Système de console avancé Avocent® ACS 800/8000

Guide d’installation et d’utilisation

Les informations contenues dans ce document peuvent être modifiées sans préavis et peuvent ne pas convenir à toutes les applications. Toutes les mesures nécessaires ont été prises afin de garantir l'exactitude et l'exhaustivité des informations contenues ce document. Vertiv rejette néanmoins toute responsabilité en cas de dommages découlant de l'utilisation de ces informations ou d'erreurs/omissions quelles qu'elles soient. Reportez-vous aux autres pratiques ou codes du bâtiment locaux applicables pour connaître les méthodes, les outils et le matériel appropriés à utiliser pour exécuter les procédures qui ne sont pas spécifiquement décrites dans ce document.

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 appartenant à Vertiv. Toute copie, divulgation ou utilisation de ces informations sans l'autorisation écrite de Vertiv est strictement interdite.

Les noms de sociétés et de produits sont des marques de commerce ou déposées appartenant à leurs 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.

Consultez la page https://www.vertiv.com/en-us/support/ pour obtenir une assistance supplémentaire.

TABLE DES MATIÈRES

1 Introduction

Le système de console avancé Avocent® ACS 800/8000 permet à la fois d'accéder à des dispositifs reliés et de les gérer, par exemple des consoles série, des modems ou des dispositifs d'alimentation. Le système de console assure la gestion sécurisée de datacenters distants et la gestion hors bande de ressources informatiques partout dans le monde.

NOTA : sauf indication contraire, toute référence à un système de console renvoie à tous les modèles de la série 800/8000.

Le système de console permet un accès local (voie console) et distant (IP et accès commuté) sécurisés. Il exécute le système d'exploitation Linux® avec un système de fichiers persistant dans une mémoire flash. Il est possible de le mettre à niveau à partir d'un fichier local sur un ordinateur connecté au système de console.

Plusieurs administrateurs peuvent se connecter simultanément au système de console et utiliser l'interface utilisateur Web, l'interface de ligne de commande (CLI) ou le logiciel DSView™ 4 pour accéder au système de console et le configurer.

NOTA : sauf indication contraire, toute référence au logiciel DSView dans ce document renvoie à la version 4 ou version ultérieure.

En fonction du modèle, le système de console est doté de quatre ou de huit voies USB, qui sont prévues pour la connexion de modems, de dispositifs de stockage, d'adaptateurs réseau, de concentrateurs USB et de consoles USB. Certains modèles possèdent un emplacement pour carte SD, qui permet de prendre en charge un dispositif de stockage supplémentaire.

Deux voies réseau permettent de connecter plusieurs réseaux. Il est également possible de les configurer pour la liaison Ethernet à des fins de redondance et de meilleure fiabilité ou pour la prise en charge du basculement réseau.

Il est possible d'installer un modem interne en option en usine ou d'utiliser un modem externe relié à une voie série ou USB pour bénéficier de l'accès entrant et du rappel sécurisé avec le protocole PPP (Point-to-Point Protocol).

Certains modèles sont équipés d'une antenne pour une connexion cellulaire.

1.1 Caractéristiques et avantages

1.1.1 Options d'accès

Les options locales (voie console analogique) et distantes (IP numérique et accès commuté) suivantes permettent un accès sécurisé :

- Connexion réseau IP LAN/WAN.
- Accès commuté vers un modem interne configuré en usine (en option) ou un modem relié à une voie série ou USB.
- Certains modèles sont équipés d'une antenne pour une connexion cellulaire.
- Connexion de dispositifs cibles. Tout utilisateur autorisé peut établir une connexion Telnet, SSH v2 ou mode brut avec un dispositif cible. Pour pouvoir établir des connexions Telnet ou SSH avec les dispositifs cibles, le service Telnet ou SSH doit être configuré dans le profil de sécurité appliqué.

- Connexion console au système de console. Les administrateurs peuvent se connecter à partir d'un terminal local ou d'un ordinateur équipé d'un émulateur de terminal relié à la voie console et utiliser l'interface de ligne de commande. L'invite de l'interface de ligne de commande (--:-cli->) s'affiche lors de la connexion.

Plusieurs administrateurs peuvent se connecter au système de console et avoir une session CLI ou interface utilisateur Web active. Le message d'avertissement suivant s'affiche pour toutes les sessions lorsqu'un autre administrateur ou le système modifie la configuration : *La configuration du matériel a été modifiée en dehors de votre session*. Lorsque ce message s'affiche, tous les administrateurs doivent vérifier qu'ils ont bien enregistré toutes les modifications apportées lors de leur session.

1.1.2 Interface utilisateur Web (IU Web)

Les utilisateurs et les administrateurs peuvent effectuer la plupart des tâches par le biais de l'interface utilisateur Web (IU Web), à laquelle ils peuvent accéder via HTTP ou HTTPS. L'interface utilisateur Web est compatible avec Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome et Apple Safari sur tout ordinateur pris en charge disposant d'un accès réseau au système de console. La liste des navigateurs clients pris en charge, ainsi que leurs versions, est disponible dans les notes de version.

NOTA : lorsque vous utilisez l'interface utilisateur Web pour accéder au système de console, ne désactivez pas l'affichage des boîtes de dialogues si votre navigateur vous propose de les bloquer, sinon vous risquez également de désactiver certaines fonctionnalités de l'interface utilisateur Web.

1.1.3 Prise en charge IPv4 et IPv6

Le système de console prend en charge les protocoles IPv4 et IPv6 double pile. L'administrateur peut choisir dans l'interface utilisateur Web ou CLI de prendre en charge les adresses IPv4 et IPv6, ou uniquement les adresses IPv4. La liste suivante décrit la prise en charge des adresses IPv6 par le système de console :

- DHCP
- Sessions d'accès entrant et d'accès sortant (liaisons PPP)
- Intégration du logiciel DSView
- Interfaces Ethernet eth0 et eth1
- Pare-feu (table d'adresses IP)
- HTTP/HTTPS
- Noyau Linux
- Authentification à distance : serveurs Radius, TACACS+, LDAP et Kerberos
- SNMP
- Accès SSH et Telnet
- Serveur Syslog

NOTA : IPSec n'est pas pris en charge avec IPv6.

1.1.4 Utilisateurs et groupes flexibles

Il est possible de définir un compte pour chaque utilisateur sur le système de console ou sur un serveur d'authentification. L'administrateur et les utilisateurs racines disposent de comptes par défaut et peuvent tous ajouter et configurer d'autres comptes utilisateurs. Il est possible de restreindre l'accès aux voies en fonction des autorisations qu'un administrateur peut attribuer à des groupes d'utilisateurs personnalisés ou à des utilisateurs individuels. Pour en savoir plus, reportez-vous à la section Comptes utilisateurs et groupes d'utilisateurs à la page 70.

1.1.5 Sécurité

Les profils de sécurité déterminent les services réseaux qui sont activés sur le système de console. Les administrateurs peuvent soit autoriser tous les utilisateurs à accéder aux voies activées, soit permettre la configuration d'autorisations pour des groupes et des utilisateurs spécifiques afin de restreindre l'accès. Vous pouvez également sélectionner un profil de sécurité qui définit les services activés (FTP, TFTP, ICMP, IPSec et Telnet), ainsi que l'accès SSH et HTTP/HTTPS. L'administrateur peut choisir un profil de sécurité préconfiguré ou créer un profil personnalisé. Pour en savoir plus, reportez-vous à la section Sécurité à la page 23.

1.1.6 Authentification

Il est possible de procéder à l'authentification localement, avec un mot de passe à usage unique (OTP), un serveur d'authentification à distance Kerberos, LDAP, RADIUS ou TACACS+, ou un serveur DSView. Le système de console prend également en charge les autorisations de groupes distantes pour les méthodes d'authentification LDAP, RADIUS et TACACS+. Des mécanismes de secours sont en outre disponibles.

Les méthodes d'authentification configurées pour le système de console ou les voies sont utilisées pour l'authentification de tout utilisateur qui tente de se connecter par l'intermédiaire de Telnet, de SSH ou de l'interface utilisateur Web. Pour en savoir plus, reportez-vous à la section Authentification à la page 67.

1.1.7 VPN basé sur IPSec avec traversée NAT

Si IPSec est activé dans le profil de sécurité sélectionné, les administrateurs peuvent utiliser la fonction VPN pour activer les connexions sécurisées. Pour en savoir plus, reportez-vous à la section IPSec (VPN) à la page 33.

1.1.8 Filtrage des paquets

Les administrateurs peuvent configurer un système de console pour filtrer des paquets de la même manière qu'un pare-feu. Le filtrage des paquets est contrôlé par des chaînes, autrement dit des profils identifiés avec des règles définies par l'utilisateur. Le tableau de filtrage du système de console intègre un certain nombre de chaînes qu'il est possible de modifier, mais pas de supprimer. Les administrateurs peuvent également créer et configurer de nouvelles chaînes.

1.1.9 SNMP

Si SNMP est activé dans le profil de sécurité sélectionné, les administrateurs peuvent configurer l'agent SNMP (Simple Network Management Protocol) sur le système de console pour répondre aux requêtes envoyées par une application de gestion SNMP.

L'agent SNMP du système de console prend en charge SNMP v1/v2 et v3, MIB-II et Enterprise MIB. Pour en savoir plus, reportez-vous à la section Configuration SNMP à la page 40.

NOTA : les fichiers texte d'Enterprise MIB (ACS8000-MIB.asn) et de TRAP MIB (ACS8000-TRAP-MIB.asn) sont disponibles dans le répertoire /usr/local/mibs du matériel.

1.1.10 Consignation des données, notifications, alarmes et mise en mémoire tampon des données

Les administrateurs peuvent configurer la consignation des données, les notifications et les alarmes pour avertir les autres administrateurs de tout problème en leur envoyant une notification par e-mail, SMS, interruption SNMP ou via le logiciel DSView. Les administrateurs peuvent également stocker les données mises en mémoire tampon localement, à distance ou à l'aide de la plate-forme d'administration logicielle DSView. Il est en outre possible d'envoyer des messages concernant le système de console et les serveurs ou dispositifs reliés vers les serveurs syslog.

1.1.11 Gestion de l'alimentation

Le système de console permet aux utilisateurs qui sont autorisés à gérer l'alimentation de mettre sous tension, de mettre hors tension et de réinitialiser les dispositifs reliés à une rampe d'alimentation électrique (PDU) connectée. Il est possible de relier les dispositifs d'alimentation à n'importe quelle voie série. Les utilisateurs autorisés peuvent surveiller et contrôler un système d'alimentation sans coupure (UPS) relié. Pour en savoir plus, reportez-vous à la section Gestion de l'alimentation à la page 81.

1.1.12 Détection automatique

Les administrateurs peuvent activer la détection automatique pour découvrir le nom d'hôte de toute cible reliée à une voie série. La plage des chaînes de demande et de réponse par défaut de la détection automatique est large. Les administrateurs peuvent configurer des chaînes spécifiques pour chaque site. Ils peuvent également configurer la détection automatique via le logiciel DSView.

1.1.13 Module FIPS

FIPS 140 (Federal Information Processing Standards) est un ensemble de normes de sécurité informatique, établies par le gouvernement des États-Unis, qui fixent les exigences concernant les modules cryptographiques.

Le système de console intègre un module cryptographique basé sur un module cryptographique conforme aux normes FIPS 140-2 (numéro de certificat 1747) exécuté sur une plate-forme Linux ARM. Pour en savoir plus, reportez-vous à la section Module FIPS à la page 24.

1.2 Exemples de configuration

La figure et le tableau suivants illustrent la configuration d'un système de console avancé Avocent® ACS 800/8000 avec toutes les options possibles. Les options varient en fonction du modèle. Aucun modèle ne dispose de toutes les options illustrées.

Figure 1.1 Configuration du système de console avancé ACS 8000 avec toutes les options illustrées

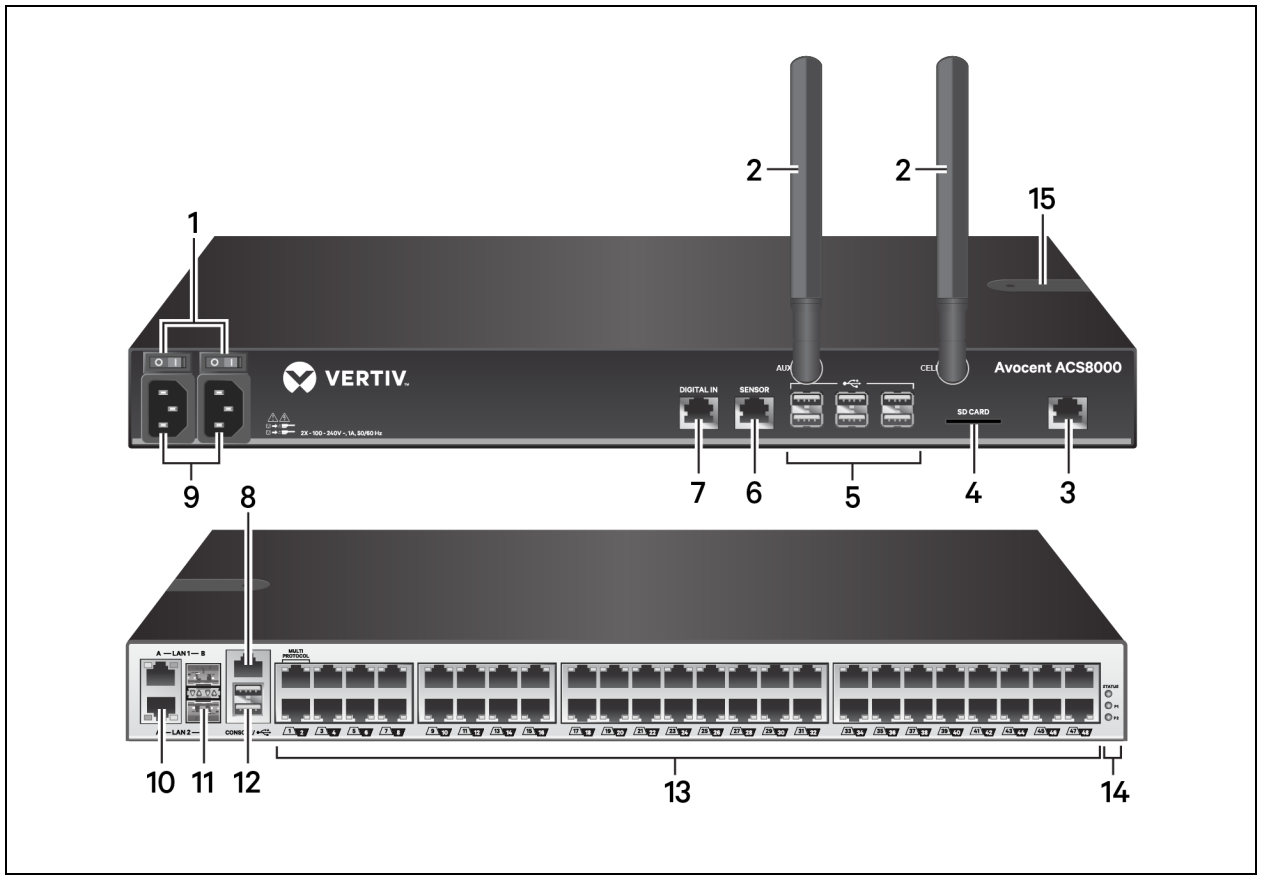


Tableau 1.1 Description de la configuration du système de console avancé ACS 8000

Numéro	Description
1	Boutons d'alimentation (alimentation double illustrée).
2	Antennes cellulaires pour le modem cellulaire (sur certains modèles uniquement).
3	Voie modem permettant de relier une ligne téléphonique au modem interne.
4	Emplacement pour carte SD (sur certains modèles uniquement).
5	Voies USB pour les dispositifs USB pris en charge (sur certains modèles uniquement).
6	Voie destinée au capteur environnemental à un fil (sur certains modèles uniquement).
7	Voie d'entrée numérique destinée aux capteurs de fumée, de fuite, de pression ou à contact sec (sur certains modèles uniquement).
8	Voie console pour la connexion d'un terminal ou d'un poste de travail. La configuration du système de console se fait à l'aide d'un terminal ou d'un émulateur de terminal avec les paramètres de session suivants : 9600, 8, N et 1, sans contrôle du flux.
9	Alimentation (alimentation double illustrée).
10/11	Voies LAN. Les voies de gauche sont prévues pour la connexion d'interfaces cuivre. Les voies de droite sont prévues pour la connexion d'interfaces fibre. Vous pouvez utiliser une voie réseau ou les deux à des fins de redondance, toutefois une seule voie LAN1 et une seule voie LAN2 peuvent être utilisées simultanément. Si vous reliez des dispositifs aux deux voies LAN1 ou LAN2, c'est la connexion fibre qui est prioritaire.
12	Deux voies USB à l'arrière du système de console permettant de relier des dispositifs USB supplémentaires.
13	Voies série. Utilisez des câbles CAT 5e ou CAT 6, ainsi que des adaptateurs console DB9 ou DB25, pour relier les dispositifs série et d'alimentation appropriés aux voies série du système de console.
14	Voyants d'état.
15	Emplacement pour carte SIM.

La figure et le tableau suivants illustrent les voies multiprotocole et les voyants.

Figure 1.2 Voies multiprotocole et voyants du système de console avancé Avocent® ACS 8000

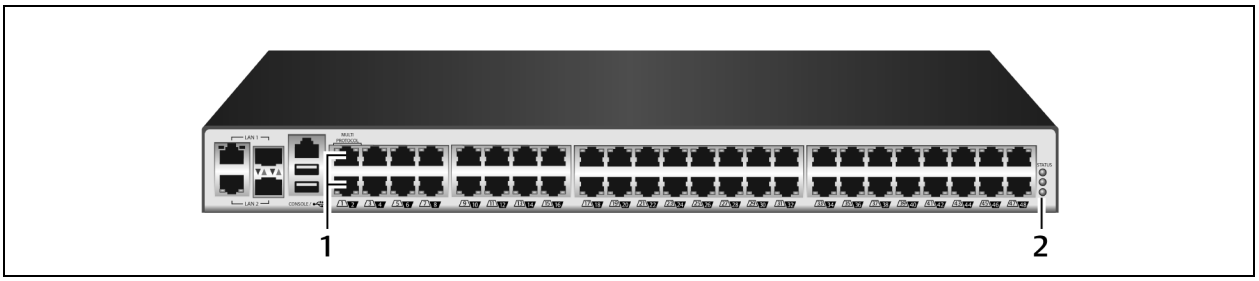


Tableau 1.2 Descriptions des voies multiprotocole et des voyants

Numéro	Description
1	Voies multiprotocole. Ces deux voies peuvent prendre en charge les connecteurs RS422 et RS485, en plus des connecteurs Cyclades et Cisco.
2	Voyants. Le voyant d'état est vert lorsque le système de console a été entièrement démarré et initialisé. Les voyants P1 et P2 indiquent que l'unité est sous tension. Le voyant P1 est vert lorsque l'alimentation 1 est sous tension. Le voyant P2 est vert lorsque l'alimentation 2 est sous tension.

Figure 1.3 Insertion d'une carte SIM

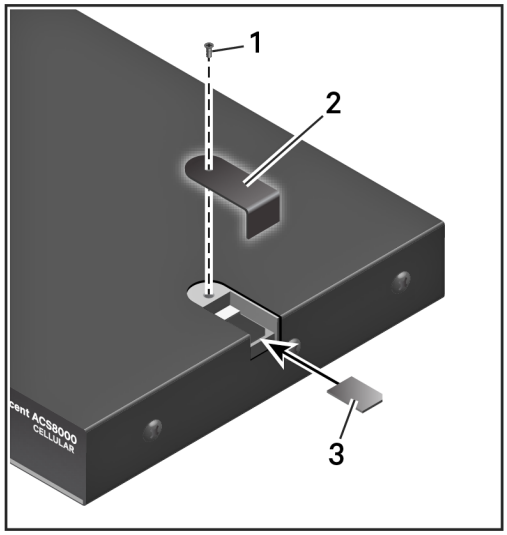


Tableau 1.3 Description de la procédure d'insertion de la carte SIM

élément	Description
1	Retirez la vis du couvercle. Une fois la carte insérée, remettez le couvercle et la vis en place.
2	Retirez le couvercle pour accéder à l'emplacement pour la carte SIM. Remettez le couvercle en place une fois la carte insérée.
3	Insérez la carte.

Figure 1.4 Configuration typique du système de console avancé ACS 800

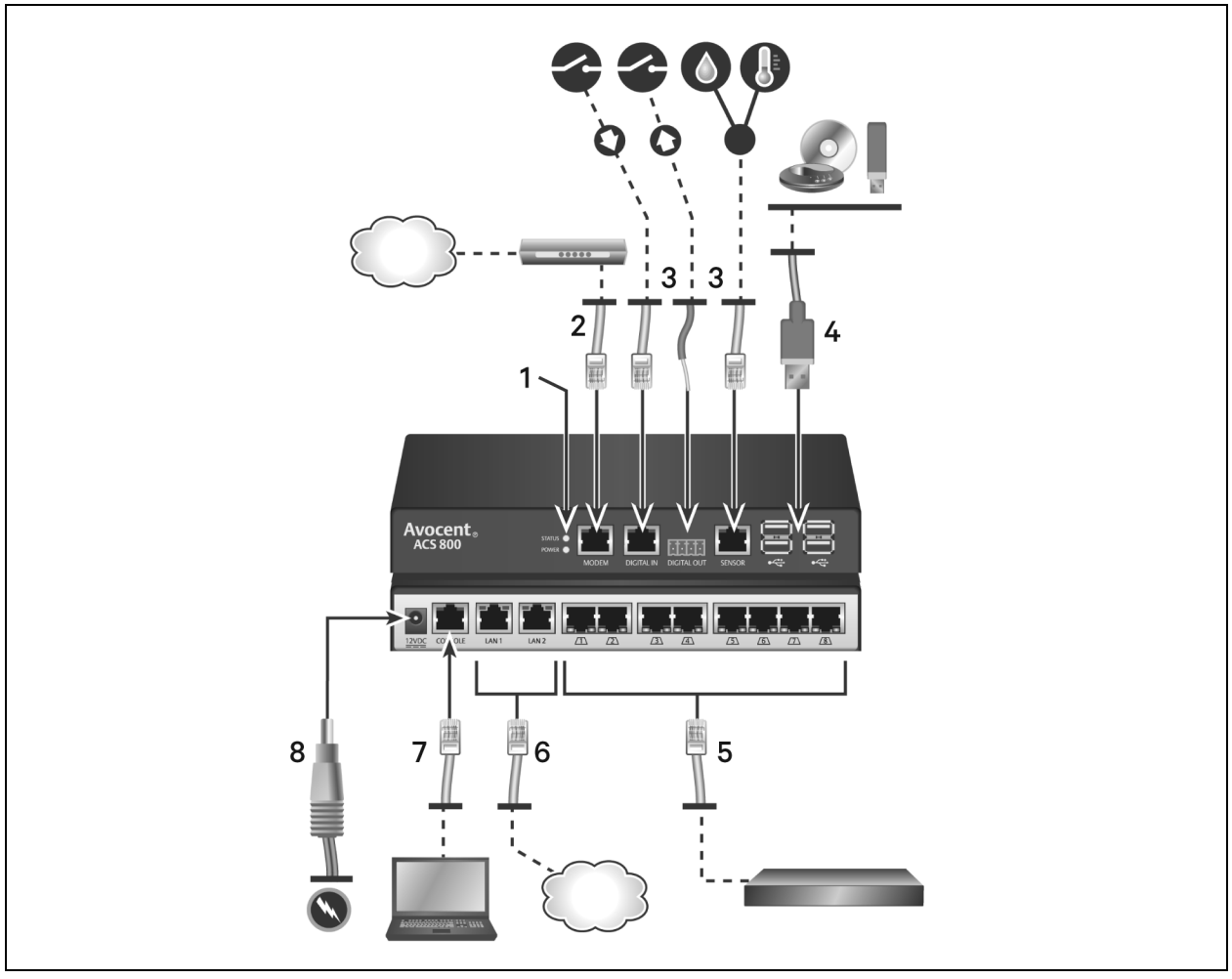


Tableau 1.4 Description de la configuration typique du système de console avancé ACS 800

Numéro	Description
1	Voyants. Le voyant d'état est vert lorsque le système de console a été entièrement démarré et initialisé. Le voyant d'alimentation est vert lorsque le système de console est sous tension.
2	Voie modem permettant de relier une ligne téléphonique au modem interne.
3	Voies destinées aux capteurs environnementaux, de fumée, de fuite, de pression ou à contact sec à un fil.
4	Voies USB pour les dispositifs USB pris en charge.
5	Voies série. Utilisez des câbles CAT 5e ou CAT 6, ainsi que des adaptateurs console DB9 ou DB25, pour relier les dispositifs série et d'alimentation appropriés aux voies série du système de console. Toutes les voies série sont multiprotocole et peuvent être sélectionnées par l'utilisateur, avec des connecteurs RS485, RS422 et RS232.
6	Voies LAN cuivre. Vous pouvez utiliser une voie réseau ou les deux à des fins de redondance.
7	Voie console.
8	Alimentation.

1.2.1 Statut des voyants des voies série

Chaque voie série possède deux voyants qui sont verts ou jaunes. Les voyants verts indiquent une connexion physique à une voie série, une connexion distante (le cas échéant) ou un transfert de données. Les voyants jaunes indiquent qu'une voie série est surveillée, ainsi que le niveau d'alerte (urgence, alerte ou aucun) d'une cible surveillée. Le tableau suivant donne la signification de l'état de chaque voyant.

Tableau 1.5 Description des voyants

État	Description des voyants verts	Description des voyants jaunes
Éteint	Pas de connexion physique.	Pas de mise en mémoire tampon des données.
Allumé (vert ou jaune fixe)	Le dispositif est physiquement relié à la voie série.	La mise en mémoire tampon des données est activée pour la voie série.
Clignotement lent	Une session Telnet, SSH ou mode brut est active.	Une alerte est active.
Clignotement rapide	Transmission ou réception des données.	Urgence.

Page laissée vierge intentionnellement.

2 Avant de commencer

2.1 Installation

Pour obtenir des informations sur l'installation du système de console, reportez-vous au guide d'installation rapide de l'ACS 800 ou de l'ACS 8000 fourni avec votre produit.

2.2 Mise sous tension du système de console

En fonction du modèle, le système de console est fourni avec une alimentation c.a. ou c.c. simple ou double.

AVERTISSEMENT ! Exécutez toujours la commande d'arrêt dans l'interface utilisateur Web, l'interface CLI ou le logiciel DSView, sous le nœud Vue d'ensemble/Outils avant de mettre le système de console hors tension, puis de nouveau sous tension. Cette procédure vous permet d'éviter toute réinitialisation pendant l'accès au système de fichiers dans la mémoire flash et toute corruption de la mémoire flash.

2.2.1 Alimentation c.a.

Pour mettre un système de console avec alimentation c.a. sous tension :

1. Assurez-vous que le système de console est hors tension.
2. Branchez le câble d'alimentation sur le système de console et sur une source d'alimentation.
3. Mettez le système de console sous tension.
4. Placez les interrupteurs d'alimentation des dispositifs reliés en position marche.

2.2.2 Alimentation c.c.

Sur un système de console avec alimentation c.c., cette dernière doit être reliée par le biais de trois fils : retour (RTN), masse (GND) et -48 V c.c. Pour assurer la redondance, deux jeux de fils peuvent être reliés à deux sources d'alimentation distinctes.

AVERTISSEMENT ! Il est essentiel que la source d'alimentation fournisse l'alimentation c.c. nécessaire pour votre système de console. Avant de continuer, assurez-vous que la source d'alimentation est du type approprié et que vos câbles d'alimentation c.c. sont en bon état, sinon vous risquez de vous blesser ou d'endommager l'équipement.

La figure suivante illustre la configuration des connecteurs pour l'alimentation c.c.

NOTA : l'alimentation c.c. est disponible uniquement sur le système de console ACS 8000.

Figure 2.1 Bloc de raccordement de l'alimentation c.c.

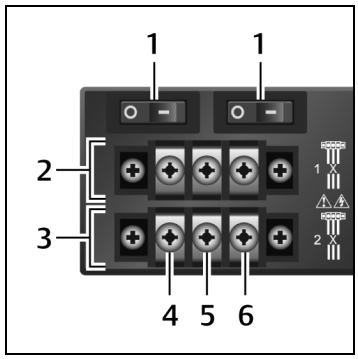


Tableau 2.1 Description de la connexion de l'alimentation c.c.

Numéro	Description	Numéro	Description
1	Interrupteur d'alimentation, un pour chaque source d'alimentation	4	RTN (retour)
2	Connexions pour la première source d'alimentation	5	GND (masse)
3	Connexions pour la seconde source d'alimentation	6	-48 V c.c.

Pour mettre un système de console avec alimentation c.c. sous tension :

1. Assurez-vous que le système de console est hors tension.
2. Assurez-vous que les câbles d'alimentation c.c. ne sont pas reliés à une source d'alimentation.
3. Retirez le couvercle de protection du bloc d'alimentation c.c. en le glissant vers la gauche ou la droite.
4. Desserrez les trois vis du bloc de raccordement de l'alimentation c.c.
5. Branchez le fil de retour sur la borne RTN, le fil de terre sur la borne GND et le fil -48 V c.c. sur la borne -48 V c.c., puis serrez les vis.
6. Replacez le couvercle de protection sur le bloc de raccordement de l'alimentation c.c.
7. Si votre système de console est équipé de deux jeux de bornes c.c., répétez les étapes 3 à 6 pour la seconde alimentation.
8. Branchez les câbles d'alimentation c.c. sur la source d'alimentation c.c. et mettez cette dernière sous tension.
9. Mettez le système de console sous tension.
10. Placez les interrupteurs d'alimentation des dispositifs reliés en position marche.

2.3 Configuration du système de console

Il est possible de configurer le système de console au niveau du matériel en utilisant l'interface de ligne de commande à laquelle vous pouvez accéder par la voie CONSOLE ou Ethernet. Vous pouvez accéder à toutes les commandes de terminal en utilisant un terminal ou un ordinateur exécutant un logiciel d'émulation de terminal.

NOTA : pour configurer le système de console à l'aide du logiciel DSView, reportez-vous au guide d'installation et d'utilisation de la plate-forme d'administration logicielle Avocent® DSView 4.5. Pour configurer le système de console à l'aide de l'interface utilisateur Web, reportez-vous à la section Présentation de l'interface utilisateur Web pour les administrateurs à la page 18. Pour configurer le système de console en utilisant Telnet ou SSH, reportez-vous au guide de référence des commandes du système de console avancé Avocent® ACS 800/8000.

Pour connecter un terminal au système de console :

1. À l'aide d'un câble null modem, connectez un terminal ou un ordinateur exécutant un logiciel d'émulation de terminal (comme HyperTerminal) à la voie CONSOLE située à l'arrière du système de console. Un adaptateur croisé RJ45-DB9 (femelle) est fourni.

   Les paramètres du terminal sont 9 600 bits par seconde (bit/s), 8 bits, 1 bit d'arrêt, sans parité et sans contrôle du flux.

2. Mettez le système de console sous tension. Une fois le système de console initialisé, le terminal affiche la bannière et l'invite de connexion.

2.3.1 Utilisation de Telnet ou de SSH

Les utilisateurs autorisés peuvent utiliser un client Telnet ou SSH pour se connecter directement à la console d'un dispositif si toutes les conditions suivantes sont remplies :

Telnet ou SSH :

- Le protocole est activé dans le profil de sécurité sélectionné.
- Le client est disponible et il est activé sur l'ordinateur utilisé pour la connexion.

Pour se connecter à un dispositif à l'aide de Telnet via une voie série :

Pour cette procédure, vous avez besoin du nom d'utilisateur configuré pour l'accès à la voie série, du nom de la voie (par exemple, 14-35-60-p-1), du nom du dispositif (par exemple, ttyS1), de l'alias TCP de la voie (par exemple, 7001) ou de l'alias IP de la voie (par exemple, 100.0.0.100) et du nom d'hôte du système de console ou de son adresse IP.

Pour utiliser un client Telnet, saisissez ces informations dans les boîtes de dialogue du client.

-ou-

Pour utiliser Telnet dans un shell, saisissez les commandes suivantes :

```
#telnet [nom d'hôte | adresse IP]
login: nom d'utilisateur:[nom de la voie | nom du dispositif | alias TCP de la voie]
-ou-
#telnet [nom d'hôte | adresse IP] alias TCP de la voie
login: nom d'utilisateur
-ou-
#telnet alias IP de la voie
login: nom d'utilisateur
```

Pour fermer une session Telnet :

Utilisez le raccourci clavier Telnet défini pour le client. Le raccourci clavier par défaut pour fermer une session est Ctrl] + q.

-ou-

Saisissez le raccourci texte de la session dans l'invite CLI, puis exit.

Pour se connecter à un dispositif à l'aide de SSH via une voie série :

Pour cette procédure, vous avez besoin du nom d'utilisateur configuré pour l'accès à la voie série, du nom de la voie (par exemple, 14-35-60-p-1), de l'alias TCP de la voie (par exemple, 7001), du nom du dispositif (par exemple, ttyS1) et du nom d'hôte du système de console, de son adresse IP ou de l'alias IP de la voie (par exemple, 100.0.0.100).

Pour utiliser un client SSH :

Saisissez ces informations dans les boîtes de dialogue du client.

-ou-

Pour utiliser SSH dans un shell, saisissez la commande suivante :

```
ssh -l  nom_d'utilisateur : nom_de_la_voie  [nom_d'hôte | adresse_IP]
-ou-
ssh -l nom_d'utilisateur:nom_du_dispositif [nom_d'hôte | adresse_IP]
-ou-
ssh -l nom_d'utilisateur:alias_TCP_voie [nom_d'hôte | adresse_IP]
-ou-
ssh -l nom_d'utilisateur alias_IP_voie
```

Pour fermer une session SSH :

Au début d'une ligne, saisissez le raccourci clavier défini pour le client SSH, suivi d'un point. Le raccourci par défaut est **~**.

-ou-

Saisissez le raccourci texte de la session dans l'invite CLI, puis **exit**.

3 Accès au système de console via l'interface utilisateur Web

Après avoir connecté votre système de console avancé Avocent® ACS 800/8000 à un réseau, vous pouvez y accéder via son interface utilisateur Web. Cette dernière vous permet d'accéder directement au système de console par le biais d'une interface utilisateur graphique au lieu d'une interface à commande.

NOTA : si vous utilisez un système de console neuf avec les paramètres par défaut, LAN1 tente d'obtenir une adresse IP en utilisant DHCP, tandis que LAN2 utilise l'adresse IP statique 192.168.161.10. Utilisez LAN2 pour la configuration initiale ou la voie console pour la détection de l'adresse IPv4 attribuée à LAN1 par DHCP.

NOTA : pour savoir comment accéder au système de console via l'interface CLI ou le logiciel DSView, reportez-vous au guide de référence des commandes du système de console avancé Avocent® ACS 800/8000 ou au guide d'installation et d'utilisation de la plate-forme d'administration logicielle Avocent® DSView 4.5.

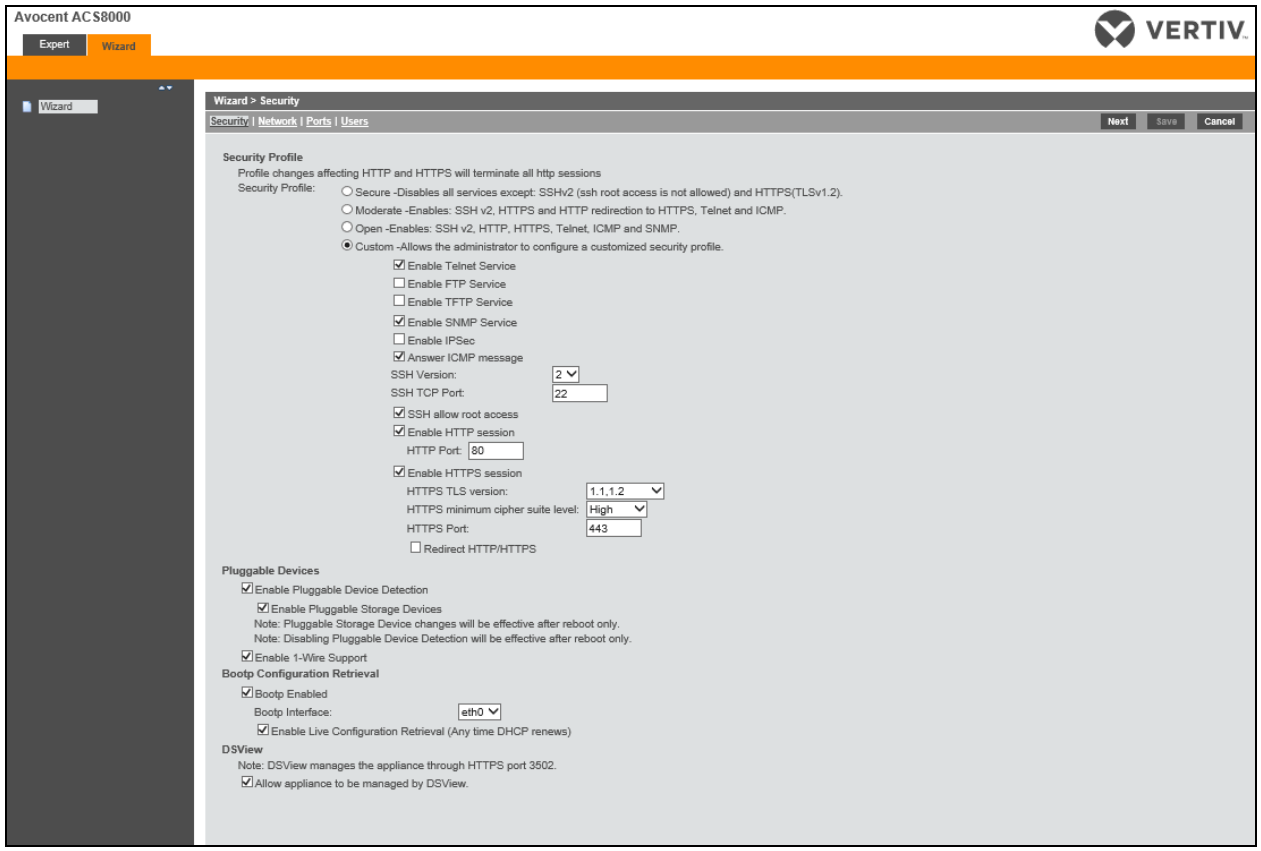
3.1 Mode Assistant

Le mode Assistant est conçu pour faciliter les procédures d'installation et de configuration en guidant l'administrateur lors des différentes étapes. Il lui permet de configurer toutes les voies d'un profil CAS et de définir le profil de sécurité, ainsi que les paramètres utilisateur et réseau.

L'assistant s'affiche par défaut lorsqu'un administrateur accède pour la première fois au système de console via l'interface utilisateur Web. Toutes les connexions ultérieures s'ouvrent en mode Expert. Une fois le système de console configuré, le mode Expert devient le mode par défaut. Les administrateurs peuvent passer du mode Expert au mode Assistant et vice-versa. Pour ce faire, il leur suffit de cliquer sur l'onglet correspondant sur l'écran de l'interface utilisateur Web.

Les images suivantes illustrent l'écran standard qui s'affiche en mode Assistant.

Figure 3.1 Écran Assistant



Les procédures suivantes expliquent comment configurer le système de console à l'aide de l'assistant.

Pour configurer les paramètres de sécurité et sélectionner un profil de sécurité :

1. Cliquez sur le lien *Sécurisé* dans la zone de contenu.
2. Sélectionnez le profil de sécurité souhaité. Si vous choisissez un profil de sécurité personnalisé, cochez les cases correspondantes et indiquez les valeurs requises pour configurer les services, ainsi que les options SSH, HTTP et HTTPS conformément à la politique de sécurité de votre site.
3. Les dispositifs enfichables, y compris ceux qui sont reliés à l'emplacement pour carte SD et aux voies USB, sont désactivés par défaut. Pour les activer, cochez la case Activer la détection des dispositifs enfichables. Les dispositifs de stockage (carte SD et dispositifs USB) sont alors activés par défaut. Pour les désactiver, décochez la case Activer les dispositifs de stockage enfichables. Les dispositifs enfichables incluent également la voie de capteur à 1 fil, activée par défaut. Pour la désactiver, décochez la case Activer prise en charge capteur 1 fil.

NOTA : ces options sont disponibles pour tous les modèles de système de console, même ceux qui ne disposent pas d'emplacement pour carte SD ou de voie destinée au capteur à 1 fil. Si c'est le cas de votre modèle, laissez ces options désactivées.

4. Dans la section Récupération de la configuration Bootp, décochez les cases pour désactiver la récupération de la configuration Bootp et/ou la récupération instantanée de la configuration.
5. Si vous n'utilisez pas le logiciel DSView pour gérer le matériel, décochez la case *Autoriser la gestion du matériel par DSView*.

6. Cliquez sur *Suivant* pour configurer le réseau ou sur le lien *Réseau*, *Voies* ou *Utilisateurs* pour afficher l'écran correspondant.

Pour configurer les paramètres réseau :

1. Cliquez sur le lien *Réseau* dans la zone de contenu.
2. Renseignez les champs correspondant au nom d'hôte, au DNS principal et au domaine.
3. Sélectionnez la méthode IPv4 ou IPv6 pour l'interface eth0. Si vous sélectionnez Statique, saisissez l'adresse, le masque et la passerelle dans les champs appropriés.
4. Activez ou désactivez LLDP (Link Layer Discovery Protocol).
5. Activez ou désactivez la prise en charge d'IPv6.
6. Cliquez sur *Suivant* pour configurer les voies ou sur le lien *Sécurisé*, *Voies* ou *Utilisateurs* pour afficher l'écran correspondant.

Pour configurer les voies :

1. Cliquez sur le lien *Voies* dans la zone de contenu.
2. Cochez la case Activer toutes les voies.
3. Sélectionnez les valeurs souhaitées dans les menus déroulants Connecteur RJ45, Vitesse, Parité, Bits de données, Bits d'arrêt, Contrôle du flux, Protocole, Type d'authentification, Statut de mise en mémoire tampon des données et Horodatage de mise en mémoire tampon des données.
4. Sélectionnez le type de mise en mémoire tampon des données. Si vous utilisez NFS, renseignez les champs Serveur NFS et Chemin NFS.
5. Cliquez sur *Suivant* pour configurer les utilisateurs ou sur le lien *Réseau*, *Sécurisé* ou *Utilisateurs* pour afficher l'écran correspondant.

Pour configurer les utilisateurs et modifier les mots de passe :

1. Cliquez sur le lien *Utilisateurs* dans la zone de contenu.
2. Cliquez sur un nom d'utilisateur (*admin* ou *root*), puis saisissez le nouveau mot de passe et confirmez-le.

   -ou-

3. Cliquez sur *Ajouter* pour ajouter un utilisateur. Saisissez les nouveaux nom d'utilisateur et mot de passe dans les champs appropriés.
4. (Facultatif) Pour inciter l'utilisateur à modifier le mot de passe lors de la prochaine connexion, cochez la case *L'utilisateur doit modifier le mot de passe à la prochaine connexion*.
5. Ajoutez l'utilisateur à un ou plusieurs groupes.
6. (Facultatif) Configurez l'expiration du compte et du mot de passe.
7. Cliquez sur *Suivant*.
8. Répétez les étapes 3 à 7 pour configurer tous les nouveaux comptes utilisateur et les ajouter aux groupes par défaut.

NOTA : par défaut, tous les utilisateurs configurés peuvent accéder à toutes les voies activées. Une configuration supplémentaire est nécessaire pour restreindre l'accès des utilisateurs aux voies si la politique de sécurité de votre site l'exige.

9. Cliquez sur *Enregistrer*, puis sur *Terminer*.

3.2 Présentation de l'interface utilisateur Web pour les administrateurs

NOTA : pour la présentation de l'interface utilisateur Web pour les utilisateurs, reportez-vous à la section Présentation de l'interface utilisateur Web pour les utilisateurs à la page 90.

Pour vous connecter à l'interface utilisateur Web :

1. Ouvrez un navigateur Web et saisissez l'adresse IP du système de console dans la barre d'adresse.
2. Connectez-vous à l'aide de votre nom d'utilisateur et de votre mot de passe. Le nom d'utilisateur par défaut est **admin**. Lors de la première connexion en tant qu'utilisateur admin, laissez le champ du mot de passe vide. Vous êtes alors invité à créer un nouveau mot de passe.

NOTA : l'utilisateur racine est désactivé par défaut. L'administrateur peut activer l'utilisateur racine sur la page Utilisateurs - Comptes locaux - Noms d'utilisateur.

Les images suivantes illustrent l'écran standard de l'interface utilisateur Web pour les administrateurs.

Figure 3.2 Écran de l'interface utilisateur Web pour les administrateurs

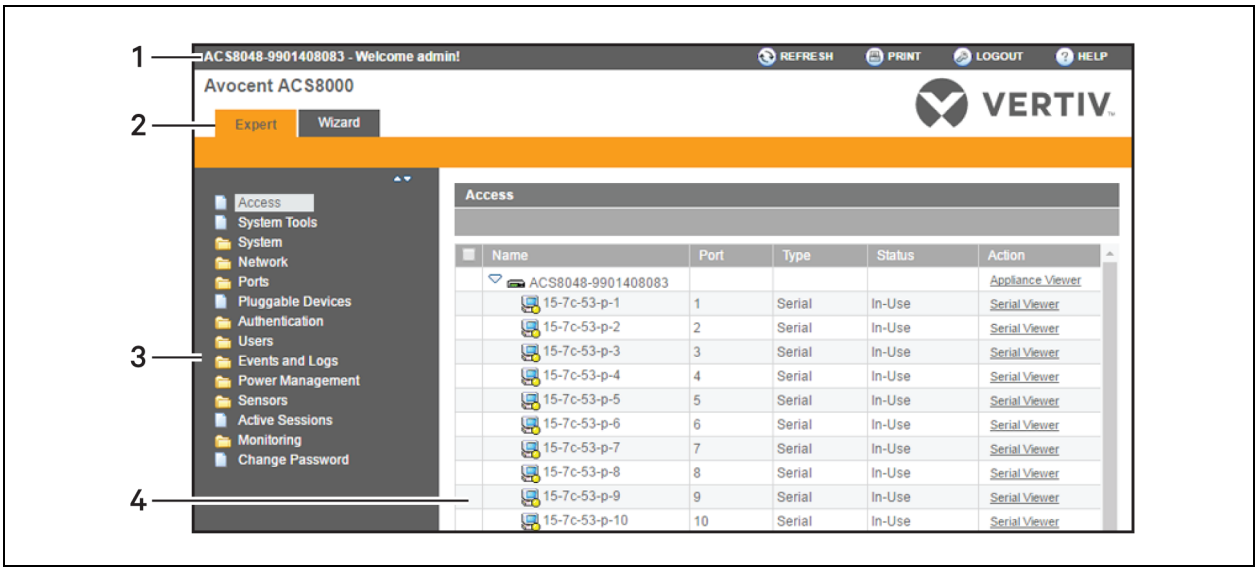


Tableau 3.1 Zones de l'interface utilisateur Web

Numéro	Description
1	Barre d'options supérieure. Les noms du matériel et de l'utilisateur connecté s'affichent à gauche. Les boutons Actualiser, Imprimer, Déconnexion et Aide sont disponibles à droite.
2	Barre d'onglets. Indique si l'administrateur est en mode Expert ou Assistant.
3	Barre de navigation latérale. Comporte les options de configuration, d'affichage des informations du système et d'accès aux dispositifs. Les options disponibles varient en fonction des droits de l'utilisateur.
4	Zone de contenu. Le contenu varie en fonction des options sélectionnées dans la barre de navigation latérale.

3.3 Mode expert

Les onglets suivants sont disponibles dans la barre de navigation latérale de l'interface utilisateur Web lorsqu'un administrateur est connecté en mode expert.

3.3.1 Accès

Cliquez sur Accès pour afficher tous les dispositifs reliés au système de console.

Pour afficher les dispositifs et s'y connecter via l'interface utilisateur Web :

1. Sélectionnez *Accès* dans la barre de navigation latérale. La zone de contenu affiche le nom du système de console, ainsi que la liste des noms et des alias de tous les dispositifs installés et configurés auxquels l'utilisateur a le droit d'accéder.
2. Sélectionnez *Visualiseur série* dans la colonne Action pour ouvrir une connexion sur la voie série choisie.

   -ou-

   Sélectionnez *Visualiseur du matériel* dans la colonne Action pour ouvrir une connexion au système de console.

NOTA : le visualiseur HTML5 s'ouvre par défaut. Toutefois, si l'administrateur a sélectionné le visualiseur JNLP, le visualiseur de l'applet Java s'affiche.

3. Si vous n'utilisez pas la connexion automatique, saisissez les informations de connexion lorsque vous y êtes invité.

3.3.2 Outils système

Cliquez sur *Outils système* pour afficher les icônes qui vous permettent de redémarrer ou d'éteindre le système de console, de mettre le firmware du système de console à niveau, d'enregistrer ou de restaurer la configuration ou d'ouvrir une session terminal avec le système de console.

Mise à niveau du firmware

Le système de console permet de stocker deux images de firmware. Lorsque vous mettez le firmware à niveau, l'image qui n'est pas active est remplacée par le nouveau firmware. Il est possible de télécharger la dernière version du firmware sur le site Web de Vertiv. Le système de console peut ensuite y accéder via un serveur FTP (File Transfer Protocol), SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol). Il est également possible de télécharger le firmware via le navigateur Web à partir de l'ordinateur local de l'utilisateur.

Pour connaître la version actuelle du firmware du système de console, cliquez sur *Système - Informations* dans la barre de navigation latérale de l'onglet Expert.

Pour mettre le firmware du système de console à niveau :

1. Rendez-vous sur le site http://www.VertivCo.com et recherchez le firmware correspondant à votre système de console dans la section des mises à jour de produits.
2. Enregistrez le nouveau firmware sur votre ordinateur ou sur un serveur accessible par FTP, SFTP ou SCP.
3. Dans la barre de navigation latérale de l'interface utilisateur Web du système de console, cliquez sur *Outils système*, puis sur *Mettre le firmware à niveau*.
4. Téléchargez le fichier à partir du serveur que vous avez sélectionné à l'étape 2.
    a. Sélectionnez le bouton radio Serveur distant, puis choisissez dans le menu déroulant le protocole du serveur sur lequel vous avez enregistré le fichier.
    b. Dans le champ correspondant, saisissez l'adresse IP du serveur sur lequel le firmware est enregistré.
    c. Saisissez le nom d'utilisateur et le mot de passe pour le serveur dans les champs appropriés.
    d. Indiquez le répertoire dans lequel le firmware est enregistré, ainsi que le nom du fichier.

    -ou-

    Téléchargez le fichier sur votre ordinateur en sélectionnant *Mon ordinateur*.

    a. Saisissez le nom du fichier du nouveau firmware ou cliquez sur *Parcourir* pour rechercher le fichier dans une nouvelle fenêtre.
5. Cliquez sur *Télécharger*. Le système de console télécharge le firmware à partir de l'emplacement indiqué et affiche un message une fois le téléchargement terminé.
6. Cliquez sur *Installer*.
7. Une fois le nouveau firmware installé, redémarrez le système de console.

Fichiers de configuration

Les administrateurs peuvent créer une image de sauvegarde de la configuration du système de console. Aucune modification ne doit être apportée à la configuration pendant la création de l'image. Il est possible de charger le fichier de configuration de sauvegarde sur un serveur distant, de le stocker en tant que fichier local sur le système de console ou de l'enregistrer sur l'ordinateur de l'utilisateur Web. Les fichiers de configuration peuvent être enregistrés en tant que fichiers compressés, scripts CLI ou fichiers XML.

Pour enregistrer le fichier de configuration actuel :

1. Dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Outils système*.
2. Cliquez sur *Enregistrer la configuration*.

3. Sélectionnez le format de fichier dans le menu déroulant.
4. Chargez le fichier sur un serveur distant.
    a. Sélectionnez le bouton radio Serveur distant, puis choisissez dans le menu déroulant le protocole du serveur sur lequel vous souhaitez enregistrer le fichier.
    b. Saisissez, dans le champ correspondant, l'adresse IP du serveur sur lequel le fichier doit être enregistré.
    c. Saisissez le nom d'utilisateur et le mot de passe pour le serveur dans les champs appropriés.
    d. Indiquez le répertoire dans lequel le fichier de configuration est enregistré, ainsi que le nom du fichier.

    -ou-

    Enregistrez le fichier localement en sélectionnant le bouton radio Fichier local et en indiquant le nom du fichier.

NOTA : le nom du fichier peut contenir le chemin complet de l'emplacement où il doit être enregistré. Si vous indiquez le chemin complet, vous pouvez enregistrer le fichier sur un dispositif de stockage USB monté, par exemple /media/sda1/nomdefichier. Sinon, le fichier est enregistré dans /mnt/hdUser/backup/<nomdefichier>.

    -ou-

    Enregistrez le fichier sur votre ordinateur en sélectionnant le bouton radio Mon ordinateur. Le fichier est alors enregistré dans votre dossier des téléchargements.

5. Cliquez sur *Enregistrer*.

Pour restaurer une configuration précédente :

1. Dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Outils système*.
2. Cliquez sur *Restaurer la configuration*.
3. Restaurez le fichier à partir d'un serveur distant.
    a. Sélectionnez le bouton radio Serveur distant, puis choisissez dans le menu déroulant le protocole du serveur sur lequel le fichier de configuration est enregistré.
    b. Saisissez, dans le champ correspondant, l'adresse IP du serveur sur lequel le fichier est enregistré.
    c. Saisissez le nom d'utilisateur et le mot de passe pour le serveur dans les champs appropriés.
    d. Indiquez le chemin et le nom du fichier de configuration.

    -ou-

    Procédez à la restauration à partir d'un fichier local en sélectionnant le bouton radio Local et en indiquant le nom du fichier.

    -ou-

    Restaurez le fichier à partir de l'ordinateur en sélectionnant le bouton radio Mon ordinateur, en naviguant jusqu'à l'emplacement du fichier et en cliquant sur *Ouvrir*.

4. Cliquez sur *Restaurer*.

Intégrité de la configuration

Pour garantir l'intégrité de la configuration, le système de console permet aux administrateurs de générer et de vérifier une signature numérique (MD5) de la configuration du système de console. Le système de console compare sa valeur de somme de contrôle MD5 avec une somme de contrôle MD5 connue pour vérifier sa configuration et la protéger de toute corruption.

Les administrateurs peuvent signaler une configuration existante comme étant fiable et indiquer au système de console de générer une balise MD5 pour cette configuration. Ils peuvent également vérifier la configuration en la comparant à une autre configuration connue ou de confiance. Une fois la vérification terminée, le système de console indique si la configuration a été modifiée ou non.

La fonction d'intégrité de la configuration s'appuie sur les fichiers de configuration du système de console enregistrés et restaurés. Elle dépend également de la fonction d'approvisionnement autonome.

NOTA : pour pouvoir utiliser la fonction d'intégrité de la configuration, vous devez enregistrer la configuration en tant que fichier compressé. Ce format capture davantage de données de configuration pour garantir l'exactitude des résultats de l'intégrité de la configuration. Si vous enregistrez la configuration en tant que script CLI ou fichier XML, les résultats de l'intégrité de la configuration ne seront pas valides.

Le système de console envoie une notification d'événement à chaque fois qu'une balise MD5 est générée. Pour en savoir plus sur les différents événements, reportez-vous à la section Liste des événements à la page 79.

Pour générer une balise MD5 :

1. Dans la barre de navigation latérale de l'interface utilisateur Web du système de console, cliquez sur *Outils système*, puis sur *Intégrité de la configuration*.
2. Sélectionnez le bouton radio Générer une balise MD5 pour la configuration actuelle et cliquez sur *Exécuter*.
3. La balise MD5 s'affiche à l'écran sous forme de valeur hexadécimale de 32 caractères. Elle est également enregistrée dans le système de console à des fins de référence. Les administrateurs peuvent couper et coller cette chaîne pour l'utiliser sur d'autres systèmes.

Pour vérifier une balise MD5 :

1. Dans la barre de navigation latérale de l'interface utilisateur Web du système de console, cliquez sur *Outils système*, puis sur *Intégrité de la configuration*.
2. Sélectionnez le bouton radio Vérifier la configuration actuelle.
3. Laissez le champ MD5 vide pour vérifier la configuration actuelle.

   -ou-

   Indiquez une somme de contrôle MD5 pour vérifier une configuration connue.
4. Cliquez sur *Exécuter*.

Certificat HTTPS

Vous pouvez générer un nouveau certificat auto-signé, télécharger sur le matériel un certificat signé existant à partir d'un serveur FTP ou utiliser un certificat qui se trouve sur votre ordinateur.

Pour générer un nouveau certificat auto-signé :

1. Dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Outils système*.

2. Cliquez sur *Générer/Télécharger le certificat*.
3. Pour générer un nouveau certificat, sélectionnez le bouton radio Générer un certificat auto-signé et ajoutez les informations souhaitées dans les champs du certificat auto-signé : Pays, État/Province, Ville/Localité, Organisation, Unité d'organisation, Nom courant, Adresse e-mail et Commentaire Netscape.

   -ou-

   Pour télécharger un certificat signé à partir d'un serveur FTP, SFTP ou SCP, sélectionnez le bouton radio Serveur distant et renseignez tous les champs concernant le serveur FTP : Adresse IP, Nom d'utilisateur, Mot de passe, Répertoire de fichier et Nom de fichier.

   -ou-

   Pour utiliser un certificat qui se trouve sur votre ordinateur, sélectionnez le bouton radio Télécharger le certificat depuis Mon ordinateur, cliquez sur *Choisir le fichier* ou *Parcourir* pour rechercher le fichier, puis cliquez sur *Ouvrir*.
4. Cliquez sur *Générer/Télécharger*. Les informations du certificat s'affichent.
5. Cliquez sur *Appliquer*. Le message suivant s'affiche : *L'application du nouveau certificat entraînera l'arrêt de toutes les sessions HTTP/HTTPS. Votre navigateur va redémarrer. Voulez-vous vraiment continuer ?*
6. Cliquez sur *OK* pour continuer. Le nouveau certificat est enregistré et le navigateur redémarre pour l'utiliser.

NOTA : toutes les sessions http/https se terminent et l'utilisateur doit rétablir la connexion.

3.3.3 Système

La section *Système* affiche les informations concernant le système de console et permet aux administrateurs de configurer les paramètres système. Les onglets suivants sont disponibles dans la section Système de la barre de navigation latérale.

Sécurité

Profil de sécurité

Les profils de sécurité déterminent les services réseau qui sont activés sur le système de console.

Lors de la configuration initiale, l'administrateur du système de console doit configurer les paramètres de sécurité conformément à la politique de sécurité du site. Les fonctions de sécurité suivantes peuvent être configurées dans l'interface utilisateur Web, l'interface CLI ou le logiciel DSView :

- Configuration du délai d'inactivité de la session
- Activation ou désactivation du service RPC
- Activation ou désactivation de la détection des dispositifs enfichables, des dispositifs de stockage et des capteurs à 1 fil
- Possibilité de configurer l'accès à la voie série pour tous les utilisateurs ou de permettre la configuration d'autorisations pour des groupes et utilisateurs spécifiques afin de restreindre l'accès
- Sélection d'un profil de sécurité qui définit :
  - Les services activés (FTP, TFTP, ICMP, IPSec, SNMP et Telnet)

- L'accès SSH et HTTP/HTTPS
- L'activation ou la désactivation de la récupération de la configuration Bootp, de l'interface Bootp et de la récupération instantanée de la configuration

L'administrateur peut choisir un profil de sécurité préconfiguré ou créer un profil personnalisé.

Tous les services et les options de configuration SSH et HTTP/HTTPS activés et désactivés pour chaque profil de sécurité s'affichent sur les pages Assistant - Sécurisé et Système - Sécurisé - Profil de sécurité.

Pour configurer un profil de sécurité :

1. Sélectionnez *Système - Sécurisé - Profil de sécurité*.
2. Dans le champ Délai d'inactivité, indiquez la durée en secondes avant que le système de console ne mette fin aux sessions ouvertes.

NOTA : cette valeur s'applique à toute session utilisateur ouverte sur le matériel via HTTP, HTTPS, SSH, Telnet ou la voie CONSOLE. Elle ne remplace pas la valeur configurée pour le groupe d'autorisation de l'utilisateur. La nouvelle valeur du délai d'inactivité ne s'applique qu'aux nouvelles sessions.

3. Dans la section Services activés, cochez ou décochez la case *RPC*.
4. Dans la section Dispositifs enfichables, activez ou désactivez la détection des dispositifs enfichables pour les dispositifs USB et les cartes SD. Si cette option est activée, il est possible de désactiver les dispositifs USB et les cartes SD afin de limiter le type de dispositifs enfichables pour des raisons de sécurité. Il est également possible de désactiver le capteur à 1 fil dans cette section.

NOTA : ces options sont disponibles pour tous les modèles de système de console, même ceux qui ne disposent pas d'emplacement pour carte SD ou de voie destinée au capteur à 1 fil. Si c'est le cas de votre modèle, laissez ces options désactivées.

NOTA : la désactivation de la détection des dispositifs enfichables ou la modification du paramètre relatif aux dispositifs de stockage ne prend effet qu'après redémarrage.

5. Dans la section Dispositifs série, indiquez si l'accès à la voie est contrôlé par l'utilisateur et l'autorisation de groupe ou si les paramètres d'accès à la voie s'appliquent à tous les utilisateurs.
6. Activez ou désactivez la récupération de la configuration Bootp dans la section correspondante.
7. Activez ou désactivez l'authentification SSH par identification nom d'utilisateur/mot de passe.
8. Dans la section Profil de sécurité, cochez la case *Personnalisé*, *Modéré*, *Ouvert* ou *Sécurisé*.
9. Cliquez sur *Enregistrer*.

Module FIPS

Le système de console intègre un module cryptographique basé sur un module cryptographique conforme aux normes FIPS 140-2 (numéro de certificat 1747) exécuté sur une plate-forme Linux ARM .

Si un administrateur active le module FIPS, le système de console utilise le module d'objet FIPS pour effectuer des opérations de chiffrement. Le module FIPS est désactivé par défaut.

Lorsque le module FIPS est activé, la page Surveillance - Mode FIPS affiche les services (SSHv2, HTTPS, SNMPv3 et ADSAP2) qui sont en mode FIPS. Toutes les fonctions de sécurité et tous les algorithmes cryptographiques utilisés par le service sont effectués en mode approuvé FIPS 140-2.

Pour activer le module FIPS :

1. Sélectionnez *Système - Sécurisé - FIPS 140*.
2. Cochez la case permettant d'activer le module FIPS 140-2 et cliquez sur *Enregistrer*.

Le système de console redémarre automatiquement. Lors du redémarrage, le système de console efface les clés SSH, met à jour la configuration des fichiers HTTPD, SSHD, ADSAP2d et SNMPD et teste l'intégrité du module d'objet FIPS. Une fois le redémarrage terminé, le système de console accepte les connexions SSH et HTTPS en utilisant uniquement le chiffrement approuvé FIPS.

Lorsque le module FIPS est activé, les restrictions suivantes s'appliquent :

Pour les sessions SSH :

- Triple-DES CBS et AES 128/192/256 sont les seuls chiffrements acceptés.
- HMAC-SHA1 et HMAC-SHA1-96 sont les seuls algorithmes d'intégrité des messages acceptés.
- Seules les clés RSA 1 024 à 16 384 sont acceptées.

Les sessions HTTPS acceptent uniquement le protocole SSL v 3.1(TLSv1) pour établir le tunnel SSL avec un des chiffrements suivants :

- AES-256-SHA
- AES-128-SHA
- Triple DES SHA (DES-CBC3-SHA)

Les requêtes de la version 3 de SNMP sont acceptées lorsque l'authentification est SHA et le chiffrement AES.

Sécurité du logiciel DSView

Vous pouvez également configurer les paramètres de sécurité du logiciel DSView. Lorsque le système de console est géré par le logiciel DSView, le serveur DSView fournit le certificat au système de console. En conditions normales, le logiciel DSView gère le certificat et le remplace par un nouveau lorsque cela est nécessaire. En cas de perte de communication avec le logiciel DSView, le serveur DSView ne peut pas effacer le certificat et il est alors impossible d'utiliser le système de console. Cliquez sur le bouton *Effacer le certificat DSView* pour configurer le mode de confiance complète dans le système de console.

Pour configurer les paramètres de sécurité du logiciel DSView :

1. Sélectionnez *Système - Sécurisé - DSView*.
2. Cochez la case *Autoriser la gestion du matériel par DSView* et cliquez sur *Enregistrer*.

Date et heure

Le système de console permet de configurer la date et l'heure de deux manières. Il peut récupérer la date et l'heure à partir du serveur de protocole d'heure réseau (NTP) ou vous pouvez les définir manuellement de sorte que l'horloge interne du système de console fournisse ces informations.

NOTA : l'heure actuelle affichée sur l'écran Date et heure indique uniquement le moment où vous avez ouvert l'écran. Ces informations ne sont pas mises à jour en temps réel.

Pour configurer la date et l'heure avec le protocole NTP :

1. Cliquez sur *Système - Date et heure*.
2. Sélectionnez *Activer le protocole d'heure réseau*.

3. Indiquez le serveur NTP de votre choix et cliquez sur *Enregistrer*.

Pour configurer la date et l'heure manuellement :

1. Cliquez sur *Système - Date et heure*.
2. Sélectionnez *Définir manuellement*.
3. Dans les menus déroulants, sélectionnez la date et l'heure, puis cliquez sur *Enregistrer*.

Pour configurer le fuseau horaire à l'aide d'un fuseau prédéfini :

1. Cliquez sur *Système - Date et heure - Fuseau horaire*.
2. Sélectionnez *Prédéfini*.
3. Sélectionnez le fuseau horaire approprié dans le menu déroulant et cliquez sur *Enregistrer*.

Pour définir des paramètres de fuseau horaire personnalisés :

1. Cliquez sur *Système - Date et heure - Fuseau horaire*.
2. Sélectionnez *Définir le fuseau horaire*.
3. Saisissez le nom du fuseau horaire et l'acronyme de l'heure standard de votre choix.
4. Indiquez le décalage par rapport à GMT.
5. Sélectionnez *Activer l'heure d'été*, si nécessaire.
6. Sélectionnez ou saisissez les valeurs appropriées pour l'heure d'été et cliquez sur *Enregistrer*.

Aide et langue

Cliquez sur *Système - Aide et langue* et sélectionnez dans le menu déroulant la langue du système de console.

NOTA : la langue sélectionnée s'applique aux sessions SSH, Telnet et voie console du système de console. La langue du navigateur est définie dans ses propres paramètres.

Aide en ligne

Lorsque la fonction d'aide en ligne est configurée sur le système de console, vous pouvez cliquer sur le bouton *Aide* de n'importe quelle page de l'interface utilisateur Web pour afficher la documentation produit de l'aide en ligne dans une nouvelle fenêtre.

Dans le champ URL d'aide en ligne, saisissez l'URL complète de l'aide en ligne sur le serveur Web local en terminant par /index.html. Cliquez sur *Enregistrer*.

NOTA : il n'est pas toujours possible d'utiliser la fonction d'aide en ligne à partir du serveur Vertiv en raison de la configuration du pare-feu et, d'ailleurs, nous ne vous le recommandons pas. Nous vous conseillons d'utiliser le système d'aide en ligne fourni avec le produit ou de télécharger le fichier .zip de l'aide en ligne et de l'exécuter sur un serveur local.

L'administrateur du système peut télécharger l'aide en ligne Vertiv™. Pour en savoir plus sur le téléchargement de l'aide en ligne, contactez l'assistance technique.

Une fois le fichier d'aide en ligne téléchargé (au format .zip), vous devez extraire les fichiers et les placer dans un répertoire de votre choix contenu dans le répertoire racine du serveur Web. L'accès au serveur Web doit être public.

Général

Cliquez sur *Système - Général* pour créer une bannière de connexion ou sélectionner le type de visualiseur.

Bannière de connexion :

Les administrateurs peuvent configurer une bannière de connexion qui s'affichera au démarrage des sessions SSHv2, Telnet, console et interface utilisateur Web.

Pour créer une bannière de connexion :

1. Cliquez sur *Système - Général* dans la barre de navigation latérale.
2. Cochez la case permettant d'activer la bannière de connexion.
3. Dans le champ Bannière de connexion, saisissez le texte que vous souhaitez afficher à la connexion et cliquez sur *Enregistrer*.

Visualiseur série

Le système de console utilise un visualiseur série HTML5 de base par défaut. Il prend également en charge un visualiseur série Java plus puissant. Les administrateurs peuvent configurer le visualiseur série à utiliser pour les voies série et le système de console.

NOTA : le visualiseur série HTML5 prend en charge 10 sessions par voie maximum, avec une limite de 48 sessions au total

Pour configurer le visualiseur série :

1. Cliquez sur *Système - Général* dans la barre de navigation latérale.
2. Sélectionnez le visualiseur HTML5 ou JNLP, puis cliquez sur *Enregistrer*.

Visualiseur série Java

NOTA : nous vous recommandons d'utiliser la version 1.8.0.91 de Java ou une version ultérieure. Pour pouvoir exécuter le visualiseur série, la version 32 bits doit être installée.

Le tableau suivant décrit les boutons disponibles dans l'applet Java.

Tableau 3.2 Boutons de l'applet Java pour la connexion au système de console

Bouton	Fonction
SendBreak	Envoyer une rupture au terminal
Disconnect	Se déconnecter de l'applet Java

NOTA : il est possible que vous deviez désactiver le bloqueur de fenêtres contextuelles du navigateur client pour pouvoir utiliser les visualiseurs série et du matériel.

NOTA : lorsque vous exécutez le visualiseur, le navigateur peut vous demander l'autorisation d'exécuter l'application Mindterm. Vous devez la lui accorder pour pouvoir exécuter l'applet du visualiseur.

Configuration de démarrage

La configuration de démarrage définit l'emplacement à partir duquel le système de console charge le système d'exploitation. Le système de console peut démarrer à partir de son firmware interne ou du réseau. Il démarre par défaut à partir du firmware interne dans la mémoire flash. Cliquez sur *Système - Configuration de démarrage* pour afficher l'écran Configuration de démarrage.

Si vous devez effectuer le démarrage à partir du réseau, vérifiez que les conditions suivantes sont remplies :

- Un serveur TFTP doit être disponible sur le réseau.
- Vous devez avoir téléchargé un fichier de firmware fourni par Vertiv et il doit être disponible sur le serveur TFTP.
- Vous devez connaître le nom du fichier de démarrage et l'adresse IP du serveur TFTP.

Pour paramétrer la configuration de démarrage :

1. Cliquez sur *Système - Configuration de démarrage*.
2. Dans Mode de démarrage, sélectionnez *Depuis la mémoire flash*, puis *Image 1* ou *Image 2*.

   -ou-

   Sélectionnez *Depuis le réseau* et indiquez les informations suivantes :

   - Adresse IP du matériel : saisissez l'adresse IP fixe ou une adresse IP attribuée au système de console par DHCP.
   - IP serveur TFTP : saisissez l'adresse IP du serveur de démarrage TFTP.
   - Nom du fichier : saisissez le nom du fichier du firmware de démarrage.
3. Vous pouvez utiliser le menu déroulant pour activer le minuteur de surveillance, si vous le souhaitez. Si vous l'activez, le système de console redémarre en cas de panne logicielle.
4. Dans le menu déroulant, sélectionnez la vitesse de la voie console et cliquez sur *Enregistrer*.

Informations

Cliquez sur *Système - Informations* pour afficher les informations concernant l'identité du système de console, les versions, l'alimentation et l'unité centrale.

Utilisation

Cliquez sur *Système - Utilisation* pour afficher l'utilisation de la mémoire et de la mémoire flash.

3.3.4 Réseau

Cliquez sur *Réseau* pour afficher et configurer les options Nom d'hôte, DNS, IPv6, Liaison, Routes statiques IPv4 et IPv6, Hôtes, Pare-feu, IPSec (VPN) et SNMP.

Paramètres

Cliquez sur *Réseau - Paramètres* pour modifier les paramètres réseau configurés.

Cette page permet aux administrateurs de configurer le nom d'hôte et les paramètres DNS du système de console, dont le DNS principal et secondaire, ainsi que les adresses de domaine et de recherche. Les administrateurs peuvent également activer IPv6 et le configurer pour obtenir le DNS et/ou le domaine à partir de DHCPv6.

Pour une configuration réseau tolérante aux pannes, il est possible de sélectionner l'option de liaison de manière à combiner eth0 et eth1 en une seule interface réseau à haute disponibilité grâce au mode de liaison à sauvegarde active. L'interface eth0 est l'interface active normale, tandis que l'interface eth1 est utilisée pour la sauvegarde. Si le signal porteur est perdu sur eth0, eth1 devient l'interface active. L'adresse MAC eth0 est toujours utilisée en mode de liaison, quelle que soit l'interface active.

NOTA : vous devez redémarrer le système de console pour que l'activation ou la désactivation de la liaison prenne effet.

Type de routage

Le système de console prend en charge des tables de multiroutage pour une stratégie de routage flexible. Il n'est pas possible d'activer le multiroutage si le basculement réseau ou la liaison sont activés.

Pour activer les tables de multiroutage :

1. Cliquez sur *Paramètres - Réseau*.
2. Sélectionnez le bouton radio Activer les tables de multiroutage IPv4 dans la section Multiroutage.

Basculement réseau

Le basculement réseau permet de garantir la fiabilité du système de console et l'accès aux dispositifs critiques lors d'une panne de réseau. Le basculement peut se produire lorsque l'interface principale tombe en panne ou qu'une adresse IP/passerelle devient inaccessible. Il est possible de l'activer avec un réseau secondaire ou une connexion ou PPP (accès sortant). Si vous avez configuré l'accès sortant, PPP0 est disponible en tant qu'interface secondaire, mais il n'est pas possible de l'utiliser en tant qu'interface principale.

L'utilisation du logiciel DSView avec le système de console garantit que celui-ci reste accessible en cas de panne. Le système de console passe alors un « appel à domicile » et met à jour son adresse IP dans le logiciel DSView.

La page Réseau - Paramètres permet aux administrateurs de configurer une interface réseau secondaire à utiliser en cas de panne. L'interface principale définit la passerelle par défaut du système, tandis que l'interface secondaire est utilisée lorsque la principale n'est pas disponible. Les administrateurs peuvent également sélectionner un des quatre déclencheurs de basculement :

- Interface principale en panne
- Passerelle par défaut principale non accessible
- DSView non accessible
- Adresse IP non accessible

Si le tunnel IPSec a été configuré (reportez-vous à la section IPSec (VPN) à la page 33), l'administrateur peut configurer l'établissement d'un tunnel IPSec sur l'interface secondaire, si nécessaire.

Pour activer le basculement réseau :

1. Dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Réseau - Paramètres*.
2. Dans la section Routage, sélectionnez le bouton radio Activer le basculement réseau.

3. Sélectionnez les interfaces principale et secondaire dans les menus déroulants, ainsi que le nom de la connexion VPN.
4. Sélectionnez le bouton radio correspondant au déclencheur de basculement que vous souhaitez utiliser.
5. Cliquez sur *Enregistrer*.

Si votre modèle est équipé d'un modem cellulaire, vous pouvez l'utiliser pour configurer le basculement. Pour en savoir plus, reportez-vous à la section Utilisation du modem cellulaire à des fins de basculement à la page 62.

NOTA : le modem cellulaire peut servir pour le basculement s'il n'est pas déjà utilisé en tant qu'interface principale.

Dispositifs

Les administrateurs peuvent sélectionner, activer et configurer les adresses IP attribuées aux interfaces réseau, et afficher l'adresse MAC. En plus des deux interfaces Ethernet standard, la liste des interfaces réseau inclut une entrée pour chaque dispositif USB Ethernet pouvant être installé.

Pour configurer un dispositif réseau :

1. Sélectionnez *Réseau - Dispositifs*. L'écran Dispositifs affiche une liste d'interfaces réseau, ainsi que leur statut (activé ou désactivé).
2. Cliquez sur le nom du dispositif réseau que vous souhaitez configurer.
3. Cochez la case correspondante si vous souhaitez définir le dispositif réseau en tant qu'interface principale. L'interface principale par défaut est eth0.
4. Sélectionnez le statut (*Activé* ou *Désactivé*) dans le menu déroulant.
5. Sélectionnez une des méthodes IPv4 suivantes :
   - Sélectionnez *DHCP* pour que l'adresse IPv4 soit définie par le serveur DHCP.
   - Sélectionnez *Statique* pour saisir manuellement l'adresse IPv4, le masque de sous-réseau et l'adresse de la passerelle.
   - Sélectionnez *Adresse IPv4 non configurée* pour désactiver IPv4.
6. Sélectionnez une des méthodes IPv6 suivantes :
   - Sélectionnez *Sans état* si la liaison se limite à l'adresse IP locale.
   - Sélectionnez *DHCPv6* pour que l'adresse IPv6 soit définie par le serveur DHCP.
   - Sélectionnez *Statique* pour saisir manuellement l'adresse IPv6 et la longueur du préfixe.
   - Sélectionnez *Adresse IPv6 non configurée* pour désactiver IPv6.

NOTA : l'adresse MAC du dispositif s'affiche après cette option.

Routes statiques IPv4 et IPv6

Pour ajouter des routes statiques :

1. Sélectionnez *Réseau - Routes statiques IPv4* ou *Routes statiques IPv6*. Les routes statiques existantes s'affichent, ainsi que les informations associées des champs IP de destination/Masque, Passerelle, Interface et Métrique.
2. Cliquez sur *Ajouter*.
3. Sélectionnez *Par défaut* pour configurer la route par défaut.

-ou-

Sélectionnez *Réseau ou IP hôte* pour saisir des paramètres personnalisés dans le champ IP de destination/Masque.

Renseignez le champ IP de destination/Bits de masque en utilisant la syntaxe <IP de destination>/<CIDR>.

4. Saisissez l'adresse IP de la passerelle dans le champ Passerelle.
5. Saisissez le nom de l'interface (Eth0, Eth1 ou PPPx) dans le champ Interface lorsque celle-ci est utilisée par la route.
6. Indiquez le nombre de tronçons vers la destination dans le champ Métrique, puis cliquez sur *Enregistrer*.

Hôtes

Les administrateurs peuvent configurer un tableau avec les noms d'hôte, les adresses IP et les alias des hôtes pour le réseau local.

Pour ajouter un hôte :

1. Sélectionnez *Réseau - Hôtes*.
2. Cliquez sur *Ajouter* pour ajouter un nouvel hôte.
3. Saisissez l'adresse IP, le nom d'hôte et l'alias de l'hôte que vous souhaitez ajouter, puis cliquez sur *Enregistrer*.

Pour modifier un hôte :

1. Sélectionnez *Réseau - Hôtes*.
2. Cliquez sur l'adresse IP du nom d'hôte que vous souhaitez modifier.
3. Saisissez un nouveau nom d'hôte et un nouvel alias, le cas échéant, puis cliquez sur *Enregistrer*.

Pare-feu

Les administrateurs peuvent configurer le système de console pour qu'il serve de pare-feu. Par défaut, trois chaînes intégrées acceptent tous les paquets INPUT, OUTPUT et FORWARD. Cliquez sur le bouton *Ajouter*, *Supprimer* ou *Changer de politique* pour ajouter une chaîne utilisateur, supprimer les chaînes ajoutées par les utilisateurs ou modifier la politique des chaînes intégrées. Il est possible de modifier la politique des chaînes par défaut (Changer de politique - Accepter ou Abandonner), mais vous ne pouvez pas les supprimer. Cliquez sur *Nom de chaîne* pour configurer des règles pour les chaînes.

La configuration du pare-feu est disponible dans *Réseau - Pare-feu*. Des écrans de configuration identiques mais distincts sont disponibles dans les options de menu *Table de filtre IPv4* ou *Table de filtre IPv6*.

Seule la politique des chaînes par défaut peut être modifiée. Les options disponibles sont ACCEPTER ou ABANDONNER.

Lorsque vous ajoutez une chaîne, seule une entrée avec son nom est créée. Vous devez configurer une ou plusieurs règles pour la chaîne après l'avoir ajoutée.

Configuration du pare-feu

Pour chacune des règles, vous devez sélectionner une action (*ACCEPTER, ABANDONNER, CONSIGNER, REJETER ou RETOURNER*) dans le menu déroulant Cible. L'action sélectionnée est appliquée sur les paquets IP qui remplissent tous les critères indiqués pour la règle.

Si vous avez sélectionné *CONSIGNER* dans le menu déroulant Cible, l'administrateur peut configurer un niveau et un préfixe de consignation.

Si vous avez sélectionné *REJETER* dans le menu déroulant Cible, l'administrateur peut sélectionner une option dans le menu déroulant Rejeter avec. Le paquet est abandonné et un paquet de réponse du type sélectionné est envoyé.

Options de protocole

Différents champs sont activés pour chacune des options disponibles dans le menu déroulant Protocole.

Si vous sélectionnez *Numérique* dans le menu Protocole, renseignez le champ Numéro de protocole.

Si vous sélectionnez *TCP* dans le menu Protocole, la section des options TCP est activée et vous permet d'indiquer les voies source et de destination, ainsi que les indicateurs TCP.

Si vous sélectionnez *UDP* dans le menu Protocole, la section UDP est activée et vous permet d'indiquer les voies source et de destination.

Tableau 3.3 Configuration du pare-feu – Champs des options TCP et UDP

Champ/option de menu	Définition
Voie source ou Voie de destination	Adresse IP unique ou plage d'adresses IP.
Indicateurs TCP	[TCP uniquement] SYN (synchroniser), ACK (confirmer), FIN (terminer), RST (réinitialiser), URG (urgent) et PSH (appliquer). Les conditions disponibles dans le menu déroulant pour chaque indicateur sont : Quelconque, Définir ou Annuler la définition.

Si vous avez sélectionné ICMP dans le menu Protocole, le menu déroulant Type ICMP est activé.

Si un administrateur indique l'interface Ethernet (eth0 ou eth1) dans les champs d'interface d'entrée ou de sortie et qu'il sélectionne une option (*2e paquets et suivants*, *Tous les paquets et fragments* ou *Paquets non fragmentés et 1ers paquets*) dans le menu déroulant Fragments, l'action cible est effectuée sur les paquets reçus de ou envoyés vers l'interface indiquée s'ils remplissent les critères de l'option du menu Fragments sélectionnée.

Pour ajouter une chaîne :

1. Sélectionnez *Réseau - Pare-feu*.
2. Sélectionnez *Table de filtre IPv4* ou *Table de filtre IPv6*.
3. Cliquez sur *Ajouter*.
4. Saisissez le nom de la chaîne à ajouter.
5. Cliquez sur *Enregistrer*.

NOTA : le nom de la chaîne ne doit comporter aucun espace.

6. Ajoutez une ou plusieurs règles pour terminer la configuration de la chaîne.

Pour modifier la politique d'une chaîne par défaut :

NOTA : il est impossible de modifier les chaînes définies par les utilisateurs. Si vous souhaitez attribuer un nouveau nom à une chaîne ajoutée par un utilisateur, vous devez la supprimer, puis en créer une nouvelle.

1. Sélectionnez *Réseau - Pare-feu*.
2. Sélectionnez *Table de filtre IPv4* ou *Table de filtre IPv6*.
3. Cochez la case à côté du nom de la chaîne à modifier (*FORWARD*, *INPUT*, *OUTPUT*).
4. Cliquez sur *Changer de politique* et sélectionnez *Accepter* ou *Abandonner* dans le menu déroulant.
5. Cliquez sur *Enregistrer*.

Pour ajouter une règle :

1. Sélectionnez *Réseau - Pare-feu*.
2. Sélectionnez *Table de filtre IPv4* ou *Table de filtre IPv6*.
3. Dans la liste des chaînes, cliquez sur le nom de la chaîne à laquelle vous souhaitez ajouter une règle.
4. Cliquez sur *Ajouter* et configurez la règle souhaitée, puis cliquez sur *Enregistrer*.

Pour modifier une règle :

1. Sélectionnez *Réseau - Pare-feu*.
2. Sélectionnez *Table de filtre IPv4* ou *Table de filtre IPv6*.
3. Dans la liste des chaînes, cliquez sur le nom de la chaîne dont vous souhaitez modifier la règle.
4. Sélectionnez la règle que vous souhaitez modifier et cliquez sur le bouton *Modifier*.
5. Apportez les modifications souhaitées, puis cliquez sur *Enregistrer*.

IPSec (VPN)

Un réseau privé virtuel (VPN) permet d'établir une communication sécurisée entre le système de console et un réseau distant en utilisant une passerelle et en créant une connexion sécurisée entre le système de console et cette passerelle. Le protocole IPSec permet de créer un tunnel sécurisé et de fournir des services de chiffrement et d'authentification au niveau de l'adresse IP de la pile de protocoles.

Avec un système de console situé sur un réseau à part, derrière un routeur, ce protocole établit un tunnel IPSec avec un certificat x.509 pour le pare-feu. Les certificats et les clés sont distribués au pare-feu et au système de console par une autorité de certification (CA).

NOTA : le système de console prend en charge un seul certificat par tunnel. Les certificats multiples ne sont pas pris en charge, de même que les tunnels IPv6. Il est possible de charger les certificats (au format PKCS12) à partir du menu Outils système.

NOTA : pour pouvoir exécuter IPSec (VPN), vous devez activer IPSec dans le profil de sécurité personnalisé.

La passerelle distante est appelée hôte distant ou droit, et le système de console, hôte local ou gauche.

Création d'un certificat d'autorité

Pour configurer le pare-feu Fortinet Fortigate, vous devez créer un serveur de certificat d'autorité (CA) interne, qui génère les certificats RSA que le système de console utilise pour l'authentification.

Pour en savoir plus sur la création d'un certificat d'autorité sur un serveur Ubuntu, reportez-vous à la section correspondante dans cette documentation (en anglais).

Création d'un tunnel sur le serveur

Pour créer un tunnel sur le serveur :

1. Dans l'onglet *System* (Système) de l'interface utilisateur Web Fortigate, cliquez sur *Certificates* (Certificats) et importez le certificat d'autorité et le certificat SERVEUR créés à partir du serveur easy-rsa.
2. Dans l'onglet *User & Device* (Utilisateur et dispositif), cliquez sur *PKI* et créez un nouvel utilisateur nommé **user1** avec le certificat d'autorité nommé **CA_Cert_1**. Créez ensuite un groupe d'utilisateurs nommé **user_group1** et ajoutez user1 à ce groupe.
3. Dans l'onglet *VPN*, cliquez sur *IPSec - Tunnels* et créez un nouveau tunnel VPN personnalisé avec la configuration ci-dessous, puis cliquez sur *OK*.

Tableau 3.4 Paramètres de configuration du tunnel VPN

Paramètre	Valeur
Network	
Remote Gateway	Dial-up User
Interface	wan1
Mode Config	Enabled
IP Version	IPv4
Client Address Range	10.77.20.100-10.77.20.110
Subnet Mask	255.255.255.0
Use System DNS	Enabled
Enable IPv4 Split Tunnel	Enabled
Accessible Networks	local_lan
NAT Traversal	Enabled
Keepalive Frequency	300
Dead Peer Detection	Enabled
Authentication	
Method	Signature
Certificate Name	server
IKE Version	2
Peer Options Accept Types	Peer Certificate Group
Peer Certificate Group	user_group1
Phase 1 Proposal	
Encryption	AES128
Authentication	SHA1
Diffie-Hellman Group	14
Key Lifetime (Seconds)	86400
Local ID	C=<pays> S=<état> L=<ville> O=<organisation>
Edit Phase 2	
Name	<nom>
Comments	<commentaires>
Local Address Subnet	0.0.0.0/0.0.0.0
Remote Address Subnet	0.0.0.0/0.0.0.0
Phase 2 Proposal	
Encryption	AES128
Authentication	SHA1
Enable Replay Detection	Enabled
Enable Perfect Forward Secrecy (PFS)	Enabled

Tableau 3.4 Paramètres de configuration du tunnel VPN (suite)

Paramètre	Valeur
Diffie-Hillman Group	14
Local Port All	Enabled
Remote Port All	Enabled
Protocol All	Enabled
Autokey Keep Alive	Enabled
Key Lifetime	Seconds
Seconds	43200

4. Dans l'onglet *Policy & Objects* (Politiques et objets), cliquez sur *Objects - Addresses* (Objets - Adresses) pour créer une plage VPN avec les paramètres ci-dessous, puis cliquez sur *OK*.

Tableau 3.5 Configuration de la plage VPN

Paramètre	Valeur
Name	ipsec_vpn_range
Type	IP Range
Subnet / IP Range	10.77.20.100 - 10.77.20.110
Interface	Any
Show in Address List	Enabled
Comments	Adresse IP attribuée aux clients VPN qui se connectent

5. Dans l'onglet *Policy & Objects* (Politiques et objets), cliquez sur *Objects - Addresses* (Objets - Adresses) pour créer une plage LAN locale avec les paramètres ci-dessous, puis cliquez sur *OK*.

Tableau 3.6 Configuration de la plage LAN local

Paramètre	Valeur
Name	local_lan
Type	IP / Netmask
Subnet / IP Range	192.168.1.0 / 255.255.255.0
Interface	internal
Show in Address List	Enabled
Comments	Local Lan - inside network

6. Dans l'onglet *Policy & Objects* (Politiques et objets), cliquez sur *Policy - IPv4* (Politique - IPv4) pour créer la politique de pare-feu 1 avec les paramètres ci-dessous, puis cliquez sur *OK*.

Tableau 3.7 Configuration de la politique de pare-feu 1

Paramètre	Valeur
Incoming Interface	forti2acs
Source Address	ipsec_vpn_range
Outgoing Interface	internal
Destination Address	local_lan
Schedule	always
Service	ALL
Action	ACCEPT
Firewall / Network Options	
NAT	ON
Use Outgoing Interface Address	Enabled
Security Profiles	
Antivirus, Web Filter, Application Control, SSL Inspection	All OFF
Traffic Shaping	
Shared Shaper, Reverse Shaper, Per-IP Shaper	All OFF
Logging Options	
Log Allowed Traffic	ON
Security Events	Enabled
Comments	<Commentaires>
Enable this policy	Enabled

7. Dans l'onglet *Policy & Objects* (Politiques et objets), cliquez sur *Policy - IPv4* (Politique - IPv4) pour créer la politique de pare-feu 2 avec les paramètres ci-dessous, puis cliquez sur *OK*.

Tableau 3.8 Configuration de la politique de pare-feu 2

Paramètre	Valeur
Incoming Interface	internal
Source Address	local_lan
Outgoing Interface	forti2acs
Destination Address	ipsec_vpn_range
Schedule	always
Service	ALL
Action	ACCEPT
Firewall / Network Options	
NAT	ON
Use Outgoing Interface Address	Enabled
Security Profiles	
Antivirus, Web Filter, Application Control, SSL Inspection	All OFF
Traffic Shaping	
Shared Shaper, Reverse Shaper, Per-IP Shaper	All OFF
Logging Options	
Log Allowed Traffic	ON
Security Events	Enabled
Comments	<Commentaires>
Enable this policy	Enabled

8. Dans l'onglet *Policy & Objects* (Politiques et objets), cliquez sur *Policy - IPv4* (Politique - IPv4) pour créer la politique de pare-feu 3 avec les paramètres ci-dessous, puis cliquez sur *OK*.

Tableau 3.9 Configuration de la politique de pare-feu 3

Paramètre	Valeur
Incoming Interface	any
Source Address	all
Outgoing Interface	any
Destination Address	all
Action	DENY
Logging Options	
Log Violation Traffic	OFF

Création d'un tunnel sur le système de console

Pour créer un tunnel sur le système de console :

1. Dans la barre de navigation latérale de l'onglet *Expert*, cliquez sur *Réseau - IPSec (VPN)*, puis sur *Ajouter*.

2. Saisissez le nom de la connexion.
3. Dans le menu déroulant, sélectionnez *IKEv2* pour la version IKE et *Démarrer*, *Ajouter* ou *Ignorer* pour l'option Action de démarrage.
    a. Démarrer : charge une connexion et l'établit immédiatement (au démarrage ou après la sauvegarde de la configuration).
    b. Ajouter : charge une connexion sans la lancer. Par exemple, il est possible de démarrer le VPN sous certaines conditions avec un script.
    c. Ignorer : ignore la connexion.
4. Configurez les paramètres suivants pour le côté distant (« droit ») :
    a. Laissez le champ de l'ID vide.
    b. Saisissez l'adresse IP du VPN distant dans le champ Adresse IP.
    c. Dans le champ Sous-réseau, indiquez le sous-réseau que le système de console va utiliser pour se connecter.
5. Configurez les paramètres suivants pour le côté local (« gauche ») :
    a. Laissez le champ de l'ID vide.
    b. Saisissez l'adresse IP de l'interface principale dans le champ Adresse IP.

NOTA : l'interface principale est celle qui est utilisée pour la connexion au pare-feu distant (etho or eth1). La valeur par défaut est eth0 et l'option Récupération de la configuration Bootp est activée. Si votre interface principale est eth1, assurez-vous que l'option Récupération de la configuration Bootp de la page Profil de sécurité est désactivée.

6. Sélectionnez le bouton radio Certificat RSA, puis cliquez sur la liste déroulante Fichiers PKCS12 locaux et sélectionnez le fichier PKCS12.

Pour activer IPSec sur le système de console :

1. Dans la barre de navigation latérale de l'onglet *Expert*, cliquez sur *Système - Sécurisé - Profil de sécurité*.
2. Sélectionnez le bouton radio Personnalisé dans la section Profil de sécurité.
3. Cochez la case Activer IPSec, puis cliquez sur *Enregistrer*.

NOTA : après avoir cliqué sur le bouton Enregistrer, la connexion VPN démarre automatiquement si l'option Action de démarrage est définie sur Démarrer. Les informations sont enregistrées et le VPN démarre (ou redémarre).

Vérification

Il est possible d'effectuer des tests de vérification pour s'assurer qu'IPSec a bien été configuré. La commande ping permet de tester la communication.

Pour vérifier le statut d'IPSec et tester la communication :

1. Connectez-vous au système de console en tant qu'utilisateur racine.
2. Vérifiez le statut d'IPSec en saisissant la commande *ipsec status* dans l'invite du shell. Notez l'adresse IP VPN DHCP.
3. Saisissez ping dans l'invite de commande, appuyez sur la barre d'espace, saisissez l'adresse que vous souhaitez tester, puis appuyez sur Entrée et attendez les résultats du test. Testez la communication à partir du système de console vers le client cible du sous-réseau distant.

4. Testez la communication à partir du client cible du sous-réseau distant vers l'adresse IP VPN DHCP du système de console.

NOTA : pour tester la communication, saisissez la commande ping à partir du client cible vers l'adresse IP VPN DHCP du système de console et à partir du système de console vers le client cible du sous-réseau.

3.3.5 Paramètres avancés d'IPSec (VPN)

La page de configuration IPSec (VPN) comporte les paramètres avancés pour le fichier ipsec.conf. Ces paramètres, décrits dans le tableau ci-dessous, s'affichent lorsque vous cochez la case Afficher les paramètres avancés.

Tableau 3.10 Description des paramètres avancés

Name	Description
Suite de chiffrement IKE (Internet Key Exchange)	Protocoles utilisés pour échanger les clés de chiffrement. Cette suite inclut des algorithmes pour les protocoles de chiffrement (confidentialité), de hachage (authentification des messages) et du groupe DH (échange de clés) lors de la configuration du VPN.
Suite de chiffrement ESP (Encapsulating Security Payload)	Protocoles utilisés pour échanger les clés de chiffrement. Cette suite inclut des algorithmes pour les protocoles de chiffrement (confidentialité), de hachage (authentification des messages) et du groupe DH (échange de clés) lors de la configuration du VPN. Si un groupe DH est utilisé, les numéros de groupe plus élevés sont plus sûrs, mais le calcul de la clé prend plus de temps.
Association de sécurité (SA)	Une association de sécurité décrit la manière dont deux dispositifs ou plus peuvent communiquer en toute sécurité.
Nouvelle authentification	Indique si le dispositif doit procéder à une nouvelle authentification lorsqu'une association de sécurité (SA) IKE change.
Durée de vie IKE	Indique la durée du canal d'échange de clés d'une connexion (ISAKMP ou IKE SA) avant que celui-ci ne soit négocié à nouveau.
Durée de vie de la clé	Indique la durée d'une instance de connexion particulière (ensemble de clés de chiffrement/d'authentification pour les paquets d'utilisateurs), depuis la négociation jusqu'à l'expiration.
Renouveler la clé	Indique si une connexion doit de nouveau être négociée lorsqu'elle est sur le point d'expirer.
Tentatives d'obtention de la clé	Indique le nombre de tentatives (nombre entier positif ou %forever) à effectuer lors de la négociation ou du remplacement d'une connexion avant de renoncer. La valeur par défaut est 3.
Délai de renouvellement de la clé	Indique le délai avant l'expiration de la connexion ou du canal d'échange de clés si les tentatives de négociation d'une nouvelle clé commencent.
Délai DPD	Indique l'intervalle d'envoi de messages R_U_THERE /INFORMATIONAL à l'homologue.

3.3.6 Configuration SNMP

Les administrateurs peuvent configurer SNMP. Cette configuration est nécessaire si des notifications doivent être envoyées à une application de gestion SNMP.

NOTA : le fichier texte Enterprise MIB du système de console avancé Avocent® ACS 800/8000 se trouve dans le matériel à l'emplacement suivant : /usr/local/mibs/ACS8000-MIB.asn. Le fichier texte TRAP Enterprise MIB du système de console avancé Avocent® ACS 800/8000 se trouve dans le matériel à l'emplacement suivant : /usr/local/mibs/ACS8000-TRAP-MIB.asn. Les deux fichiers sont également disponibles sur le site www.VertivCo.com.

Pour configurer SNMP :

1. Cliquez sur *Réseau - SNMP*.
2. Cliquez sur le bouton *Système*.
   a. Saisissez les informations de contact système (adresse e-mail de l'administrateur du système de console, par exemple, acs8000_admin@vertivco.com).
   b. Saisissez les informations d'emplacement système (emplacement physique du système de console, par exemple Avocent_ACS8000), puis cliquez sur *Enregistrer* pour revenir à l'écran SNMP.
3. Cliquez sur *Ajouter* pour ajouter une nouvelle communauté ou un nouvel utilisateur v3.
4. Saisissez le nom de la communauté pour SNMP v1/v2 ou le nom d'utilisateur pour SNMP v3 dans le champ Nom, puis saisissez l'OID.
5. Sélectionnez les autorisations souhaitées dans le menu déroulant. Vous avez le choix entre *Lecture et écriture* ou *Lecture seule*.
6. Si la version SNMP requise est v1 ou v2, cliquez sur le bouton *Version v1, v2* et indiquez la source (adresse de sous-réseau).

   -ou-

   Si la version SNMP requise est v1 ou v2 avec un réseau IPv6, cliquez sur le bouton *Version v1, v2 pour réseau IPv6* et indiquez la source (adresse de sous-réseau).

   -ou-

   Si la version SNMP requise est v3, cliquez sur le bouton *Version v3*, sélectionnez le type d'authentification (*MD5* ou *SHA*), saisissez la phrase secrète ou le mot de passe d'authentification, sélectionnez la méthode de chiffrement (DES ou AES), saisissez la phrase secrète pour la confidentialité et sélectionnez le niveau minimal d'authentification (*NoAuthNoPriv*, *AuthNoPriv*, *AuthPriv*).
7. Cliquez sur *Enregistrer*.

NOTA : pour SNMP v1/v2c, le système de console permet aux administrateurs de configurer le même nom de communauté avec des sources (filtres) différentes pour pouvoir accéder à des identifiants d'objet (OID) spécifiques.

3.3.7 Voies

Les administrateurs peuvent activer et configurer les voies série, les voies auxiliaires, le profil CAS et le profil d'accès entrant à partir de l'onglet Voies de la barre de navigation latérale. Vous pouvez activer et configurer le modem interne sur l'écran Voies auxiliaires.

Les voies série du système de console peuvent avoir différents rôles en fonction du profil configuré pour chaque voie.

Voies série

Dans le tableau Voies série, vous pouvez indiquer le profil de connexion (CAS, Accès entrant, Alimentation, Accès sortant ou Prise client) en fonction du type de dispositif relié. Vous pouvez également cloner la voie, la réinitialiser aux valeurs par défaut, activer/désactiver des voies ou ouvrir une session série.

Le tableau indique le numéro de la voie, l'ID du dispositif, le statut, le nom, le profil, les signaux et les paramètres. La colonne Paramètres indique le brochage utilisé pour la voie par les abréviations suivantes :

- CYC - Cyclades
- CIS - Cisco
- 422 - RS422
- 485 - RS485

NOTA : il est possible que le tableau n'indique pas de brochage si aucun dispositif n'est relié à la voie.

Pour activer ou désactiver une ou plusieurs voies série :

1. Sélectionnez *Voies - Voies série*.
2. Cochez les cases correspondant aux voies que vous souhaitez activer ou désactiver.
3. Cliquez sur le bouton *Activer* ou *Désactiver*.

Pour configurer ou modifier une ou plusieurs voies série avec le profil CAS :

1. Sélectionnez *Voies - Voies série*.
2. Cochez les cases correspondant aux voies que vous souhaitez configurer.
3. Cliquez sur le bouton *Définir CAS*. Activez ou désactivez les voies à l'aide des menus déroulants et définissez le brochage RJ45, la vitesse, la parité, les bits de données, les bits d'arrêt et le contrôle du flux.

NOTA : si vous sélectionnez AUTO pour le brochage RJ45, la détection automatique des connecteurs Cyclades ou Cisco pour les dispositifs RS232 est activée.

4. Cliquez sur le bouton *Suivant* ou sur le lien *CAS*.
    a. Indiquez le nom de la voie (si vous avez sélectionné une seule voie) ou le préfixe du nom de la voie (si vous en avez sélectionné plusieurs). Le nom de la voie se présente au format <préfixe du nom de la voie>-p-<numéro de voie>.
    b. Cochez la case permettant d'activer la détection automatique. Dans ce cas, le nom de la voie est utilisé lorsque la détection automatique n'arrive pas à localiser le nom du serveur.
    c. Cochez la case permettant d'activer la détection automatique de la vitesse.

NOTA : pour utiliser la fonction de détection automatique de la vitesse, vous devez configurer des paramètres supplémentaires sur l'écran Profil CAS - Paramètres de détection automatique.

    d. Sélectionnez le protocole et le type d'authentification dans les menus déroulants correspondants.
    e. Indiquez les touches de raccourci de session de texte, de session de gestion de l'alimentation et RESTful dans les champs appropriés.
    f. Saisissez l'alias de voie TCP pour chaque type de protocole (Telnet, SSH et mode brut).
    g. Indiquez l'alias IPv4 ou IPv6, ainsi que l'interface utilisée.
    h. Cochez les cases appropriées si vous souhaitez n'autoriser la session que si DCD est activé et pour activer la réponse automatique.
    i. Dans le menu déroulant, sélectionnez le mode DTR et saisissez l'intervalle d'arrêt DTR.
    j. Activez ou désactivez les options Suppression de saut de ligne et NULL après suppression CR dans les menus déroulants.
    k. Indiquez l'intervalle de transmission, la séquence de rupture et l'intervalle de rupture.

NOTA : l'intervalle de transmission indique le délai (en millisecondes) avant la réception des données transmises à Ethernet par l'intermédiaire d'une voie série La valeur par défaut est 20 ms.

l. Activez ou désactivez le menu Sessions multiples dans le menu déroulant. Pour en savoir plus, reportez-vous à la section Menu Sessions multiples à la page 49.

m. Dans les menus déroulants, activez ou désactivez la notification de connexion/déconnexion en cas de sessions multiples et la notification de message d'information.

5. Cliquez sur le bouton *Suivant* ou sur le lien *Mise en mémoire tampon des données* pour activer et configurer cette option à l'aide des menus déroulants.
6. Cliquez sur le bouton *Suivant* ou sur le lien *Alertes*.
   a. Cliquez sur *Activer les alertes* pour activer la détection des alertes.
   b. Cliquez sur *Ajouter* pour ajouter une chaîne d'alerte. Dans le champ de la chaîne d'alerte, saisissez la chaîne. Dans le champ Script, indiquez le script du shell qui va être exécuté en cas de correspondance. Cochez la case Urgence pour activer le clignotement rapide orange du voyant de la voie série lorsque cette alerte se déclenche. Un clignotement lent indique que l'alerte n'est pas urgente. Cliquez sur *Suivant* pour revenir à l'écran Alertes.

NOTA : le système de console permet à l'administrateur d'associer un script du shell à la chaîne d'alerte. Lorsqu'une correspondance avec la chaîne d'alerte est détectée, le système de console appelle le script et transmet le numéro de voie et la ligne où la correspondance s'est produite sous forme d'arguments.

   c. Cochez la case à côté d'une alerte existante et cliquez sur *Supprimer* pour supprimer la chaîne.
   d. Cliquez sur *Supprimer quelconque* pour supprimer toutes les chaînes, sélectionnées ou non.

NOTA : l'option *Supprimer quelconque* supprime toutes les chaînes d'alerte. Le résultat n'est pas le même que si vous sélectionnez toutes les chaînes d'alerte et cliquez sur *Supprimer*, car cette action ne supprime pas les chaînes d'alerte qui ne figurent pas dans le tableau.

7. Cliquez sur le bouton *Suivant* ou sur le lien *Alimentation*.
   a. Cliquez sur *Ajouter* pour ajouter une nouvelle prise. Cliquez sur *Sélectionner une PDU* et sélectionnez un dispositif dans la liste des PDU détectées. Indiquez les prises dans le champ correspondant, puis cliquez sur *Suivant*.
   b. Cochez la case à côté d'une prise fusionnée, puis cliquez sur *Supprimer* pour l'effacer.

NOTA : le lien Alimentation est disponible uniquement lorsqu'une seule voie série est sélectionnée.

8. Cliquez sur *Enregistrer*.

Tableau 3.11 Paramètres du profil CAS

Paramètre	Description
Physique	
Statut	Définit le statut de la voie série (activé ou désactivé). Valeur par défaut : Désactivé.
Connecteur RJ45	Définit le brochage de la voie série : Auto, Cyclades ou Cisco. Les voies 1 et 2 prennent également en charge les connecteurs RS422 et RS485. Valeur par défaut : Auto.
Vitesse	Définit la vitesse (1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 ou 230 400). Valeur par défaut : 9 600.
Parité	Définit la parité (Paire, Impaire, Aucune). Valeur par défaut : Aucune.
Bits de données	Définit les bits de données (5, 6, 7 ou 8). Valeur par défaut : 8.
Bits d'arrêt	Définit les bits d'arrêt (1 ou 2). Valeur par défaut : 1.
Contrôle du flux	Définit le contrôle du flux (Aucun, Matériel, Logiciel, Logiciel RxON, Logiciel TxON). Valeur par défaut : Aucun.
CAS	
Nom de la voie	Indique le nom associé à la voie série (alias). Valeur par défaut : <adresse mac du dispositif>-p-<numéro de voie>.
Activer la détection automatique	Permet de détecter le nom de la cible et de l'associer à cette voie série. Si l'opération échoue, le nom de la voie est utilisé. Valeur par défaut : Désactivé.
Activer la détection automatique de la vitesse	Tente de détecter la vitesse de la voie série. Pour utiliser cette fonction, vous devez configurer des paramètres supplémentaires sur l'écran Profil CAS - Détection automatique - Paramètres. Valeur par défaut : Désactivé.
Protocole	Indique le protocole qui sera utilisé par les utilisateurs autorisés pour accéder à la cible/voie série. Le système de console accepte trois protocoles pour la connexion à la cible : Telnet pour les connexions Telnet, SSH pour les connexions sécurisées et mode brut pour la connexion à la prise en mode brut. Les administrateurs peuvent configurer cette voie avant d'accepter un, deux ou les trois types de connexion. **NOTA :** vous devez configurer l'alias mode brut de la voie pour pouvoir utiliser le protocole en mode brut. Valeur par défaut : SSH.
Type d'authentification	Indique le type d'authentification qui sera utilisé pour authentifier l'utilisateur lors de la session cible. Valeur par défaut : Locale.
Touche de raccourci de session de texte	Indique la touche de raccourci permettant de suspendre la session cible et d'afficher l'invite CLI. Cette fonction n'est pas disponible en mode brut. Valeur par défaut : **Ctrl+Z**. Nota : la commande d'interruption par défaut dans ts_menu est **Ctrl+X**.
Touche de raccourci de session de gestion de l'alimentation	Indique la touche de raccourci permettant de suspendre la session cible et d'afficher le menu Gestion de l'alimentation pour gérer les prises fusionnées avec la cible. Cette fonction n'est pas disponible en mode brut. Valeur par défaut : **Ctrl+P**. Nota : la commande d'interruption par défaut dans ts_menu est **Ctrl+X**.
Touche de raccourci RESTful	Indique la touche de raccourci permettant de suspendre la session cible et d'afficher le menu RESTful, utilisé pour effectuer des actions RESTful définies par l'utilisateur. Valeur par défaut : non configuré (champ vide).
Alias TCP de la voie	Alias Telnet de la voie : voie TCP permettant de se connecter directement à une voie série à l'aide du protocle Telnet. Alias SSH de la voie : voie TCP permettant de se connecter directement à une voie série à l'aide du protocle SSH. Alias mode brut de la voie : voie TCP permettant de se connecter directement à une voie série à l'aide d'une prise en mode brut.
Alias IPv4/IPv6 de la voie	Indique l'adresse IPv4/IPv6 utilisée pour se connecter directement à une voie série. Valeur par défaut : non configuré (champ vide).
Interface de l'alias IPv4/IPv6 de la voie	Indique l'interface (ETH0/ETH1) associée à l'alias IPv4/IPv6. Valeur par défaut : ETH0.

Tableau 3.11 Paramètres du profil CAS (suite)

Paramètre	Description
N'autoriser la session que si DCD est activé	Indique au matériel de refuser l'accès à cette voie série si DCD est désactivé. Valeur par défaut : Désactivé (autoriser l'accès si DCD est désactivé).
Activer la réponse automatique	Transmet la chaîne de sortie à la voie série lorsque les données d'entrée correspondent à une chaîne d'entrée configurée pour la réponse automatique. Valeur par défaut : Désactivé.
Mode DTR	Permet de configurer le mode DTR : Toujours sous tension ; Normal : le statut DTR dépend de l'existence d'une session CAS ; Intervalle d'arrêt : le mode DTR est arrêté pendant la durée définie lorsqu'une session CAS est fermée. Valeur par défaut : Normal.
Intervalle d'arrêt DTR	Indique la durée (en secondes) utilisée par l'intervalle d'arrêt du mode DTR en millisecondes. Valeur par défaut : 100.
Suppression de saut de ligne	Permet de supprimer le caractère LF après le caractère CR. Valeur par défaut : Désactivé.
NULL après suppression CR	Permet de supprimer le caractère NULL après le caractère CR. Valeur par défaut : Désactivé.
Intervalle de transmission	Indique la durée (en millisecondes) pendant laquelle la voie attend avant d'envoyer des données à un client distant. Valeur par défaut : 20.
Séquence de rupture	Permet à l'administrateur de configurer une touche de contrôle pour la séquence de rupture en saisissant ^ avant la commande. Cette fonction n'est pas disponible en mode brut. Valeur par défaut : ~break.
Intervalle de rupture	Indique l'intervalle (en millisecondes) pour le signal de rupture. Cette fonction n'est pas disponible en mode brut. Valeur par défaut : 500.
Afficher le menu Sessions multiples	Permet d'afficher le menu Sessions multiples lors de la connexion à une voie déjà utilisée par un autre utilisateur. Valeur par défaut : Désactivé.
Notification de connexion/déconnexion des sessions multiples	Permet l'envoi de notifications aux utilisateurs de sessions multiples, les avertissant de la connexion d'un nouvel utilisateur ou de la déconnexion d'un utilisateur existant. Cette fonction n'est pas disponible en mode brut. Valeur par défaut : Désactivé.
Notification de message d'information	Affiche un message informant l'utilisateur lorsqu'une session cible est ouverte. Cette fonction n'est pas disponible en mode brut. Valeur par défaut : Activé.
Mise en mémoire tampon des données	
Statut	Active ou désactive la mise en mémoire tampon des données. Valeur par défaut : Désactivé.
Type	Affiche le type de mise en mémoire tampon des données : Locale – stocke le fichier de mise en mémoire tampon des données dans le système de fichiers local ; NFS – stocke le fichier de mise en mémoire tampon des données sur le serveur NFS ; Syslog – envoie les données au serveur syslog ; DSView – envoie les données au serveur DSView. Valeur par défaut : Locale.
Type local	Indique l'emplacement où les fichiers de mise en mémoire tampon des données sont stockés sur le système local. Les emplacements possibles sont la mémoire intégrée (mmcblk0) ou les dispositifs de stockage USB ou la carte SD reliés. Valeur par défaut : mmcblk0.
Horodatage	Ajoute l'horodatage à la ligne de la mise en mémoire tampon des données pour une base de données locale ou NFS. Valeur par défaut : Désactivé.
Message de connexion/déconnexion	Inclut des notifications spéciales suite aux connexions et aux déconnexions dans la mise en mémoire tampon des données. Valeur par défaut : Désactivé.
Consignation de session série	Activé : stocke les données à tout moment. Désactivé : stocke les données lorsqu'aucune session CAS n'est ouverte. Valeur par défaut : Activé.
Alertes	
Statut	Génère une notification d'événement spéciale lorsque les données d'entrée correspondent à une chaîne d'alerte. Valeur par défaut : Désactivé.

Tableau 3.11 Paramètres du profil CAS (suite)

Paramètre	Description
Chaînes d'alerte	Chaînes utilisées pour générer les notifications d'événement. Valeur par défaut : champ vide.
Scripts	Indique le nom du script de shell invoqué en cas de correspondance avec une chaîne d'alerte dans la ligne. Le script est invoqué avec deux arguments : le numéro de la voie et la ligne où la correspondance s'est produite.
Urgence	Provoque un clignotement rapide orange du voyant de la voie série lors d'une alerte d'urgence (le clignotement est lent dans le cas contraire).

Pour configurer le profil d'accès entrant pour une voie série reliée à un modem :

1. Sélectionnez *Voies - Voies série*.
2. Cochez la case correspondant à une voie série reliée à un modem.
3. Cliquez sur le bouton *Définir l'accès entrant* et configurez les paramètres d'accès entrant dans les menus déroulants.
4. Configurez les paramètres PPP (adresse, authentification, etc.), puis cliquez sur *Enregistrer*.

Tableau 3.12 Paramètres d'accès entrant

Paramètre	Description
Statut	Active ou désactive la voie. Valeur par défaut : Désactivé.
Vitesse	Indique la vitesse utilisée par mgetty pour configurer le dispositif série. Valeur par défaut : 38 400 bit/s.
Lancer discussion	Discussion pour l'initialisation du modem. Valeur par défaut : "" \d\d\d+++\d\d\dATZ OK.
Adresse PPP	Permet de configurer les adresses IP locale et distante pour la liaison PPP. Si vous sélectionnez *Accepter la configuration de l'homologue distant*, l'homologue distant envoie les deux adresses IP (locale et distante) lors de la négociation. Valeur par défaut : Aucune adresse.
Adresse IPv4/IPv6 locale	Permet de configurer l'adresse IPv4/IPv6 locale pour cette connexion PPP.
Adresse IPv4/IPv6 distante	Permet de configurer l'adresse IPv4/IPv6 distante pour cette connexion PPP.
Protocole d'authentification PPP	Sélectionnez l'option requise à l'aide des boutons radio : Aucun, PAP, CHAP ou EAP. Aucun : pas d'authentification. • PAP : utilise le protocole PAP et le type d'authentification PPP configuré sur la page Authentification/Authentification d'unité. • CHAP : utilise le protocole CHAP. La configuration des secrets CHAP se fait en modifiant le fichier /etc/ppp/chap-secrets. • EAP : utilise le protocole EAP. Authentifications disponibles : CHAP, SRP-SHA1 et TLS. La configuration des secrets CHAP se fait en modifiant le fichier /etc/ppp/chap-secrets. La configuration des secrets SRP-SHA1 se fait en modifiant le fichier /etc/ppp/srp-secrets. Nota : l'authentification EAP n'est disponible qu'avec le système d'exploitation Windows XP. Valeur par défaut : Aucun.
CHAP	Permet de configurer les champs CHAP-interval, CHAP-max-challenge et CHAP-restart. Valeurs par défaut : • CHAP-interval = 0. • CHAP-max-challenge = 10. • CHAP-restart = 3.
Délai d'inactivité PPP	Indique la durée d'inactivité (en secondes) avant expiration de la connexion PPP. Valeur par défaut : 0 (pas de délai d'expiration).

Pour configurer ou modifier une ou plusieurs voies série reliées à une PDU :

1. Sélectionnez *Voies - Voies série*.
2. Cochez la case correspondant à une ou plusieurs voies série reliées à une PDU.
3. Cliquez sur le bouton *Définir comme alimentation* et configurez les paramètres physiques à l'aide des menus déroulants.
4. Cliquez sur le bouton *Suivant* ou sur le lien *Alimentation*.
    a. Sélectionnez le type de PDU dans le menu déroulant.
    b. Cochez la case pour activer la détection automatique de la vitesse.
    c. Configurez le taux d'interrogation.
    d. Pour les PDU Avocent/Cyclades, indiquez l'intervalle de redémarrage, puis activez ou désactivez les options Syslog, Alarme sonore et Protection contre la surintensité du matériel dans les menus déroulants.
5. Cliquez sur *Enregistrer*.

Tableau 3.13 Paramètres de l'alimentation

Paramètre	Description
Physique	
Connecteur RJ45	Définit le brochage de la voie série : Auto, Cyclades ou Cisco. Valeur par défaut : Auto.
Statut	Définit le statut de la voie série (activé ou désactivé). Valeur par défaut : Désactivé.
Vitesse	Définit la vitesse (1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 ou 230 400). Valeur par défaut : 9 600.
Parité	Définit la parité (Paire, Impaire, Aucune). Valeur par défaut : Aucune.
Bits de données	Définit les bits de données (5, 6, 7 ou 8). Valeur par défaut : 8.
Bits d'arrêt	Définit les bits d'arrêt (1 ou 2). Valeur par défaut : 1.
Contrôle du flux	Définit le contrôle du flux (Aucun, Matériel, Logiciel, Logiciel RxON, Logiciel TxON). Valeur par défaut : Aucun.
Alimentation	
Type d'UPS	Définit le type ou le fournisseur de l'UPS relié à la voie série. Les UPS Liebert GXT4 et Liebert GXT5 sont pris en charge. Valeur par défaut : Liebert GXT4.
Type de PDU	Définit le type ou le fournisseur de la PDU reliée à la voie série. Valeur par défaut : Auto. • Auto : détection du fournisseur. • Avocent-Cyclades : gamme de PM PDU Avocent-Cyclades. • Vertiv : PDU Vertiv. • SPC : gamme de dispositifs de contrôle de l'alimentation SPC. • ServerTech/Server Tech PRO2 : gamme ServerTech. • Raritan : gamme de PDU PX G2 Raritan. • APC : gamme rPDU2 APC. • Eaton : ePDU G3 Eaton. • Geist : gamme de PDU Geist.
Activer la détection automatique de la vitesse	Détecte la vitesse de la voie. Valeur par défaut : Désactivé.
Taux d'interrogation	Indique l'intervalle de mise à jour des informations provenant de la PDU (en secondes). Valeur par défaut : 20.
PDU Avocent/Cyclades	
Intervalle de redémarrage	Indique l'intervalle entre les actions de mise hors tension et de mise sous tension pour la commande de redémarrage (en secondes). Valeur par défaut : 15.
Syslog	Permet à la PDU d'envoyer des messages syslog au matériel. Valeur par défaut : Activé.
Alarme sonore	Permet d'activer ou de désactiver l'alarme sonore de la PDU. Valeur par défaut : Activée.
Protection contre la surintensité du matériel	Permet d'activer la fonction de protection contre la surintensité incluse dans le logiciel. Valeur par défaut : Désactivée.

Pour copier/cloner la configuration d'une voie et l'appliquer aux autres :

1. Sélectionnez *Voies - Voies série*.
2. Cochez la case correspondant à la voie série que vous souhaitez cloner.
3. Cliquez sur le bouton *Cloner*.
4. Indiquez la ou les voies série que vous souhaitez configurer dans le champ Copier la configuration vers, puis cliquez sur *Enregistrer*.

NOTA : si la voie sélectionnée est configurée en tant que profil CAS, les paramètres suivants ne sont pas copiés : Nom de voie, Alias TCP de la voie, Alias IPv4 de la voie, Alias IPv6 de la voie et Alimentation (prises fusionnées).

Pour restaurer la configuration par défaut d'une ou plusieurs voies série :

1. Sélectionnez *Voies - Voies série*.
2. Cochez la case correspondant à la ou aux voies série que vous souhaitez réinitialiser, puis cliquez sur le bouton *Réinitialiser aux valeurs par défaut*.

NOTA : dans la configuration par défaut, les voies série sont définies en tant que profil CAS et désactivées.

Menu Sessions multiples

Les administrateurs peuvent activer ou désactiver le menu Sessions multiples. Lorsqu'il est activé, les utilisateurs peuvent accéder au menu à partir de l'interface utilisateur Web, de l'interface CLI ou du logiciel DSView. Par ailleurs, plusieurs utilisateurs peuvent se connecter simultanément à une même voie série. L'utilisateur doit disposer des droits d'accès à la voie pour pouvoir s'y connecter ou lancer une session partagée. Si plusieurs sessions ont été établies sur une même voie série, le système de console affiche le menu Sessions multiples. Si la session établie est la première sur cette voie série, une session normale avec la cible s'ouvre. L'utilisateur de la première session peut accéder au menu Sessions multiples grâce au raccourci clavier (Ctrl+Z par défaut).

Pour activer le menu Sessions multiples :

1. Dans la barre de navigation latérale de l'onglet *Expert*, cliquez sur *Voies - Voies série*.
2. Cliquez sur la voie pour laquelle vous souhaitez activer le menu Sessions multiples.
3. Cliquez sur la section *CAS* et sélectionnez l'option *Afficher le menu Sessions multiples* dans le menu déroulant situé dans la partie inférieure des paramètres CAS.
4. Cliquez sur *Enregistrer*.

Le menu Sessions multiples comporte des options qui dépendent des droits d'accès de l'utilisateur. Seules les options pour lesquelles l'utilisateur dispose des droits nécessaires s'affichent. Par exemple, seules les options 0, 2 et 5 du tableau ci-dessous s'affichent aux utilisateurs qui disposent uniquement du droit d'ouvrir des sessions en lecture seule.

Tableau 3.14 Options du menu Sessions multiples

Numéro	Option	Description
0	Fermer	Ferme la session client.
1	Lancer une session normale	Ouvre une session en lecture/écriture.
2	Lancer une session en lecture seule	Ouvre une session en lecture seule.
3	Envoyer un message à un autre utilisateur	Permet d'envoyer un message à tous les autres utilisateurs de la voie série.
4	Arrêter les sessions	Affiche toutes les sessions et permet d'arrêter une ou plusieurs sessions partagées.
5	Afficher les sessions partagées	Affiche toutes les autres sessions partagées.
6	Afficher la mise en mémoire tampon des données	Affiche le contenu du fichier cible de mise en mémoire tampon des données.
7	Effacer la mise en mémoire tampon des données	Efface le contenu du fichier cible de mise en mémoire tampon des données.

Voies auxiliaires

Sur l'écran Voies auxiliaires, le nom de voie ttyM1 indique que le modem interne est présent et qu'il est possible de l'activer et de le configurer. Si le tableau des voies auxiliaires est vide, il n'y a pas de modem interne et il n'est pas possible d'utiliser cette voie.

Sur les modèles équipés d'un modem cellulaire, le nom de voie affiche ttyM1 et le type de dispositif LTE. Le modem cellulaire peut uniquement être configuré pour le mode d'accès sortant. Le modem cellulaire est désactivé par défaut. Pour en savoir plus sur la configuration d'un modem cellulaire, reportez-vous à la section Modem cellulaire à la page 59.

Pour configurer ou modifier une voie auxiliaire avec modem interne :

1. Sélectionnez *Voies - Voies auxiliaires*.
2. Cliquez sur le bouton *Définir l'accès entrant* ou *Définir l'accès sortant* et configurez les paramètres d'accès entrant dans les menus déroulants.
3. Configurez les paramètres PPP (adresse, authentification, etc.).
4. Cliquez sur *Enregistrer*.

Profil CAS

Le profil CAS (Console Access Server) offre un accès à distance aux voies de console série RS232 sur vos dispositifs. Il vous permet de configurer l'authentification, la configuration des voies (contrôle de la vitesse et du flux), l'attribution d'alias aux voies, la détection automatique de la cible, le type de mise en mémoire tampon des données, les alertes de voie, l'intégration de l'alimentation, etc.

Les administrateurs peuvent configurer le profil CAS en cliquant sur *Voies - Profil CAS*.

Détection automatique

La fonction de détection automatique permet de détecter le nom de cible du serveur relié à la voie série. Ce nom est alors utilisé en tant qu'alias de la voie série.

Lorsque la détection automatique est activée pour un dispositif série, le matériel envoie des chaînes de sonde et analyse les réponses du dispositif cible en utilisant des expressions régulières une fois la connexion à la cible établie (événement DCD activé). Il utilise des chaînes de sonde et de correspondance à la fois prédéfinies et définies par l'utilisateur.

Pour chaque chaîne de sonde envoyée, toutes les expressions régulières définies par les chaînes de correspondance sont testées. La séquence recommence après le dernier cycle. Cette procédure se poursuit pendant la durée définie par le délai d'expiration de la détection automatique ou jusqu'à la détection de la cible. Si la détection automatique échoue, le nom utilisé pour la cible est celui qui a été configuré ou le nom de cible unique par défaut correspondant.

NOTA : le nom de cible configuré est utilisé uniquement en cas d'échec du processus de détection automatique.

NOTA : le processus de détection automatique démarre lorsque le signal DCD est activé (déconnexion/connexion du câble de la cible, mise hors tension/sous tension de la cible) et lorsque la configuration de la voie série passe de l'état désactivé à activé alors qu'une cible est reliée à la voie.

Les chaînes de sonde sont utilisées pour stimuler le serveur (par exemple « \r » : un seul retour chariot).

Les chaînes de correspondance sont des expressions régulières dans lesquelles « %H » est utilisé comme paramètre fictif pour le nom de la cible que vous souhaitez détecter, par exemple %H .*ogin:

ou xxx%Hyyy

La première commande extrait le nom de la cible, par exemple dans la chaîne MyServer Login: pour afficher le nom de la cible de MyServer.

La deuxième commande affiche le nom de la cible TARGET dans la chaîne Server xxxTARGETyyy.

Pour configurer les chaînes de sonde/correspondance utilisées par la détection automatique :

La procédure ci-dessous vous permet de modifier les paramètres par défaut ou les chaînes de sonde/correspondance utilisées lors de la détection automatique.

1. Sélectionnez *Voies - Profil CAS - Détection automatique*. Les options Paramètres, Chaînes de sonde et Chaînes de correspondance s'affichent dans la barre de navigation latérale.
2. Pour modifier le délai d'expiration par défaut de la détection automatique ou de la sonde, procédez comme suit :
   a. Sélectionnez *Paramètres*.
   b. Saisissez une nouvelle valeur dans les champs Délai d'expiration de détection automatique et Délai d'expiration de sonde.
   c. Sélectionnez une vitesse dans le menu déroulant Vitesse par défaut en cas d'échec de la détection automatique et dans la liste des vitesses des sondes.
   d. Cliquez sur *Enregistrer*.
3. Pour ajouter une nouvelle chaîne de sonde ou de correspondance ou pour supprimer une chaîne existante, procédez comme suit :
   a. Sélectionnez *Chaînes de sonde* ou *Chaînes de correspondance*.
   b. Pour ajouter une chaîne, cliquez sur *Ajouter* et saisissez la nouvelle chaîne dans le champ Nouvelle chaîne de sonde ou Nouvelle chaîne de correspondance, puis cliquez sur *Enregistrer*.
   c. Pour supprimer une chaîne, cochez la case correspondante, puis cliquez sur *Supprimer*.
4. Cliquez sur *Enregistrer*.

Pour configurer les chaînes d'entrée/de sortie utilisées par la réponse automatique :

1. Sélectionnez *Voies - Profil CAS - Réponse automatique*.
2. Pour ajouter des chaînes d'entrée et de sortie de réponse automatique, cliquez sur *Ajouter*.
   Saisissez une nouvelle chaîne dans le champ Chaîne d'entrée ou Chaîne de sortie, puis cliquez sur *Enregistrer*.

   -ou-

   Pour supprimer une chaîne d'entrée ou de sortie de réponse automatique, cochez la case à côté de la chaîne à supprimer. Cliquez sur *Supprimer*, puis sur *Enregistrer*.

Pool de voies

Les administrateurs peuvent créer un pool de voies série dans lequel chaque voie série partage le nom du pool, l'alias Telnet de la voie, l'alias SSH de la voie, l'alias mode brut de la voie, l'alias IPv4 et l'alias IPv6. La première voie disponible du pool sert de voie série pour la connexion.

NOTA : le droit d'accès aux sessions multiples n'a aucun effet lors de l'utilisation d'un pool de voies CAS. Lorsque toutes les voies du pool sont occupées, il est impossible de se connecter au pool.

NOTA : toutes les voies du pool doivent partager le même protocole CAS. Le protocole est validé lors de la connexion à la voie série. Si le protocole ne correspond pas, la connexion ne peut pas être établie.

Pour configurer un pool de voies CAS :

1. Cliquez sur *Voies - Ensemble de voies*.
2. Pour créer un pool, cliquez sur le bouton *Ajouter*.

   -ou-

   Pour modifier un pool existant, cliquez sur le nom du pool.

   -ou-

   Pour supprimer un pool, cochez la case à côté du pool concerné, puis cliquez sur le bouton *Supprimer*.
3. Indiquez les paramètres du pool dans les champs appropriés.
4. À gauche du champ Membres du pool, sélectionnez les voies à ajouter au pool, puis cliquez sur *Ajouter*.

   -ou-

   À droite du champ Membres du pool, sélectionnez les voies à supprimer du pool, puis cliquez sur *Supprimer*.
5. Cliquez sur *Enregistrer*.

NOTA : une voie série ne peut faire partie que d'un seul pool à la fois, mais l'utilisateur peut créer un pool vide et y ajouter des voies ultérieurement.

Tableau 3.15 Paramètres des pools de voies CAS

Paramètre	Description
Nom du pool	Nom attribué au pool. Ce champ est obligatoire et doit respecter les critères pour le nom d'hôte, ne pas contenir plus de 64 caractères et commencer par une lettre.
Alias de la voie	Alias de la voie utilisée par le pool pour répondre à chaque protocole : • Alias Telnet de la voie pour le protocole Telnet. Ce champ est facultatif. • Alias SSH de la voie pour le protocole SSH. Ce champ est facultatif. • Alias mode brut de la voie pour le protocole mode brut. • Ce champ est obligatoire lorsque le mode brut est configuré en tant que protocole pour les voies.
Alias IPv4 du pool	Adresse IPv4 utilisée par le pool. Ce paramètre est facultatif.
Interface de l'alias IPv4 du pool	Interface utilisée par l'alias IPv4. Valeur par défaut : Eth0.
Alias IPv6 du pool	Adresse IPv6 utilisée par le pool. Ce paramètre est facultatif.
Interface de l'alias IPv6 du pool	Interface utilisée par l'alias IPv6. Valeur par défaut : Eth0.

Client RESTful

Le système de console prend en charge une interface client RESTful programmable. Une fois les URL RESTful configurées, le système de console effectue, dans une session série, les opérations GET et POST sélectionnées dans le menu avec les URL HTTP/HTTPS préprogrammées pour les serveurs disponibles sur le réseau.

NOTA : les options d'URL doivent être configurées à l'aide du protocole HTTP ou HTTPS avec le menu client RESTful.

Pour configurer le client RESTful :

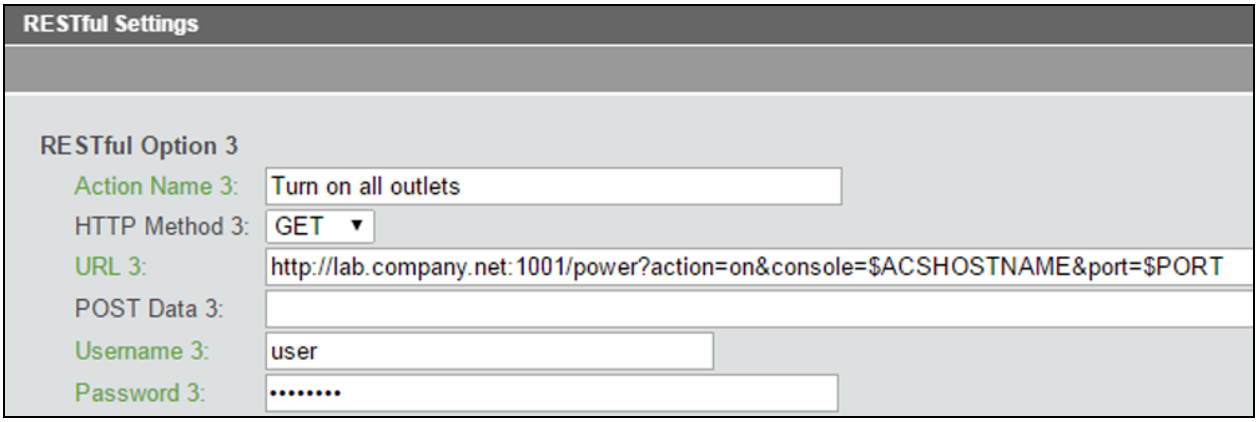
1. Cliquez sur *Voies - Profil CAS - Paramètres RESTful*.
2. Saisissez le nom de l'action, l'URL, les données POST, le nom d'utilisateur et le mot de passe dans les champs appropriés et sélectionnez, dans le menu déroulant, GET ou POST en tant que méthode HTTP pour chacune des options RESTful. Cliquez sur *Enregistrer* lorsque vous avez terminé.

Lors de la configuration des actions, vous pouvez utiliser les variables de contexte ci-dessous.

Tableau 3.16 Description des variables de contexte

Variable de contexte	Description
$PORT	Identification de la voie série (1-48) lors de l'appel du menu.
$PORTNAME	Nom de la voie.
$IPPORTALIAS	Alias IPv4 de la voie.
$TCPPORTALIAS	Alias TCP (voie Telnet) de la voie.
$ACSHOSTNAME	Nom d'hôte du système de console.
$ACSIPADDR	Adresse IP du système de console.

Figure 3.3 Exemple de configuration du client RESTful



NOTA : la requête HTTP POST peut parfois utiliser le corps de la requête HTTP pour envoyer les informations appropriées aux serveurs, généralement avec le code XML ou JSON.

Pour activer le client RESTful :

1. Si l'accès aux voies s'applique à tous les utilisateurs, dans la barre de navigation latérale de l'onglet *Expert*, cliquez sur *Système - Sécurisé - Profil de sécurité*, puis cochez la case Menu RESTful dans la section Dispositifs série et cliquez sur *Enregistrer*.

   -ou-

   Si l'accès aux voies est contrôlé par les autorisations attribuées aux groupes d'utilisateurs, dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Utilisateurs - Autorisation - Groupes*.

   a. Cliquez sur le groupe pour lequel vous souhaitez activer le client RESTful.
   b. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Série*.
   c. Cliquez sur la voie pour laquelle vous souhaitez activer le menu RESTful. Cochez la case Menu RESTful dans Droits d'accès cible.
2. Dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Voies - Voies série*.
3. Cliquez sur la voie pour laquelle vous souhaitez activer le menu RESTful, puis cliquez sur la section CAS dans la partie supérieure de la fenêtre.
4. Saisissez la touche de raccourci que vous souhaitez utiliser pour lancer le client RESTful dans le champ Touche de raccourci RESTful, puis cliquez sur *Enregistrer*.

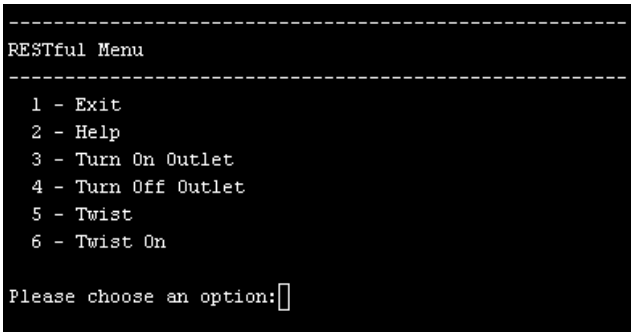
NOTA : la touche de raccourci n'est pas définie par défaut.

Utilisation de l'interface du client RESTful

Après avoir ouvert une session série, appuyez sur la touche de raccourci définie pour ouvrir l'interface du client RESTful pour la session en cours. Indiquez le nombre de requêtes du client RESTful que vous souhaitez effectuer. Exit et Help sont par défaut les deux premières requêtes dans le menu. Vous pouvez configurer jusqu'à huit autres requêtes à partir de l'interface utilisateur Web du système de console.

Voici un exemple du menu RESTful à partir d'une session série.

Figure 3.4 Exemple de client RESTful



Profil d'accès entrant

Les administrateurs peuvent configurer les paramètres d'accès entrant sécurisé, comme la connexion OTP, la connexion PPP, l'authentification PPP/PAP, le rappel et les utilisateurs OTP pour les connexions PPP.

NOTA : si des dispositifs enfichables sont utilisés pour l'accès sortant, l'accès entrant doit être désactivé.

Pour configurer les paramètres d'accès entrant sécurisé aux voies dans le Profil d'accès entrant :

1. Sélectionnez *Voies - Profil d'accès entrant - Paramètres*.
2. Pour activer la connexion au système de console via le modem et sélectionner une condition dans laquelle la connexion est autorisée, procédez comme suit.
   a. Pour autoriser les connexions de rappel uniquement, sélectionnez *Rappel*.
   b. Pour autoriser toutes les connexions, sélectionnez *Activer*.
3. Pour activer l'authentification OTP, sélectionnez *Activer* dans le menu Authentification de connexion OTP.
4. Pour activer et sélectionner une condition pour les connexions PPP, procédez comme suit.
   a. Pour autoriser les connexions de rappel PPP uniquement, sélectionnez *Rappel*.
   b. Pour autoriser toutes les connexions, sélectionnez *Activer*.
5. Lorsque le protocole d'authentification PAP est configuré pour la voie, sélectionnez le type d'authentification dans le menu Authentification PPP/PAP.
6. Activez/désactivez le filtre d'appels dans le menu déroulant.
7. Cliquez sur *Enregistrer*.

Pour configurer les utilisateurs de rappel et les numéros de téléphone pour les voies dans le Profil d'accès entrant :

1. Sélectionnez *Voies - Profil d'accès entrant - Accès entrant sécurisé - Utilisateurs de rappel*.
2. Cliquez sur *Ajouter*.
3. Saisissez le nom et le numéro de téléphone utilisés pour le rappel, puis cliquez sur *Enregistrer*.

Pour configurer les utilisateurs PPP OTP pour les voies dans le Profil d'accès entrant :

1. Sélectionnez *Voies - Profil d'accès entrant - Accès entrant sécurisé - Utilisateurs PPP OTP*.
2. Cliquez sur *Ajouter*.
3. Saisissez le nom d'utilisateur et la phrase secrète dans les champs correspondants, puis cliquez sur *Enregistrer*.

NOTA : cet utilisateur PPP OTP pourra établir une connexion PPP après l'authentification.

Pour configurer EAP-TLS en tant qu'authentification PPP pour les voies dans le Profil d'accès entrant :

1. Sélectionnez *Voies - Voies auxiliaires*.
2. Cochez la case à côté de la voie à laquelle le modem est relié, puis cliquez sur *Définir l'accès entrant*.
3. Configurez les paramètres d'adresse PPP. Par exemple, définissez l'adresse PPP sur Configuration locale, utilisez 10.0.0.1 en tant qu'adresse IPv4 locale et 10.0.0.2 en tant qu'adresse IPv4 distante.
4. Pour configurer l'authentification PPP, sélectionnez le bouton à côté du champ Par matériel, puis celui à côté du champ EAP pour le protocole. Cliquez sur Enregistrer.
5. Sélectionnez *Voies - Profil d'accès entrant - Paramètres*.
6. Activez la connexion PPP dans le menu déroulant, puis cliquez sur *Enregistrer*.
7. Copiez les certificats et les clés dans le répertoire /etc/ppp/cert. Les fichiers doivent être nommés server.crt (certificat ACS 800/8000), ca.crt (certificat émis par l'autorité de certification) et server.key (clé asymétrique ACS 800/8000).

Fonction de présentation du numéro

Vous pouvez filtrer les appels en fonction du numéro en activant le Filtre d'appels dans les paramètres Accès entrant sécurisé. Lorsque le filtre est activé, le numéro de téléphone doit être inclus dans une liste définie pour que l'appel soit pris en charge. Cette option est désactivée par défaut.

Vous pouvez ajouter des numéros directement, par plage ou par préfixe.

Pour ajouter un numéro directement, saisissez-le sans symboles. Par exemple : 8881234567.

Vous pouvez indiquer une plage en ajoutant un tiret (-) entre deux numéros. Tout appel provenant d'un numéro compris dans cette plage sera accepté. Par exemple : 8881234560-8881234569.

NOTA : la plage doit contenir moins de 100 numéros de téléphone.

Vous pouvez indiquer un préfixe en ajoutant un astérisque (*) après un numéro de téléphone partiel. L'appel sera pris en charge si le numéro de téléphone commence par le numéro indiqué. Par exemple : 8881234*.

Si le Filtre d'appels est activé, mais qu'aucun numéro n'est indiqué, tous les appels sont bloqués. Les appels bloqués ne sont pas pris en charge et persistent tant que le délai d'attente n'est pas dépassé. Si la fonction de présentation du numéro est désactivée, tous les appels sont pris en charge.

Pour créer une liste de numéros de téléphone :

1. Sélectionnez *Voies - Profil d'accès entrant - Accès entrant sécurisé - Présentation du numéro*.
2. Cliquez sur *Ajouter* et indiquez le numéro de téléphone, la plage ou le préfixe.
3. Cliquez sur *Enregistrer*.

Pour supprimer un numéro de téléphone de la liste :

1. Sélectionnez *Voies - Profil d'accès entrant - Accès entrant sécurisé - Présentation du numéro*.
2. Cochez la case correspondant au numéro que vous souhaitez supprimer.
3. Cliquez sur *Supprimer*.

Profil d'accès sortant

Pour configurer le profil d'accès sortant pour une voie série reliée à un modem :

1. Sélectionnez *Voies - Voies série*.
2. Cochez la case correspondant à une voie série reliée à un modem.
3. Cliquez sur le bouton *Définir l'accès sortant*.
4. Activez/désactivez la voie dans le menu déroulant.
5. Configurez le numéro de téléphone à composer sur demande dans le champ N° de téléphone.
6. Choisissez la vitesse du modem dans la liste déroulante.
7. Configurez la discussion initiale avec le modem dans le champ Lancer discussion.
8. Configurez les paramètres PPP (adresse, authentification, etc.), puis cliquez sur *Enregistrer*.

NOTA : le profil d'accès sortant établit uniquement la liaison PPP sur demande. L'administrateur doit configurer une route statique pour transmettre les paquets à l'interface PPP.

Tableau 3.17 Paramètres d'accès sortant

Paramètre	Description
Statut	Activation ou désactivation de la voie. Valeur par défaut : désactivée.
N° de téléphone	Numéro de téléphone à composer.
Vitesse	Vitesse utilisée pour configurer le dispositif série et communiquer avec le modem relié.
Lancer discussion	Discussion pour l'initialisation du modem.
Adresse IPv4/IPv6 locale	Configuration de l'adresse IPv4/IPv6 locale pour cette connexion PPP. Si ce champ est vide, la connexion PPP accepte l'adresse de l'homologue distant.
Adresse IPv4/IPv6 distante	Configuration de l'adresse IPv4/IPv6 distante pour cette connexion PPP. Si ce champ est vide, la connexion PPP accepte l'adresse de l'homologue distant.
Protocole d'authentification PPP	Configuration de la partie de la connexion contrôlant cette authentification PPP et sélection de la méthode à utiliser.
Délai d'inactivité PPP	Durée d'inactivité (en secondes) avant expiration de la connexion PPP. Valeur par défaut : 0 (pas de délai d'expiration).
CHAP	Configuration des paramètres d'authentification PPP CHAP.

Profil de connecteur client

Pour configurer le profil de connecteur client pour une voie série reliée à un dispositif :

1. Sélectionnez *Voies - Voies série*.
2. Cochez la case correspondant à une voie série reliée à un dispositif.
3. Cliquez sur *Définir comme connecteur client* et configurez les paramètres physiques à l'aide des menus déroulants.
4. Configurez les paramètres de connecteur client (adresse de serveur distant, voie TCP et déclencheur d'événement), puis cliquez sur *Enregistrer*.

Tableau 3.18 Paramètres de connecteur client

Paramètre	Description
Connecteur RJ45	Définit le brochage de la voie série.
Statut	Définit le statut de la voie série (activé ou désactivé). Valeur par défaut : Désactivé.
Vitesse	Définit la vitesse (1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 ou 230 400). Valeur par défaut : 9 600.
Parité	Définit la parité (Paire, Impaire, Aucune). Valeur par défaut : Aucune.
Bits de données	Définit les bits de données (5, 6, 7 ou 8). Valeur par défaut : 8.
Bits d'arrêt	Définit les bits d'arrêt (1 ou 2). Valeur par défaut : 1.
Contrôle du flux	Définit le contrôle du flux (Aucun, Matériel, Logiciel, Logiciel RxON, Logiciel TxON). Valeur par défaut : Aucun.
Serveur distant	Définit l'adresse IPv4 ou IPv6 du serveur distant.
Voie TCP distante	Indique la voie TCP à utiliser pour établir une connexion avec un serveur distant.
Établir connexion	Permet de configurer l'événement qui va déclencher la connexion : Sensibilité DCD ou Toujours.

3.3.8 Modem cellulaire

La configuration du modem cellulaire du système de console avancé Avocent® ACS 800/8000 est similaire à l'interface de configuration du modem 56k interne. La configuration du modem cellulaire s'effectue par le biais de la voie auxiliaire du système de console.

Pour configurer ou modifier une voie auxiliaire avec modem cellulaire :

1. Sélectionnez *Voies - Voies auxiliaires*.
2. Cliquez sur le lien *ttyM1* pour afficher la page de configuration de l'accès sortant du modem.

NOTA : il n'est possible de configurer le modem cellulaire que pour le mode d'accès sortant.

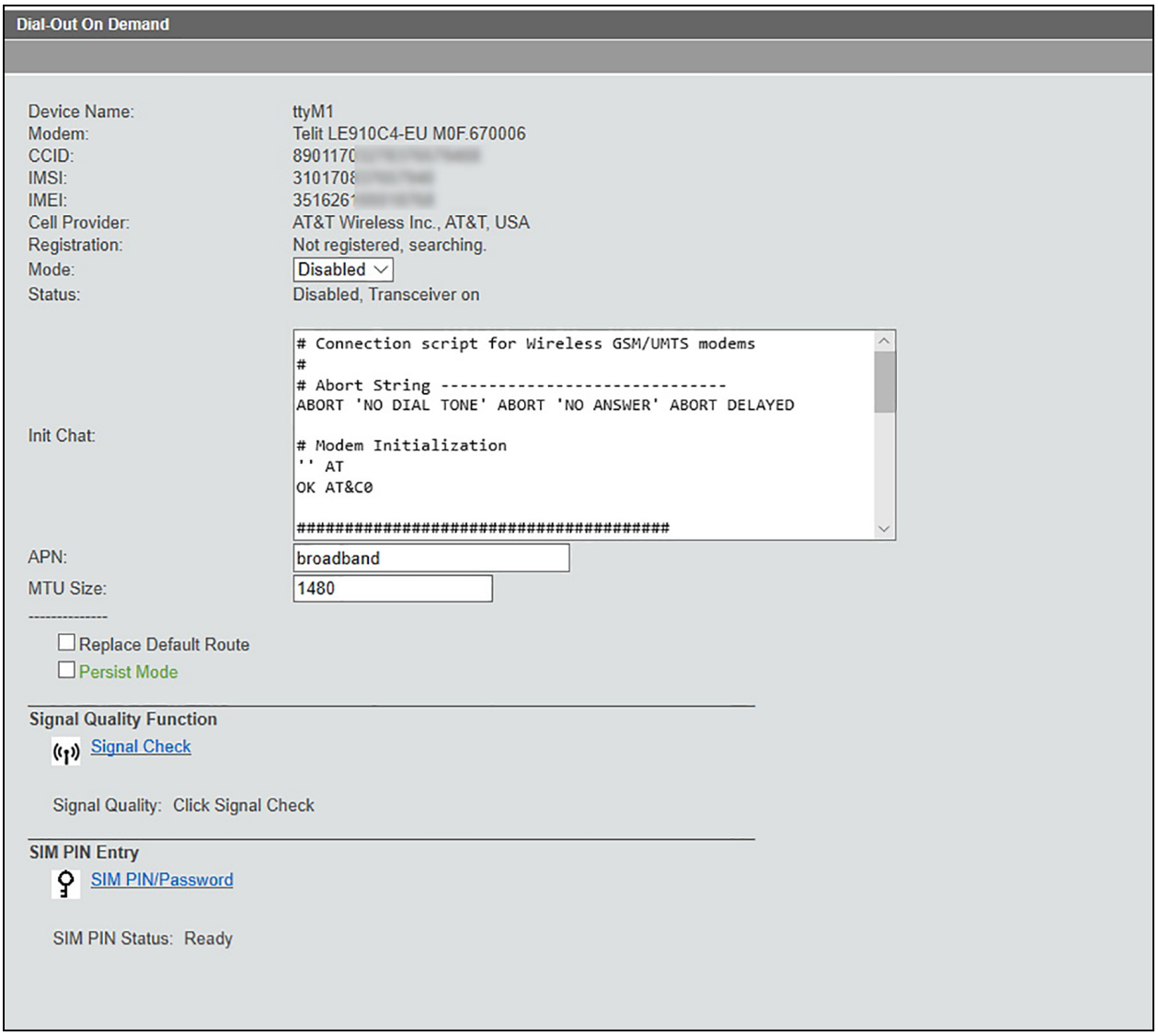
3. Utilisez le menu déroulant pour activer le modem. Lorsqu'il est activé, le modem démarre après chaque redémarrage du système.
4. Le contenu du script de discussion est défini par défaut par le fournisseur. Vous pouvez le modifier si vous le souhaitez dans la fenêtre Lancer discussion.
5. Le champ APN indique le nom du point d'accès par défaut. Il vous permet de modifier l'APN directement, sans passer par le script de discussion.

NOTA : si vous modifiez l'APN, toutes les modifications apportées au script de discussion seront perdues.

6. Activez ou désactivez l'option permettant de remplacer la route par défaut.
7. Activez ou désactivez le mode persistant.

Pour en savoir plus sur la configuration du modem cellulaire, reportez-vous aux sections ci-après.

Figure 3.5 Page de configuration de l'accès sortant pour le modem cellulaire



Les numéros CCID et IMSI de la carte SIM sont indiqués dans la partie supérieure de l'écran. Si ces numéros ne sont pas indiqués ou s'ils ne sont pas valides, cela signifie qu'un problème est survenu lors de la lecture de la carte SIM. Vérifiez que la carte SIM est installée correctement. Le numéro IMEI provient du jeu de puces du modem cellulaire.

Mode

La sélection du mode est désactivée par défaut. Si vous l'activez, le démon du protocole point à point (pppd) démarre et active le modem cellulaire. Lorsque cette option est activée, le modem cellulaire démarre après chaque redémarrage du système.

En mode de basculement, le modem cellulaire démarre même s'il est désactivé. Les conditions de basculement restent activées.

Statut

La ligne de statut indique l'état actuel :

- Désactivé ou Activé – Indique si le modem cellulaire est activé ou désactivé. Le modem peut être activé manuellement ou par basculement.
- Émetteur-récepteur désactivé – Paramètre par défaut. L'émetteur-récepteur est désactivé lorsque le modem l'est également.
- Émetteur-récepteur activé – L'émetteur-récepteur est activé lorsque le modem l'est également, que ce soit manuellement ou par basculement.
- Basculement : non – Si le modem est configuré comme dispositif de basculement, cela indique s'il est en mode de basculement.
- Marche ou arrêt – Indique si l'interface réseau du modem est en état de marche.

Lancer discussion

Il s'agit du script de discussion, qui se présente dans une fenêtre d'édition. Vous pouvez modifier le script de discussion dans cette fenêtre. Le contenu du script de discussion par défaut est défini par le fournisseur de services.

NOTA : la plupart des utilisateurs peuvent utiliser le script de discussion par défaut.

APN

Il s'agit du nom du point d'accès indiqué dans le script de discussion. Ce champ vous permet de modifier l'APN, sans passer par le script de discussion. Si vous modifiez l'APN ici, toutes les modifications apportées au script de discussion seront perdues.

Remplacer la route par défaut

Cette fonction envoie une option de configuration au démon ppp pour faire du modem cellulaire la passerelle par défaut. La passerelle est restaurée lorsque le modem cellulaire est arrêté. Le résultat est similaire à celui que vous obtenez lorsque vous indiquez une route statique, mais cette option est utile pour faire du modem cellulaire la passerelle par défaut pour le basculement.

Mode persistant

Lorsque le mode persistant est activé, le système de console tente de redémarrer le modem cellulaire si le démon ppp cesse de fonctionner pour une raison ou une autre. Lorsque cette option est désactivée et que le démon ppp cesse de fonctionner (par exemple, en cas de perte du service cellulaire), le modem cellulaire ne s'active pas.

Contrôle de la qualité du signal

Cette fonction permet d'obtenir le niveau de signal brut et des informations sur le taux d'erreur binaire pour diagnostiquer les problèmes de connexion au réseau cellulaire ou de connexion lente. Cliquez sur *Vérification du signal* pour obtenir une réponse.

Le niveau du signal peut aller de -113 db ou moins à -51 db ou plus. Le taux d'erreur binaire peut aller de moins de 1 % à 12,8 % ou plus.

Il n'est pas possible de vérifier la qualité du signal lorsqu'une session modem est en cours. L'émetteur-récepteur du modem est activé, mais le script de discussion n'est pas actif. Lors d'une session, l'interface série du modem cellulaire est verrouillée au démon ppp.

Saisie du code PIN de la carte SIM

Cliquez sur *Mot de passe/PIN SIM* pour saisir votre code PIN afin d'activer le service cellulaire avec une carte SIM.

Vérification de la connexion cellulaire

La ligne de statut sur l'écran de l'accès sortant indique si le modem cellulaire est en marche. Vous pouvez obtenir l'adresse IP du modem cellulaire sur la page Surveillance. Cliquez sur *Surveillance - Réseau - Dispositifs*.

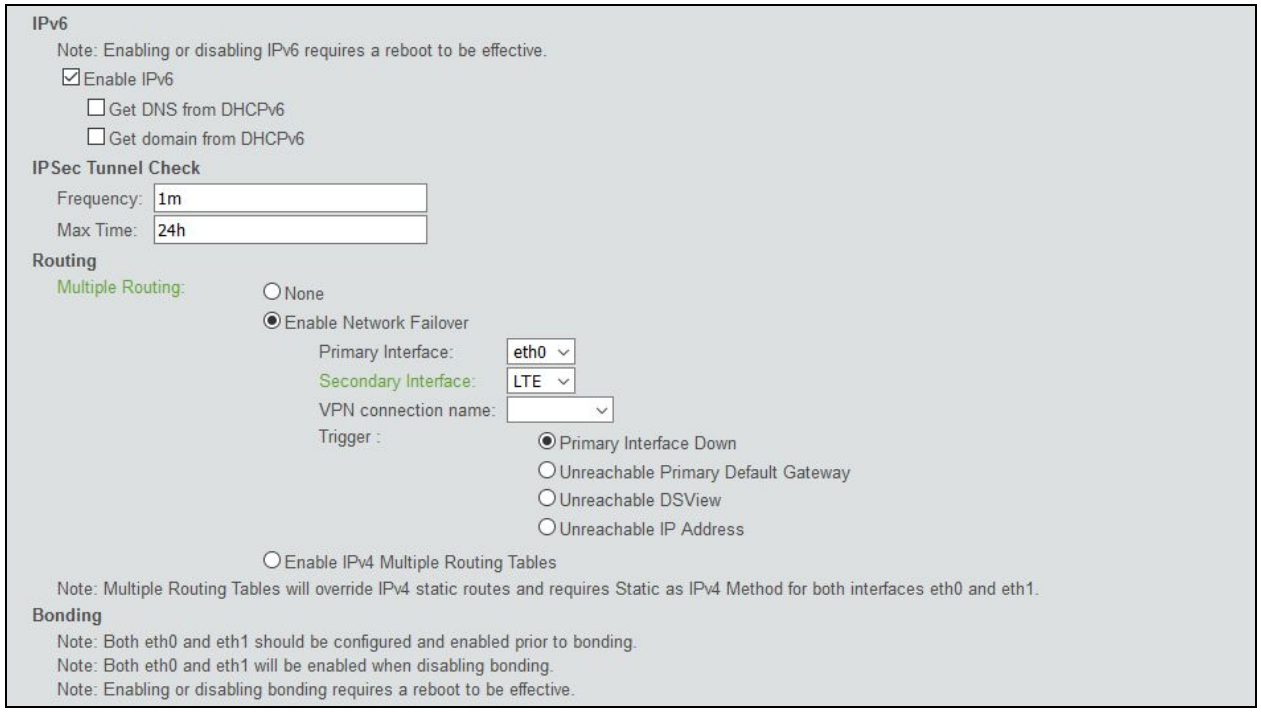
Sur la page Dispositifs, le dispositif ppp0-LTE correspond au modem. L'adresse IPv4 s'affiche avec le statut de la liaison lorsque le modem est activé. L'adresse IP est pour le service réseau privé. L'adresse IPv4 n'est pas fixe et change à chaque fois que vous redémarrez ou rétablissez la connexion au réseau cellulaire.

NOTA : les utilisateurs avancés peuvent exécuter un script pour obtenir de plus amples informations de débogage.

Utilisation du modem cellulaire à des fins de basculement

Cliquez sur *Réseau - Paramètres* et sélectionnez *Routage - Activer le basculement réseau*. Sélectionnez le dispositif ppp0 (ou lte0) dans la liste Interface secondaire. Vous pouvez effectuer cette procédure que le modem soit activé ou non.

Figure 3.6 Configuration du modem cellulaire en tant que dispositif de basculement



Dans l'exemple ci-dessus, la condition de basculement est une panne de l'interface principale. Lorsque le basculement est activé, le modem cellulaire prend le relais en cas de problème avec eth0. Si le problème survient au niveau du fournisseur de services, cette option fournit uniquement l'accès à Internet. Un serveur sur Internet ne peut pas se connecter directement. Un autre type de service, ou fournisseur, peut fournir l'accès.

Il est également possible d'utiliser un service VPN. Configurez le VPN pour vous connecter à une passerelle sécurisée via IPsec avec une adresse IP publique et ainsi accéder au système de console par l'intermédiaire du tunnel IPsec.

Pour configurer IPsec :

1. Activez le service IPsec. Rendez-vous sur la page *Système - Sécurisé - Profil de sécurité* et cochez la case Activer IPSec en bas de la page.
2. Rendez-vous sur la page *Réseau - IPSec (VPN)* et ajoutez un nouveau profil VPN.
3. Saisissez les paramètres du VPN. L'image ci-dessous fournit un exemple. Lorsque vous avez terminé, cliquez sur *Enregistrer*.
4. Revenez à l'écran de basculement sur la page *Réseau - Paramètres* et sélectionnez le VPN pour le basculement.

Figure 3.7 Exemple de configuration du VPN IPsec

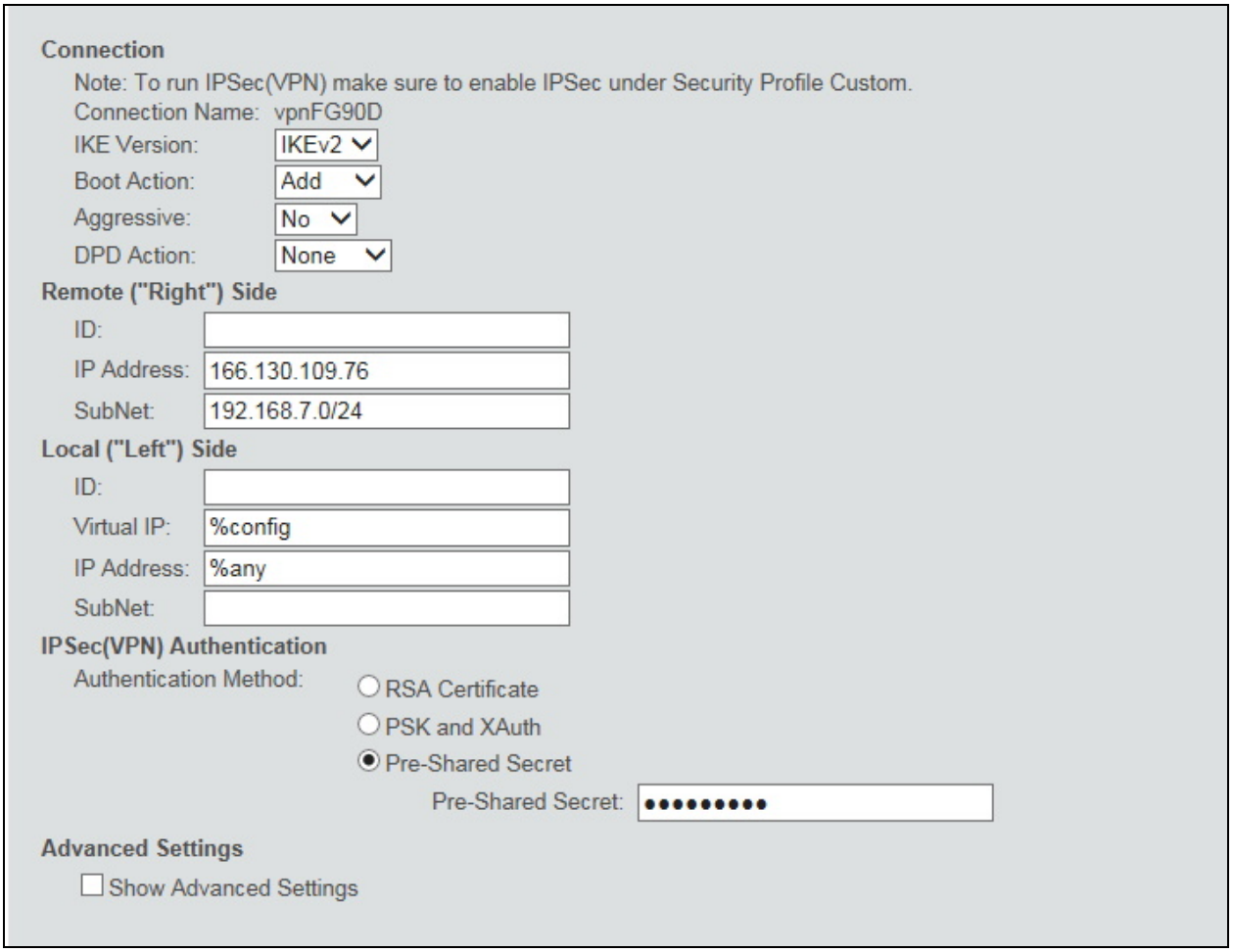
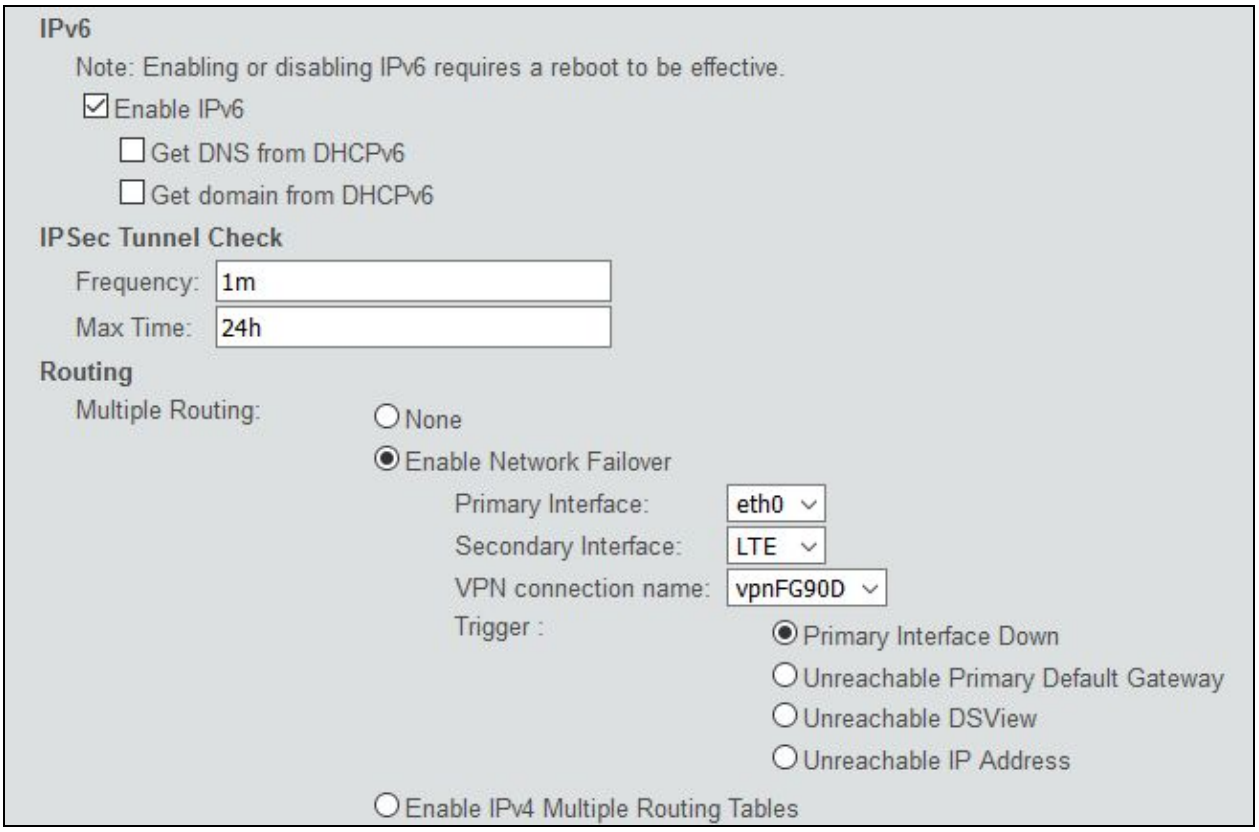


Tableau 3.19 Description d'IPsec

Élément	Description
Version IKE	En général IKEv2 sauf si la passerelle de connexion est obsolète.
Action de démarrage	Sélectionnez Ajouter pour le basculement. Si vous définissez cette option sur Démarrer, le VPN tente de prendre la relève dès le démarrage du système de console.
Mode agressif	Cette option doit être définie sur Non.
Action DPD	Aucune. Il est possible de définir cette option sur Redémarrer. L'acronyme DPD signifie « Dead Peer Detection ».
ID	Laissez ce champ vide pour permettre l'identification de la passerelle distante grâce à l'adresse IP.
Sous-réseau	Il s'agit du sous-réseau auquel nous souhaitons accéder par l'intermédiaire d'une passerelle sécurisée distante. Dans ce cas, nous utilisons un pare-feu Fortigate et son sous-réseau LAN.
Côté local ("gauche")	
ID	Les ID permettent d'identifier chaque côté. Si vous laissez ce champ vide, l'adresse IP est utilisée.
IP virtuelle	Cette option attribue l'adresse IP au tunnel. En la définissant sur **%config**, nous obtenons une adresse à partir de la passerelle sécurisée distante.
Adresse IP	Il s'agit de l'adresse IP du système de console participant au tunnel. Pour une connexion Ethernet standard, vous pouvez choisir une adresse IP fixe. Dans le cas du modem cellulaire, le fournisseur attribue une adresse IP qui peut changer, comme c'est le cas avec le fournisseur AT&T. Vous pouvez sélectionner **%any** pour utiliser n'importe quelle interface ou adresse IP disponible.
Authentification IPSec (VPN)	Sélectionnez Secret pré-partagé pour utiliser une clé de sécurité/un mot de passe unique pour le tunnel. Chaque côté de ce tunnel IPsec doit utiliser le même mot de passe/mot secret. Bien évidemment, vous pouvez également utiliser des certificats X509/RSA.
Paramètres avancés	Laissez les paramètres par défaut afin qu'IPSec puisse négocier la suite de chiffrement.

Figure 3.8 Exemple de VPN sélectionné pour le basculement



Avec l'option Remplacer la route par défaut, un événement de basculement (par exemple, eth0 tombe en panne) déclenche le modem cellulaire et démarre le VPN. Les clients LAN sur la passerelle distante peuvent accéder au système de console via l'adresse IP virtuelle du tunnel.

3.3.9 Dispositifs enfichables

Le système de console prend en charge divers dispositifs enfichables reliés à ses voies USB. Certains modèles permettent également d'insérer une carte SD dans l'emplacement prévu à cet effet.

NOTA : si un dispositif enfichable ne se trouve pas dans la liste des dispositifs actuellement pris en charge, le système de console peut tenter de le configurer avec les paramètres standard pour permettre un fonctionnement normal. Par ailleurs, lorsqu'un dispositif enfichable n'est pas présent dans la base de données interne, la colonne Infos sur le dispositif peut être vide ou indiquer diverses informations en fonction du type de carte, par exemple Dispositif inconnu f024 (rev 01).

Pour installer et détecter un dispositif enfichable :

1. Dans la barre de navigation latérale, sélectionnez *Dispositifs enfichables*.
2. Cliquez sur *Activer la détection des dispositifs enfichables* pour détecter les dispositifs enfichables reliés, à moins d'avoir déjà activé cette option sur la page Système - Sécurisé.
3. Connectez un dispositif à une voie USB ou insérez une carte SD dans l'emplacement prévu à cet effet du système de console.
4. Le tableau des dispositifs enfichables affiche tous les dispositifs détectés.

NOTA : pour désactiver cette option, cliquez sur *Désactiver la détection des dispositifs enfichables*.

Pour éjecter ou supprimer un dispositif enfichable :

1. Dans la barre de navigation latérale, sélectionnez *Dispositifs enfichables*.
2. Cochez la case à côté du dispositif enfichable que vous souhaitez éjecter ou supprimer.
3. Cliquez sur *Éjecter* ou *Supprimer*. Cliquez sur *Enregistrer*.

NOTA : pensez à toujours éjecter le dispositif enfichable à partir de l'interface utilisateur Web avant de le retirer physiquement.

Configuration du dispositif

Les dispositifs de stockage sont montés et configurés automatiquement une fois qu'ils ont été détectés par le système de console, à moins que la prise en charge des dispositifs de stockage ne soit désactivée. Les cartes Ethernet, les modems et les consoles USB doivent être configurés.

NOTA : la configuration des dispositifs sans fil ne prend effet qu'une fois le dispositif éjecté puis réinséré.

Pour configurer un dispositif enfichable :

1. Dans la barre de navigation latérale, cliquez sur *Dispositifs enfichables*.
2. Dans le cas d'un dispositif réseau, cliquez sur son nom pour configurer ses paramètres réseau.

   -ou-

   Dans le cas d'un modem (V.92), cochez la case à côté de son nom, puis cliquez sur *Définir l'accès entrant* ou *Définir l'accès sortant* pour configurer ses paramètres d'accès entrant ou sortant.

   -ou-

   Dans le cas d'une console USB, cochez la case à côté de son nom, puis cliquez sur *Définir la console* pour l'ajouter au système en tant que nouvelle voie. Vous pouvez accepter la voie attribuée par défaut ou indiquer une voie libre dans le champ Voie et cliquer sur *Attribuer*. Rendez-vous ensuite sur la page *Voies - Voies série* pour configurer et activer cette voie.

Mappage de consoles USB

La voie utilisée par défaut par les consoles USB dépend du nombre de voies série présentes sur le système de console. Le tableau suivant indique les voies attribuées par défaut.

Tableau 3.20 Mappage de consoles USB sur un ACS80X

	Voies USB			
MODÈLE	En haut à gauche	En bas à gauche	En haut à droite	En bas à droite
ACS 802	3	4	5	6
ACS 804	5	6	7	8
ACS 808	9	10	11	12

Tableau 3.21 Mappage de consoles USB sur un ACS80XX

	Voies USB à l'arrière						Voies USB à l'avant	
Modèle	En haut à gauche	En bas à gauche	En haut au milieu	En bas au milieu	En haut à droite	En bas à droite	En haut	En bas
ACS 8008	9	10	11	12	13	14	15	16
ACS 8016	17	18	19	20	21	22	23	24
ACS 8032	33	34	35	36	37	38	39	40
ACS 8048	49	50	51	52	53	54	55	56

Si la voie attribuée par défaut est déjà utilisée ou si le dispositif USB n'est pas branché directement sur le système de console, la prochaine voie disponible après la voie réservée sera utilisée. Par exemple, sur un système de console ACS808 , la voie 13 est la prochaine voie disponible.

Connexion à chaud

Il est possible de débrancher puis de rebrancher des consoles séries sur la même voie USB sans interrompre les sessions série ouvertes. Dans la plupart des cas, le dispositif USB reçoit le même nom de dispositif attribué par Linux. Dans certains cas, un autre nom de dispositif est attribué si le nom d'origine est déjà utilisé.

NOTA : le dispositif doit être rebranché sur la même voie qu'avant pour que la connexion à chaud soit possible.

3.3.10 Authentification

Il est possible de procéder à l'authentification localement, avec un mot de passe à usage unique (OTP), ou à distance sur un serveur d'authentification LDAP, Radius, Kerberos ou TACACS+. Si le système de console est géré par un serveur DSView, l'authentification DSView est également possible. Le système de console prend également en charge les autorisations de groupes distantes pour les méthodes d'authentification LDAP, RADIUS, Kerberos et TACACS+.

Les mécanismes de secours suivants sont disponibles :

Vous pouvez d'abord tenter l'authentification locale, puis à distance si la première échoue (Méthode_ locale/distance).

-ou-

Vous pouvez d'abord tenter l'authentification à distance, puis l'authentification locale (Méthode_ distance/locale).

-ou-

Vous pouvez tenter l'authentification locale uniquement si un serveur d'authentification à distance est défaillant (méthode_distance_défaillance_local).

Les administrateurs peuvent configurer l'authentification grâce à l'utilitaire CLI et à l'interface utilisateur Web. L'authentification locale est la méthode par défaut pour le système de console et les voies série. La méthode d'authentification configurée pour le système de console ou les voies est utilisée pour l'authentification de tous les utilisateurs qui tentent de se connecter via Telnet, SSH ou l'interface utilisateur Web.

Authentification du matériel

Le système de console s'authentifie lui-même et authentifie les voies, individuellement ou en groupes.

NOTA : si vous utilisez des autorisations de groupe, nous vous recommandons d'utiliser la même authentification pour le système de console et toutes les voies série, ou d'utiliser l'authentification unique pour les autorisations de groupe.

Lorsque l'authentification unique est désactivée, le système de console utilise la configuration individuelle en fonction de la destination de l'accès, à savoir le système de console lui-même ou chaque voie série. Les utilisateurs doivent saisir leur mot de passe à chaque fois qu'ils accèdent à une voie individuelle. Si elle est activée, l'authentification unique utilise le serveur d'authentification sélectionné dans le menu déroulant pour tous les accès. Aucune authentification ultérieure n'est nécessaire.

NOTA : si vous sélectionnez *non configuré* dans le menu déroulant, les voies continuent à utiliser les serveurs d'authentification individuels et vous devez saisir votre mot de passe la première fois que vous accédez à une voie. Vous n'aurez plus à le faire par la suite si l'option Authentification unique est activée.

Pour définir le type d'authentification pour le système de console :

1. Cliquez sur *Matériel - Authentification du matériel*.
2. Sélectionnez le serveur d'authentification souhaité dans le menu déroulant Type d'authentification.
3. Sélectionnez *Activer le secours sur le type Local pour l'utilisateur racine sur la voie console du matériel* lorsque l'authentification à distance échoue et qu'un administrateur souhaite accéder au matériel en tant qu'utilisateur racine via le voie console.
4. Cliquez sur *Activer l'authentification unique* et sélectionnez le serveur d'authentification souhaité dans le menu déroulant Type d'authentification.
5. Cliquez sur *Enregistrer*.

Serveurs d'authentification

Lorsque vous utilisez un serveur d'authentification, vous devez configurer son adresse IP et, dans la plupart des cas, d'autres paramètres avant de pouvoir l'utiliser. Voici les serveurs d'authentification qui doivent être configurés : RADIUS, TACACS+, LDAP(S)|AD, Kerberos, et DSView.

Pour configurer un serveur d'authentification RADIUS :

1. Sélectionnez *Authentification - Serveurs d'authentification - RADIUS*.
2. Saisissez l'adresse IP du premier serveur d'authentification et du premier serveur de gestion de comptes.
3. Si nécessaire, saisissez l'adresse IP du second serveur d'authentification et du second serveur de gestion de comptes.
4. Saisissez votre mot secret ou phrase secrète dans le champ Secret (s'applique aux première et seconde authentifications et aux premier et second serveurs de gestion de comptes), puis confirmez-les dans le champ Confirmer le secret.
5. Dans le champ Délai d'expiration, indiquez la durée en secondes souhaitée pour le délai d'expiration du serveur.
6. Dans le champ Nouvelles tentatives, indiquez le nombre de tentatives souhaité.

7. Si vous cochez la case *Activer l'attribut ServiceType pour spécifier le groupe d'autorisation*, indiquez le nom du groupe d'autorisation pour chacun des types de services suivants : connexion, tramé, rappel pour connexion, rappel tramé, sortant et administratif.
8. Cliquez sur *Enregistrer*.

Pour configurer un service d'authentification TACACS+ :

1. Sélectionnez *Authentification - Serveurs d'authentification - TACACS+*.
2. Saisissez l'adresse IP du premier serveur d'authentification et du premier serveur de gestion de comptes.
3. Si nécessaire, saisissez l'adresse IP du second serveur d'authentification et du second serveur de gestion de comptes.
4. Sélectionnez le service souhaité (PPP ou accès en lecture seule) dans le menu déroulant Service.
5. Saisissez votre mot secret ou phrase secrète dans le champ Secret (s'applique aux première et seconde authentifications et aux premier et second serveurs de gestion de comptes), puis confirmez-les dans le champ Confirmer le secret.
6. Dans le champ Délai d'expiration, indiquez la durée en secondes souhaitée pour le délai d'expiration du serveur.
7. Dans le champ Nouvelles tentatives, indiquez le nombre de tentatives souhaité.
8. Si vous cochez la case *Activer l'attribut User-Level pour spécifier le groupe d'autorisation*, indiquez le nom du groupe d'autorisation pour 15 niveaux d'utilisateurs maximum.
9. Cliquez sur *Enregistrer*.

Pour configurer un serveur d'authentification LDAP(S)|AD :

1. Sélectionnez *Authentification - Serveurs d'authentification - LDAP(S)|AD*.
2. Saisissez l'adresse IP du serveur.
3. Indiquez la base.
4. Dans le menu déroulant Sécurisé, sélectionnez *Désactiver*, *Activer* ou *Start_TLS*.
5. Saisissez le nom d'utilisateur de base de données.
6. Saisissez votre mot de passe de base de données, puis confirmez-le dans le champ Confirmer le mot de passe.
7. Saisissez les attributs de connexion souhaités.
8. Cliquez sur *Enregistrer*.

Pour configurer un serveur d'authentification Kerberos :

1. Sélectionnez *Authentification - Serveurs d'authentification - Kerberos*.
2. Saisissez l'adresse IP (Realm) du serveur.
3. Saisissez le nom de domaine Realm (par exemple, AVOCENT.com).
4. Saisissez le nom de domaine (par exemple, .avocent.com).
5. Cliquez sur *Enregistrer*.

Pour configurer un serveur d'authentification DSView :

1. Sélectionnez *Authentification - Serveurs d'authentification - DSView*.
2. Saisissez les adresses IP 1 à 4 des serveurs DSView dans les champs correspondants.

3. Cliquez sur *Enregistrer*.

3.3.11 Comptes utilisateurs et groupes d'utilisateurs

Il est possible de gérer l'accès aux voies et autres droits sur la base d'autorisations attribuées par un administrateur aux groupes d'utilisateurs personnalisés ou aux comptes utilisateurs individuels.

Vous pouvez également autoriser les groupes et les utilisateurs à gérer l'alimentation pendant qu'ils sont connectés aux dispositifs. Le système de console prévoit deux utilisateurs par défaut (admin et racine) et quatre groupes d'utilisateurs prédéfinis : admin, appliance-admin, shell-login-profile et user.

Il est possible de définir un compte utilisateur pour chaque utilisateur sur le système de console ou sur un serveur d'authentification. L'administrateur et les utilisateurs racines disposent de comptes par défaut. Chaque administrateur peut ajouter et configurer d'autres comptes utilisateurs. Chaque compte utilisateur local est attribué à un ou plusieurs groupes d'utilisateurs.

NOTA : lorsque vous supprimez un utilisateur de tous les groupes, ses droits sont alors ceux du groupe d'utilisateurs par défaut. C'est pour cette raison que nous recommandons d'utiliser des groupes personnalisés et de ne pas attribuer de droits supplémentaires au groupe d'utilisateurs par défaut.

Par défaut, tous les utilisateurs peuvent accéder à toutes les voies du système de console. Pour autoriser l'accès via les groupes d'utilisateurs, l'administrateur doit activer le contrôle de l'accès aux voies par les autorisations attribuées aux groupes d'utilisateurs.

Pour activer le contrôle de l'accès aux voies par les autorisations attribuées aux groupes d'utilisateurs :

1. Dans la barre de navigation latérale de l'onglet Expert, cliquez sur *Système - Sécurisé - Profil de sécurité*.
2. Dans la section Dispositifs série, cliquez sur le bouton Contrôlé par les droits d'accès attribués aux groupes d'utilisateurs et aux utilisateurs spécifiques, puis cliquez sur *Enregistrer*.

Comptes locaux

Le système de console inclut deux comptes utilisateurs locaux par défaut :

- admin : effectue la configuration réseau initiale. L'utilisateur admin est membre du groupe admin. Il peut configurer le système de console et les voies, ainsi que les autorisations des utilisateurs et des groupes.
- racine : dispose des mêmes autorisations administratives que l'utilisateur admin, mais également de droits illimités au shell. L'utilisateur racine est membre des groupes admin et shell-login-profile. Lorsqu'un utilisateur racine se connecte via la voie CONSOLE, SSH ou Telnet, la session est prédéfinie par le profil de connexion pour aller directement au shell. Il est possible de personnaliser le profil de connexion pour ne pas aller directement au shell.

Pour consulter les droits d'accès au matériel de l'utilisateur :

1. Cliquez sur *Utilisateurs - Comptes locaux - Noms d'utilisateur*. La liste des noms d'utilisateurs s'affiche dans la zone de contenu.
2. Cliquez sur un nom d'utilisateur dans la section correspondante. La zone de contenu affiche les informations concernant l'utilisateur sélectionné.

NOTA : lorsque vous sélectionnez un nom d'utilisateur, la zone de contenu et la barre de navigation latérale changent. La barre de navigation latérale affiche des options de menu spécifiques pour les sections Membres et Droits d'accès (dont Série, Alimentation et Matériel).

3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Série* ou *Droits d'accès - Alimentation* pour afficher les écrans contenant les droits d'accès et les autorisations fixes de l'utilisateur sélectionné.

NOTA : les écrans Série et Alimentation sont en lecture seule et leur contenu ne peut pas être modifié.

4. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Matériel*. L'écran Droits d'accès au matériel s'affiche et indique tous les droits d'accès disponibles pour l'utilisateur. Les droits d'accès au matériel disponibles sont :
   - Afficher les informations du matériel
   - Déconnecter les sessions
   - Redémarrer le matériel
   - Mettre à niveau la mémoire flash du matériel et redémarrer le matériel
   - Configurer les paramètres du matériel
   - Configurer les comptes utilisateur
   - Sauvegarder/Restaurer la configuration
   - Accéder au shell
   - Transférer les fichiers
   - Accès entrant

Pour ajouter de nouveaux utilisateurs :

1. Cliquez sur *Utilisateurs - Comptes locaux - Noms d'utilisateur*. L'écran Noms d'utilisateur affiche la liste de tous les utilisateurs.
2. Cliquez sur *Ajouter*. L'écran Informations utilisateur local s'affiche.
3. Saisissez le nom d'utilisateur et un mot de passe, puis confirmez le mot de passe.
4. Cochez ou décochez la case *L'utilisateur doit modifier le mot de passe à la prochaine connexion*.
5. Pour ajouter l'utilisateur à un groupe d'utilisateurs disponible, sélectionnez le nom du groupe d'utilisateurs à gauche, puis cliquez sur *Ajouter* (le groupe par défaut est « user »). Vous pouvez supprimer un groupe d'utilisateurs de la section de droite. Pour ce faire, sélectionnez le groupe, puis cliquez sur *Supprimer*.
6. Indiquez les paramètres souhaités dans la section Expiration du mot de passe.
   - Jours min : indiquez le nombre minimal de jours devant s'écouler avant la modification du mot de passe. Toute tentative de modification du mot de passe avant ce délai sera rejetée. Laissez ce champ vide si vous souhaitez désactiver la restriction concernant le nombre de jours devant s'écouler avant la nouvelle modification du mot de passe.
   - Jours max : indiquez le nombre maximal de jours pendant lesquels le mot de passe est valide. Après cette période, le mot de passe doit être modifié. Laissez ce champ vide si vous souhaitez désactiver la restriction concernant le nombre maximal de jours pendant lesquels un mot de passe est valide.

- Jours d'avertissement : indiquez le nombre de jours qui doivent s'écouler avant l'affichage d'un avertissement indiquant l'expiration prochaine du mot de passe. Si la valeur est 0, l'avertissement s'affiche le jour de l'expiration. Laissez ce champ vide pour désactiver l'avertissement.

7. Indiquez la date d'expiration du compte souhaitée (AAAA-MM-JJ).
8. Cliquez sur *Enregistrer*.

Pour configurer les règles de mot de passe :

1. Cliquez sur *Utilisateurs - Comptes locaux - Règles de mot de passe*.
2. Pour n'accepter que des mots de passe complexes (option recommandée), sélectionnez *Vérifier la complexité du mot de passe*.
3. Si la complexité du mot de passe est activée, indiquez les valeurs souhaitées.
4. Saisissez les valeurs souhaitées dans le champ Expiration par défaut.
5. Cliquez sur *Enregistrer*.

Groupes d'utilisateurs

Les groupes d'utilisateurs disposent des droits d'accès et des autorisations prévus par défaut ou attribués par un administrateur. Les administrateurs peuvent modifier les autorisations et les droits d'accès des utilisateurs appartenant aux groupes appliance-admin ou user. Ils peuvent également créer des groupes supplémentaires avec des autorisations et des droits d'accès personnalisés. Les administrateurs peuvent à tout moment ajouter, supprimer ou modifier les autorisations et les droits d'accès des utilisateurs d'un groupe.

Si un administrateur restreint l'accès des utilisateurs aux voies du système de console, il peut ajouter des utilisateurs aux groupes qui sont autorisés à y accéder. L'administrateur peut également autoriser des groupes à gérer l'alimentation et les tampons de données.

Le présent document et logiciel concernent les utilisateurs dont le compte est configuré sur les serveurs d'authentification à distance (utilisateurs distants). Les utilisateurs distants n'ont pas besoin de comptes locaux.

NOTA : lorsque vous supprimez un utilisateur de tous les groupes, ses droits sont alors ceux du groupe d'utilisateurs par défaut. C'est pour cette raison que nous recommandons d'utiliser des groupes personnalisés et de ne pas attribuer de droits supplémentaires au groupe d'utilisateurs par défaut.

Les serveurs d'authentification Radius, TACACS+ et LDAP permettent les configurations de groupe. Si un utilisateur distant est membre d'un groupe distant, le serveur d'authentification fournit le nom du groupe au système de console au moment de l'authentification de l'utilisateur. Un groupe local portant le même nom doit être configuré sur le système de console. Si un serveur d'authentification authentifie un utilisateur distant, mais n'indique aucun groupe, l'utilisateur distant est alors attribué par défaut au groupe user.

Groupe admin

Les membres du groupe admin disposent de l'intégralité des droits d'administration qu'il n'est pas possible de modifier. Ils ont les mêmes droits d'accès et de configuration que l'utilisateur admin par défaut. Les administrateurs peuvent configurer des voies, ajouter des utilisateurs et gérer les dispositifs d'alimentation reliés au système de console.

Pour consulter les droits d'accès au matériel du groupe admin :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*. L'écran Noms des groupes s'affiche avec les trois groupes d'utilisateurs par défaut, ainsi que tout autre groupe créé.
2. Cliquez sur *admin* dans la section Nom du groupe. La section Membres s'affiche dans la zone de contenu, avec tous les membres appartenant au groupe admin (les membres par défaut sont les utilisateurs admin et racine).

NOTA : lorsque vous sélectionnez le nom d'un groupe, la zone de contenu et la barre de navigation latérale changent. La barre de navigation latérale affiche des options de menu spécifiques pour les sections Membres et Droits d'accès (dont Série, Alimentation et Matériel).

3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Série* ou *Droits d'accès - Alimentation* pour afficher les écrans contenant les droits d'accès et les autorisations fixes des membres du groupe admin concernant les voies série et la gestion de l'alimentation.

NOTA : les écrans Série et Alimentation sont en lecture seule et leur contenu ne peut pas être modifié.

4. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Matériel*. L'écran Droits d'accès au matériel s'affiche et indique tous les droits d'accès disponibles pour les utilisateurs appartenant au groupe admin. Tous les droits d'accès au matériel répertoriés sont activés (cochés). Les droits d'accès au matériel disponibles sont :
    - Afficher les informations du matériel
    - Déconnecter les sessions
    - Redémarrer le matériel
    - Mettre à niveau la mémoire flash du matériel et redémarrer le matériel
    - Configurer les paramètres du matériel
    - Configurer les comptes utilisateur
    - Sauvegarder/Restaurer la configuration
    - Accéder au shell
    - Transférer les fichiers
    - Accès entrant

NOTA : l'écran Droits d'accès au matériel est en lecture seule pour les groupes d'utilisateurs admin et appliance-admin. Il ne peuvent pas y apporter de modifications. Si l'utilisateur décoche une case et clique sur *Enregistrer*, un message d'erreur s'affiche. Tous les droits restent sélectionnés dans le système de console.

Groupe appliance-admin

Les membres du groupe appliance-admin peuvent accéder aux voies série et aux options de gestion de l'alimentation, à moins que ces droits d'accès ne soient restreints par le profil de sécurité. Les membres de ce groupe disposent également des mêmes droits d'accès au matériel que les utilisateurs admin, sauf en ce qui concerne les droits Configurer les comptes utilisateur et Accéder au shell, qui sont désactivés.

Groupe user

Les membres du groupe user peuvent accéder aux dispositifs cibles, à moins que ce droit d'accès ne soit restreint par un administrateur. Si un profil de sécurité restreint l'accès global aux voies, un administrateur peut tout de même autoriser les membres du groupe user à y accéder. Les membres du groupe user ne sont pas autorisés à accéder au système de console.

Les administrateurs peuvent ajouter des droits d'accès au matériel et des autorisations. Ils peuvent également ajouter des utilisateurs à des groupes d'utilisateurs personnalisés pour leur attribuer des autorisations et des droits d'accès selon les besoins. Par défaut, toutes les options de l'écran Droits d'accès au matériel sont désactivées.

NOTA : les administrateurs peuvent modifier à tout moment les options de l'écran Droits d'accès au matériel pour le groupe user. Ils peuvent ainsi modifier les droits d'accès de tous les membres du groupe user du système de console.

Groupe shell-login-profile

Les membres du groupe shell-login-profile peuvent accéder au shell après la connexion. L'utilisateur racine appartient par défaut à ce groupe. Ce groupe n'est pas protégé et peut être supprimé.

Gestion des groupes d'utilisateurs

Les administrateurs et les membres du groupe admin peuvent créer des groupes d'utilisateurs personnalisés et y ajouter n'importe quel utilisateur.

Pour créer un groupe d'utilisateurs personnalisé :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*. L'écran Groupes affiche la liste des trois groupes d'utilisateurs par défaut, ainsi que tout groupe d'utilisateurs personnalisé qui a été créé.
2. Cliquez sur *Ajouter* dans la zone de contenu.
3. Attribuez un nom au groupe d'utilisateurs que vous allez créer.
4. Cliquez sur *Enregistrer*.

Pour ajouter des membres à un groupe d'utilisateurs :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du groupe d'utilisateurs.
3. Cliquez sur *Ajouter*. L'écran Attribution de membres affiche la liste des utilisateurs disponibles dans la partie de gauche et une zone vide à droite.
4. Déplacez les utilisateurs de la section Utilisateurs disponibles à gauche vers la partie de droite. Pour ce faire, double-cliquez sur le nom d'utilisateur ou sélectionnez un nom, puis cliquez sur le bouton *Ajouter*. Vous pouvez supprimer les noms de la section de droite en double-cliquant dessus ou en les sélectionnant, puis en cliquant sur le bouton *Supprimer*.
5. Si vous souhaitez ajouter des utilisateurs distants au nouveau groupe d'utilisateurs (il doit s'agir de noms valides sur le serveur d'authentification à distance), ajoutez-les dans le champ Nouveaux utilisateurs distants.
6. Cliquez sur *Enregistrer*.

Pour supprimer des membres d'un groupe d'utilisateurs :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du groupe d'utilisateurs.
3. Cochez les cases des membres que vous souhaitez supprimer. Cliquez sur *Supprimer* pour supprimer les membres sélectionnés.

Pour configurer le délai d'inactivité d'une session et/ou le profil de connexion d'un groupe :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du groupe pour lequel vous souhaitez configurer le délai d'inactivité de la session et/ou le profil de connexion. Dans la barre de navigation latérale, cliquez sur *Profil de connexion*.
3. Sélectionnez le bouton radio permettant d'utiliser les paramètres globaux pour le délai d'expiration de la session ou des paramètres personnalisés pour le groupe d'utilisateurs. Si vous choisissez les paramètres personnalisés, indiquez le délai d'expiration de la session (en secondes).
4. Cochez la case *Activer le profil de connexion*.
5. Cliquez sur *ts_menu* pour utiliser l'application ts_menu lorsqu'un membre du groupe d'utilisateurs sélectionné ouvre une session sur le système de console. Indiquez les options ts_menu dans le champ Options.

   -ou-

   Cliquez sur *CLI* pour utiliser l'interface CLI lors de l'ouverture d'une session. Saisissez la commande CLI dans le champ CLI cmd et cochez la case permettant de quitter l'interface après l'exécution de la commande, si vous le souhaitez.
6. Cliquez sur *Enregistrer*.

NOTA : si l'utilisateur appartient à plusieurs groupes, le profil de connexion utilisé est le premier profil de connexion activé en fonction de l'ordre alphabétique du groupe.

Tableau 3.22 Options ts_menu

Commande	Description
-p	Affichage de la voie TCP.
-i	Affichage de l'adresse IPv4 locale attribuée à la voie série.
-i6	Affichage de l'adresse IPv6 locale attribuée à la voie série.
-u <nom>	Nom d'utilisateur pour la session cible.
-e <[^]char>	Commande d'interruption permettant de fermer la session cible. Valeur par défaut : Ctrl+X
-l	Affichage des voies triées et fermeture.
-ro	Mode lecture seule.
<nom_de_la_voie>	Connexion directe à une voie série.
-t	Délai d'inactivité en secondes pour choisir la cible.

Pour attribuer le droit d'accès aux voies série à un groupe d'utilisateurs :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du nouveau groupe d'utilisateurs.
3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès*.
4. Cliquez sur *Ajouter* dans la zone de contenu.
5. Déplacez les dispositifs cibles série de la section Cible disponible à gauche vers la partie de droite. Pour ce faire, double-cliquez sur le nom de la cible série.

   -ou-

Sélectionnez la cible et cliquez sur le bouton *Ajouter*. Vous pouvez supprimer les cibles de la section de droite en double-cliquant dessus ou en les sélectionnant, puis en cliquant sur le bouton *Supprimer*.

6. Sélectionnez les droits d'accès souhaités.
7. Cliquez sur *Enregistrer*. L'écran Série affiche les dispositifs série cibles que le groupe d'utilisateurs peut utiliser avec les autorisations configurées.
8. Modifiez les droits d'accès en cochant la case d'un ou plusieurs noms de cibles dans la liste, puis cliquez sur *Modifier*. L'écran Droits d'accès cible affiche les droits d'accès. Sélectionnez les droits d'accès souhaités, puis cliquez sur *Enregistrer*.

Pour attribuer l'accès à la PDU à un groupe d'utilisateurs :

NOTA : en autorisant un groupe d'utilisateurs à accéder à la PDU, vous leur permettez d'accéder à toutes les fonctions de gestion de l'alimentation pour cette PDU. Si vous souhaitez autoriser le groupe à accéder uniquement aux prises, suivez la procédure de la section *Pour autoriser un nouveau groupe d'utilisateurs personnalisé à accéder aux prises* ci-dessous.

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du groupe d'utilisateurs.
3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Alimentation*.
4. Cliquez sur *Ajouter* dans la zone de contenu. L'écran Attribution de PDU affiche la liste des PDU disponibles dans la partie de gauche.
5. Déplacez les PDU de la section PDU disponible à gauche vers la partie de droite. Pour ce faire, double-cliquez sur le nom de la PDU ou sélectionnez la PDU, puis cliquez sur le bouton *Ajouter*. Vous pouvez supprimer les PDU de la partie de droite en double-cliquant dessus ou en les sélectionnant, puis en cliquant sur le bouton *Supprimer*.
6. Vous pouvez indiquer un ID de PDU personnalisé dans le champ correspondant en bas de l'écran.

NOTA : l'ID de PDU personnalisé permet d'autoriser un groupe d'utilisateurs à gérer les PDU qui n'ont pas encore été reliées au système de console.

7. Cliquez sur *Enregistrer*.

Pour attribuer l'accès aux prises à un nouveau groupe d'utilisateurs personnalisé :

NOTA : l'attribution de l'accès aux prises à des groupes d'utilisateurs permet à leurs membres de mettre les prises sous tension ou hors tension, et d'activer les fonctions de verrouillage et de redémarrage sur les PDU compatibles.

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du nouveau groupe d'utilisateurs.
3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Alimentation - Prises*.
4. Cliquez sur *Ajouter*. L'écran Ajouter une prise s'affiche.
5. Si des PDU sont reliées, cliquez sur le bouton *Sélectionner une PDU* pour activer les champs PDU connectées et Prises.
6. Sélectionnez *PDU connectées* dans le menu déroulant.
7. Indiquez les prises attribuées à ce groupe d'utilisateurs.

NOTA : vous pouvez indiquer des prises individuelles (par exemple, 1,3,6,8), une plage de prises (par exemple, 1-4) ou les deux (par exemple, vous pouvez saisir 1-4,6,8 pour attribuer l'accès aux prises 1, 2, 3, 4, 6 et 8).

8. Si vous avez créé un ID de PDU personnalisé pour une utilisation ultérieure et que vous souhaitez attribuer des prises à l'avance, cliquez sur le bouton *Personnaliser* pour indiquer l'ID de PDU personnalisé et les prises.
9. Cliquez sur *Enregistrer*.

Pour attribuer l'accès à l'UPS à un groupe d'utilisateurs :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du groupe d'utilisateurs.
3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Alimentation - UPS*.
4. Cliquez sur *Ajouter* dans la zone de contenu. L'écran Attribution d'UPS affiche la liste des UPS disponibles dans la partie de gauche.
5. Déplacez les UPS de la section UPS disponibles à gauche vers la partie de droite. Pour ce faire, double-cliquez sur le nom de l'UPS ou sélectionnez l'UPS, puis cliquez sur le bouton *Ajouter*. Vous pouvez supprimer les UPS de la partie de droite en double-cliquant dessus ou en les sélectionnant, puis en cliquant sur le bouton *Supprimer*.
6. Vous pouvez indiquer un ID d'UPS personnalisé dans le champ correspondant en bas de l'écran.

NOTA : l'ID d'UPS personnalisé permet d'autoriser un groupe d'utilisateurs à gérer les UPS qui n'ont pas encore été reliés au système de console.

Pour attribuer des droits d'accès au matériel à des groupes d'utilisateurs personnalisés :

1. Cliquez sur *Utilisateurs - Autorisation - Groupes*.
2. Cliquez sur le nom du nouveau groupe d'utilisateurs.
3. Dans la barre de navigation latérale, cliquez sur *Droits d'accès - Matériel*.
4. Sélectionnez les droits d'accès au matériel souhaités et cliquez sur *Enregistrer*.

Pour configurer un groupe sur le serveur d'authentification TACACS+ :

1. Sur le serveur, ajoutez le service d'accès en lecture seule à la configuration utilisateur.
2. Indiquez les groupes dont l'utilisateur fait partie pour le service d'accès en lecture seule en respectant la syntaxe suivante :

group_name = <Groupe1>[,<Groupe2,...,GroupeN>];

Par exemple :

Dans le système de console, configurez un nouveau groupe d'autorisation TACACS_1, ainsi que ses droits d'accès. Sur le serveur TACACS+, configurez l'utilisateur « regina » avec les attributs suivants : `raccess = group_name=TACACS_1 ;`

Configurez ensuite l'attribut de l'utilisateur « spécial », comme suit : `raccess = group_name=admin;`

Lors de la phase d'authentification, le système de console reçoit l'attribut d'accès en lecture seule à partir du serveur TACACS+. L'utilisateur regina appartient au groupe d'autorisation TACACS_1 et l'utilisateur spécial au groupe d'autorisation admin.

Pour configurer un groupe sur le serveur d'authentification RADIUS :

Indiquez les groupes dont l'utilisateur fait partie grâce à l'attribut FRAMED_FILTER_ID en respectant la syntaxe suivante :

```
[:group_name=]<acs800/8000_group1>[,<acs800/8000_group2>];
```

NOTA : les noms de groupe doivent être séparés par des virgules et la liste doit se terminer par un point-virgule.

NOTA : l'ACS 800/8000 accepte plusieurs attributs FRAMED_FILTER_ID.

Par exemple :

Dans le système de console, configurez de nouveaux groupes d'autorisation RADIUS_1 et RADIUS_2, ainsi que leurs droits d'accès. Sur le serveur Radius, configurez l'utilisateur regina avec l'attribut suivant :

```
FramedFilterID = group_name=RADIUS_1,RADIUS_2;
```

-ou-

```
FramedFilterID = RADIUS_1,RADIUS_2;
```

-ou-

```
FramedFilterID = RADIUS_1;
FramedFilterID += RADIUS_2;
```

Configurez ensuite l'attribut de l'utilisateur spécial, comme suit :

```
FramedFilterID = group_name=admin;
```

Lors de la phase d'authentification, le système de console reçoit l'attribut FramedFilterID à partir du serveur RADIUS. L'utilisateur regina appartient aux groupes d'autorisation RADIUS_1 et RADIUS_2, et l'utilisateur spécial au groupe d'autorisation admin.

Pour configurer un groupe sur le serveur d'authentification LDAP :

Sur le serveur LDAP, modifiez l'attribut info de l'utilisateur en respectant la syntaxe suivante :

```
info: group_name=<Group1>[,<Group2>,...,<GroupN>];
```

Droits d'accès du logiciel DSView

Les administrateurs peuvent mapper les droits de session du visualiseur du logiciel DSView sur les droits d'accès du système de console lorsqu'un utilisateur accède à la cible via le visualiseur série du logiciel DSView.

Pour mapper les droits d'accès du logiciel DSView sur ceux du système de console :

1. Cliquez sur *Utilisateurs - Autorisation - Droits d'accès DSView*.
2. Sélectionnez les droits d'accès souhaités, puis cliquez sur *Enregistrer*.

3.3.12 Notifications des événements

Le système de console envoie des notifications pour divers événements. Vous pouvez le configurer pour qu'il transfère ou stocke ces notifications vers plusieurs destinations, pour une utilisation immédiate ou une analyse ultérieure.

Liste des événements

L'écran Liste des événements affiche les événements du système de console pour lesquels il est possible de configurer des notifications par interruption SNMP, message Syslog, logiciel DSView, e-mail et SMS.

Pour configurer les événements :

1. Cliquez sur *Événements et journaux - Événements*.
2. Recherchez les événements pour lesquels vous souhaitez activer les notifications et cochez la case à côté du numéro de chaque événement.
3. Cliquez sur *Modifier*.
4. Si vous souhaitez qu'une notification d'événement soit envoyée pour tout type de destination d'événement configuré, cochez la case *Envoyer* correspondante.
5. Cliquez sur *Enregistrer*. Si vous avez coché la case Envoyer sur l'écran Paramètres des événements, l'écran Événements affiche un X dans la colonne au-dessous du type de destination.

Destinations des événements

Pour configurer les destinations des événements :

1. Cliquez sur *Événements et journaux - Destinations des événements*.
2. Sélectionnez Site dans le menu déroulant de la section Syslog.

   Sélectionnez *Serveur distant - IPv4* pour activer l'envoi de messages syslog à un ou plusieurs serveurs IPv4 syslog distants. Indiquez l'adresse IPv4 ou le nom d'hôte, ainsi que la voie UDP, pour chaque serveur syslog distant.

   -ou-

   Sélectionnez *Serveur distant - IPv6* pour activer l'envoi de messages syslog à un ou plusieurs serveurs IPv6 syslog distants. Indiquez l'adresse IPv6 ou le nom d'hôte, ainsi que la voie UDP, pour chaque serveur syslog distant.
3. Sélectionnez *Console de matériel* pour envoyer des messages à la console du système.
4. Sélectionnez *Session racine* pour envoyer des messages syslog à toutes les sessions auxquelles vous êtes connecté en tant qu'utilisateur racine.
5. Dans le champ Communauté de la section Interruption SNMP, saisissez le nom de la communauté définie sur un ou plusieurs serveurs d'interruption SNMP, puis indiquez les adresses IP de cinq serveurs maximum dans les champs correspondants.

6. Dans la section SMS, renseignez les champs concernant le serveur SMS, la voie et le numéro de pager.
7. Dans la section E-mail, renseignez les champs concernant le serveur, la voie et l'e-mail du destinataire.
8. Dans le champ Serveur DSView de la section DSView, indiquez l'adresse IP du serveur DSView auquel les notifications doivent être envoyées. Renseignez les champs concernant le numéro de voie du serveur syslog pour le serveur DSView, les informations SSH et l'avertissement en cas de problème avec le tampon.
9. Cliquez sur *Enregistrer*.

Envoi d'interruptions

Le système de console reçoit les interruptions SNMP et les transfère à un serveur d'interruptions SNMP distant.

Pour ajouter un serveur d'interruptions SNMP auquel transférer les interruptions :

1. Cliquez sur *Événements et journaux - Envoi d'interruptions*.
2. Cliquez sur *Ajouter*.
3. Saisissez l'adresse IP du serveur distant et de la voie UDP.
4. Indiquez l'OID pour filtrer les interruptions à envoyer au serveur (facultatif).

Pour modifier une configuration de serveur d'interruptions SNMP :

1. Cliquez sur *Événements et journaux - Envoi d'interruptions*.
2. Cliquez sur l'index du serveur que vous souhaitez modifier.
3. Modifiez la voie UDP et/ou l'OID, puis cliquez sur *Enregistrer*.

Mise en mémoire tampon des données

Lorsque la mise en mémoire tampon des données est activée sur une ou plusieurs voies série, les paramètres définis sur la page Événements et journaux - Mise en mémoire tampon des données s'appliquent au type (à la destination) de la mise en mémoire tampon. La taille de segment, exprimée en kilooctets, indique la taille de chaque fichier de mise en mémoire tampon des données enregistré. Le champ Segments de rechange indique combien de fichiers de mise en mémoire tampon de l'historique supplémentaires de la taille de segment seront conservés, avec les suffixes .1, .2, etc. ajoutés au nom de fichier.

Pour configurer la mise en mémoire tampon des données :

1. Sélectionnez *Événements et journaux - Mise en mémoire tampon des données*.
2. Indiquez la taille de segment (en kilooctets) et les segments de rechange dans la section Paramètres de mise en mémoire tampon des données locale.
3. Dans la section Paramètres de mise en mémoire tampon des données NFS, renseignez les champs suivants : Serveur NFS, Chemin NFS, Taille de segment (Koctets) et Segments de rechange.

NOTA : le service RPC doit être activé sur la page Profil de sécurité avant la configuration des paramètres de mise en mémoire tampon des données NFS.

4. Pour segmenter les fichiers de mise en mémoire tampon des données tous les jours, à une heure précise, indiquez l'heure souhaitée dans le champ Fermer les fichiers journaux et en ouvrir de nouveaux à l'heure (HH:MM). Ce paramètre s'applique à la mise en mémoire tampon des données locale et NFS.
5. Pour configurer le stockage du tampon des données sur un serveur syslog, sélectionnez un numéro de site dans le menu déroulant de la section Paramètres de mise en mémoire tampon des données Syslog : Consigner en local 0, Consigner en local 1, Consigner en local 2, Consigner en local 3, Consigner en local 4 ou Consigner en local 5.
6. Cliquez sur *Enregistrer*.

Pour activer la mise en mémoire tampon des données :

1. Sélectionnez *Voies - Voies série*.
2. Cliquez sur la voie sur laquelle vous souhaitez activer la mise en mémoire tampon des données.
3. Dans l'onglet Mise en mémoire tampon des données, *activez* la mise en mémoire dans le menu déroulant Statut.

Consignation des données du matériel

Lorsque la consignation des données du matériel est activée, les commandes (entrée) et les sorties à partir de sessions SSH et Telnet vers le matériel sont enregistrées à des fins de vérification.

Pour configurer la consignation des données du matériel :

1. Cliquez sur *Activer la consignation des données de session du matériel*.
2. Sélectionnez dans le menu déroulant la destination pour les journaux de données de session du matériel. Vous avez le choix entre *Locale*, *NFS*, *Syslog* et *DSView*.
    a. Si vous utilisez une destination locale, sélectionnez-la dans le menu déroulant. La destination *mmcblk0* est la mémoire de stockage flash interne. La carte SD (si présente et activée) est *mmcblk1*. Les dispositifs USB (si présents et activés) sont *sda1*, *sda2*, etc.

NOTA : lorsque la destination locale est mmcblk0, le répertoire de consignation des données sur le matériel est /mnt/hdUser/db. Lorsque la destination locale est mmcblk1 ou un dispositif USB, le répertoire de consignation des données est le répertoire de niveau supérieur (racine) du dispositif.

3. Activez ou désactivez l'horodatage des journaux de données de session du matériel.
4. Cliquez sur *Activer les alertes de consignation des données de session du matériel*.
5. Saisissez les chaînes d'alerte souhaitées (dix chaînes maximum) dans les champs correspondants.
6. Cliquez sur *Enregistrer*.

3.3.13 Gestion de l'alimentation

Il est possible de gérer l'alimentation à distance à l'aide de dispositifs d'alimentation reliés. Le système de console permet aux utilisateurs qui sont autorisés à gérer l'alimentation de mettre sous tension, de mettre hors tension et de réinitialiser les dispositifs reliés à une rampe d'alimentation électrique (PDU) connectée. Les utilisateurs autorisés peuvent également surveiller et contrôler un système d'alimentation sans coupure (UPS) Liebert GXT4 ou GXT5 connecté.

Les types de PDU ci-dessous peuvent être reliés à n'importe quelle voie série.

- Rampe d'alimentation électrique et de gestion de l'alimentation (PM PDU) Avocent.

- Rampes d'alimentation électrique (PDU) à montage en rack MPH2 Vertiv, et PDU à montage en rack MPX et MPH avec cartes RPC2 installées.
- Rampes d'alimentation électrique intelligentes et de gestion de l'alimentation (PM IPDU) Cyclades. Les PM IPDU Cyclades permettent de relier en cascade et de gérer jusqu'à 128 prises à partir d'une seule voie série.
- Dispositifs de contrôle de l'alimentation SPC Avocent.
- Gamme de rampes d'alimentation électrique en armoire commutées (Switched Cabinet Power Distribution Units, CDU), de rampes d'alimentation électrique en armoire intelligentes (Smart Cabinet Power Distribution Units, Smart CDU) et de modules d'extension de CDU commutée (Switched CDU Expansion Module, CW/CX) Server Technology Sentry. Les modules d'extension ServerTech permettent de relier en cascade un niveau supplémentaire de dispositifs d'alimentation.
- Dispositifs d'alimentation Power Tower XL (PTXL) et Power Tower Expansion Module (PTXM) de Server Technology Sentry.
- ePDU G3 Eaton. Il est possible de relier en cascade jusqu'à huit ePDU et de les gérer à partir d'une seule voie série.
- PDU PX G2 Raritan.
- PDU rPDU2 APC.
- PDU GU2 et série R en rack Geist, version du firmware 5.3 ou ultérieure.

NOTA : le terme PDU fait référence à n'importe lequel de ces types de dispositifs d'alimentation.

Le système de console reconnaît et prend en charge automatiquement les cartes Liebert RPC2, les PM PDU Avocent, les PM PDU Cyclades, les PDU Raritan, les ePDU Eaton, les PDU APC, les PDU Vertiv, les PDU Geist et les SPC Avocent lorsque la voie série correspondante est configurée pour la gestion de l'alimentation.

PDU

Pour gérer une PDU :

1. Sélectionnez *Gestion de l'alimentation - PDU*.
2. Cochez la case à côté de la PDU que vous souhaitez gérer.
3. Cliquez sur *Allumer, Éteindre, Redémarrer, Redémarrer la PDU, Réinitialiser la protection contre la surintensité du matériel* ou *Valeurs par défaut*. Un message de confirmation s'affiche. Cliquez sur *OK*.

NOTA : le contrôle de l'alimentation (Allumer, Éteindre et Redémarrer) s'applique à toutes les prises de la PDU.

4. Pour modifier l'ID d'une PDU, cliquez sur *Renommer* et saisissez un nouveau nom dans le champ Nouvel ID de PDU.
5. Cliquez sur *Enregistrer*.

Pour mettre le firmware à niveau :

1. Cochez la case à côté de la PDU que vous souhaitez mettre à niveau et cliquez sur le bouton *Mettre le firmware à niveau*.

NOTA : pour les PM PDU Avocent et Vertiv (MPH2, MPH et MPX avec cartes RPC2), vous pouvez mettre à niveau le firmware de plusieurs PDU à la fois. Si vous procédez à la mise à niveau des PDU connectées en cascade, sélectionnez uniquement la première PDU. Les autres PDU seront mises à niveau automatiquement.

2. Sélectionnez *Site distant* et indiquez les informations relatives au serveur distant.

   -ou-

   Sélectionnez *Mon ordinateur* et recherchez le fichier de firmware.

3. Cliquez sur *Télécharger* pour télécharger le firmware sur le système de console.
4. Une fois le téléchargement terminé, le système de console affiche la version actuelle du firmware, ainsi que la version téléchargé. Si la version téléchargée est correcte, cliquez sur *Mettre à niveau maintenant* pour lancer la mise à niveau du firmware dans la PDU.
5. Une fois la mise à niveau lancée, cliquez sur *Terminer*. Un message vous informant que la mise à niveau a démarré s'affiche. La page de vue d'ensemble de la PDU affiche la progression de la mise à niveau. La PDU redémarre lorsque la mise à niveau est terminée.

Pour afficher les informations relatives à une PDU et gérer les prises :

1. Sélectionnez *Gestion de l'alimentation - PDU*.
2. Cliquez sur le nom de la PDU que vous souhaitez afficher ou gérer.
3. Une fenêtre contenant le tableau des prises et les options de contrôle de l'alimentation s'ouvre. La barre de navigation latérale inclut la liste des options disponibles.
4. Pour gérer les prises de la PDU :
   a. Cochez les cases correspondant aux numéros des prises que vous souhaitez gérer.
   b. Cliquez sur *Allumer*, *Éteindre*, *Redémarrer*, *Verrouiller* ou *Déverrouiller* pour appliquer cette action aux prises sélectionnées.
5. Cliquez sur *Informations* dans la barre de navigation latérale pour afficher les informations relatives à la PDU.
6. Cliquez sur *Vue d'ensemble* dans la barre de navigation latérale pour afficher les informations concernant la surveillance des données.
7. Cliquez sur *Courant, Tension, Consommation électrique, Consommation énergétique* ou *Environnement*, dans la barre de navigation latérale, pour afficher un tableau contenant les informations correspondantes. Cliquez sur *Réinitialiser les valeurs* pour effacer les valeurs maximale, minimale et moyenne.

Pour configurer une PDU :

1. Cliquez sur *Paramètres* pour développer la barre de navigation latérale.
2. Cliquez sur *Prises*.
3. Cliquez sur le numéro d'une prise pour modifier ses paramètres. Cliquez sur *Enregistrer*, puis sur *Fermer*.

   -ou-

Cochez au moins deux cases à côté des prises dont vous souhaitez modifier les paramètres. Cliquez sur *Modifier* pour changer les paramètres des prises sélectionnées. Cliquez sur *Enregistrer*.

4. Cliquez sur *PDU* pour afficher et configurer les paramètres de la PDU. Cliquez sur *Enregistrer* lorsque vous avez terminé.
5. Cliquez sur *Phases* ou *Banques*.
    a. Cliquez sur le nom d'une phase ou d'une banque pour modifier ses paramètres ou cochez les cases à côté des phases ou des banques que vous souhaitez modifier.
    b. Cliquez sur *Enregistrer* pour enregistrer les paramètres, puis cliquez sur *Fermer* pour revenir à l'écran Phase.

NOTA : les options disponibles dans la fenêtre Paramètres dépendent du modèle de PDU.

UPS

Pour gérer un UPS :

1. Sélectionnez *Gestion de l'alimentation - UPS*.
2. Cochez la case à côté de l'UPS que vous souhaitez gérer.
3. Cliquez sur *Désactiver la sortie*, *Activer la sortie* ou *Redémarrer la sortie*. Vous avez la possibilité d'indiquer un délai avant l'exécution de l'opération. Cliquez sur le bouton pour effectuer l'opération.
4. Pour modifier l'ID d'un UPS, cliquez sur *Renommer* et saisissez un nouveau nom dans le champ Nouvel ID d'UPS.
5. Cliquez sur *Enregistrer*.

Pour afficher les informations relatives à un UPS :

1. Sélectionnez *Gestion de l'alimentation - UPS*.
2. Cliquez sur le nom de l'UPS que vous souhaitez afficher ou gérer.
3. Cliquez sur les options disponibles dans la barre de navigation latérale pour afficher les informations relatives à l'UPS.

Pour configurer un UPS :

1. Cliquez sur *Paramètres* pour développer la barre de navigation latérale.
2. Cliquez sur les options disponibles dans la barre de navigation latérale pour configurer l'UPS.

Connexion

Les administrateurs peuvent modifier le mot de passe de connexion des types de PDU pris en charge. Le système de console utilise ce mot de passe pour communiquer avec la PDU (toutes les PDU d'un même type sont associées au même mot de passe).

Pour modifier le mot de passe d'une PDU :

1. Sélectionnez *Gestion de l'alimentation - Connexion*.
2. Saisissez le nouveau mot de passe pour chaque type de PDU souhaité.
3. Cliquez sur *Enregistrer*.

Groupes de prises

L'onglet *Groupes de prises* vous permet d'afficher et de configurer le statut, les prises et la consommation électrique des différents groupes de prises. Vous pouvez également allumer, éteindre ou redémarrer les groupes de prises sélectionnés.

Pour gérer les groupes de prises :

1. Sélectionnez *Gestion de l'alimentation - Groupes de prises*.
2. Cochez la case à côté du nom du groupe de prises que vous souhaitez gérer.
3. Sélectionnez le bouton radio *Allumer*, *Éteindre* ou *Redémarrer*.

   -ou-

4. Cliquez sur *Ajouter* pour ajouter un groupe de prises. L'écran Ajouter un groupe s'affiche. Renseignez le champ Nom du groupe.
5. Cliquez sur *Enregistrer*.

Pour afficher et modifier les informations relatives à un groupe de prises :

1. Sélectionnez *Gestion de l'alimentation - Groupes de prises*.
2. Cliquez sur le nom du groupe de prises que vous souhaitez afficher ou gérer.
3. Pour ajouter une nouvelle prise au groupe, cliquez sur *Ajouter*. Renseignez les champs nécessaires, puis cliquez sur *Enregistrer* pour revenir à l'écran Détails du groupe de prises.
4. Pour supprimer des prises, cochez la case à côté des prises que vous souhaitez supprimer du groupe. Cliquez sur *Supprimer*, puis sur *Fermer* lorsque vous avez terminé.

PDU réseau

Il est possible de gérer l'alimentation à distance à l'aide de dispositifs d'alimentation connectés au réseau avec le protocole SNMP (lecture/écriture) activé. Le système de console permet alors aux utilisateurs autorisés de mettre sous tension et hors tension les dispositifs branchés sur la PDU réseau.

NOTA : vous devez activer SNMP et disposer d'une communauté avec autorisation d'accès en écriture sur la PDU.

En sélectionnant le nœud *PDU réseau*, les administrateurs peuvent ajouter de nouvelles PDU réseau ou modifier la configuration des PDU réseau existantes.

Les fonctionnalités suivantes sont prises en charge pour les PDU réseau : contrôle de l'alimentation des prises (allumer, éteindre et redémarrer), modification du nom de la PDU et modification du nom des prises.

Pour ajouter une PDU réseau :

1. Sélectionnez *Gestion de l'alimentation - PDU réseau*.
2. Cliquez sur *Ajouter*.
3. Saisissez l'adresse IP de la PDU réseau.
4. Sélectionnez un type de PDU.
5. Saisissez l'intervalle d'interrogation de la PDU pour vérifier le statut des prises.
6. Saisissez le nom de la communauté qui dispose de l'autorisation d'accès en écriture pour la PDU.

UPS réseau

Il est possible de surveiller et de contrôler les UPS GXT4 et GXT5 Liebert équipés de cartes Liebert Intellislot Unity et connectés au réseau avec le protocole SNMP (lecture/écriture) activé. Le système de console permet aux utilisateurs autorisés de surveiller les informations concernant la batterie, l'entrée et la sortie du système, ainsi que de contrôler les prises de sortie.

NOTA : vous devez activer SNMP et disposer d'une communauté avec autorisation d'accès en écriture sur l'UPS.

En sélectionnant le nœud UPS réseau, les administrateurs peuvent ajouter de nouveaux UPS réseau ou modifier la configuration des UPS réseau existants.

3.3.14 Capteurs

Internes

Le système de console est équipé de capteurs qui surveillent sa température interne. Vous pouvez indiquer une plage de fonctionnement du système de console en fonction de son environnement. Deux capteurs de température interne peuvent générer des notifications d'événement : le capteur de température de l'UC et le capteur de température de la carte.

ATTENTION : n'utilisez pas de valeur supérieure à la température maximale ou inférieure à la température minimale. **Annexes à la page 91.**

Pour configurer les capteurs de température :

1. Cliquez sur *Capteurs - Matériel - Interne* pour ouvrir la page Interne qui affiche les informations sur les capteurs de température de l'UC et de la carte.
2. Dans le champ de température maximale de l'UC ou de la carte, indiquez la température (en degrés Celsius) entraînant l'envoi d'une notification d'événement si la température de fonctionnement est supérieure à cette valeur.
3. Dans le champ de seuil de température maximale de l'UC ou de la carte, indiquez un seuil de température (en degrés Celsius) inférieur à la température maximale.

NOTA : le champ de seuil de température maximale définit une zone autour de la température maximale. Lorsque la température de fonctionnement dépasse la température maximale plus le seuil, une notification d'événement est générée. Lorsque la température de fonctionnement redevient inférieure à la température maximale moins le seuil, une notification d'événement est générée vous informant que la température de fonctionnement du système de console est redevenue normale. Le principe est le même pour le seuil de température minimale.

4. Dans le champ de température minimale, indiquez la température (en degrés Celsius) entraînant l'envoi d'une notification d'événement si la température de fonctionnement du système de console est inférieure à cette valeur.
5. Dans le champ de seuil de température minimale de l'UC ou de la carte, indiquez un seuil de température (en degrés Celsius) supérieur à la température minimale.
6. Cliquez sur *Enregistrer*.

Capteurs externes à 1 fil

Il est possible de relier un capteur externe à 1 fil à la voie SENSOR qui se trouve à l'avant du système de console à l'aide d'un câble CAT 5. La prise en charge du capteur à 1 fil est activée par défaut. Il est possible de la désactiver sur la page Profil de sécurité.

Pour configurer un capteur à 1 fil :

Dans la barre de navigation latérale, cliquez sur *Capteurs - Matériel - À 1 fil*. Les capteurs détectés s'affichent dans un tableau qui indique le type de capteur et la valeur actuelle.

NOTA : cette option est disponible pour tous les modèles de système de console, même ceux qui ne disposent pas d'une voie SENSOR. Si c'est le cas de votre modèle, laissez cette option désactivée.

NOTA : si un capteur connecté ne s'affiche pas, cliquez sur *Mettre la liste à jour* pour actualiser la page.

NOTA : les options de configuration du capteur dépendent de son type. Les paramètres de configuration communs à tous les capteurs sont Nom et Emplacement.

Capteurs de contact (SN-2D/SN-3C)

Ce type de capteur peut générer une notification d'événement en cas de modification du statut d'une ou plusieurs de ses entrées. Les statuts possible sont : *Désactivé*, *Alarme si ouvert* ou *Alarme si fermé*.

Température externe

Ce type de capteur peut générer une notification d'événement lorsque la température dépasse un certain seuil défini par l'utilisateur. Vous pouvez choisir l'unité de mesure utilisée, degrés *Celsius* ou *Fahrenheit*. Pour que des événements puissent être générés, vous devez définir les seuils Avertissement faible, Critique faible, Avertissement élevé ou Critique élevé. Par ailleurs, le statut de l'alarme doit être *activé* pour qu'une alerte puisse être générée.

Humidité externe

Ce type de capteur peut générer une notification d'événement lorsque l'humidité dépasse un certain seuil défini par l'utilisateur. Pour que des événements puissent être générés, vous devez définir les seuils Avertissement faible, Critique faible, Avertissement élevé ou Critique élevé. Par ailleurs, le statut de l'alarme doit être *activé* pour qu'une alerte puisse être générée.

Pression différentielle (SN-DP)

Ce type de capteur peut générer une notification d'événement lorsque la pression différentielle dépasse un certain seuil défini par l'utilisateur. Pour que des événements puissent être générés, vous devez définir les seuils Avertissement faible, Critique faible, Avertissement élevé ou Critique élevé. Par ailleurs, le statut de l'alarme doit être *activé* pour qu'une alerte puisse être générée.

Capteur de fuite (SN-L)

Ce type de capteur peut générer deux types d'alarmes : une alarme de fuite si une fuite est détectée et une alarme de défaillance de câble en cas de problème de connexion des câbles. Le paramètre de configuration est Durée du filtrage (secondes). Il s'agit de la durée (en secondes) pendant laquelle la fuite doit être présente pour qu'un événement soit généré.

Capteurs d'entrée numérique

Il est possible de relier un capteur d'entrée numérique externe à la voie DIGITAL IN qui se trouve à l'avant du système de console à l'aide d'un câble CAT 5.

Pour configurer un capteur d'entrée numérique :

1. Dans la barre de navigation latérale, cliquez sur *Capteurs - Matériel - Numérique entrant*. Les entrées numériques détectées s'affichent dans un tableau.
2. Cliquez sur le numéro correspondant à la position du capteur pour ouvrir la page des paramètres.
3. Saisissez le nom et l'emplacement du capteur et sélectionnez son type dans le menu déroulant.
4. Vous pouvez configurer un capteur d'entrée numérique pour qu'il génère un événement grâce au paramètre Alarme. Dans le menu déroulant, sélectionnez *Alarme si ouvert*, *Alarme si fermé* ou *désactivez* l'alarme.

NOTA : cette option est disponible pour tous les modèles de système de console, même ceux qui ne disposent pas d'une voie DIGITAL IN. Si c'est le cas de votre modèle, laissez cette option désactivée.

Capteurs de sortie numérique

Le système de console avancé ACS 800 prend en charge deux sorties numériques. Les sorties numériques sont des voies de relais contrôlées à distance qui permettent d'ouvrir ou de fermer un circuit électrique.

NOTA : le système de console avancé ACS 8000 ne prend pas en charge les sorties numériques.

Pour configurer un capteur de sortie numérique :

1. Dans la barre de navigation latérale, cliquez sur Sortie numérique.
2. Cliquez sur le numéro correspondant à la position du capteur pour ouvrir la page des paramètres.
3. Saisissez le nom du capteur, si nécessaire.
4. Dans le menu déroulant, choisissez de mettre *SOUS TENSION* ou *HORS TENSION* un circuit électrique et cliquez sur *Enregistrer*.

3.3.15 Sessions actives

Le système de console autorise plusieurs utilisateurs à se connecter et à exécuter des sessions simultanément. La fonction Sessions actives vous permet d'afficher toutes les sessions actives et de mettre fin aux sessions indésirables. Cliquez sur *Sessions actives* pour afficher toutes les sessions ouvertes sur le système de console.

NOTA : si vous lancez une nouvelle session sur le système de console alors que cet écran est ouvert, elle n'est pas visible tant que vous n'avez pas cliqué sur *Actualiser* en haut de la fenêtre de l'interface utilisateur Web.

Pour mettre fin à une session active :

1. Cliquez sur *Sessions actives*. L'écran Sessions actives s'affiche et indique toutes les sessions ouvertes sur le système de console, ainsi que l'adresse IP du poste de l'utilisateur.

2. Cochez la case à côté de la session à laquelle vous souhaitez mettre fin, puis cliquez sur le bouton *Arrêter*. Au bout de quelques secondes, l'écran Sessions Actives affiche de nouveau les sessions ouvertes. Celle que vous venez d'arrêter ne se trouve plus dans la liste.

3.3.16 Surveillance

La section *Surveillance* vous permet de consulter diverses informations relatives au réseau et aux voies console. Ces données sont affichées à titre informatif uniquement et ne peuvent pas être modifiées. Le tableau suivant indique les types d'informations disponibles.

Tableau 3.23 Écrans Surveillance

Nom de l'écran	Définition
Réseau - Dispositifs	Affiche les informations suivantes : Voies Ethernet, Adaptateur réseau USB, Statut (activé/désactivé), Adresse IPv4, Masque IPv4 et Adresse IPv6.
Réseau - Table de routage IPv4	Affiche les informations suivantes : Destination, Passerelle, Masque du réseau, Indicateurs, Métrique, Réf, Utilisation et Interface.
Réseau - Table de routage IPv6	Affiche les informations suivantes : Destination, Tronçon suivant, Indicateurs, Métrique, Réf, Utilisation et Interface.
Voies série	Affiche les informations suivantes : Nom du dispositif, Profil, Paramètres, Signaux, Octets TX, Octets RX, Erreur de trame, Erreur de parité, Rupture et Dépassement. Le bouton Réinitialiser les compteurs permet aux administrateurs de réinitialiser les statistiques pour les voies sélectionnées.
Mode FIPS	Affiche les informations suivantes : Nom du service et Indication de mode.
Journal autonome	Affiche le fichier de journal d'approvisionnement autonome et permet aux administrateurs de l'effacer.
Journal des appels	Affiche les 20 derniers appels.
Statut du tunnel IPSec	Affiche les informations sur la connexion IPSec, dont le statut du tunnel, l'adresse IP distante, la durée de vie IKE, le délai fixé, l'algorithme des phases et le nom du certificat.

3.3.17 Modifier le mot de passe

Cet écran permet aux administrateurs ou aux utilisateurs de modifier leur mot de passe.

Pour modifier votre mot de passe :

1. Sélectionnez *Modifier le mot de passe*.
2. Saisissez l'ancien et le nouveau mot de passe dans les champs correspondants.
3. Confirmez le nouveau mot de passe, puis cliquez sur *Enregistrer*.

3.4 Présentation de l'interface utilisateur Web pour les utilisateurs

Tableau 3.24 Options de l'interface utilisateur Web pour les utilisateurs

Option de menu	Description
Accès	Affiche tous les dispositifs auxquels l'utilisateur peut accéder. Cliquez sur *Visualiseur série* dans la colonne Action d'un dispositif pour lancer une session terminal sur ce dispositif.
Groupes de prises des PDU pour la gestion de l'alimentation	Cliquez sur *PDU* pour allumer, éteindre, redémarrer, restaurer les valeurs par défaut ou renommer les PDU reliées au système de console ou réinitialiser la protection contre la surintensité du matériel. Cliquez sur *Groupes de prises* pour gérer les groupes de prises des PDU connectées. Cliquez sur UPS pour surveiller et contrôler les UPS connectés.
Modifier le mot de passe	Option vous permettant de modifier votre mot de passe.

Annexes

Annexe A: Caractéristiques techniques

Tableau A.1 Caractéristiques techniques du système de console avancé ACS 8000

Catégorie	Valeur
Informations générales	
UC	Dual Core ARM Cortex-A9 à 766 MHz
Mémoire	DDR3L 1 Go / eMMC FLASH 16 Go
Interfaces	• Deux voies 1000Base-TX cuivre/1 Gbit/s SFP fibre double support • 48 voies série avec prise en charge de la détection automatique et de la commutation des brochages Cyclades et Cisco • Deux des voies série prennent en charge le multiprotocole RS232/422/485 avec détection automatique et commutation des brochages Cyclades et Cisco en mode RS232 • Une voie console série • Huit voies hôtes USB 2.0 (les voies avant ne sont pas disponibles sur certains modèles) • Un emplacement pour carte SD (sur certains modèles uniquement) • Voie MODEM analogique V.92/56K en option • Interface à 1 fil pour les capteurs externes (sur certains modèles uniquement) • Connecteur RJ45 unique avec quatre voies d'entrée numérique pour les capteurs externes à fermeture par contact (sur certains modèles uniquement)
Informations sur l'alimentation	
Alimentation	Alimentation interne de 100-240 V c.a., 50/60 Hz, double entrée en option, blocs d'alimentation redondants de -48 V c.c. disponibles en option
Consommation électrique	Tension nominale de 120 V c.a. : typique 0,17 A, 20 W, maximale 0,25 A, 30 W Tension nominale de 230 V c.a. : typique 0,1 A, 23 W, maximale 0,15 A, 35 W Tension nominale de -48 V c.c. (tolérance de 20 %) : typique 0,5 A
Conditions ambiantes	
Température de fonctionnement	De 0 °C à 50 °C (alimentation c.c.) De -10 °C à 70 °C (alimentation c.a.)
Température de stockage	De -20 °C à 70 °C
Humidité	20 à 80 % d'humidité relative (sans condensation) sur toute la plage de températures de fonctionnement
Dimensions	
Hauteur x largeur x profondeur	4,318 x 43,434 x 24,13 cm
Poids	2,722 à 3,175 kg selon le modèle

Tableau A.2 Caractéristiques techniques du système de console avancé ACS 800

Catégorie	Valeur
Informations générales	
UC	Dual Core ARM Cortex-A9 à 766 MHz
Mémoire	DDR3L 1 Go / eMMC FLASH 16 Go
Interfaces	• Deux voies 1000Base-TX cuivre double support • Huit voies série avec prise en charge de la détection automatique et de la commutation des brochages Cyclades et Cisco • Huit voies série multiprotocoles RS232/422/485 avec prise en charge de la détection automatique et de la commutation des brochages Cyclades et Cisco en mode RS232 • Une voie console série • Quatre voies hôtes USB 2.0 • Voie MODEM analogique V.92/56K • Interface à 1 fil pour les capteurs externes • Connecteur RJ45 unique avec quatre entrées numériques pour les capteurs externes à fermeture par contact • Connecteurs de sortie numérique fournissant quatre signaux de sortie
Informations sur l'alimentation	
Alimentation	Alimentation interne de 100-240 V c.a., 50/60 Hz
Consommation électrique	Tension nominale de 120 V c.a. : typique 80,5 mA/3,5 W, maximale 306 mA/17 W Tension nominale de 240 V c.a. : typique 60 mA/3,75 W, maximale 191 mA/17 W
Conditions ambiantes	
Température de fonctionnement	De -20 °C à 70 °C
Température de stockage	De -20 °C à 70 °C
Humidité	20 à 80 % d'humidité relative (sans condensation) sur toute la plage de températures de fonctionnement
Dimensions	
Hauteur x largeur x profondeur	3,302 x 21,2852 x 18,1864 cm
Poids	1,72365 kg

Annexe B: Approvisionnement autonome

La fonction d'approvisionnement autonome vient s'ajouter à la récupération de la configuration Bootp du système de console et permet de déployer de nombreux systèmes de console dans un même environnement. Pour utiliser cette fonction, vous devez disposer de serveurs DHCP et TFTP valides. Vous pouvez configurer vos serveurs DHCP de sorte qu'ils demandent aux nouveaux systèmes de console de télécharger un modèle de configuration et de mettre à niveau/rétrograder leur firmware si nécessaire.

La création de fichiers de configuration/DHCP/TFTP ne prend que quelques minutes et peut vous faire gagner plusieurs heures lors de la configuration des systèmes de console ajoutés par la suite au réseau. Une fois l'étape d'approvisionnement terminée, vous pouvez accéder aux systèmes de console individuellement pour toute autre configuration nécessaire (par exemple, pour attribuer une adresse IP statique et un nom d'hôte).

Grâce à l'approvisionnement autonome, vous pouvez configurer automatiquement les systèmes de console et les mettre à niveau après leur démarrage et leur initialisation. Cette fonction simplifie l'ajout et l'installation de systèmes de console à un réseau existant.

Les administrateurs peuvent consulter le journal des configurations autonomes en cliquant sur *Surveillance - Journal autonome* dans la barre de navigation latérale de l'onglet Expert.

B.1 Fichier de configuration d'approvisionnement autonome

Pour utiliser la fonction d'approvisionnement autonome, les administrateurs doivent d'abord sauvegarder le fichier de configuration d'un système de console sur un serveur distant. Ce fichier est référencé par le fichier de montage créé pour l'approvisionnement autonome. Pour en savoir plus sur la création et la sauvegarde d'un fichier de configuration, reportez-vous à la section Fichiers de configuration à la page 20.

NOTA : les paramètres inclus dans le fichier de configuration s'appliquent à tous les systèmes de console qui reçoivent ce fichier. Si vous ne souhaitez pas qu'un paramètre s'applique à tous les systèmes de console, par exemple un nom d'hôte, ajoutez le signe dièse (#) devant le paramètre concerné.

B.2 Fichier de montage

Une fois le fichier de configuration enregistré sur un serveur distant et le serveur DHCP configuré, l'administrateur doit créer un fichier de montage. Ce fichier permet au système de console d'identifier les paramètres de configuration et les informations d'approvisionnement importantes, comme le nom du fichier image du firmware, le nom du fichier de configuration et l'adresse IP du serveur distant sur lequel se trouve le fichier de configuration. Après avoir créé le fichier de montage, vous devez le stocker sur un serveur TFTP, FTP ou SFTP. L'adresse IP du serveur TFTP, FTP ou SFTP est envoyée dans le message d'offre DHCP.

NOTA : si vous stockez le fichier de montage sur un serveur TFTP, nous vous recommandons de l'enregistrer dans le dossier racine de ce serveur.

Voici un exemple de fichier de montage :

```
ONE_TIME_CONFIG=YES
FIRMWARE_VERSION=1.0.1
FIRMWARE_FILENAME=/var/tftp/acs8000/acs8000_1.0.1.bin

FIRMWARE_SERVER_IP=192.168.100.2
FIRMWARE_SERVER_USERNAME=required username
FIRMWARE_SERVER_PASSWORD=required password
FIRMWARE_SERVER_PROTOCOL=SFTP
CONFIG_FILENAME=/tftp/config-xml
CONFIG_SERVER_IP=192.168.100.2
CONFIG_SERVER_USERNAME=
CONFIG_SERVER_PASSWORD=
CONFIG_SERVER_PROTOCOL=SFTP
```

Tableau B.1 Descriptions du fichier de montage

Paramètre	Description
ONE_TIME_CONFIG	Lorsque ce paramètre est défini sur Yes, le système de console récupère le fichier de configuration lors du démarrage initial. Il n'est pas envoyé lors des démarrages suivants. Lorsque ce paramètre est défini sur No, le système de console récupère le fichier de configuration à chaque démarrage.
FIRMWARE_VERSION	Version du firmware qui doit être envoyé au matériel.
FIRMWARE_FILENAME	Chemin et nom de fichier du firmware.
FIRMWARE_SERVER_IP	Adresse IP ou nom d'hôte du serveur qui héberge le firmware.
FIRMWARE_SERVER_USERNAME	Informations permettant d'accéder au serveur si le firmware se trouve sur un serveur sécurisé.
FIRMWARE_SERVER_PASSWORD	
FIRMWARE_SERVER_PROTOCOL	Protocole du serveur qui héberge le firmware. Les protocoles pris en charge sont tftp, ftp, stfp, scp et wget.
CONFIG_FILENAME	Chemin et nom du fichier de configuration.
CONFIG_SERVER_IP	Adresse IP ou nom d'hôte du serveur qui héberge le fichier de configuration.
CONFIG_SERVER_USERNAME	Informations permettant d'accéder au serveur si le fichier de configuration se trouve sur un serveur sécurisé. Ces informations sont nécessaires dans la plupart des cas. Le nom d'utilisateur est au format texte brut, mais le mot de passe doit être chiffré.
CONFIG_SERVER_PASSWORD	
CONFIG_SERVER_PROTOCOL	Protocole du serveur qui héberge le fichier de configuration. Les protocoles pris en charge sont ftp, stfp, scp et wget.

Chiffrement du mot de passe

Une empreinte numérique chiffrée du mot de passe doit être créée pour les paramètres FIRMWARE_SERVER_PASSWORD ou CONFIG_SERVER_PASSWORD. Cette empreinte doit être générée à partir d'un environnement Linux exécutant OpenSSL. Saisissez les commandes suivantes dans l'invite de commande Linux ou dans le shell du système de console. Saisissez ensuite l'empreinte numérique du mot de passe affichée dans le fichier de montage pour le type de serveur défini.

```
echo ACS6000KEYAVOCENTEMERSON > mykey
echo <MonMotDePasse> | openssl enc -base64 -salt -aes-256-cbc -pass file:./mykey
```

NOTA : dans l'exemple ci-avant, remplacez <MonMotDePasse> par un mot de passe valide.

B.3 Stockage du fichier de montage sur le serveur

Après avoir créé le fichier de montage, vous devez le stocker sur un serveur TFTP. L'exemple suivant vous montre ce que vous devez saisir dans le système pour stocker les fichiers sur le serveur et vérifier que le système de console peut les télécharger.

Pour stocker le fichier de montage sur un serveur TFTP :

```
Exemple : tftpd-hpa
Default TFTP root directory /var/lib/tftpboot
~$ sudo cp zerotouch.setup /var/lib/tftpboot
```

B.4 Obtention du fichier de montage

Après avoir obtenu les adresses IP pour le système de console et le serveur TFTP sur lequel se trouve le fichier de montage, le processus d'approvisionnement autonome tente de télécharger le fichier de montage. Après avoir téléchargé le fichier de montage, le système de console utilise les informations qu'il contient pour obtenir l'image et/ou le processus de configuration.

B.5 Configuration du serveur DHCP

Le système de console peut vous demander au cours du processus de démarrage d'attribuer une adresse IP, si nécessaire. Le serveur DHCP demande alors au serveur DNS l'emplacement du serveur TFTP ou HTTP sur lequel se trouve le fichier de montage. Les administrateurs peuvent, s'ils le souhaitent, créer une entrée sur le serveur DHCP afin d'identifier de manière unique un système de console particulier ou un ensemble de systèmes de console. Cette entrée filtre les systèmes de console approvisionnés.

L'administrateur doit configurer deux options. L'option 66 définit le nom d'hôte ou l'adresse IP du serveur TFTP sur lequel se trouve le fichier de montage. L'option 67 définit le nom du fichier de montage (par exemple, acszero.cfg).

Pour configurer les options 66 et 67 :

1. Utilisez le Gestionnaire de serveur Windows ou les outils DHCP des composants logiciels enfichables Microsoft Management Console (MMC) pour ouvrir votre console de serveur DHCP.
2. Dans le volet de gauche de la fenêtre du serveur DHCP, cliquez sur *IPv4*.
3. Cliquez avec le bouton droit de la souris sur *Options de serveur*, puis cliquez sur *Configurer les options* pour configurer une étendue globale.

   -ou-

   Cliquez avec le bouton droit sur *Options d'étendue*, puis cliquez sur *Configurer les options* pour configurer une seule étendue.
4. Cliquez sur l'option *066* pour indiquer l'emplacement du serveur qui va héberger le fichier de montage.
5. Saisissez le nom d'hôte pour le serveur TFTP.
6. Cliquez sur l'option *067* pour indiquer le nom du fichier de montage.

Les administrateurs peuvent utiliser deux options DHCP supplémentaires pour filtrer l'approvisionnement autonome pour les systèmes de console sélectionnés. L'option 60 définit la catégorie de fournisseur, Avocent_ACS800/8000<numéro de série du système de console>. L'option 61 définit l'adresse MAC du système de console.

Pour créer les options 60 et 61 (facultatif) :

1. Utilisez le Gestionnaire de serveur Windows ou les outils DHCP des composants logiciels enfichables MMC pour ouvrir votre console de serveur DHCP.
2. Dans le volet de gauche de la fenêtre DHCP, cliquez sur *IPv4*.
3. Dans la barre supérieure, cliquez sur *Action*, puis sélectionnez *Définir les options prédéfinies*.
4. Sélectionnez *Options DHCP standard* dans le champ Classe d'options, puis cliquez sur *Ajouter*.
5. Attribuez un nom à l'option dans le champ Nom, sélectionnez *Chaîne* dans le menu déroulant Type de données, saisissez 060 dans le champ Code et ajoutez une description pour l'option. Cliquez sur *OK*.
6. Répétez l'étape 5 en saisissant 061 dans le champ Code.

Serveur DNS

Si l'option d'étendue DNS n'est pas déjà définie sur votre serveur DHCP et que l'entrée de l'option 66 est un nom d'hôte plutôt qu'une adresse IP, vous pouvez configurer le serveur DNS.

Pour configurer le serveur DNS :

1. Utilisez le Gestionnaire de serveur Windows ou les outils DHCP des composants logiciels enfichables MMC pour ouvrir votre console de serveur DHCP.
2. Dans le volet de gauche de la fenêtre DHCP, cliquez sur *IPv4*.
3. Cliquez avec le bouton droit de la souris sur *Options de serveur*, puis cliquez sur *Configurer les options*.
4. Cliquez sur l'option *006* pour définir les serveurs DNS.
5. Saisissez l'adresse IP dans le champ correspondant, puis cliquez sur *Ajouter*.

NOTA : si vous saisissez le nom du serveur, le serveur DNS le résout.

Réservations

Vous pouvez réserver des adresses IP pour chaque système de console que vous souhaitez mettre à jour. Une réservation est une adresse IP qui sera toujours envoyée à un système de console spécifique lors du renouvellement de son bail DHCP.

Pour réserver une adresse IP :

1. Utilisez le Gestionnaire de serveur Windows ou les outils DHCP des composants logiciels enfichables Microsoft Management Console (MMC) pour ouvrir votre console de serveur DHCP.
2. Dans le volet de gauche de la fenêtre DHCP, cliquez sur *IPv4*.
3. Cliquez avec le bouton droit de la souris sur *Réservations*, puis sur *Nouvelle réservation*.
4. Saisissez le nom de la réservation, l'adresse IP à attribuer au système de console, l'adresse MAC du système de console et la description dans les champs correspondants.

NOTA : l'adresse MAC du système de console est indiquée au-dessous de l'unité.

5. Dans Types pris en charge, sélectionnez le bouton radio Les deux ou DHCP seulement.
6. Cliquez sur *Ajouter*. L'adresse IP réservée s'affiche dans le tableau des réservations.

Voici un exemple de configuration du serveur Linux DHCP.

```
Exemple : Serveur DHCP ISC pour Linux
Edit /etc/dhcp/dhcpd.conf ...
host acs8048 {
hardware ethernet 00:e0:86:12:34:56;
fixed-address 10.207.24.134;
filename "zerotouch.setup";
next-server 10.207.24.18;
```

B.6 Activation de l'approvisionnement autonome

Un administrateur peut activer l'approvisionnement autonome à partir de l'interface utilisateur Web ou de l'interface CLI. Après avoir activé cette fonction, vous devez effacer le journal d'approvisionnement autonome.

Pour activer l'approvisionnement autonome à partir de l'interface utilisateur Web :

1. Dans la barre de navigation latérale de l'interface utilisateur Web, cliquez sur *Système - Sécurisé - Profil de sécurité*.
2. Dans la section Récupération de la configuration Bootp, cochez les cases pour activer Bootp et activez la récupération instantanée de la configuration.
3. Sélectionnez l'interface Bootp *eth0* dans le menu déroulant.
4. Cliquez sur *Enregistrer*.
5. Dans la barre de navigation latérale de l'interface utilisateur Web, cliquez sur *Surveillance - Journal autonome* puis sur *Effacer le journal*.

Pour activer l'approvisionnement autonome à partir de l'interface CLI :

1. Connectez-vous au système de console en tant qu'utilisateur racine.
2. Saisissez cd system/security/security_profile/ pour arriver au niveau du profil de sécurité.
3. Saisissez bootp_enabled=yes et appuyez sur Entrée.
4. Saisissez bootp_interface=eth0 et appuyez sur Entrée.
5. Saisissez enable_live_configuration_retrieval_(any_time_dhcp_renews)=yes et appuyez sur Entrée.
6. Saisissez commit pour enregistrer la configuration.
7. Saisissez cd /monitoring/zero-touch_log/ pour arriver au niveau du journal autonome.
8. Saisissez clear_log. Saisissez Yes lorsque le système vous demande si vous souhaitez effacer le journal d'approvisionnement autonome.

Annexe C: Récupération de la configuration Bootp

Vous pouvez choisir de reconfigurer votre système de console lors du démarrage ou du renouvellement de l'adresse IP.

Pour activer la récupération de la configuration :

1. Cliquez sur *Outils système - Enregistrer la configuration* et enregistrez la configuration sur un site FTP ou localement.

   -ou-

   Utilisez la commande list_configuration pour obtenir les scripts de modèle CLI, modifiez la configuration du système de console et enregistrez-la en tant que fichier texte.

   -ou-

   Modifiez un fichier à l'aide des commandes CLI et enregistrez-le.

2. Transférez le fichier enregistré sur un serveur DHCP.
3. Configurez le serveur DHCP de sorte qu'il transfère le fichier de configuration au système de console.

Pour reconfigurer un système de console avec Bootp :

1. Cliquez sur *Système - Sécurisé - Profil de sécurité*. Assurez-vous que la case *Activé* est cochée dans la section Récupération de la configuration Bootp.
2. Décochez la case *Activer la configuration instantanée*. La configuration enregistrée est récupérée et appliquée au prochain démarrage.

   -ou-

   Assurez-vous que la case *Activer la configuration instantanée* est cochée. La configuration enregistrée est récupérée et appliquée au prochain renouvellement de l'adresse IP.

NOTA : vous devez configurer votre serveur DHCP pour pouvoir transférer le fichier de configuration au système de console.

Annexe D: Récupération du mot de passe du système de console

Pour récupérer le mot de passe racine du système de console :

1. Connectez-vous directement à la voie CONSOLE du système de console.
2. Mettez le système de console hors tension, puis rallumez-le.
3. Appuyez sur la barre d'espace pour afficher l'invite uboot.
4. Saisissez hw_boot single et appuyez sur Entrée.
5. Le système de console démarre en mode mono-utilisateur. Saisissez passwd et appuyez sur Entrée.
6. Saisissez le nouveau mot de passe et confirmez.
7. Saisissez reboot pour que le système de console démarre en mode normal.

Annexe E: Configuration de SSH permettant l'authentification par paire de clés RSA à la place de l'identification par nom d'utilisateur/mot de passe

Pour définir l'accès au système de console avancé ACS 800/8000 sur un client Linux :

1. Créez un nouvel utilisateur admin sur le système de console. Par exemple : acsadmin.
2. Ajoutez le nouvel utilisateur aux groupes admin et shell-login-profile.
3. Sur votre système exécutant un client Linux, générez une paire de clés qui sera utilisée lors de chaque accès ssh au système de console.

```
ssh-keygen -t rsa -b 4096 -C "acsadmin" -f ~/.ssh/acsadmin-id_rsa
```

4. Si vous ne souhaitez pas définir une phrase secrète sur votre serveur pour cette paire de clés, appuyez deux fois sur **Entrée**,

   -ou-

   Saisissez une phrase secrète.

NOTA : les deux fichiers suivants sont créés à l'aide de la commande ssh-keygen ci-dessus :

```
$HOME/.ssh/acsadmin-id_rsa
$HOME/.ssh/acsadmin-id_rsa.pub
```

5. Dans le fichier $HOME/.ssh/config du système exécutant un client Linux, ajoutez des lignes comme celles de l'exemple ci-dessous :

```
Host acsadmin132
HostName <Adresse IP du système de console> par exemple, 10.207.24.132
User acsadmin
IdentityFile ~/.ssh/acsadmin-id_rsa
```

6. Connectez-vous au système de console via SSH en tant qu'utilisateur **acsadmin** (le nouvel utilisateur).
7. Utilisez les quatre commandes ci-dessous pour installer la clé publique pour le compte acsadmin du système de console.

```
mkdir -p ~/.ssh
touch .ssh/authorized_keys
chmod 600 .ssh/authorized_keys
ssh username@linuxclientsystem "cat .ssh/acsadmin-id_rsa.pub" >> .ssh/authorized_keys
```

Par exemple, dans le cas de la commande ssh :

```
ssh adminuser@10.207.24.28 "cat .ssh/acsadmin-id_rsa.pub" >> .ssh/authorized_keys
```

8. Dans l'onglet *Système - Sécurisé - Profil de sécurité* de l'interface utilisateur Web, décochez la case *SSH permet l'authentification par identification nom d'utilisateur/mot de passe* pour désactiver cette option. Lors de la prochaine connexion SSH au système de console à partir de votre système exécutant un client Linux, la paire de clés sera utilisée pour l'authentification et aucun mot de passe ne vous sera demandé.

NOTA : si vous désactivez cette fonction, les utilisateurs ne disposant pas d'une paire de clés sur le système client et le système de console ne pourront pas se connecter au système de console via SSH. Par ailleurs, vous ne pourrez pas lancer de sessions série à partir de l'interface utilisateur Web, car leur authentification requiert l'utilisation de la combinaison nom d'utilisateur/mot de passe.

Voici un exemple de commande pour la connexion ssh avec l'entrée ssh/config pour l'hôte de l'exemple utilisé précédemment : ssh acsadmin@acsadmin132.

Annexe F: Informations concernant les voies pour la communication avec le logiciel DSView

Les voies suivantes du système de console avancé Avocent® ACS 800/8000 peuvent accepter les connexions provenant de la plate-forme d'administration logicielle DSView :

- Voie TCP 3502 (https)
- Voie TCP 3871 (adsap2)
- Voie UDP 3211 (aidp)
- Voie TCP 22 (sshd)

Les voies suivantes du logiciel DSView peuvent accepter les connexions provenant du système de console :

- Voie TCP 4122 (valeur par défaut : serveur SSH)
- Voie TCP 4514 (valeur par défaut : consignation des données ou serveur Syslog)

Annexe G: Accès commuté au système de console avec le logiciel DSView

Lorsqu'un utilisateur du logiciel DSView établit une session série, les événements suivants se produisent :

- L'utilisateur doit sélectionner une voie série pour l'accès.
- Un visualiseur est téléchargé sur le poste de travail de l'utilisateur à partir du serveur DSView.
- Le logiciel DSView transfère des informations au visualiseur, comme la clé d'autorisation, l'adresse IP et la voie série du système de console.
- Le visualiseur accède à la voie série du système de console par l'intermédiaire d'une session SSH en transférant la clé d'autorisation obtenue auprès du serveur DSView.
- La session série démarre.

Pour garantir une connectivité constante, une configuration hors bande du serveur DSView est possible afin de permettre à celui-ci de contacter le système de console via le modem en cas de panne du réseau ou de la connexion Internet.

G.1 Installation du logiciel DSView hors bande

Le serveur DSView doit être exécuté sur un matériel avec modem connecté et le système de console doit être équipé d'un modem intégré ou accéder à un modem via une voie USB ou une voie série.

Pour ce type d'installation, le serveur DSView doit être le point de réception central des paquets envoyés par le visualiseur téléchargé et le système de console. Pour ce faire, vous devez configurer le mode proxy dans le logiciel DSView. Le visualiseur dirige alors les données vers le serveur DSView (et non pas le système de console) pour établir la connexion SSH. Le serveur DSView, qui sert alors de point de communication intermédiaire, transfère les paquets en modifiant les adresses IP source et de destination.

En conditions normales, les paquets reçus du visualiseur série transitent par le serveur DSView via la connexion Ethernet. En cas d'erreur, le serveur DSView détecte l'interruption du chemin normal vers le système de console, établit un accès sortant vers le système de console, procède à l'authentification et établit une connexion PPP. Les paquets qui, en conditions normales, seraient transférés via Ethernet sont alors acheminés via la connexion PPP.

Compte tenu de la différence de vitesse entre Ethernet et l'accès commuté, les performances sont sensiblement limitées. Elles le sont encore plus en cas de connexions d'utilisateurs multiples, ce qui est donc déconseillé. C'est pour cette raison que nous ne recommandons le recours à un accès commuté qu'en cas d'urgence.

G.2 Configuration de l'accès commuté pour le système de console

Pour configurer l'accès commuté au système de console avec le logiciel DSView :

1. Dans la fenêtre Unités contenant les matériels, sélectionnez le système de console ACS 800/8000 que vous souhaitez configurer. Pour l'accès entrant avec rappel, vous devez d'abord sélectionner *Serveur DSView - Propriétés - Sessions de modem DSView* dans l'onglet Système, puis indiquer le numéro de téléphone attribué au serveur DSView dans le champ Numéro de téléphone analogique.
2. Sélectionnez *Paramètres DSView - Accès commuté*, puis cliquez sur *Activer l'accès commuté*.
3. Sélectionnez *Type de modem - Analogique*.

4. Indiquez le numéro de téléphone pour le système de console que vous souhaitez utiliser.
5. Indiquez l'utilisateur PPP et sélectionnez le protocole d'authentification PPP dans les champs correspondants.
6. Pour l'accès entrant avec rappel, cochez la case correspondant au rappel.
7. Sélectionnez *Paramètres DSView - Accès commuté - Mot de passe PPP*, puis saisissez et confirmez le mot de passe permettant d'accéder au système de console ACS 800/8000.
8. Sélectionnez *Paramètres DSView - Accès commuté - Adresses IP*.
9. Cliquez sur *Générer automatiquement* pour définir l'adresse IP automatiquement ou indiquez manuellement l'adresse IP locale PPP et l'adresse IP du matériel.
10. Sélectionnez Paramètres DSView - Accès commuté, puis cliquez sur Enregistrer.
11. Pour configurer le système de console de sorte à recevoir la connexion avec accès commuté au sein du logiciel DSView :
12. Dans la fenêtre Unités contenant les matériels, sélectionnez le système de console ACS 800/8000 que vous souhaitez configurer.
13. Dans le cas d'un modem interne, sélectionnez *Voies - Voies auxiliaires*, puis le modem.
14. Sélectionnez Paramètres DSView - Accès commuté, puis cliquez sur *Appliquer la configuration*.

NOTA : l'étape suivante est nécessaire uniquement si vous avez sélectionné *CHAP* dans le champ Protocole d'authentification PPP dans la fenêtre Accès commuté des paramètres du logiciel DSView.

15. Connectez-vous à l'interface CLI du système de console pour accéder au shell Linux. Modifiez le fichier /etc/ppp/chap-secrets et ajoutez une ligne au format approprié. Vous devez indiquer l'utilisateur PPP dans la première colonne et le mot de passe PPP dans la troisième, comme dans l'exemple suivant :

    utilisateurppp * "motdepasseppp" *

Annexe H: Modem interne

Certains modèles de système de console sont équipés d'un modem interne. Ce modem permet de passer et de recevoir des appels téléphoniques, et de communiquer avec d'autres modems afin de leur transmettre des données.

Vous pouvez contrôler les fonctions du modem grâce aux commandes AT. Ces commandes permettent d'envoyer au modem des instructions pour qu'il effectue certaines fonctions, par exemple passer ou recevoir des appels. Elles sont généralement émises automatiquement par le logiciel de communication. Vous devez cependant, dans certains cas, créer un logiciel personnalisé en l'absence d'un système d'exploitation normal.

Le modem accepte et traite automatiquement les commandes AT aux vitesses DTE (Data Terminal Equipment, Équipement terminal de traitement de données) et selon les paramètres de parité standard. À chaque commande envoyée, le modem répond par un code de résultat pour vous informer de son statut. Le format des commandes AT et des codes de résultats de base sont les suivantes :

AT<Commande><CR>

OK

AT = Attention

<Commande> = Toute commande valide

<CR> = retour chariot ou touche Entrée

OK = code du résultat

Tableau H.1 Exemple de chaînes de commande

Commande	Description
ATDT7678900<CR>	Indique au modem de composer le numéro 7678900 et de tenter de se connecter à un dispositif distant.
ATS0=2<CR>	Active l'option de réponse automatique. Lorsque le modem détecte une sonnerie, il laisse sonner deux fois avant de tenter de répondre.

Tableau H.2 Commandes AT de base

Commande	Description
ATA/	Répéter la commande précédente.
ATA	Répondre.
ATB0	Mode CCITT à 300 ou à 1200 bit/s.
ATB1	Mode Bell à 300 ou à 1200 bit/s (par défaut).
ATD	Composer.
ATD0-9	Composer la numérotation DTMF 0 à 9.
ATDA-D	Composer la numérotation DTMF A, B, C et D.
ATDP	Sélectionner la numérotation par impulsions ; s'applique à la numérotation en cours et aux numérotations suivantes.
ATDT	Sélectionner la numérotation par tonalités ; s'applique à la numérotation en cours et aux numérotations suivantes.
ATD!	Flash : couper la ligne en fonction du délai défini par le registre S29.
ATDW	Attendre la détection de la tonalité avant de composer un numéro. Si aucune tonalité n'est détectée pendant le délai défini par le registre S7, le modem abandonne le reste de la séquence, coupe la ligne et génère un message d'erreur.
ATD@	Attendre cinq secondes de silence avant de continuer avec la chaîne de composition suivante, puis terminer la séquence d'échanges.
ATD,	Pause. Le modem effectue une pause pendant la durée indiquée par le registre S8 avant de composer le numéro. Cette fonction est souvent utilisée pour obtenir une ligne extérieure avec un PBX.
ATD;	Revenir en mode de commande après le traitement.
ATE0	Désactiver l'écho des commandes.
ATE1	Activer l'écho des commandes (par défaut).
ATH0	Raccrocher.
ATH1	Forcer le modem à décrocher.
ATI0	Afficher le code du produit.
ATI2	Afficher OK (pour la compatibilité logicielle).
ATI3	Afficher la version du firmware du modem. Exemple : CX810801-V90.
ATL0	Couper le haut-parleur.
ATL1	Définir un volume de haut-parleur faible (par défaut).
ATL2	Définir un volume de haut-parleur moyen.
ATL3	Définir un volume de haut-parleur élevé.
ATM0	Ne jamais activer le haut-parleur.
ATM1	Activer le haut-parleur lorsque l'appel est établi et le désactiver lorsque le signal porteur est détecté (par défaut).
ATM2	Activer toujours le haut-parleur.
ATM3	Désactiver le haut-parleur lors de la composition du numéro et lors de la réception du signal porteur, mais l'activer lors de la réponse à l'appel.
ATQ0	Activer l'affichage des codes de résultat sur le DTE (par défaut).
ATQ1	Désactiver l'affichage des codes de résultat sur le DTE.
ATSr	Définir le registre S « r » comme le registre par défaut.
ATSr=n	Définir le registre S « r » sur la valeur « n ».
ATSr?	Afficher la valeur du registre S « r ».
ATV0	Activer l'affichage des codes de résultat au format court.

Tableau H.2 Commandes AT de base (suite)

Commande	Description
ATV1	Activer l'affichage des codes de résultat au format long.
ATW0	Indiquer uniquement la vitesse DTE à la connexion (par exemple, CONNECT 9600). Les réponses ultérieures sont désactivées (par défaut).
ATW1	Indiquer le type de modulation, la vitesse de la ligne, le protocole de correction des erreurs et la vitesse DTE à la connexion. Les réponses ultérieures sont désactivées.
ATW2	Indiquer la vitesse DTE à la connexion (par exemple, CONNECT 2400). Les réponses ultérieures sont désactivées.
ATX0	Ignorer la tonalité de numérotation et d'occupation. Afficher le message CONNECT lorsqu'une connexion est établie par numérotation aveugle.
ATX1	Désactiver la surveillance des tonalités d'occupation. Afficher uniquement les messages OK, CONNECT, RING, NO CARRIER et ERROR. Si la détection de la tonalité d'occupation est activée et qu'une tonalité d'occupation est détectée, le message NO CARRIER s'affiche au lieu du message BUSY. Si l'option de détection de la tonalité de numérotation est activée ou sélectionnée, mais qu'aucune tonalité de numérotation n'est détectée, le message NO CARRIER s'affiche à la place du message NO DIALTONE.
ATX2	Désactiver la surveillance des tonalités d'occupation. Afficher uniquement les messages OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE et CONNECT XXXX. Si la détection de la tonalité d'occupation est activée et qu'une tonalité d'occupation est détectée, le message NO CARRIER s'affiche au lieu du message BUSY. Si l'option de détection de la tonalité de numérotation est activée ou sélectionnée, mais qu'aucune tonalité de numérotation n'est détectée, le message NO CARRIER s'affiche à la place du message NO DIALTONE.
ATX3	Activer la surveillance des tonalités d'occupation. Afficher uniquement les messages OK, CONNECT, RING, NO CARRIER, ERROR, NO DIALTONE et CONNECT ou CARRIER XXXX. Si la détection de la tonalité de numérotation est activée et qu'aucune tonalité de numérotation n'est détectée, le message NO CARRIER s'affiche.
ATX4	Activer la surveillance des tonalités d'occupation. Afficher tous les messages (par défaut).
ATZ0	Réinitialisation logicielle.
AT&C0	Activer le DCD en permanence.
AT&C1	Appliquer l'état du signal porteur au DCD (par défaut).
AT&D0	Ignorer DTR.
AT&D1	Passer au mode d'échappement lorsque la transition ACTIVÉ vers DÉSACTIVÉ est détectée sur le DTR.
AT&D2	Raccrocher, passer en mode de commande et désactiver la réponse automatique lorsque la transition ACTIVÉ vers DÉSACTIVÉ est détectée sur le DTR (par défaut).
AT&D3	Réinitialisation logicielle du modem suite à la transition ACTIVÉ vers DÉSACTIVÉ, comme si une commande ATZ avait été envoyée.
AT&F	Restaurer la configuration par défaut.
AT&G0	Désactiver la tonalité de protection (par défaut).
AT&G1	Activer la tonalité de protection 550 Hz.
AT&G2	Activer la tonalité de protection 1 800 Hz.
AT&K0	Désactiver le contrôle du flux.
AT&K3	Activer le contrôle du flux RTS/CTS (par défaut pour les modes de données).
AT&K4	Activer le contrôle du flux XON/XOFF.
AT&K5	Prendre en charge le contrôle du flux XON/XOFF transparent.
AT&P0	Sélectionner 39:61 comme rapport numérotation/pause à 10 impulsions par seconde (par défaut).
AT&P1	Sélectionner 33:67 comme rapport numérotation/pause à 10 impulsions par seconde.
AT&P2	Sélectionner 39:61 comme rapport numérotation/pause à 20 impulsions par seconde.
AT&P3	Sélectionner 33:67 comme rapport numérotation/pause à 20 impulsions par seconde.

Tableau H.2 Commandes AT de base (suite)

Commande	Description
AT&Q0	Sélectionner le fonctionnement asynchrone direct.
AT&Q5	Sélectionner le mode de correction des erreurs.
AT&Q6	Sélectionner le fonctionnement asynchrone en mode normal (mise en mémoire tampon de la vitesse et contrôle du flux, mais pas de correction des erreurs).
AT&V	Afficher la configuration actuelle du modem. Lorsque cette commande est exécutée, le modem affiche les paramètres actuels des commandes et des registres.
AT%C0	Désactiver la compression des données.
AT%C1	Activer la compression des données MNP 5.
AT%C2	Activer la compression des données V.42 bis (définit S46 bit 1).
AT%C3	Activer la compression des données V.42 bis et MNP 5 (valeur par défaut).
AT%E0	Désactiver le contrôle de la qualité de la ligne et le recyclage automatique.
AT%E1	Activer le contrôle de la qualité de la ligne et le recyclage automatique.
AT%E2	Activer le contrôle de la qualité de la ligne et la gestion vitesse inférieure/vitesse normale (valeur par défaut).
AT%L	Niveau du signal de la ligne. La valeur affichée indique le niveau du signal reçu. Exemple : 009 = -9dBM.
AT%Q	Qualité du signal de la ligne. Affiche la qualité du signal de la ligne (dépend du dispositif d'accès au réseau). L'octet le plus important de la valeur EQM est affiché. En fonction de la valeur EQM, le recyclage ou la gestion vitesse inférieure/vitesse normale peuvent être activés si la commande AT%E1 ou AT%E2 le permet.
AT+MS	Sélectionner/forcer la modulation.

H.1 Sélection de la modulation AT+MS

Ce paramètre composé au format étendu contrôle les capacités de modulation du modem. Il accepte six sous-paramètres :

+MS=<carrier>, <automode>, <min_tx_rate>, <max_tx_rate>, <min_rx_rate), <max_rx_rate><CR>.

Pour connaître les paramètres actuels, saisissez AT+MS?<CR>.

Tableau H.3 Débits pris en charge de la commande +MS

Modulation	Signal porteur	Description
Bell 103	B103	300
Bell 212	B212	1 200
V.21	V21	300
V.22	V22	1 200
V.22 bis	V22	2 400 ou 1 200
V.23	V23C	1 200 réception/75 transmission ou 75 réception/1 200 transmission
V.32	V32	9 600 ou 4 800
V.32 bis	V32B	14 400, 12 000, 9 600, 7 200 ou 4 800
V.34	V34	33 600, 31 200, 28 800, 26 400, 19 200, 16 800, 14 400, 12 000, 9 600, 7 200, 4 800 ou 2 400
V.90	V90	56 000, 54 667, 53 333, 52 000, 50 667, 49 333, 48 000, 46 667, 45 333, 42 667, 41 333, 40 000, 38 667, 37 333, 36 000, 34 667, 33 333, 32 000, 30 667, 29 333, 28 000
K56flex	K56	56 000, 54 000, 52 000, 50 000, 48 000, 46 000, 44 000, 42 000, 40 000, 38 000, 36 000, 34 000, 32 000
V92 en aval	V92	56 000, 54 667, 53 333, 52 000, 50 667, 49 333, 48 000, 46 667, 45 333, 42 667, 41 333, 40 000, 38 667, 37 333, 36 000, 34 667, 33 333, 32 000, 30 667, 29 333, 28 000
V92 en amont	V92	48 000, 46 667, 45 333, 42 667, 41 333, 40 000, 38 667, 37 333, 36 000, 34 667, 33 333, 32 000, 30 667, 29 333, 28 000, 26 667, 25 333, 24 000

H.2 Définir les options de poste téléphonique

Cette commande permet d'activer/de désactiver les options « ligne occupée » et « récupération d'appel sur le poste téléphonique ».

Tableau H.4 Définir les options de poste téléphonique

Valeur de -STE=n	Récupération d'appel sur le poste téléphonique	Ligne occupée
0 (valeur par défaut)	Désactivé	Désactivé
1	Désactivé	Activé
2	Activé	Désactivé
3	Activé	Activé

Si la ligne est occupée et que le modem reçoit une commande ATDT pour un accès sortant, il affiche le code de résultat « LINE-IN-USE » au lieu de décrocher. Si le modem et le poste téléphonique décrochent tous les deux, le modem interrompt la connexion et affiche le code de résultat « OFF-HOOK INTRUSION ».

H.3 Registres S AT

Les registres S utilisent le format suivant : ATSr=n<CR> où « r » correspond au numéro du registre S et « n » au paramètre choisi. Pour connaître le paramètre actuel d'un registre S, saisissez la commande ATSr?<CR> où « r » correspond au registre en question. Le modem affiche alors la valeur du registre S.

Tableau H.5 Registres S AT

Registre	Plage	Unité	Par défaut	Description
S0	0-255	Sonneries	0	Nombre de sonneries avant la réponse. ATS0=1<CR> signifie que la réponse est activée dès la première sonnerie détectée.
S1	0-255	Sonneries	0	Nombre de sonneries comptées.
S2	0-127	ASCII	43	Caractère du code d'échappement.
S3	0-127	ASCII	13	Caractère <CR> utilisé pour terminer une commande.
S4	0-127	ASCII	10	Caractère de saut de ligne.
S5	0-127	ASCII	8	Caractère de retour arrière.
S6	2-255	Secondes	2	Délai d'attente de tonalité.
S7	1-255	Secondes	50	Délai d'attente du signal porteur.
S8	0-255	Secondes	2	Pause lors de la composition (virgule dans la chaîne à composer).
S10	1-255	0,1 s	14	Délai entre la perte du signal porteur et le raccrochage.
S11	50-255	0,01 s	85	Durée de la tonalité DTMF.
S12	0-127	1/50 s	50	Délai de sécurité pour la séquence du code d'échappement.
S24	0-255	1 s	0	Temporisateur de mise en veille.
S29	0-255	10 ms	70	Durée du modificateur de numérotation flash.
S30	0-255	10 s	0	Temporisateur de déconnexion pour cause d'inactivité.
S95			0	Contrôle des codes de résultat.

H.4 Codes de résultat de base du modem

Le modem renvoie certains codes de base en réponse aux commandes AT. Ces codes de résultat peuvent être sous forme de mot (V1) ou numériques (V0) grâce à la commande Vn. La commande Qn contrôle l'envoi des codes (Q0 : envoi activé ; Q1 : envoi désactivé). Les commandes Xn et Wn, ainsi que le registre S95, déterminent le format des codes de résultat que le modem affiche pour indiquer le type de connexion établie. Plus de 300 codes sont disponibles. Les codes les plus courants sont indiqués dans le tableau ci-dessous.

Tableau H.6 Liste des codes de résultat de base

Numérique	Texte	Description
0	OK	Le modem a reçu et traité la commande.
1	CONNECT	La connexion à 300 bit/s a été établie ou les codes de résultat étendus sont désactivés (X0).
2	RING	Un signal d'appel entrant a été détecté.
3	NO CARRIER	Ce code de résultat indique soit une déconnexion intentionnée soit l'impossibilité d'établir une connexion.
4	ERROR	Une commande non valide a été envoyée au modem.
5	CONNECT 1200	Indique une ligne ou une connexion DTE à 1 200 bit/s.
6	NO DIALTONE	
7	BUSY	Le modem a détecté une tonalité d'occupation.
8	NO ANSWER	Le serveur distant n'a pas répondu avant expiration du délai S7.
10	CONNECT 2400	Vitesse de ligne ou connexion DTE à 2 400 bit/s.
12	CONNECT 9600	Vitesse de ligne ou connexion DTE à 9 600 bit/s.
15	CONNECT 14400	Vitesse de ligne ou connexion DTE à 14 400 bit/s.
16	CONNECT 19200	Vitesse de ligne ou connexion DTE à 19 200 bit/s.
17	CONNECT 38400	Vitesse de ligne ou connexion DTE à 38 400 bit/s.
18	CONNECT 57600	Vitesse de ligne ou connexion DTE à 57 600 bit/s.

H.5 Protection des lignes numériques

Le modem possède un circuit de protection des lignes numériques en option, qui détecte automatiquement toute surintensité sur les broches Tip et Ring. Lorsque le modem décroche, il vérifie immédiatement le courant sur les broches Tip et Ring. Si le courant dépasse 150 mA, le modem affiche le code de résultat « DIGITAL LINE DETECTED » avant de couper la communication. Le modem continue à afficher ce code de résultat jusqu'à ce qu'il détecte un courant normal sur les broches Tip et Ring pendant l'utilisation de la ligne. La fonction de protection des lignes numériques protège le modem dans l'éventualité où il serait accidentellement connecté à une ligne téléphonique numérique.

H.6 Utilisation du mode veille

Il est possible de configurer le modem pour passer en mode veille/économie d'énergie grâce à la commande ATS24=n. Dans cette commande, « n » correspond à la durée, en secondes, pendant laquelle le modem fonctionne en mode normal avant de passer en mode veille/économie d'énergie s'il ne détecte aucune activité sur la ligne téléphonique ou la connexion DTE. Le temporisateur est réinitialisé suite à une activité sur la ligne téléphonique ou la connexion DTE. Si S24 est défini sur 0, le modem ne passe jamais en mode veille/économie d'énergie.

H.7 Déconnexion d'un appel

Il existe plusieurs manières de déconnecter un appel. Elles sont décrites ci-dessous.

La réinitialisation de l'alimentation du modem ou l'activation de Reset Line (broche n° 12) entraîne la déconnexion du modem et le fait passer hors ligne.

La désactivation du signal DTR (broche n° 4) désactive également le modem. Si vous utilisez cette méthode, vérifiez que la commande DTR est définie sur &D2 ou &D3 et non pas forcée (&D0).

Un dispositif distant peut également entraîner la déconnexion du modem. Si le modem distant se déconnecte, votre modem perd automatiquement le signal porteur et passe hors ligne.

Vous pouvez également utiliser la commande ATH ou ATZ pour déconnecter un appel. Pour pouvoir envoyer une commande au modem lorsqu'il est en ligne, celui-ci doit être en mode de commande en ligne. Pour ce faire, vous devez utiliser une séquence d'échappement spéciale. La valeur par défaut de cette séquence d'échappement à trois chiffres est le caractère « + » (voir registre S2 pour la modifier). La séquence « +++ » est protégée par un délai d'une seconde avant et après son envoi (voir registre S12 pour modifier ce délai). Lorsque le modem détecte la séquence d'échappement, il affiche le code de résultat OK. Le modem est alors en mode de commande en ligne. Vous pouvez désormais utiliser la commande ATH ou ATZ pour déconnecter l'appel.

H.8 Sélection du code pays

La commande +GCI permet de définir le code pays du modem. Pour sélectionner un des 30 pays disponibles, exécutez la commande AT+GCI=n, où « n » correspond au code à deux chiffres du pays souhaité. Vous devez répéter cette commande à chaque fois que vous allumez le modem, car ce paramètre n'est pas stocké ou enregistré automatiquement. Il doit faire partie de la chaîne d'initialisation.

Exemple : AT+GCI=00<CR> Signification : sélectionner le code pays correspondant au Japon.

OK Signification : le modem a accepté la commande et

il est désormais configuré pour être utilisé au Japon.

AT+GCI?<CR> Signification : afficher le code pays actuel.

+GCI:00 Signification : le code pays actuel correspond au Japon.

OK

Pour connaître les pays disponibles dans le firmware du modem, saisissez AT+GCI=?<CR>.

Le modem affiche tous les codes pays à deux chiffres disponibles.

Tableau H.7 Liste des codes pays

Pays	Code	Pays	Code	Pays	Code
Australie	09	Hong Kong	50	Pologne	8A
Autriche	0A	Inde	53	Portugal	8B
Belgique	0F	Irlande	57	Afrique du Sud	9F
Brésil	16	Italie	59	Singapour	9C
Chine	26	Japon	00	Espagne	A0
Danemark	31	Corée	61	Suède	A5
Finlande	3C	Mexique	73	Suisse	A6
France	3D	Pays-Bas	7B	Taïwan	Fe
Allemagne	42	Norvège	82	TBR21	FD
États-Unis	B5	Royaume-Uni	B4		

H.9 Fonction de présentation du numéro

Le modem peut être utilisé pour afficher certaines informations concernant les appels téléphoniques entrants, à savoir la date, l'heure, le numéro de téléphone et le nom associé à l'appel. Lorsque l'option CID est activée, les informations s'affichent entre la première et la deuxième sonnerie entrante (« RING »). Pour utiliser cette fonctionnalité, la ligne téléphonique connectée au modem doit être abonnée au service de présentation du numéro de l'opérateur téléphonique local. Voici un exemple des informations affichées :

RING

DATE = 0513

TIME = 1346

NMBR = 408 767 8900

NAME = RADICOM RESEARCH

RING

Les informations de l'option CID peuvent être sans format ou au format ci-dessous. Les commandes +VCID et +VRID permettent de contrôler l'option CID du modem.

Tableau H.8 Présentation du numéro (CID)

Commande	Paramètre	Description
+VCID?	N/A	Affiche le paramètre +VCID actuel (0-2).
+VCID=	0	Désactive la présentation du numéro (par défaut).
+VCID=	1	Active la présentation du numéro formatée sur le DTE.
+VCID+	2	Active la présentation du numéro sans format sur le DTE.
+VRID=	0	Affiche le numéro formaté pour le dernier appel reçu.
+VRID+	1	Affiche le numéro sans format pour le dernier appel reçu.

Annexe I: Réglementation concernant le modem analogique installé dans ce produit

I.1 Analog Telecom Safety Warnings

Before servicing, disconnect this product from its power source and telephone network. Also:

- Never install telephone wiring during a lightning storm.
- Never install a telephone jack in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

I.2 Avertissements de sécurité concernant les télécommunications analogiques

Avant l'entretien, débranchez ce produit de la source d'alimentation et du réseau téléphonique. Par ailleurs :

- Ne raccordez jamais les câbles téléphoniques pendant un orage.
- Ne raccordez jamais les prises téléphoniques dans des endroits humides à moins que la prise ne soit spécialement conçue pour ce type d'endroit.
- Ne touchez jamais les câbles ou terminaux téléphoniques non isolés à moins que la ligne téléphonique n'ait été déconnectée de l'interface réseau.
- Faites preuve de prudence lors du raccordement ou de la modification des lignes téléphoniques.

I.3 Restrictions concernant les modèles internationaux de modems

Les paramètres par défaut et les restrictions concernant la numérotation et la réponse peuvent varier selon les modèles internationaux de modems. Lorsque vous modifiez les paramètres, il est possible que le modem ne soit plus conforme aux réglementations nationales en vigueur dans certains pays. Notez également que des fonctionnalités ou le manque de restrictions de certains packs logiciels peut entraîner la non-conformité du modem.

États-Unis, 47 CFR Partie 68 - Télécommunications

1. Cet équipement est conforme à la partie 68 du règlement 47 CFR, ainsi qu'aux exigences adoptées par l'ACTA (Administrative Council for Terminal Attachments). Cet équipement comporte une étiquette qui indique, entre autres, le numéro d'enregistrement et le numéro REN (Ringer Equivalence Number) ou un identifiant produit au format suivant :

   Produits actuels : US:AAAEQ##Txxxx.

   Anciennes versions des produits : AU7USA-xxxxx-xx-x.

   Vous devez indiquer ce numéro à l'opérateur téléphonique s'il vous le demande.

2. La fiche et la prise utilisées pour brancher cet équipement sur les câbles du site et du réseau téléphonique doivent être conformes au règlement 47 CFR Partie 68 applicable adoptée par l'ACTA. L'équipement est conçu pour être branché sur une prise modulaire compatible également conforme.
3. Le Ringer Equivalence Number (REN) sert à déterminer le nombre de dispositifs pouvant être connectés à une ligne téléphonique. En cas de REN excessif sur une ligne téléphonique, il est possible que les dispositifs ne sonnent pas en réponse à un appel entrant. Dans la plupart des régions, la somme des REN ne doit pas dépasser cinq (5,0). Pour vous assurer du nombre total de dispositifs que vous pouvez connecter à une ligne, tel que déterminé par le total des REN, contactez votre opérateur téléphonique local. Dans le cas des produits approuvés après le 23 juillet 2001, le REN fait partie de l'identifiant qui se présente au format US:AAAEQ##Txxxx. Les chiffres représentés par ## sont le REN sans la virgule (par exemple, 03 correspond à un REN de 0,3). Dans le cas des produits antérieurs, le REN est indiqué à part sur l'étiquette.
4. Si cet équipement venait à endommager le réseau téléphonique, l'opérateur téléphonique pourra, le cas échéant, vous informer à l'avance de l'interruption temporaire du service téléphonique. S'il ne peut pas vous envoyer de préavis, l'opérateur téléphonique vous avertira dès que possible. Vous serez par ailleurs informé de votre droit de vous plaindre auprès de la FCC si vous l'estimez nécessaire.
5. L'opérateur téléphonique peut modifier ses installations, équipements, opérations ou procédures, ce qui peut affecter le fonctionnement de cet équipement. Dans ce cas, l'opérateur téléphonique vous en avertira à l'avance pour vous permettre d'effectuer les changements nécessaires au maintien du service.
6. En cas de problèmes avec cet équipement, veuillez contacter Vertiv à l'adresse indiquée ci-dessous afin de savoir comment le faire réparer. Si cet équipement endommage le réseau téléphonique, l'opérateur téléphonique pourra vous demander de le débrancher jusqu'à ce que le problème soit résolu.
7. Informations de fabrication relatives au dispositif de télécommunication (modem) :

   Fabricant : Multi-Tech Systems, Inc.

   Nom commercial : Socket Modem SocketModem SocketModem

   Numéro de modèle : MT5692SMI

   Numéro d'enregistrement : US:AU7MM01BMT5692SMI

   REN : 0,1 B

   Prise modulaire (USOC) : RJ11C, RJ11W ou RJ45 (ligne simple)

   Vertiv

   4991 Corporate Drive

   Huntsville, AL 35805 États-Unis

   1-888-793-8763

I.4 Autorisation en Thaïlande pour le modèle MT5692SMI

Ce dispositif de télécommunications est conformes aux exigences de NTC1.

1NTC (National Telecommunications Commission) est l'organisme chargé de réguler les télécommunications en Thaïlande.

"เครื่องโทรคมนาคมและอุปกรณ์นี้มีความสอดคล้องตามข้อกำหนดของ กทช."

I.5 Avertissement concernant les dispositifs de télécommunications en Nouvelle-Zélande

1. L'octroi de la licence Telepermit pour un équipement de terminal indique que Telecom accepte la conformité de cet article aux exigences minimales de connexion à son réseau. Cette licence n'indique en aucun cas que le produit a été approuvé par Telecom et n'implique aucune garantie quelle qu'elle soit. En particulier, elle ne garantit pas un fonctionnement correct dans tous les aspects avec un autre équipement de marque ou de modèle différent ayant également obtenu la licence Telepermit. Elle n'implique pas non plus la compatibilité d'un produit avec tous les services du réseau de Telecom.

   Cet équipement n'est pas capable, quelles que soient les conditions de fonctionnement, de fonctionner correctement à des vitesses plus élevées que celles pour lesquelles il a été conçu. Le débit des connexions à 33,6 kbit/s et à 56 kbit/s peut être réduit lorsque l'équipement est relié à un réseau téléphonique public commuté. Telecom décline toute responsabilité en cas de difficultés provoquées par de telles circonstances.

2. Si l'équipement a subi des dommages physiques, débranchez-le immédiatement et faites-le réparer ou remplacer.
3. Ce modem ne doit en aucun cas être utilisé d'une manière qui pourrait nuire aux autres clients de Telecom.
4. Cet équipement est doté de la numérotation par impulsions, alors que la norme de Telecom est la numérotation par tonalités DTMF. Rien ne garantit que les lignes de Telecom seront toujours compatibles avec la numérotation par impulsions.

   L'utilisation de la numérotation par impulsions sur une ligne partagée par plusieurs équipements peut provoquer un déclenchement de la sonnerie ou des parasites, ainsi qu'une réponse erronée. Si ce type de problème se produit, l'utilisateur ne doit PAS contacter les services techniques de Telecom.

   La méthode de numérotation recommandée est la numérotation DTMF, car elle est plus rapide que la numérotation par impulsions (décimale) et qu'elle est disponible sur presque tous les standards téléphoniques néo-zélandais.

5. Avertissement : il est impossible d'appeler le 111 (services d'urgence) ou un autre numéro sur cet appareil lors d'une coupure de courant.
6. Cet équipement ne permet pas de transmettre un appel sur un autre dispositif branché sur la même ligne.
7. Certains paramètres nécessaires pour la conformité avec la licence Telepermit dépendent de l'équipement (ordinateur) associé au dispositif. L'équipement associé doit respecter les limites suivantes pour être conforme aux exigences de Telecom :

Pour les appels répétés au même numéro :

- Le nombre de tentatives d'appel vers le même numéro sur une période de 30 minutes par appel manuel initié ne doit pas dépasser 10.
- L'appareil doit être raccroché pendant au moins 30 secondes entre chaque tentative d'appel.
- Pour les appels automatiques vers des numéros différents :
- L'équipement doit être configuré de sorte que les appels automatiques vers des numéros différents soient espacés d'au moins 5 secondes entre la fin d'un appel et le début de l'appel suivant.

8. Pour garantir un fonctionnement correct, le total des REN de tous les appareils branchés sur une même ligne ne doit pas dépasser 5.

I.6 Avis pour le Japon

Ce modem est conforme à la norme JATE (Japan Approval Institute for Telecommunications Equipment) suivante :

MT5692SMI - Approbation JATE A09-0123001

Connect with Vertiv on Social Media


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


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


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


https://www.twitter.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, États-Unis

590-1536-506H