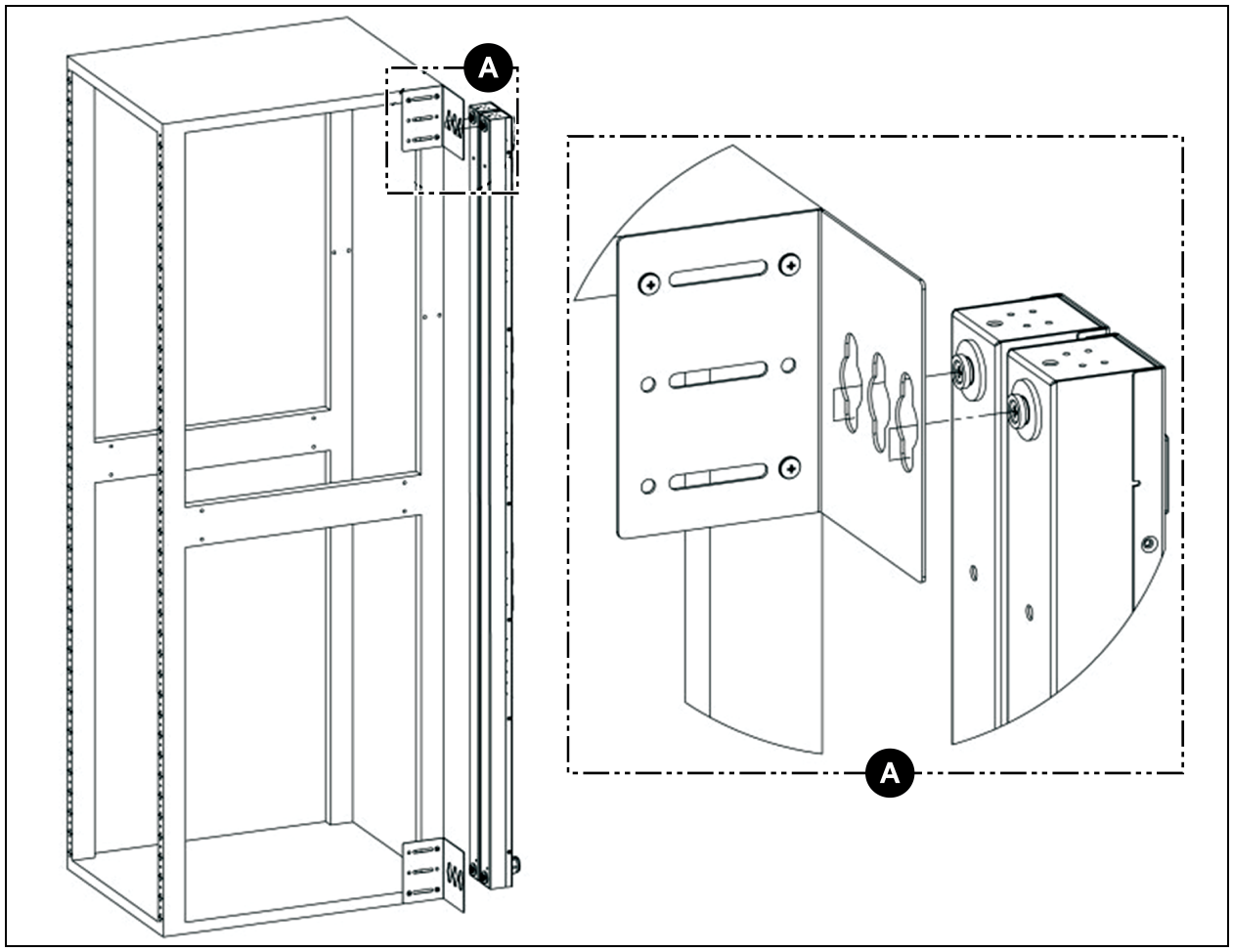
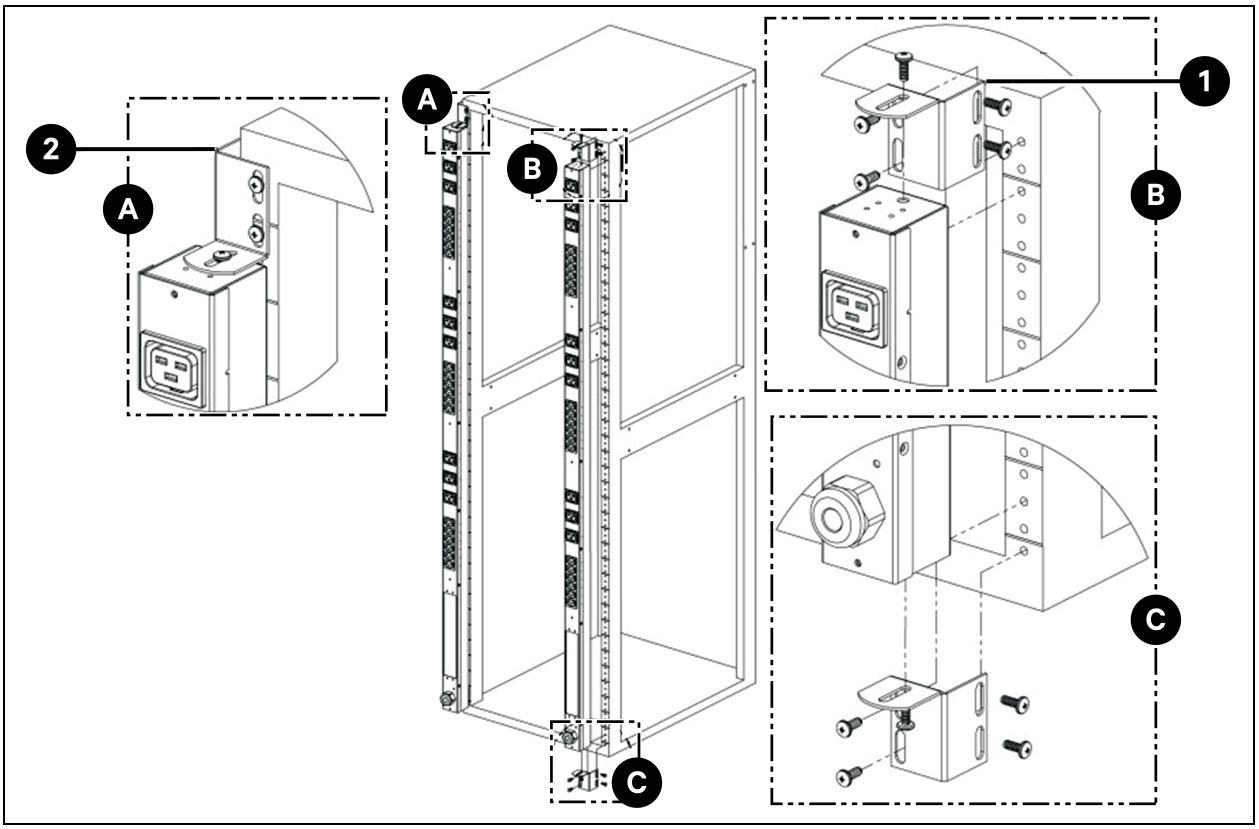


Figure 3.7 Supports de montage décalés/latéraux



Élément	Description
1	Option côté droit
2	Option côté gauche

Figure 3.8 Supports d'extension de 7 pouces

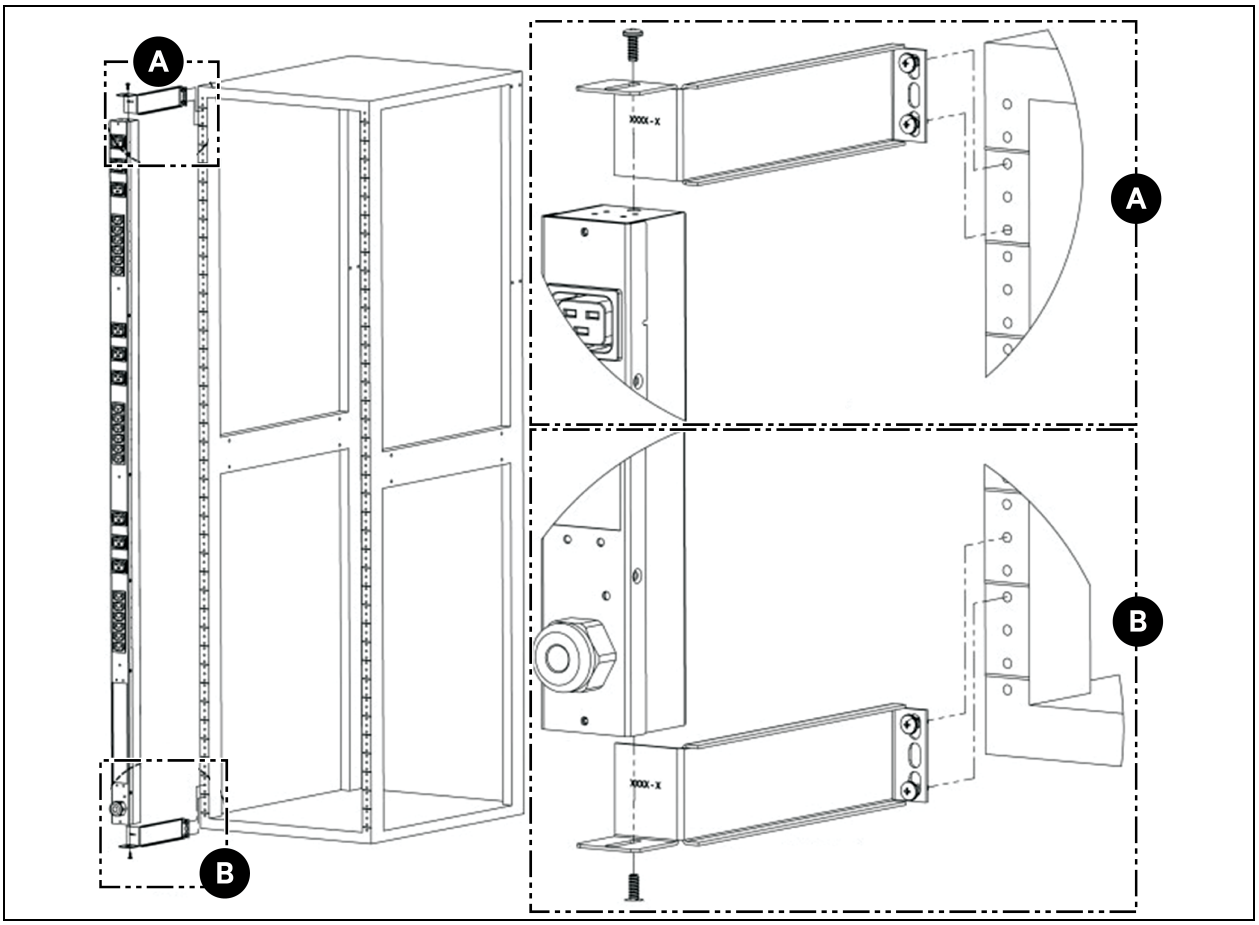


Figure 3.9 Support de montage encastré

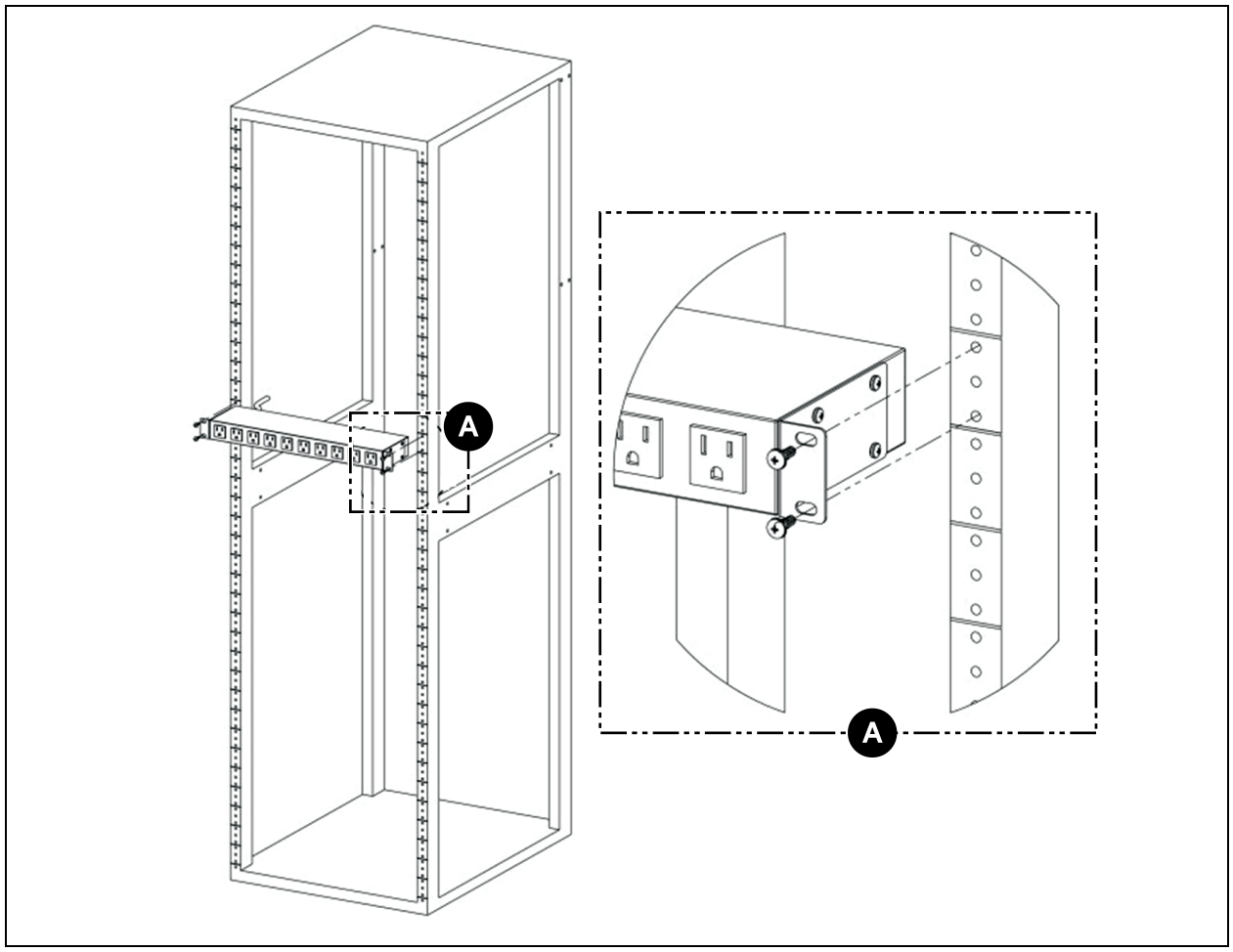


Figure 3.10 Support de montage réglable

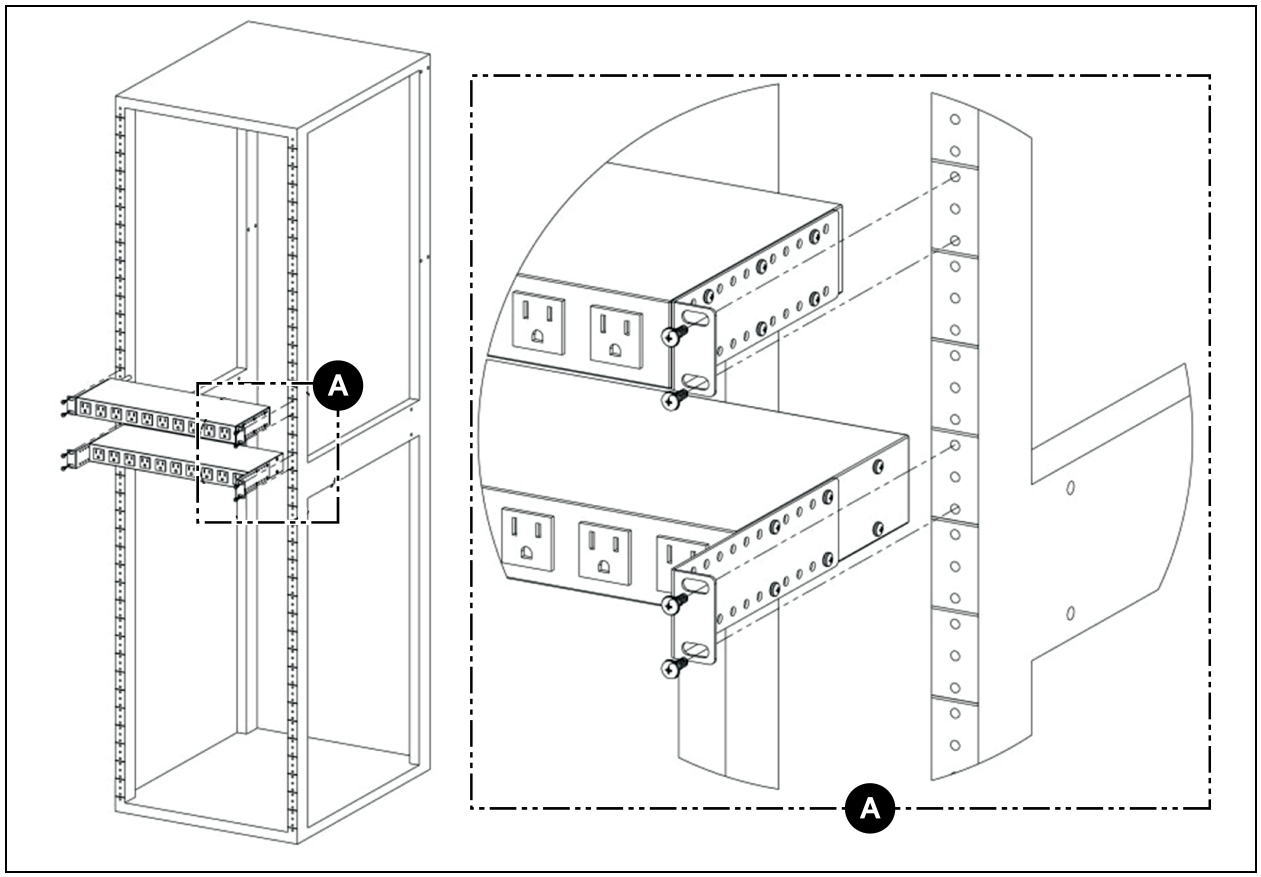


Figure 3.11 Support de montage sur panneau

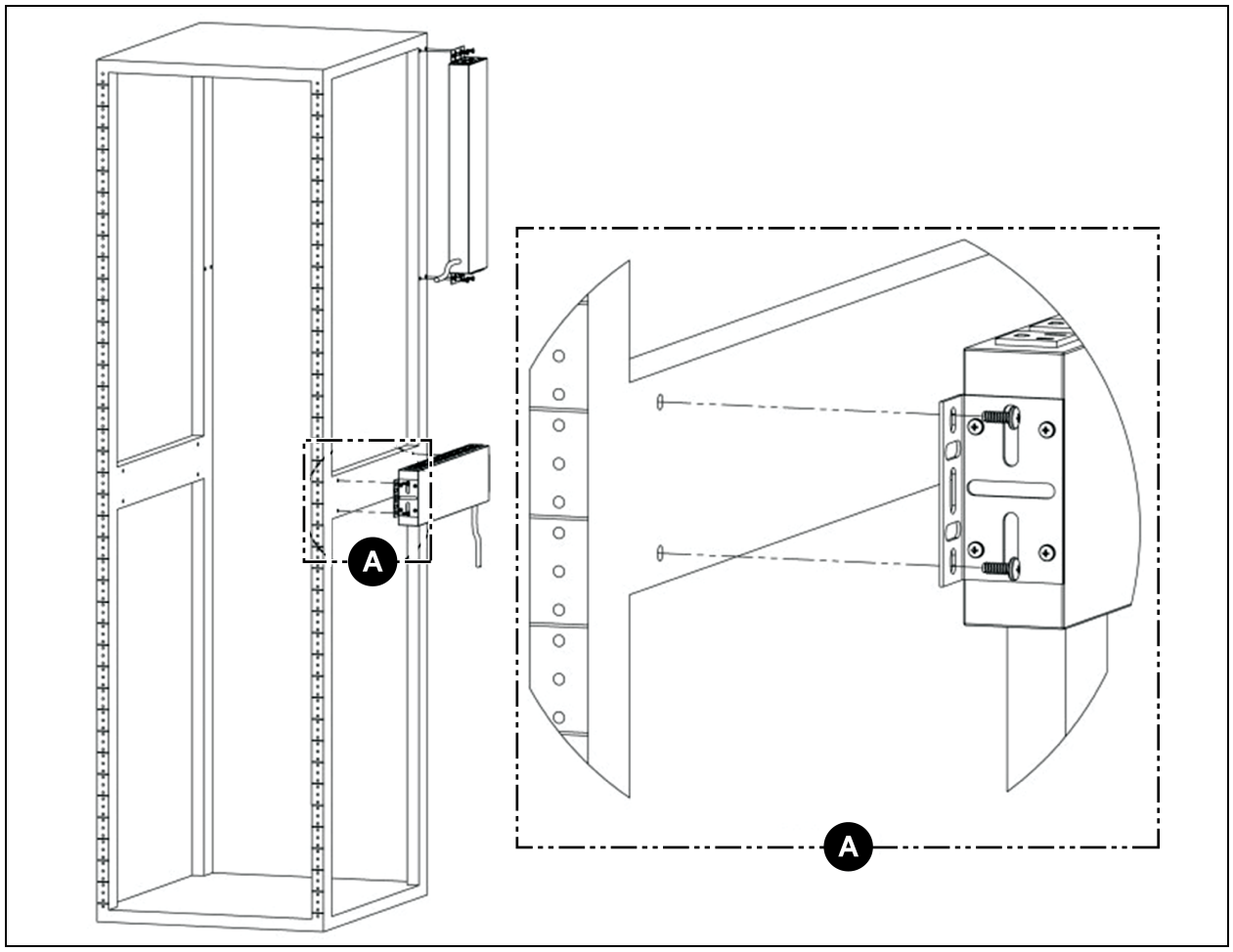


Figure 3.12 Supports de montage de conversion de 23 pouces

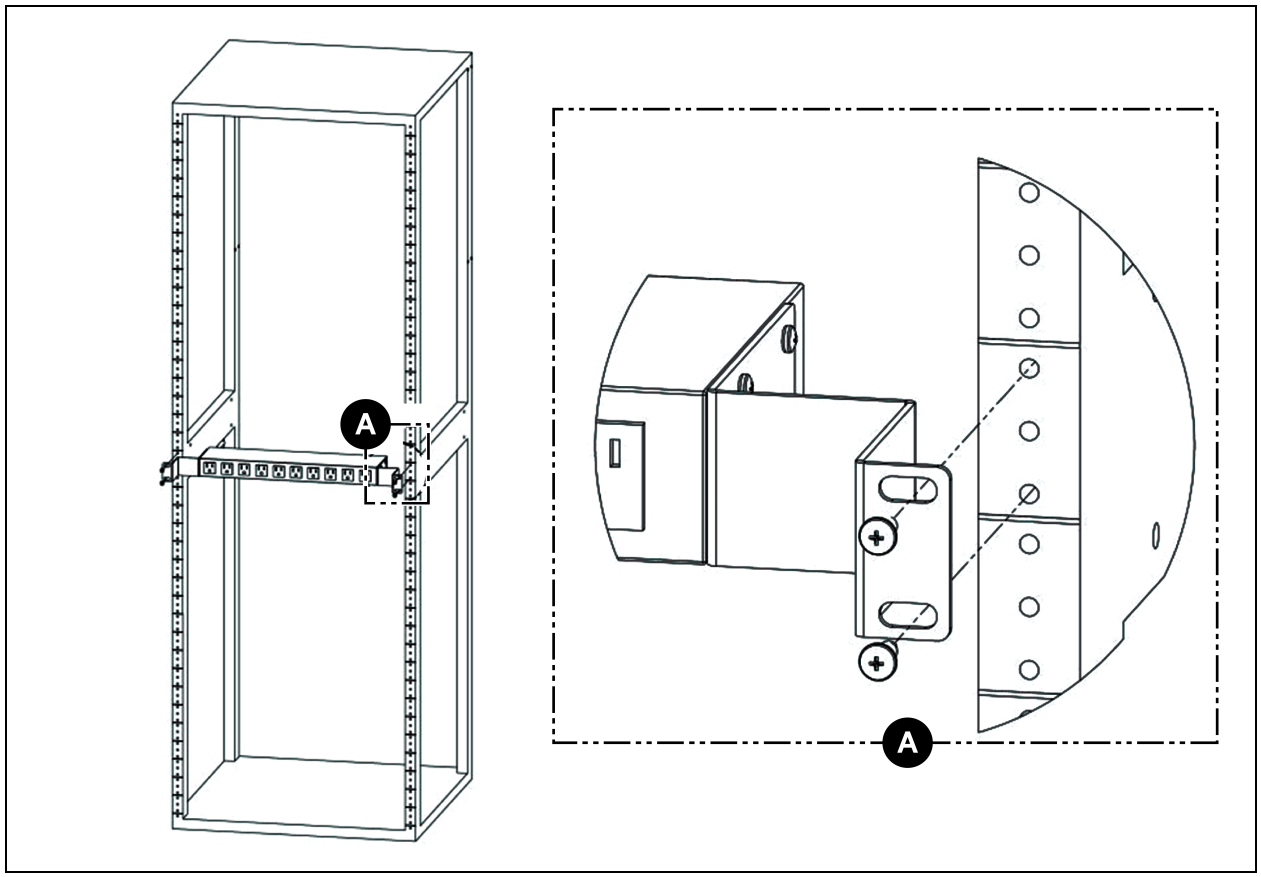


Figure 3.13 Supports de montage horizontaux/sur panneau de 19 pouces

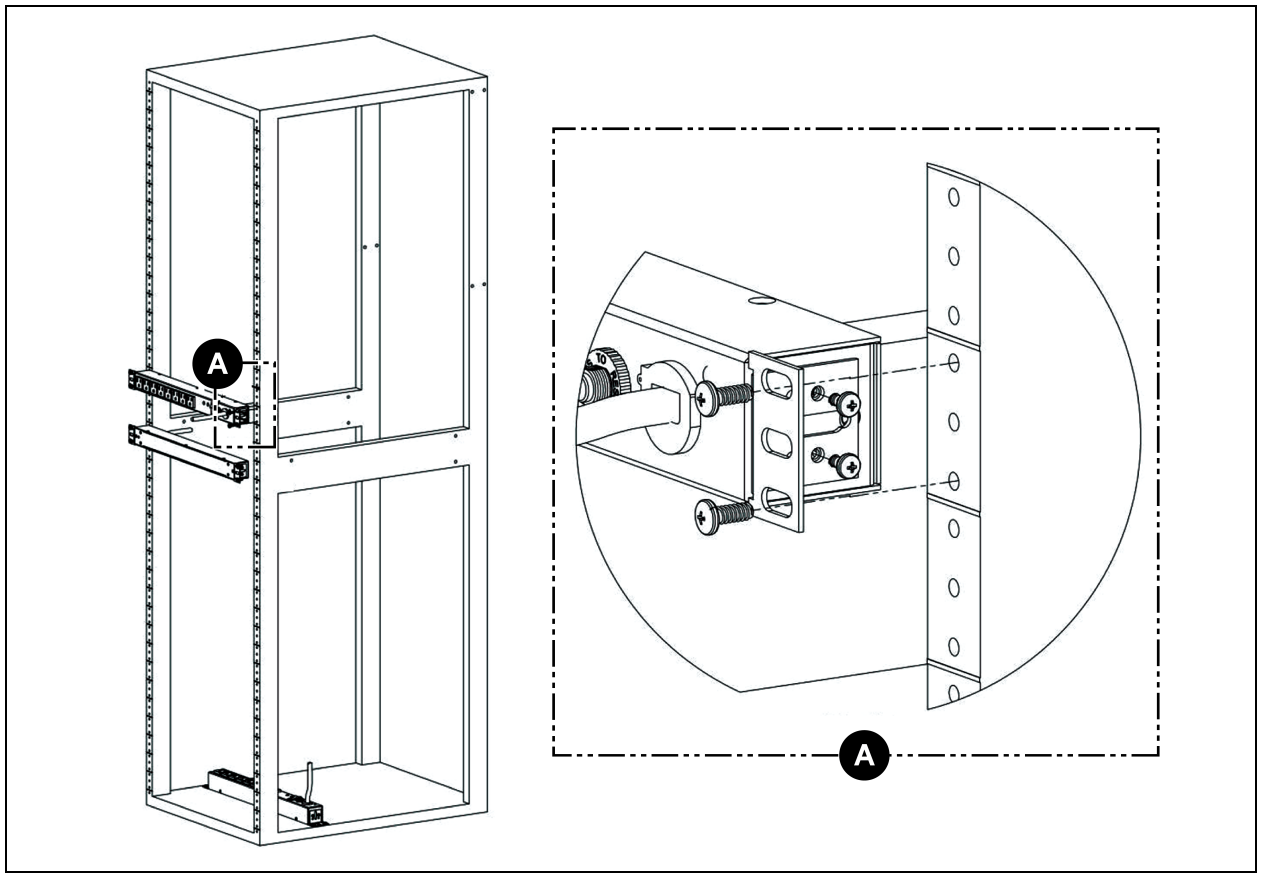
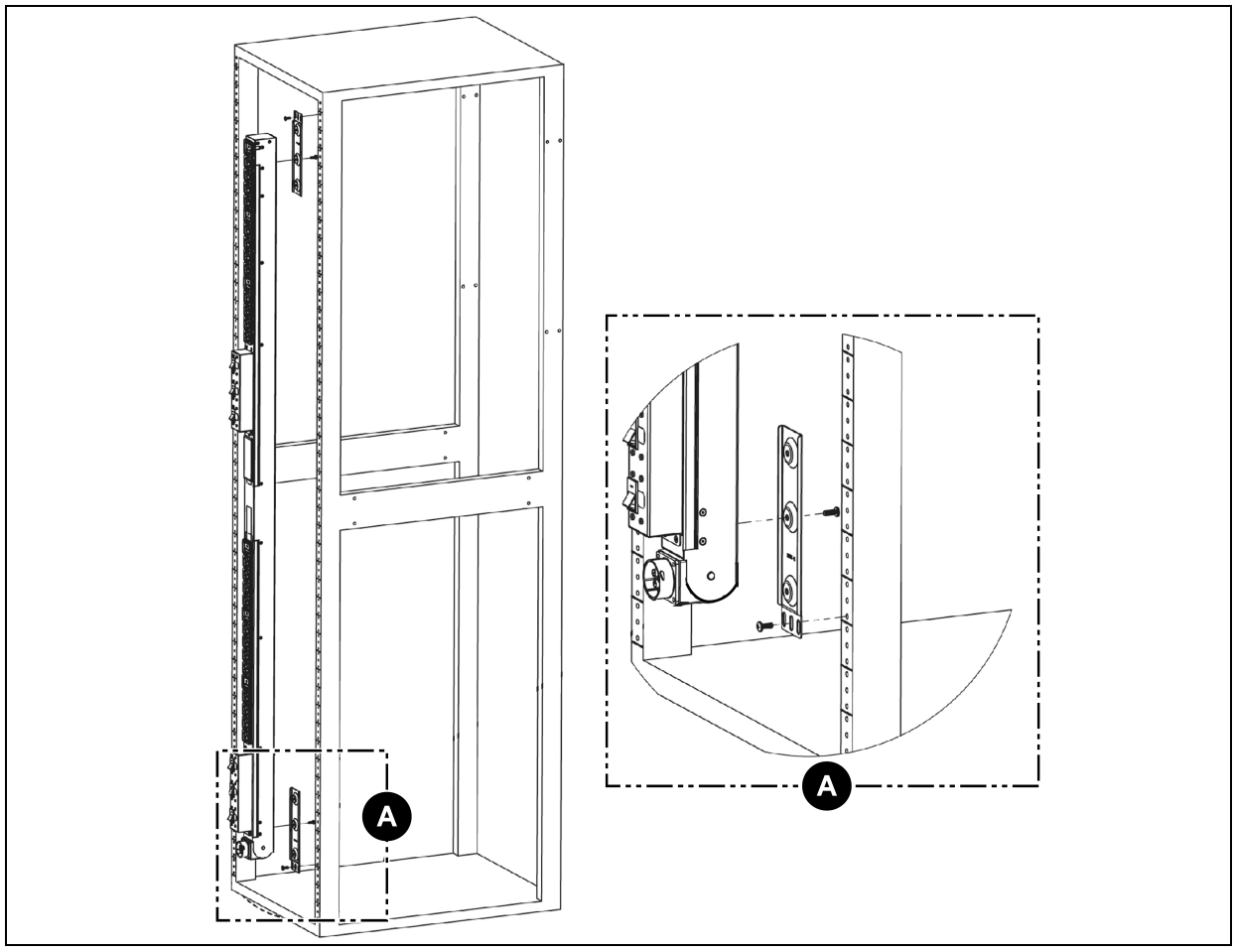


Figure 3.14 Supports de montage pour unité de distribution électrique universelle (UPDU) Vertiv™ PowerIT avec extrémité pivotante



3.2 Raccordement électrique

Branchez la rPDU Vertiv™ PowerIT sur une prise de circuit de dérivation de taille adéquate et correctement protégée. Assurez-vous que le câble d'alimentation ne dépasse pas le rayon de courbure du fabricant (8X).

3.2.1 Fonctionnement du mécanisme U-Lock

Branchez les dispositifs qui doivent être alimentés par la rPDU Vertiv™ PowerIT.

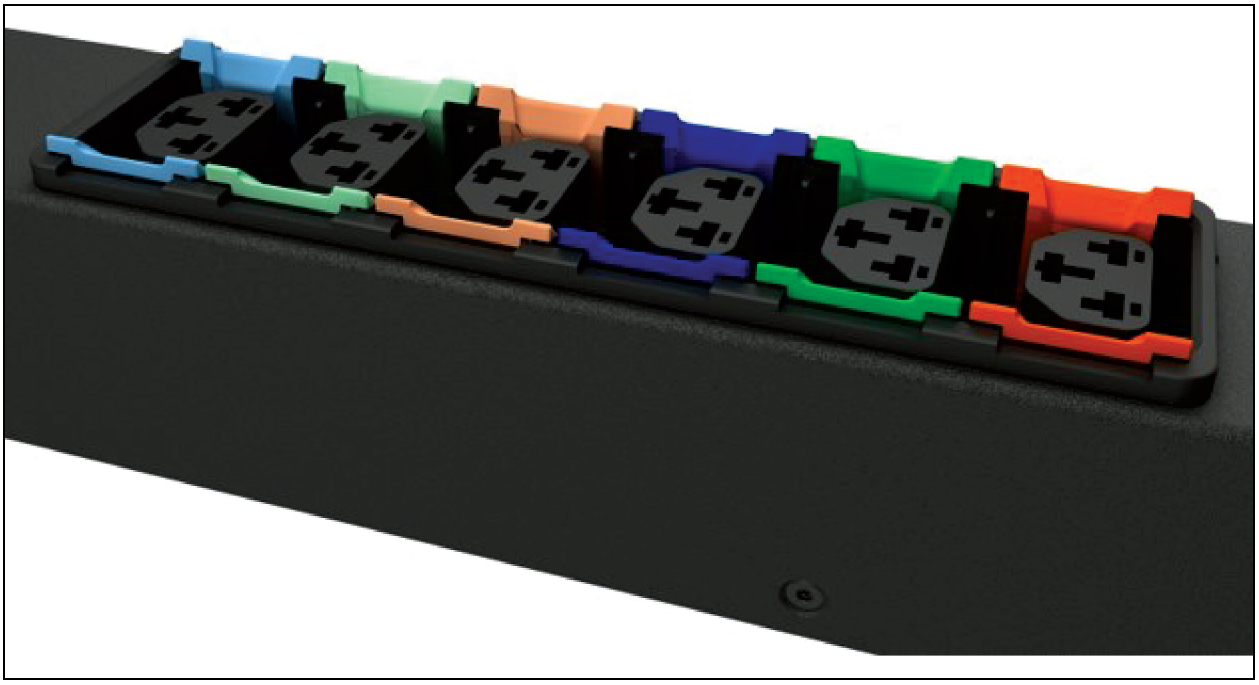
- Retenue du cordon d'alimentation U-Lock brevetée de Vertiv.
- Utilisation de cordons d'alimentation standard.
- Système de verrouillage activé par l'insertion du cordon.
- Fonction de déverrouillage facile du cadre par pression et maintien.

Figure 3.15 Fonctionnement du mécanisme de retenue du cordon U-Lock

3.2.2 Fonctionnement du mécanisme P-Lock

- Branchez les dispositifs qui doivent être alimentés par la rPDU Vertiv™ PowerIT .
- Vertiv™ utilise une prise combinée C13/C19 avec retenue du cordon d'alimentation P-Lock.
- Est compatible avec les cordons d'alimentation P-Lock.
- Utilisez les languettes à pression du cordon P-Lock pour les dégager de la prise.

Figure 3.16 Fonctionnement du mécanisme de retenue du cordon P-Lock



4 Meilleures pratiques de sécurité

Les paramètres par défaut sur le support de la carte sont définis sur la configuration la plus sécurisée pour le déploiement. Pour garantir la sécurité adéquate des composants essentiels de l'infrastructure, il faut une configuration appropriée de TOUS les services de communication. Cette section présente un résumé des paramètres.

Tout au long du cycle de vie de nos produits Vertiv SECURE, Vertiv s'engage à minimiser les risques de cybersécurité liés à ses produits en déployant les meilleures pratiques de cybersécurité dans la conception technique de ses produits et de ses solutions, en les rendant plus sûrs, plus fiables et plus compétitifs pour ses clients.

Quelques recommandations en matière de cybersécurité tout au long du cycle de vie sont présentée ci-dessous. Les recommandations en matière de cybersécurité ne visent pas à fournir un guide complet sur la cybersécurité, mais plutôt à compléter les programmes de cybersécurité existants des clients. Vous pouvez consulter les sites suivants pour obtenir des informations complémentaires sur les meilleures pratiques et les directives générales en matière de cybersécurité :

https://www.cisa.gov/topics/cybersecurity-best-practices

https://www.vertiv.com/en-us/support/security-support-center/

Le **Tableau 4.1** ci-dessous, fournit une liste d'éléments à examiner. Chacun doit être examiné, configuré en fonction des besoins opérationnels de gestion de l'équipement, et il convient de vérifier que les paramètres prennent en charge la fonctionnalité opérationnelle souhaitée sans ajouter d'accès inutile ou non autorisé aux composants essentiels de l'infrastructure. Une référence à la section appropriée de ce document est fournie pour la configuration de chaque élément.

Tableau 4.1 Paramètres à examiner et à vérifier pour réduire le risque d'accès non autorisé

Élément	Description	Référence
Comptes et mots de passe	Modifiez immédiatement les noms et les mots de passe des comptes d'administrateur et d'utilisateur pour éliminer l'accès aux informations d'identification par défaut.	Reportez-vous à la section Utilisateurs à la page 66.
Accès au réseau IP	Activez/désactivez l'accès réseau IPV4 et IPV6 à la carte – désactivez l'accès réseau inutilisé.	Reportez-vous à la section Réseau à la page 70.
Accès SSHv2	Activez/désactivez l'accès SSHv2 pour la prise en charge du diagnostic et de la configuration – désactivez ce paramètre lorsqu'il n'est pas utilisé.	Reportez-vous à la section SSH à la page 87.
Protocole de service Web	Sélectionnez HTTPS pour utiliser le chiffrement SSL lors de l'accès aux données via l'interface utilisateur Web.	Reportez-vous à la section Serveur Web à la page 80.

Tableau 4.1 Paramètres à examiner et à vérifier pour réduire le risque d'accès non autorisé (suite)

Élément	Description	Référence
Certificats TLS	Lorsque vous utilisez HTTPS, installez vos propres certificats TLS provenant d'une autorité de certification de confiance ou générez d'autres certificats auto-signés.	Reportez-vous à la section SSL Certificate : vous permet de télécharger votre propre fichier de certificat SSL signé pour remplacer le certificat par défaut. Le certificat peut être auto-signé ou signé par une autorité de certification. Le certificat SSL doit être au format PEM ou PFX (PKCS12). à la page 80.
Accès Web en écriture à distance	Pour contrôler/écrire via l'interface Web, vous devez vous connecter à distance et avoir un compte utilisateur de niveau administrateur ou de niveau contrôle. Pour interdire l'accès à distance, désactivez HTTP et HTTPS. **AVERTISSEMENT ! La désactivation des protocoles HTTP et HTTPS mettra immédiatement fin à cette connexion et l'accès à distance ne sera disponible qu'à l'aide de SSH.**	Reportez-vous à la section Serveur Web à la page 80.
Protocoles de communication	Activez/désactivez SNMP – désactivez les protocoles inutilisés.	Reportez-vous la section Modbus à la page 93.
Paramètres de version SNMP	Activez/désactivez les versions SNMP souhaitées, envisagez d'utiliser SNMPv3 avec le chiffrement et l'authentification des utilisateurs.	Reportez-vous à la section SNMP à la page 91.
Paramètres de la table d'accès SNMP	Pour chaque entrée de la table d'accès SNMPv1/v2c, réglez le paramètre SNMP Access Type sur Read-Only pour empêcher les modifications apportées au périphérique par les hôtes identifiés dans l'entrée de la table.	Reportez-vous à la section SNMP à la page 91.
Chaînes de communauté SNMP	Utilisez des valeurs suffisamment fortes pour la communication SNMP, conformément à la politique des mots de passe de votre organisation.	Reportez-vous à la section SNMP à la page 91.
Paramètres SNMPv3	Utilisez des algorithmes de hachage et de chiffrement appropriés pour les paramètres d'authentification et de confidentialité SNMPv3 afin de renforcer la sécurité des communications SNMPv3.	Reportez-vous à la section SNMP à la page 91.
Compte utilisateur invité	Ce compte doit rester désactivé, sauf s'il est nécessaire. Étant donné qu'il fournit un accès en lecture seule au dispositif et peut donner un contexte supplémentaire aux paramètres du dispositif s'il est activé.	Reportez-vous à la section Utilisateurs à la page 66.

Pour renforcer la sécurité, le pare-feu et la passerelle du réseau local peuvent être restreints pour autoriser uniquement le trafic nécessaire sur les voies réseau requises. Les voies utilisées par la carte IMD-5M sont répertoriées dans le tableau suivant. Certains paramètres de voie peuvent être modifiés par l'administrateur.

Tableau 4.2 Voies utilisées par la carte IMD-5M (v6.1 ou supérieure)

Service réseau	Voie utilisée	Par défaut	Modification requise
HTTP	TCP80	N	O
HTTPS	TCP443	O	O
DNS	TCP et UDP 53	O	N
NTP	TCP et UDP 123	O	N
SMTP	TCP25	O	O
SSH	TCP UDP 22	O	N
SNMP	UDP 161, 162	N	Seule la voie d'interruption 162 peut être modifiée.
Modbus	TCP 502	N	O
VID/VIP	GDP/HTTP	N	N
Client DHCP	UDP 68	O	N
GDP (Geist Discovery Protocol)	UDP 6687	O	N
LDAP	TCP 389	N	O
RADIUS	UDP1812/1813/1645/1646	N	N
TACACS	TCP 49	N	N
Syslog à distance	TCP 514	N	O

La configuration de toutes les options est décrite en détail dans le reste de ce guide.

4.1 Évaluation des risques

Vertiv recommande de procéder à une évaluation des risques pour identifier et évaluer les risques internes et externes raisonnablement prévisibles concernant la sécurité, la disponibilité et l'intégrité du système et de son environnement. Cet exercice doit être réalisé conformément aux cadres techniques et réglementaires applicables tels que les normes CEI 62443 et NERC-CIP. L'évaluation des risques doit être répétée régulièrement.

4.2 Sécurité physique

L'IMD-5M est conçu et destiné à être déployé et utilisé dans un emplacement physiquement sécurisé. Vertiv recommande l'examen de la sécurité physique et de l'environnement dans lequel l'unité est utilisée. Étant donné qu'un pirate ou une menace interne peut provoquer de graves perturbations, vous trouverez ci-dessous quelques bonnes pratiques recommandées, notamment :

- Restreignez l'accès aux zones, aux racks et aux unités avec des cartes/badges RFID chiffrés, une authentification par code d'accès multifacteur unique pour l'accès, des sas de sécurité et des lecteurs biométriques pour l'accès physique à l'équipement.
- Des agents de sécurité fiables et dont les antécédents ont été vérifiés, avec une présence physique 24 heures sur 24, 7 jours sur 7, 365 jours par an, et des registres sur papier pour aider à documenter et consigner les accès physiques à un centre de données, un bâtiment et un rack.

- Assurez un accès physique restreint aux équipements de télécommunications et au câblage du réseau. L'accès physique aux lignes de télécommunication et au câblage du réseau doit être restreint pour se protéger contre les tentatives d'interception ou de sabotage des communications. Les meilleures pratiques incluent l'utilisation de conduits métalliques pour le câblage du réseau reliant les armoires d'équipement.
- Toutes les voies USB, RJ45 et/ou toute autre voie physique doivent être restreintes sur les unités.
- Ne connectez pas de support amovible (tel que des périphériques USB et des cartes SD) pour toute opération (telle qu'une mise à niveau du firmware, un changement de configuration ou un changement d'application de démarrage) à moins que l'origine du support ne soit connue et fiable. Avant de connecter un dispositif portable via une voie USB ou un emplacement pour carte SD, analysez le dispositif afin de détecter les logiciels malveillants et les virus.

4.3 Accès aux comptes

Les privilèges d'accès aux comptes IMD-5M doivent être administrés de manière à fournir le moins de fonctions de compte possible, mais suffisamment pour permettre à l'utilisateur final d'effectuer son travail. La connexion à l'IMD-5M doit être limitée aux utilisateurs légitimes. Certaines des meilleures pratiques suivantes doivent être adoptées dans le cadre des procédures écrites d'une organisation pour l'accès au réseau et aux équipements :

- Lors de la première connexion à l'IMD-5M, il convient de créer les informations d'identification.
- Interdiction de tout partage de compte/connexion. Chaque utilisateur doit avoir son propre compte et son propre mot de passe. Pour pouvoir se connecter à l'IMD-5M, chaque compte doit correspondre à un utilisateur unique non partagé.
- Les administrateurs doivent restreindre l'accès et les privilèges aux seules fonctions requises par les obligations professionnelles de l'utilisateur.
- Limitez tous les privilèges de niveau administrateur (tels que les mises à jour du firmware, l'activation/la désactivation du protocole) aux seuls administrateurs approuvés.
- Assurez-vous que les exigences relatives à la force, à la complexité et à la longueur des mots de passe soient appliquées au plus haut niveau conformément à la politique informatique de l'entreprise.
- Veillez immédiatement à ce que les employés licenciés ne puissent plus accéder à l'unité. Quelques exemples incluent l'utilisateur d'un processus d'authentification utilisateur AAA, TACACS+.
- Appliquez le délai d'expiration de session après une période d'inactivité.
- Utilisez la fonction Syslog à distance pour vous alerter des événements système et réseau, des menaces pour la sécurité et de la visibilité sur l'appareil afin de résoudre les problèmes (cela peut également être requis dans votre environnement pour garantir la conformité aux normes PCI-DSS/SOX/HIPAA).

5 Configuration

5.1 Dispositif de surveillance interchangeable

Le dispositif de surveillance interchangeable (IMD) est au cœur de la gamme de produits d'alimentation électrique que constituent les rPDU Vertiv™ PowerIT évolutives. L'IMD peut être remplacé et mis à niveau pour permettre aux datacenters de pérenniser leurs emplacements. L'installation d'un mauvais IMD de remplacement dans une rPDU peut endommager l'IMD.

5.1.1 Configuration de base

La rPDU Vertiv™ PowerIT évolutive de base intègre le module IMD-01X, qui fournit une distribution électrique à faible coût avec une possibilité de mise à niveau pour ajouter à l'avenir un compteur local et/ou une surveillance à distance et d'autres fonctionnalités.

5.1.2 À compteur

La rPDU Vertiv™ PowerIT évolutive à compteur est une option à compteur local. Elle intègre le module IMD-01D, qui fournit un affichage local pour visualiser l'appel de courant (ampères) avec une possibilité de mise à niveau pour ajouter à l'avenir la surveillance et d'autres fonctionnalités.

Figure 5.1 Module IMD-01D

Tableau 5.1 Description du module IMD-01D

Élément	Nom	Description
1	Affichage local	L'affichage local indique les valeurs du courant de phase, de ligne et de circuit (en ampères).
2	Boutons de l'affichage	Trois boutons sont disponibles près de l'affichage de l'IMD : Précédent, Suivant et bouton central. Les fonctions de ces boutons sont décrites au **Tableau 5.2** sur la page suivante.

Tableau 5.2 Fonctions des boutons de l'affichage

Bouton	Symbole	Description
Bouton Précédent		Revient au canal précédent.
Bouton Suivant		Passe au canal suivant.
Bouton central		Bascule entre les modes de défilement et d'affichage statique. En maintenant ce bouton enfoncé pendant 10 secondes, vous réinitialiserez le réseau, restaurerez l'adresse IP par défaut et réinitialiserez les informations du compte utilisateur.
Boutons Précédent et Suivant	et	En appuyant sur les deux boutons simultanément, vous inverserez l'affichage de 180 degrés.

REMARQUE : la fonctionnalité des boutons de l'affichage peut varier en fonction de la configuration de l'unité.

5.1.3 Unité surveillée

Les versions antérieures des rPDU Vertiv™ PowerIT de surveillance au niveau de l'unité Vertiv™ étaient livrées avec le module IMD-03E-G.

Figure 5.2 Module IMD-03E-G

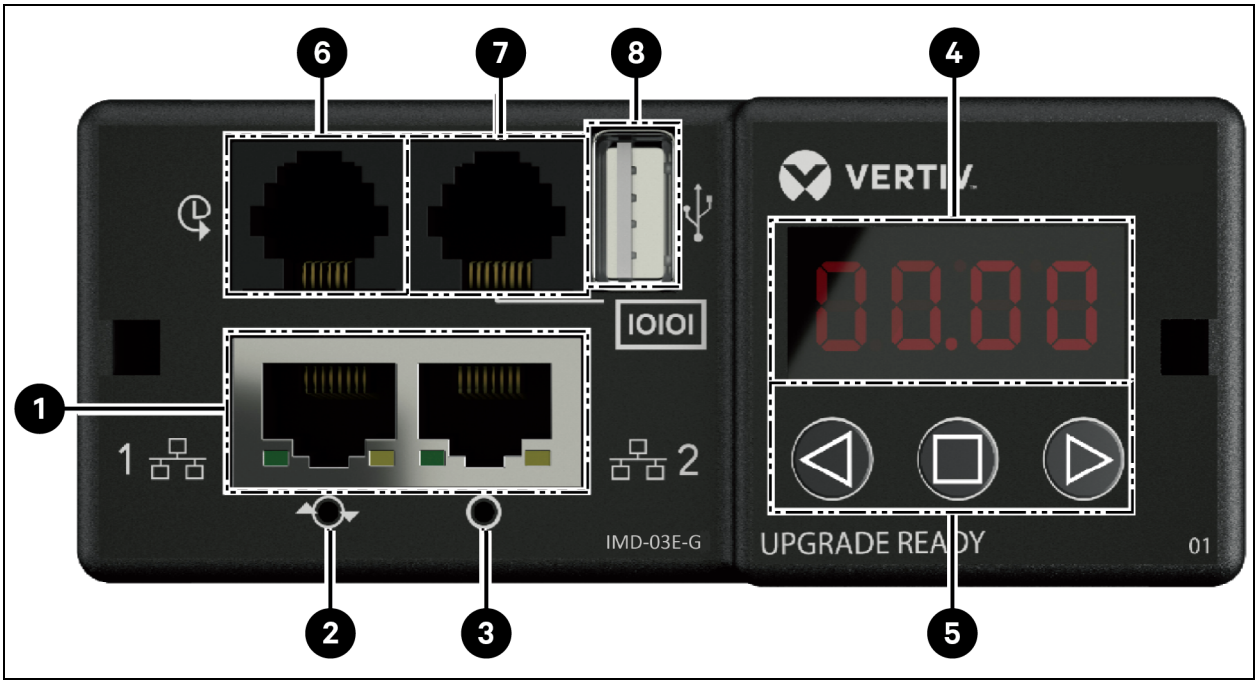


Tableau 5.3 Description du module IMD-03E-G

Numéro	Nom	Description
1	Deux voies Ethernet	Les deux voies Ethernet fonctionnent comme un commutateur Ethernet à deux voies, permettant la connexion en cascade de plusieurs dispositifs. Les deux voies Ethernet peuvent être des interfaces réseau Ethernet doubles configurées indépendamment, permettant à la rPDU de se connecter à deux réseaux différents.
2	Bouton de redémarrage forcé	En appuyant sur le bouton de redémarrage forcé, vous redémarrez l'IMD. Cela a pour effet de redémarrer l'IMD, aucune information utilisateur n'est modifiée ni supprimée.
3	Bouton de réinitialisation du réseau	En maintenant le bouton de réinitialisation du réseau enfoncé pendant 5 secondes en mode de fonctionnement normal, vous restaurerez l'adresse IP par défaut et réinitialiserez les comptes utilisateur.
4	Affichage local	L'affichage local indique les valeurs du courant de phase, de ligne et de circuit (en ampères).
5	Boutons de l'affichage	Trois boutons sont disponibles près de l'affichage de l'IMD : un bouton Précédent, un bouton Suivant et un bouton central. Les fonctions de ces boutons sont décrites au **Tableau 5.4** ci-dessous.
6	Voies des capteurs distants	Voie RJ-12 pour la connexion de capteurs numériques distants plug-and-play Vertiv™ (vendus séparément). Chaque capteur numérique a un numéro de série unique et est automatiquement détecté. Les PDU surveillées au niveau de l'unité prennent en charge jusqu'à 16 capteurs. Un convertisseur Vertiv™ A2D peut être ajouté en option pour la prise en charge de la détection analogique. Un adaptateur SN-ADAPTER peut être ajouté en option pour la prise en charge des capteurs intégrés et modulaires Liebert. Pour plus d'informations, reportez-vous à la section Capteurs disponibles à la page 121.
7	Voie série	RS-232 via la voie RJ-45.
8	Voie USB	Voie USB utilisée pour charger le firmware, sauvegarder/restaurer la configuration des dispositifs, augmenter la capacité de journalisation via un dispositif de stockage USB ou prendre en charge les adaptateurs USB sans fil TP-Link. La voie USB doit être activée – reportez-vous à la section USB à la page 88. Fournit une capacité de puissance allant jusqu'à 100 mA pour les dispositifs connectés par USB.

REMARQUE : la connexion série ne prend pas en charge le contrôle du flux.

Tableau 5.4 Fonctions des boutons de l'affichage

Bouton	Symbole	Description
Bouton Précédent		Appuyez sur ce bouton pour revenir au canal précédent. Maintenez ce bouton enfoncé pendant 3 secondes pour lancer une sauvegarde de la configuration. L'écran affiche le message **bcup** pendant la création de la sauvegarde et revient ensuite au mode de fonctionnement normal. La sauvegarde est stockée sur des dispositifs de stockage USB disponibles. En leur absence, l'opération n'a aucun effet.
Bouton Suivant		Appuyez sur ce bouton pour passer au canal suivant. Maintenez ce bouton enfoncé pendant 3 secondes pour lancer une restauration de la configuration. L'écran affiche le message **load**, suivi du message **conf**, puis d'un compte à rebours de 3 secondes. À l'expiration du compte à rebours, le message **8888** s'affiche et la sauvegarde est appliquée. La sauvegarde est lue à partir de dispositifs de stockage USB. Si le bouton est relâché au cours de cette séquence, la restauration est abandonnée. Une fois la sauvegarde appliquée, s'il n'y a aucune image de sauvegarde ou si aucun dispositif de stockage USB n'est connecté, l'écran revient au mode de fonctionnement normal.

Tableau 5.4 Fonctions des boutons de l'affichage (suite)

Bouton	Symbole	Description
Bouton central		Bascule entre les modes de défilement et d'affichage statique. En maintenant ce bouton enfoncé pendant 3 secondes, vous lancerez une séquence de réinitialisation des paramètres. Cette séquence se compose d'un message **rset**, suivi d'un message **dflt**, puis d'un compte à rebours de 3 secondes. À l'expiration du compte à rebours, le message **8888** s'affiche. Les valeurs par défaut du réseau, des comptes utilisateur *http* et des informations *LDAP/RADIUS* sont rétablies. Si le bouton est relâché au cours de cette séquence, la réinitialisation est abandonnée.
Boutons Précédent et Suivant		En appuyant sur les deux boutons simultanément, vous inverserez l'affichage de 180 degrés.
Boutons Précédent et central		En appuyant sur les deux boutons simultanément, vous afficherez l'adresse IPv4 principale de l'unité.

5.1.4 Niveau d'unité commutée et niveau de prise commutée

Les versions antérieures des rPDU Vertiv™ PowerIT avec surveillance au niveau des unités commutées, surveillance au niveau des prises et surveillance au niveau des prises commutées étaient fournies avec le module IMD-3E-G.

Figure 5.3 Module IMD-3E-G

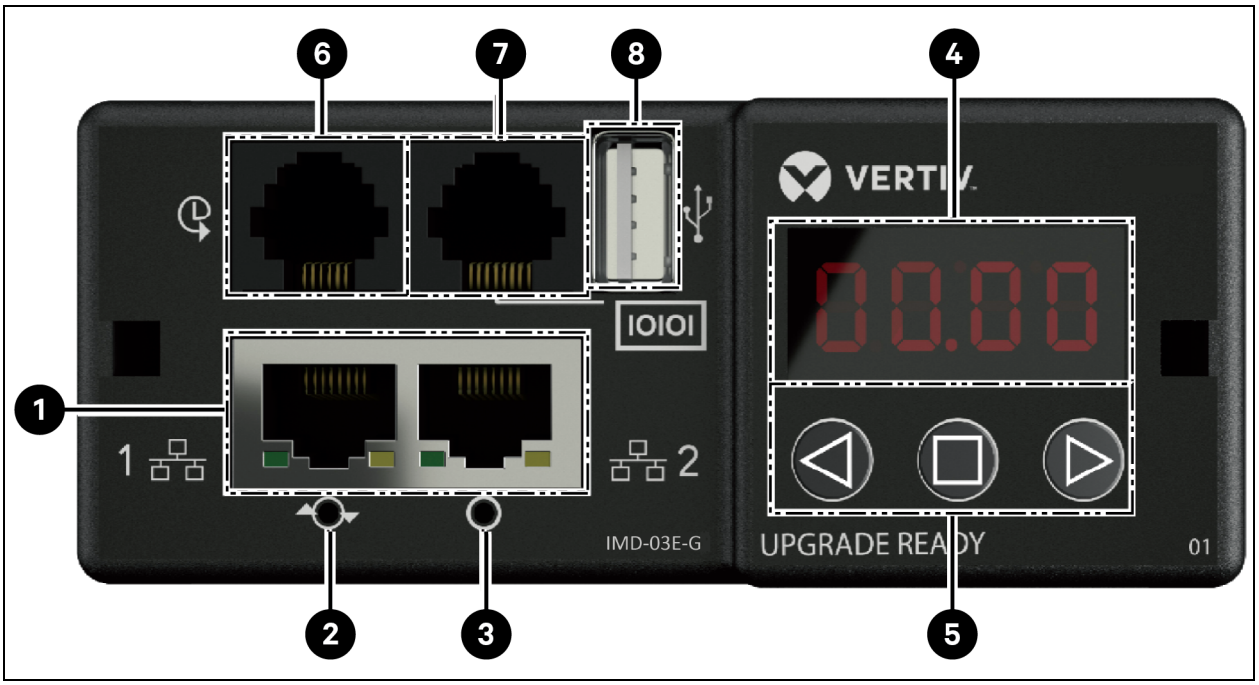


Tableau 5.5 Description du module IMD-3E-G

Numéro	Nom	Description
1	Deux voies Ethernet	Les deux voies Ethernet fonctionnent comme un commutateur Ethernet à deux voies, permettant la connexion en cascade de plusieurs dispositifs. Les deux voies Ethernet peuvent être des interfaces réseau Ethernet doubles configurées indépendamment, permettant à la rPDU de se connecter à deux réseaux différents.
2	Bouton de redémarrage forcé	En appuyant sur le bouton de redémarrage forcé, vous redémarrez l'IMD. Cela a pour effet de redémarrer l'IMD, aucune information utilisateur n'est modifiée ni supprimée.
3	Bouton de réinitialisation du réseau	En maintenant le bouton de réinitialisation du réseau enfoncé pendant 5 secondes en mode de fonctionnement normal, vous restaurerez l'adresse IP par défaut et réinitialiserez les comptes utilisateur.
4	Affichage local	L'affichage local indique les valeurs du courant de phase, de ligne et de circuit (en ampères).
5	Boutons de l'affichage	Trois boutons sont disponibles près de l'affichage de l'IMD : un bouton Précédent, un bouton Suivant et un bouton central. Les fonctions de ces boutons sont décrites à la section Fonctions des boutons de l'affichage sur la page suivante.
6	Voies des capteurs distants	Voie RJ-12 pour la connexion de capteurs numériques distants Vertiv plug-and-play (vendus séparément). Chaque capteur numérique a un numéro de série unique et est automatiquement détecté. Les PDU à prises surveillées et commutées prennent en charge jusqu'à 16 capteurs. Un convertisseur Vertiv™ A2D peut être ajouté en option pour la prise en charge de la détection analogique. Un adaptateur SN-ADAPTER peut être ajouté en option pour la prise en charge des capteurs intégrés et modulaires Liebert. Pour plus d'informations, reportez-vous à la section Capteurs disponibles à la page 121.
7	Voie série	RS-232 via la voie RJ-45.
8	Voie USB	Voie USB utilisée pour charger le firmware, sauvegarder/restaurer la configuration des dispositifs, augmenter la capacité de journalisation via un dispositif de stockage USB ou prendre en charge les adaptateurs USB sans fil TP-Link. La voie USB doit être activée – reportez-vous à la section USB à la page 88. Fournit une capacité de puissance allant jusqu'à 100 mA pour les dispositifs connectés par USB.

REMARQUE : les dispositifs MSC USB tels que des clés USB ou des disques durs externes sont pris en charge. Les dispositifs de stockage USB doivent être formatés en FAT32.

REMARQUE : la connexion série ne prend pas en charge le contrôle du flux.

Boutons de l'affichage

Trois boutons sont disponibles près de l'affichage de l'IMD : un bouton Précédent, un bouton Suivant et un bouton central. Les fonctions de ces boutons sont décrites dans le tableau suivant.

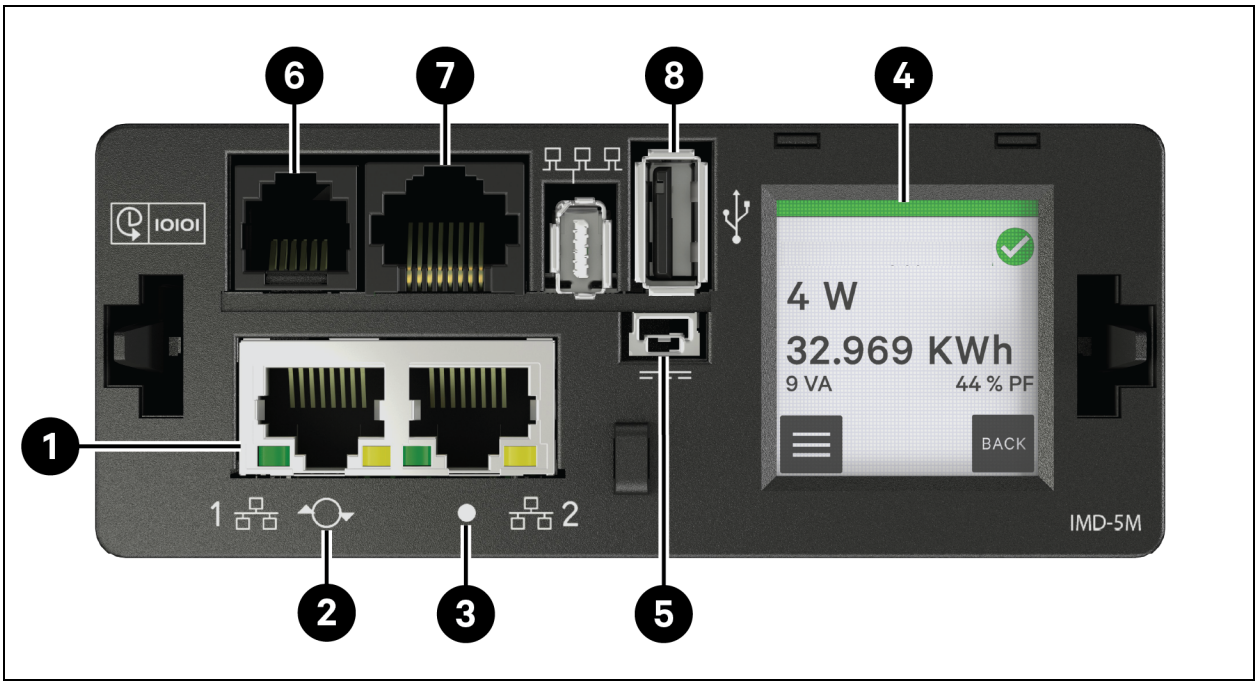
Tableau 5.6 Fonctions des boutons de l'affichage

Bouton	Symbole	Description
Bouton Précédent		Appuyez sur ce bouton pour revenir au canal précédent. Maintenez ce bouton enfoncé pendant 3 secondes pour lancer une sauvegarde de la configuration. L'écran affiche le message **bcup** pendant la création de la sauvegarde et revient ensuite au mode de fonctionnement normal. La sauvegarde est stockée sur des dispositifs de stockage USB disponibles. En leur absence, l'opération n'a aucun effet.
Bouton Suivant		Appuyez sur ce bouton pour passer au canal suivant. Maintenez ce bouton enfoncé pendant 3 secondes pour lancer une restauration de la configuration. L'écran affiche le message **load**, suivi du message **conf**, puis d'un compte à rebours de 3 secondes. À l'expiration du compte à rebours, le message **8888** s'affiche et la sauvegarde est appliquée. La sauvegarde est lue à partir de dispositifs de stockage USB. Si le bouton est relâché au cours de cette séquence, la restauration est abandonnée. Une fois la sauvegarde appliquée, s'il n'y a aucune image de sauvegarde ou si aucun dispositif de stockage USB n'est connecté, l'écran revient au mode de fonctionnement normal.
Bouton central		Bascule entre les modes de défilement et d'affichage statique. En maintenant ce bouton enfoncé pendant 3 secondes, vous lancerez une séquence de réinitialisation des paramètres. Cette séquence se compose d'un message **rset**, suivi d'un message **dflt**, puis d'un compte à rebours de 3 secondes. À l'expiration du compte à rebours, le message **8888** s'affiche et les valeurs par défaut du réseau, des comptes utilisateur et des informations http et LDAP/RADIUS sont rétablies. Si le bouton est relâché au cours de cette séquence, la réinitialisation est abandonnée.
Boutons Précédent et Suivant		En appuyant sur les deux boutons simultanément, vous inverserez l'affichage de 180 degrés.
Boutons Précédent et central		En appuyant sur les deux boutons simultanément, vous afficherez l'adresse IPv4 principale de l'unité.

5.1.5 Surveillance et commutation (IMD-5M)

Toutes les rPDU Vertiv™ PowerIT surveillées et commutées sont expédiées avec le module IMD-5M.

Figure 5.4 Module IMD-5M



Élément	Nom	Description
1	Deux voies Ethernet	Les deux voies Ethernet fonctionnent comme un commutateur Ethernet à deux voies, permettant la connexion en cascade de plusieurs dispositifs. Les deux voies Ethernet peuvent être des interfaces réseau Ethernet doubles configurées indépendamment, permettant à la rPDU de se connecter à deux réseaux différents.
2	Bouton Redémarrer/Réintialiser	Appuyez sur le bouton pendant 10 secondes pour redémarrer l'IMD. Cela a pour effet de redémarrer l'IMD, aucune information utilisateur n'est modifiée ni supprimée. En maintenant le bouton de réinitialisation du réseau enfoncé pendant 25 secondes en mode de fonctionnement normal, vous restaurerez l'adresse IP par défaut et réinitialiserez les comptes utilisateur.
3	LED d'état RVB	LED verte : l'unité est opérationnelle. LED jaune : l'unité démarre.
4	Menu sur l'écran tactile	Utilisez le menu sur l'écran tactile pour rechercher les valeurs de courant de phase, de ligne et de circuit (en ampères).
5	Entrée d'alimentation redondante	L'alimentation redondante ne fonctionnera pas avec les anciennes rPDU évolutives de base et à compteur, ni avec les rPDU surveillées par unité mises à niveau avec l'IMD-5M.

Élément	Nom	Description
6	Voies des capteurs distants	Voie RJ-12 pour la connexion de capteurs numériques distants plug-and-play Vertiv™ (vendus séparément). Chaque capteur numérique a un numéro de série unique et est automatiquement détecté. Les PDU surveillées et commutées prennent en charge jusqu'à 16 capteurs. Un convertisseur Vertiv™ A2D peut être ajouté en option pour la prise en charge de la détection analogique. Un adaptateur SN-ADAPTER peut être ajouté en option pour la prise en charge des capteurs intégrés et modulaires Liebert®. Pour plus d'informations, reportez-vous à la section Capteurs disponibles à la page 121.
7	Voie série	RS-232 via la voie RJ-45.
8	Voie USB	Voie USB utilisée pour charger le firmware, sauvegarder/restaurer la configuration des dispositifs, augmenter la capacité de journalisation via un dispositif de stockage USB ou prendre en charge les adaptateurs USB sans fil TP-Link. La voie USB doit être activée – reportez-vous à la section USB à la page 88. Fournit jusqu'à 0,5 watt pour le niveau surveillé de l'unité et 5 watts pour le niveau de prise surveillée/niveau d'unité commutée/niveau de prise commutée.

REMARQUE : la connexion série ne prend pas en charge le contrôle du flux.

Flux de travail du menu sur l'écran tactile

Chaque section est composée d'un ou plusieurs groupes de pages, chaque groupe de pages contenant une ou plusieurs pages. La plupart des pages comportent des boutons Accueil, Entrée et Suivant. Les seules exceptions sont l'écran de démarrage, la page d'accueil, les pages affichées lors de la mise à jour du firmware et les pages momentanément affichées confirmant les résultats d'une opération. Le bouton Home permet d'accéder à la page d'accueil. Le bouton Enter permet d'accéder à la page suivante du groupe de pages. Si vous vous trouvez sur la dernière page du groupe de pages, la navigation se fait vers la première page du groupe de pages. Le bouton Next permet d'accéder à la première page du groupe de pages suivant. Si vous vous trouvez sur le dernier groupe de pages, la navigation se fait vers le premier groupe de pages.

La ligne supérieure de chaque page comprend le libellé du système sur un fond vert, jaune ou rouge indiquant l'alarme non confirmée de priorité la plus élevée, ainsi qu'une icône indiquant elle aussi l'état d'alarme. De plus, la mesure d'alarme est affichée en jaune ou en rouge.

Page d'accueil

La page d'accueil comporte des liens vers les trois sections suivantes :

- System
- Devices
- Alarms

La page d'accueil est la seule page sans boutons de navigation Accueil, Suivant et Entrée.

Figure 5.5 Flux de travail du menu sur l’écran tactile

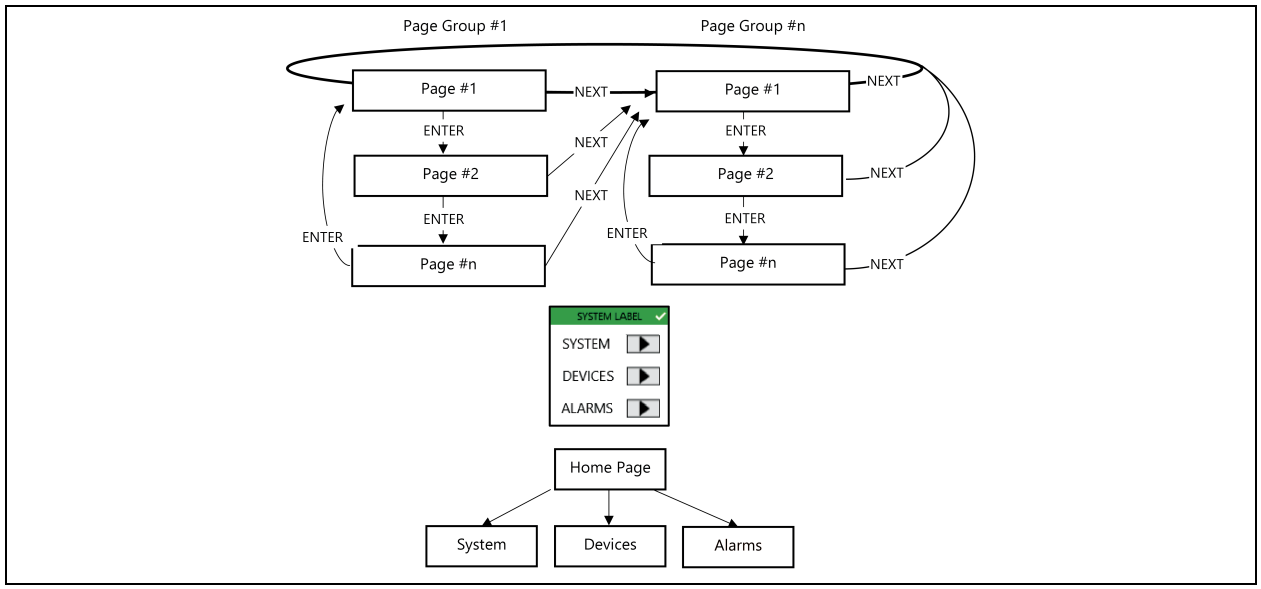


Figure 5.6 Section System

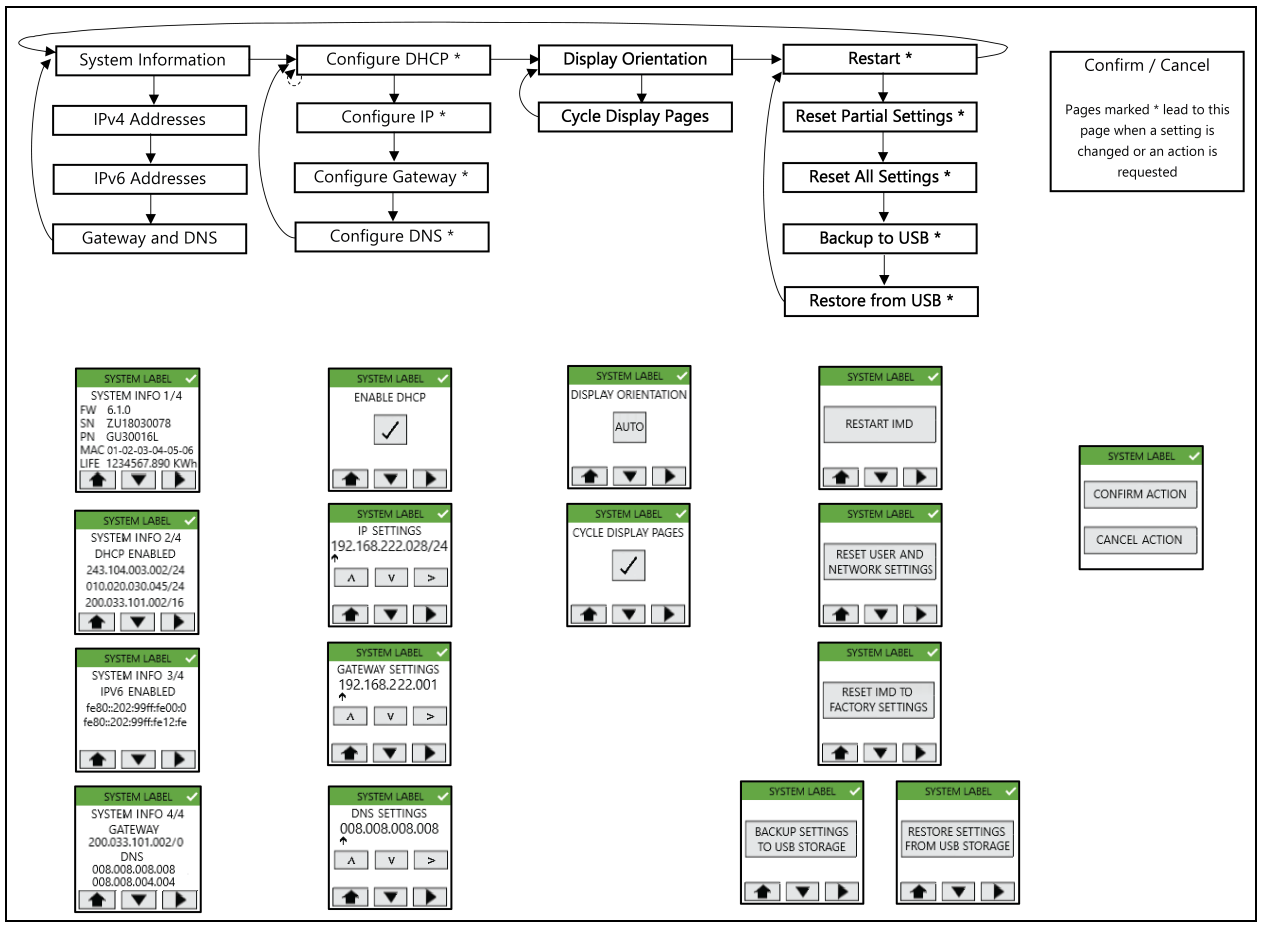


Figure 5.7 Section Device

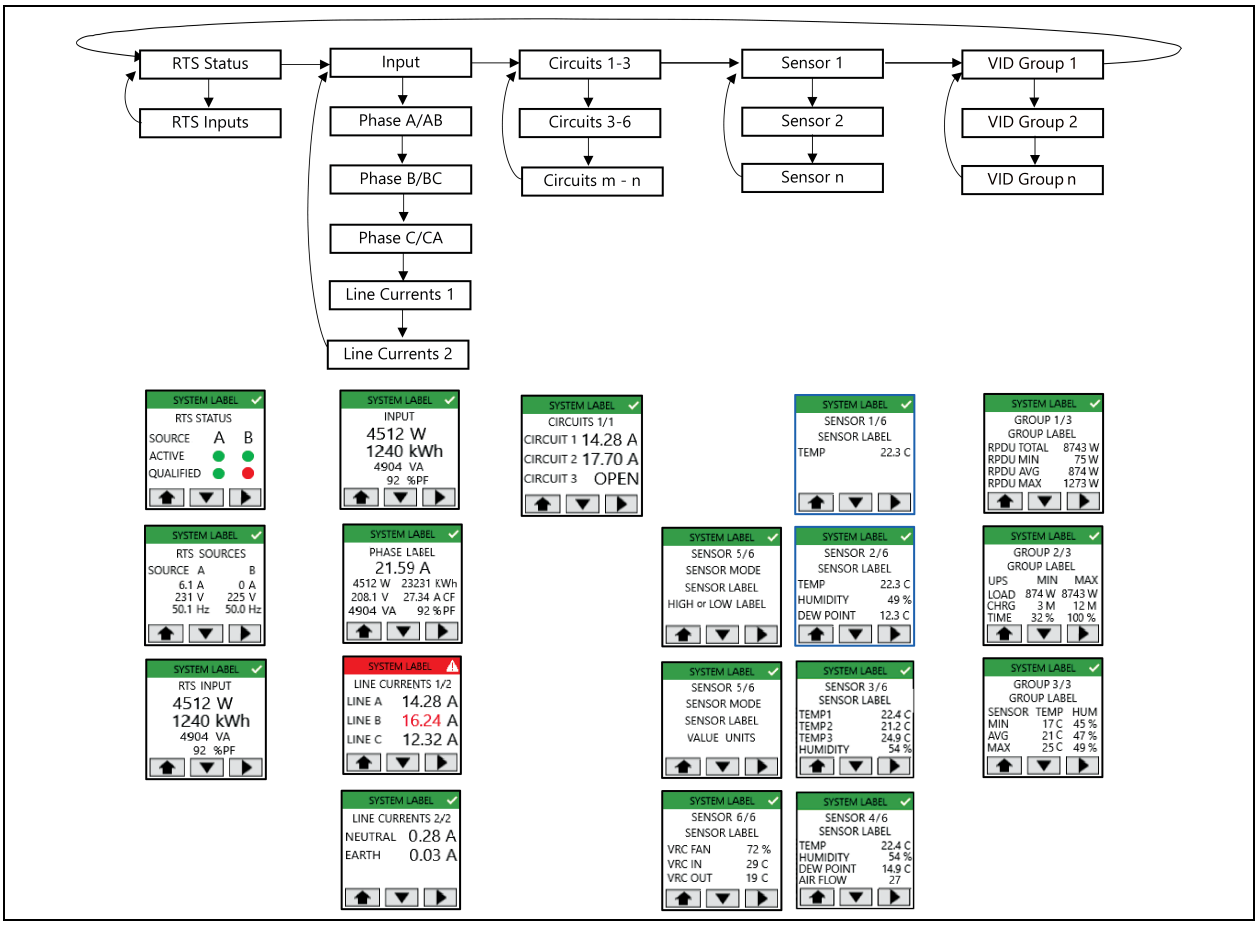
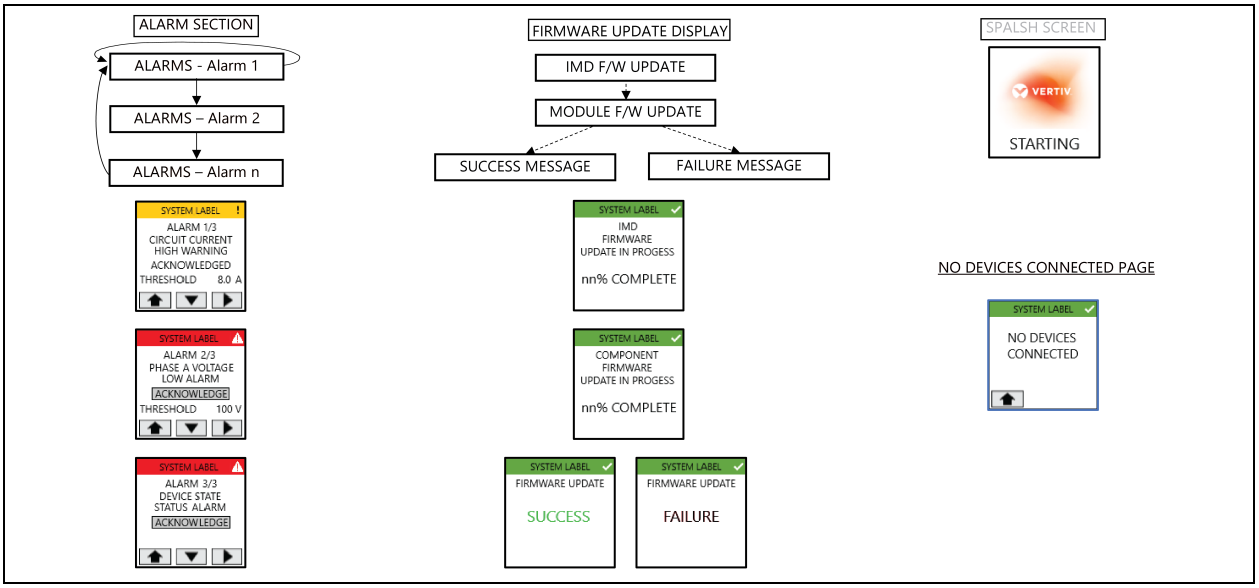


Figure 5.8 Section Alarm et affichage des mises à jour du firmware



Fonctionnalités du menu sur l'écran tactile

- La page de l'écran de démarrage s'affiche lors de l'initialisation de l'IMD.
- La page par défaut s'affiche après la mise sous tension ou après un délai d'inactivité de 60 secondes dans le menu de l'écran tactile. Elle est déterminée en fonction du type de dispositif :
  - RTS : page d'état du RTS
  - PDU en rack : page de saisie
  - RDU202 : page du Capteur 1
- Le rétroéclairage de l'écran est réduit au bout de 75 secondes d'inactivité du menu de l'écran tactile.
- Dans la plupart des cas, les noms sont affichés. Le libellé du système défile pour s'afficher en intégralité. D'autres libellés peuvent être tronqués s'ils dépassent 10 caractères.
- Chaque ligne d'en-tête de page aura un fond de couleur verte, orange ou rouge indiquant l'état d'alarme active (non confirmée) de priorité la plus élevée, ainsi qu'une icône indiquant les états d'avertissement et d'alarme.
- Le point coloré de la page de la prise indique l'état de la prise (vert = activée, rouge = désactivée) avec les PDU en rack à prises commutées. Aucun point n'est affiché lorsque la rPDU n'est pas à prises commutées.
- Les pages de paramètres IP font uniquement référence aux paramètres IPv4 et la configuration de l'adresse IP configure uniquement la première adresse IP et l'adresse DNS.
- Lorsque DHCP est activé, les pages de configuration de l'adresse IP, de la passerelle et de l'adresse DNS ne s'affichent pas.
- La coche de la page DHCP apparaît/disparaît lorsque vous appuyez sur le bouton pour indiquer l'option sélectionnée.
- L'écran de mise à jour du firmware s'affiche dès lors que commence une mise à jour du firmware, quelle que soit la source (interface utilisateur Web, interface de ligne de commande, API, SCP, USB). Le pourcentage de progression de la mise à jour du firmware des composants est calculé comme suit : (cartes mises à jour à ce stade) / (nombre total de cartes à mettre à jour) * 100.
- Une fois toutes les mises à jour de firmware terminées, la page Firmware Update Success ou Firmware Update Failure s'affiche pendant 15 secondes. La page par défaut s'affiche ensuite.
- Lors de la mise à jour du firmware, le rétroéclairage de l'écran est réglé sur une intensité de 100 %. Une fois la mise à jour terminée, le rétroéclairage de l'écran est réduit au bout de 75 secondes d'inactivité du menu de l'écran tactile.
- Seules les trois premières adresses IPv4 et/ou IPv6 sont affichées. Les adresses sont affichées dans le groupe de pages System Information.
- Une action en attente, telle que l'attente de la confirmation d'une action ou de la confirmation de l'adresse IP saisie, sera annulée par un événement asynchrone comme l'expiration d'un délai d'affichage (voir La page par défaut s'affiche après la mise sous tension ou après un délai d'inactivité de 60 secondes dans le menu de l'écran tactile. Elle est déterminée en fonction du type de dispositif : ci-dessus) ou une mise à jour du firmware.
- En appuyant sur n'importe quel bouton de navigation après avoir apporté des modifications à DHCP, à l'adresse IP, à la passerelle ou à la configuration DNS, une page d'action de confirmation/annulation s'affiche. L'option Confirm active la modification et renvoie à la page précédente, qui affiche les paramètres modifiés. L'option Cancel annule la modification et renvoie à la page précédente, qui affiche les paramètres inchangés.
- Lorsque l'option Cycle Display Pages est sélectionnée, l'affichage par défaut parcourt les pages du groupe de pages du dispositif, affichant chaque page pendant 5 secondes. Par exemple, l'activation du défilement des pages d'affichage pour une PDU en rack entraînera le défilement de l'affichage sur les pages d'entrée, de phase et de ligne.
- Lorsqu'un groupe VID comprend plusieurs types de dispositifs (par exemple, PDU en rack et ASI), une page de groupe VID s'affiche pour chaque type de dispositif au sein du groupe.

- Le lien Alarms de la page d'accueil ne s'affiche que lorsqu'une alarme a été déclenchée.
- Les alarmes peuvent être confirmées à l'aide du bouton Acknowledge dont le libellé change en Acknowledged une fois activé.
- La page Display Orientation permet de choisir parmi les options d'orientation de l'affichage : automatique, 0 degré, 90 degrés, 180 degrés et 270 degrés lorsque vous appuyez sur le bouton (après le réglage de 270 degrés, l'affichage revient sur automatique). L'action est instantanée suite à la pression sur le bouton.
- Lorsqu'une action Restart, Reset User/Network, Factory Reset, Backup ou Restore est sélectionnée, une page Confirm/Cancel s'affiche. Si elle est confirmée, l'action se poursuit ; si elle est annulée, l'affichage revient à la page précédemment affichée. Une fois qu'une action Reset User/Network, Factory Reset, Backup ou Restore est effectuée, la page Action Completed s'affiche pendant 5 secondes, puis le menu de l'écran tactile revient à la page par défaut.
- La page No Devices Connected doit remplacer la page de menu par défaut de l'écran tactile (ou les pages de menu de défilement de l'écran tactile par défaut) lorsqu'aucune branche api/dev à l'état normal n'est détectée.
- Lors de la sélection d'une action de groupe de pages utilitaires (telle que Restart), une page de confirmation/d'annulation de l'action s'affiche. L'option Confirm active l'action et renvoie à la page d'accueil. L'option Cancel annule l'action et renvoie à la page précédemment affichée.

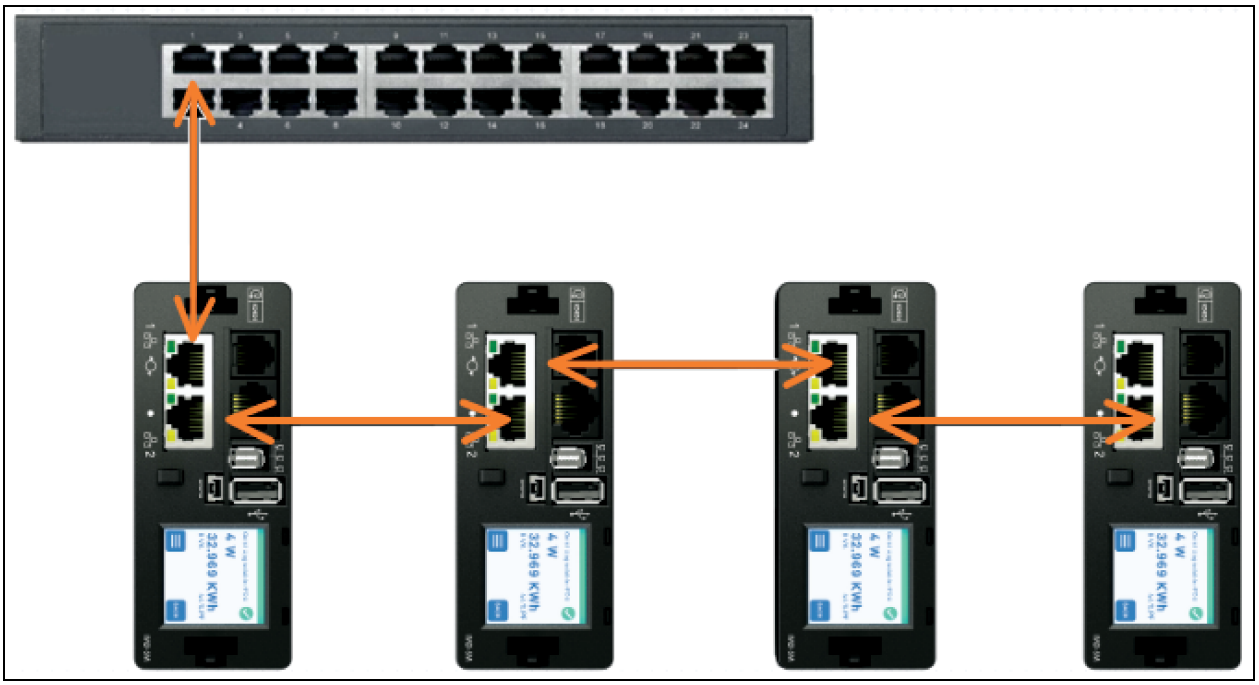
5.1.6 Rapid Spanning Tree Protocol (RSTP)

Les dispositifs surveillés évolutifs, construits avec l'IMD-5M, comportent deux voies Ethernet qui fonctionnent ensemble comme un pont Ethernet interne. Une de ces voies peut être utilisée pour connecter l'IMD à un réseau existant ou les deux voies peuvent être utilisées en même temps pour connecter un IMD à un autre dans une configuration en cascade.

Connexion en cascade

- Utilisez la connexion en cascade pour réduire le nombre de voies du commutateur réseau.
- Les PDU en rack sont connectées via une connexion Ethernet en cascade.
- La première PDU en rack de la connexion en cascade se connecte à une voie de commutateur réseau.
- Chaque PDU en rack possède sa propre adresse IP unique.

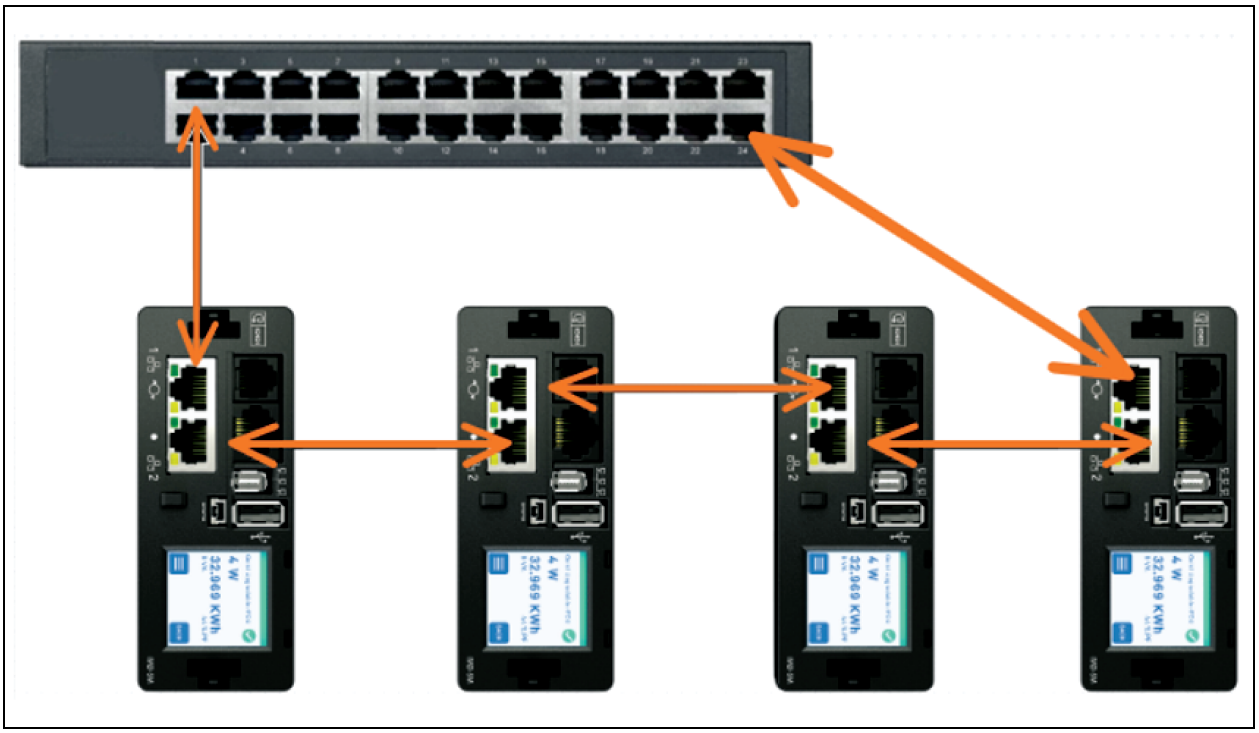
Figure 5.9 Connexion en cascade



Connexion en cascade tolérante aux pannes

- Utilisez la connexion en cascade tolérante aux pannes pour fournir une connectivité réseau résiliente.
- Les PDU en rack sont connectées via une connexion Ethernet en cascade.
- La première et la dernière PDU en rack de la connexion en cascade se connectent aux voies du commutateur réseau.
- Chaque PDU en rack possède sa propre adresse IP unique.
- Le protocole Rapid Spanning Tree (RSTP) doit être configuré pour gérer la tolérance aux pannes et maintenir la connectivité en cas de panne de câble ou de perte d'alimentation de la PDU en rack.

Figure 5.10 Connexion en cascade tolérante aux pannes



Lorsque les deux interfaces réseau sont connectées, l'IMD implémente un protocole de création de ponts réseau appelé Rapid Spanning Tree Protocol (RSTP). Le protocole RSTP est une norme IEEE implémentée par tous les ponts gérés. En utilisant le protocole RSTP, les ponts du réseau échangent des informations pour trouver des chemins ou des boucles redondants. IPv6 doit être désactivé lors de l'utilisation d'une connexion réseau redondante.

Quand une boucle est détectée, les ponts du réseau fonctionnent ensemble pour désactiver temporairement les chemins redondants. Cela permet au réseau d'éviter les tempêtes de diffusion causées par les boucles. En outre, le protocole RSTP vérifie régulièrement les modifications de la topologie du réseau. En cas de perte d'une connexion, le protocole RSTP permet aux ponts de basculer rapidement vers un chemin redondant.

REMARQUE : le protocole RSTP impose une limite de 40 liaisons entre les ponts, notamment les IMD.

REMARQUE : Vertiv Intelligence Director ne peut pas être utilisé conjointement avec RSTP et une connexion réseau redondante.

5.2 Configuration du réseau

L'IMD évolutif a une adresse IP par défaut pour la configuration et l'accès initiaux.

Pour rétablir l'adresse IP par défaut et réinitialiser toutes les informations du compte utilisateur pour l'IMD-5M :

1. Si vous maintenez le bouton RESET/RESTART (premier trou de broche) situé à côté de l'affichage ACL pendant 25 secondes, vous réinitialiserez les informations relatives au réseau et au compte utilisateur.
2. Si vous maintenez le bouton RESET/RESTART (premier trou de broche) situé à côté de l'affichage ACL pendant 10 secondes, vous mettez l'IMD hors tension puis à nouveau sous tension sans modifier aucune information utilisateur.

La page Network, située dans l'onglet System, vous permet d'affecter manuellement les propriétés réseau ou d'utiliser le protocole DHCP pour vous connecter à votre réseau. Vous devez connaître l'adresse IP pour pouvoir accéder à l'unité. Il est recommandé d'utiliser une adresse IP statique ou une adresse DHCP réservée. L'adresse par défaut est affichée sur la face avant de l'unité.

- IP Address : *192 168 123 123*
- Masque de sous-réseau : *255.255.255.0*
- Passerelle : *192.168.123.1*

Pour accéder à l'unité pour la première fois, vous devez modifier temporairement les paramètres réseau de votre ordinateur de sorte qu'ils correspondent au sous-réseau 192.168.123. xxx. Pour configurer l'unité, connectez-la à la voie Ethernet de votre ordinateur, puis suivez les instructions appropriées pour le système d'exploitation de votre ordinateur.

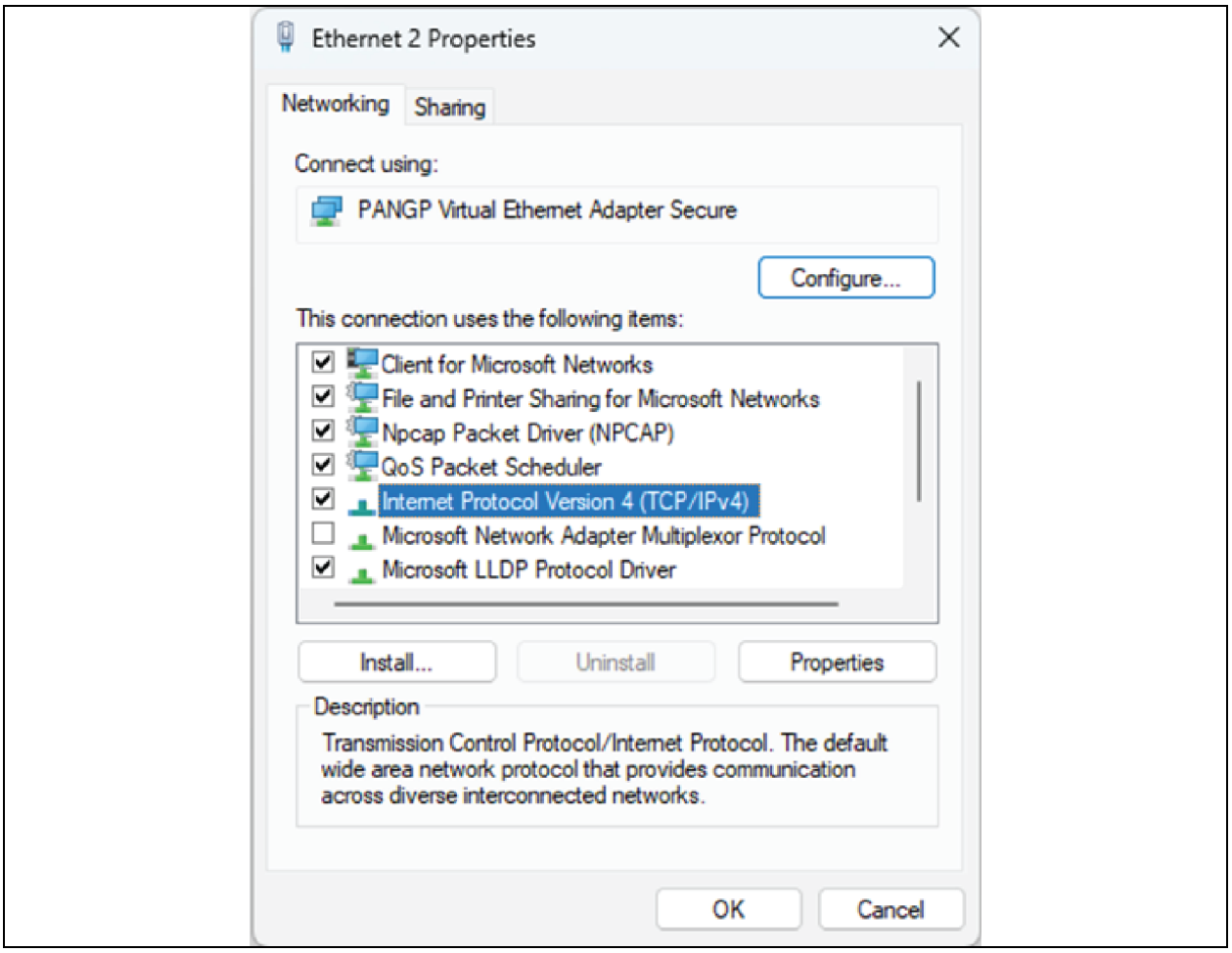
Pour configurer le réseau pour un système d'exploitation Windows :

1. Accédez aux paramètres réseau de votre système d'exploitation.
   - Windows Server 2022 et 2019.
   - Sous Microsoft Windows 10, cliquez sur *Start>Network and Internet>Change Adapter Settings*.
   - Sous Microsoft Windows 11, cliquez sur *Start>Network and Internet>Change Adapter Settings*.
2. Recherchez l'entrée correspondant à la carte réseau (NIC) sous LAN, High Speed Internet ou Local Area Connection. Double-cliquez sur l'entrée de la carte réseau dans la liste Network Connections.

REMARQUE : la plupart des ordinateurs possèdent une seule carte réseau Ethernet, mais un adaptateur de données cellulaires ou Wi-Fi apparaît également comme une carte réseau dans cette liste. Assurez-vous de choisir l'entrée correcte.

3. Cliquez sur *Properties* pour afficher la fenêtre Local Properties.

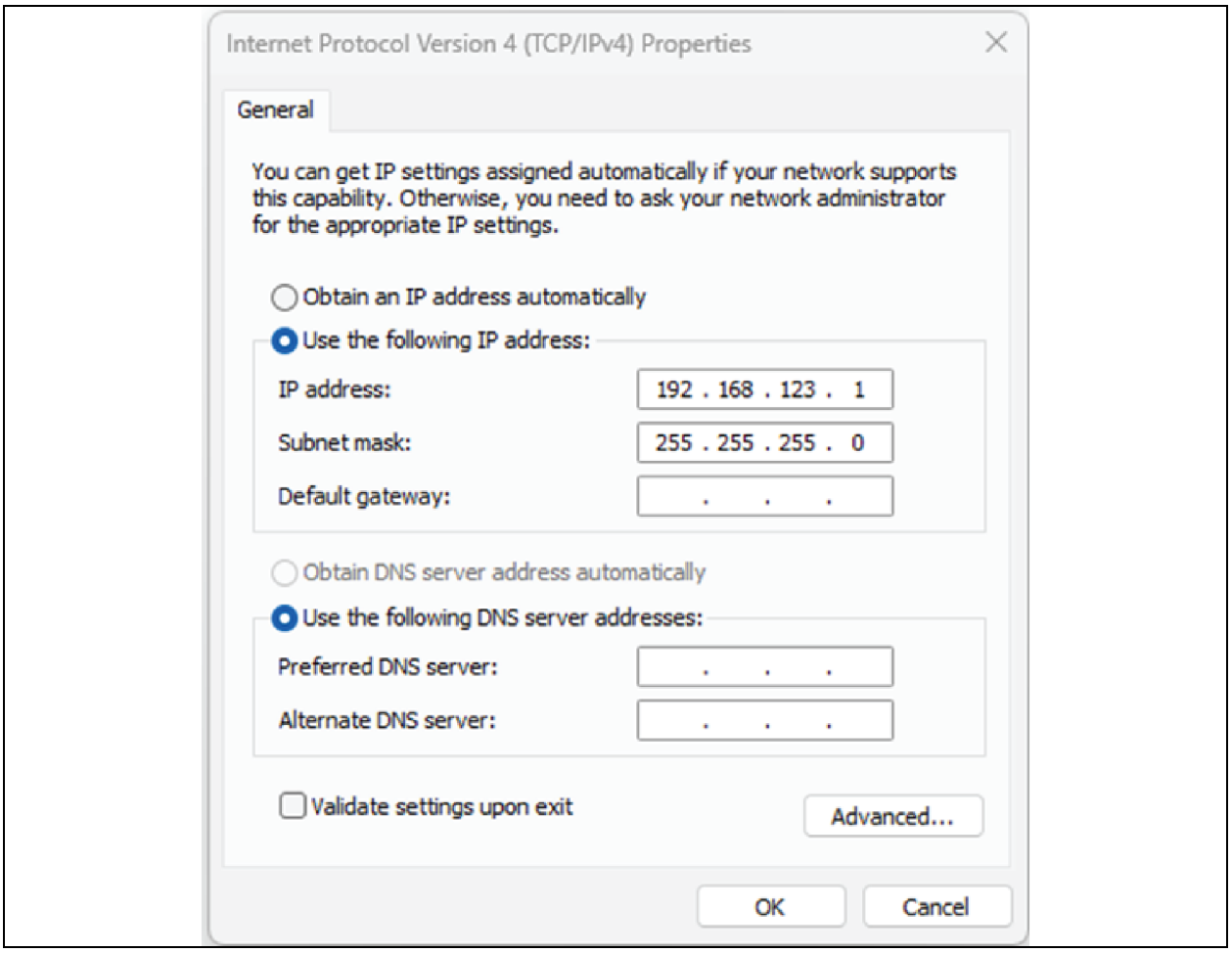
Figure 5.11 Propriétés de la connexion au réseau local



4. Sélectionnez *Internet Protocol Version 4 (TCP/IPv4)* dans la liste, puis cliquez sur *Properties*.

REMARQUE : si vous voyez plus d'une entrée TCP/IP, comme dans l'exemple ci-dessus, l'ordinateur peut être configuré pour la prise en charge des protocoles IPv6 et IPv4. Veillez à sélectionner l'entrée correspondant au protocole IPv4. Notez les paramètres actuels de la carte réseau afin de pouvoir les rétablir une fois la procédure de configuration terminée.

Figure 5.12 Protocole Internet Version 4



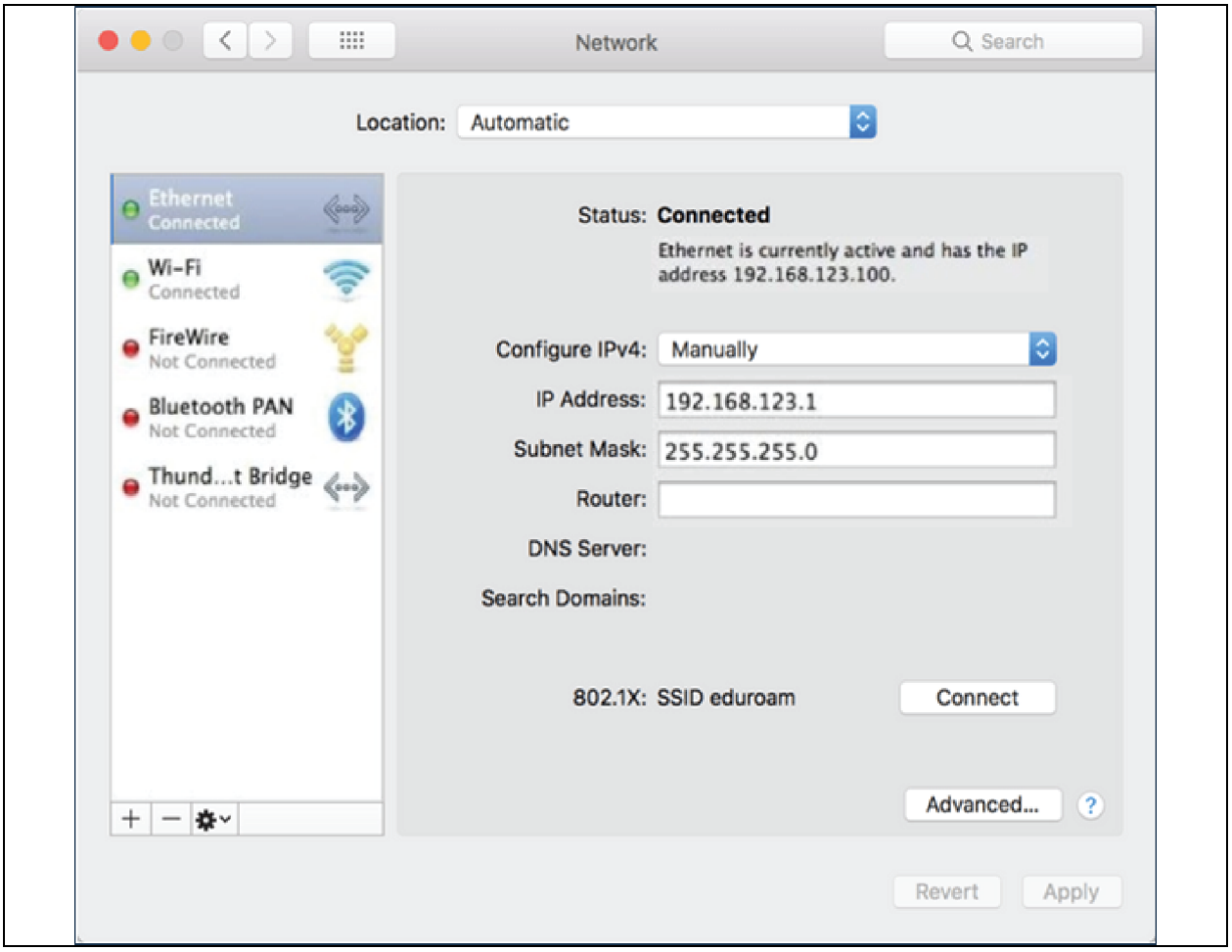
5. Choisissez *Use the following IP address*, renseignez le champ IP address par **192.168.123.1** et le champ Subnet Mask par **255.255.255.0**. Pour la configuration initiale, les entrées Default Gateway et DNS Server peuvent rester vides. Sélectionnez *OK* - *OK* pour fermer les fenêtres Internet Protocol Properties et Local Properties.
6. Dans un navigateur Web, saisissez **http://192.168.123.123** pour accéder à l'unité. Si vous configurez l'unité pour la première fois, l'unité vous invite à créer un compte administrateur et un mot de passe avant de pouvoir continuer.
7. Une fois le compte administrateur créé, connectez-vous à l'unité.
8. Par défaut, la page des capteurs par défaut s'affiche. Accédez à l'onglet *System*, puis à la page *Network* pour configurer les propriétés réseau du dispositif. L'adresse IP, le masque de sous-réseau, la passerelle et les paramètres DNS de l'unité peuvent être affectés manuellement ou obtenus via DHCP.
9. Cliquez sur *Save*.

REMARQUE : une fois les modifications enregistrées, le navigateur ne pourra plus recharger la page Web à partir de l'adresse 192.168.123.123 et affichera le message Page not Found ou Host Unavailable. C'est normal. Une fois que vous avez terminé de configurer l'adresse IP de l'unité, répétez les étapes ci-dessus, en remplaçant les paramètres de la carte réseau Ethernet de l'ordinateur par ceux que vous avez notés avant de les modifier.

Pour configurer le réseau pour un MAC :

1. Cliquez sur l'icône System Preferences sur la station, puis choisissez *Network*.

Figure 5.13 Préférences système MAC



2. Assurez-vous que l'entrée Ethernet est mise en surbrillance sur le côté gauche de la fenêtre de la carte réseau. Dans la plupart des cas, il y aura une seule entrée Ethernet sur un Mac. Notez les paramètres actuels afin de pouvoir les rétablir une fois la procédure de configuration terminée.
3. Sélectionnez *Manually* dans la liste déroulante Configure IPv4, puis renseignez le champ IP address par **192.168.123.1** et le champ Subnet Mask par **255.255.255.0**, puis cliquez sur *Apply*.

REMARQUE : les paramètres du routeur et du serveur DNS peuvent être laissés vides pour cette configuration initiale. Dans un navigateur Web, saisissez http://192.168.123.123 pour accéder à l'unité. Si vous configurez l'unité pour la première fois, l'unité vous invite à créer un compte administrateur et un mot de passe avant de pouvoir continuer.

4. Une fois le compte administrateur créé, connectez-vous à l'unité.
5. Par défaut, la page des capteurs par défaut s'affiche. Accédez à l'onglet *System*, puis à la page *Network* pour configurer les propriétés réseau du dispositif. L'adresse IP, le masque de sous-réseau, la passerelle et les paramètres DNS de l'unité peuvent être affectés manuellement ou obtenus via DHCP.
6. Cliquez sur *Save*.

REMARQUE : une fois les modifications enregistrées, le navigateur ne pourra plus recharger la page Web à partir de l'adresse 192.168.123.123 et affichera le message Page not Found ou Host Unavailable. C'est normal. Une fois que vous avez terminé de configurer l'adresse IP de l'unité, répétez les étapes ci-dessus, en remplaçant les paramètres de la carte réseau Ethernet de l'ordinateur par ceux que vous avez notés avant de les modifier.

5.3 Interface utilisateur Web

L'unité est accessible via une connexion HTTP standard non chiffrée ainsi qu'une connexion HTTPS (TLS) chiffrée. Les unités seront par défaut redirigées de HTTP vers HTTPS, sauf si l'administrateur active explicitement HTTP.

REMARQUE : un compte administrateur (nom d'utilisateur et mot de passe) doit être créé lors de la première connexion au dispositif.

REMARQUE : si Clock not set. s'affiche dans le coin inférieur droit de la page, suivez les procédures décrites à la section Time à la page 87.

REMARQUE : le taux d'actualisation des données de l'interface Web est de 5 secondes. À ne pas confondre avec les calculs du compteur d'énergie en continu et les notifications d'alarme instantanées.

5.3.1 Menu principal

Le menu principal est situé verticalement à l'extrémité gauche. Reportez-vous à la Figure 5.14 sur la page suivante, pour voir le menu principal.

AVERTISSEMENT ! Ne raccordez pas de radiateurs électriques, d'appareils de chauffage électrique ou tout autre appareil électrique susceptible de provoquer un incendie, un choc électrique ou des blessures en cas de fonctionnement sans surveillance.

Figure 5.14 Menu principal

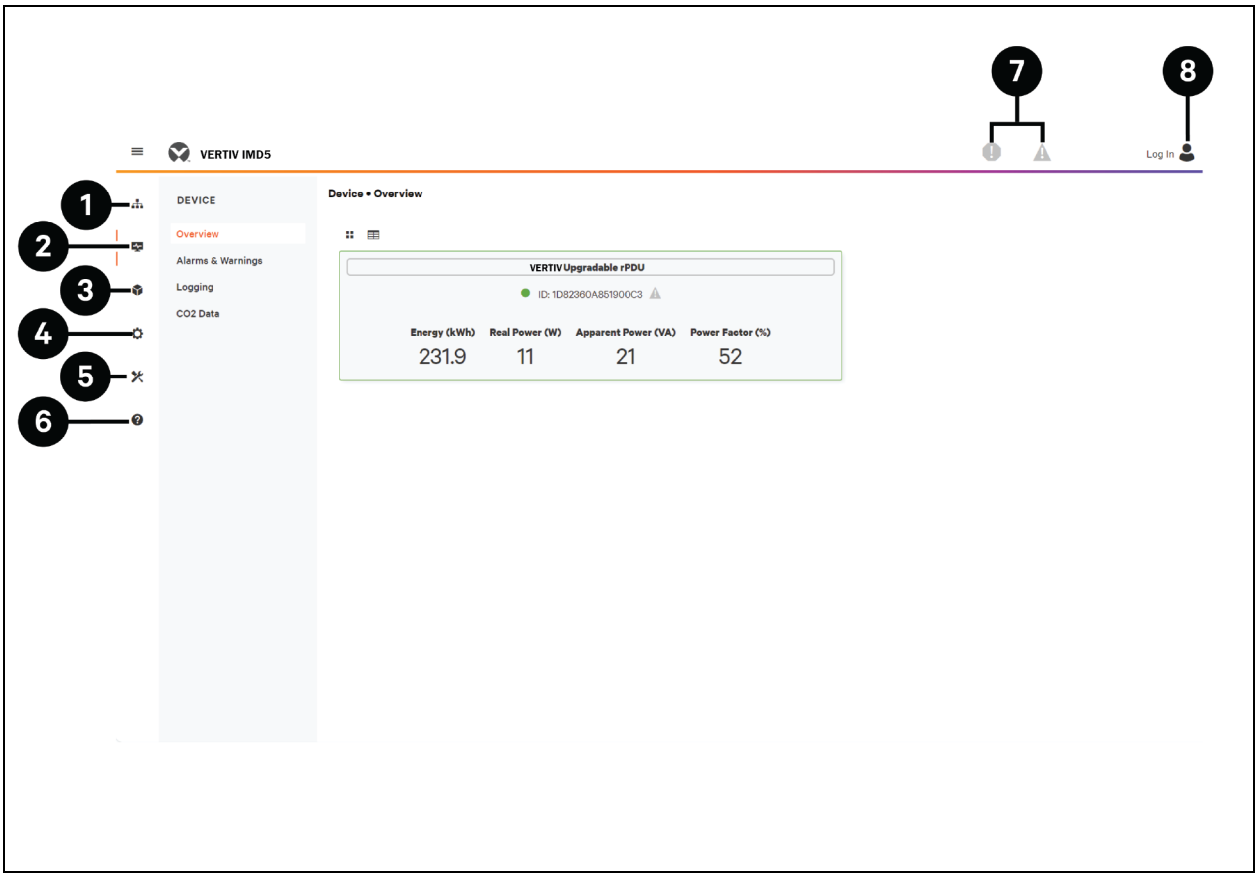


Tableau 5.7 Descriptions du menu principal

Élément	Description
1	Consolidation
2	Dispositif
3	Provisionnement
4	Système
5	Utilitaires
6	Aide
7	Alarmes et avertissements
8	Connexion/déconnexion

5.4 Sous-menu Device

Cliquez sur le sous-menu Device pour accéder aux menus *Overview, Alarms & Warnings, Logging* et *CO2 Data*.

5.4.1 Présentation

Vous devez vous connecter avant de pouvoir effectuer des modifications. Seuls les utilisateurs possédant des autorisations de niveau de contrôle ou supérieures ont accès à ces paramètres.

Figure 5.15 Descriptions des sous-menus Device Overview

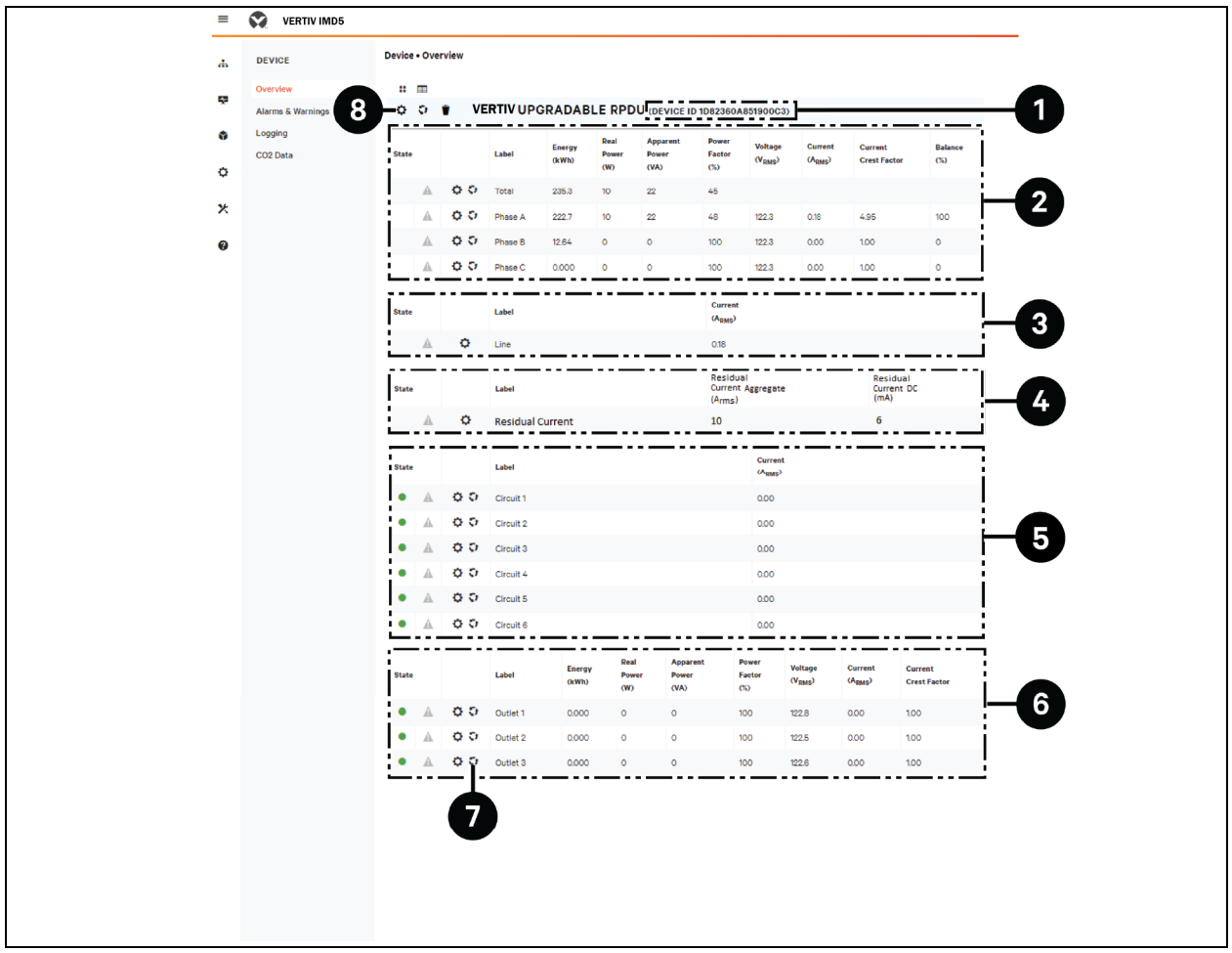


Tableau 5.8 Descriptions des sous-menus Device Overview

Numéro	Nom	Description
1	Identifiant du dispositif	Identifiant unique du produit, qui ne peut pas être modifié. Peut être requis pour l'assistance technique.
2	Surveillance de phases individuelles et totales	Affiche les statistiques relatives au courant alternatif, à la tension et à la puissance pour chaque phase individuelle et pour le total de toutes les phases combinées. Le facteur de courant de crête et l'équilibre de phase (%) sont également indiqués.
3	Ligne	Affiche le courant (en ampères RMS) sur les unités triphasées en étoile. Cette information n'est pas

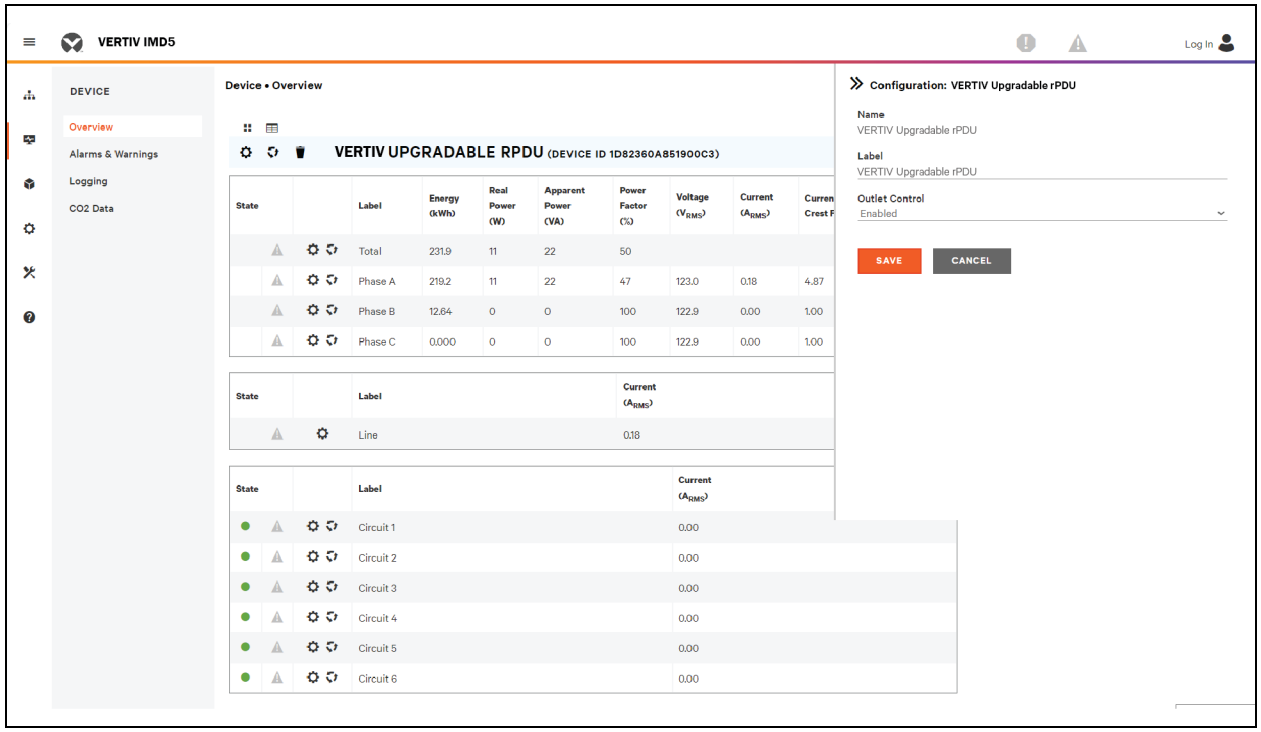
Tableau 5.8 Descriptions des sous-menus Device Overview (suite)

Numéro	Nom	Description
		indiquée sur les unités monophasées et triphasées Delta.
4	Courant résiduel	Uniquement pour les rPDU dotées de la fonctionnalité RCM-B. Affiche les informations pour Residual Current Aggregate (mA) et Residual Current DC (mA). Affiche le courant résiduel pour chaque phase, le cas échéant.
5	Moniteur de courant	Affiche les statistiques relatives à l'appel de courant alternatif pour chaque circuit individuel sur la rPDU.
6	Moniteur de prises	S'applique UNIQUEMENT aux rPDU à prises surveillées/prises commutées – Affiche les statistiques relatives au courant alternatif, à la tension et à la puissance pour chaque circuit et prise. Le facteur de courant de crête est également indiqué. (surveillance de l'alimentation au niveau des prises et surveillance au niveau des prises commutées uniquement). Affiche l'état des prises. (Surveillance au niveau de prises et surveillance au niveau de prises commutées uniquement).
7	Icône d'opération	S'applique UNIQUEMENT aux rPDU à prises surveillées/prises commutées – Permet de modifier les paramètres.
8	Icône de configuration	S'applique UNIQUEMENT aux rPDU à prises surveillées/prises commutées – Permet de modifier le nom du libellé.

Pour modifier le libellé d'un dispositif :

1. Cliquez sur l'icône Configuration pour modifier le libellé de la rPDU Vertiv™ PowerIT et modifiez le libellé. Le nom est le modèle ou le nom défini en usine de la rPDU et ne peut pas être modifié.
2. Cliquez sur *SAVE*.

Figure 5.16 Modification du libellé d'un dispositif



Pour modifier le fonctionnement du dispositif :

1. Cliquez sur l'icône d'opération .
2. Sélectionnez l'opération à effectuer :
   - **On/Off :** active ou désactive toutes les prises.
   - **Reboot :** si des prises sont actuellement activées, le redémarrage désactive les prises, puis les réactive après un délai d'attente. Si les prises sont actuellement désactivées, le redémarrage active les prises.
   - **Cancel :** annule l'opération en cours si elle n'est pas terminée.
   - **Reset Energy :** réinitialise l'énergie totale mesurée en kWh.
   - **Restore Defaults :** rétablit les paramètres d'usine par défaut du dispositif. Cela inclut les libellés, les délais et les actions de mise sous tension du dispositif.

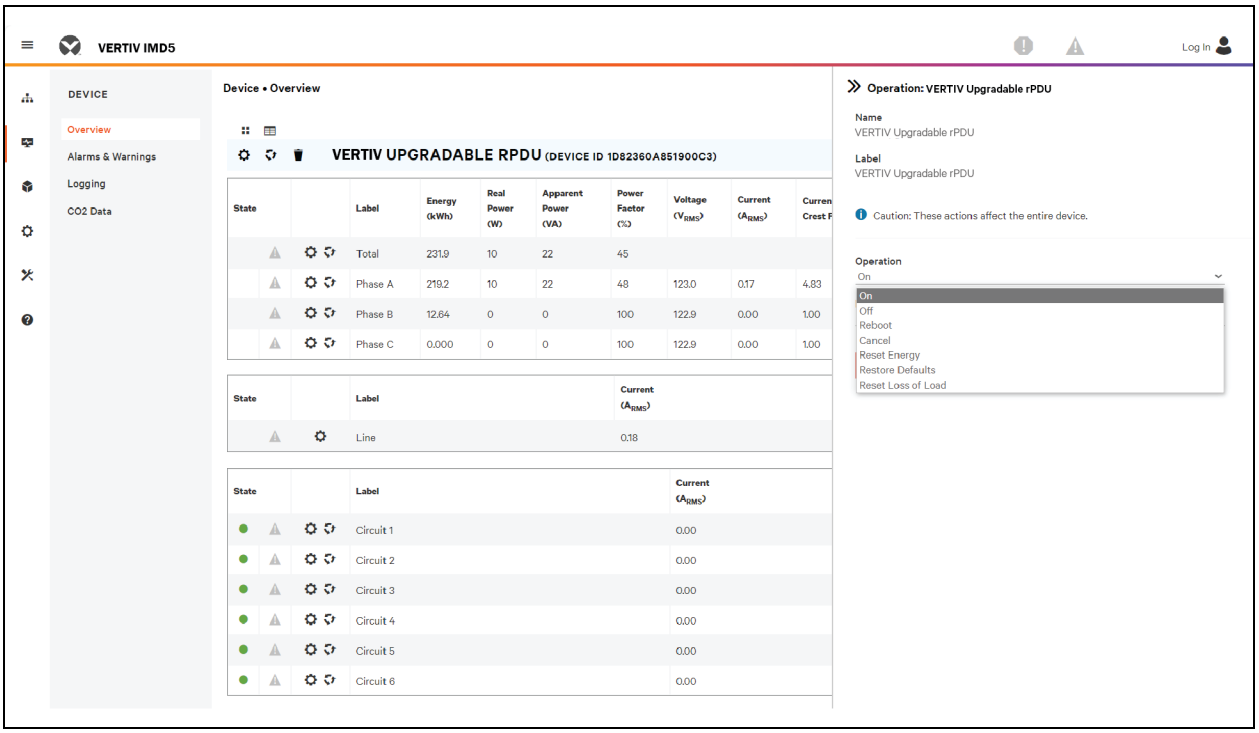
REMARQUE : ces actions affectent l'ensemble du dispositif.

REMARQUE : les opérations d'activation/de désactivation et de redémarrage s'appliquent uniquement aux rPDU Vertiv™ PowerIT à prises commutées.

3. Pour les opérations impliquant l'état des prises, le réglage du paramètre Delay sur *True* utilise la configuration de délai actuelle pour chaque prise lors de l'exécution de l'opération sélectionnée.
4. Cliquez sur *SAVE* pour lancer l'action.

REMARQUE : les délais d'action de mise sous tension se réfèrent au temps écoulé depuis le branchement de l'unité, et non au temps écoulé depuis son démarrage complet. Ils peuvent s'exécuter avant que l'unité ne démarre complètement.

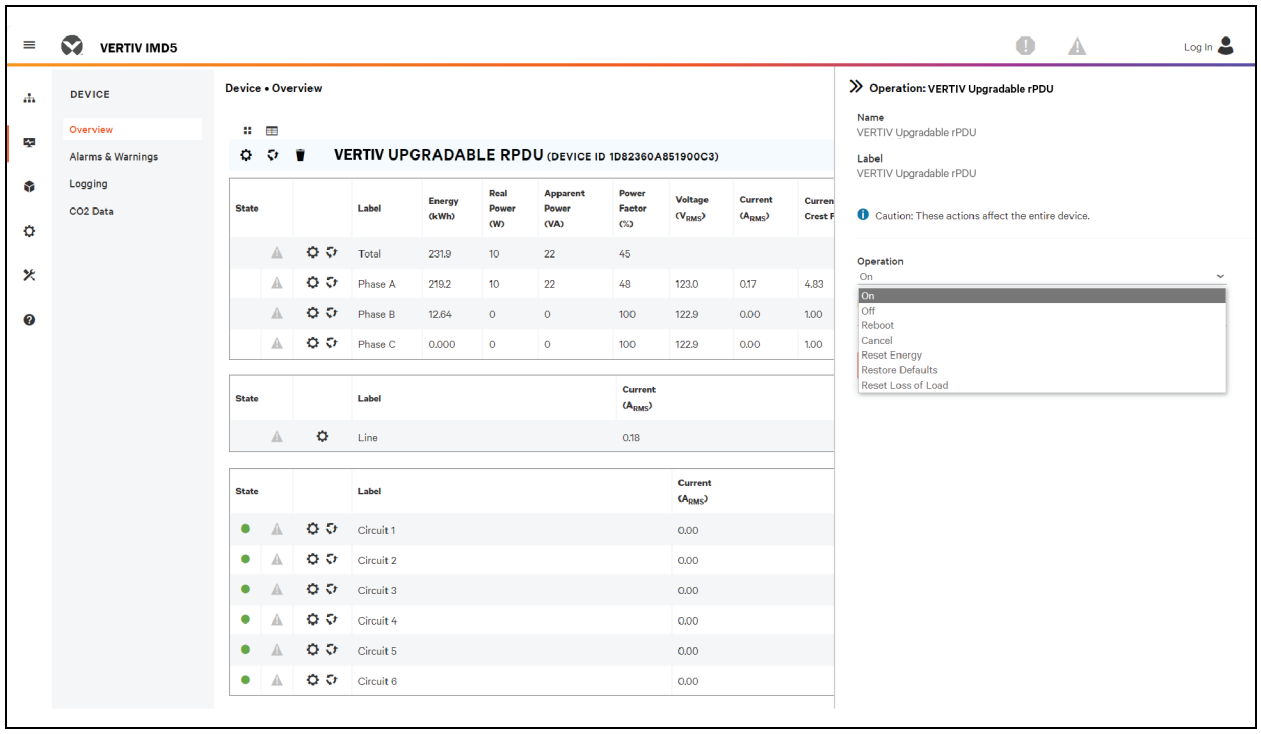
Figure 5.17 Modification d'une opération du dispositif



Pour modifier le libellé d'une phase ou d'un circuit :

1. Cliquez sur l'icône de configuration de la phase ou du circuit et modifiez le libellé. Le nom correspond au nom de la phase physique ou du circuit et ne peut pas être modifié.
2. Cliquez sur *SAVE*.

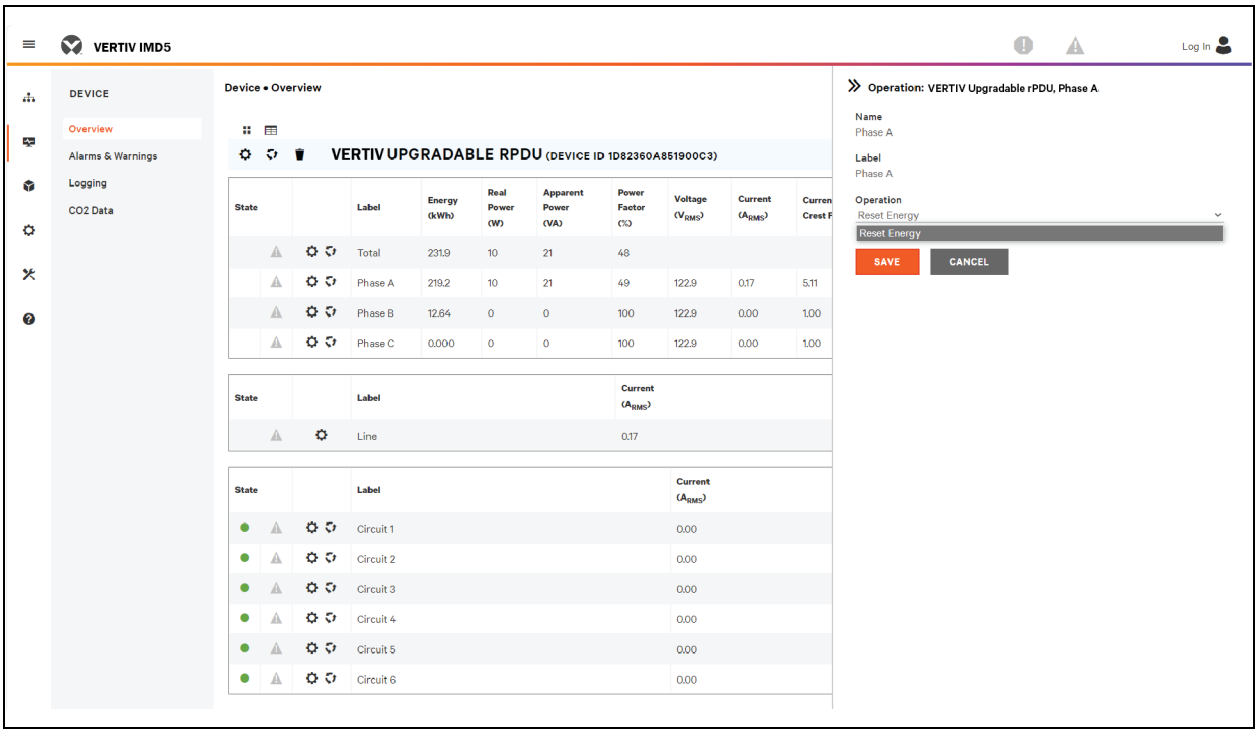
Figure 5.18 Modification du libellé d'une phase ou d'un circuit



Pour modifier l'opération de phase :

1. Cliquez sur l'icône d'opération .
2. Sélectionnez *Reset Energy* pour réinitialiser l'énergie totale mesurée en kWh pour la phase sélectionnée.
3. Cliquez sur *SAVE* pour lancer l'action.

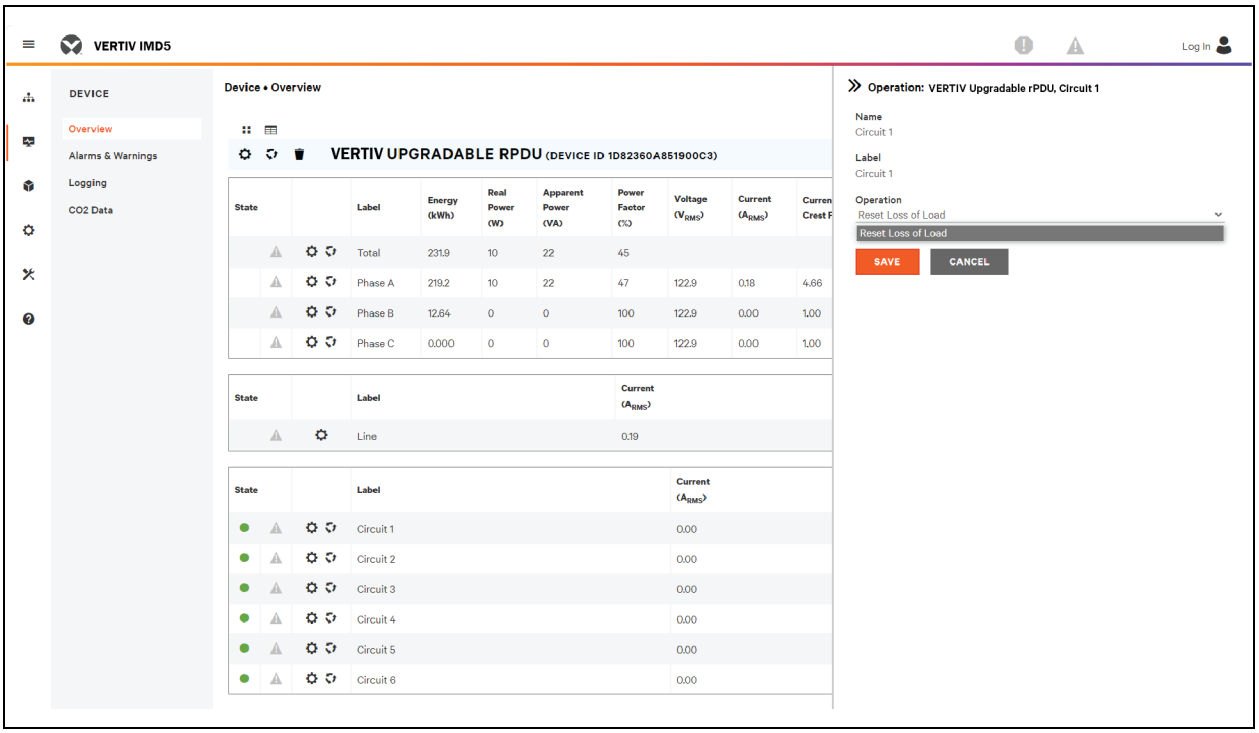
Figure 5.19 Modification d’une opération de phase



Pour modifier l’opération du circuit :

1. Cliquez sur l’icône d’opération .
2. Sélectionnez *Reset Loss of Load* pour réinitialiser l’alarme de perte de charge.
3. Cliquez sur *SAVE* pour lancer l’action.

Figure 5.20 Modification d'une opération du circuit



REMARQUE : cette étape est requise lorsque l'état affiche une alarme de perte de charge et que le problème a été résolu. L'alarme de perte de charge est déclenchée par une chute soudaine de courant détectée par le transducteur de mesure de courant du disjoncteur en cas de fonctionnement proche de la limite de charge du circuit. Pour les unités horizontales évolutives commutées, l'alarme de perte de charge est en outre déclenchée par la perte de tension du disjoncteur (quelle que soit la charge du circuit).

Pour configurer une prise :

REMARQUE : s'applique uniquement aux rPDU Vertiv™ PowerIT à prises surveillées/prises commutées.

1. Cliquez sur l'icône de configuration des prises .
2. Modifiez les configurations, si nécessaire.
   a. Libellé de la prise.

REMARQUE : les étapes 2b à 2k s'appliquent uniquement aux prises commutées.

   b. **State :** état actuel de la prise (Activation ou Désactivation).
   c. **Mode :** mode de contrôle de la prise :
      - **Manual Control :** l'état de la prise est contrôlé à l'aide de l'interface utilisateur Web, de SNMP ou de l'API.
      - **Alarm Control (normalement désactivé, activé quand une alarme associée se déclenche) :** l'état de la prise est réglé normalement sur désactivé et basculera sur activé si un événement d'alarme de prise quelconque se déclenche.
      - **Alarm Control (normalement activé, désactivé quand une alarme associée se déclenche) :** l'état de la prise est réglé normalement sur activé et basculera sur désactivé si un événement d'alarme de prise quelconque se déclenche.

- **Alarm Control (normalement désactivé, activé quand toutes les alarmes associées se déclenchent) :** l'état de la prise est réglé normalement sur désactivé et basculera sur activé si tous les événements d'alarme de prise se déclenchent.
- **Alarm Control (normalement activé, désactivé quand toutes les alarmes associées se déclenchent) :** l'état de la prise est réglé normalement sur activé et basculera sur désactivé quand tous les événements d'alarme de prise se déclenchent.

d. **Pending State :** état vers lequel la prise est en train de basculer.

e. **Time To Action :** temps restant avant que l'action en attente ne s'exécute. Ce paramètre est ajusté à l'aide du paramètre Delays.

f. **On Delay :** temps d'attente, en secondes, qui s'écoule avant que l'unité active une prise.

g. **Off Delay :** temps d'attente, en secondes, qui s'écoule avant que l'unité ne désactive une prise.

h. **Reboot Delay :** temps d'attente, en secondes, qui s'écoule avant que l'unité ne redémarre une prise.

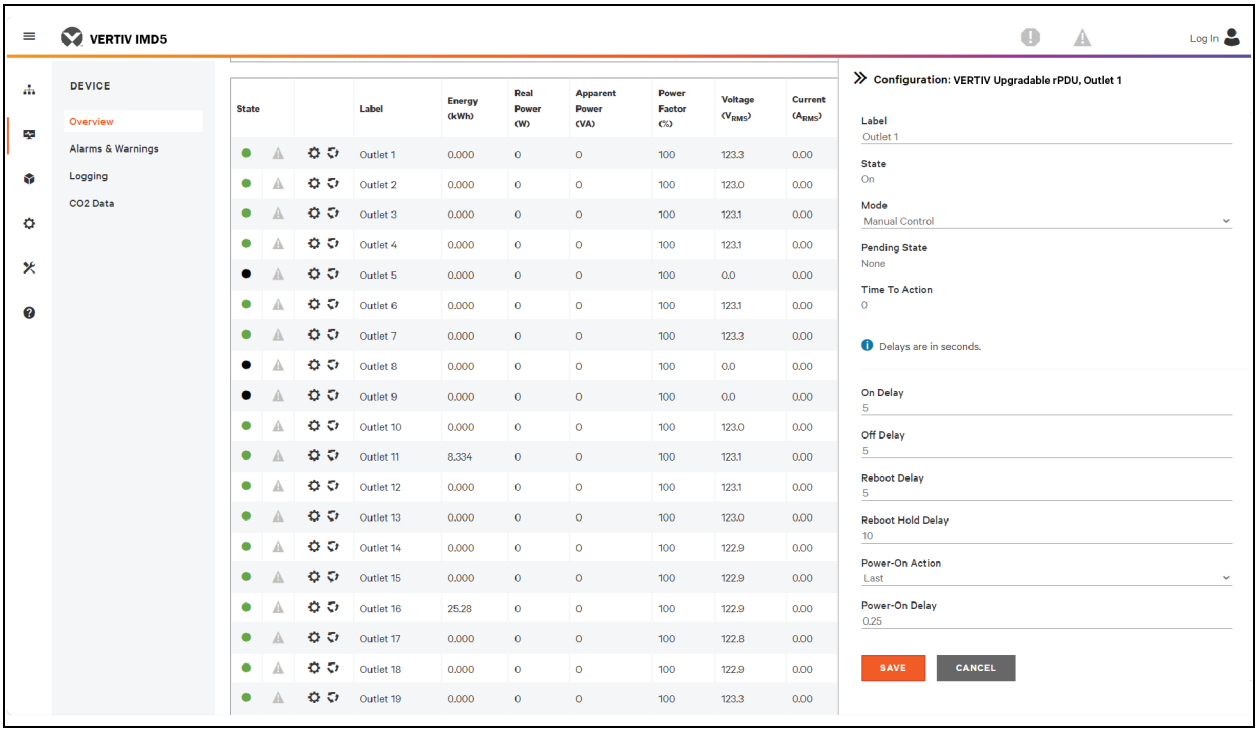
i. **Reboot Hold Delay :** temps d'attente, en secondes, qui s'écoule après que l'unité a désactivé la prise, avant de la réactiver lors d'un redémarrage.

j. **Power-On Action :** définit l'état dans lequel la prise démarrera lorsqu'elle sera mise sous tension (On, Off ou Last). Par défaut, le réglage initial est paramétré sur **Last** et les prises sont activées (ON) en usine.

k. **Power-On Delay :** temps d'attente, en secondes, qui s'écoule avant que l'unité, après sa mise sous tension, mette la prise sous tension.

3. Cliquez sur *SAVE*.

Figure 5.21 Configuration des prises

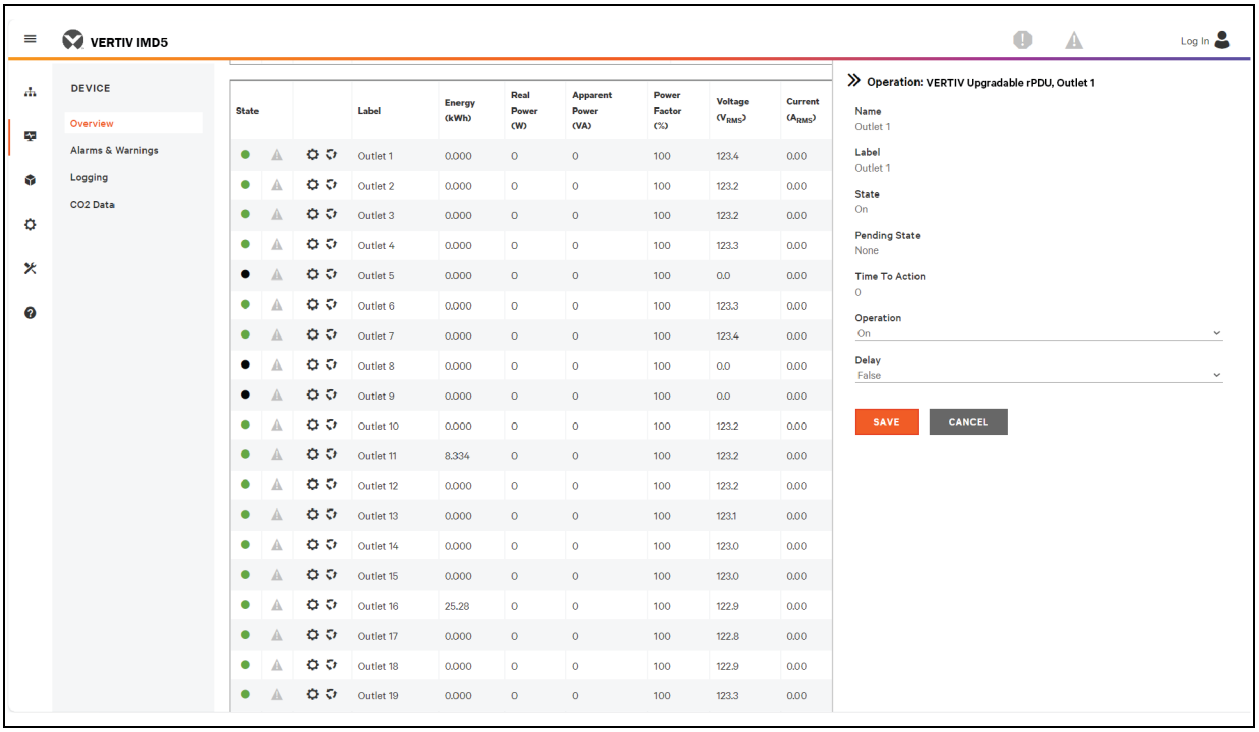


Pour modifier l'opération de la prise :

REMARQUE : s'applique uniquement aux rPDU Vertiv™ PowerIT à prises surveillées/prises commutées.

1. Cliquez sur l'icône des opérations de la prise souhaitée.
2. Sélectionnez l'opération à effectuer :
   - **On/Off :** active ou désactive la prise sélectionnée.
   - **Reboot :** si des prises sont actuellement activées, le redémarrage désactive les prises, puis les réactive après un délai d'attente. Si les prises sont actuellement désactivées, le redémarrage active les prises.
   - **Cancel :** annule l'opération en cours si elle n'est pas terminée.
   - **Reset Energy :** réinitialise l'énergie totale mesurée en kWh pour la prise sélectionnée.
3. Pour les opérations impliquant l'état des prises, le réglage du paramètre Delay sur *True* utilise la configuration de délai actuelle pour chaque prise lors de l'exécution de l'opération sélectionnée.
4. Sélectionnez *SAVE* pour lancer l'action.

Figure 5.22 Pour modifier l'opération d'une prise



State		Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V_{RMS})	Current (A_{RMS})
		Outlet 1	0.000	0	0	100	123.4	0.00
		Outlet 2	0.000	0	0	100	123.2	0.00
		Outlet 3	0.000	0	0	100	123.2	0.00
		Outlet 4	0.000	0	0	100	123.3	0.00
		Outlet 5	0.000	0	0	100	0.0	0.00
		Outlet 6	0.000	0	0	100	123.3	0.00
		Outlet 7	0.000	0	0	100	123.4	0.00
		Outlet 8	0.000	0	0	100	0.0	0.00
		Outlet 9	0.000	0	0	100	0.0	0.00
		Outlet 10	0.000	0	0	100	123.2	0.00
		Outlet 11	8.334	0	0	100	123.2	0.00
		Outlet 12	0.000	0	0	100	123.2	0.00
		Outlet 13	0.000	0	0	100	123.1	0.00
		Outlet 14	0.000	0	0	100	123.0	0.00
		Outlet 15	0.000	0	0	100	123.0	0.00
		Outlet 16	25.28	0	0	100	122.9	0.00
		Outlet 17	0.000	0	0	100	122.8	0.00
		Outlet 18	0.000	0	0	100	122.9	0.00
		Outlet 19	0.000	0	0	100	123.3	0.00

5.4.2 Alarmes et avertissements

La page Alarms & Warnings vous permet d'établir des conditions d'alarme ou d'avertissement (événements) pour chaque mesure d'alimentation et de circuit relevée. Des événements sont déclenchés lorsqu'une mesure dépasse un seuil défini par l'utilisateur, soit au-dessus du seuil (déclenchement haut), soit en dessous (déclenchement bas). Les événements sont affichés dans différentes sections, en fonction du dispositif ou de la mesure auquel l'événement est associé. Chaque événement peut impliquer l'exécution d'une ou de plusieurs actions lorsqu'il se produit.

Figure 5.23 Page Alarms & Warnings

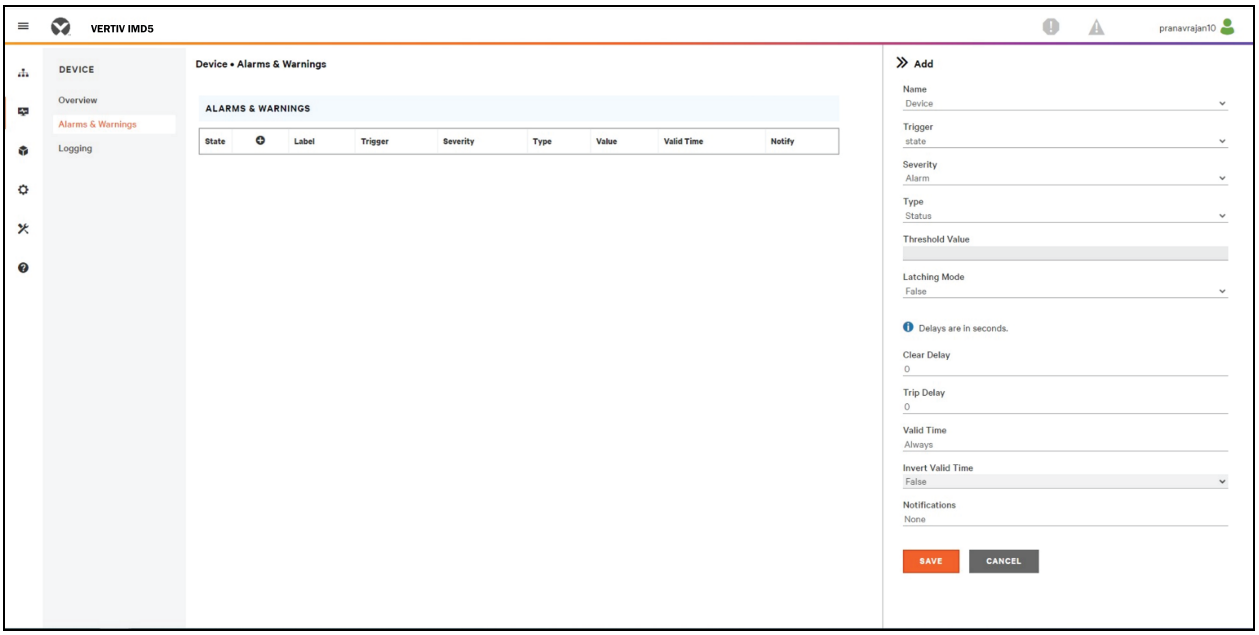


Tableau 5.9 Description des alarmes et avertissements

Numéro	Description	Symbole	Description
1	État de chaque événement.		Symbole d'avertissement. L'événement est affiché en orange.
			Symbole d'alarme. L'alarme est affichée en rouge.
			Symbole d'événement confirmé. Le symbole persiste jusqu'à ce que la condition mesurée revienne à la normale.
2	Ajouter/supprimer/modifier des alarmes et des avertissements.		Ajout de nouveaux avertissements et de nouvelles alarmes.
			Modification d'alarmes et d'avertissements existants.
			Suppression d'alarmes et d'avertissements existants.
3	Avertir l'utilisateur des événements déclenchés et demander confirmation.	S.O.	Vide, s'il n'y a pas de condition d'alerte.
			Lorsqu'un événement d'avertissement ou d'alarme se produit, vous pouvez cliquer sur ce symbole pour confirmer l'événement afin que l'unité cesse d'envoyer d'autres notifications à son sujet. **REMARQUE : en cliquant sur ce symbole, vous n'effacerez pas l'événement d'avertissement ou d'alarme ; vous empêcherez simplement la répétition des notifications.**
4	Affiche les conditions des paramètres d'alarmes et d'avertissements.		

Pour ajouter un nouvel événement d'alarme ou d'avertissement :

1. Cliquez sur le bouton *Add/Modify Alarms* et *Warnings*.
2. Définissez les conditions souhaitées pour cet événement comme suit :
    a. Dans les listes déroulantes, sélectionnez le nom de la phase ou du circuit, la mesure de déclenchement, la gravité et le type.

REMARQUE : déclenchements hauts si la mesure relevée dépasse le seuil et déclenchements bas si la mesure passe en dessous du seuil.

    b. Saisissez la valeur de seuil souhaitée (tout nombre compris entre -999,0 et 999,0).
    c. Saisissez le délai d'effacement souhaité en secondes. Toute valeur autre que *0* signifie qu'une fois cet événement déclenché, la mesure doit revenir à la normale pendant ce nombre de secondes avant que l'événement s'efface et se réinitialise. Le délai d'effacement peut atteindre 14 400 secondes (4 heures).
    d. Saisissez le délai de déclenchement souhaité en secondes. Toute valeur autre que *0* signifie que la mesure doit dépasser le seuil pendant ce nombre de secondes avant que l'événement ne se déclenche. Le délai de déclenchement peut atteindre 14 400 secondes (4 heures).
    e. Si le mode de verrouillage est activé, cet événement et les actions qui lui sont associées restent actifs jusqu'à ce que l'événement soit confirmé, même si la mesure revient par la suite à la normale.
    f. Pour spécifier la destination des notifications d'alerte lorsque cet événement d'alarme ou d'avertissement se produit, cliquez sur l'icône d'ajout pour créer une nouvelle action.
    g. Sélectionnez les options souhaitées dans le menu déroulant :
        - Le champ Target contient l'adresse e-mail ou le gestionnaire SNMP auquel les notifications sont envoyées lorsque l'événement est déclenché. Pour plus d'informations sur la configuration d'une adresse e-mail cible, reportez-vous à la section Email à la page 90.
        - Ou bien, si un numéro de prise est sélectionné comme cible, l'état de la prise commute lorsqu'un événement est déclenché et reste à l'état commuté jusqu'à ce que l'événement se réinitialise ou soit confirmé. Pour cette option, le mode de la prise doit être configuré pour le contrôle d'alarme ; reportez-vous à la section Alarmes et avertissements à la page 54.

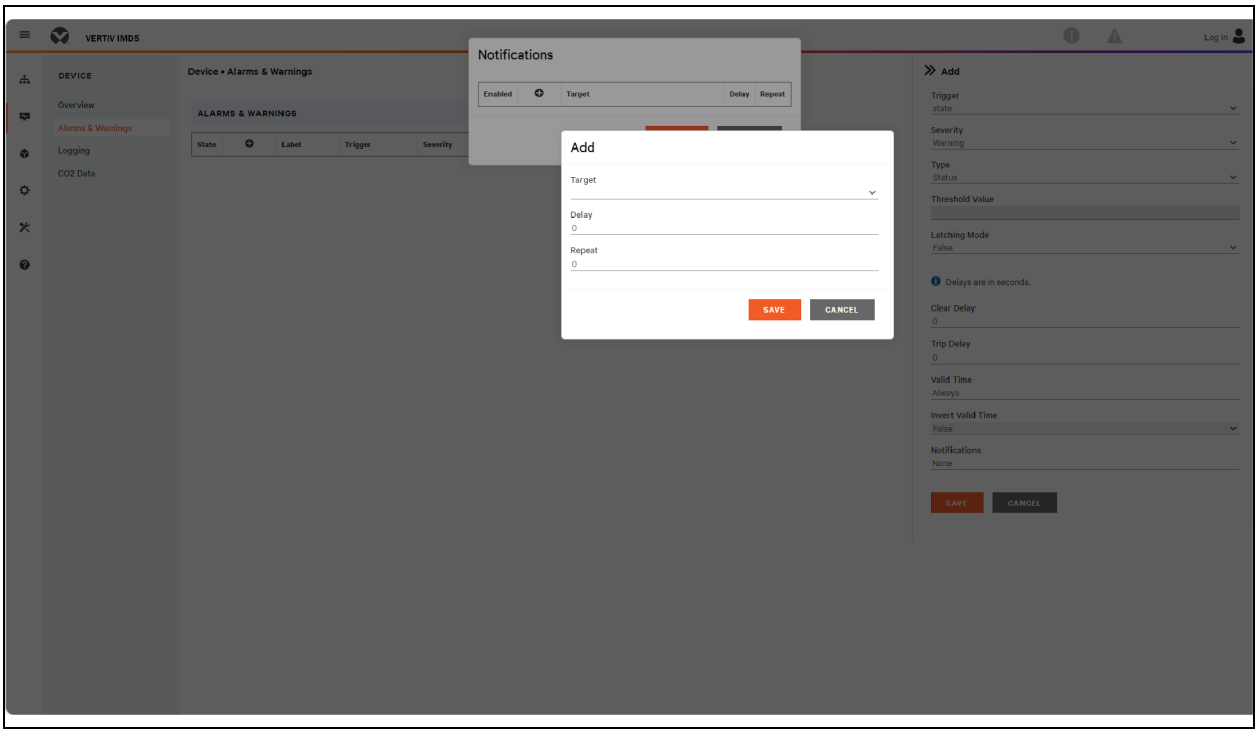
REMARQUE : les délais et les répétitions cibles sont partagés entre toutes les alarmes. Si plusieurs valeurs de délai ou de répétition sont nécessaires pour des cibles spécifiques, chacune doit être ajoutée à la liste des cibles, puis la case Enabled appropriée doit être cochée sur chaque alarme.

REMARQUE : s'applique uniquement aux rPDU Vertiv™ PowerIT à prises surveillées/prises commutées.

        - Le délai détermine pendant combien de temps cet événement doit rester déclenché avant l'envoi de la première notification de cette action. Ce paramètre est différent du délai de déclenchement ci-dessus. Le délai de déclenchement détermine la durée pendant laquelle la valeur seuil doit être dépassée avant que l'événement proprement dit ne soit déclenché. Ce délai détermine pendant combien de temps cet événement doit rester déclenché avant l'exécution de cette action. Le délai peut atteindre 14 400 secondes (4 heures). Si le délai est réglé sur *0*, la notification sera envoyée immédiatement.
        - Le paramètre Repeat détermine si plusieurs notifications seront envoyées pour cette action d'événement. Des notifications de répétition sont envoyées aux intervalles spécifiés jusqu'à ce que l'événement soit confirmé ou effacé et réinitialisé. L'intervalle de répétition peut atteindre 14 400 secondes (4 heures). Si l'intervalle de répétition est réglé sur *0*, cette fonction sera désactivée et une seule notification sera envoyée.
3. Cliquez sur *SAVE* pour enregistrer cette action de notification.

REMARQUE : plusieurs actions peuvent être définies pour une alarme ou un avertissement. Pour ajouter plusieurs actions, cliquez à nouveau sur l’icône d’ajout et définissez chacune d’elles comme vous le souhaitez. Chaque alerte peut être associée à 32 actions au maximum.

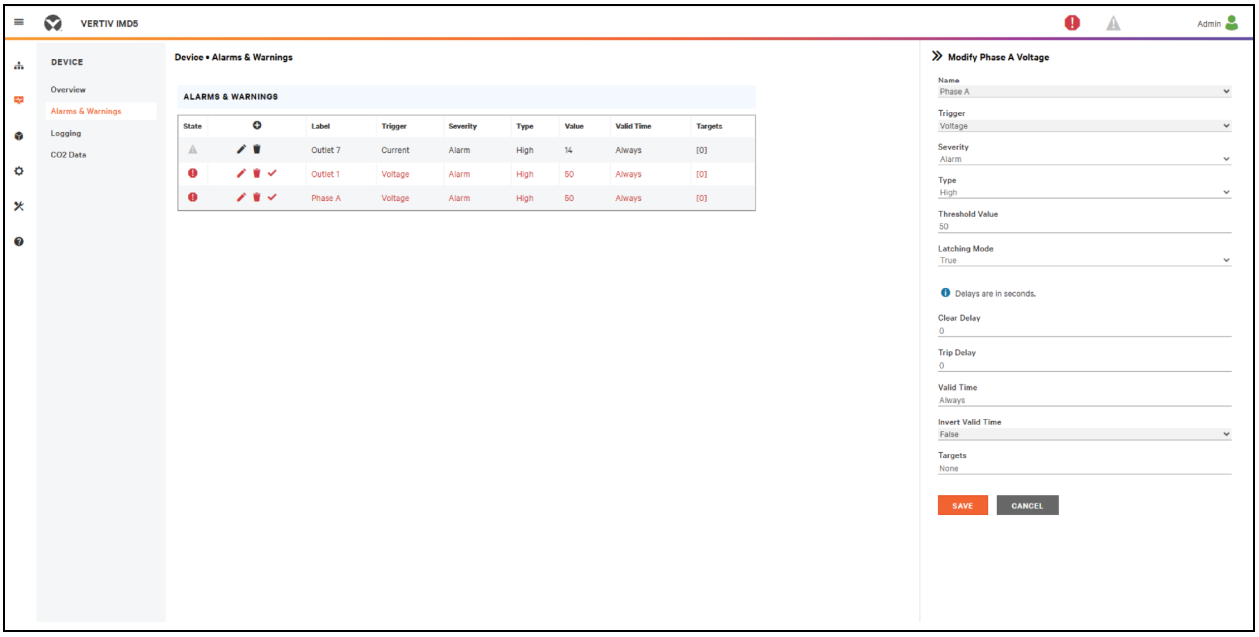
Figure 5.24 Fenêtre d’ajout d’alarmes et d’avertissements



Pour modifier un événement d'alarme ou d'avertissement existant :

1. Cliquez sur l'icône de modification à côté de l'événement d'alarme ou d'avertissement que vous souhaitez modifier.
2. Modifiez les paramètres comme requis, puis cliquez sur *SAVE*.
3. Après l'ajout d'une action, une case est cochée dans la colonne Enabled à l'extrémité gauche. Par défaut, lorsqu'une action est ajoutée, elle est décochée (désactivée). Cochez la *case* pour l'activer. Cela vous permet d'activer et de désactiver de manière sélective différentes actions pour les tests.

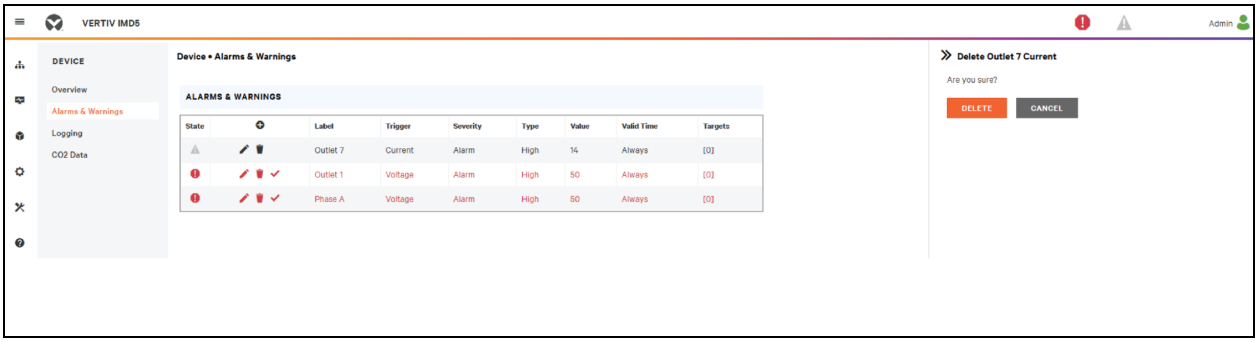
Figure 5.25 Fenêtre de modification d'alarmes et d'avertissements



Pour supprimer un événement d'alarme ou d'avertissement existant :

1. Cliquez sur l'icône de suppression à côté de l'événement d'alarme ou d'avertissement que vous souhaitez supprimer.
2. Cliquez sur *DELETE* et *SAVE* pour confirmer.

Figure 5.26 Suppression d'un événement d'alarme et d'avertissement



5.4.3 Logging

La page Logging vous permet d'accéder aux données historiques enregistrées par la rPDU Vertiv™ PowerIT en sélectionnant les capteurs souhaités et les intervalles de temps à consigner. Elle permet de sélectionner tous les éléments ou de n'en sélectionner aucun.

Pour sélectionner ou désélectionner la valeur de mesure :

1. Cliquez sur l'icône Dispositif et cliquez sur le sous-menu Logging.
2. Dans la page Logging, cliquez sur *Select All* pour sélectionner la valeur de mesure et cliquez sur *Select None* pour désélectionner la valeur de mesure.

Figure 5.27 Page Logging

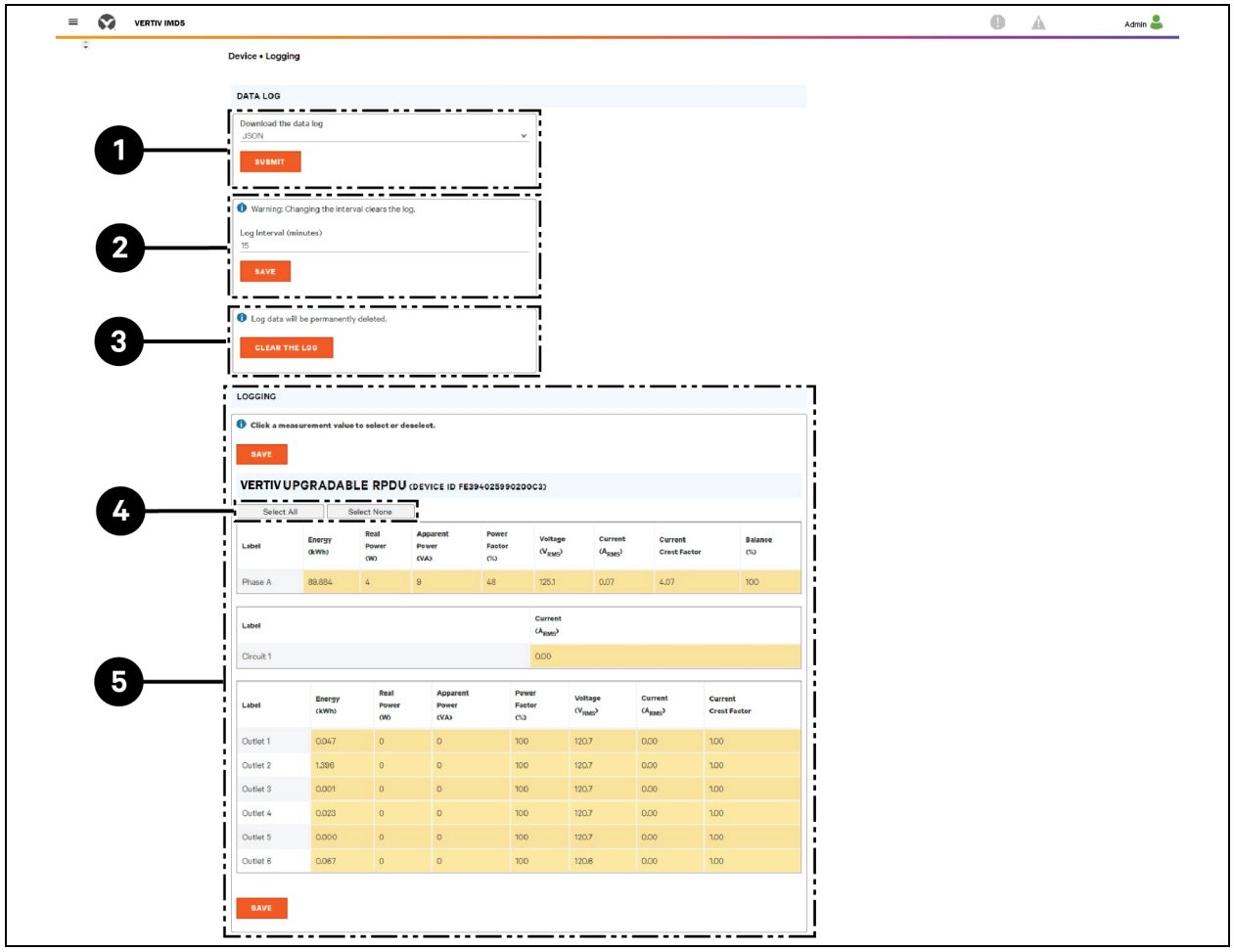


Tableau 5.10 Description de la page Logging

Élément	Nom	Description
1	Download the data log	Cliquez sur le menu déroulant et sélectionnez l'une des options : *JSON* pour le format *JSON*. CSV pour le format .csv dans un tableur. Cliquez sur le bouton *SUBMIT* pour télécharger le journal de données.
2	Log interval	Fréquence à laquelle les données sont écrites dans le fichier journal. L'intervalle de journalisation peut être compris entre 1 et 600 minutes ; le réglage par défaut de ce paramètre est de 15 minutes. **AVERTISSEMENT ! Les données du journal seront définitivement supprimées.**
3	Clear the log	Supprimez le fichier journal. **AVERTISSEMENT ! Les données du journal seront définitivement supprimées.**
4	Select All/Select None	Cliquez sur *Select All* pour sélectionner la valeur de mesure et cliquez sur *Select None* pour désélectionner la valeur de mesure.
5	Logging	Cliquez sur la valeur de mesure pour sélectionner ou désélectionner les paramètres de journalisation souhaités. Par défaut, toutes les mesures sont sélectionnées. Cliquez sur *SAVE* pour enregistrer les modifications.

REMARQUE : l'intervalle de journalisation maximal est déterminé par le nombre de mesures consignées et l'intervalle auquel les données sont écrites dans le fichier journal.

5.4.4 Données relatives au CO2

Figure 5.28 Page d'accueil relative au CO2

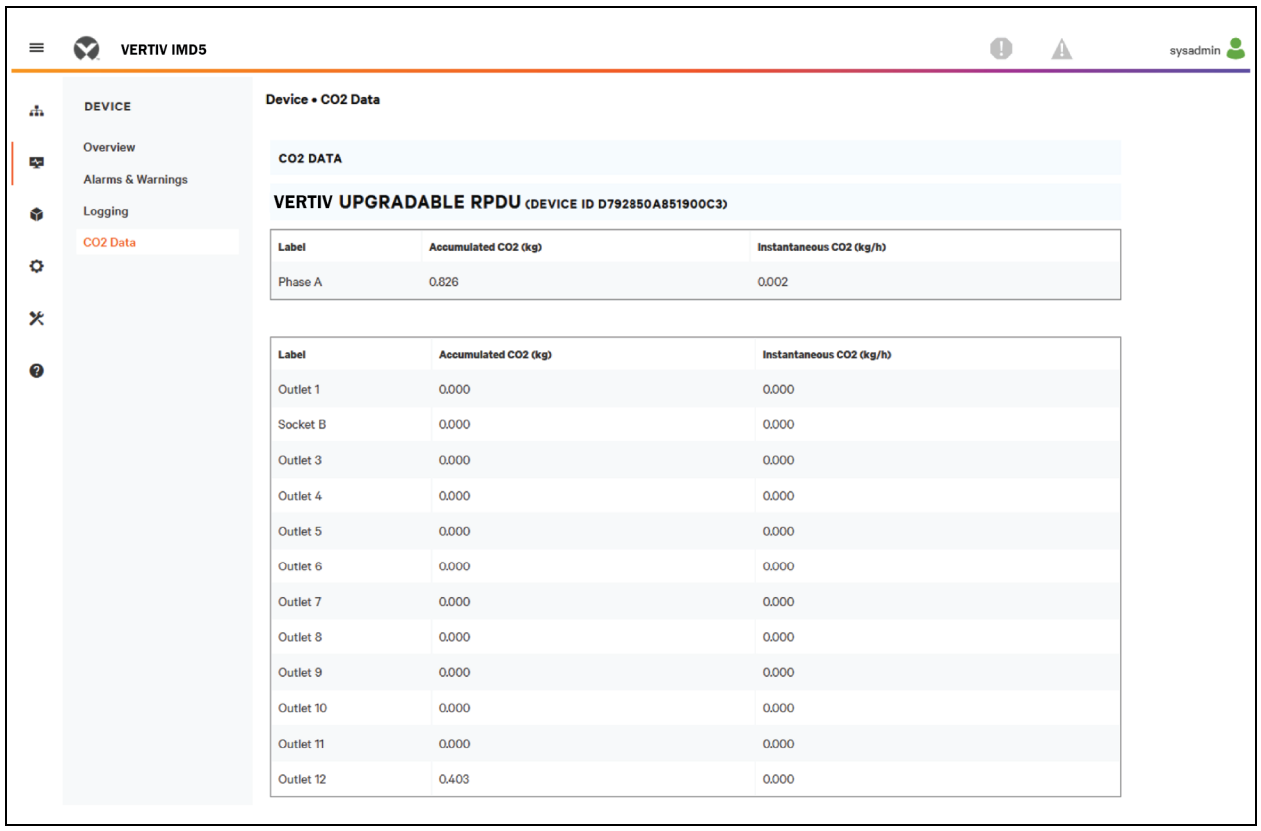
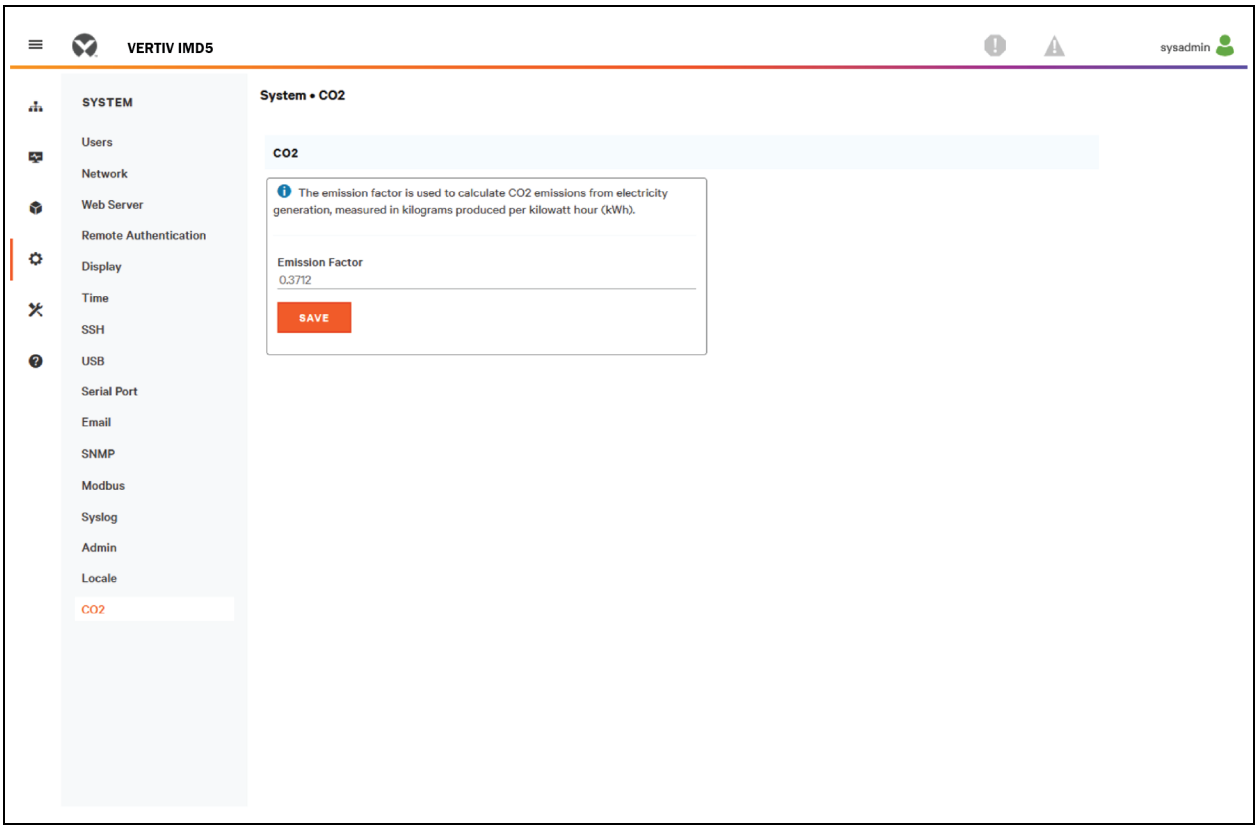


Figure 5.29 Onglet System relatif au CO2



REMARQUE : trois pages sont associées à la page CO2. La première page est la page de données relatives au CO2 sous Device (Figure 5.28 sur la page précédente), qui affiche les calculs cumulés et instantanés pour les phases et les prises. La deuxième page est la page relative au CO2 sous System où vous définissez le facteur d'émission pour calculer le CO2 par kWh. Le facteur d'émission de CO2 par défaut sera défini sur 0,3172. La troisième page se trouve sur la page d'informations d'aide ; le paramètre CO2 tout au long de la vie est basé sur la valeur Lifetime Energy. Si un utilisateur réinitialise la consommation d'énergie sur une PDU ou une prise spécifique, la valeur reviendra à 0. Cependant, la valeur Énergie tout au long de la vie de ce composant ne sera pas réinitialisée à 0.

5.5 Sous-menu Provisioner

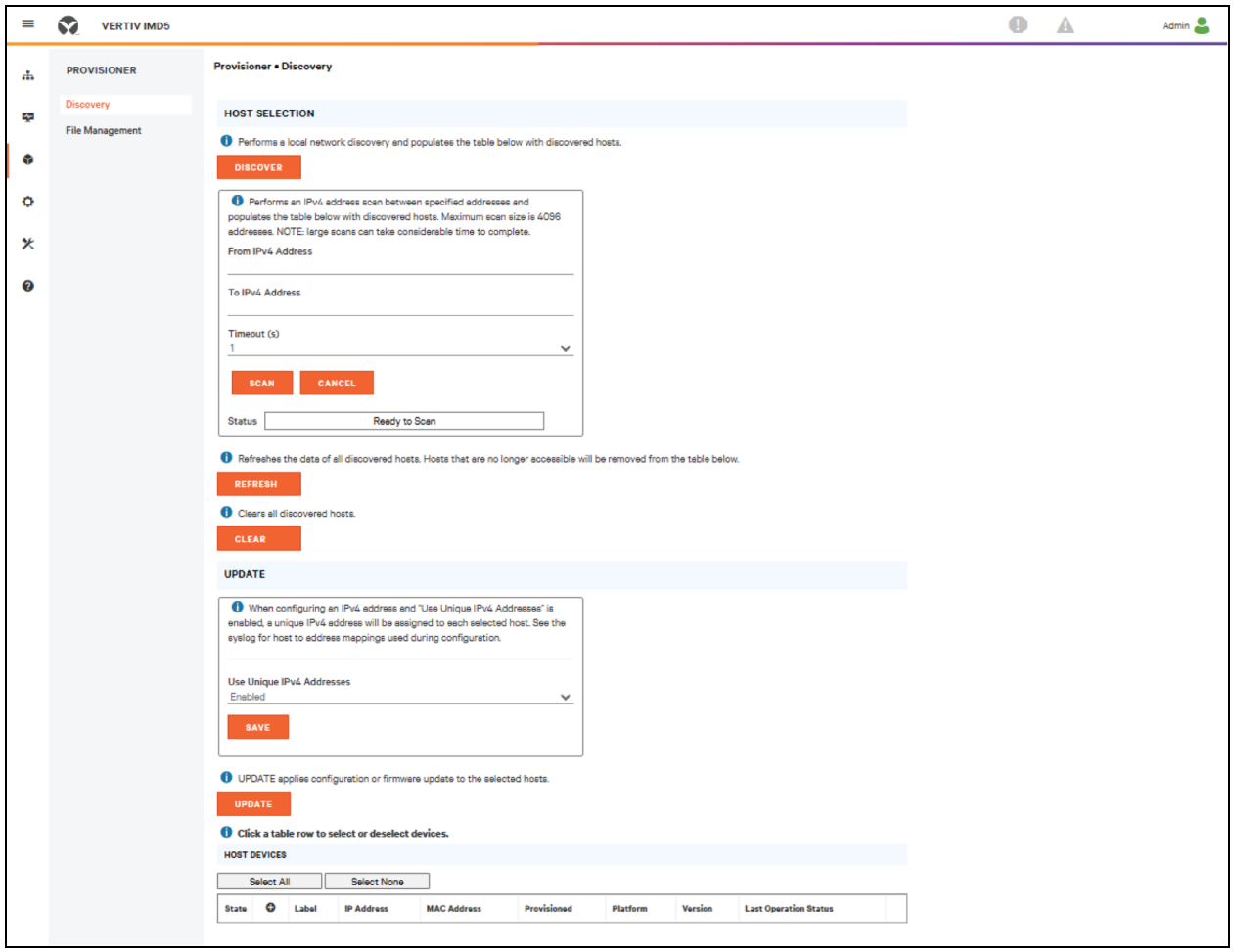
Le sous-menu Provisioner permet à l'utilisateur de détecter les rPDU Vertiv™ PowerIT connectées localement. L'utilisateur peut ainsi mettre à jour les firmwares et les configurer en chargeant un fichier contenant les paramètres de configuration.

Le sous-menu Provisioner permet de configurer les paramètres des dispositifs (par exemple, les alarmes) et les paramètres du système. Cette fonctionnalité peut provisionner :

- Les IMD-5M exécutant le firmware 6.x.x.
- Les rPDU exécutant le firmware 5.x.x (modèles d'IMD 3E, 03E, 3E-S et 03E-S).
- Les rPDU Vertiv™ PowerIT avec les paramètres d'usine ou précédemment configurées avec la version 6.1.0.
- Les PDU en rack connectées directement au réseau local ou au réseau (de consolidation) Vertiv Intelligence Director.
- Toutes les rPDU Vertiv™ PowerIT détectées ou uniquement celles qui ont été sélectionnées.

REMARQUE : vous devez être connecté en tant qu'administrateur pour pouvoir utiliser l'outil de provisionnement. L'IPV6 doit être activé sur la rPDU Vertiv™ PowerIT pour être détecté. La plupart des options du menu de l'interface utilisateur du système peuvent être configurées. D'autres paramètres, comme ceux des capteurs ou les alarmes, ne peuvent pas être configurés avec cette version de l'outil de provisionnement.

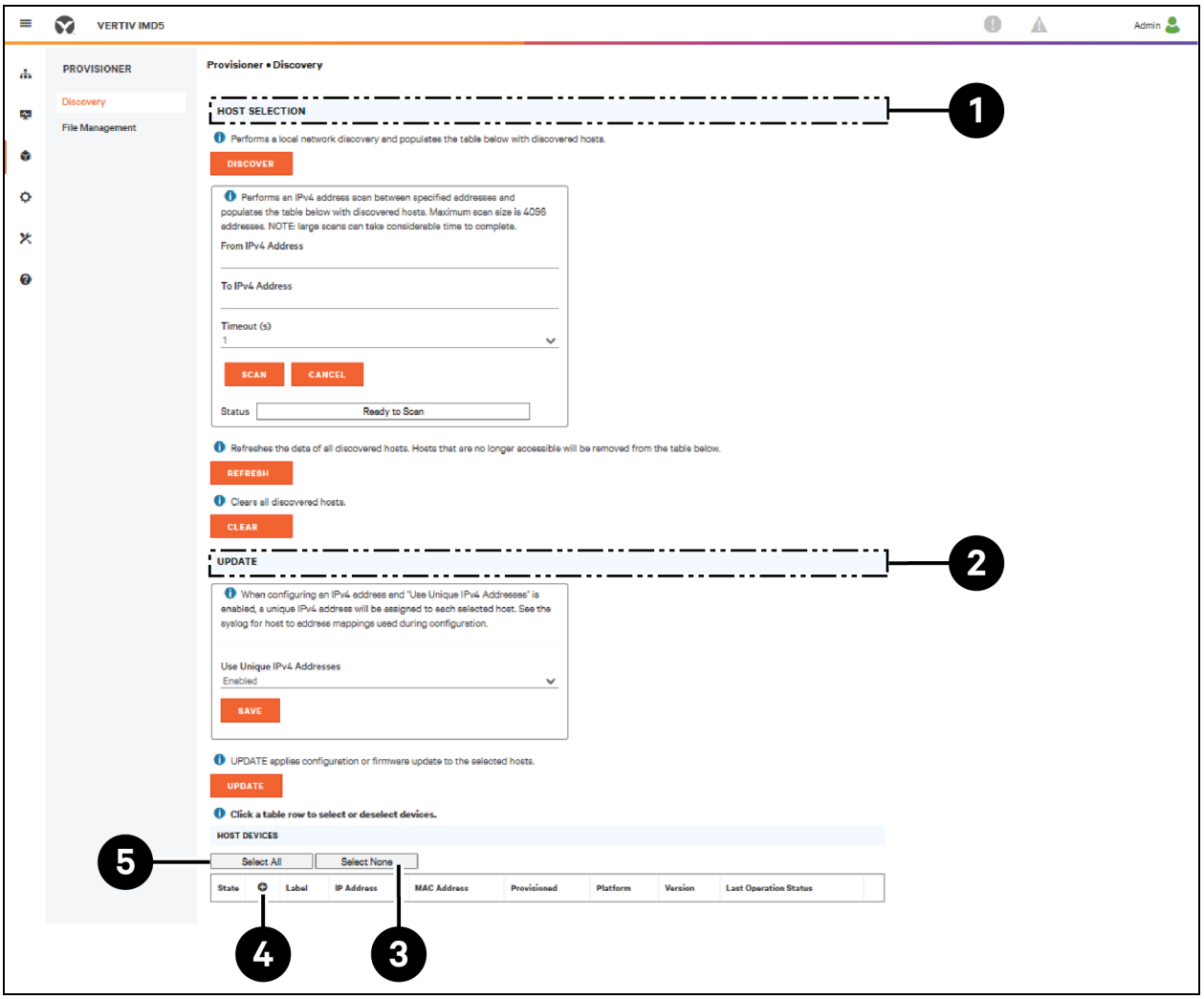
Figure 5.30 Page du sous-menu Provisioner



5.5.1 Détection

1. Cliquez sur *DISCOVER* pour rechercher les rPDU Vertiv™ PowerIT connectées localement.
2. Cliquez sur toutes les rPDU Vertiv™ PowerIT de la liste dont vous souhaitez mettre à jour le firmware et/ou la configuration. Les unités sélectionnées s'affichent en vert. Vous pouvez également cliquer sur l'option *Select All* pour mettre à jour toutes les rPDU Vertiv™ PowerIT de la liste.
3. Cliquez sur *UPDATE* pour mettre à jour toutes les rPDU Vertiv™ PowerIT sélectionnées en utilisant un fichier de firmware et/ou un fichier de configuration.

Figure 5.31 Détection



Numéro	Nom	Description
1	Host Selection	Permet d'identifier les PDU en rack connectées localement et au réseau
2	Update	Permet de mettre à jour le firmware et/ou la configuration des rPDU sélectionnées
3	Select None	Sélectionnez aucun pour désélectionner toutes les sélections
4	Add MAC address	Permet de saisir manuellement des rPDU grâce à leur adresse MAC
5	Select All	Permet de sélectionner toutes les rPDU connectées.

REMARQUE : vous devez d'abord charger les fichiers de firmware et de configuration sur l'onglet de gestion des fichiers avant de pouvoir effectuer les étapes ci-dessus.

5.5.2 Gestion des fichiers

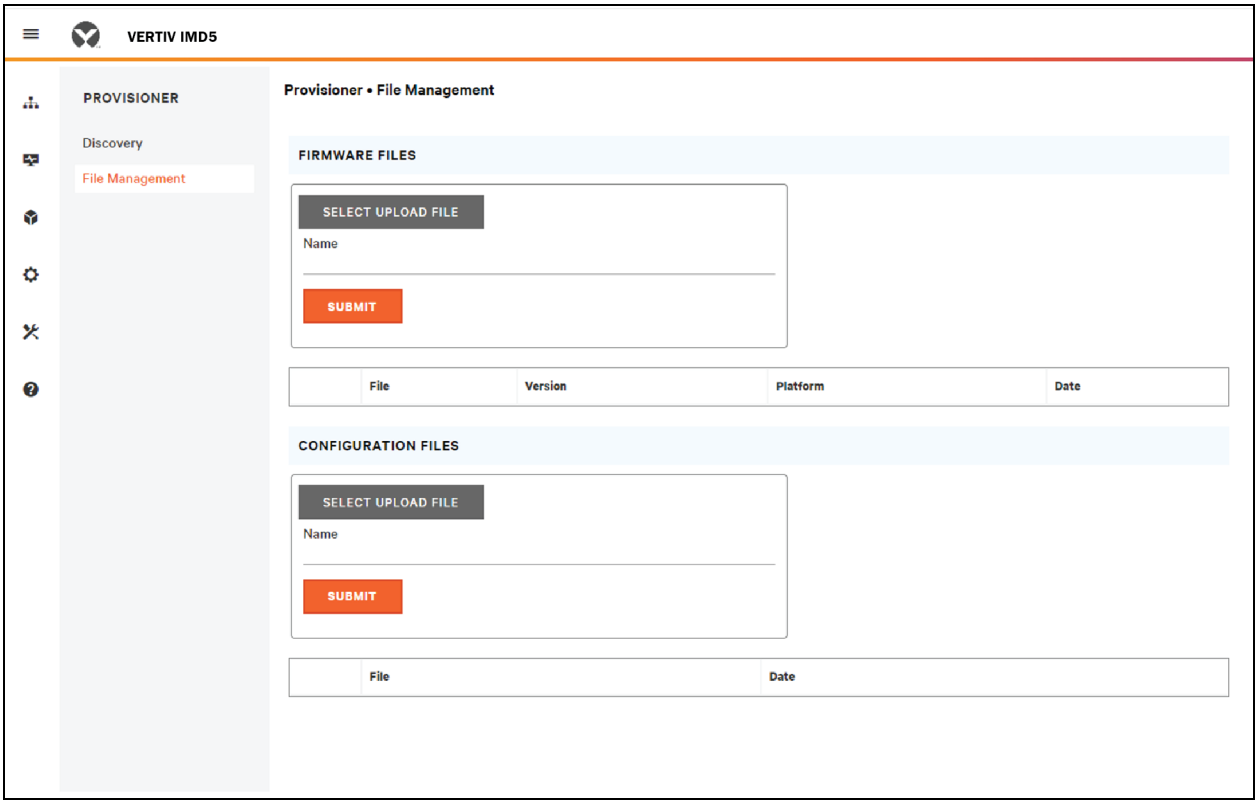
Firmware Files :

1. Cliquez sur *SELECT UPLOAD FILE* et sélectionnez le ***fichier .firmware*** dans la fenêtre Open.
2. Cliquez sur *SUBMIT*. Le fichier de firmware s'affiche dans la liste.

Configuration Files :

1. Cliquez sur *SELECT UPLOAD FILE* et sélectionnez le ***fichier .config*** dans la fenêtre Open.
2. Cliquez sur *SUBMIT*. Le fichier de configuration s'affiche dans la liste.

Figure 5.32 Page de gestion des fichiers



Reportez-vous à la section Provisionnement – Format du fichier contenant les paramètres de configuration à la page 127 pour des exemples de fichiers de paramètres de configuration utilisés par l'outil de provisionnement, ainsi que le format requis.

5.6 Sous-menu System

REMARQUE : vous devez être connecté en tant qu'administrateur pour pouvoir modifier des paramètres dans l'onglet System.

5.6.1 Utilisateurs

La page Users du menu System vous permet de gérer ou de restreindre l'accès aux fonctions de l'unité en créant des comptes pour différents utilisateurs.

REMARQUE : politique de verrouillage de compte Web/SSH/CLI : un compte est verrouillé pendant 30 minutes si 10 tentatives de connexion infructueuses consécutives ont lieu dans un intervalle de 60 minutes. Ce comportement peut être modifié avec la dernière version du firmware.

L'option Scope permet à un compte de niveau administrateur de limiter l'accès des utilisateurs aux informations des prises sélectionnées.

Figure 5.33 Page Users

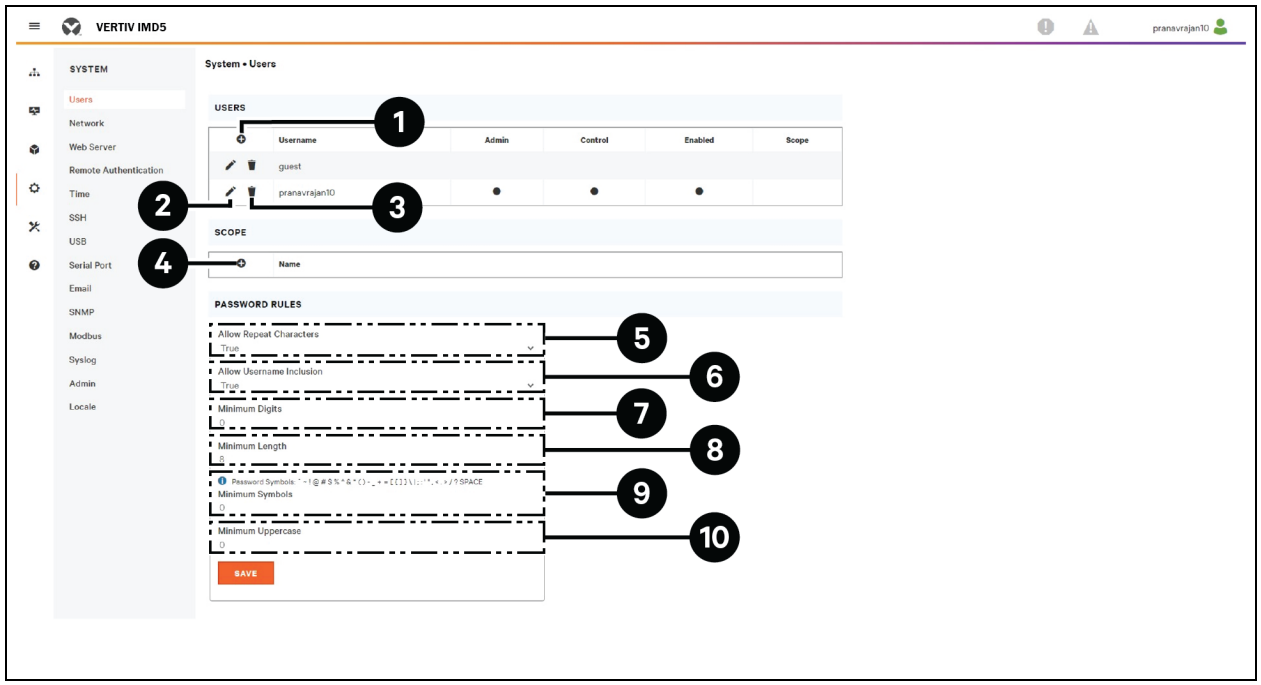


Tableau 5.11 Description de la page Users

Numéro	Description
1	Ajouter un nouveau compte utilisateur
2	Modifier un compte utilisateur
3	Supprimer un compte utilisateur
4	Ajouter une portée d'utilisateur : visible uniquement lorsque vous êtes connecté en tant qu'administrateur*
5	Autoriser les caractères répétés : restreindre le nombre de répétitions de caractères à 2 maximum (False, par défaut)*

Tableau 5.11 Description de la page Users (suite)

Numéro	Description
6	Autoriser l'inclusion du nom d'utilisateur : restreindre l'inclusion du nom d'utilisateur dans le mot de passe (False, par défaut)*
7	Chiffres minimum : saisissez le nombre minimum de caractères numériques (0 par défaut)*
8	Longueur minimum : saisissez le nombre minimal de caractères du mot de passe (8 par défaut, 6 au minimum)*
9	Symboles minimum : saisissez le nombre minimum de caractères de symbole (0 par défaut)*
10	Majuscule minimum : saisissez le nombre minimum de caractères majuscules (par défaut 0)*
REMARQUE : *visible uniquement lorsque vous êtes connecté en tant qu'administrateur.	

REMARQUE : seul un compte de niveau administrateur peut ajouter, modifier ou supprimer des utilisateurs et les portées correspondantes. Les comptes de niveau contrôle et lecture seule peuvent modifier leurs propres mots de passe à l'aide de l'icône de modification d'un utilisateur, mais ils ne peuvent pas ajouter, supprimer ou modifier d'autres comptes. Le compte invité ne peut ajouter, supprimer ou modifier aucun compte, pas même le sien.

Pour ajouter ou modifier un compte utilisateur :

1. Cliquez sur l'icône d'ajout ou de modification d'un utilisateur.
2. Créez ou modifiez les informations du compte comme requis.
    a. Username : nom du compte. Les noms d'utilisateur peuvent comporter jusqu'à 24 caractères, sont sensibles à la casse et ne peuvent pas contenir d'espaces ni aucun des caractères interdits suivants : $& ` :<>[ ] { }"+%@/ ; =?\^|~',

REMARQUE : une fois un compte créé, il n'est plus possible de modifier le nom d'utilisateur.

    b. Administrator : si ce paramètre est réglé sur *True*, ce compte dispose d'un accès de niveau administrateur à l'unité et peut modifier n'importe quel paramètre.
    c. Control : si ce paramètre est réglé sur *True*, ce compte dispose d'un accès de niveau contrôle. En réglant le paramètre Administrator sur *True*, le paramètre Control sera aussi réglé automatiquement sur *True*. En réglant ce paramètre sur *False*, le compte devient un compte Enabled, qui est accessible en lecture seule.
    d. Scope : sélectionnez la portée appropriée pour le compte, le cas échéant. Reportez-vous à l'étape Pour ajouter ou modifier une portée d'utilisateur : à la page 69.
    e. New Password : le mot de passe du compte peut comporter jusqu'à 24 caractères, est sensible à la casse et ne peut pas contenir d'espaces.
    f. Account Status : réglez le compte sur *Enabled* ou *Disabled*. La désactivation d'un compte l'empêche d'être utilisé pour la connexion, mais elle ne le supprime pas de la liste des comptes.
3. Cliquez sur *SAVE*.

Types de comptes utilisateur

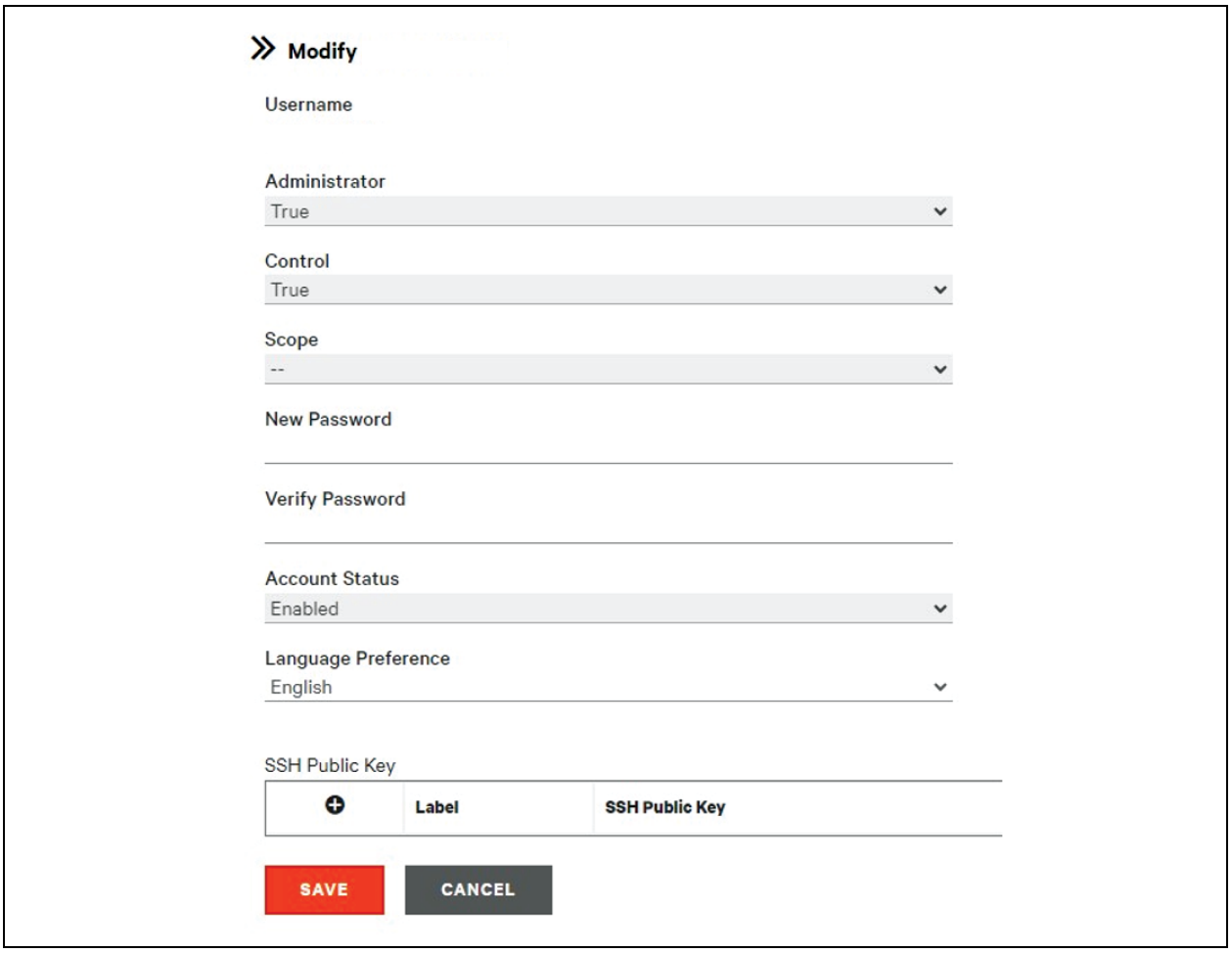
- Administrator : les comptes administrateur (comptes dont les droits administrateur et contrôle sont réglés sur *True*, comme indiqué ci-dessus) ont un contrôle total sur toutes les fonctions et tous les paramètres disponibles sur le dispositif, notamment la possibilité de modifier les paramètres du système et d'ajouter, de modifier ou de supprimer les comptes d'autres utilisateurs.

- Control : les comptes de niveau contrôle (comptes dont seul le paramètre Control est réglé sur *True*) contrôlent tous les paramètres relatifs aux capteurs du dispositif. Ils peuvent ajouter, modifier ou supprimer des alarmes et des événements d'avertissement, ainsi que des actions de notification, et ils peuvent modifier les noms ou les libellés du dispositif et de ses capteurs. Les comptes de niveau contrôle ne peuvent pas modifier les paramètres système ni apporter des modifications aux comptes d'autres utilisateurs.
- View-Only : si les droits administrateur et contrôle sont réglés sur *False*, le compte est un compte en lecture seule. Les seules modifications qu'un compte en lecture seule est autorisé à effectuer sont la modification de son propre mot de passe et la modification de la langue préférée de son propre compte. Les comptes en lecture seule ne peuvent modifier aucun paramètre du dispositif ou du système.
- Guest : tout utilisateur qui consulte la page Web de l'unité sans se connecter le fait en tant qu'invité. Par défaut, le compte Invité est un compte en lecture seule et ne peut modifier aucun paramètre, empêchant quiconque de modifier les noms, les libellés, les événements d'alarme ou les notifications sans se connecter. Le compte Invité ne peut pas être supprimé, mais il peut être désactivé, ce qui exige que l'utilisateur se connecte pour visualiser l'état du système.

Pour modifier le mot de passe d'un utilisateur :

1. Connectez-vous à votre compte.
2. Cliquez sur l'icône de modification d'un utilisateur.
3. Cliquez sur Username dans le coin supérieur droit de la page.
4. Saisissez un nouveau mot de passe et confirmez-le en le saisissant à nouveau dans le champ Verify Password.
5. Cliquez sur *SAVE*.

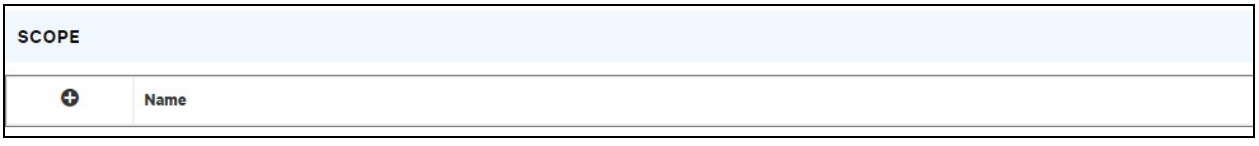
Figure 5.34 Page de modification du mot de passe d'un utilisateur



Pour ajouter ou modifier une portée d'utilisateur :

1. Cliquez sur l'icône d'ajout ou de modification d'une portée. Reportez-vous à la Figure 5.35 ci-dessous.
2. Créez ou modifiez les informations relatives à la portée si besoin.
   a. Label : saisissez le nom souhaité de la portée sélectionnée.
   b. Remote Authentication Attribute : utilisé pour tous les types d'authentification à distance.
   c. Cliquez sur les prises auxquelles l'utilisateur doit pouvoir accéder. (Elles s'affichent en vert)
3. Cliquez sur *OK* pour enregistrer les modifications.

Figure 5.35 Ajout d'une portée



Règles de mot de passe et paramètres de stratégie de compte

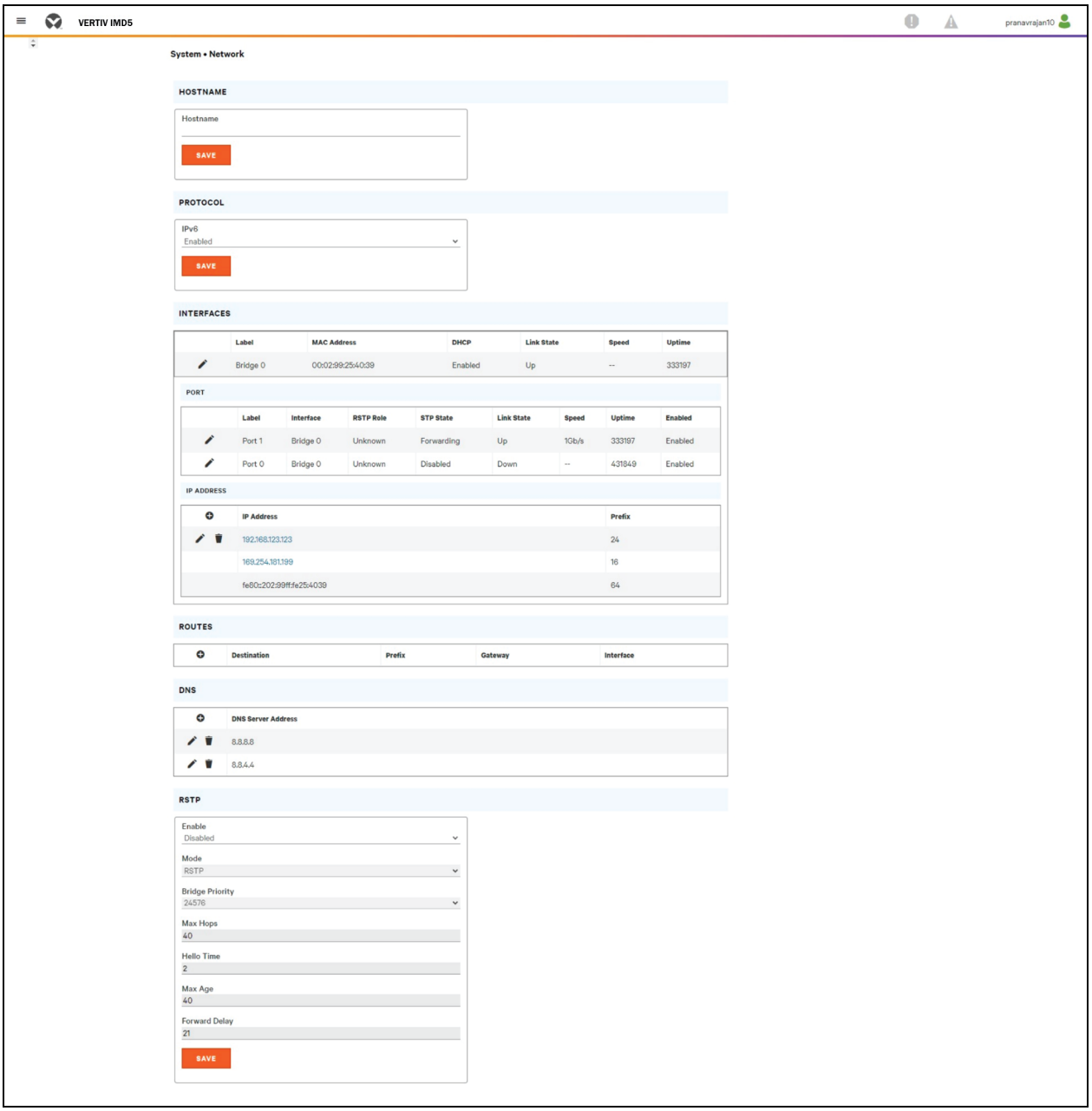
REMARQUE : un utilisateur sera automatiquement déconnecté au bout de 10 minutes d'inactivité.

5.6.2 Réseau

La configuration réseau de l'unité est définie dans l'onglet *Network* du menu System. Les paramètres relatifs à la connexion réseau de l'unité sont les suivants :

- **Hostname :** le nom d'hôte peut être utilisé comme méthode d'identification des dispositifs sur le réseau.
- **Protocol :** cliquez sur le menu déroulant IPv6, sélectionnez *Enabled* ou *Disabled*, puis cliquez sur *Save*.
- **Interfaces :** permet de configurer l'adresse IP de la rPDU Vertiv™ PowerIT, d'activer/de désactiver le protocole DHCP et d'afficher l'état de la liaison, la vitesse et le temps de disponibilité. Le dispositif prend en charge jusqu'à huit entrées d'adresses IP configurées par l'utilisateur.
- **Ports :** permet d'afficher et/ou de modifier les réglages de la voie Ethernet et l'état RSTP, l'interface, l'état STP, la vitesse et l'état de la liaison, la disponibilité et l'activation de chaque voie sur la rPDU PowerIT.
- **IP Address :** permet d'ajouter ou de modifier les adresses IP.
- **Routes :** affiche les routes configurées et c'est ici que vous définirez l'adresse de votre passerelle pour la rPDU Vertiv™ PowerIT. Les routes par défaut se distinguent par une *destination* **0.0.0.0** ou **::**, un préfixe **0** et une interface **all**. Une seule route par défaut peut exister pour IPv4 et un pour IPv6.
- **DNS :** permet à l'unité de résoudre les noms d'hôte des serveurs de messagerie, **NTP** et **SNMP**.
- **RSTP :** permet d'afficher et de modifier l'état de RSTP, le mode ainsi que les paramètres Bridge priority, Max Hops, Hello time Maximum age (Max) et Forward Delay.

Figure 5.36 Page de configuration du réseau

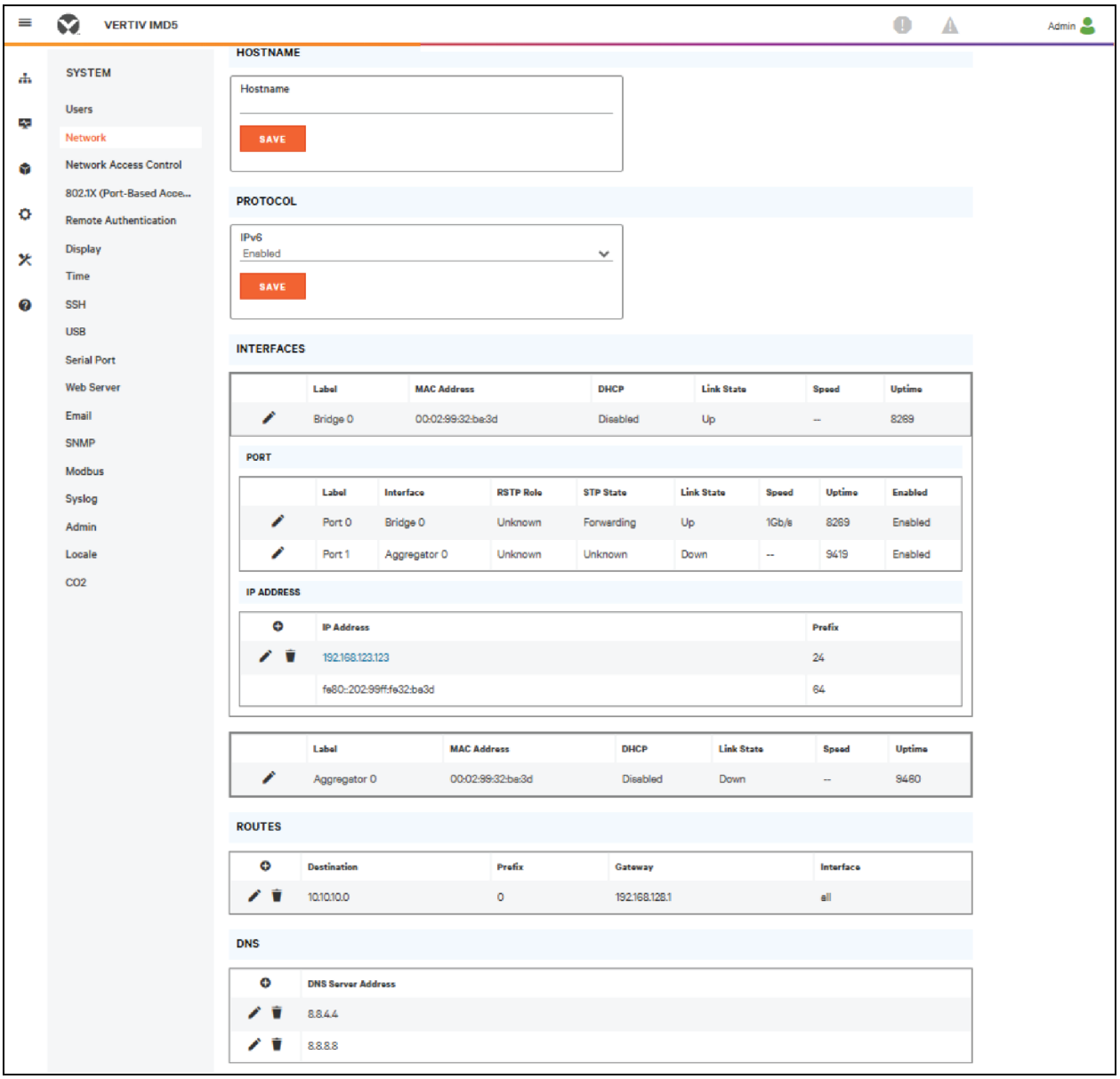


Pour modifier les paramètres de l'interface :

1. Cliquez sur l'icône de modification.
2. Modifiez les champs souhaités.
   a. **Label :** *modifiez* le nom souhaité de l'interface sélectionnée.
   b. **Enable :** *activez/désactivez* l'interface sélectionnée. Si une seule interface est disponible, la désactivation de l'interface restreint l'accès au dispositif, nécessitant une réinitialisation du réseau.
   c. **DHCP :** *activez/désactivez* le protocole DHCP sur l'interface sélectionnée.
3. Cliquez sur *SAVE*.

REMARQUE : toutes les modifications apportées aux paramètres de l'interface réseau prennent effet après que vous avez cliqué sur le bouton *Save*. Si vous avez modifié l'adresse IP, le dispositif ne répondra plus, car le navigateur ne pourra pas recharger la page Web. Fermez la fenêtre du navigateur, saisissez la nouvelle adresse IP dans la barre d'adresse du navigateur et l'unité sera accessible.

Figure 5.37 Paramètres de l'interface



Pour ajouter une interface pour un adaptateur USB sans fil :

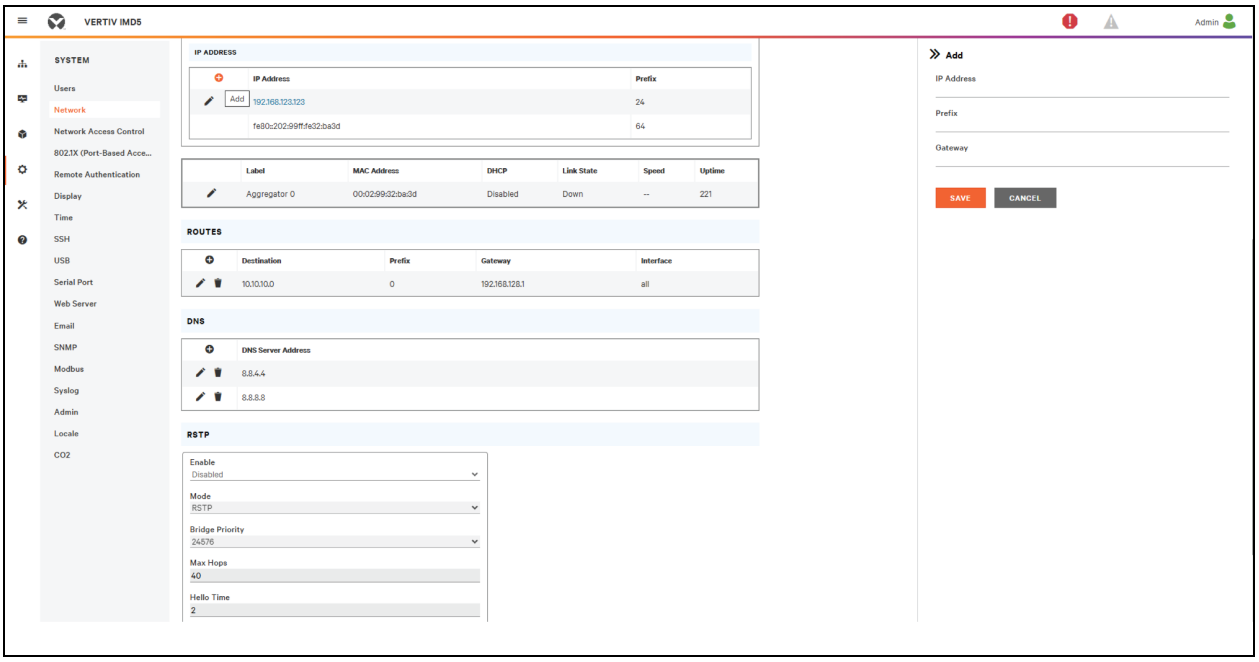
1. Insérez l'adaptateur USB sans fil dans la voie USB. (La rPDU sera inaccessible pendant quelques secondes pendant que la pile réseau se reconfigure.)
2. Une fois l'adaptateur détecté automatiquement, une interface Wi-Fi apparaît.
3. Cliquez sur l'icône de modification. Sélectionnez le SSID applicable dans le menu déroulant Detected SSIDs.

REMARQUE : reportez-vous à la section Adaptateurs USB sans fil TP-Link à la page 122 pour obtenir la liste des appareils sans fil TP-Link.

Pour ajouter une nouvelle adresse IP :

1. Cliquez sur l'icône d'ajout.
2. Saisissez l'adresse IPv4 ou IPv6 et le préfixe/masque de sous-réseau dans les champs appropriés. Jusqu'à huit adresses IP peuvent être attribuées de manière statique.
3. Cliquez sur *SAVE*.

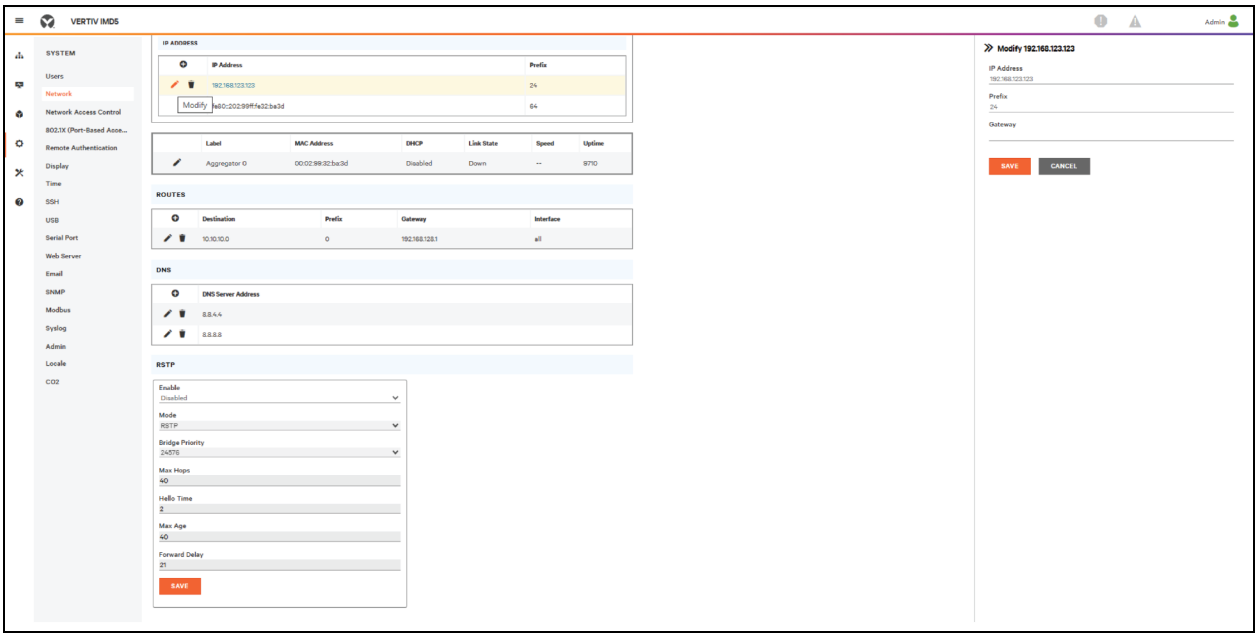
Figure 5.38 Ajouter une nouvelle adresse IP



Pour modifier une adresse IP existante :

1. Cliquez sur l'icône de modification.
2. Modifiez l'adresse IP et les champs Prefix/Subnet Mask, si nécessaire.
3. Cliquez sur *SAVE*.

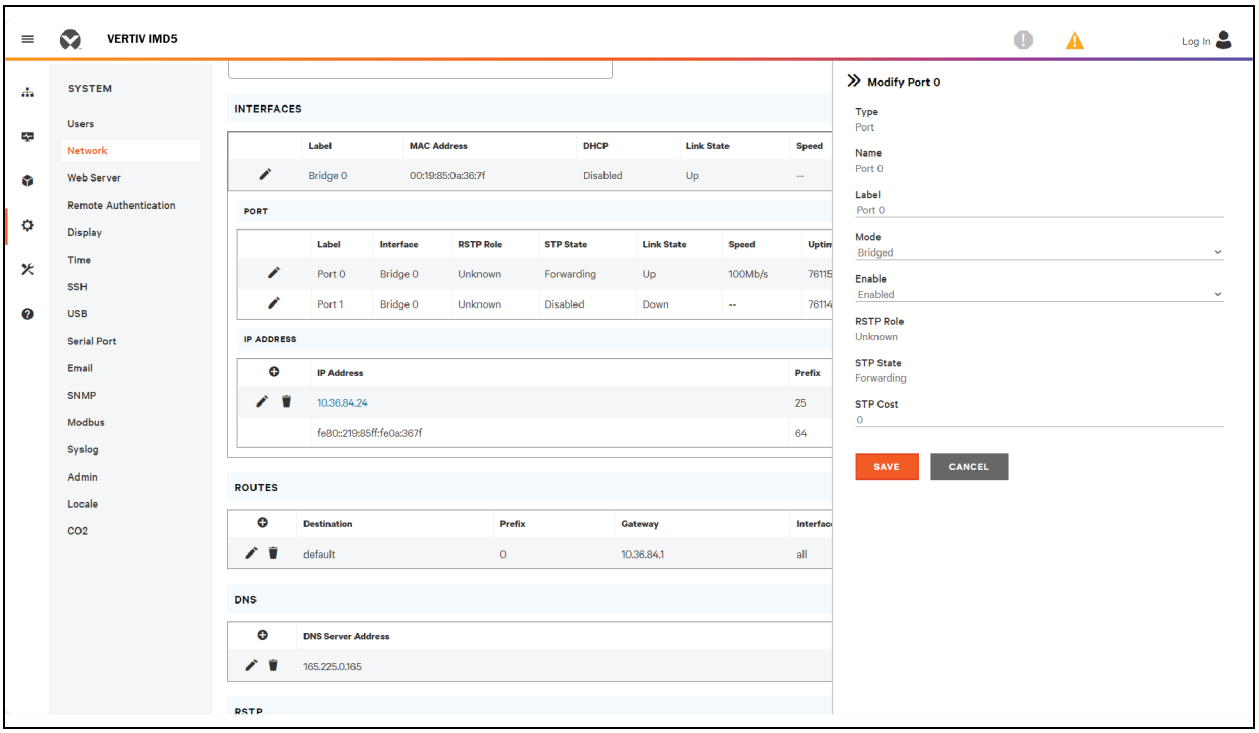
Figure 5.39 Modification de l'adresse IP



Pour modifier les paramètres de la voie :

1. Cliquez sur l'icône de modification.
2. Saisissez les informations appropriées.
   a. Modifiez le libellé de la voie si vous le souhaitez.
   b. Sélectionnez le mode Bridged/Independent.
   c. Activez/désactivez la voie.
   d. Attribuez l'état STP. Ce paramètre désigne la contribution de cette interface au coût du chemin racine lorsqu'elle sert de voie racine.
3. Cliquez sur *SAVE*.

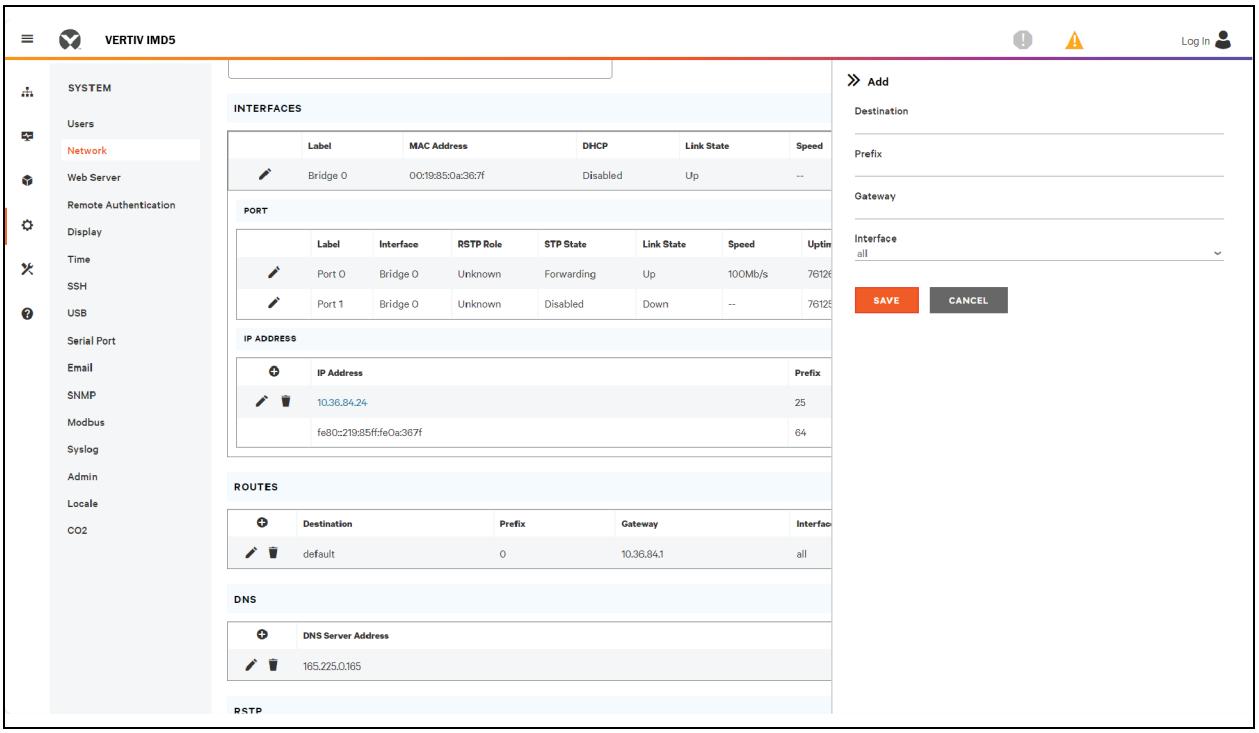
Figure 5.40 Modification du paramètre de la voie



Pour ajouter une nouvelle route :

1. Cliquez sur l'icône d'ajout.
2. Saisissez les informations appropriées.
    a. Adresse IP de destination de la route souhaitée.
    b. Renseignez le champ *Prefix* de la route souhaitée.
    c. Saisissez l'adresse IP de la passerelle.
    d. Sélectionnez l'*Interface* à laquelle s'applique la route.
3. Cliquez sur *SAVE*.

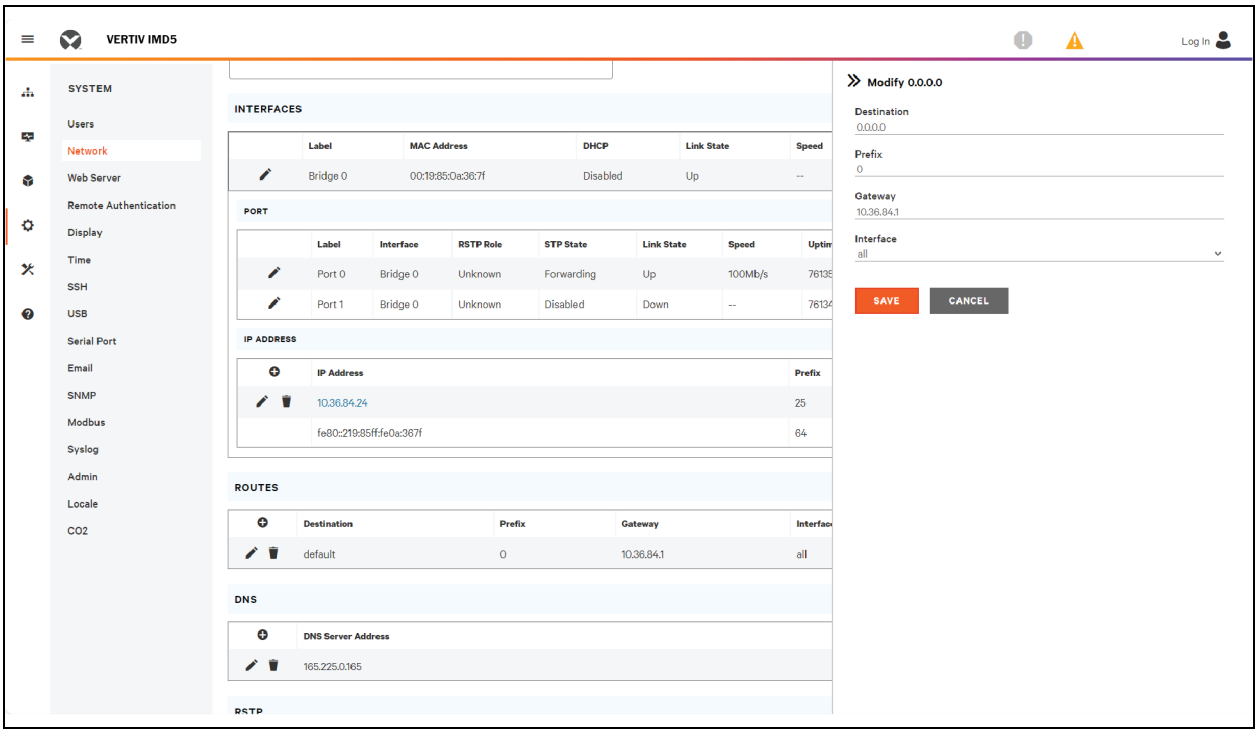
Figure 5.41 Ajout d'une route



Pour modifier une route existante :

1. Cliquez sur l'icône de modification.
2. Modifiez les champs souhaités.
3. Cliquez sur *SAVE*.

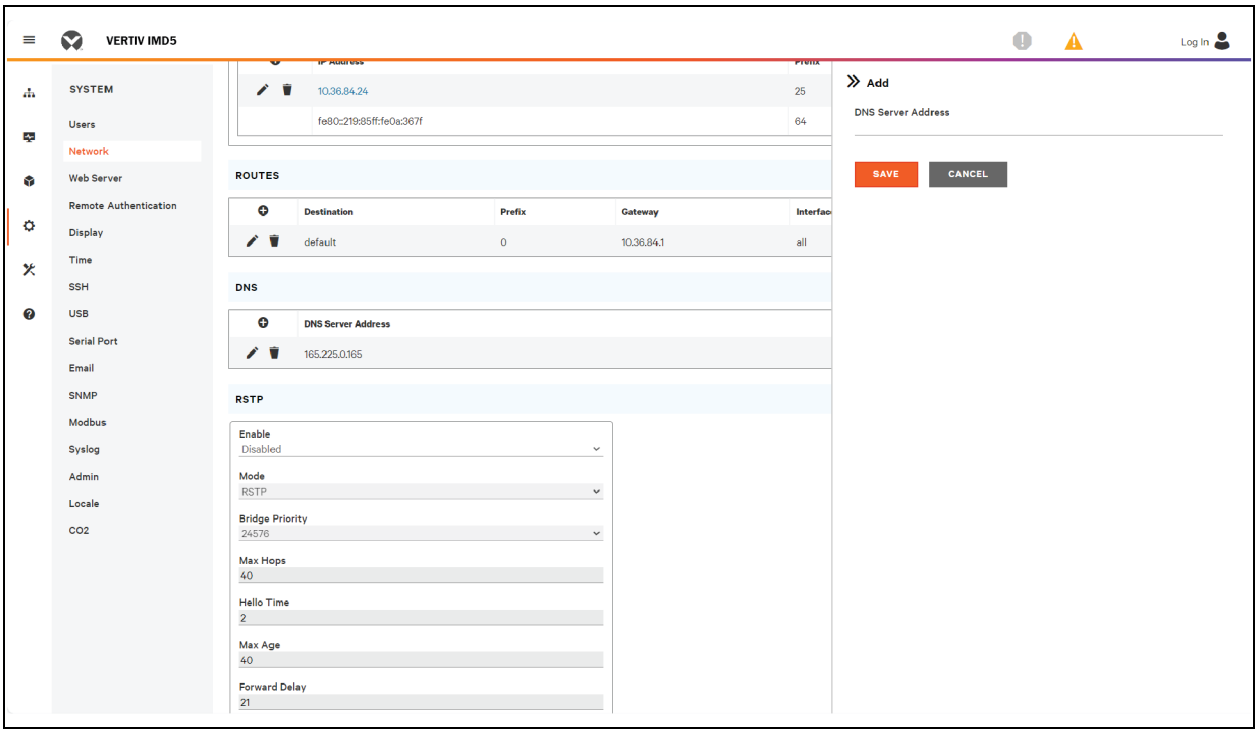
Figure 5.42 Modification d'une route



Pour ajouter une nouvelle adresse de serveur DNS :

1. Cliquez sur l'icône d'ajout.
2. Saisissez l'adresse IP du serveur DNS souhaité. Il est possible d'ajouter jusqu'à deux serveurs DNS.
3. Cliquez sur *SAVE*.

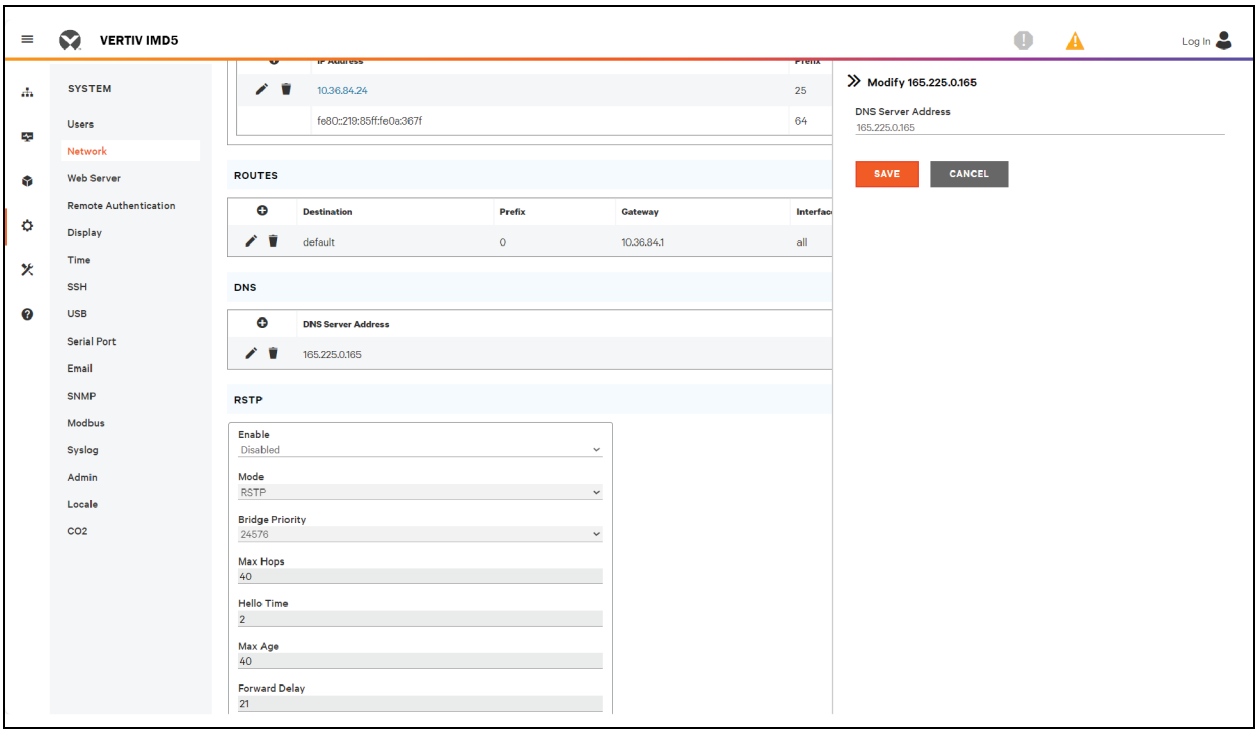
Figure 5.43 Ajout d'une adresse de serveur DNS



Pour modifier une adresse de serveur DNS existante :

1. Cliquez sur l'icône de modification.
2. Modifiez le champ DNS Server Address comme requis.
3. Cliquez sur *SAVE*.

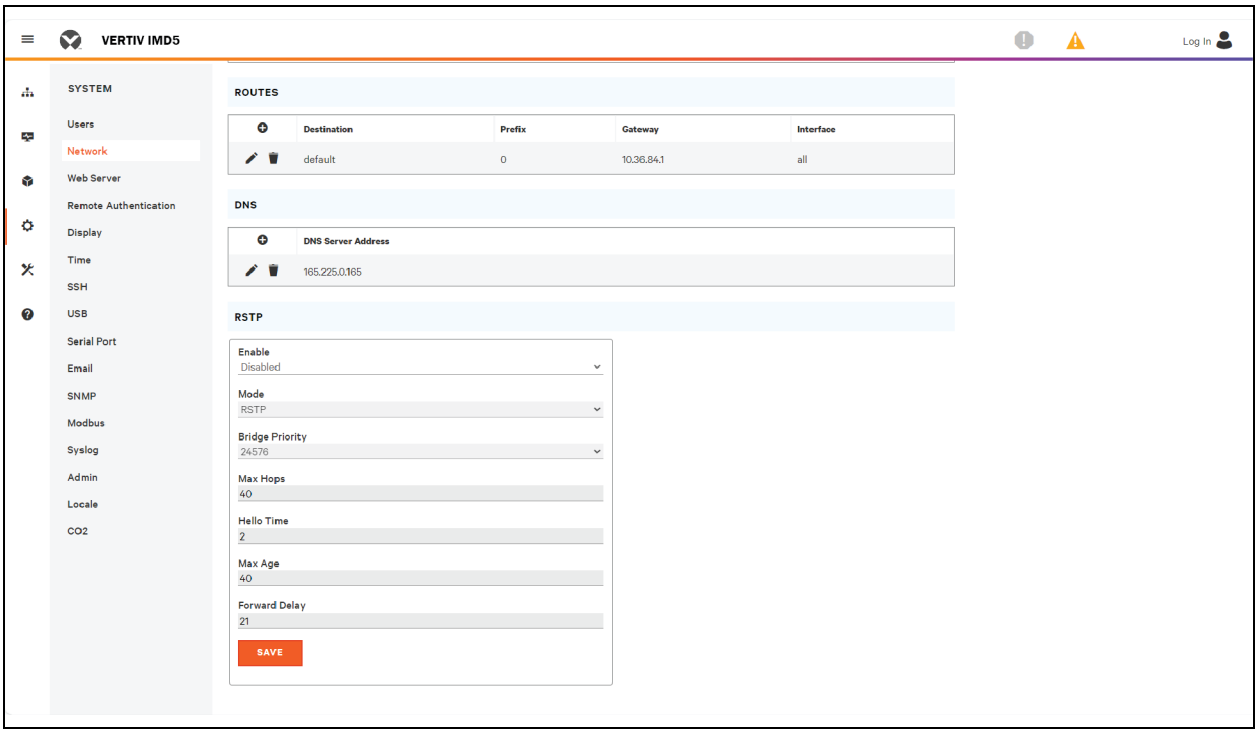
Figure 5.44 Modification de l'adresse d'un serveur DNS



Pour modifier les paramètres RSTP, procédez comme suit :

1. Modifiez les paramètres comme vous le souhaitez.
   a. **Enable :** activez ou désactivez le protocole RSTP.
   b. **Mode :** le mode RSTP prend en charge le retour à STP lorsque cela est nécessaire.
   c. **Bridge Priority :** cliquez sur le menu déroulant, sélectionnez la valeur appropriée, puis cliquez sur *Save*.
   d. **Max Hops :** ce paramètre est utilisé lorsque le mode RSTP est activé.
   e. **Hello Time :** intervalle, en secondes, entre les transmissions périodiques des messages de configuration par les voies désignées.
   f. **Max Age :** l'âge maximum, en secondes, des informations transmises par cette interface, lorsqu'elle sert de pont racine. Réglez cette valeur sur 2 secondes.
   g. **Forward Delay :** délai, en secondes, utilisé par les ponts pour faire passer le pont racine et les voies désignées en mode de transfert. Réglez cette valeur sur 21 secondes.
2. Cliquez sur *SAVE*.

Figure 5.45 Modification du paramètre RSTP



5.6.3 Serveur Web

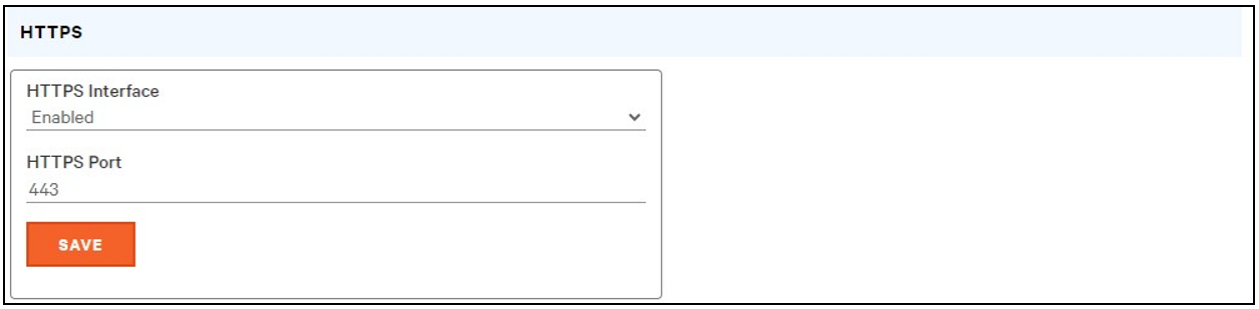
La configuration du serveur Web de l'unité peut être mise à jour dans l'onglet Web Server du menu System.

- HTTP Interface : activé ou redirigé vers HTTPS, tandis que l'interface HTTPS peut être activée ou désactivée. Lorsque l'interface HTTP est redirigée vers HTTPS et que l'interface HTTPS est désactivée, l'interface HTTP sera aussi effectivement désactivée.

REMARQUE : notez qu'il n'est pas possible de désactiver les protocoles HTTP, HTTPS et SSH simultanément.

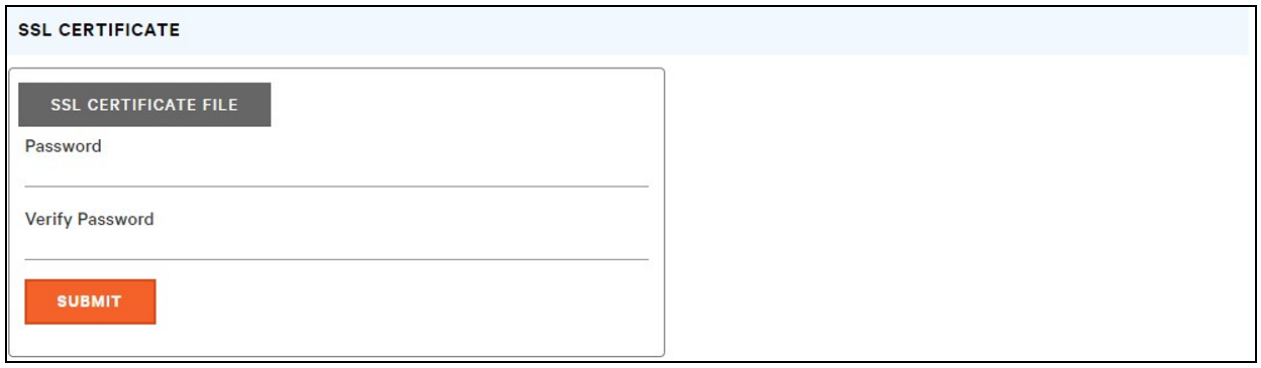
- HTTP/HTTPS Server Port : vous permet de modifier les voies TCP sur lesquelles les services HTTP et HTTPS écoutent les connexions entrantes. Les valeurs par défaut sont la voie 80 pour HTTP et la voie 443 pour HTTPS.

Figure 5.46 Page de configuration HTTP



- SSL Certificate : vous permet de télécharger votre propre fichier de certificat SSL signé pour remplacer le certificat par défaut. Le certificat peut être auto-signé ou signé par une autorité de certification. Le certificat SSL doit être au format *PEM* ou *PFX* (PKCS12).

Figure 5.47 Certificat SSL



- Format *PEM* :
  - Le certificat public et la clé privée doivent résider dans le même fichier.
  - Le certificat doit être conforme à la norme x.509.
  - La clé privée doit être générée avec l'algorithme RSA ou ECDSA. Elle doit être au format *PEM*.
    - Les clés RSA 2 048 bits ou inférieures ne sont pas prises en charge.
    - ECDSA prend en charge la taille de clé P-384.
  - La clé privée *PEM RSA* peut être protégée par mot de passe.
- Format *PFX* : la prise en charge de la norme PKCS12 (*.pfx*) est également disponible. Il s'agit d'une combinaison chiffrée binaire d'un certificat public *PEM* et de sa clé privée *PEM*. Lors de la génération d'un certificat *PFX*, vous êtes invité à saisir un mot de passe facultatif.

5.6.4 Authentification à distance

La page Remote Authentication vous permet de désigner l'un des trois protocoles d'authentification pour accéder au dispositif à distance. Par défaut, le dispositif utilise la base de données locale pour authentifier les utilisateurs. L'authentification à distance permet au dispositif d'authentifier un utilisateur auprès d'un serveur distant. En cas d'échec de l'authentification à distance, le système reviendra à l'authentification locale.

Pour modifier les paramètres d'authentification à distance :

1. Sélectionnez le mode requis dans le menu déroulant.
   - Disabled : Authentification locale.
   - LDAP : Lightweight Directory Access Protocol.
   - TACACS+ : Terminal Access Controller Access Control System Plus.
   - RADIUS : Remote Authentication Dial-In User Service.
2. Cliquez sur *SAVE*.

LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) peut être configuré via ce menu.

REMARQUE : vous devez connaître les paramètres de votre serveur LDAP pour pouvoir configurer la rPDU Vertiv™ PowerIT pour ce protocole d'authentification à distance. Si vous ne connaissez pas ces paramètres, consultez votre administrateur de serveur LDAP.

Configuration de l'authentification à distance à l'aide du protocole LDAP :

- **LDAP Server Address :** indiquez l'adresse de l'hôte pour LDAP. Le champ *HOST* peut être renseigné par une adresse IPv4, une adresse IPv6 entre crochets (p. ex., *[2001:0DB8:AC10:FE01::]*) ou un nom d'hôte.
- **LDAP Server Port :** utilisé pour définir le numéro de voie LDAP. La voie par défaut du protocole LDAP est *389* – utilisez cette voie pour le type de sécurité *None* ou *StartTLS*. Utilisez la voie *636* pour le type de sécurité *SSL*.
- **LDAP Mode :** Dans le menu déroulant, sélectionnez *Active Directory* ou **OpenLDAP**. Reportez-vous à la section Exemple de configuration de LDAP pour les informations d'identification Active Directory à la page 151.
- **Security Type :** dans le menu déroulant, sélectionnez *None*, *SSL* ou *StartTLS*.
- **Bind DN :** nom distinctif utilisé pour la liaison au serveur d'annuaire. Si les champs Bind DN et Bind Password sont laissés vides, cela signifie que la liaison est anonyme.
- **Bind Password :** mot de passe utilisé pour la liaison au serveur d'annuaire.
- **Base DN :** DN à utiliser pour la base de recherche.

Les champs restants proviennent du schéma NIS, défini dans RFC2307. Ils servent à authentifier les utilisateurs dans LDAP. Si ces champs sont laissés vides, les valeurs par défaut seront utilisées.

- **User Filter :** filtre LDAP pour la sélection d'utilisateurs.
- **« uid » Mapping :** nom de l'attribut serveur qui correspond à l'attribut *uid* dans le schéma.
- **« uidNumber » Mapping :** nom de l'attribut serveur qui correspond à l'attribut *uidNumber* dans le schéma.
- **Group Filter :** filtre LDAP pour la sélection de groupes.
- **« gid » Mapping :** nom de l'attribut serveur qui correspond à l'attribut *gid* dans le schéma.
- **« memberUid » Mapping :** nom de l'attribut serveur qui correspond à l'attribut *memberUid* dans le schéma.

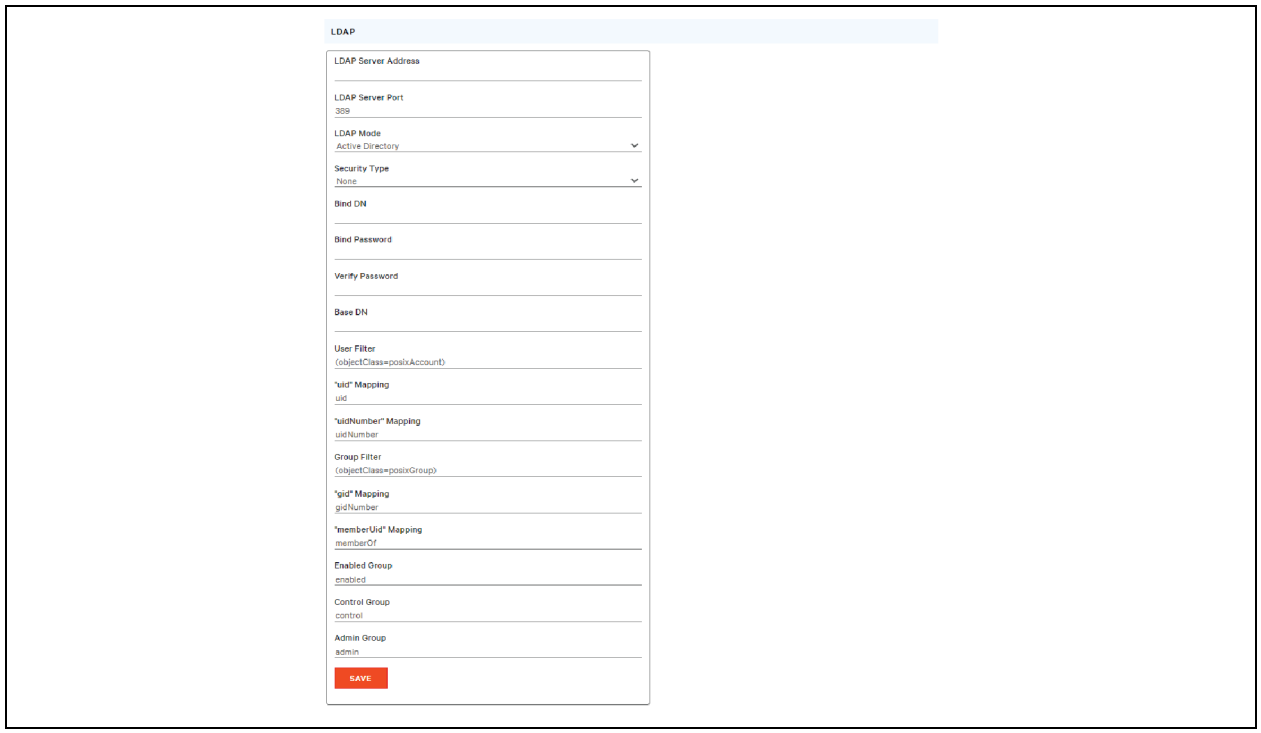
REMARQUE : les utilisateurs *doivent* renseigner le champ uidNumber. Une valeur nulle ou manquante entraînera l'échec d'une connexion valide. L'uidNumber *doit* être supérieur ou égal à 1 000. Une valeur inférieure à 1 000 entraînera l'échec d'une connexion valide.

- **Enabled Group :** les utilisateurs de ce groupe ont des droits de lecture seule, comme décrit dans la section Utilisateurs de ce manuel.
- **Control Group :** les utilisateurs de ce groupe ont des droits de contrôle, comme décrit dans la section Utilisateurs de ce manuel.
- **Admin Group :** les utilisateurs de ce groupe ont des droits d'administrateur, comme décrit dans la section Utilisateurs de ce manuel. Les utilisateurs LDAP ne sont pas comptabilisés dans le nombre minimum d'utilisateurs administrateur requis.

Cliquez sur *SAVE*.

Les champs Enabled Group, Control Group et Admin Group indiquent comment mapper des groupes sur les autorisations des utilisateurs. Un utilisateur doit appartenir à l'un de ces groupes pour pouvoir accéder au dispositif. Si un utilisateur appartient à plusieurs groupes, le groupe possédant l'autorisation la plus élevée est utilisé.

Figure 5.48 Menu LDAP



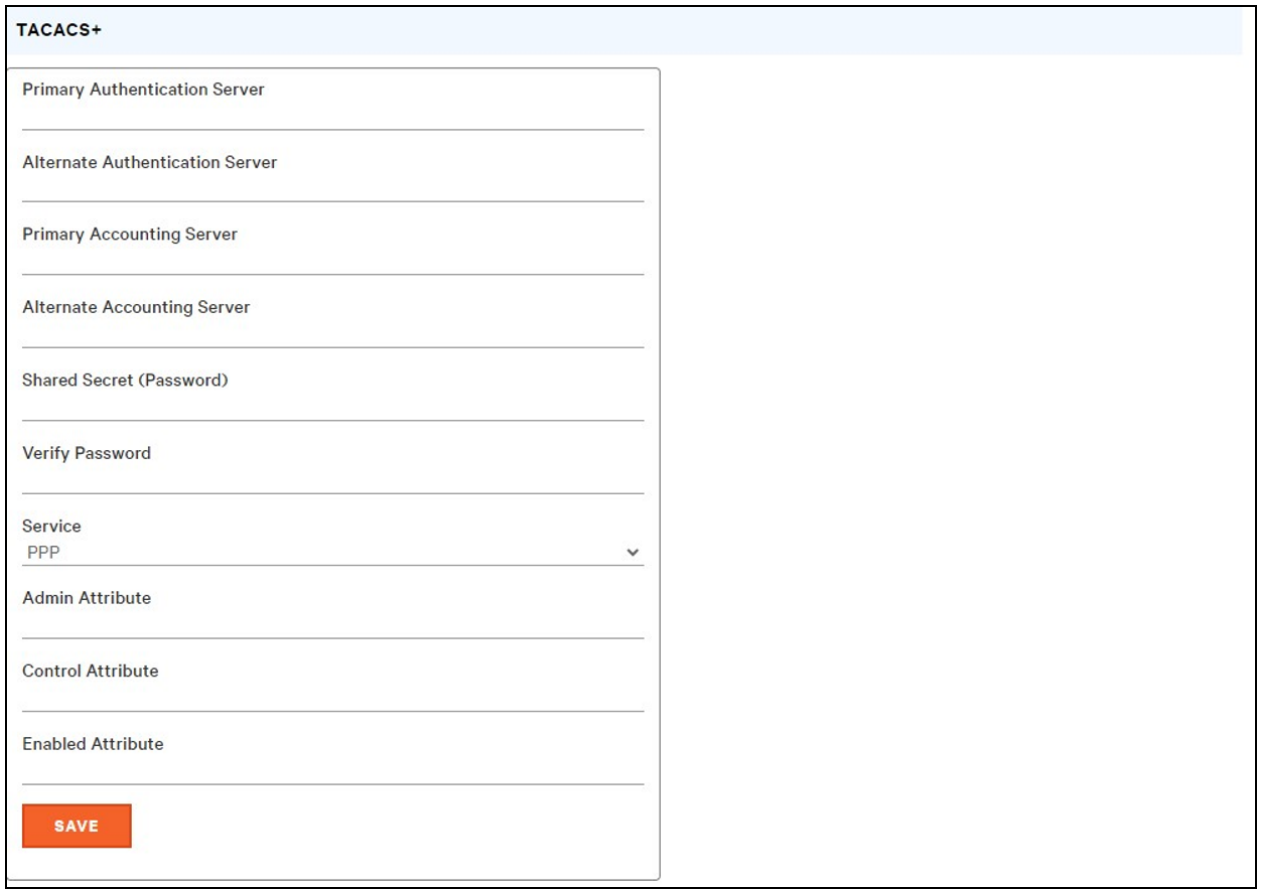
TACACS+

Le protocole TACACS+ (Terminal Access Controller Access-Control Plus) peut être configuré via ce menu.

REMARQUE : vous devez connaître les paramètres de votre serveur TACACS+ pour pouvoir configurer la rPDU Vertiv™ PowerIT pour ce protocole d'authentification à distance. Si vous ne connaissez pas ces paramètres, consultez votre administrateur serveur TACACS+.

Configuration de l'authentification à distance à l'aide du protocole TACACS+.

Figure 5.49 Menu TACACS+



- **Primary Authentication Server :** serveur d'authentification/d'autorisation principal, qui peut correspondre à une adresse IPv4, à une adresse IPv6 entre crochets (p. ex., *[2001:0DB8:AC10:FE01::]*) ou à un nom d'hôte. Le serveur d'authentification principal est utilisé à la fois pour l'authentification et l'autorisation. Cette adresse de serveur/nom d'hôte AA est obligatoire.
- **Alternate Authentication Server :** serveur d'authentification/d'autorisation alternatif, qui peut correspondre à une adresse IPv4, à une adresse IPv6 entre crochets ou à un nom d'hôte. Le serveur d'authentification secondaire est utilisé à la fois pour l'authentification et l'autorisation.
- **Primary Accounting Server :** serveur de comptabilité principal, qui peut correspondre à une adresse IPv4, à une adresse IPv6 entre crochets ou à un nom d'hôte. Le serveur de comptabilité principal est facultatif. S'il est configuré, le serveur est averti lorsqu'un utilisateur est autorisé.
- **Alternate Accounting Server :** serveur de comptabilité alternatif, qui peut correspondre à une adresse IPv4, à une adresse IPv6 entre crochets ou à un nom d'hôte. Le serveur de comptabilité secondaire est facultatif. S'il est configuré, le serveur est averti lorsqu'un utilisateur est autorisé.
- **Shared Secret (Password) :** saisissez un mot secret ou une phrase secrète dans le champ Shared Secret (s'applique aux serveurs d'authentification et de comptabilité principaux et secondaires).
- **Service :** valeur à utiliser pour le champ de service dans les demandes TACACS+. Les options valides sont *PPP* et *raccess*.
- **Admin Attribute :** un utilisateur possédant cet attribut aura des droits d'*administrateur*, comme décrit dans la section Utilisateurs de ce manuel. Les utilisateurs TACACS+ ne sont pas comptabilisés dans le nombre minimum d'utilisateurs administrateur requis.

- Control Attribute : les utilisateurs possédant cet attribut auront des droits de contrôle, comme décrit dans la section Utilisateurs de ce manuel.
- Enabled Attribute : les utilisateurs possédant cet attribut auront des droits de lecture seule, comme décrit dans la section Utilisateurs de ce manuel.

Cliquez sur *SAVE*.

REMARQUE : les paires attribut-valeur (PAV) renvoyées par le serveur lors de l'authentification/ autorisation déterminent les autorisations de l'utilisateur. Le champ Group Attribute indique au système quelle PAV contient le groupe d'accès de l'utilisateur. Si la valeur PAV correspond au champ Admin Group, l'utilisateur dispose d'un accès administrateur (total). Si la valeur PAV correspond au champ Control Group, l'utilisateur dispose d'un accès de contrôle. Si la valeur PAV correspond au champ Enabled Group, l'utilisateur dispose d'un accès en lecture seule. Si aucune correspondance n'est trouvée, l'utilisateur n'aura pas accès à l'unité. Un champ Group vide ne correspondra à aucune valeur PAV.

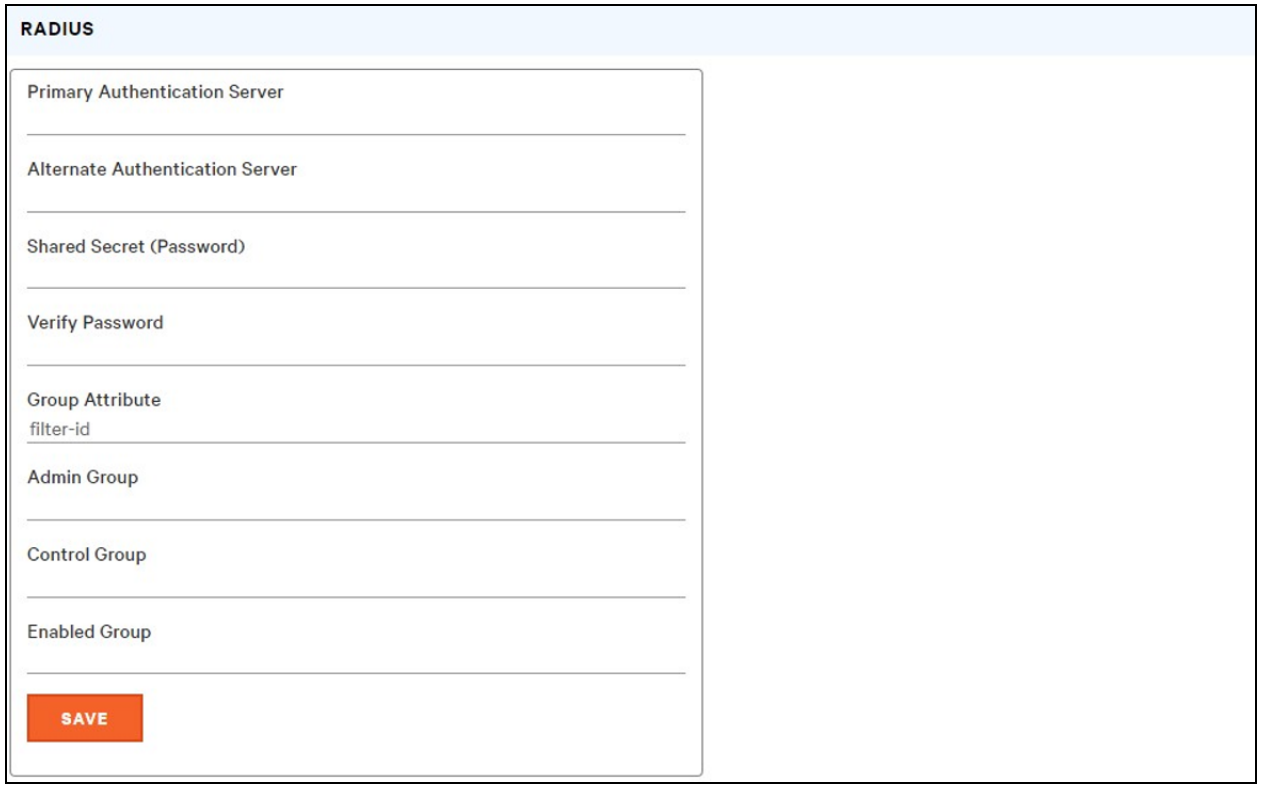
RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service) peut être configuré via ce menu.

REMARQUE : vous devez connaître les paramètres de votre serveur RADIUS pour pouvoir configurer la rPDU Vertiv™ PowerIT pour ce protocole d'authentification à distance. Si vous ne connaissez pas ces paramètres, consultez votre administrateur de serveur RADIUS.

Configuration de l'authentification à distance à l'aide du protocole RADIUS.

Figure 5.50 Menu RADIUS



- **Primary Authentication Server :** saisissez l'adresse IP du serveur d'authentification/d'autorisation/de comptabilité principal. Le serveur d'authentification principal peut correspondre à une adresse IPv4, à une adresse IPv6 entre crochets (p. ex., *[2001:0DB8:AC10:FE01::]*) ou à un nom d'hôte. Le serveur d'authentification principal est utilisé à la fois pour l'authentification, l'autorisation et la comptabilité. Ce serveur AA est obligatoire.
- **Alternate Authentication Server :** le cas échéant, saisissez l'adresse IP de l'autre serveur d'authentification/autorisation/comptabilité. Le serveur d'authentification alternatif peut correspondre à une adresse IPv4, à une adresse IPv6 entre crochets ou à un nom d'hôte. Le serveur d'authentification secondaire est utilisé à la fois pour l'authentification, l'autorisation et la comptabilité.
- **Shared Secret (Password) :** saisissez un mot secret ou une phrase secrète dans le champ Shared Secret (s'applique aux serveurs d'authentification et de comptabilité principaux et secondaires).
- **Group Attribute :** identifie la paire attribut-valeur (PAV) qui indique à quel groupe d'accès appartient l'utilisateur. Les valeurs correctes sont *filter-id* et *management-privilege-level*.
- **Admin Group :** les utilisateurs de ce groupe ont des droits d'administrateur, comme décrit dans la section Utilisateurs de ce manuel.
- **Control Group :** les utilisateurs de ce groupe ont des droits de contrôle, comme décrit dans la section Utilisateurs de ce manuel.
- **Enabled Group :** pour les utilisateurs de ce groupe, les droits de lecture seule sont **activés** comme décrit dans la section Utilisateurs de ce manuel.

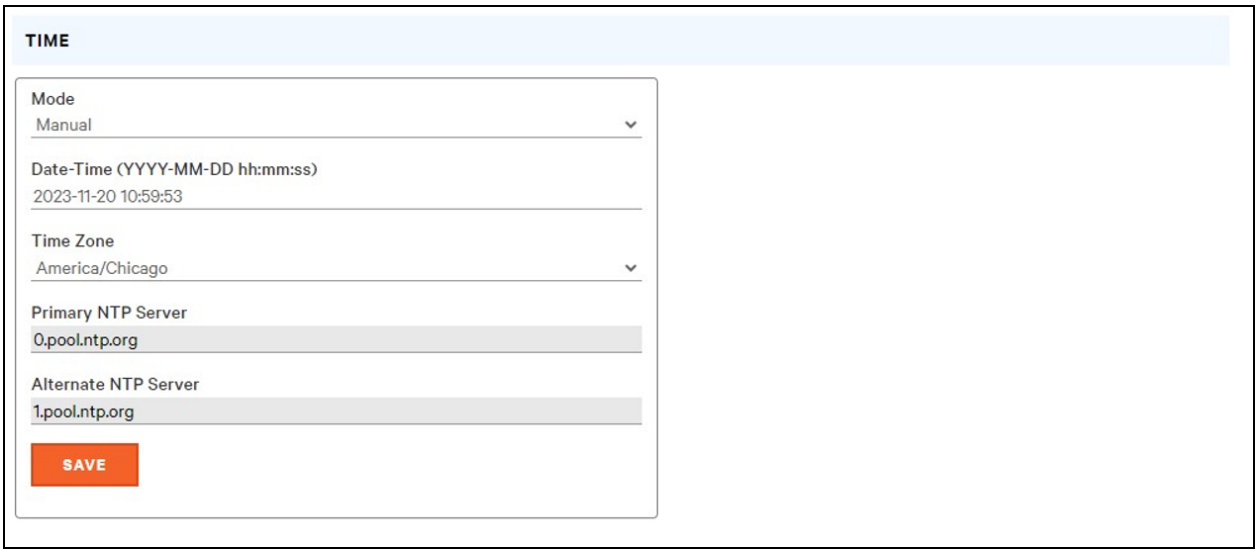
Cliquez sur *SAVE*.

REMARQUE : les paires attribut-valeur (PAV) renvoyées par le serveur lors de l'authentification/autorisation déterminent les autorisations de l'utilisateur. Le champ Group Attribute indique au système quelle PAV contient le groupe d'accès de l'utilisateur. Si la valeur PAV correspond au champ Admin Group, l'utilisateur dispose d'un accès administrateur (total). Si la valeur PAV correspond au champ Control Group, l'utilisateur dispose d'un accès de contrôle. Si la valeur PAV correspond au champ Enabled Group, l'utilisateur dispose d'un accès en lecture seule. Si aucune correspondance n'est trouvée, l'utilisateur n'aura pas accès à l'unité. Un champ Group vide ne correspondra à aucune valeur PAV.

5.6.5 Time

L'heure et la date du dispositif sont réglées sur cette page.

Figure 5.51 Page de configuration de l'heure



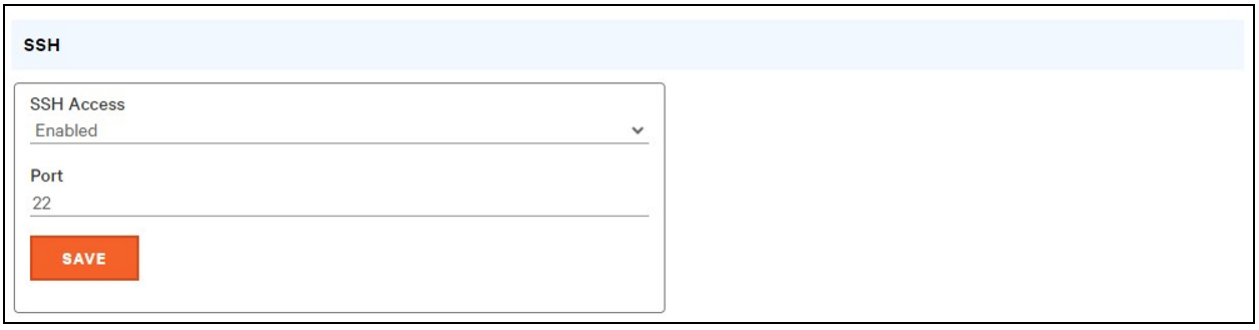
Deux modes sont disponibles :

- Network Time Protocol (NTP) : synchronise l'heure et la date de l'unité avec le fuseau horaire spécifié à l'aide des serveurs NTP répertoriés. Les serveurs NTP peuvent être reconfigurés.
- Manual : dans ce mode, la date et l'heure doivent être saisies comme indiqué à gauche du champ.

5.6.6 SSH

Le menu SSH vous permet de configurer les réglages d'accès SSH au dispositif.

Figure 5.52 Page de configuration SSH



- SSH Access : active ou désactive l'accès via SSH.
- SSH Port : vous permet de modifier la voie sur laquelle le service SSH écoute les connexions entrantes. La valeur par défaut est la voie 22.

REMARQUE : un utilisateur SSH sera automatiquement déconnecté après 10 minutes d'inactivité.

5.6.7 USB

Pour activer ou désactiver la voie USB :

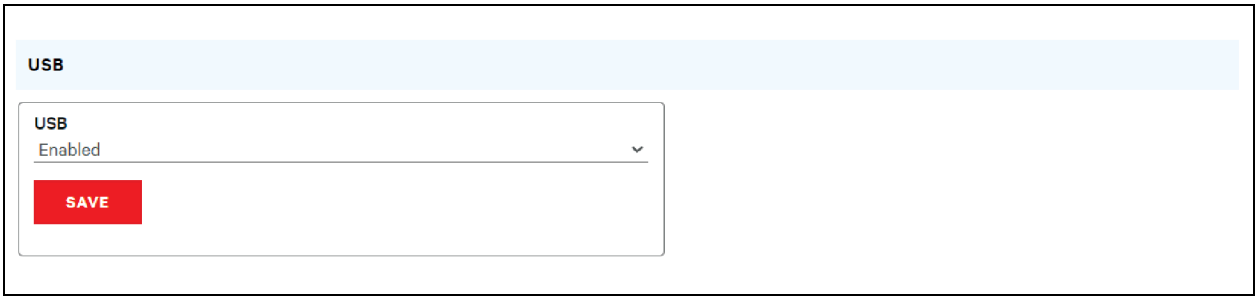
1. Sélectionnez Enable ou Disable dans le menu déroulant.
2. Cliquez sur le bouton *SAVE*.

Lorsque la voie USB est activée, les dispositifs USB connectés sont affichés sur l'interface Web.

REMARQUE : le dispositif USB doit être formaté en FAT32.

Si un dispositif de stockage USB valide est détecté et des données historiques sont enregistrées, ces données sont également stockées dans un fichier sur le dispositif de stockage USB. S'il n'existe pas déjà, un fichier appelé log-1.csv est créé dans un répertoire log au niveau supérieur du système de fichiers. Si des fichiers journaux existent déjà, celui qui porte le numéro d'identifiant le plus élevé dans le titre est utilisé comme point de départ. À chaque période de journalisation, de nouvelles données sont ajoutées dans ce fichier au même format que la récupération CSV. Si des points de données sont créés ou supprimés par rapport à ceux répertoriés dans l'en-tête CSV, un nouveau fichier est créé avec le numéro séquentiel suivant. Si le système de fichiers est plein, la journalisation cesse.

Figure 5.53 USB



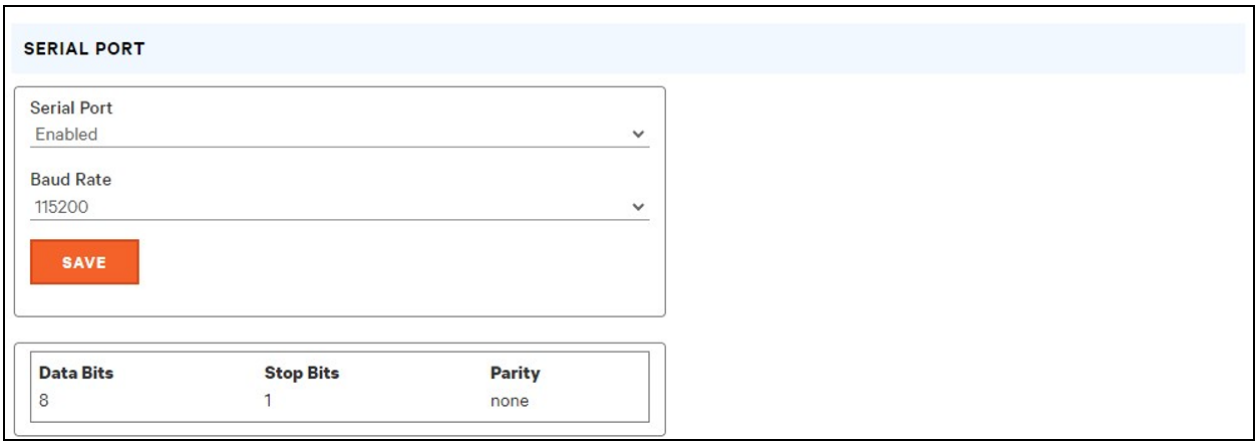
5.6.8 Voie série

REMARQUE : la connexion série ne prend pas en charge le contrôle du flux.

Le menu Serial Port permet de configurer les paramètres de la voie série, d'activer ou de désactiver la voie et de définir le débit en bauds.

1. Cliquez sur le menu déroulant Serial Port et sélectionnez *Enabled/Disabled*.
2. Cliquez sur le menu déroulant *Baud Rate* et sélectionnez la valeur du débit en bauds.
3. Cliquez sur *SAVE*.

Figure 5.54 Menu déroulant System, Menu – Serial Port



5.6.9 Email

L'unité peut envoyer des notifications par e-mail à un maximum de dix (10) adresses e-mail en cas d'alarme ou d'avertissement.

Figure 5.55 Page de configuration de la messagerie

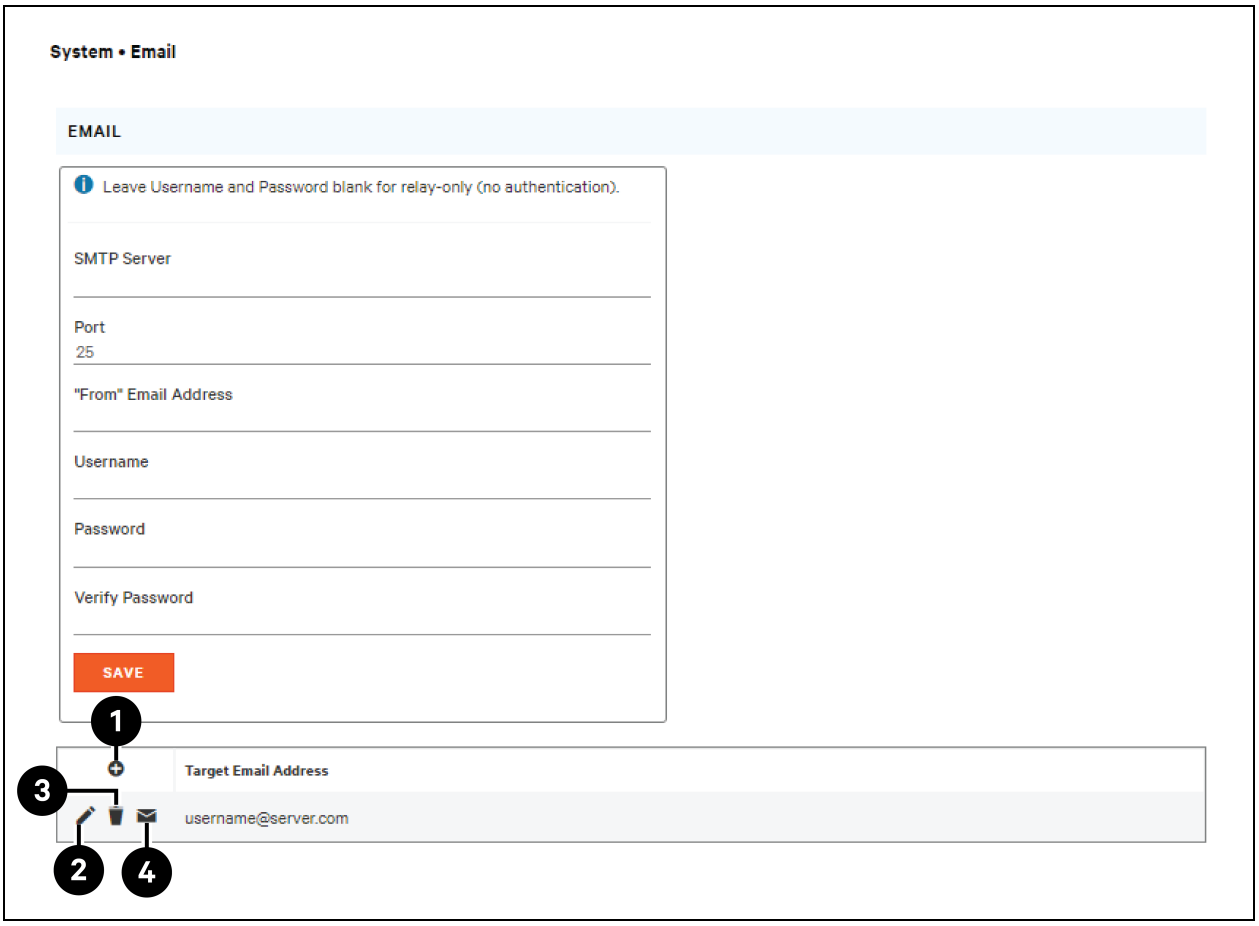


Tableau 5.12 Description de la page de configuration de la messagerie

Élément	Description
1	Ajouter une nouvelle adresse e-mail cible.
2	Modifier l'adresse e-mail cible existante.
3	Supprimer l'adresse e-mail cible existante.
4	Envoyer un e-mail de test.

Pour envoyer des e-mails, l'unité doit être configurée pour accéder au serveur de messagerie, comme suit :

- SMTP Server : nom ou adresse IP d'un serveur SMTP ou ESMTP approprié.
- Port : voie TCP que le serveur SMTP utilise pour fournir les services de messagerie. Les valeurs typiques sont la voie 25 pour une connexion non chiffrée ou 465 et 587 pour une connexion chiffrée TLS/SSL, mais celles-ci peuvent varier en fonction de la configuration du serveur de messagerie.
- From Email Address : adresse d'où semblent provenir les e-mails de l'unité. De nombreux services de messagerie hébergés, tels que Gmail, exigent qu'il s'agisse du compte de messagerie d'un utilisateur valide.
- Username et Password : informations de connexion du serveur de messagerie. Si votre serveur ne nécessite pas d'authentification (relais ouvert), ces champs peuvent être laissés vides.

Les serveurs Microsoft Exchange doivent être configurés pour autoriser le relais SMTP depuis l'adresse IP de l'unité. En outre, le serveur Exchange doit être configuré pour autoriser l'authentification de base, afin que l'unité puisse se connecter avec la méthode AUTH LOGIN d'envoi de ses informations de connexion. Les autres méthodes, par exemple AUTH PLAIN et AUTH MD5, ne sont pas prises en charge.

Pour ajouter ou modifier une adresse e-mail cible :

1. Cliquez sur l'icône d'ajout ou de modification.
2. Saisissez l'adresse e-mail, puis cliquez sur *Save*.

Pour supprimer une adresse e-mail cible :

1. Cliquez sur l'icône de suppression à côté de l'adresse que vous souhaitez supprimer.
2. Cliquez sur *Delete* dans la fenêtre contextuelle pour confirmer.

Pour envoyer un e-mail de test :

1. Cliquez sur l'icône d'e-mail de test à côté de l'adresse à tester.
2. Une fenêtre contextuelle indique que l'e-mail de test est en cours d'envoi ; cliquez sur *OK* pour fermer la fenêtre contextuelle.

5.6.10 SNMP

Le protocole SNMP (Simple Network Management Protocol) peut être utilisé pour surveiller les mesures et l'état de l'unité. Le système prend en charge les services SNMP V1, V2c et V3. En outre, les interruptions d'alarme peuvent être envoyées à dix adresses IP au maximum.

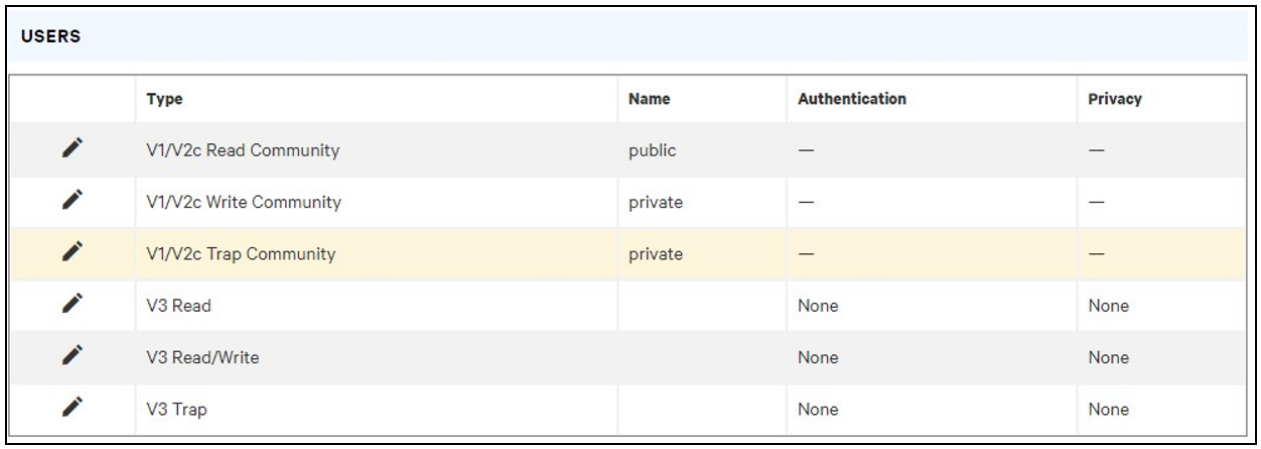
Cliquez sur ***ZIP*** pour télécharger le fichier ***mib.zip*** contenant à la fois le fichier MIB et la feuille de calcul au format CSV.

Les services SNMP-V1/V2c et SNMP-V3 peuvent être activés ou désactivés de manière indépendante. Le service écoute les demandes de lecture de données sur la voie 161, qui est la valeur par défaut habituelle pour les services SNMP ; ce paramètre peut aussi être modifié.

La base d'informations de gestion (MIB) peut être téléchargée à partir de l'unité, via le lien ZIP en haut de la page Web. Si vous cliquez sur ce lien, vous téléchargerez une archive .Zip contenant à la fois le fichier MIB et une feuille de calcul au format CSV décrivant les OID disponibles sous une forme lisible par l'homme afin de vous aider à configurer votre gestionnaire SNMP pour lire les données à partir de l'unité.

Figure 5.56 Page de configuration SNMP

Figure 5.57 Page de configuration des utilisateurs SNMP



La section Users vous permet de configurer les différentes communautés de lecture, d'écriture et d'interruptions pour les services SNMP. Vous pouvez également configurer les types d'authentification et les méthodes de chiffrement utilisés pour le service SNMP V3, si vous le souhaitez. Cliquez sur l'icône de modification pour modifier les paramètres.

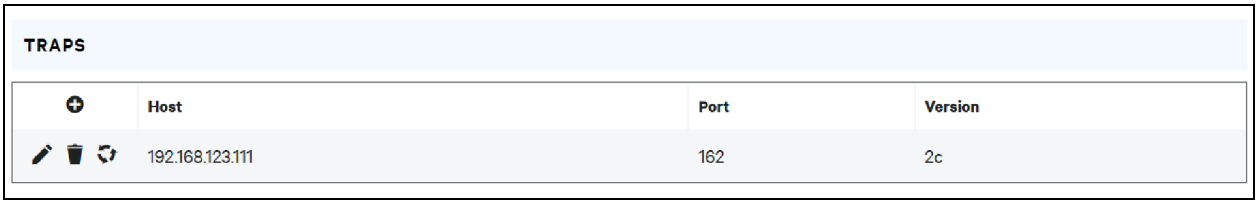
Les interruptions permettent de définir les types SNMP que vous souhaitez envoyer et les adresses IP des destinataires.

Pour configurer une destination d'interruption :

1. Localisez la section *Traps* de la page SNMP, puis cliquez sur l'icône d'ajout.
2. Saisissez l'adresse IP à laquelle l'interruption doit être envoyée dans le champ Host.
3. Modifiez le numéro de voie, si nécessaire.
4. Sélectionnez la version d'interruption à utiliser (V1, V2c ou V3) et cliquez sur *SAVE*.

Une interruption de test peut être envoyée en cliquant sur l'icône de test à côté de l'adresse IP de l'hôte. Vous pouvez également mettre à jour/modifier les paramètres de l'interruption. Cliquez sur l'icône de modification à côté de l'adresse IP de l'hôte.

Figure 5.58 Interruption



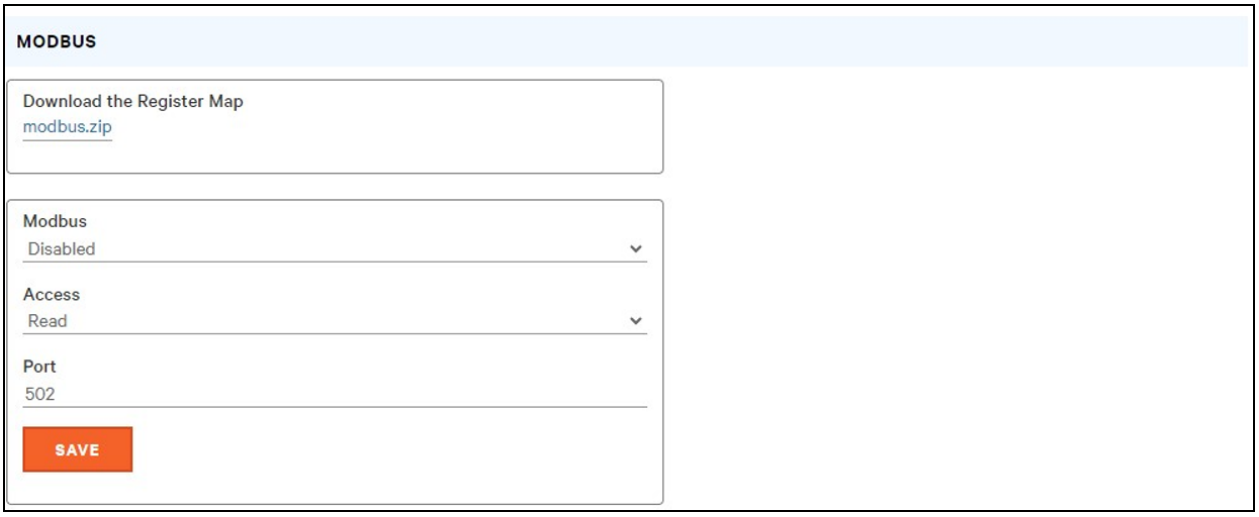
5.6.11 Modbus

Le protocole de communication Modbus TCP peut être utilisé pour surveiller les mesures et l'état de l'unité. Il permet également à l'utilisateur de régler les paramètres de l'unité.

La carte du registre peut être téléchargée à partir de l'unité, via le lien ZIP en haut de la page Web. Si vous cliquez sur ce lien, vous téléchargerez une archive .zip contenant une feuille de calcul au format CSV décrivant le mappage Modbus sous une forme lisible par l'homme afin de vous aider à configurer votre gestionnaire Modbus pour lire/écrire les données sur l'unité.

Le protocole de communication Modbus peut être activé ou désactivé. L'accès Modbus à l'unité peut être *Read* ou *Read/Write*. Les demandes de lecture ou d'écriture de données sont effectuées sur la voie 502, qui est la valeur par défaut habituelle pour le protocole Modbus ; cette voie peut également être modifiée.

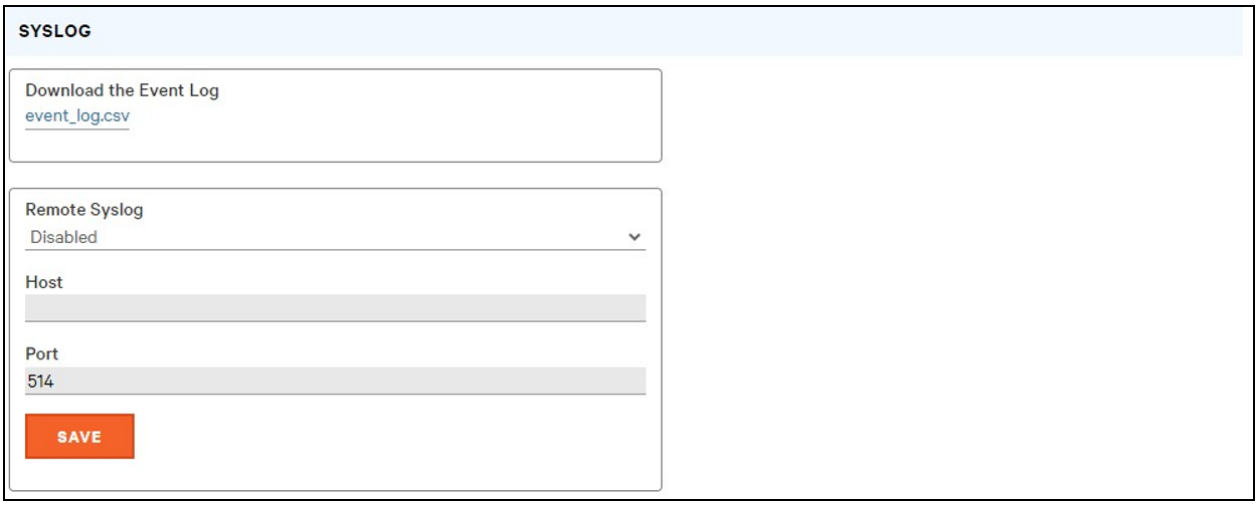
Figure 5.59 Modbus



5.6.12 SYSLOG

Les données Syslog peuvent être capturées à distance, mais elles doivent d'abord être configurées et activées sur la page SYSLOG.

Figure 5.60 SYSLOG



REMARQUE : cette fonction est principalement utile à des fins de diagnostic et doit normalement être laissée désactivée à moins que le service d'assistance technique de Vertiv™ ne conseille de l'activer pour résoudre un problème particulier.

L'utilisation du bouton Download the Event Log CSV nécessite que l'utilisateur dispose d'un accès administrateur.

5.6.13 Admin

La page Admin permet à l'administrateur du dispositif d'enregistrer ses coordonnées ainsi que la description et l'emplacement du dispositif. Une fois que les informations sont enregistrées par un administrateur, d'autres utilisateurs (non-administrateurs) peuvent les consulter. En outre, le libellé du système peut être modifié sur cette page. Ce libellé apparaît généralement dans la barre de titre de la fenêtre du navigateur Web et/ou dans les onglets du navigateur qui observent actuellement le dispositif.

5.6.14 Paramètres régionaux

La page Locale permet de définir la langue et les unités de température par défaut du dispositif. Ces paramètres deviendront les options d'affichage par défaut du dispositif, bien que les utilisateurs individuels puissent modifier ces options pour leurs propres comptes. Le compte invité ne pourra voir le dispositif qu'avec les options définies ici.

5.7 Sous-menu Utilities

Le sous-menu Utilities offre la possibilité de rétablir les valeurs par défaut, de redémarrer le système de communication et de mettre à jour le firmware.

5.7.1 Sauvegarde et restauration de la configuration

Enregistrez les paramètres de configuration actuels et restaurez les paramètres de configuration précédents, si nécessaire.

Tableau 5.13 Options de sauvegarde et de restauration

Option	Description
Download Configuration Backup File	Les téléchargements ne nécessitent pas d'authentification de l'utilisateur. Le nom du fichier téléchargé est **backup_XXX.bin**, XXX représentant sous forme de chaîne l'adresse MAC de l'interface **Ethernet** de l'unité sans les caractères :.
Backup File	Charge le fichier de sauvegarde de la configuration. Cela nécessite une authentification de l'utilisateur et l'utilisateur doit disposer de droits d'administrateur. Un fichier de sauvegarde ne peut être utilisé que pour charger la configuration sur des unités dont le numéro de modèle est identique.

Pour enregistrer les paramètres de configuration actuels :

1. Sélectionnez *Download Configuration Backup File*.
2. Cliquez sur *BIN*.

REMARQUE : l'enregistrement de la configuration ne nécessite pas d'authentification de l'utilisateur.

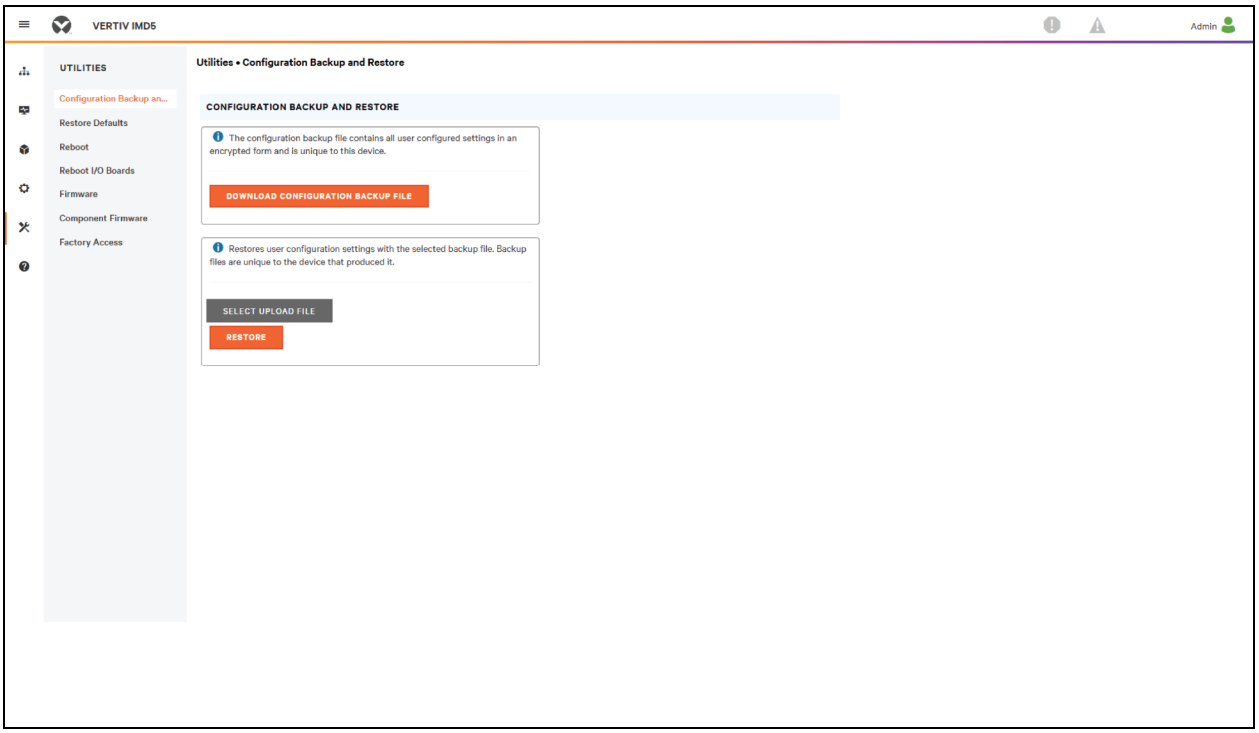
Pour restaurer un paramètre de configuration antérieur :

1. Cliquez sur *Backup File*.
2. Cliquez sur *SELECT UPLOAD FILE*.
3. Sélectionnez le fichier de sauvegarde.
4. Cliquez sur *RESTORE*.

REMARQUE : la restauration des configurations nécessite une authentification de l'utilisateur et celui-ci doit disposer de droits d'administrateur.

REMARQUE : un fichier de sauvegarde ne peut être utilisé que pour charger la configuration sur des unités dont le numéro de modèle est identique.

Figure 5.61 Présentation de la sauvegarde et de la restauration de la configuration



5.7.2 Restaurer les paramètres par défaut

Vous avez la possibilité de restaurer les paramètres par défaut.

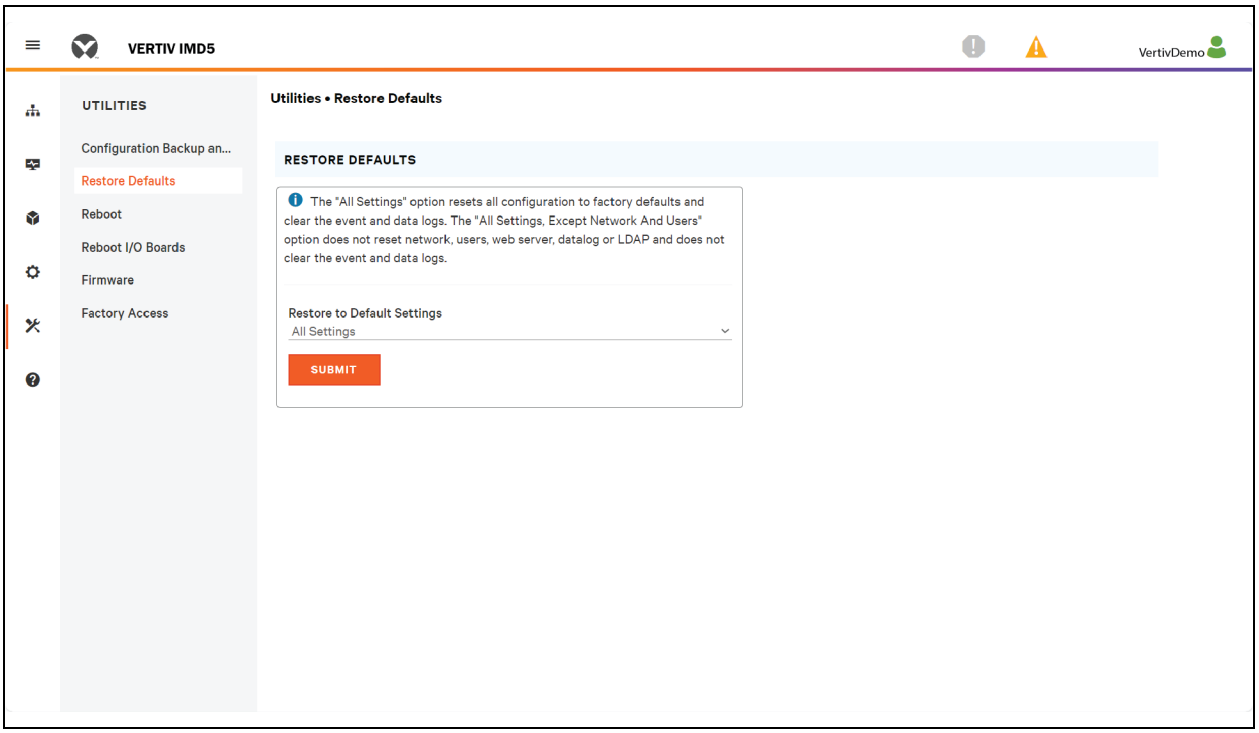
Tableau 5.14 Options de restauration des paramètres par défaut

Option	Description
All Settings	Rétablit les paramètres d'usine par défaut de toutes les configurations sur /conf, /alarm et /dev. Cette option efface aussi le journal des événements et le journal des données, et exécute la commande de suppression sur tous les dispositifs dont l'état est **unavailable**. Cela entraîne la réinitialisation de certaines parties du système. Un message vous informant de la réussite de l'opération s'affiche, suivi d'une courte période pendant laquelle l'accès au système n'est pas disponible.
All Settings, Except Networks And Users	Similaire à l'option **defaults** ci-dessus, mais ne réinitialise pas /conf/network, /conf/http, /conf/datalog, /auth ou /conf/ldap et n'efface pas le journal des événements ni le journal des données. Cela entraîne la réinitialisation de certaines parties du système. Un message vous informant de la réussite de l'opération s'affiche, suivi d'une courte période pendant laquelle l'accès au système n'est pas disponible.

Pour restaurer les paramètres par défaut :

1. Sélectionnez *All Settings* ou *All Settings, Except Networks And Users* dans le menu déroulant.
2. Cliquez sur *SUBMIT*.

Figure 5.62 Présentation de la restauration des paramètres par défaut



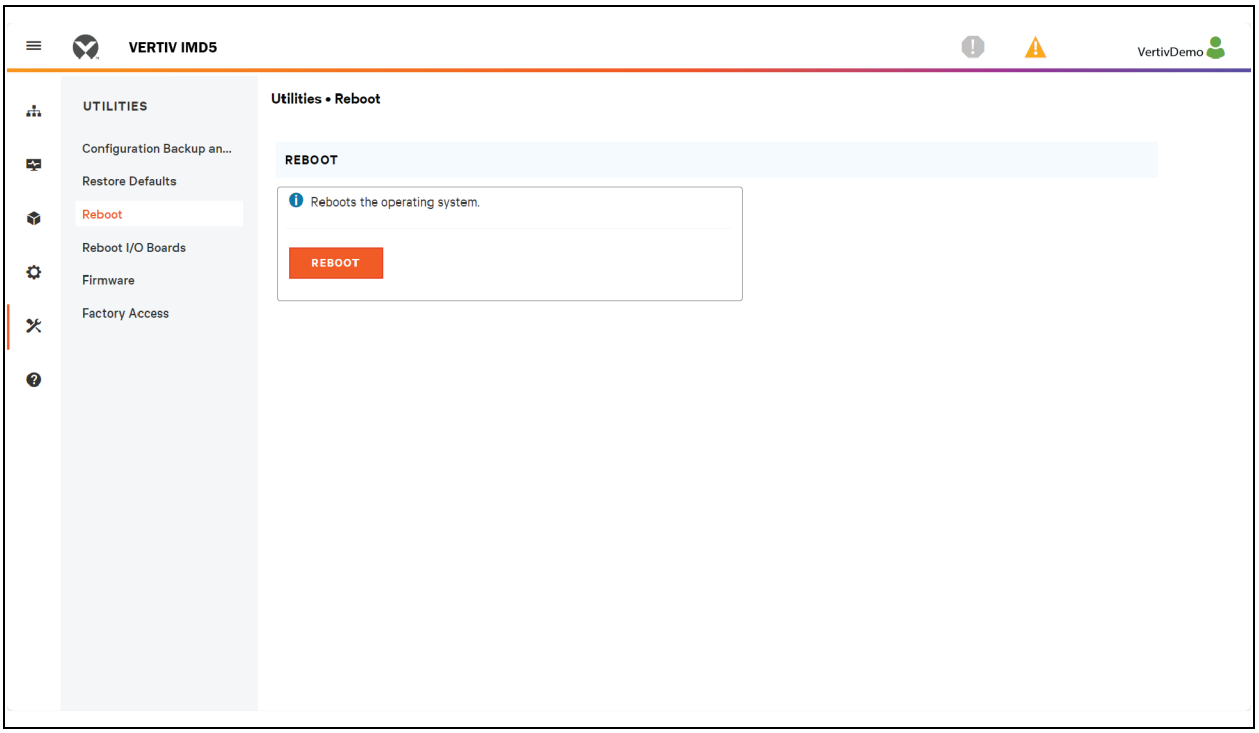
5.7.3 Redémarrage

Redémarre le système d'exploitation. Réinitialise le processeur IMD provoquant le redémarrage de l'IMD.

Cliquez sur *REBOOT* pour redémarrer le système d'exploitation.

REMARQUE : l'alimentation des dispositifs connectés n'est pas affectée.

Figure 5.63 Présentation de la fonction de redémarrage



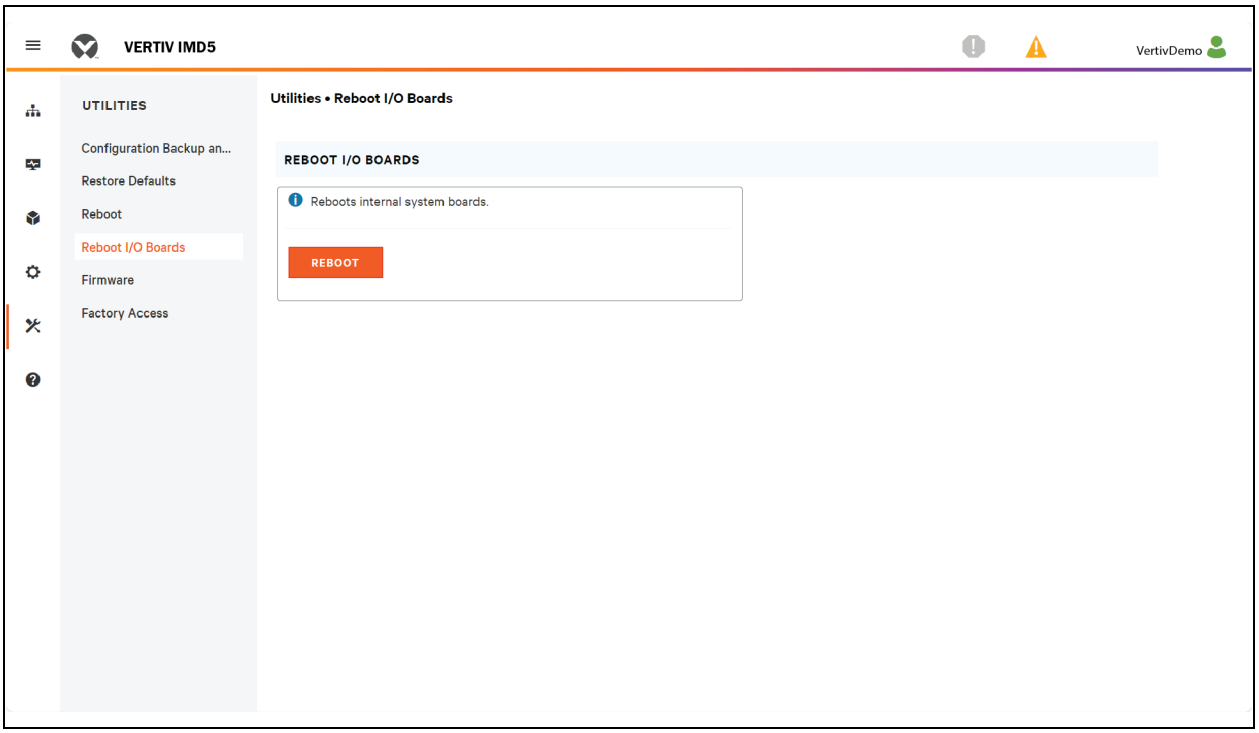
5.7.4 Redémarrage des cartes d'E/S

Si la rPDU Vertiv™ PowerIT ne répond pas ou n'affiche pas toutes les valeurs, le redémarrage des cartes internes entraînera la réinitialisation du système. Cela réinitialisera les processeurs sur la carte d'entrée interne et les cartes de sortie, entraînant leur redémarrage.

Cliquez sur *REBOOT* pour redémarrer les cartes système internes.

REMARQUE : l'alimentation des dispositifs connectés n'est pas affectée.

Figure 5.64 Présentation du redémarrage des cartes d'E/S



5.7.5 Mises à jour de firmware

Charge un fichier de firmware qui met à jour le système. Cette action nécessite une authentification de l'utilisateur et celui-ci doit disposer de droits d'administrateur. Les mises à jour du firmware sont généralement fournies dans un fichier d'archive **.zip** contenant plusieurs fichiers, notamment le package du firmware proprement dit, une copie de la MIB SNMP, un fichier texte Lisez-moi expliquant comment installer le firmware et divers autres fichiers de prise en charge, si nécessaire. Veillez à décompresser l'archive, puis suivez les instructions fournies.

Pour mettre à jour le firmware par le biais du fichier du package du firmware :

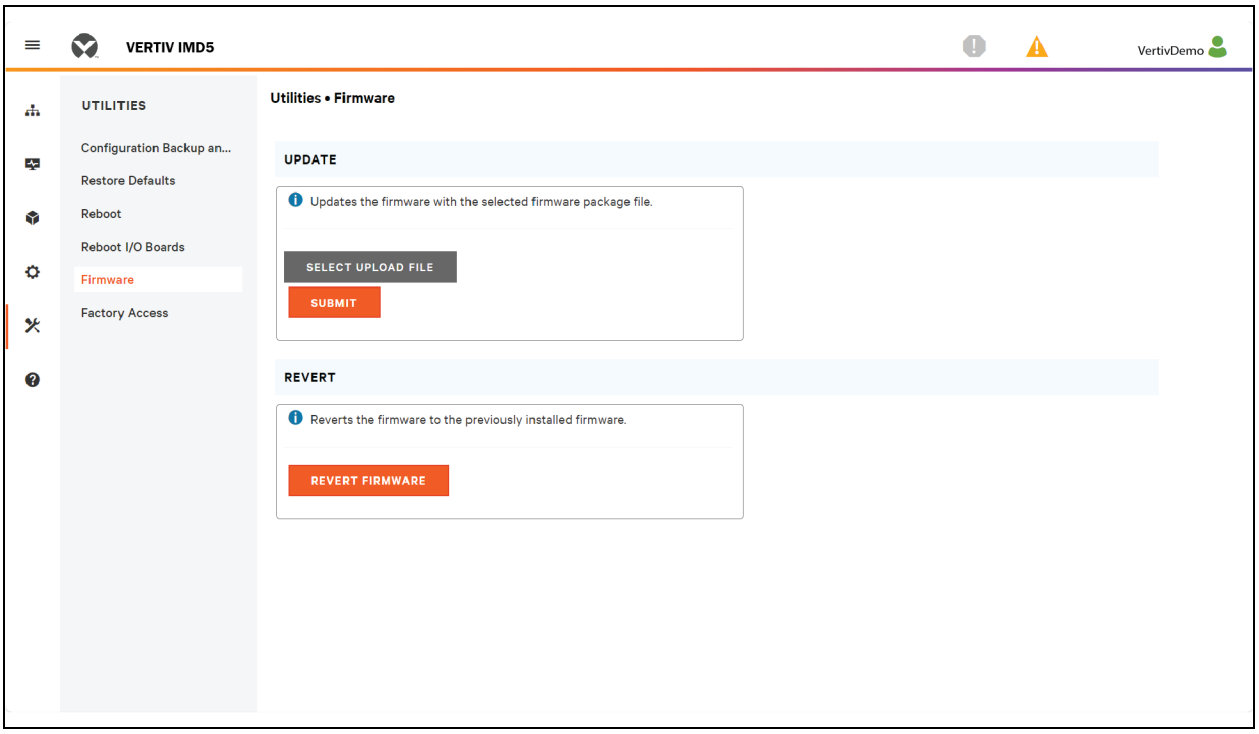
1. Cliquez sur *SELECT UPLOAD FILE* et sélectionnez le fichier ***.firmware*** dans la fenêtre *Open*.
2. Cliquez sur *SUBMIT*.
3. Si un problème est découvert (l'unité ne se comporte pas correctement) après l'installation réussie du firmware, cliquez sur *REVERT FIRMWARE*.

Pour mettre à jour le firmware via une clé USB :

1. Téléchargez le firmware le plus récent depuis *https://www.vertiv.com/en-us/support/software-download/power-distribution/geist-upgradeable-series-v5-firmware/* et décompressez le dossier.
2. Utilisez une clé USB et formatez-la en FAT32.
3. Créez un répertoire sur la clé USB appelé *FIRMWARE* (les majuscules ne sont pas obligatoires).
4. Ouvrez le dossier du firmware décompressé et copiez le fichier **.firmware**.
5. Collez ce fichier dans le dossier *FIRMWARE* sur la clé USB.
6. Insérez la clé USB dans la PDU.

Pendant la mise à jour, l'IMD cesse de faire défiler les données. Une fois la mise à jour terminée, un message de démarrage s'affiche à l'écran. Une fois le redémarrage terminé, l'IMD reprend le défilement des données à l'écran.

Figure 5.65 Présentation du firmware



5.7.6 Factory Access

Accès usine fournit des informations pour l'assistance technique.

Tableau 5.15 Options d'accès usine

Option	Description
Download Factory Support Package	Télécharge un package de diagnostic chiffré qui peut être envoyé au personnel d'assistance technique.
Factory Access	Permet l'accès d'usine à l'unité via SSH (à des fins de débogage).

Pour télécharger un package d'assistance d'usine :

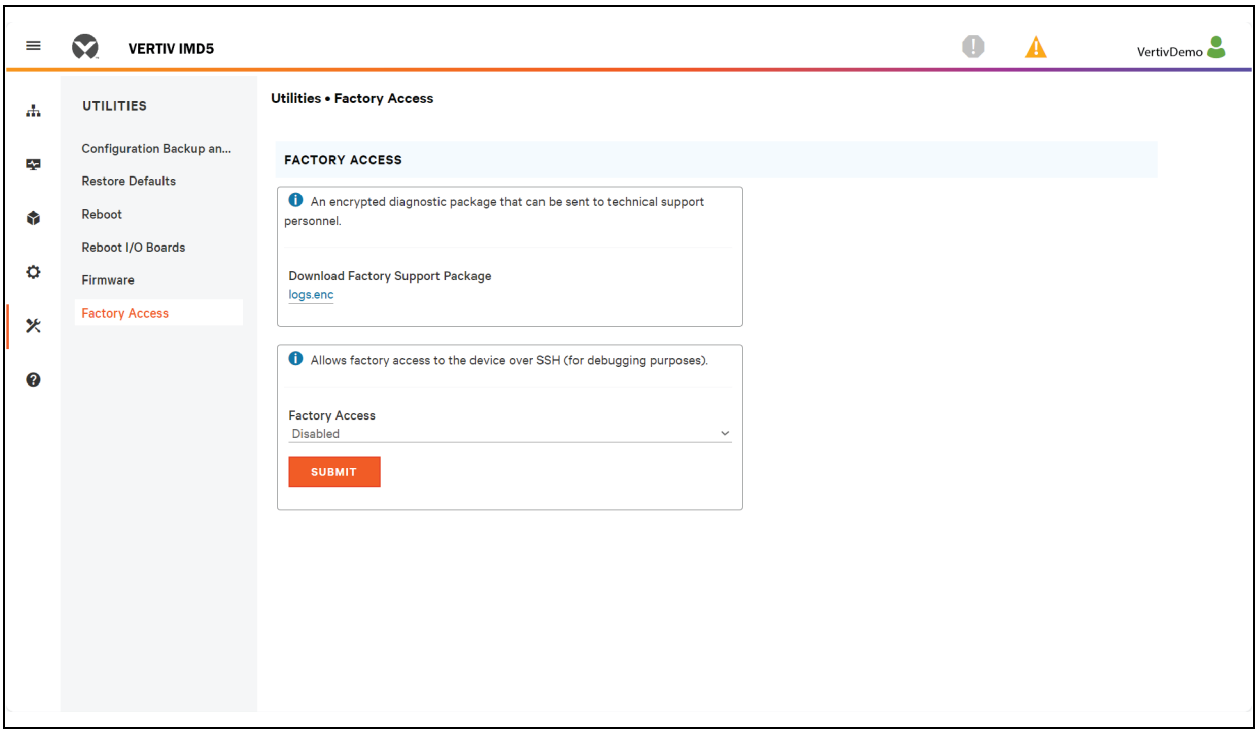
1. Cliquez sur *Download Factory Support Package*.
2. Cliquez sur *ENC*.

Pour activer/désactiver l'accès d'usine :

1. Sélectionnez *Enable* ou *Disable* dans le menu déroulant.
2. Cliquez sur *SUBMIT*.

REMARQUE : cela nécessite une authentification de l'utilisateur et l'utilisateur doit disposer de droits d'administrateur.

Figure 5.66 Présentation de l’accès d’usine

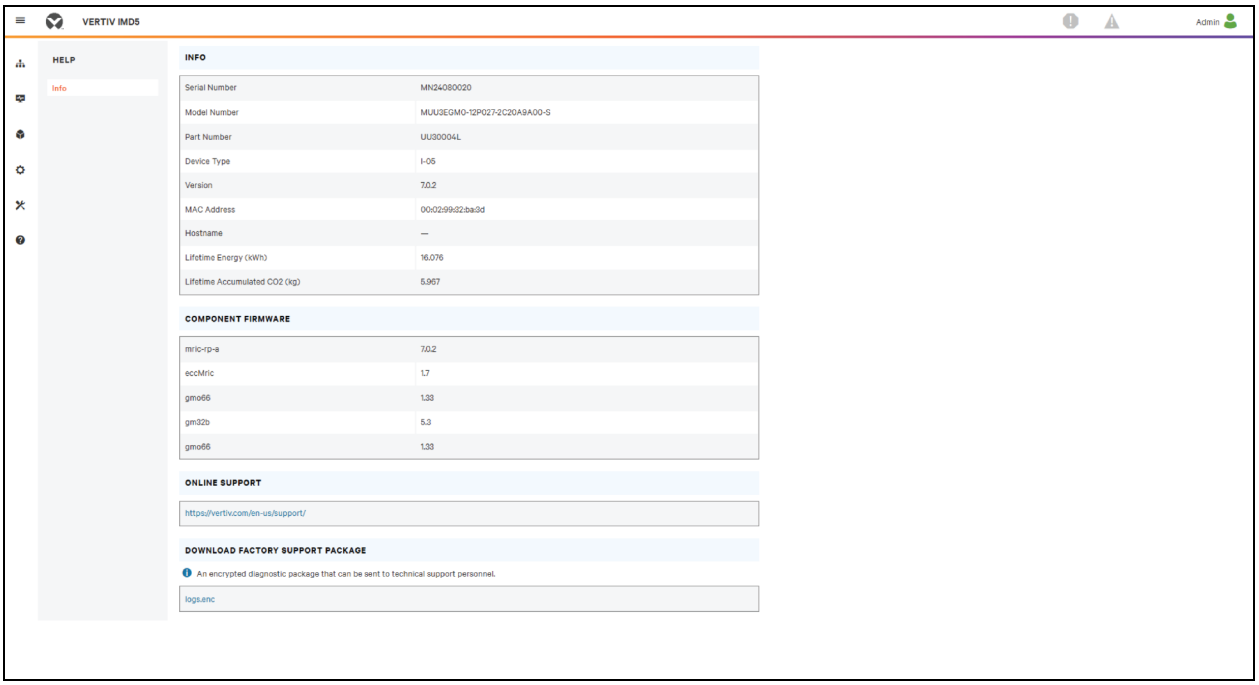


5.8 Sous-menu Help

Page Info

La page Info affiche les informations de configuration actuelles de l'unité, notamment le nom et l'ID du dispositif, le type d'IMD installé, les versions actuelles du firmware de l'unité et les informations réseau. Les informations sur l'assistance fournie par le fabricant sont également disponibles ici.

Figure 5.67 Page Info



6 Vertiv™ Intelligence Director

Vertiv Intelligence Director apporte une couche de visualisation unique et unifiée pour les déploiements de petite envergure de rPDU Vertiv™ PowerIT, d'ASI Vertiv™, de capteurs environnementaux et de prises de rPDU Vertiv™ PowerIT. Lorsqu'il est déployé, Vertiv Intelligence Director offre des fonctionnalités améliorées, en utilisant la rPDU Vertiv™ PowerIT non pas comme un dispositif autonome, mais comme une passerelle pour comprendre l'écosystème de dispositifs plus étendu dans lequel il est installé.

6.1 Consolidation

La consolidation est l'élément à la base de Vertiv Intelligence Director, disponible avec les rPDU Vertiv™ PowerIT exécutant le firmware 5.3.0 ou toute version ultérieure. Cet élément unique vous permet d'effectuer les opérations suivantes :

- Utilisez la consolidation pour réduire le nombre d'adresses IP, consolider les données de plusieurs PDU en rack et permettre la gestion des groupes de prises de PDU en rack.
- Les PDU en rack sont connectées à l'aide d'une connexion en cascade Ethernet, comme dans l'exemple de connexion en cascade ci-dessus.
- La tête de la PDU en rack de la chaîne est configurée en tant que gestionnaire de groupes.
- Le réseau des dispositifs de groupe peut inclure des commutateurs réseau.
- Une seule adresse IP attribuée au gestionnaire de groupes peut être utilisée pour accéder à un maximum de 50 dispositifs (le gestionnaire de groupes et 49 dispositifs de groupe).
- Les paramètres réseau du dispositif de groupe sont automatiquement configurés.
- Les dispositifs de groupe sont accessibles à l'aide de l'adresse IP du gestionnaire de groupes et d'un numéro de voie. Le numéro de voie peut être obtenu en accédant à la page *Device>List page* et en survolant le dispositif.
- Les utilisateurs peuvent définir des groupes de dispositifs. Par exemple, représentant des racks.
- Le gestionnaire de groupes génère des mesures consolidées telles que la puissance totale du groupe et la puissance totale, notamment les moyennes, les valeurs minimales et les valeurs maximales.
- La connexion en cascade tolérante aux pannes n'est pas autorisée lors de l'utilisation de Vertiv Intelligence Director.

Figure 6.1 Onglet Aggregation

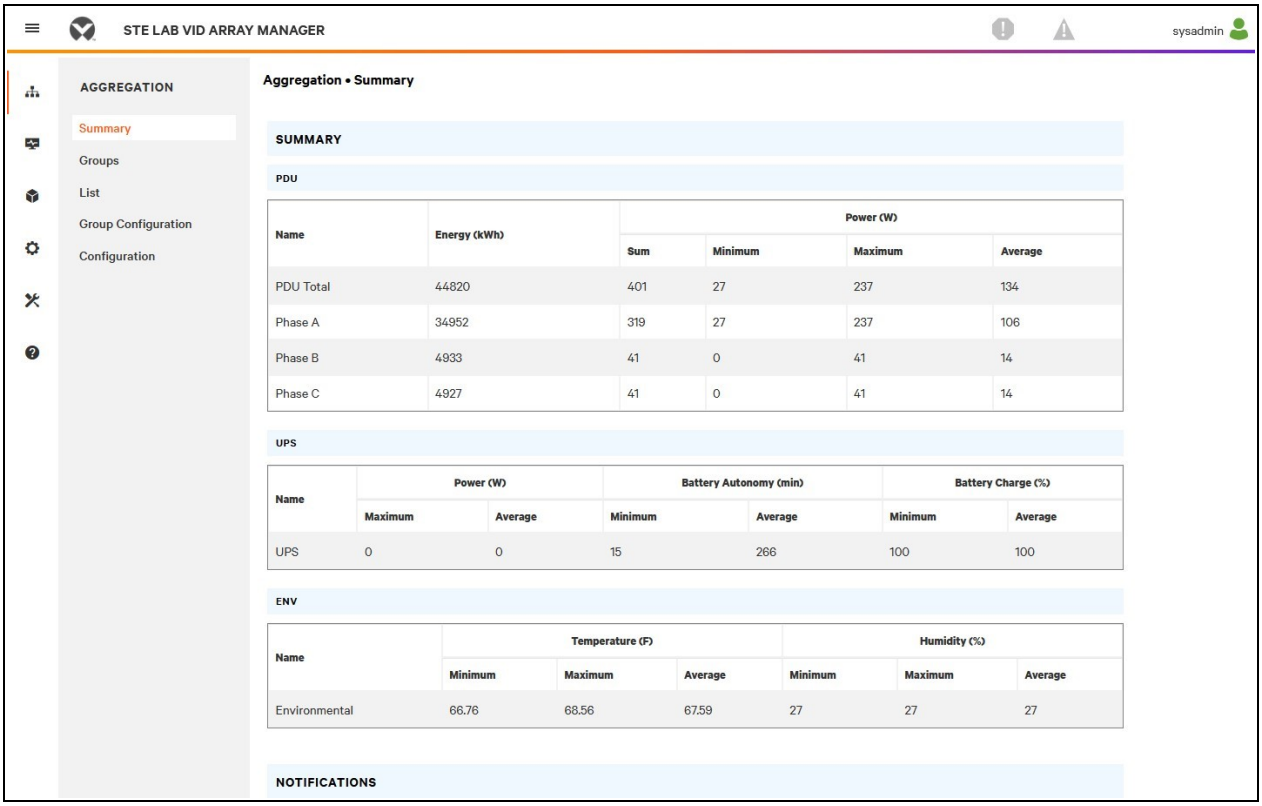
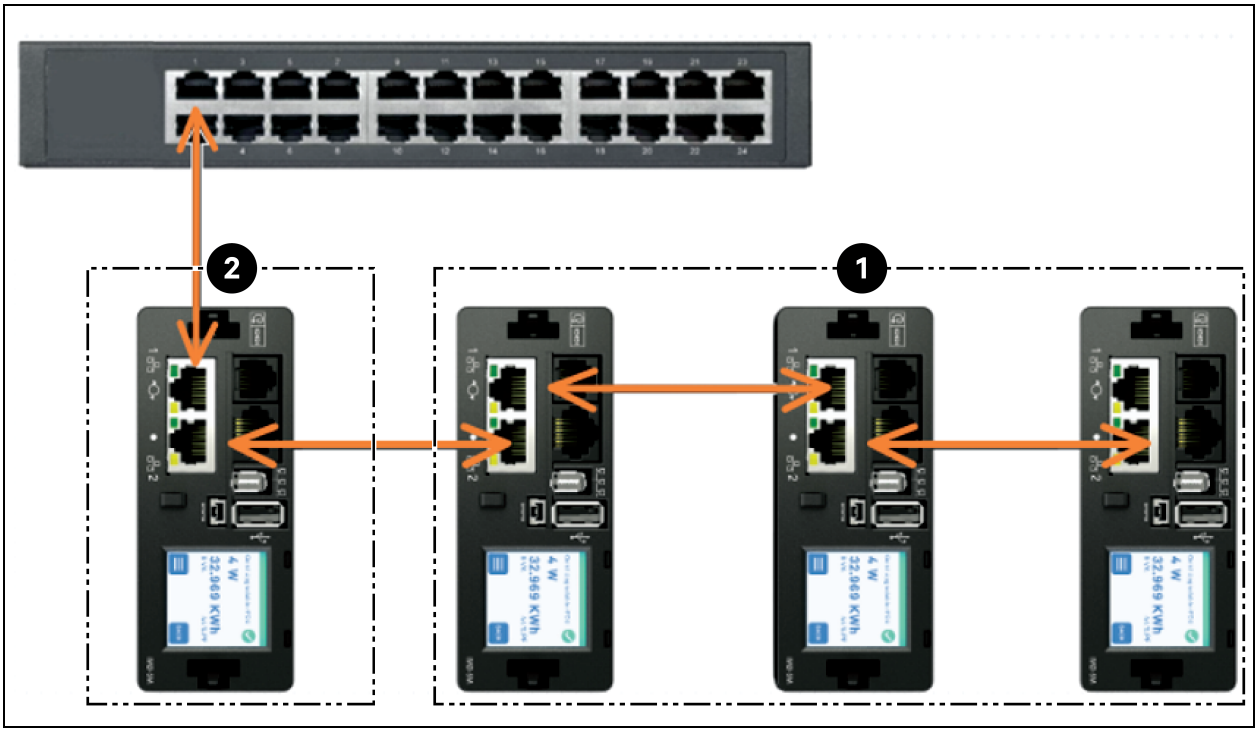


Figure 6.2 Consolidation



Élément	Description
1	Dispositif de groupe
2	Gestionnaire de groupes

Un autre élément de Vertiv Intelligence Director, disponible avec les rPDU Vertiv™ PowerIT exécutant le firmware 5.7.0 ou toute version ultérieure, est le Rack PDU Outlet Grouping. Cet élément vous permet d'effectuer les opérations suivantes :

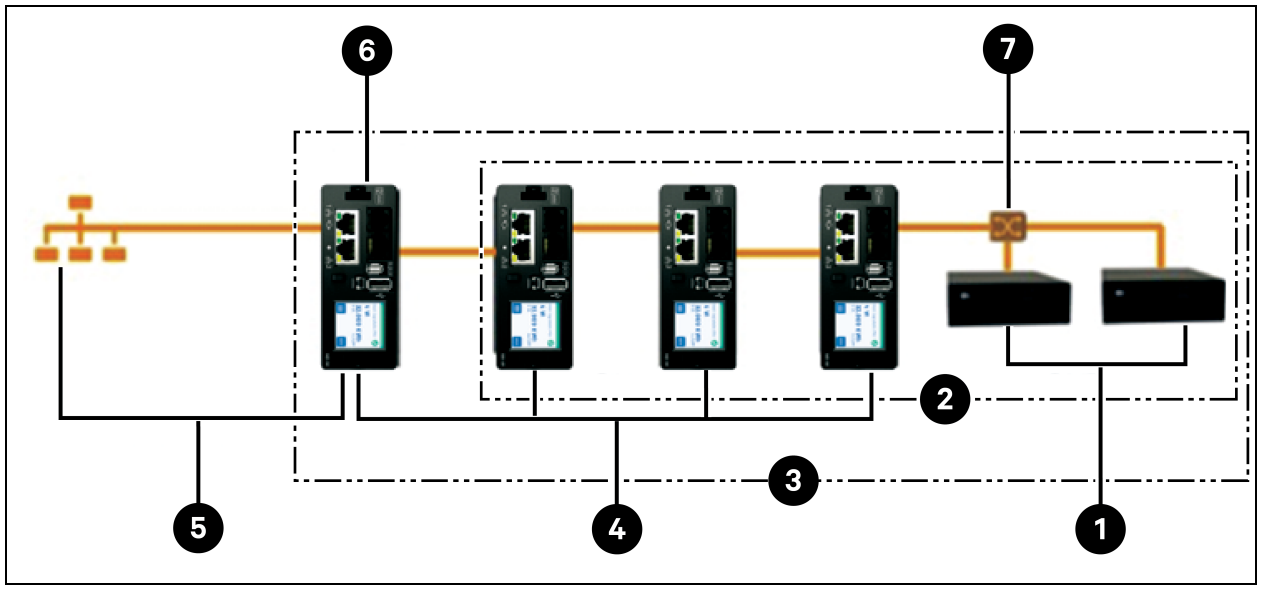
- Créer des groupes de prises de rPDU Vertiv™ PowerIT d'une ou plusieurs rPDU Vertiv™ PowerIT.
- Créer des rapports sur la puissance et l'énergie totales pour le groupe de prises (avec les rPDU Vertiv™ PowerIT qui créent des rapports selon les mesures des prises).
- Mettre hors tension/sous tension ou redémarrer le groupe de prises à partir d'une seule commande (sur les rPDU Vertiv™ PowerIT qui prennent en charge la commutation des prises).

Avec le firmware 5.10.1 ou version ultérieure, une visibilité complète des dispositifs Vertiv Intelligence Director (consolidés) est disponible via les interfaces de ligne de commande de voie série et SSH.

6.2 Gestionnaire de groupes

La consolidation nécessite la désignation d'un gestionnaire de groupes, déployé avec des PDU en rack équipées du modèle IMD 5M exécutant la version 6.3.0 ou ultérieure du firmware ou de modèles IMD 3E, 03E, 3E-S, 03E-S, 3E-G ou 03E-G qui exécutent actuellement les versions 5.3.0 et ultérieures du firmware (bien que la dernière version du firmware soit vivement recommandée). L'IMD du gestionnaire de groupes facilite et configure le réseau de dispositifs, l'ensemble interconnecté de rPDU Vertiv™ PowerIT, d'ASI Vertiv™, de dispositifs de refroidissement Vertiv™, de capteurs environnementaux et de prises rPDU Vertiv™ PowerIT, tout en regroupant certains points de données à partir de ces dispositifs. Il interagit également avec le réseau de gestion pour sa propre surveillance et gestion, ainsi que celles des dispositifs de groupe.

Figure 6.3 Exemple de configuration



Élément	Description
1	Vertiv™ Liebert® GXT4
2	Dispositifs en aval
3	Réseau de dispositifs
4	Dispositifs de groupe (rPDU PowerIT)
5	Réseau de gestion
6	Gestionnaire de groupes (rPDU PowerIT)
7	Commutateur Ethernet

Il n'est plus possible d'embarquer de nouvelles PDU en rack IMD-02x lors de l'utilisation d'un gestionnaire de groupes exécutant le firmware 6.1.0 ou toute version ultérieure.

6.3 Configuration réseau

Dans la version initiale de la consolidation, les dispositifs de groupe sont définis comme des rPDU Vertiv™ PowerIT au sein des plateformes de produits Vertiv™ PowerIT surveillées et commutées (3E, 03E, 3E-S, 03E-S, 3E-G, 03E-G et 5M), ainsi que des PDU en rack Vertiv™ MPH2™ et Vertiv™ MPX™, des ASI Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, Vertiv™ Liebert® APM et Vertiv™ Liebert® ITA2, du système de refroidissement en rangée Vertiv™ Liebert® CRV et du système de refroidissement Vertiv™ Liebert® VRC connecté par USB. Chaque gestionnaire de groupes peut prendre en charge jusqu'à 49 dispositifs de groupe, de sorte que le nombre de gestionnaires dépend de la taille globale de l'installation et de l'architecture réseau préférée.

Le gestionnaire de groupes doit être mis en service avant d'être connecté au réseau de gestion principal ou au réseau des dispositifs de groupe. Cette mise en service est généralement effectuée à l'aide d'un ordinateur portable ou d'une machine locale connecté directement à la voie 1 de l'IMD.

Une fois la connectivité locale établie, vous pouvez mettre en service le gestionnaire de groupes.

Pour mettre en service le gestionnaire de groupes :

1. Accédez à *System>Locale*. Sélectionnez la langue par défaut et les unités de température appropriées dans les menus déroulants. Ces paramètres sont transmis aux dispositifs connectés à son réseau.
2. Accédez à *System>Network*. Dans Protocol IPv6, choisissez *Enabled* dans le menu déroulant.
3. Accédez à *Aggregation>Configuration*. Modifiez les paramètres comme vous le souhaitez.
    a. Aggregation : choisissez *Enabled* dans le menu déroulant.
    b. Array device Username : définit le nom d'utilisateur à configurer sur tous les dispositifs de groupe.
    c. Array device Password : définit le mot de passe à configurer sur tous les dispositifs de groupe.
    - Saisissez le nouveau mot de passe, vérifiez-le, puis cliquez sur *Submit*. Lors de la configuration de la consolidation, assurez-vous que le mot de passe du dispositif géré respecte toutes les règles de complexité des mots de passe du dispositif de groupe. Sauf modification par l'utilisateur, ceux-ci nécessitent un mot de passe d'une longueur minimale de 8 caractères avec les rPDU exécutant le firmware 5.9.0 ou ultérieur.
4. Cliquez sur *Submit*.

Une fois la consolidation activée dans le gestionnaire de groupes, configurez les paramètres restants de ce dernier. Connectez le gestionnaire de groupes au réseau de gestion (voie 1) sur l'IMD et le réseau des dispositifs (voie 2).

REMARQUE : le gestionnaire de groupes intègre un réseau DHCP pour attribuer des adresses aux dispositifs de groupe. Ce réseau DHCP utilise les adresses *192.168.123 / 192.168.124*, qui ne peuvent pas être utilisées pour le réseau de gestion.

Dispositifs de groupe

Dans la version initiale de la consolidation, les dispositifs de groupe sont définis comme des rPDU Vertiv™ PowerIT au sein des plateformes de produits Vertiv™ PowerIT commutées et surveillées, ainsi que des PDU en rack Vertiv™ MPH2™ et Vertiv™ MPX™, des ASI Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, Vertiv™ Liebert® APM et Vertiv™ Liebert® ITA2, du système de refroidissement en rangée Vertiv™ Liebert® CRV et du système de refroidissement Vertiv™ Liebert® VRC connecté par USB. Toutes les rPDU Vertiv™ PowerIT (modèles IMD 02, 02E) doivent exécuter la version de firmware 3.4 ou ultérieure ; les rPDU Vertiv™ PowerIT (3E, 03E, 3E-S, 03E-S, 3E-G, 03E-G) et les PDU en rack de la série R doivent exécuter la version de firmware 5.3.0 ou ultérieure. Ces dispositifs de groupe énumérés dans la phrase précédente ne peuvent pas être intégrés avec des contrôleurs de groupes dotés du firmware version 6.1.0 ou ultérieure. Dans tous les cas, il est vivement recommandé de mettre à jour toutes les rPDU avec la dernière version du firmware disponible. Si de nouvelles rPDU Vertiv™ PowerIT sont commandées et n'ont jamais été configurées, elles sont prêtes pour la consolidation immédiate. Si les rPDU Vertiv™ PowerIT ont été déployées dans un environnement informatique et mises en service avec des comptes utilisateur et des paramètres LAN locaux, les paramètres d'usine par défaut de chaque rPDU Vertiv™ PowerIT doivent être rétablis à l'aide des options *Utilities>Restore Defaults*. Sélectionnez *All Settings*, puis cliquez sur *Submit*. Le gestionnaire de groupes transmettra ensuite les données de configuration aux dispositifs de groupe.

Pour configurer une nouvelle installation avec un seul gestionnaire de groupe :

1. Installez les dispositifs de groupe dans les racks et mettez les racks sous tension.
2. Connectez les dispositifs de groupe en cascade les uns aux autres, le cas échéant, à l'aide des voies libellées 1 et 2 sur l'IMD.
    - Si vous utilisez des connexions de rPDU en cascade, assurez-vous qu'aucune connexion en cascade ne comprend plus de 20 rPDU.
    - Les dispositifs de groupe peuvent être mis en réseau à l'aide de connexions en cascade, de connexions en étoile ou d'une combinaison des deux.
3. Installez le gestionnaire de groupes dans un rack. À l'aide d'un ordinateur portable ou d'une machine locale, connectez-vous à la voie 1 pour configurer la consolidation.
4. Connectez le gestionnaire de groupes au réseau de gestion à l'aide de la voie 1.
5. Connectez le gestionnaire de groupes au réseau des dispositifs de groupe à l'aide de la voie 2.

Pour configurer une installation existante avec un seul gestionnaire de groupes :

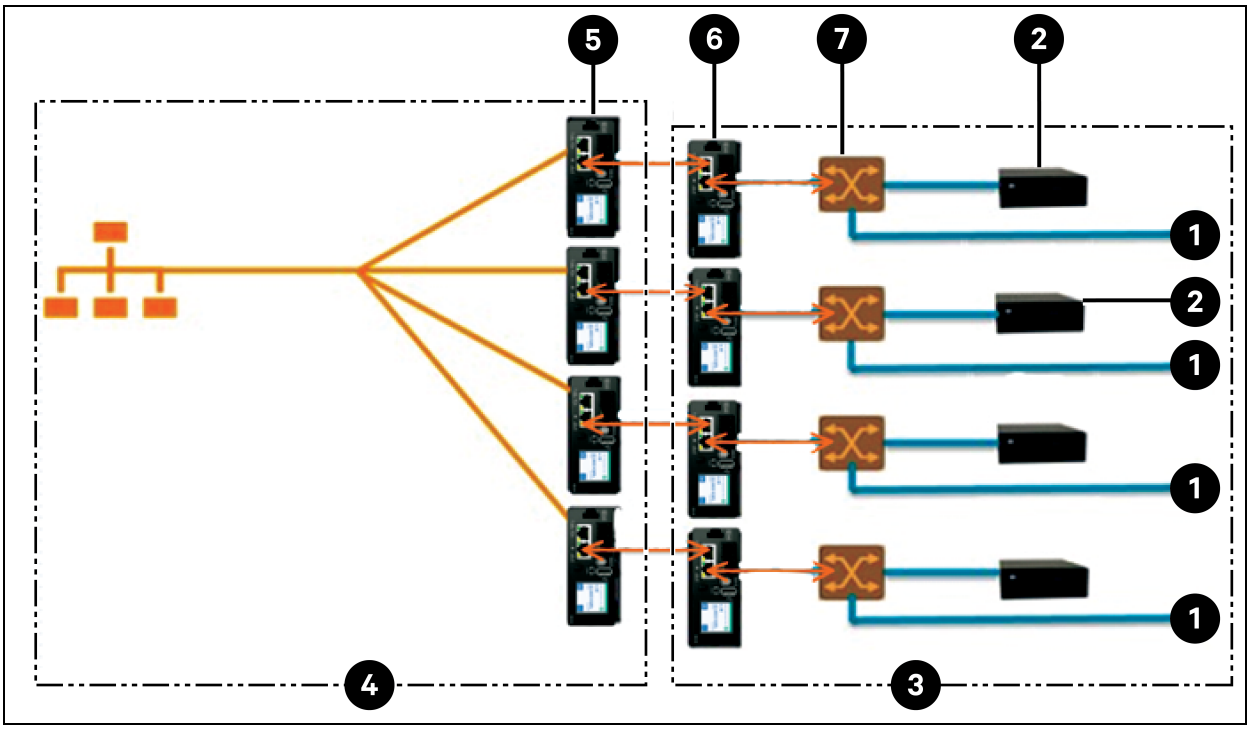
REMARQUE : suivez les instructions suivantes si des rPDU Vertiv™ PowerIT existantes sont connectées en cascade.

1. Désignez un gestionnaire de groupes et déconnectez-le du réseau de gestion.
2. Rétablissez les paramètres d'usine par défaut de tous les dispositifs de groupe. Les connexions Ethernet physiques dans la structure en cascade peuvent rester les mêmes ; cependant, si les dispositifs étaient précédemment connectés dans une configuration en boucle, la dernière rPDU Vertiv™ PowerIT de la chaîne doit être déconnectée du commutateur réseau.
3. Activez la fonction consolidation sur le gestionnaire de groupes.
4. Connectez le gestionnaire de groupes au réseau de gestion à l'aide de la voie 1.
5. Connectez le gestionnaire de groupes au réseau de groupes à l'aide de la voie 2.

Plusieurs gestionnaires de groupes

Pour les installations incluant plusieurs gestionnaires de groupes, gardez à l'esprit que chaque réseau de dispositifs doit fonctionner comme un réseau autonome et isolé. Prenons un exemple de 200 rPDU, représenté dans la Figure 6.4 ci-dessous. Cette installation nécessite au moins quatre gestionnaires de groupes, chacun exploitant son propre réseau de dispositifs autonome. Chaque gestionnaire de groupes est visible sur le réseau de gestion et agit comme un serveur DHCP pour ses dispositifs de groupe. Un utilisateur du réseau de gestion peut parcourir chaque gestionnaire de groupes pour atteindre l'interface d'un dispositif de groupe. D'autres considérations peuvent affecter le nombre de gestionnaires de groupes. Si vous avez une architecture réseau par rangée, vous pouvez préférer avoir un gestionnaire de groupes au début de chaque rangée, au lieu d'un gestionnaire de groupes traversant plusieurs rangées. Selon la façon dont ces 200 armoires sont divisées en rangées, vous pouvez avoir plus de quatre gestionnaires de groupes. Lorsque vous avez choisi la configuration, suivez le processus approprié pour la consolidation.

Figure 6.4 Exemple de configuration réseau



Élément	Description
1	Autres dispositifs
2	ASI
3	Réseau de dispositifs
4	Réseau de gestion
5	Gestionnaire de groupes (rPDU PowerIT)
6	Dispositifs de groupe (rPDU PowerIT)
7	Commutateur Ethernet

REMARQUE : un commutateur Ethernet de réseau de dispositifs ne sera requis qu'en cas de connexion de plusieurs dispositifs à voie réseau unique à l'extrémité d'une connexion en cascade de rPDU ou si vous n'utilisez pas de connexions en cascade.

6.4 Vues

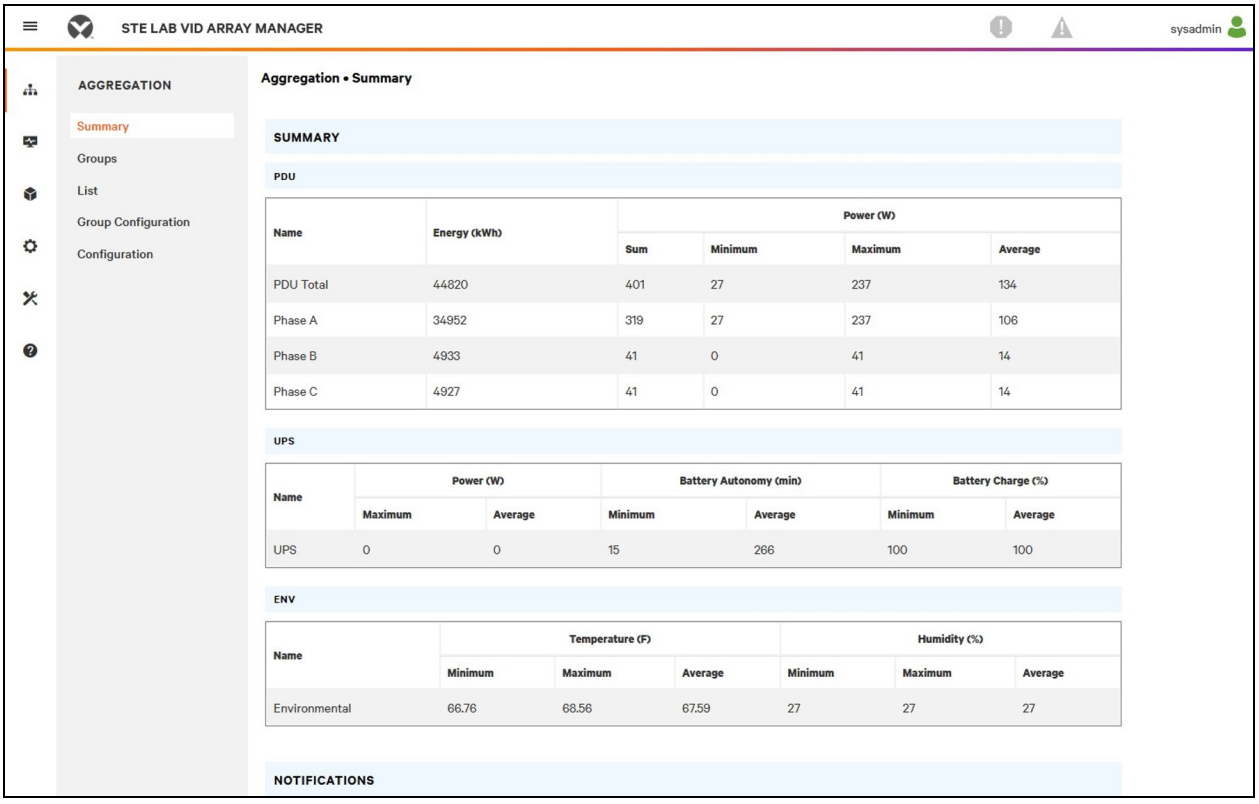
Lorsque la communication est établie entre le gestionnaire de groupes et les dispositifs de groupe, plusieurs vues sont automatiquement renseignées dans l'interface utilisateur. Les nouvelles vues sous l'onglet Device dans la barre de navigation supérieure sont les suivantes :

- Summary
- Groups
- List
- Group Configuration
- Configuration

6.4.1 Summary

La vue Summary regroupe les données de tous les dispositifs de groupe, présentant un aperçu concis des détails pertinents concernant l'alimentation, l'environnement et les alarmes.

Figure 6.5 Onglet Summary



PDU en rack

Le réseau des rPDU Vertiv™ PowerIT est résumé par les points de données suivants :

- **Energy (kWh) :** énergie totale des rPDU Vertiv™ PowerIT au sein du réseau de dispositifs.
- **Power (W) Sum :** charge de puissance totale des rPDU Vertiv™ PowerIT au sein du réseau de dispositifs.
- **Power (W) Minimum :** charge de puissance de groupe la plus basse des rPDU Vertiv™ PowerIT au sein du réseau de dispositifs.
- **Power (W) Maximum :** charge de puissance de groupe la plus élevée des rPDU Vertiv™ PowerIT au sein du réseau de dispositifs.
- **Power (W) Average :** charge de puissance de groupe moyenne des rPDU Vertiv™ PowerIT au sein du réseau de dispositifs.

REMARQUE : Ces mesures sont répétées par phase (affichées uniquement lorsque des rPDU Vertiv™ PowerIT triphasées sont présentes).

ASI

Le réseau des ASI est résumé par les points de données suivants :

- **Power (W) Maximum :** charge de puissance de groupe des ASI la plus élevée au sein du réseau de dispositifs.
- **Power (W) Average :** charge de puissance de groupe moyenne des ASI au sein du réseau de dispositifs.
- **Battery Autonomy (min) Minimum :** durée de fonctionnement de la batterie de l'ASI la plus faible au sein du réseau de dispositifs.
- **Battery Autonomy (min) Average :** durée de fonctionnement moyenne de la batterie de l'ASI au sein du réseau de dispositifs.
- **Battery Charge (%) Minimum :** charge de la batterie de l'ASI la plus faible au sein du réseau de dispositifs.
- **Battery Charge (%) Average :** charge moyenne de la batterie de l'ASI au sein du réseau de dispositifs.

Capteurs environnementaux (ENV)

La catégorie Environmental est résumée par les points de données suivants :

REMARQUE : les valeurs d'humidité seront vides lors de l'utilisation de capteurs de température seulement.

- **Temperature (F) Minimum :** température la plus faible au sein du réseau de dispositifs.
- **Temperature (F) Maximum :** température la plus élevée au sein du réseau de dispositifs.
- **Temperature (F) Average :** température moyenne au sein du réseau de dispositifs.
- **Humidity (%) Minimum :** humidité la plus faible au sein du réseau de dispositifs.
- **Humidity (%) Maximum :** humidité la plus élevée au sein du réseau de dispositifs.
- **Humidity (%) Average :** humidité moyenne au sein du réseau de dispositifs.

Refroidissement thermique

- **Fan Speed (%) Minimum :** vitesse de ventilateur des dispositifs thermiques la plus faible au sein du réseau de dispositifs.
- **Fan Speed (%) Maximum :** vitesse de ventilateur des dispositifs thermiques la plus élevée au sein du réseau de dispositifs.
- **Fan Speed (%) Average :** vitesse moyenne de ventilateur des dispositifs thermiques au sein du réseau de dispositifs.
- **Temperature (F) Minimum :** température des dispositifs thermiques la plus faible au sein du réseau de dispositifs.

- **Temperature (F) Maximum :** température des dispositifs thermiques la plus élevée au sein du réseau de dispositifs.
- **Temperature (F) Average :** température moyenne des dispositifs thermiques au sein du réseau de dispositifs.
- **Capacity (%) Minimum :** capacité des dispositifs thermiques la plus faible au sein du réseau de dispositifs.
- **Capacity (%) Maximum :** capacité des dispositifs thermiques la plus élevée au sein du réseau de dispositifs.
- **Capacity (%) Average :** capacité moyenne des dispositifs thermiques au sein du réseau de dispositifs.

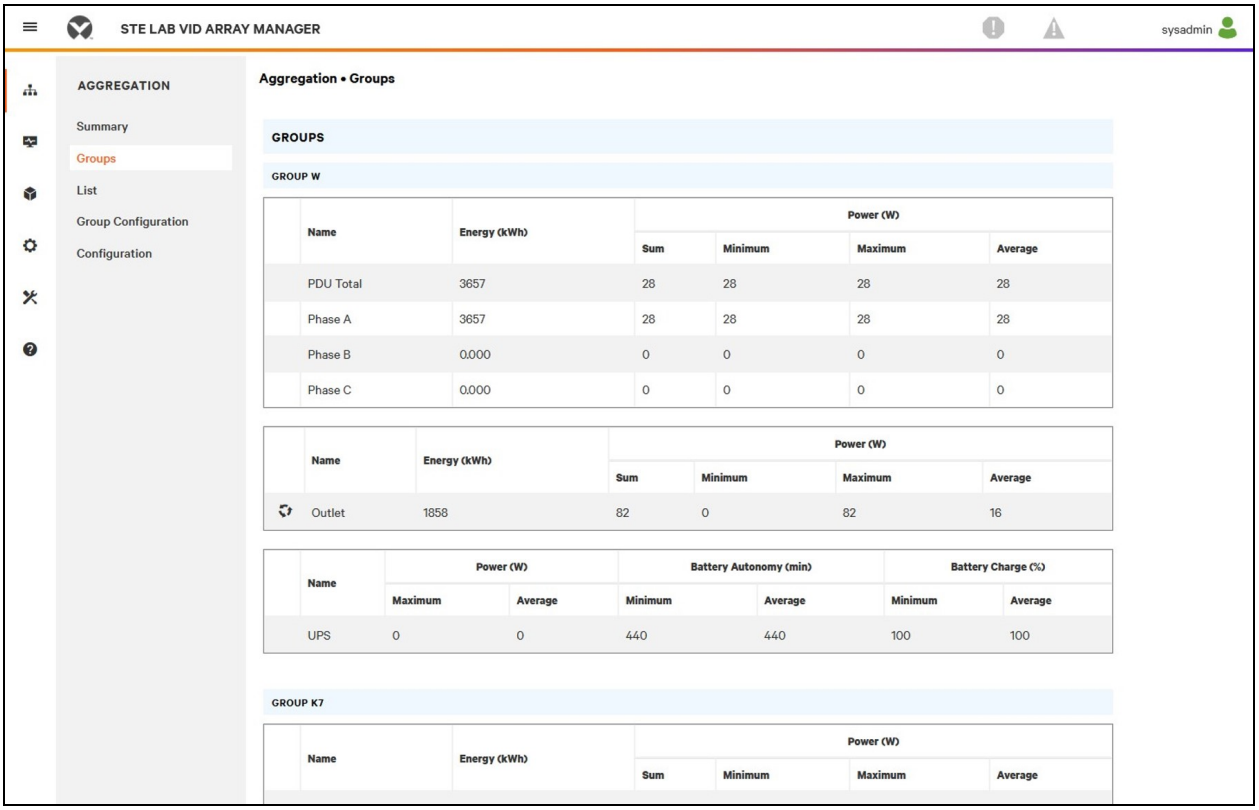
Notifications

Les notifications affichent les alarmes en suspens des dispositifs connectés au réseau de dispositifs.

6.4.2 Groups

Une fois les groupes établis sur la page Group Configuration, la vue Groups résume les données concernant l'alimentation et l'environnement.

Figure 6.6 Onglet Groups



Les points de données disponibles sont les suivants :

rPDU du groupe

- **Energy (kWh) :** énergie totale des rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Sum :** charge de puissance totale des rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Minimum :** charge de puissance la plus basse des rPDU Vertiv™ PowerIT au sein du groupe.

- **Power (W) Maximum :** charge de puissance la plus élevée des rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Average :** charge de puissance moyenne des rPDU Vertiv™ PowerIT au sein du groupe.

REMARQUE : ces mesures sont répétées par phase (affichées uniquement lorsque des rPDU triphasées sont présentes).

Prise rPDU du groupe

- **Energy (kWh) :** énergie totale des prises rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Sum :** charge de puissance totale des prises rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Minimum :** charge de puissance la plus basse des prises rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Maximum :** charge de puissance la plus élevée des prises rPDU Vertiv™ PowerIT au sein du groupe.
- **Power (W) Average :** charge de puissance moyenne des prises rPDU Vertiv™ PowerIT au sein du groupe.

Ces mesures sont répétées pour chaque groupe de prises de rPDU Vertiv™ PowerIT si au moins une prise y est surveillée. Si le groupe comporte aussi bien des PDU en rack à prises surveillées qu'à prises non surveillées, les mesures affichent le total pour les PDU en rack à prises surveillées uniquement.

Ces mesures sont répétées pour chaque phase (affichées uniquement en présence de PDU triphasées).

REMARQUE : les mesures d'énergie reflètent la somme des mesures d'énergie des prises. La réinitialisation des mesures d'énergie de chaque prise réinitialise également l'énergie totale mesurée pour ce groupe de prises.

L'icône des opérations est disponible pour chaque groupe comportant au moins une prise de PDU en rack avec possibilité de commutation.

Pour modifier l'opération du groupe de prises :

1. Cliquez sur l'icône d'opération.
2. Sélectionnez l'opération à effectuer (s'applique uniquement aux prises de PDU en rack du groupe qui peuvent être commutées) :
   - **On/Off :** active ou désactive toutes les prises.
   - **Reboot :** si des prises sont actuellement activées, le redémarrage désactive les prises, puis les réactive après un délai d'attente.

     Si les prises sont actuellement désactivées, le redémarrage active les prises.
   - **Cancel :** annule l'opération en cours si elle n'est pas terminée.
3. Pour les opérations impliquant l'état des prises, le réglage du paramètre Delay sur True applique la configuration de délai actuelle à chaque prise.
4. Sélectionnez *Submit* pour lancer l'action.

ASI du groupe

- **Power (W) Maximum :** charge de puissance la plus élevée des ASI au sein du groupe.
- **Power (W) Average :** charge de puissance moyenne des ASI au sein du groupe.
- **Battery Autonomy (min) Minimum :** durée de fonctionnement de la batterie de l'ASI la plus faible au sein du groupe.
- **Battery Autonomy (min) Average :** durée de fonctionnement moyenne de la batterie de l'ASI au sein du groupe.
- **Battery Charge (%) Minimum :** charge de la batterie de l'ASI la plus faible au sein du groupe.

- **Battery Charge (%) Average :** charge moyenne de la batterie de l'ASI au sein du groupe.

Caractéristiques environnementales du groupe

- **Temperature (F) Minimum :** température la plus basse au sein du groupe.
- **Temperature (F) Maximum :** température la plus élevée au sein du groupe.
- **Temperature (F) Average :** température moyenne au sein du groupe.
- **Humidity (%) Minimum :** humidité la plus basse au sein du groupe.
- **Humidity (%) Maximum :** humidité la plus élevée au sein du groupe.
- **Humidity (%) Average :** humidité moyenne au sein du groupe.

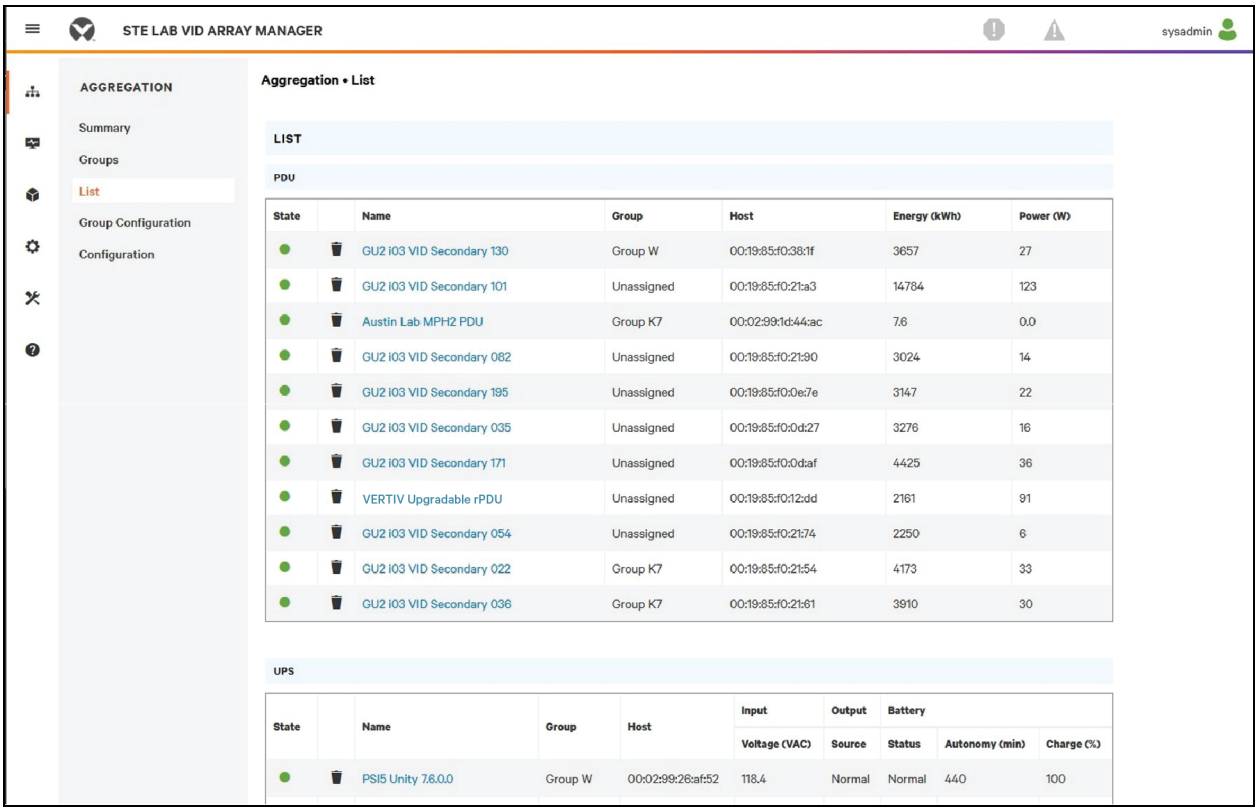
Refroidissement thermique du groupe

- **Fan Speed (%) Minimum :** vitesse de ventilateur des dispositifs thermiques la plus faible au sein du groupe.
- **Fan Speed (%) Maximum :** vitesse de ventilateur des dispositifs thermiques la plus élevée au sein du groupe.
- **Fan Speed (%) Average :** vitesse moyenne de ventilateur des dispositifs thermiques au sein du groupe.
- **Temperature (F) Minimum :** température des dispositifs thermiques la plus faible au sein du groupe.
- **Temperature (F) Maximum :** température des dispositifs thermiques la plus élevée au sein du groupe.
- **Temperature (F) Average :** température moyenne des dispositifs thermiques au sein du groupe.
- **Capacity (%) Minimum :** capacité des dispositifs thermiques la plus faible au sein du groupe.
- **Capacity (%) Maximum :** capacité des dispositifs thermiques la plus élevée au sein du groupe.
- **Capacity (%) Average :** capacité moyenne des dispositifs thermiques au sein du groupe.

6.4.3 List

La vue List présente un inventaire de tous les dispositifs connectés au réseau des dispositifs dans le gestionnaire de groupes.

Figure 6.7 Onglet List



L'inventaire est subdivisé dans les catégories suivantes :

PDU en rack

Toutes les rPDU Vertiv™ PowerIT du réseau de dispositifs entrent dans cette catégorie et présentent les points de données suivants :

- **State :** état de la rPDU Vertiv™ PowerIT. L'état est Normal ou Unavailable (perte de connectivité).
- **Name :** Vertiv™ PowerIT libellé de la rPDU. En cliquant sur le nom, vous ouvrez un onglet de navigateur pour accéder aux dispositifs.
- **Group :** nom du groupe. S'il n'y a pas de groupe créé par l'utilisateur, le nom du groupe est Unassigned.
- **Energy :** Vertiv™ PowerIT énergie de la rPDU.
- **Power :** charge électrique totale de la rPDU Vertiv™ PowerIT.

ASI

Toutes les ASI du réseau de dispositifs entrent dans cette catégorie et présentent les points de données suivants :

- **State :** état de l'ASI. L'état est Normal ou Unavailable (perte de connectivité).
- **Name :** libellé de l'ASI. En cliquant sur le nom, vous ouvrez un onglet de navigateur pour accéder aux dispositifs.
- **Group :** nom du groupe. S'il n'y a pas de groupe créé par l'utilisateur, le nom du groupe est Unassigned.
- **Input Voltage :** tension d'entrée de l'ASI.

- **Output Source :** mode de fonctionnement de l'ASI, qui peut être : Normal, Bypass, Battery, Booster, Reducer, Off ou Other.
- **Status :** état de la batterie, qui peut être : Normal, Low, Depleted ou Unknown.
- **Battery Autonomy :** durée de fonctionnement de la batterie de l'ASI.
- **Charge :** charge de batterie de l'ASI.

Capteurs environnementaux (ENV)

Tous les capteurs environnementaux du réseau de dispositifs entrent dans cette catégorie et présentent les points de données suivants :

- **State :** état du capteur. L'état est Normal ou Unavailable (perte de connectivité).
- **Name :** libellé du capteur. En cliquant sur le nom, vous ouvrez un onglet de navigateur pour accéder aux dispositifs.
- **Group :** nom du groupe. S'il n'y a pas de groupe créé par l'utilisateur, le nom du groupe est Unassigned.
- **Device :** affiche le libellé et l'adresse MAC de la rPDU Vertiv™ PowerIT parente du capteur.
- **Temperature (F) :** mesure de la température (température principale uniquement avec les capteurs GT3HD).
- **Humidity (%) :** mesure de l'humidité. Ce champ est vide si seuls les capteurs de température SRT sont déployés.

Les capteurs environnementaux signalent leurs valeurs via le MIB des rPDU Vertiv™ PowerIT auxquelles ils sont connectés. Ce ne sont pas des capteurs autonomes possédant leur propre adresse IP. Dans cette version, les seuls capteurs valides sont les capteurs Vertiv™ PowerIT SRT, GTHD ou GTHD3 connectés aux rPDU Vertiv™ PowerIT.

REMARQUE : vous pouvez personnaliser le libellé de tout dispositif en vous connectant à ce dernier et en modifiant son nom en cliquant sur l'icône de configuration.

REMARQUE : pour supprimer un dispositif qui a été supprimé du réseau, cliquez sur l'icône de corbeille à côté du dispositif. Si vous sélectionnez l'icône de suppression, le dispositif et tous les capteurs environnementaux connectés à ce dispositif seront supprimés.

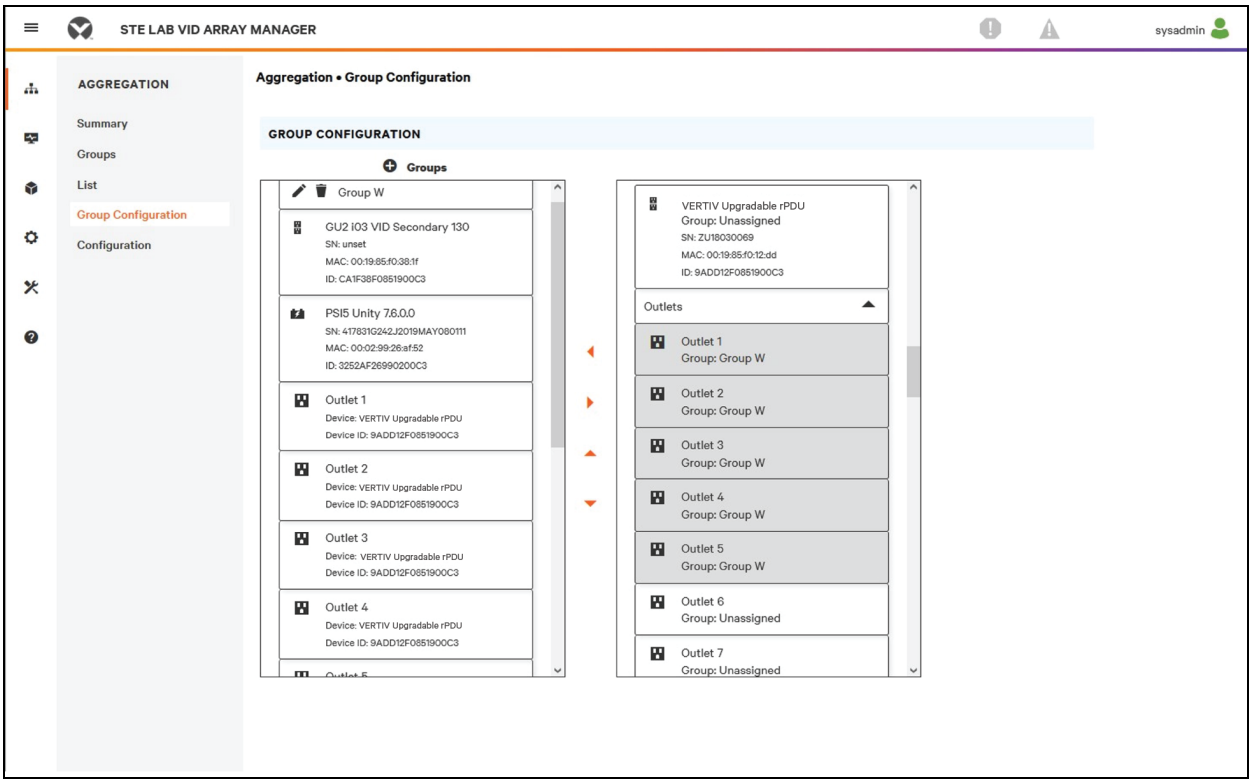
Refroidissement thermique

- **State :** état du refroidissement. L'état est Normal ou Unavailable (perte de connectivité).
- **Name :** libellé du dispositif de refroidissement thermique. En cliquant sur le nom, vous ouvrez un onglet de navigateur pour accéder aux dispositifs.
- **Group :** nom du groupe. S'il n'y a pas de groupe créé par l'utilisateur, le nom du groupe est Unassigned.
- **Host :** adresse MAC.
- **Fan Speed (%) :** vitesse du ventilateur du dispositif thermique.
- **Temperature (F) :** température du dispositif thermique.
- **Capacity (%) :** capacité du dispositif thermique.

6.4.4 Group Configuration

Sur la page Group Configuration, vous pouvez définir des groupes de dispositifs aux fins de consolidation de données et d'analyse. Un groupe fait souvent référence à une unité de mesure dans un environnement informatique qui comprend plusieurs dispositifs de groupe, comme un rack avec deux rPDU Vertiv™ PowerIT, des systèmes d'alimentation sans interruption et des capteurs environnementaux ou une ligne qui comprend plusieurs racks.

Figure 6.8 Group Configuration



La page Group Configuration répertorie les dispositifs détectés automatiquement dans la colonne *Unassigned* indiquant :

- Une ou plusieurs icônes définissant le type de dispositif, p. ex. rPDU Vertiv™ PowerIT, capteur environnemental, ASI ou prise de rPDU Vertiv™ PowerIT.
- Le libellé du dispositif
- Le numéro de série
- L'adresse MAC
- ID

Les groupes de dispositifs configurés (représentant généralement des racks) sont affichés à gauche.

Pour créer un nouveau groupe :

1. Cliquez sur le *signe plus (+)* à gauche de Groups pour ajouter un nouveau groupe sous Groups.
2. Cliquez sur l'icône Configuration pour modifier le nom du libellé du groupe.
3. Modifiez le libellé, si vous le souhaitez, puis cliquez sur *Save*.
4. Pour attribuer des dispositifs au groupe, mettez en surbrillance le groupe souhaité (dans la catégorie Groups), puis mettez en surbrillance les dispositifs souhaités dans la catégorie Unassigned.

REMARQUE : vous devez cliquer sur la flèche vers le bas qui se trouve sous la PDU pour afficher la liste des prises correspondantes.

5. Cliquez sur la *flèche droite* pour affecter les dispositifs au groupe.
6. Répétez la procédure pour d'autres groupes, comme requis.

REMARQUE : vous pouvez réorganiser les groupes en cliquant sur les flèches vers le haut ou vers le bas.

Pour supprimer des dispositifs d'un groupe :

Mettez les dispositifs en surbrillance, puis cliquez sur la *flèche droite*.

Pour supprimer un groupe :

Cliquez sur l'icône de corbeille à côté du nom du groupe.

REMARQUE : la suppression d'un groupe renvoie tous ses dispositifs vers le groupe Unassigned

6.5 Interfaces

Les dispositifs de groupe sont combinés pour former des groupes. Chaque dispositif conserve sa propre interface utilisateur autonome et ses données SNMP.

Pour accéder à l'interface utilisateur des dispositifs de groupe :

1. Dans la vue List, utilisez la souris pour survoler les entrées du tableau. Lorsque vous vous arrêtez sur les dispositifs, ceux-ci sont mis en surbrillance en jaune et une zone de texte apparaît. La zone de texte révèle l'adresse IP et le numéro de voie du dispositif.
2. Accédez à une adresse IP et un numéro de voie pour ouvrir l'interface du serveur Web du dispositif.

   -ou-

3. Cliquez sur le nom du dispositif pour accéder au lien hypertexte de l'interface Web du dispositif.

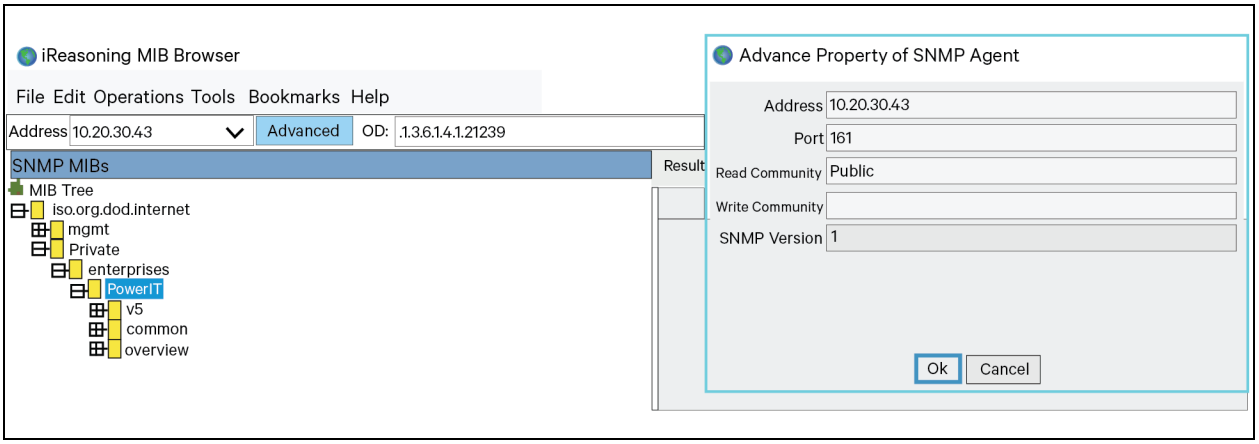
Pour accéder aux données SNMP des dispositifs de groupe :

Les données de la PDU en rack PowerIT SNMP sont disponibles par le biais d'un accès mappé par voie via l'adresse IP du dispositif gestionnaire de groupes à l'aide du MIB Vertiv™ PowerIT v5. Le fichier MIB est téléchargeable à partir de la page SNMP du gestionnaire de groupes.

1. Dans la vue List, utilisez la souris pour survoler les entrées du tableau. Lorsque vous vous arrêtez sur un dispositif, celui-ci est mis en surbrillance en jaune et une zone de texte contenant la voie SNMP du dispositif s'affiche.
2. Dans le navigateur MIB, saisissez la voie SNMP indiquée.

REMARQUE : les logiciels de surveillance des différents dispositifs de groupe doivent être capables d'accepter un numéro de voie SNMP unique par dispositif surveillé.

Figure 6.9 Navigateur MIB



6.5.1 Données SNMP de groupe

Les données consolidées, à la fois récapitulatives (telles que les valeurs kWh total et kW maximum) et les données du groupe, sont disponibles via la voie SNMP 161 par défaut et l'adresse IP de la rPDU Vertiv™ PowerIT du gestionnaire de groupes. Deux MIB sont disponibles pour la PDU en rack PowerIT du contrôleur de groupe :

- v5 : contient les points de données de la rPDU Vertiv™ PowerIT du gestionnaire de groupes individuel.
- Oneview : contient les points de données des données consolidées sur tous les dispositifs de groupe.

6.5.2 Conseils et dépannage

- Il est recommandé de mettre à jour tous les dispositifs vers la dernière version du firmware avant de configurer la consolidation.
- Assurez-vous que la PDU en rack désignée comme gestionnaire de groupes est entièrement configurée et que la consolidation est activée avant de connecter des dispositifs de groupe.
- Assurez-vous que tous les dispositifs de groupe sont dans un état défini en usine par défaut avant de les connecter au gestionnaire de groupes. Si les paramètres ont déjà été modifiés ou si des utilisateurs ont été définis sur un dispositif, les paramètres d'usine doivent être rétablis sur ce dernier avant la connexion au gestionnaire de groupes.
- Si vous rétablissez les paramètres d'usine par défaut sur une PDU en rack, assurez-vous d'utiliser la fonction *Utilities>Restore defaults>All Settings*. L'utilisation du bouton central de l'IMD ou du commutateur de réinitialisation encastré sous la voie réseau 2 pour réinitialiser les paramètres ne permet pas de réinitialiser tous les paramètres et peut empêcher l'identification correcte des dispositifs de groupes.
- Après avoir rétabli les paramètres d'usine par défaut d'une PDU en rack et avant de connecter cette dernière en tant que dispositif de groupe, déconnectez la PDU en rack du réseau et redémarrez-la en appuyant sur le bouton situé sous la voie réseau 1. Cela garantit la libération de toute adresse DHCP attribuée lors du rétablissement des paramètres d'usine par défaut.
- La reconnaissance des dispositifs de groupe après la configuration initiale peut prendre jusqu'à 20 minutes.
- Les données récapitulatives et consolidées du groupe ne peuvent pas être utilisées pour générer des alarmes.
- L'outil de provisionnement (*Provisioner>Discovery and Provisioner>File Management*) peut être utilisé pour mettre à jour facilement le firmware du gestionnaire de groupes et des PDU en rack des dispositifs de groupe.
- Les données récapitulatives et consolidées du groupe ne peuvent pas être utilisées pour générer des interruptions SNMP.
- Les noms de communauté SNMP sont configurés sur chaque dispositif. Suivez les liens des dispositifs affichés sur la page List sous le menu Devices et connectez-vous à chaque dispositif pour configurer le protocole SNMP.
- Ne modifiez pas le numéro de voie SNMP par défaut, les paramètres réseau ou les paramètres du serveur Web lorsque vous êtes connecté à un dispositif de groupe.
- Les interruptions et alarmes SNMP sont acheminées d'un dispositif vers le réseau de gestion via le gestionnaire de groupes.

Annexes

Annexe A: Assistance technique

A.1 Réinitialisation d'une rPDU Vertiv™ PowerIT

En cas de perte de communication d'une rPDU Vertiv™ PowerIT, il est possible de redémarrer le processeur manuellement sans incidence sur l'alimentation des prises. Si vous appuyez sur le bouton de redémarrage sur la face avant de l'IMD, vous redémarrerez le processeur. L'interface Web reste hors ligne pendant le démarrage. Pour plus d'informations, reportez-vous à la section Dispositif de surveillance interchangeable à la page 27.

A.2 Entretien et maintenance

Aucune opération d'entretien ou de maintenance n'est requise. L'ouverture de la rPDU Vertiv™ PowerIT peut invalider la garantie. La rPDU Vertiv™ PowerIT ne contient aucune pièce réparable par l'utilisateur autre que le dispositif de surveillance interchangeable (IMD) remplaçable sur site. Vertiv™ PowerIT recommande de couper l'alimentation de l'unité avant d'installer ou de retirer tout équipement.

L'IMD est conçu pour être remplacé sur site, uniquement par le personnel d'entretien dûment formé et qualifié. L'IMD est conçu pour être remplacé pendant que la rPDU Vertiv™ PowerIT est toujours connectée à l'alimentation secteur. Reportez-vous au Guide de remplacement des modules IMD de la rPDU Vertiv™ PowerIT pour plus d'informations.

A.3 Assistance technique supplémentaire

Vous pouvez contacter l'assistance technique à l'adresse www.Vertiv.com/support.

Amériques

- Site Web : *www.Vertiv.com/geist*
- E-mail : geistsupport@vertiv.com
- Téléphone : 1-888-630-4445

Europe et Moyen-Orient

- Assistance technique : *www.Vertiv.com/en-emea/support*
- E-mail : eoc@Vertiv.com
- Téléphone : 44 1823 275100

Asie

- Téléphone (anglais) : 1-888-630-4445 (États-Unis)
- Téléphone (Chine) : +86 755 23546462

A.4 Utilisation de Microsoft Exchange comme serveur SMTP

Si votre site utilise un serveur de messagerie Microsoft Exchange, celui-ci peut être utilisé par la rPDU IMD Vertiv™ PowerIT pour envoyer par e-mail des notifications d'alarme et d'avertissement. Cependant, il est possible que le serveur Exchange doive être configuré pour autoriser d'abord les connexions SMTP à partir de l'unité, car les services SMTP ou l'authentification de base sont souvent désactivés par défaut dans les versions ultérieures du serveur Exchange. Si la rPDU IMD Vertiv™ PowerIT n'arrive pas à envoyer des
e-mails via votre serveur Exchange, les conseils suivants peuvent vous aider.

REMARQUE : ces suggestions s'appliquent uniquement si vous utilisez votre propre serveur Exchange physique. Le service Office 365 hébergé de Microsoft n'est pas compatible avec la rPDU IMD Vertiv™ PowerIT utilisant des versions de firmware antérieures à la version 3.0.0, car Office 365 nécessite une connexion StartTLS. Les versions de firmware 3.0.0 et ultérieures prennent en charge StartTLS et sont compatibles avec Office 365.

Tout d'abord, étant donné que la rPDU IMD Vertiv™ PowerIT ne peut pas utiliser le protocole IMAP ou les protocoles MAPI/RPC Exchange/Outlook exclusifs de Microsoft pour envoyer des messages, vous devez activer SMTP en configurant un connecteur d'envoi SMTP sur le serveur Exchange. Pour plus d'informations sur la configuration d'un connecteur d'envoi SMTP dans Exchange, consultez cet article Microsoft TechNet : *http://technet.microsoft.com/en-us/library/aa997285.aspx*

Dans un deuxième temps, vous devrez peut-être configurer votre serveur Exchange pour autoriser le relais des messages à partir de l'unité de surveillance. En règle générale, cela impliquera d'activer l'option *Reroute incoming SMTP mail* dans les propriétés de routage du serveur Exchange, puis d'ajouter l'adresse IP de la rPDU IMD Vertiv™ PowerIT en tant que domaine autorisé à relayer le courrier via le serveur Exchange. Pour plus d'informations sur l'activation et la configuration du relais SMTP dans Exchange, consultez cet article Microsoft TechNet : *http://technet.microsoft.com/en- us/library/dd277329.aspx*.

Les méthodes d'authentification SMTP AUTH PLAIN et AUTH LOGIN pour la connexion au serveur ne sont souvent plus activées par défaut sur le serveur Exchange ; seule la méthode d'authentification NTLM exclusive de Microsoft est activée.

Pour réactiver la méthode AUTH LOGIN :

1. Dans la console Exchange, sélectionnez *Server Configuration - Hub Transport*.
2. Cliquez avec le bouton droit de la souris sur *Client Server*, puis sélectionnez *Properties*.
3. Sélectionnez l'onglet *Authentication* et cochez la case *Basic Authentication*.
4. Décochez la case *Offer Basic only after TLS*.
5. Cliquez sur *Apply* ou *Save*, puis cliquez sur *Exit*.

REMARQUE : vous devrez peut-être redémarrer le serveur Exchange après avoir effectué ces modifications.

Enfin, une fois que vous aurez activé SMTP, le relais et la méthode d'authentification de base AUTH LOGIN, vous devrez peut-être également créer un compte utilisateur spécifiquement pour que la rPDU IMD Vertiv™ PowerIT s'y connecte. Si vous avez créé un compte avant d'activer le connecteur d'envoi SMTP ou si vous essayez d'utiliser un compte créé pour un autre utilisateur et que la rPDU IMD Vertiv™ PowerIT ne peut toujours pas se connecter au serveur Exchange, le compte n'a probablement pas hérité correctement des nouvelles autorisations lorsque vous l'avez activé comme indiqué ci-dessus. Cela tend à se produire plus souvent sur les serveurs Exchange qui ont été mis à niveau depuis la création du compte que vous essayez d'utiliser, mais cela peut parfois se produire avec des comptes lorsque de nouveaux connecteurs et des modules d'extension sont ajoutés, quelle que soit la version d'Exchange. Supprimez les comptes utilisateur, puis créez-en un nouveau que l'unité de surveillance utilisera. Le nouveau compte devrait hériter correctement des autorisations d'authentification SMTP et de relais de messagerie.

Si aucune des suggestions ci-dessus ne résout le problème d'envoi d'e-mails par la rPDU IMD Vertiv™ PowerIT via votre serveur Exchange, vous devrez peut-être contacter l'assistance technique de Microsoft pour obtenir de l'aide pour configurer votre serveur Exchange afin d'autoriser l'envoi d'e-mails SMTP depuis un appareil tiers, autre que Windows, sur votre réseau.

Annexe B: Capteurs disponibles

B.1 Capteurs à distance

- SRT : capteur de température à distance en acier inoxydable.
- GTHD : température/humidité/point de rosée.
- GT3HD : température/humidité/point de rosée avec deux capteurs SRT.
- RTAFHD3 : température/débit d'air/humidité/point de rosée.
- A2D : convertit les capteurs d'E/S analogiques en capteurs numériques distants.

B.2 Capteurs d'E/S analogiques

- FS-15 : capteur d'inondation (eau).
- PFS-100 US/PFS-100 UN : capteur de panne de courant.
- RPDS : kit de commutateur de porte.

B.3 Capteurs intégrés et modulaires Liebert®

REMARQUE : un adaptateur est nécessaire pour utiliser l'un des capteurs suivants.

- SN-T : une sonde de température.
- SN-TH : une sonde de température et une sonde d'humidité.
- SN-Z01 : câble intégré avec une sonde de température.
- SN-Z02 : câble intégré avec trois sondes de température.
- SN-Z03 : câble intégré avec quatre sondes (trois capteurs de température et un capteur d'humidité).
- SN-2D : capteur de surveillance de commutation à deux portes.

B.4 Connexion des capteurs distants

Il est possible de connecter à l'unité jusqu'à 16 capteurs distants plug-and-play à tout moment via les connecteurs RJ-12 situés sur la face avant de l'unité. Dans certains cas, des répartiteurs peuvent être nécessaires pour ajouter des capteurs supplémentaires. Chaque capteur a un numéro de série unique et est automatiquement détecté et ajouté à la page Web. Le numéro de série des capteurs détermine leur ordre d'affichage sur le Web. Les noms des capteurs peuvent être personnalisés sur la page Sensors Overview.

REMARQUE : les capteurs utilisent des câbles Cat 5, un fil CMP et des connecteurs RJ-12. Le câblage doit être direct. L'inversion de polarité désactive temporairement tous les capteurs jusqu'à ce qu'elle soit corrigée. Les capteurs utilisent un protocole de communication série et sont soumis à des contraintes de signalisation réseau dépendant du blindage, du bruit ambiant et de la longueur du câble. Les installations typiques permettent des déploiements allant jusqu'à 600 ft (180 m) de câble de capteur.

Annexe C: Adaptateurs USB sans fil TP-Link

- Archer T2U Nano (adaptateur USB sans fil AC600 Nano)
- Archer T2U Plus (adaptateur USB sans fil bibande à gain élevé AC600)
- Archer T2U v3 (adaptateur USB sans fil bibande AC600)
- Archer T3U (mini adaptateur USB sans fil AC1300 MU-MIMO)
- Archer T3U Plus (adaptateur USB sans fil bibande à gain élevé AC1300)
- Archer T4U v3 (adaptateur USB sans fil bibande AC1300)

REMARQUE : ces dispositifs sont autodétectés lorsqu'ils sont connectés et ils peuvent être configurés en tant qu'interface de réseau supplémentaire.

Page laissée vierge intentionnellement

Annexe D: Voyants des prises

REMARQUE : cette annexe s'applique uniquement aux rPDU Vertiv™ PowerIT à prises surveillées/prises commutées.

Les voyants des prises fournissent une indication visuelle de l'état de l'alimentation des prises (activée, désactivée ou erreur). Les voyants sont numérotés dans l'ordre avec des chiffres blancs faciles à lire sur fond noir. Selon l'état de l'alimentation des prises, les voyants s'allument dans des couleurs fixes ou clignotantes.

Tableau D.1 Voyants des prises

LED	Description
Vert	Tension présente au niveau des prises et supérieure au seuil minimal
Rouge	Aucune tension au niveau des prises
Orange	Erreur de sortie d'alimentation détectée

Tableau D.2 Description de l'état des voyants

Tension mesurée	État du relais	État	LED	
Activé	Activé ou inconnu	Fixe	Vert	
Éteint	Désactivé ou inconnu	Fixe	Rouge	
Éteint	Activé	Clignotant[1]	Orange	Rouge
Activé	Éteint	Clignotant[2]	Orange	Vert

[1] La prise est détectée comme étant désactivée, mais elle devrait être activée.

[2] La prise est détectée comme étant activée, mais elle devrait être désactivée.

Code d'erreur

Les voyants s'allument en orange fixe dans les cas suivants :

- Panne de courant (tous les relais sont forcés à s'ouvrir en cas de panne de courant pour permettre le séquencement de la mise sous tension)
- Disjoncteur ouvert
- Aucune tension d'entrée détectée

Annexe E: Codes d'affichage IMD

Tableau E.1 Codes d'affichage IMD

Affichage	Type d'IMD	Explication
Err1	IMD-01 (à compteur uniquement)	L'IMD n'a découvert aucune carte d'entrée ou en a découvert plusieurs. Cela peut être dû à des problèmes de câblage interne ou à une carte d'entrée qui ne répond pas. Cette erreur s'affiche également en cas d'erreur de mesure signalée par la carte d'entrée.
8888	IMD-02, IMD-03, IMD-3	L'IMD est en train de démarrer et n'a pas encore détecté l'affichage simple. Le message *boot* s'affiche. Si ce message s'affiche pendant plus de quelques secondes, cela signifie qu'il y a un problème au niveau du tableau d'affichage ou du câblage interne.
-- (deux tirets à la position d'affichage la plus à droite)	IMD-02, IMD-03, IMD-3	L'IMD ne peut pas communiquer avec la carte d'entrée. Cette erreur peut également s'afficher par intermittence pour des mesures individuelles. Un problème lié à la carte d'entrée ou au câblage interne s'est produit.
boot	IMD-01	L'IMD démarre et la détection de la carte d'entrée est en cours.
boot	IMD-02, IMD-03, IMD-3	Le firmware est en cours d'initialisation. Ce message est affiché pendant la mise à jour du firmware dans les cartes internes.
updt	IMD-02, IMD-03, IMD-3	Mise à jour du firmware en cours.
rset dflt	IMD-02, IMD-03, IMD-3	Après l'action de l'utilisateur, *rset* (réinitialisation) apparaîtra pendant une séquence de réinitialisation des paramètres. Lors de la réinitialisation d'un paramètre, le message *dflt* (valeur par défaut) s'affiche brièvement.
bcup	IMD-02, IMD-03, IMD-3	*bcup* (sauvegarde) apparaîtra lors d'une sauvegarde de la configuration.
rest conf	IMD-02, IMD-03, IMD-3	*rest* (restauration) et *Conf* (configuration) apparaîtront lors de la restauration d'une configuration.
____ (quatre traits de soulignement au bas de l'affichage)	IMD-03 IMD-3	L'affichage IMD a été configuré de telle sorte que la puissance totale, la tension et le courant ont été désactivés.

REMARQUE : l'IMD-5M n'a pas de codes d'affichage ; l'écran tactile affiche des informations d'état.

Page laissée vierge intentionnellement

Annexe F: Provisionnement – Format du fichier contenant les paramètres de configuration

REMARQUE : la section suivante décrit le format du fichier contenant les paramètres de configuration utilisés par l'outil de provisionnement. Les exemples suivent globalement les paramètres disponibles dans l'interface utilisateur Web de la rPDU Vertiv™ PowerIT.

1. Dans les exemples ci-dessous, vous pouvez copier les parties en bleu dans un fichier texte et les modifier selon les besoins. Vous pouvez ensuite charger le fichier texte dans l'outil de provisionnement.
2. Lorsque vous modifiez les fichiers de configuration, utilisez un éditeur de texte comme le Bloc-notes, qui enregistre les fichiers au format .txt.
3. Vous pouvez ignorer les indentations contenues dans les exemples.
4. Veillez à utiliser les guillemets appropriés lorsque vous modifiez la configuration.
5. Si un paramètre n'est pas contenu dans le fichier de configuration, sa valeur ne sera pas modifiée.
6. Lors de la configuration d'une rPDU Vertiv™ PowerIT qui n'a encore jamais été configurée (tout juste sortie d'usine), le premier paramètre à configurer doit être la définition d'un utilisateur administrateur. Reportez-vous à la section Utilisateurs locaux ci-dessous.
7. Pour combiner plusieurs paramètres (autres que ceux des utilisateurs locaux) dans un même fichier (reportez-vous également à la section Exemple 1 à la page 139 à la fin de ce document) :
   - Rassemblez tous les paramètres nécessaires dans un même fichier.
   - Supprimez toutes les occurrences de {"conf":{ sauf pour la première ligne du fichier.
   - Remplacez toutes les lignes contenant uniquement }} par une, (virgule) sauf pour la dernière ligne du fichier.
8. Si vous combinez des paramètres utilisateur locaux et d'autres paramètres dans un même fichier, reportez-vous à l'Exemple 2 à la page 140 à la fin de ce document.
9. Après avoir sélectionné *Provisioner>Discovery>Update*, saisissez le nom d'utilisateur et le mot de passe uniquement pour la configuration de rPDU Vertiv™ PowerIT qui ont déjà été configurées (le nom d'utilisateur et le mot de passe sont ceux des rPDU Vertiv™ PowerIT à provisionner). Il n'est pas nécessaire de saisir le nom d'utilisateur et le mot de passe lorsque vous configurez une unité pour la première fois (vous pouvez identifier ces unités par leur attribut Provisioned défini sur False).

Utilisateurs locaux

```
{ "auth": {
"username": {
"password": "userpw",
"enabled": true,
"control": false,
"admin": false,
"language": "en"}
}}
```

username	Nom d'utilisateur que vous allez créer (entre guillemets)
password	Mot de passe (entre guillemets)
enabled	Activation de l'utilisateur, déterminée par les options true ou false
control	Droits de contrôle attribués à l'utilisateur, déterminés par les options true ou false
admin	Droits d'administrateur attribués à l'utilisateur, déterminés par les options true ou false
language	Option permettant de remplacer la langue par défaut de l'utilisateur ; options possibles : « de », « en », « es », « fr », « ja », « ko », « pt », « zh »

LDAP

```
{"conf":{
"remoteAuth": {
"mode": "ldap",
"ldap": {
"host": "192.168.123.1",
"port": 389,
"mode": "activeDirectory",
"securityType": "ssl",
"bindDn": "",
"password": null,
"baseDn": "",
"userFilter": "(objectClass=posixAccount)",
"userId": "uid",
"userIdNum": "uidNumber",
"groupFilter": "(objectClass=posixGroup)",
"groupId": "gidNumber",
"groupMemberUid": "memberOf",
"enabledGroup": "enabled",
"controlGroup": "control",
"adminGroup": "admin"}}
}}
```

host	URL LDAP (ref RFC4516 > RFC2255) (entre guillemets), requise si le protocole LDAP est activé.
port	Voie du protocole de communication
mode	Compatibilité par défaut entre les différents types LDAP ; options possibles : « openLdap » ou « activeDirectory »
securityType	Chiffrement à utiliser lors de la connexion au serveur LDAP ; options possibles : « ssl » et « starttls »
bindDn	Nom distinctif (entre guillemets) (ref RFC4514 > RFC2253) utilisé pour la liaison au serveur d'annuaire ; si aucune valeur n'est définie, il s'agit d'une liaison anonyme
password	Mot de passe (entre guillemets) utilisé pour la liaison au serveur d'annuaire
baseDn	Nom distinctif (entre guillemets) (ref RFC4514 > RFC2253) à utiliser pour la base de recherche

userFilter	Filtre de recherche LDAP (entre guillemets) (ref RFC4515 > RFC2254), valeur posixAccount définie pour l'attribut objectClass (ref RFC2307)
userId	Équivalent à l'attribut « uid » (entre guillemets) ref (RFC2307)
userIdNum	Équivalent à l'attribut « uidNumber » (entre guillemets) (ref RFC2307)
groupFilter	Filtre de recherche LDAP (entre guillemets) (ref RFC4515 > RFC2254), valeur posixGroup définie pour l'attribut objectClass (RFC2307)
groupId	Équivalent à l'attribut « gidNumber » (entre guillemets) (ref RFC2307)
groupMemberUid	Équivalent à l'attribut « memberUid » (entre guillemets) (ref RFC2307)
enabledGroup	Droit « enabled » défini pour l'utilisateur (entre guillemets) dans ce groupe
controlGroup	Droit « control » défini pour l'utilisateur (entre guillemets) dans ce groupe
adminGroup	Droit « admin » défini pour l'utilisateur (entre guillemets) dans ce groupe

```
{"conf":{
"remoteAuth": {
"mode": "tacacs",
"tacacs": {
"authenticationServer1": "10.20.30.21",
"authenticationServer2": "10.20.30.70",
"accountingServer1": "10.20.30.21",
"accountingServer2": "10.20.30.70",
"sharedSecret": "secret",
"service": "raccess",
"adminAttribute": "admin=true",
"controlAttribute": "control=true",
"enabledAttribute": "enabled=true"}}
}}
```

authenticationServer1	Serveur d'authentification/d'autorisation principal (entre guillemets)
authenticationServer2	Autre serveur d'authentification/d'autorisation (entre guillemets)
accountingServer1	Serveur de gestion de comptes principal (entre guillemets)
accountingServer2	Autre serveur de gestion de comptes (entre guillemets)
sharedSecret	Secret (entre guillemets) partagé par le client et le serveur (une valeur nulle supprime le secret)
service	Valeur pour le champ de service dans les demandes TACACS. options possibles : « ppp » et « raccess »
adminAttribute	Droit « admin » octroyé à l'utilisateur (entre guillemets) avec cette paire attribut-valeur
controlAttribute	Droit « control » octroyé à l'utilisateur (entre guillemets) avec cette paire attribut-valeur
enabledAttribute	Droit « enabled » octroyé à l'utilisateur (entre guillemets) avec cette paire attribut-valeur

Radius

```
{"conf":{
"remoteAuth": {
"mode": "radius",
"radius": {
"authenticationServer1": "",
"authenticationServer2": "",
"accountingServer1": "",
"accountingServer2": "",
"sharedSecret": "Secret",
"groupAttribute": "filter-id",
"adminGroup": "admin",
"controlGroup": "control",
"enabledGroup": "enabled"}}
}}
```

authenticationServer1	Serveur d'authentification principal (entre guillemets)
authenticationServer2	Autre serveur d'authentification (entre guillemets)
accountingServer1	Serveur de gestion de comptes principal (entre guillemets)
accountingServer2	Autre serveur de gestion de comptes (entre guillemets)
sharedSecret	Secret partagé par le client et le serveur (entre guillemets)
groupAttribute	PAV indiquant le groupe d'accès de l'utilisateur ; valeurs possibles : « filter-id » et « management-privilege-level ».
adminGroup	Droit « admin » défini pour l'utilisateur (entre guillemets) appartenant à ce groupe
controlGroup	Droit « control » défini pour l'utilisateur (entre guillemets) appartenant à ce groupe
enabledGroup	Valeur « enabled » (activé) définie pour l'utilisateur (entre guillemets) appartenant à ce groupe

Nom d'hôte et adresses IP du réseau

```
{"conf":{
"system": {
"hostname": "rPDUhostname",
"ip6Enabled": true},
"network": {
"ethernet": {
"label": "Bridge 0",
"enabled": true,
"dhcpOn": false,
"address": {
"0": {"address": "192.168.123.123","prefix": 24},
"1": {"address": "10.20.30.43","prefix": 24}}}}
}}
```

Hostname	Nom (entre guillemets) identifiant l'unité au sein du réseau
ip6Enabled	Options true ou false disponibles, permettant d'activer ou de désactiver la prise en charge du protocole IPV6
label	Libellé du pont (entre guillemets)
enabled	Options true ou false disponibles, permettant d'activer ou de désactiver le pont réseau
dhcpOn	Options true ou false disponibles, permettant d'activer ou de désactiver le protocole DHCP
address	Adresse IP (entre guillemets) de l'interface
prefix	Préfixe de l'adresse IP de l'interface

Voies réseau

```
{"conf":{
"network": {
"port0": {
"label": "Port 0",
"enabled": true,
"stp": {"cost": 0}},
"port1": {
"label": "Port 1",
"enabled": true,
"stp": {"cost": 0}}}
}}
```

label	Libellé de la voie (entre guillemets)
enabled	Activation de la voie, déterminée par les options true ou false
cost	Coût STP du contrôle

Routage réseau

```
{"conf":{
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
}}
```

gateway	Adresse de la passerelle (entre guillemets) pour le routage
prefixDestination	Préfixe réseau, 0 pour la passerelle par défaut
destination	Adresse réseau de destination (entre guillemets), « 0.0.0.0 » pour le réseau par défaut

DNS réseau

```
{"conf":{
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
}}
```

address	Adresse du serveur DNS (entre guillemets). la deuxième adresse correspond à l'autre serveur DNS.

RSTP réseau

```
{"conf":{
"network": {
"ethernet": {
"stp": {
"enabled": false,
"mode": "rstp",
"bridgePriority": 24576,
"helloTime": 2,
"maxAge": 40,
"maxHops": 40,
"forwardDelay": 21}}}
}}
```

enabled	Activation du protocole STP, déterminée par les options true ou false
mode	Options possibles : « stp » ou « rstp » ; le protocole RSTP prend en charge le retour à STP si nécessaire
bridgePriority	Priorité du pont STP de cette interface
helloTime	Intervalle, en secondes, entre les transmissions périodiques des messages de configuration
maxAge	Ancienneté maximale des informations transmises par cette interface lorsqu'elle sert de pont racine. paramètre utilisé lorsque « mode » est défini sur « stp ». valeur minimale : 2 * (helloTime + 1)
maxHops	Nombre maximal de fois où les informations transmises par cette interface traversent le pont lorsque l'interface sert de pont racine ; paramètre utilisé lorsque « mode » est défini sur « rstp »
forwardDelay	Délai utilisé par les ponts pour faire passer le pont racine et les voies désignées en mode de transfert ; valeur minimale : (maxAge / 2) + 1

Serveur Web

```
{"conf":{
"http": {
"httpEnabled": true,
"httpPort": 80,
"httpsPort": 443}
}}
```

httpEnabled	Options true ou false disponibles pour autoriser les communications non chiffrées
httpPort	Numéro de voie pour les communications HTTP
httpsPort	Numéro de voie pour les communications HTTPS

Rapports

```
{"conf":{
"report": {
"0": {
"start": "00:00",
"days": "MTWTFSS",
"targets": ["1","2"],
"interval": 1},
"1": {
"start": "00:00",
"days": "MT-----",
"targets": ["1"],
"interval": 1}}
}}
```

start	Heure de début de l'intervalle. Format « (00-23):(00-59) » configurable par incréments de 15 minutes
days	Première lettre des jours sélectionnés (entre guillemets), du lundi au dimanche (en anglais). les tirets (« - ») représentant les jours non sélectionnés
	Liste de clés indiquant les cibles e-mail (entre guillemets)
interval	Durée en heures entre les rapports ; options possibles : 1, 2, 3, 4, 6, 8, 12 et 24

Affichage

```
{"conf":{
"display": {
"gmsd": {
"mode": "currentAndTotalPower",
"inverted": false,
"vlc": {"enabled": false}}}
}}
```

mode	Sélection des données à présenter sur l'affichage ; options possibles : « current », « totalPower » et « currentAndTotalPower »
inverted	Options true ou false indiquant l'orientation de l'affichage

Time

```
{"conf":{
"time": {
"mode": "ntp",
"datetime": "2021-03-09 12:05:36",
"zone": "UTC",
"ntpServer1": "0.pool.ntp.org",
"ntpServer2": "1.pool.ntp.org"}
}}
```

mode	Mode ; options possibles : « ntp » et « manual »
datetime	Date et heure au format « AAAA-MM-JJ HH:MM:SS », les heures allant de 0 à 23 (affichage de l'heure locale) ; à utiliser uniquement lorsque le mode est défini sur « manual »
Zone	Nom (entre guillemets) valide issu de la base de données de fuseaux horaires
ntpServer1	Adresse du serveur NTP principal (entre guillemets) ; à utiliser uniquement lorsque le mode est défini sur « ntp »
ntpServer2	Adresse du serveur NTP secondaire (entre guillemets) ; à utiliser uniquement lorsque le mode est défini sur « ntp »

SSH

```
{"conf":{
"ssh": {
"enabled": true,
"port": 22}
}}
```

enabled	Options true ou false disponibles, permettant d'activer ou de désactiver le protocole SSH
port	Numéro de voie pour les communications SSH

USB

```
{"conf":{
"usb": {"enabled": true}
}}
```

enabled	Options true ou false disponibles, permettant d'activer ou de désactiver la voie USB

Voie série

```
{"conf":{
"serial": {
"baudRate": 115200,
"dataBits": 8,
"enabled": true,
"parity": "none",
"stopBits": 1}
}}
```

baudRate	Débit en bauds ; options possibles : 1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600 et 115 200
dataBits	Nombre de bits de données par trame ; options possibles : 7 et 8
enabled	Options true ou false disponibles, permettant d'activer ou de désactiver l'interface de ligne de commande série sur un dispositif
parity	Type de bits de parité utilisé dans la trame ; options possibles : « none », « even » et « odd »
stopBits	Nombre de bits d'arrêt utilisés pour terminer chaque trame ; options possibles : 1 et 2

Email

```
{"conf":{
"email": {
"server": "Example-server",
"port": 25,
"sender": "From email address",
"username": "username",
"password": "password",
"target": {
"0": {"name": "email1@domain.com"},
"1": {"name": "email2@domain.com"}}}
}}
```

Server	Adresse du serveur SMTP (entre guillemets)
port	Numéro de voie SMTP
sender	Adresse e-mail de l'expéditeur (entre guillemets)
username	Nom d'utilisateur SMTP (entre guillemets)
password	Mot de passe SMTP (entre guillemets)
name	Adresse e-mail du destinataire (entre guillemets)

SNMP v1 ou v2c


```
{"conf":{
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.10",
"trapVersion": "1"},
"1": {
"port": 162,
"name": "10.20.30.11",
"trapVersion": "1"},
"2": {
"port": 162,
"name": "10.20.30.12",
"trapVersion": "2c"}}}
}}
```


v1v2cEnabled	Options true ou false disponibles, permettant d'activer ou de désactiver les versions SNMP 1 et 2c
port	Numéro de voie pour les communications SNMP
readCommunity	Nom de la communauté (entre guillemets) possédant les droits en lecture ; doit être différent du nom défini pour writeCommunity
writeCommunity	Nom de la communauté (entre guillemets) possédant les droits en écriture ; doit être différent du nom défini pour readCommunity
trapCommunity	Nom de la communauté d'interruption (entre guillemets)
port	Numéro de voie pour les interruptions SNMP
name	Adresse (entre guillemets) de destination des interruptions SNMP
trapVersion	Version des interruptions SNMP ; options possibles : « 1 » ou « 2c »

SNMP v3


```
{"conf":{
"snmp": {
"v3Enabled": true,
"port": 161,
"user": {
"0": {
"privPassword": "password",
"type": "read",
"username": "name",
"privType": "aes",
"authPassword": "password",
"authType": "sha1"},
"1": {
"privPassword": "password",
"type": "write",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"},
"2": {
"privPassword": "password",
"type": "trap",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"}}}
}}
```


v3Enabled	Options true ou false disponibles, permettant d'activer ou de désactiver les versions SNMP 1 et 2c
port	Numéro de voie pour les communications SNMP
type	Type d'autorisation ; valeurs possibles : « read », « write » ou « trap »
username	Nom d'utilisateur SMTPv3 (entre guillemets)
privPassword	Mot de passe de confidentialité (entre guillemets)
privType	Type de chiffrement pour la confidentialité ; valeurs possibles : « aes », « des » ou « none »
authPassword	Mot de passe d'authentification (entre guillemets)
authType	Type d'authentification ; valeurs possibles : « sha1 »,« md5 » ou « none »

Syslog

```
{"conf":{
"syslog": {
"enabled": true,
"target": "10.20.30.40",
"port": 514}
}}
```

enabled	Options true ou false disponibles, permettant d'activer ou de désactiver la transmission de messages Syslog vers une destination distante
target	Adresse (entre guillemets) de la destination distante pour les messages Syslog
port	Numéro du voie de destination des messages

Admin

```
{"conf":{
"contact": {
"description": " PowerIT PDU ",
"location": "Example Location",
"contactName": "Example Contact",
"contactEmail": "email@example.com",
"contactPhone": "123 456 789"},
"system": {"label": "System Label"}
}}
```

description	Description de l'unité (entre guillemets)
location	Emplacement de l'unité (entre guillemets)
contactName	Nom de la personne en charge de l'unité (entre guillemets)
contactEmail	Adresse e-mail de la personne en charge de l'unité (entre guillemets)
contactPhone	Numéro de téléphone de la personne en charge de l'unité (entre guillemets)
label	Libellé du système de l'unité (entre guillemets)

Paramètres régionaux

```
{"conf":{
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

defaultLang	Langue ; options possibles : « de », « en », « es », « fr », « ja », « ko », « pt », « zh »
units	Unités ; options possibles : « metric » et « imperial »

Intervalle de journalisation des données

```
{"conf":{
"datalog": {"interval": 15}
}}
```

interval	Intervalle de journalisation des données en minutes

Consolidation

```
{"conf":{
"oneview": {
"enabled": true,
"username": "x",
"password": "pass"}
}}
```

enabled	Activation de la consolidation, déterminée par les options true ou false
username	Nom d'utilisateur (entre guillemets) pour les dispositifs de groupe
password	Mot de passe (entre guillemets) pour les dispositifs de groupe (une valeur nulle supprime le mot de passe)

Exemple 1

Fichier de configuration d'un nom d'hôte, de l'adresse IP, de la passerelle, des noms de communauté SNMP v1 et des paramètres régionaux :

```
{"conf":{
"system": {
"hostname": "hostname1"},
"network": {
"ethernet": {
"dhcpOn": false,
"address": {
"0": {"address": "10.20.30.40","prefix": 24}}}}
,
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
,
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
```

```
,
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.60",
"trapVersion": "1"}}}
,
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

Exemple 2

Fichier de configuration d'un utilisateur admin, de désactivation du protocole HTTP et de configuration d'un serveur NTP :

```
{ "auth": {
"username": {
"password": "userpw",
"enabled": true,
"control": false,
"admin": false,
"language": "en"}
},
"conf":{
"http": {
"httpEnabled": false}
,
"time": {
"mode": "ntp",
"zone": "UTC",
"ntpServer1": "0.pool.ntp.org", "ntpServer2": "1.pool.ntp.org"} }}
```

Paramètres des capteurs et alarmes

```
{"dev": {
    "0000000000000000": {
        "label": "PDU 22A",
        "type": "i03",
        "conf": {"outletControlEnabled": true},
        "outlet": {
```

```
            "0": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.25,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 1"
            },
            "1": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.50,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 2"
            }
        },
        "entity": {
            "total0": {"label": "Total"},
            "breaker0": {"label": "Circuit 1"},
            "breaker1": {"label": "Circuit 2"},
            "phase0": {"label": "Phase A"},
            "phase1": {"label": "Phase B"},
            "phase2": {"label": "Phase C"},
            "line3": {"label": "Neutral Line"}
        }
    }
},
"alarm": {
    "action": {
        "0": {
            "target": "trap0",
            "delay": 0,
            "repeat": 0
        },
        "1": {
            "target": "email0",
            "delay": 0,
            "repeat": 0
        }
   },
    "trigger": {
        "0": {
            "path": "0000000000000000/entity/phase0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 222.0,
            "tripDelay": 0,
            "clearDelay": 1,
            "latching": false,
            "selectedActions": ["0","1"]
        },
        "1": {
            "path": "0000000000000000/outlet/0/measurement/0",
```

```
            "severity": "alarm",
            "type": "low",
            "threshold": 55.0,
            "tripDelay": 2,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "2": {
            "path": "0000000000000000/entity/breaker0/measurement/4",
            "severity": "alarm",
            "type": "high",
            "threshold": 12.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "3": {
            "path": "0000000000000000/entity/total0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 7200.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        }
    }
}}
```


0000000000000000 — Paramètre ID de dispositif (disponible sur la page sensors>overview) de la rPDU à configurer. Si cet ID de dispositif ne correspond à aucun des dispositifs sélectionnés en cours de provisionnement, tous les dispositifs sélectionnés seront provisionnés. La définition d'ID de dispositif sur 0000000000000000 garantit la configuration de tous les dispositifs sélectionnés.

label — Libellé de la rPDU (affiché sur la page sensors>overview)

type — Pour définir des alarmes sur les mesures internes de la PDU, le « type » doit correspondre à l'IMD utilisé sur la PDU ; ce champ doit donc être renseigné par « i03 » pour les PDU utilisant n'importe quel IMD-03x ou IMD-3x, et « i05 » pour les PDU utilisant l'IMD-5M.

Pour définir des alarmes sur des capteurs externes, le champ « type » doit être renseigné par le type du capteur externe. Les valeurs correctes sont « remotetemp », « afht3 », « thd », « t3hd », « a2d », « snt », « snh » et « snd ».

Si ce paramètre est omis, cela empêche la configuration de toute rPDU sélectionnée lorsque l'ID de dispositif ne correspond à celui d'aucune rPDU.

outletControlEnabled	S'applique uniquement aux rPDU à prises commutées et détermine s'il est possible de contrôler les prises sur une rPDU à prises commutées. La valeur true permet de contrôler les prises, la valeur false empêche le contrôle des prises.
outlet	La section Outlet s'applique uniquement aux rPDU à prises commutées et définit les paramètres de chaque prise de rPDU. Notez que la numérotation des prises commence à 0 (prise de rPDU numéro 1). Des prises individuelles (ou toute la section Outlet) peuvent être omises si ces paramètres ne nécessitent pas de modification.
poaAction	Définit l'état dans lequel la prise démarrera lorsqu'elle sera mise sous tension (« on », « off » ou « last »).
rebootHoldDelay	Temps d'attente, en secondes, qui s'écoule après que l'unité a mis la prise hors tension, avant de la remettre en marche lors d'un redémarrage. Peut être n'importe quel nombre entier compris entre 0 et 14 400.
rebootDelay	Temps d'attente, en secondes, qui s'écoule avant que l'unité redémarre une prise. Peut être n'importe quel nombre entier compris entre 0 et 14 400.
poaDelay	Temps d'attente, en secondes, qui s'écoule avant que l'unité, après sa mise sous tension, mette la prise sous tension. Peut être n'importe quel nombre entier compris entre 0 et 14 400.
onDelay	Temps d'attente, en secondes, qui s'écoule avant que l'unité mette une prise en marche. Peut être n'importe quel nombre entier compris entre 0 et 14 400.
mode	Devrait avoir la valeur « manual » pour les prises contrôlées par l'utilisateur.
offDelay	Temps d'attente, en secondes, qui s'écoule avant que l'unité arrête une prise. Peut être n'importe quel nombre entier compris entre 0 et 14 400.
label	Libellé de la prise.
entity	La section entity est utilisée pour libeller les mesures qui ne sont pas liées aux prises sur la page sensors>overview.
total0 label	Libellé du total des rPDU dans la page sensors>overview
breaker0 label	Libellé du premier circuit (le cas échéant). Les autres circuits, s'ils sont présents, peuvent être libellés breaker1, breaker2, etc.
phase0 label	Libellé de la première phase. Les autres phases, si elles sont présentes, peuvent être libellées phase1 et phase2.
line3 label	Libellé de la ligne neutre.
alarm	La section Alarm définit les méthodes qui peuvent être utilisées pour envoyer des alarmes. Chaque méthode est numérotée à partir de 0 et définit :
target	Pour l'émission d'alarmes d'interruptions SNMP, la cible peut avoir les valeurs « trap0 », « trap1 », etc. qui désignent la première, la deuxième, etc. interruptions SNMP définies dans la page System>SNMP.

Pour l’émission d’alarmes par e-mail, la cible peut avoir les valeurs « email0 », « email1 », etc. qui désignent le premier, le deuxième, etc. e-mail cible défini dans la page System>Email.

Notez que la cible ne doit pas spécifier d’interruptions SNMP ou de cibles d’e-mail qui n’ont pas été configurées.

delay Détermine pendant combien de temps cet événement doit rester déclenché avant l’envoi de la première notification verticale de cette action.

repeat Détermine si plusieurs notifications seront envoyées pour cette action d’événement.

trigger Cette section définit les alarmes qui ont été configurées, en commençant par la première alarme portant le numéro 0.

Chemin Définit la mesure qui doit déclencher une alarme. Le format de ce champ est le suivant :

« 0000000000000000/entity/phase0/measurement/0 » définit les alarmes des mesures de phase d’entrée de la rPDU, phase0 désignant la première phase d’entrée de la rPDU, phase1 la deuxième phase (le cas échéant), etc. Le nombre suivant immédiatement la mesure indique le type de mesure à associer à une alarme comme défini ci-dessous :

0 : Tension

4 : courant

8 : puissance réelle

9 : puissance apparente

10 : facteur de puissance

11 : énergie

14 : facteur de courant de crête

« 0000000000000000/outlet/0/measurement/0 » définit les alarmes de sortie des rPDU avec surveillance des prises, le nombre suivant immédiatement outlet désignant le numéro de la prise (à partir de zéro). Le nombre suivant immédiatement la mesure indique le type de mesure à associer à une alarme comme défini ci-dessous :

0 : Tension

4 : courant

8 : puissance réelle

9 : puissance apparente

10 : facteur de puissance

11 : énergie

12 : équilibre

	14 : facteur de courant de crête « 0000000000000000/entity/total0/measurement/0 » définit les alarmes des mesures d’entrée totales de phase de la rPDU. Le nombre suivant immédiatement la mesure indique le type de mesure à associer à une alarme comme défini ci-dessous : 0 : puissance réelle 1 : puissance apparente 2 : facteur de puissance 3 : énergie « 0000000000000000/entity/breaker0/measurement/4 » définit les alarmes de circuit de la rPDU, breaker0 désignant le premier circuit, breaker1 le deuxième circuit, etc. Le nombre suivant immédiatement la mesure indique le type de mesure à associer à une alarme comme défini ci-dessous : 4 : courant « 0000000000000000/entity/line3/measurement/4 » définit les alarmes de courant neutre de la rPDU. Le nombre suivant immédiatement la mesure indique le type de mesure à associer à une alarme comme défini ci-dessous : 0 : courant
severity	Peut être « warning » ou « alarm », ce qui détermine la gravité de l’alarme générée.
type	Peut être « high » ou « low », ce qui définit s’il s’agit d’un seuil haut ou bas.
threshold	Valeur de seuil qui peut être n’importe quel nombre compris entre -999,0 et 999,0. Le courant de ligne neutre peut contenir jusqu’à deux décimales.
tripDelay	La mesure doit dépasser le seuil pendant ce nombre de secondes avant que l’événement ne se déclenche. Il peut s’agir de n’importe quel nombre entier compris entre 0 et 14 400.
clearDelay	La mesure doit revenir à la normale pendant ce nombre de secondes avant que l’événement ne soit effacé et réinitialisé. Il peut s’agir de n’importe quel nombre entier compris entre 0 et 14 400.
latching	Peut être true ou false. Si True, l’événement et les actions qui lui sont associées restent actifs jusqu’à ce que l’événement soit confirmé, même si la mesure revient par la suite à la normale.
selectedActions	Définit les actions définies ci-dessus à utiliser pour envoyer l’alarme. Par exemple, [« 0 », « 1 » définit les actions 0 et 1 qui sont définies comme des actions utilisant trap0 et email0 dans l’exemple ci-dessus.

Page laissée vierge intentionnellement

Annexe G: Codes d'erreur API/CLI

G.1 Success

Code	Explication
Success	Réussite de l'opération

Erreurs d'authentification

Code	Explication
No Admin user configured	Vous devez configurer au moins un utilisateur admin dans le système
Not Authorized	L'utilisateur actuel ne dispose pas de l'autorisation nécessaire
Not Authorized: Session expired	Le jeton utilisé n'est plus valide
Not Authorized: Not enough permissions	L'utilisateur actuel ne dispose pas d'autorisations suffisantes pour effectuer cette opération
Invalid credential combination	La combinaison nom d'utilisateur/mot de passe a été fournie avec le jeton ou seul le nom d'utilisateur ou le mot de passe a été fourni
Must have at least one admin user	Vous devez configurer au moins un utilisateur admin dans le système

Erreurs de format JSON

Code	Explication
Malformed JSON	Structure JSON reçue non valide ou corrompue
Missing field	Un champ qui devait être défini n'a pas été trouvé dans la structure JSON
Duplicate fields	Un même champ a été défini plusieurs fois, par exemple dans le corps HTTP et dans la chaîne de requête

Erreurs de chemin

Code	Explication
Invalid path	Le chemin indiqué ne répond pas aux exigences du système
Path not found	Le chemin indiqué n'a pas été trouvé
Identifier not found	Un des champs de la structure JSON reçue n'existe pas
Field not applicable	Un champ de la structure JSON existant n'aurait pas dû être envoyé

Erreurs de validation des données

Code	Explication
Invalid input	Un champ de saisie n'est pas valide et ne correspond pas aux autres catégories de validation des données
Input too long	Un champ de saisie contient une valeur dépassant la longueur maximale autorisée
Invalid characters	Un champ de saisie contient des caractères non valides pour ce champ
Invalid serial	Un champ de saisie contient un numéro de série non valide
Invalid Boolean	Un champ de saisie contient une valeur booléenne non valide
Out of range	Un champ de saisie contient une valeur en dehors de la plage autorisée pour ce champ
Invalid integer	Un champ de saisie acceptant uniquement des nombres entiers contient un nombre non entier
Invalid number	Un champ de saisie acceptant uniquement les nombres contient une valeur non numérique
Invalid URL	Un champ de saisie d'URL contient une URL non valide
Invalid IP	Un champ de saisie d'adresse IP contient une adresse IP non valide
Paths not allowed	Un champ de saisie contient un chemin alors qu'une autre valeur devrait être saisie
Invalid username	Un champ de saisie contient un nom d'utilisateur non pris en charge
Invalid email address	Un champ de saisie d'adresse e-mail contient une adresse e-mail non valide
Invalid option	Un champ de saisie contient une option non valide
Invalid datetime	Un champ de saisie de date/d'heure contient une date ou une heure non valide
Out of bounds	Une valeur en dehors de la plage autorisée a été saisie dans le champ
Invalid week	Un champ de saisie contient une sélection de jours de la semaine non valide
Duplicate entry	Un champ de saisie va entraîner la création d'une valeur dupliquée non autorisée
Invalid Route	Routage réseau mal configuré

Autres erreurs

Code	Explication
Unknown error	Erreur système ne correspondant à aucun code d'erreur
Command not allowed	La commande reçue n'est pas autorisée au niveau du chemin spécifié
System busy	L'action tentée par l'utilisateur ne peut pas être exécutée pour le moment. La tentative doit être renouvelée ultérieurement

Erreurs de cohérence des données

Code	Explication
Inconsistent state	La commande a été refusée, car elle provoquerait un état incohérent du système
Syslog enabled requires target	Un hôte cible doit être spécifié pour l'activation d'un serveur Syslog distant
NTP mode requires servers	Un serveur doit être spécifié pour l'envoi de requêtes lorsque le mode NTP est activé

Code	Explication
Start time must come before end time	L'heure de début saisie est postérieure à l'heure de fin
Invalid SNMPv3 auth/priv combination	Impossible d'utiliser la confidentialité SNMPv3 sans l'authentification
Port not available	L'utilisateur a tenté de définir un numéro de voie déjà utilisé
Vertiv Intelligence Director missing credentials	Pour activer Vertiv Intelligence Director, il faut définir un nom d'utilisateur et un mot de passe
Time not settable	Le mode de réglage de l'heure doit être défini sur manuel pour que la date et l'heure puissent être configurées

Erreurs de chargement

Code	Explication
Invalid firmware package	Le format de package est incorrect ou le package est corrompu
Invalid file key	La clé OEM spécifiée pour le package est erronée et ne peut pas être utilisée avec cette unité
Invalid version	La version utilisée est obsolète ou n'est pas prise en charge
Invalid product	Le package est destiné à une architecture matérielle différente
Invalid certificate file	Impossible d'analyser le certificat SSL fourni
Invalid certificate password	Le mot de passe ne correspond pas au certificat SSL fourni

Page laissée vierge intentionnellement

Annexe H: Exemple de configuration de LDAP pour les informations d'identification Active Directory

H.1 Présentation

L'intégration d'Active Directory au dispositif de surveillance interchangeable (IMD) de marque Vertiv et PowerIT permet l'authentification et l'autorisation des utilisateurs au niveau de l'interface Web et CLI de l'IMD à l'aide de leurs informations d'identification Active Directory d'entreprise. L'utilisateur sera également autorisé dans l'un des trois rôles IMD basés sur un groupe de sécurité Active Directory dont il est membre. Ces rôles sont les suivants :

- Admin : droits de configuration complets, y compris les autorisations du rôle Control.
- Control : possibilité de contrôler l'état des prises, le cas échéant, de modifier les noms des dispositifs et les paramètres d'alarme/d'événement.
- Enabled : lecture seule des paramètres de configuration et aucun droit de contrôle des prises.

H.2 Exigences générales et remarques

- L'IMD version 5.3.3 ou le firmware le plus récent peuvent être utilisés pour cette procédure.
- Les exemples sont représentés en vert.

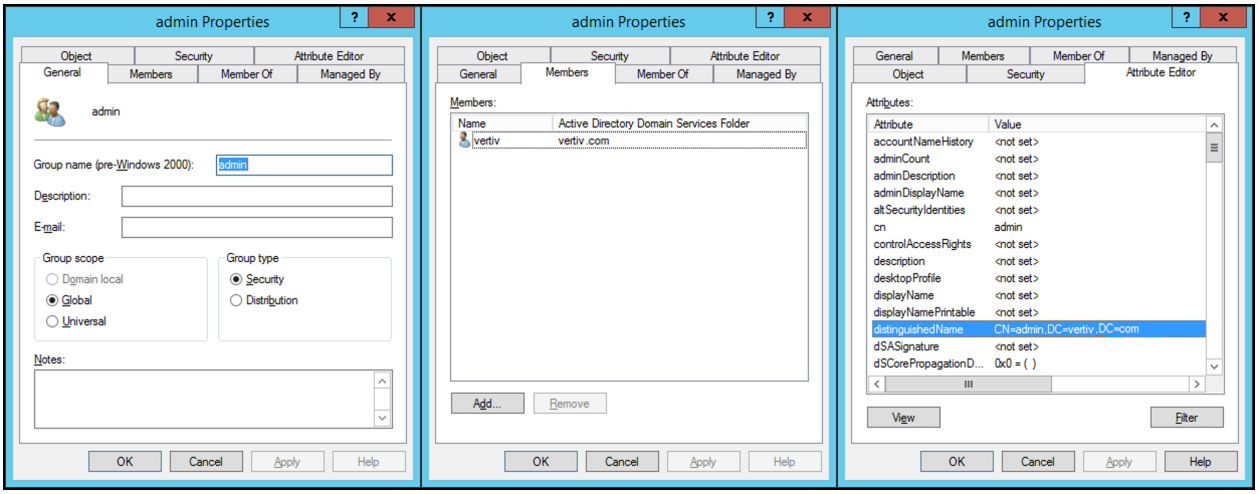
H.3 Procédure de configuration d'Active Directory

- Créez ou utilisez un compte de liaison AD existant pour l'IMD. Ce compte sera utilisé par l'IMD pour rechercher le domaine AD et authentifier les utilisateurs. Le mot de passe de ce compte doit être défini de manière à ne jamais expirer.
- Créez un ou plusieurs groupes de sécurité AD pour représenter les rôles Admin, Control et Enabled IMD.
- Définissez l'utilisateur AD comme un membre du groupe de sécurité pertinent.
    - Le compte AD « vertiv » a été attribué à un membre du groupe de sécurité « admin » dans l'exemple ci-dessous. Par conséquent, le compte d'utilisateur AD « vertiv » assumera le rôle d'administrateur de l'IMD lors de la connexion.

REMARQUE : la dénomination du groupe de sécurité est à votre discrétion. Le nom et le DN du groupe de sécurité doivent correspondre aux valeurs définies dans la section « Group » LDAP de l'IMD.

REMARQUE : un utilisateur AD appartenant à plusieurs de ces groupes de sécurité mappés par rôle IMD héritera des privilèges associés au rôle le plus élevé.

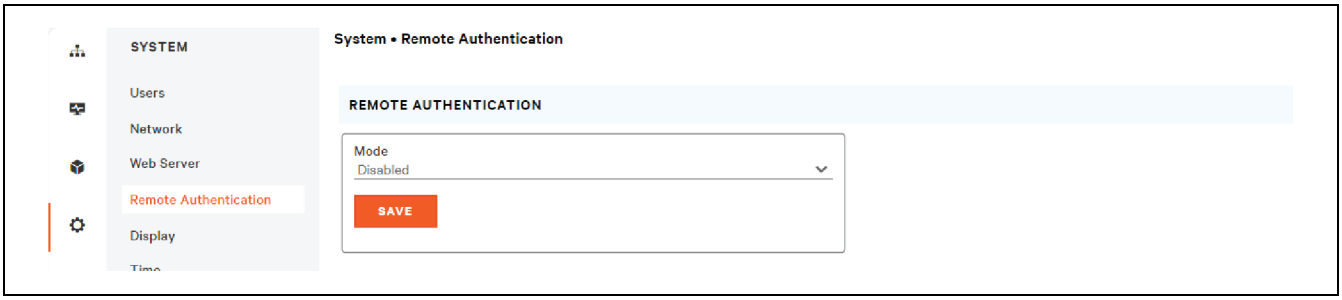
Figure H.1 Paramètres des propriétés d'administration



H.4 Procédure de configuration de l'IMD (interface Web)

- Ouvrez un navigateur Web sur le nom IP ou DNS de l'IMD et connectez-vous en tant qu'administrateur local.
- Accédez à *System >Remote Authentication.*
- Réglez le mode d'authentification à distance sur LDAP et enregistrez.

Figure H.2 Authentification à distance



- Reportez-vous à l'illustration ci-dessous pour les descriptions des paramètres de la section LDAP.

Figure H.3 Paramètre LDAP

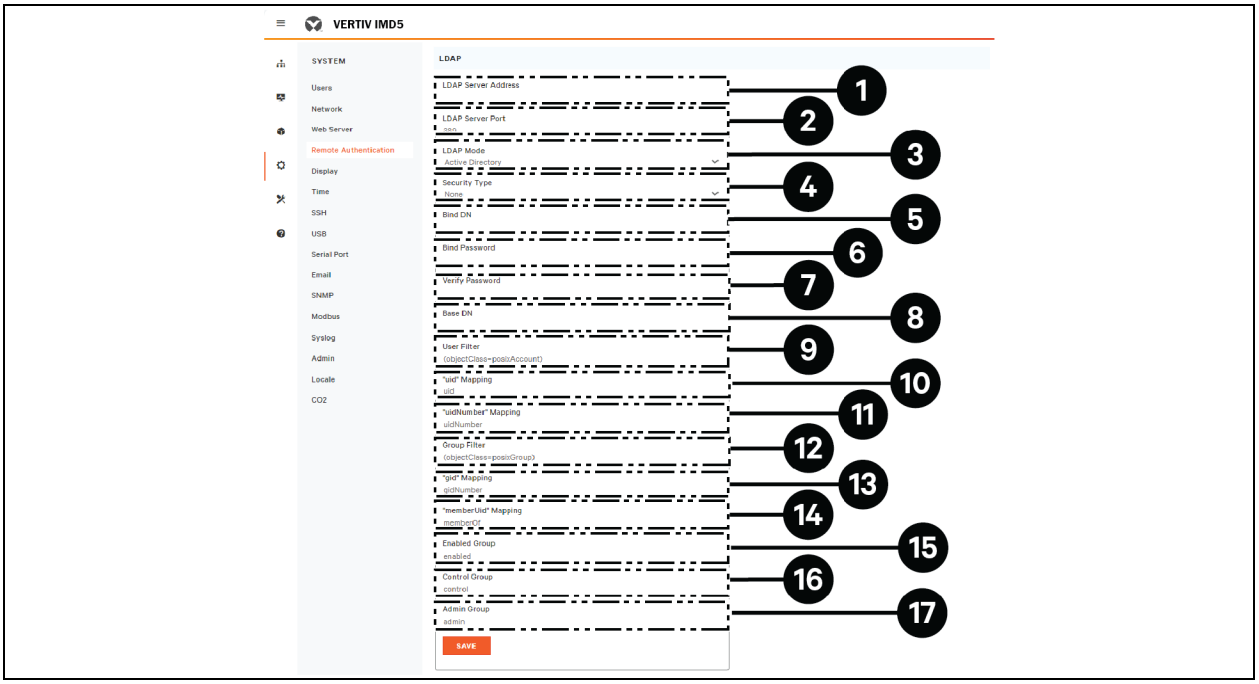


Tableau H.1 Paramètre LDAP

Élément	Description
1	Adresse IP du serveur Active Directory
2	Voie TCP Active Directory[2] 389 - Non SSL 636 – SSL
3	Mode LADAP OpenLDAP - Active Directory
4	Sécurité d'Active Directory[2] None – SSL – StartTLS
5	Compte AD utilisé pour la liaison au serveur AD Doit être au format de notation de chemin DN complet CN=adbindacct,CN=Users,DC=vertiv,DC=com Le mot de passe du compte ne doit pas expirer
6	Définir le mot de passe du compte de liaison AD
7	Vérifier le mot de passe
8	Chemin du domaine de base pour rechercher les utilisateurs AD[1] Doit être au format de notation de chemin DN complet DC=vertiv, DC=com
9	Filtre d'attribut ObjectClass d'utilisateur AD (objectClass=user)

Tableau H.1 Paramètre LDAP (suite)

Élément	Description
10	Filtre des noms de compte utilisateur AD samaccountname
11	Mappage « uidNumber » uidNumber
12	Filtre d'attribut ObjectClass du groupe AD (objectClass=group)
13	Mappage « gid » gidNumber
14	Paramètre obligatoire memberOf
15	Mappage du groupe de sécurité AD sur le rôle Enabled Doit être au format de notation de chemin DN complet CN=enabled, DC=vertiv, DC=com
16	Mappage du groupe de sécurité AD sur le rôle Control Doit être au format de notation de chemin DN complet CN=control, DC=vertiv, DC=com
17	Mappage du groupe de sécurité AD sur le rôle Admin Doit être au format de notation de chemin DN complet CN=admin, DC=vertiv, DC=com
REMARQUE : [1]la meilleure pratique consiste à réduire le champ de traversée du domaine AD pour rechercher des utilisateurs authentifiés. Essayez d'éviter de simplement spécifier le domaine de base lorsqu'il existe un schéma AD volumineux et imbriqué. • Idéal : OU=Enabled Users, OU=User Accounts, DC=vertiv, DC=com • Non idéal : DC=vertiv, DC=com	
REMARQUE : [2]StartTLS utilise la voie TCP 389. Il établit initialement la session non chiffrée, mais la chiffrera à partir de ce moment si la requête LDAP_START_TLS_OID est acceptée par le serveur Active Directory.	

Connect with Vertiv on Social Media

 https://www.facebook.com/vertiv/

 https://www.instagram.com/vertiv/

 https://www.linkedin.com/company/vertiv/

 https://www.x.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 États-Unis

SL-71211_REVC_02-26