Raritan EMX

Manuel d'utilisation
Version 2.1.0

EMX-0C-v2.1-F

Mars2012

255-80-6107-00

Informations FCC

Le présent équipement a été soumis à des essais, de manière à établir sa conformité avec les limites afférentes à un appareil numérique de classe A, en vertu de la section 15 des réglementations de la FCC. Ces limites sont destinées à assurer une protection raisonnable contre les interférences nocives dans une installation commerciale. Cet appareil génère, utilise et émet de l'énergie de fréquences radio et peut, en cas d'installation ou d'utilisation non conforme aux instructions, engendrer des interférences nuisibles au niveau des communications radio. L'utilisation de l'équipement dans un environnement résidentiel peut générer des interférences nuisibles.

Informations VCCI (Japon)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan n'est pas responsable des dommages causés à ce produit suite à un accident, un désastre, une mauvaise utilisation, un abus d'utilisation, une modification non Raritan apportée au produit, ou à d'autres événements échappant au contrôle raisonnable de Raritan ou ne résultant pas de conditions normales de fonctionnement.

CE c UL us LISTED 1F61 I.T.E.

Table des matières

Chapitre 10 Utilisation de l'interface de ligne de commande 211

Chapitre 1 Introduction

Dans ce chapitre

Aperçu

Le dispositif EMX fournit une solution de gestion des racks alliant des fonctionnalités de gestion des ressources et de surveillance d'environnement.

Avec la fonctionnalité de gestion des ressources, vous pouvez assurer le suivi à distance de l'emplacement des équipements informatiques après avoir étiqueté ceux-ci électroniquement. Cette fonction est particulièrement utile lorsque vous devez gérer des centaines de dispositifs informatiques.

Les éléments ci-après sont nécessaires pour le paramétrage d'un système de gestion des ressources :

- Etiquettes de gestion des ressources Raritan : vous libellez un dispositif informatique en collant une étiquette électronique de gestion des ressources dessus.
- Capteurs de gestion des ressources Raritan (capteurs de ressources) : chaque capteur de ressources transmet les données concernant l'étiquette et l'emplacement au dispositif EMX.
- Dispositif EMX : vous pouvez localiser à distance chaque dispositif informatique étiqueté par le biais du dispositif EMX.

Grâce aux capteurs d'environnement Raritan connectés au dispositif EMX, vous pouvez surveiller à distance les conditions d'environnement du centre de données ou de la salle de serveurs, telles que la température ou l'humidité.

Lorsqu'une webcam Logitech® QuickCam® Pro 9000 est connectée, un système simple de caméra et de vidéosurveillance est construit, qui affiche des instantanés ou des vidéos en temps réel de la salle de serveurs ou du centre de données pour améliorer la surveillance et la sécurité.

Les événements et les actions déclenchés lorsqu'un événement a lieu sont pris en charge par EMX. Particulièrement, des courriels, des événements de journal, des messages syslog, des instantanés de webcam, des traps SNMP et des SMS peuvent être déclenchés lorsque les événements que vous définissez ont lieu. Des textes personnalisés peuvent être configurés pour les courriels, et des images capturées par la webcam peuvent être envoyées aux utilisateurs par courriel.

De plus, le dispositif EMX prend en charge l'intégration avec un échangeur thermique Schroff® LHX-20 ou LHX-40, qui attire l'air chaud dans l'échangeur thermique air/eau pour refroidir l'air. Cette intégration offre une solution de surveillance à distance de l'échangeur thermique. EMX peut également être utilisé conjointement à l'application de gestion des centres de données Raritan, dcTrack™.

Ce manuel d'utilisation décrit les modèles suivants :

- EMX2-111
- EMX2-888

Modèles du produit

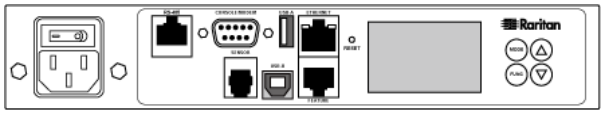
Les dispositifs EMX comprennent deux modèles : EMX2-111 et EMX2-888.

Les modèles ont des fonctionnalités identiques mais sont de taille différente et disposent d'un nombre total de ports différent.

EMX2-111

EMX2-111 est un modèle Zéro U comportant les ports et composants suivants :

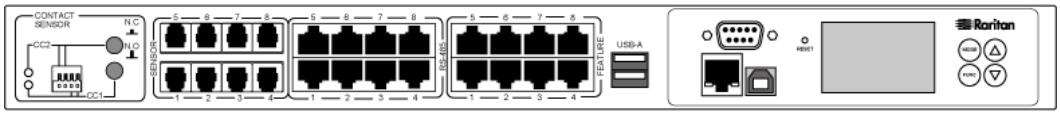
- 1 port de capteur
- 1 port de fonction
- 1 port RS-485
- 2 ports USB (1 USB-A et 1 USB-B)
- 1 port RS-232
- 1 port Ethernet
- 1 écran LCD
- Boutons de contrôle



EMX2-888

EMX2-888 est un modèle 1U comportant les ports et composants suivants :

- 8 ports de capteur
- 8 ports de fonction
- 8 ports RS-485
- 3 ports USB (2 USB-A et 1 USB-B)
- 1 port RS-232
- 1 port Ethernet
- 1 écran LCD
- Boutons de contrôle
- Terminaison de capteur de fermeture de contact



Caractéristiques du produit

En général, les fonctions de EMX comprennent :

- la possibilité d'effectuer le suivi de l'emplacement de chaque équipement informatique étiqueté électroniquement à l'aide des étiquettes de gestion des ressources Raritan ;
- le changement de couleur du voyant sur le capteur de ressources pour faire la différence entre les étiquettes de gestion des ressources détectées et non détectées ;
- la prise en charge d'un câblage de 10 mètres au maximum sur le dispositif EMX-888 et d'1 mètre pour le dispositif EMX-111 pour chaque capteur de ressources connecté ;
- la possibilité de surveiller les facteurs d'environnement, tels que la température externe et l'humidité ;
- des attributs d'emplacement spécifiés par l'utilisateur pour les capteurs d'environnement ;
- la possibilité d'afficher les températures en Celsius ou en Fahrenheit, la hauteur en mètres ou en pieds, et la pression en pascal ou en psi selon les informations d'identification de l'utilisateur.
- la prise en charge de 130 capteurs d'environnement pour EMX-888 et de 16 pour EMX-111 ;
- la prise en charge de la mise en cascade des dispositifs AMS et/ou PX2 connectés à EMX ;
- la prise en charge de SNMP v1, v2 et v3 ;
- la capacité d'envoyer des traps à l'aide du protocole SNMP ;
- la capacité de configurer et de définir des valeurs via SNMP ;
- la prise en charge des services SSH et Telnet ;
- Pour SSH, les authentifications de mot de passe et de clé publique sont prises en charge.
- la prise en charge de la publication des services ;
- la capacité d'enregistrer les paramètres de configuration d'un dispositif EMX, puis de déployer ceux-ci sur d'autres dispositifs EMX identiques ;
- la prise en charge du détecteur d'inclinaison implémenté sur des capteurs de ressources Raritan ;
- la connexion sans fil via un adaptateur LAN USB sans fil fourni par Raritan ;
- la capacité de surveiller l'environnement de centre de données à l'aide d'une webcam Logitech® QuickCam® Pro 9000 connectée ;
- la prise en charge d'images de webcam envoyées par courriel à des destinataires désignés ;

- la prise en charge des modems GSM Cinterion® MC52i qui vous permettent d'envoyer des SMS personnalisés à des destinataires désignés pour des événements particuliers ;
- la capacité d'envoyer des courriels, des détails de journal et/ou de définir des traps SNMP pour des événements particuliers ;
- la capacité de surveiller un échangeur thermique Schroff® LHX-20 ou LHX-40 connecté ;
- la capacité d'établir un diagnostic du réseau, tel qu'un test ping d'un hôte ou la liste des connexions TCP
- la capacité à surveiller l'accessibilité du serveur ;
- Option de reprise totale après sinistre en cas d'une panne catastrophique lors d'une mise à niveau de firmware

Contenu de l'emballage

Le tableau suivant décrit le matériel livré avec chaque dispositif EMX. Si des pièces manquent ou sont endommagées, contactez le revendeur local ou le support technique de Raritan pour obtenir de l'aide.

- Dispositif EMX
- Câble d'alimentation
- Paquet de pattes de fixation et vis
- Capteurs de ressources (facultatif)
- Etiquettes de gestion de ressources (facultatif)

Chapitre 2 Installation et configuration du dispositif EMX

Dans ce chapitre

Avant de commencer

Préparez le site d'installation. Assurez-vous que la zone d'installation est propre et non exposée à des températures extrêmes ou à l'humidité. Veillez à laisser un espace suffisant autour du dispositif EMX pour le câblage et le branchement des capteurs de ressources.

Montage du dispositif EMX

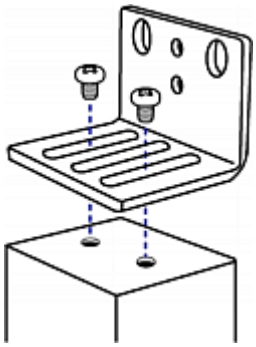
Suivant le modèle acheté, la méthode de montage d'un dispositif EMX varie.

Montage d'un dispositif EMX Zéro U

Cette section décrit comment monter un dispositif EMX Zéro U à l'aide de pattes de fixation en L et de deux boutons.

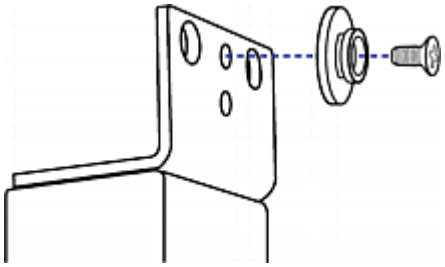
Pour monter des modèles Zéro U avec des pattes de fixation en L et deux boutons :

1. Alignez le deux fentes extérieures de la patte de fixation en L avec les deux trous de vis en haut du dispositif EMX.
2. Vissez la patte de fixation en L au dispositif et assurez-vous qu'elle est solidement installée.



3. Répétez les étapes 1 et 2 pour visser une autre patte de fixation en L au bas du dispositif.
4. Une fois les deux pattes de fixation en L installées sur le dispositif, vous pouvez choisir une des méthodes suivantes pour monter le dispositif dans le rack.
   - A l'aide des vis du rack, fixez le dispositif au rack à l'aide des deux trous identiques près du bord de chaque patte de fixation en L.

- Montez le dispositif en vissant un bouton de montage dans le trou central de chaque patte de fixation en L et en engageant les deux boutons dans les trous de montage du rack. Le couple recommandé pour le bouton est de 1,96 N·m (20 kgf·cm).



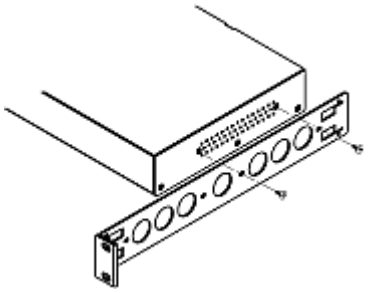
Montage d'un dispositif EMX 1U

A l'aide des supports de fixation et des outils appropriés, attachez le dispositif EMX 1U au rack ou à l'armoire.

Pour monter le dispositif EMX 1U :

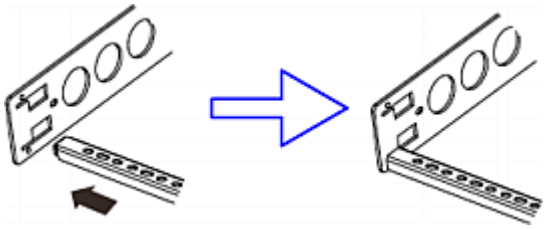
1. Attachez une patte de fixation pour le montage en rack à l'un des côtés du dispositif EMX.
   a. Alignez deux trous ovales de la patte de fixation pour le montage en rack avec deux trous taraudés sur un côté du dispositif EMX.
   b. Fixez la patte de fixation pour le montage en rack avec deux des vis fournies par Raritan.

Remarque : l'emplacement approprié des trous ovales de la patte de fixation pour le montage en rack peut varier selon les trous taraudés de votre modèle.

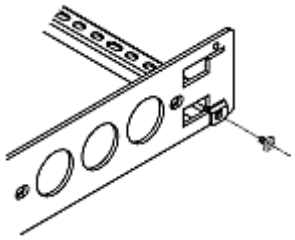


2. Répétez l'étape 1 pour fixer l'autre patte de fixation de l'autre côté de EMX.

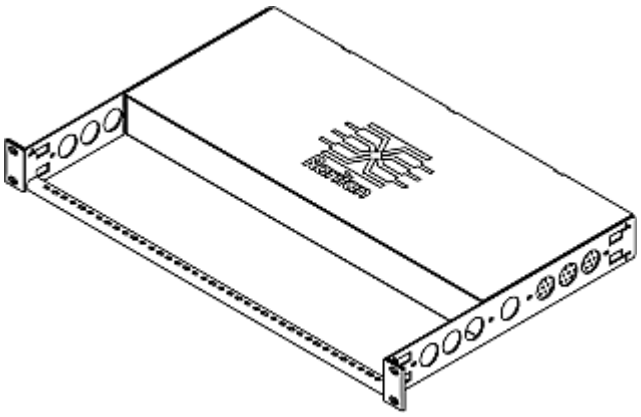
3. Insérez une extrémité de la barre de support de câble dans le trou en L de la patte de fixation pour le montage en rack, et alignez le trou à l'extrémité de la barre avec le trou taraudé adjacent au trou en L.



4. Fixes la barre de support de câble avec une des vis filetées fournies par Raritan.



5. Répétez les étapes 3 et 4 pour fixer l'autre extrémité de la barre de support de câble à l'autre patte de fixation pour le montage en rack.

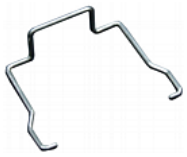


6. Montez le dispositif EMX sur le rack en serrant les oreilles des pattes de fixation pour montage en rack sur les rails avant du rack avec vos propres vis, boulons, écrous à cage, etc.

Connexion de EMX à une source d'alimentation

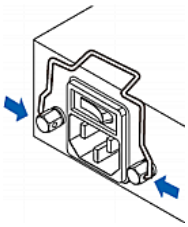
Si votre dispositif EMX est conçu pour utiliser un clip de maintien de câble, installez le clip avant de brancher un cordon d'alimentation. Le clip empêche au cordon branché de se détacher ou de tomber.

L'utilisation des clips de maintien des câbles est fortement recommandée dans les régions à forte activité sismique, et les environnements où les chocs et les vibrations sont à prévoir.

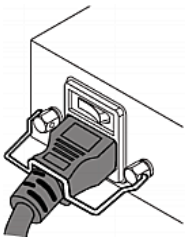


Pour connecter le dispositif EMX à une source d'alimentation :

1. Installez le clip de maintien de câble en insérant les deux extrémités dans les petits orifices des deux vis hexagonales placées de chaque côté de la prise.



2. Branchez l'une des extrémités du cordon d'alimentation fourni par Raritan dans la prise et enfoncez le clip de maintien de câble vers le cordon d'alimentation jusqu'à ce que ce dernier soit bien maintenu.



3. Branchez l'autre extrémité du cordon d'alimentation sur une autre source d'alimentation appropriée.

Configuration du dispositif EMX

Pour configurer le dispositif EMX :

1. Reliez le dispositif EMX à un ordinateur à l'aide d'une connexion série ou USB.

2. Reliez le dispositif EMX au réseau à l'aide d'une connexion câblée ou sans fil.
3. Configurez le dispositif EMX à l'aide de l'interface de ligne de commande.

Connexion du dispositif EMX à un ordinateur

Pour configurer EMX à l'aide d'un ordinateur, il doit être connecté à ce dernier par le biais d'une interface série RS-232. L'ordinateur doit être doté d'un programme de communication, tel que HyperTerminal ou PuTTY.

Si votre ordinateur ne comporte pas de port série, utilisez un câble USB standard pour connecter EMX à l'ordinateur pour la configuration initiale. Le dispositif EMX peut émuler un convertisseur USB vers série après l'installation correcte du pilote USB-série dans le système d'exploitation Windows®.

Remarque : les convertisseurs série vers USB ne fonctionnent pas tous correctement avec le dispositif EMX. Cette section ne présente donc pas leur utilisation.

Connectez maintenant EMX à un ordinateur pour la configuration initiale en suivant l'une des procédures ci-après.

Pour établir une connexion série :

1. Connectez une extrémité du câble null-modem au port RS-232 libellé CONSOLE / MODEM sur le dispositif EMX.
2. Connectez l'autre extrémité du câble null-modem au port série (COM) de l'ordinateur.

Pour établir une connexion USB :

1. Branchez une extrémité d'un câble USB standard sur le port USB-B du dispositif EMX.
2. Connectez l'autre extrémité du câble USB au port USB-A de l'ordinateur.

Installation du pilote USB vers série

Le dispositif EMX peut émuler un convertisseur USB vers série via une connexion USB. Un pilote USB-série nommé Dominion Serial Console est requis pour les systèmes d'exploitation Microsoft® Windows®. Téléchargez le fichier de pilote *dominion-serial.zip*, qui contient les fichiers *dominion-serial.inf* et *dominion-serial-setup.exe*, du ***site Web de Raritan http://www.raritan.com*** sous la section ***Firmware and Documentation http://www.***, ***http://www.raritan.com/support/firmware-and-documentation/*** du dispositif EMX.

Pour installer le pilote sous Windows® Vista et 7 :

1. Déconnectez le câble USB du dispositif EMX de l'ordinateur.
2. Lancez dominion-serial-setup.exe. Dominion Serial Console Driver Setup Wizard (Assistant de paramétrage du pilote de la console série Dominion) apparaît.
3. Cliquez sur Install pour installer le pilote.
4. Cliquez sur Finish lorsque l'installation est terminée.
5. Connectez le câble USB du dispositif EMX à l'ordinateur. Le pilote est installé automatiquement.

Pour installer le pilote sous Windows® XP :

1. Déconnectez le câble USB du dispositif EMX de l'ordinateur.
2. Vérifiez que le fichier usbser.sys est disponible dans C:\Windows\ServicePackFiles\i386. Sinon, vous devez l'extraire du CD d'installation de Windows et le copier dans le répertoire où est stocké le pilote USB-série.
   - Sur un CD comportant la version SP3, le fichier est extrait de I386\SP3.CAB.
   - Sur un CD comportant la version SP2, il est extrait de I386\SP2.CAB.
   - Sur un CD sans SP, il est extrait de I386\DRIVER.CAB.
3. Connectez le câble USB du dispositif EMX à l'ordinateur.
4. L'ordinateur détecte le nouveau dispositif et la boîte de dialogue Assistant Matériel détecté s'ouvre. Si la boîte de dialogue n'apparaît pas, choisissez Panneau de configuration > Système > Matériel > Gestionnaire de périphériques, cliquez avec le bouton droit de la souris sur Dominion Serial Console et choisissez Mettre le pilote à jour.
5. Sélectionnez Installer à partir d'une liste ou d'un emplacement spécifié, puis définissez l'emplacement de stockage du pilote.

6. Si le message réclamant le fichier usbser.sys apparaît, indiquez l'emplacement de ce fichier.
7. L'installation est terminée.

Sous Linux :

Aucun pilote supplémentaire n'est requis, mais vous devez fournir le nom du dispositif tty présent dans la sortie de dmesg après la connexion du dispositif EMX à l'ordinateur. Habituellement, le dispositif tty est /dev/ttyACM# ou /dev/ttyUSB#, # étant un nombre entier.

Par exemple, si vous utilisez le programme de terminal kermit et que le dispositif tty est /dev/ttyACM0, effectuez les commandes suivantes :

> set line /dev/ttyACM0

> connect

Connexion du dispositif EMX au réseau

Pour utiliser l'interface Web afin d'administrer EMX, vous devez connecter le dispositif EMX au réseau local (LAN). EMX peut être connecté à un réseau câblé ou sans fil.

Pour établir une connexion câblée :

1. Raccordez un câble UTP Catégorie 5e/6 standard au port ETHERNET du dispositif EMX.
2. Branchez l'autre fiche du câble sur le réseau local.

Pour établir une connexion sans fil :

Effectuez une des opérations suivantes :

- Branchez un adaptateur de réseau local USB sans fil 802.11n dans le port USB-A du dispositif EMX.
- Branchez une station d'accueil USB sur le port USB-A du dispositif EMX et connectez l'adaptateur de réseau local USB sans fil 802.11n au port USB approprié de la station d'accueil.

Configuration du réseau local sans fil pris en charge

Si vous sélectionnez la connexion sans fil, assurez-vous que l'adaptateur de réseau local USB et la configuration du réseau sans fil répondent aux exigences suivantes.

- Type de réseau : 802.11n
- Protocole : WPA2 (RSN)
- Gestion des clés : WPA-PSK
- Chiffrement : CCMP (AES)

Important : actuellement, seuls les adaptateurs de réseau USB sans fil fournis par Raritan sont pris en charge. Adressez-vous au support technique Raritan pour plus d'informations.

Configuration initiale du réseau

Une fois le dispositif EMX connecté au réseau, vous devez lui fournir une adresse IP et d'autres informations de réseau.

Cette section décrit la configuration initiale via une connexion série ou USB. Pour configurer EMX via le réseau local, reportez-vous à ***Modification de la configuration du réseau (BCM, EMX, PX2, PXE)*** (voir "***Modification de la configuration réseau***" à la page 80).

Pour configurer le dispositif EMX :

1. Sur l'ordinateur que vous avez connecté à EMX, ouvrez un programme de communication, tel que HyperTerminal ou PuTTY.
2. Sélectionnez le port COM approprié et assurez-vous que les paramètres du port sont configurés comme suit :
   - Bits par seconde = 115200 (115,2Kbps)
   - Bits de données = 8
   - Bits d'arrêt = 1
   - Parité = Néant
   - Contrôle de flux = Néant

   Conseil : pour une connexion USB, vous pouvez déterminer le port COM affecté à EMX en choisissant Panneau de configuration > Système > Matériel > Gestionnaire de périphériques et en repérant la console série Dominion sous le groupe Ports.
3. Appuyez sur Entrée.
4. EMX vous invite à vous connecter. Notez que le nom d'utilisateur et le mot de passe sont sensibles à la casse.
   a. A l'invite Username, tapez `admin` et appuyez sur Entrée.
   b. A l'invite Password, tapez `raritan` et appuyez sur Entrée.
5. S'il s'agit de la première connexion à EMX, vous êtes invité à modifier le mot de passe. Suivez les instructions à l'écran pour taper votre nouveau mot de passe.
6. L'invite # apparaît lorsque la connexion aboutit.
7. Tapez `config` et appuyez sur Entrée.
8. Pour configurer des paramètres réseau, tapez les commandes appropriées et appuyez sur Entrée. Toutes les commandes sont sensibles à la casse.

a. Pour définir le mode de mise en réseau, tapez cette commande :

```
network mode <mode>
```

où <mode> est *wired* pour une connexion câblée (valeur par défaut) ou *wireless* pour une connexion sans fil.

b. Pour le mode de réseau câblé, vous pouvez configurer les paramètres d'interface LAN. Dans la plupart des cas, le paramètre par défaut (auto) fonctionne bien et ne devrait être modifié qu'en cas de besoin.

Pour définir	Utilisez cette commande
LAN interface speed (Vitesse de l'interface LAN)	`network interface LANInterfaceSpeed <option>` où <option> est *auto*, *10Mbps* ou *100Mbps*.
LAN interface duplex mode (Mode bidirectionnel de l'interface LAN)	`network interface LANInterfaceDuplexMode <mode>` où <mode> est *half*, *full* ou *auto*.

Conseil : vous pouvez combiner plusieurs commandes pour modifier plusieurs paramètres en même temps. Par exemple, `network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>`

c. Pour le mode réseau sans fil, vous devez configurer le paramètre de nom de réseau sans fil (SSID).

Pour définir	Utilisez cette commande
SSID	`network wireless SSID <ssid>` où <ssid> représente la chaîne SSID.

Au besoin, configurez les paramètres sans fil supplémentaires présentés dans le tableau suivant.

Pour définir	Utilisez cette commande
BSSID	`network wireless BSSID <bssid>` où <bssid> représente l'adresse MAC du point d'accès.
la méthode d'authentification	`network wireless authMethod <method>` où <method> est *psk* pour Clé prépartagée ou *eap* pour Extensible Authentication Protocol.
PSK	`network wireless PSK <psk>` où <psk> représente la chaîne PSK.
l'authentification externe EAP	`network wireless eapOuterAuthentication <outer_auth>` où <outer_auth> représente *PEAP*.
l'authentification interne EAP	`network wireless eapInnerAuthentication <inner_auth>` où <inner_auth> représente *MSCHAPv2*.
l'identité EAP	`network wireless eapIdentity <identity>` où <identity> représente votre nom d'utilisateur pour l'authentification EAP.
le mot de passe EAP	`network wireless eapPassword` A l'invite, tapez le mot de passe d'authentification EAP.
le certificat d'autorité de certification EAP	`network wireless eapCACertificate` Lorsque vous êtes invité à entrer le certificat d'autorité de certification, ouvrez-le à l'aide d'un éditeur de texte, copiez et collez le contenu dans le programme de communication.

Remarque : le contenu à copier du certificat d'autorité de certification N'INCLUT PAS la première ligne contenant BEGIN CERTIFICATE et la dernière contenant END CERTIFICATE.

d. Pour déterminer le protocole IP activé et l'adresse IP renvoyée par le serveur DNS utilisée, configurez les paramètres suivants.

Pour définir	Utilisez cette commande
le protocole IP	`network ip proto <protocol>` où <protocol> est *v4Only* pour activer IPv4, *v6Only* pour activer IPv6 ou *both* pour activer les deux protocoles.
adresse IP retournée par le serveur DNS	`network ip dnsResolverPreference <resolver>` où <resolver> est *preferV4* pour les adresses IPv4 ou *preferV6* pour les adresses IPv6.

e. Si vous avez activé le protocole IPv4 lors de l'étape précédente, configurez les paramètres réseau IPv4.

Pour définir	Utilisez cette commande
la méthode de configuration IP	`network ipv4 ipConfigurationMode <mode>` où <mode> est *dhcp* pour une configuration automatique (valeur par défaut) ou *static* pour indiquer une adresse IP statique.

- Pour la configuration IPv4 DHCP, configurez ce paramètre.

Pour définir	Utilisez cette commande
le nom d'hôte privilégié (facultatif)	`network ipv4 preferredHostName <name>` où <name> est le nom d'hôte privilégié.

Conseil : pour remplacer les serveurs DNS IPv4 affectés par DHCP par ceux que vous indiquez manuellement, tapez cette commande :

`network ipv4 overrideDNS <option>`

où <option> est `enable` ou `disable`. Consultez le tableau ci-dessous pour obtenir les commandes IPv4 permettant de définir manuellement les serveurs DNS.

- Pour la configuration IPv4 statique, configurez ces paramètres.

Pour définir	Utilisez cette commande
l'adresse IPv4 statique	`network ipv4 ipAddress <ip address>` où <ip address> est l'adresse IP à affecter.
le masque de sous-réseau	`network ipv4 subnetMask <netmask>` où <netmask> est le masque de sous-réseau.
la passerelle	`network ipv4 gateway <ip address>` où <ip address> est l'adresse IP de la passerelle.
le serveur DNS principal	`network ipv4 primaryDNSServer <ip address>` où <ip address> est l'adresse IP du serveur DNS principal.
le serveur DNS secondaire (facultatif)	`network ipv4 secondaryDNSServer <ip address>` où <ip address> est l'adresse IP du serveur DNS secondaire.

f. Si vous avez activé IPv6 lors de l'étape précédente, configurez les paramètres réseau IPv6.

Pour définir	Utilisez cette commande
la méthode de configuration IP	`network ipv6 ipConfigurationMode <mode>` où <mode> est *automatic* pour une configuration automatique (valeur par défaut) ou *static* pour indiquer une adresse IP statique.

Conseil : pour remplacer les serveurs DNS IPv6 affectés par DHCP par ceux que vous indiquez manuellement, tapez cette commande :

`network ipv6 overrideDNS <option>`

où <option> est `enable` *ou* `disable`*. Consultez le tableau ci-dessous pour obtenir les commandes IPv6 permettant de définir manuellement les serveurs DNS.*

- Pour la configuration IPv6 statique, configurez les paramètres suivants. Notez que l'adresse IP doit suivre le format IPv6.

Pour définir	Utilisez cette commande
l'adresse IPv6 statique	`network ipv6 ipAddress <ip address>` où <ip address> est l'adresse IP à affecter.
la passerelle	`network ipv6 gateway <ip address>` où <ip address> est l'adresse IP de la passerelle.
le serveur DNS principal	`network ipv6 primaryDNSServer <ip address>` où <ip address> est l'adresse IP du serveur DNS principal.
le serveur DNS secondaire (facultatif)	`network ipv6 secondaryDNSServer <ip address>` où <ip address> est l'adresse IP du serveur DNS secondaire.

9. Pour quitter le mode de configuration en enregistrant ou non les modifications, tapez une des deux commandes et appuyez sur Entrée.

Commande	Description
`apply`	Enregistrer toutes les modifications de configuration et quitter le mode de configuration.

Commande	Description
`cancel`	Abandonner toutes les modifications de configuration et quitter le mode de configuration.

L'invite # apparaît, indiquant que vous avez quitté le mode de configuration.

10. Pour vérifier si tous les paramètres sont corrects, tapez les commandes suivantes une par une. Les paramètres réseau en cours sont affichés.

Commande	Description
`show network`	Afficher les paramètres réseau.
`show network ip` all	Afficher tous les paramètres de configuration IP.
`show network wireless details`	Afficher tous les paramètres sans fil. (N'exécutez cette commande que si vous activez le mode sans fil.)

Conseil : vous pouvez également taper `show network wireless` *pour afficher une version abrégée des paramètres sans fil.*

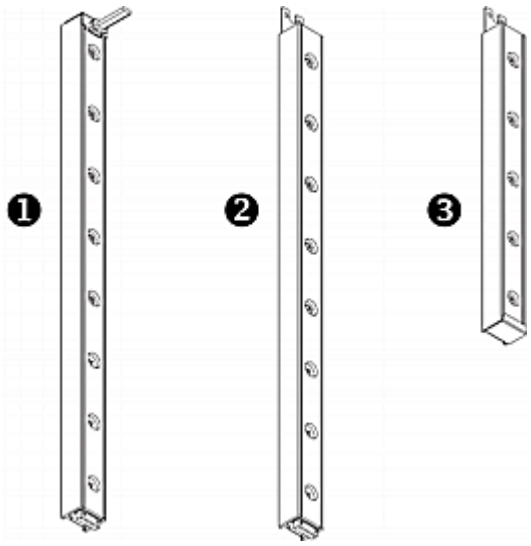
11. S'ils sont tous corrects, tapez `exit` pour vous déconnecter de EMX. En cas d'erreurs, répétez les étapes 7 à 10 pour modifier des paramètres réseau.

L'adresse IP configurée devient effective après plusieurs secondes.

Combinaison des capteurs de ressources

Chaque port d'étiquette sur les capteurs de ressources correspond à une unité de rack et peut servir à localiser les dispositifs informatiques d'un rack (ou cabinet) spécifique. Sur chaque rack, vous pouvez brancher jusqu'à 6 capteurs de ressources pour une longueur de 64U : un MAITRE et plusieurs ESCLAVES. La différence entre un capteur de ressources maître et un esclave réside dans le fait que le premier est doté d'un connecteur RJ-45 et le second, non.

Le diagramme suivant illustre plusieurs capteurs de ressources. Notez que Raritan fournit plus de types de capteurs de ressources qu'indiqué sur le diagramme.

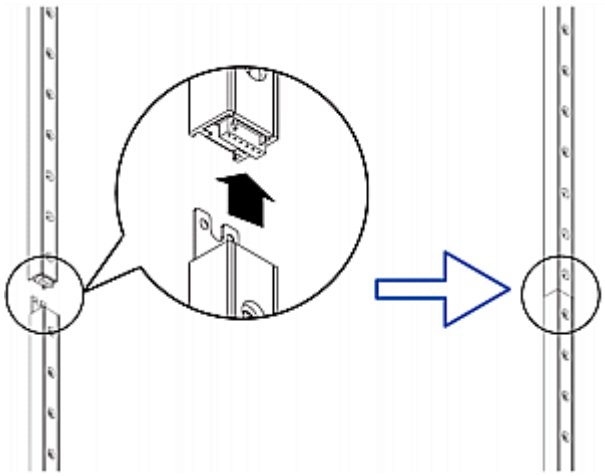


Numéro	Elément
❶	Capteur de ressources MAITRE 8U avec 8 ports d'étiquette
❷	Capteur de ressources ESCLAVE 8U avec 8 ports d'étiquette
❸	Capteur de ressources ESCLAVE 5U de fin avec 5 ports d'étiquette

Remarque : contrairement aux capteurs de ressources esclaves standard, qui comportent un connecteur DIN respectivement à chacune des extrémités, le capteur de fin n'en comporte qu'un à une seule extrémité. Un capteur de ressources de fin est installé à l'extrémité de l'assemblage de capteurs de ressources.

Pour assembler des capteurs de ressources :

1. Connectez un capteur de ressources MAITRE à un capteur de ressources ESCLAVE 8U.
   - Branchez le connecteur DIN mâle blanc du capteur esclave au connecteur DIN femelle blanc du capteur maître.
   - Assurez-vous que la patte de métal en forme de U à côté du connecteur DIN mâle est insérée dans la fente à l'arrière du capteur de ressources maître. Vissez la patte de métal en forme de U pour renforcer la connexion.



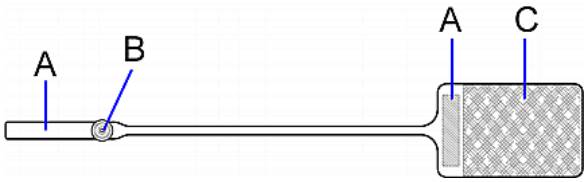
2. Connectez un autre capteur de ressources esclave 8U à celui qui est branché au capteur maître de la même manière qu'à l'étape 1.
3. Répétez l'étape précédente pour brancher d'autres capteurs esclaves. La longueur de l'assemblage de capteurs de ressources peut atteindre 64U.
   - Le dernier capteur de ressources peut mesurer 8U ou 5U suivant la hauteur réelle du rack.
   - Il est fortement recommandé d'utiliser le capteur de ressources de fin comme dernier capteur.
4. Attachez verticalement l'assemblage de capteurs de ressources au rack, à côté de l'équipement informatique, en alignant horizontalement chaque port d'étiquette sur une unité de rack. Les capteurs de ressources sont automatiquement attirés par le rack à cause des bandes magnétiques placées au dos.

Remarque : le capteur de ressources est doté d'un détecteur d'inclinaison et peut donc être monté sens dessus-dessous.

Connexion des capteurs de ressources à EMX

Le suivi des dispositifs informatiques requiert des capteurs de ressources et des étiquettes de gestion des ressources. Ces dernières, qui sont apposées aux dispositifs informatiques, fournissent un numéro d'identification pour chacun, alors que les capteurs transmettent les numéros d'identification et les données d'emplacement au dispositif EMX connecté.

Le diagramme suivant illustre une étiquette de gestion des ressources.



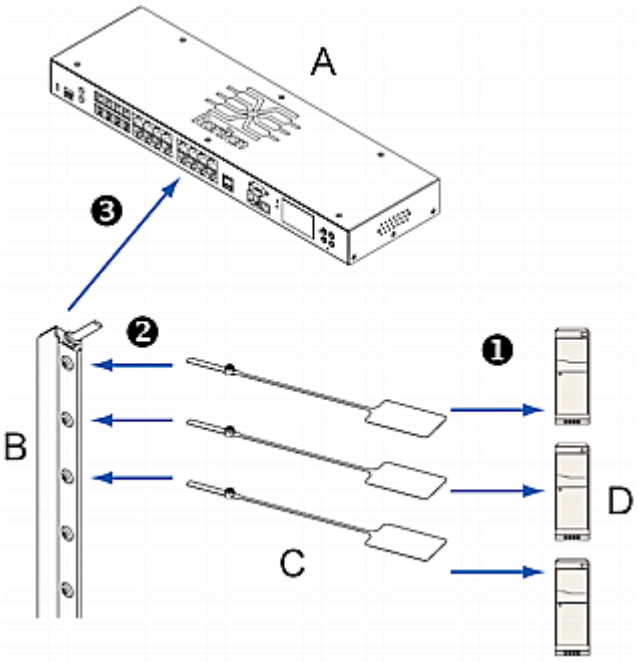
Lettre	Elément
A	Code à barres (numéro d'identification), disponible de chaque côté de l'étiquette de gestion des ressources
B	Connecteur d'étiquette
C	Zone adhésive avec bande

Remarque : le code à barres de chaque étiquette de gestion des ressources est unique et affiché dans l'interface Web du dispositif EMX facilitant ainsi l'identification.

Pour connecter des capteurs de ressources au dispositif EMX :

1. Collez le côté adhésif de chaque étiquette de gestion des ressources à chaque dispositif informatique.
2. Branchez le connecteur à l'autre extrémité de chaque étiquette de gestion des ressources dans le port d'étiquette correspondant sur le capteur de ressources.
3. Connectez l'assemblage de capteurs de ressources sur le rack au dispositif EMX en suivant cette procédure :
   a. Branchez une extrémité du câble Catégorie 5e/6 au connecteur RJ-45 sur le capteur de ressources MASTER.
   b. Connectez l'autre extrémité du câble au port FEATURE du dispositif EMX.

Le dispositif EMX alimente l'assemblage des capteurs de ressources via le câble Catégorie 5e/6. Tous les voyants de l'assemblage peuvent passer par différentes couleurs au cours de la mise sous tension si le firmware du capteur de ressources est mis à niveau par le dispositif EMX. Une fois la mise sous tension ou la mise à niveau du firmware terminée, la couleur des voyants reste fixe. Notez que la couleur de voyant des ports auxquels des étiquettes de gestion des ressources sont connectées sera différente de celle des ports sans étiquette.



Lettre	Elément
A	Dispositif EMX
B	Capteurs de ressources
C	Etiquettes de gestion des ressources
D	Dispositifs informatiques, tels que des serveurs

EMX2-111 prend en charge une longueur maximum d'1 mètre de câble pour la connexion de l'assemblage de capteurs de ressources, tandis que le dispositif EMX2-888 prend en charge un longueur maximum de 10 mètres de câble pour la connexion de chaque assemblage de capteurs de ressources.

4. Si votre dispositif dispose de plusieurs ports FEATURE, répétez les étapes précédentes pour connecter des capteurs de ressources supplémentaires aux ports FEATURE restants.

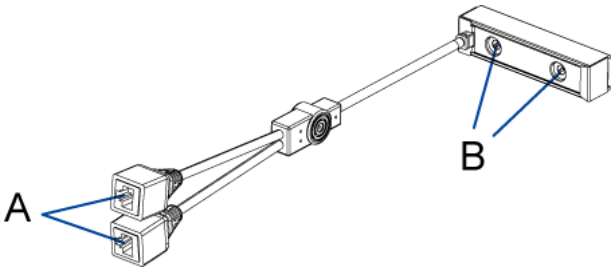
5. Configurez le capteur de ressources. Reportez-vous à ***Configuration du capteur de ressources*** (à la page 180).

Connexion des capteurs de ressources AMS-M2-Z (facultatif)

AMS-M2-Z est un type spécial de capteur de ressources fonctionnant de la même façon que les capteurs de ressources MAITRES, hormis les différences suivantes.

- Il est doté de deux connecteurs RJ-45.
- Plusieurs capteurs de ressources AMS-M2-Z peuvent être connectés en guirlande.
- Seuls deux ports d'étiquette sont disponibles sur chaque AMS-M2-Z ; deux étiquettes de gestion des ressources seulement peuvent donc être connectées.

Ce produit est particulièrement utile pour le suivi de dispositifs importants, tels que des boîtiers SAN dans une armoire.

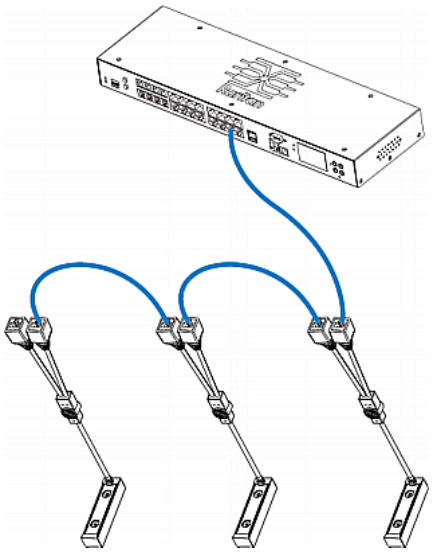


Elément	Description
A	Connecteurs RJ-45
B	Ports d'étiquette

Pour connecter les capteurs de ressources AMS-M2-Z au dispositif EMX :

1. Connectez l'AMS-M2-Z à EMX via un câble Catégorie 5e/6.
   a. Connectez une extrémité du câble au port RJ-45 libellé Input (Entrée) sur l'AMS-M2-Z.
   b. Connectez l'autre extrémité du câble au port FEATURE du dispositif EMX.
2. Apposez une étiquette de gestion des ressources au dispositif informatique et connectez-la à l'AMS-M2-Z en branchant son connecteur sur le port d'étiquette de l'AMS-M2-Z. Reportez-vous à ***Connexion des capteurs de ressources à EMX*** (à la page 24) pour en savoir plus.

3. Au besoin, connectez en guirlance plusieurs AMS-M2-Z pour effectuer le suivi de plus de deux dispositifs informatiques via ce dispositif EMX.
   a. Vérifiez que la longueur du câble Catégorie 5e/6 respecte les limites. Reportez-vous à ***Restrictions de la connexion en guirlande des capteurs AMS-M2-Z*** (à la page 185) pour obtenir ces limites de longueur.
   b. Branchez une extrémité du câble Catégorie 5e/6 sur le connecteur RJ-45 libellé Output (Sortie) de l'AMS-M2-Z à relier à EMX.
   c. Connectez l'autre extrémité du câble au port RJ-45 libellé Input (Entrée) sur un autre AMS-M2-Z.
   d. Répétez les étapes précédentes pour connecter en guirlande des AMS-M2-Z supplémentaires. Reportez-vous à ***Restrictions de la connexion en guirlande des capteurs AMS-M2-Z*** (à la page 185) pour connaître le nombre maximum de capteurs de ressources AMS-M2-Z pris en charge.
   e. Il est fortement recommandé d'utiliser des attaches de câble pour supporter le poids de tous les câbles de connexion.



4. Répétez l'étape 2 pour connecter des dispositifs informatiques à l'autre AMS-M2-Z de la guirlande au moyen d'étiquettes de gestion des ressources.

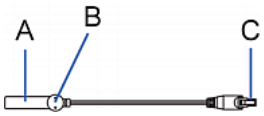
Connexion des bandeaux d'extension de lame

Vous pouvez effectuer le suivi des serveurs lames, figurant sur un même châssis, à l'aide d'un bandeau d'extension de lame.

Le bandeau d'extension de lame Raritan fonctionne de manière similaire à un capteur de ressources Raritan, mais requiert un câble de connecteur d'étiquette pour le branchement sur un port d'étiquette du capteur de ressources standard ou de l'AMS-M2-Z. Le bandeau d'extension de lame contient 4 à 16 ports d'étiquette, selon le modèle acheté.

Le diagramme illustre un câble de connecteur d'étiquette et le bandeau d'extension de lame comportant 16 ports d'étiquette.

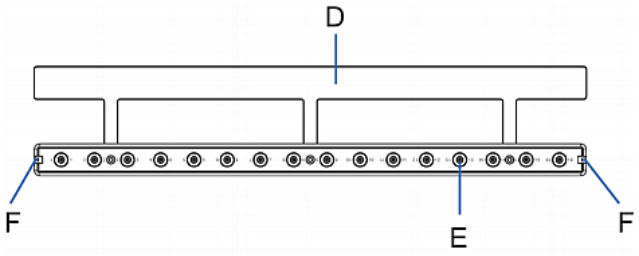
Câble de connecteur d'étiquette



Elément	Description
A	Code à barres (numéro d'identification) pour le câble de connecteur d'étiquette
B	Connecteur d'étiquette
C	Connecteur de câble pour la connexion du bandeau d'extension de lame

Remarque : un câble de connecteur d'étiquette est doté d'un code à barres unique, affiché dans l'interface Web du dispositif EMX pour identifier chaque bandeau d'extension de lame là où il est connecté.

Bandeau d'extension de lame



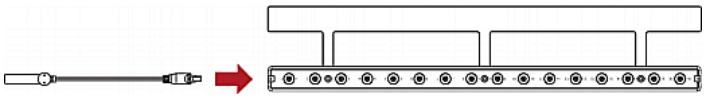
Elément	Description
D	Section en mylar avec la bande adhésive
E	Ports d'étiquette

Elément	Description
F	Prise(s) de câble pour la connexion du câble de connecteur d'étiquette

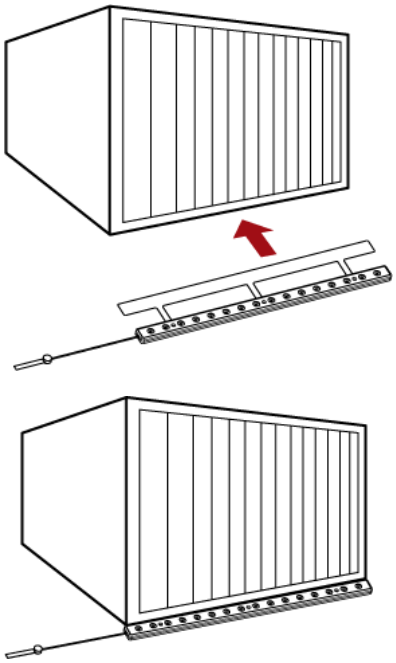
Remarque : chaque port d'étiquette du bandeau d'extension de lame est libellé d'un numéro, affiché comme numéro de fente dans l'interface Web du dispositif EMX.

Pour installer un bandeau d'extension de lame :

1. Branchez le câble du connecteur d'étiquette sur le bandeau d'extension de lame.
   - Branchez le connecteur du câble dans la prise à l'une des extrémités du bandeau d'extension de lame.



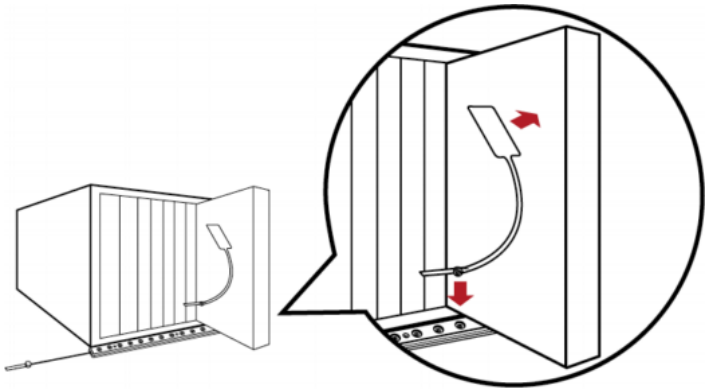
2. Déplacez le bandeau d'extension de lame vers le bas du châssis de lame jusqu'à ce que sa section en mylar se trouve entièrement sous le châssis. Vérifiez ensuite que le bandeau ne se détache pas facilement. Au besoin, vous pouvez utiliser la bande adhésive au dos de la section en mylar pour maintenir le bandeau en place.



3. Connectez une extrémité d'une étiquette de gestion des ressources à un serveur lame et l'autre, au bandeau d'extension de lame.

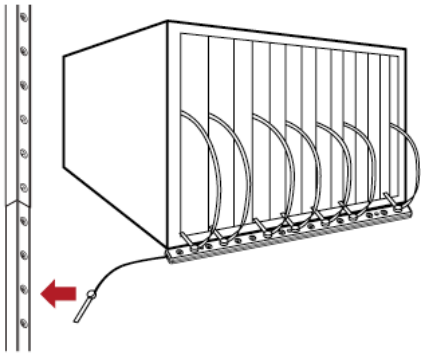
a. Apposez la partie adhésive de l'étiquette de gestion des ressources à un côté d'un serveur lame.

b. Branchez le connecteur de l'étiquette de gestion des ressources sur le port d'étiquette du bandeau d'extension de lame.



4. Répétez l'étape précédente jusqu'à ce que tous les serveurs lames du châssis soient connectés au bandeau d'extension de lame au moyen d'étiquettes de gestion des ressources.

5. Branchez le connecteur d'étiquette du bandeau d'extension de lame sur le port d'étiquette le plus proche de l'assemblage de capteurs de ressources ou du capteur AMS-M2-Z du rack.



Remarque : si vous devez déconnecter temporairement le connecteur d'étiquette du bandeau d'extension de lame, patientez au moins une seconde avant de le reconnecter, ou le dispositif EMX risque de ne pas le détecter.

Connexion de capteurs d'environnement (facultatif)

Pour activer la détection des facteurs d'environnement autour du dispositif EMX, connectez-lui un ou plusieurs capteurs d'environnement Raritan.

La distance maximum pour le câblage de tous les capteurs branchés sur le port de capteur du produit ne doit pas dépasser 30 mètres. En cas de doute, contactez le support technique de Raritan.

Lorsqu'un concentrateur de capteurs Raritan est utilisé, vous pouvez connecter jusqu'à 16 capteurs d'environnement par port SENSOR. C'est-à-dire,

- Sur EMX2-111, qui n'a qu'un port SENSOR, 16 capteurs d'environnement au plus peuvent être connectés.
- Sur EMX2-888, qui a huit ports SENSOR, 128 capteurs d'environnement au plus peuvent être connectés. Comme le dispositif EMX2-888 est mis en œuvre avec deux canaux de terminaison de fermeture de contact embarqué, il prend en charge jusqu'à 130 capteurs d'environnement.

Chaque port SENSOR peut uniquement prendre en charge un maximum de deux capteurs de fermeture de contact Raritan, qui utilise l'intervalle de mise à jour le plus court de tous les capteurs Raritan. Reportez-vous à ***Informations sur l'intervalle de mise à jour*** (à la page 172).

Notez qu'un capteur d'environnement Raritan comporte habituellement plusieurs capteurs. Par exemple, DPX-T2H2 et DPX-T3H1 comportent quatre capteurs.

Avertissement : pour un bon fonctionnement, patientez 15 à 30 secondes entre chaque connexion ou déconnexion de capteurs d'environnement.

Pour connecter directement un ou plusieurs capteurs d'environnement :

- Branchez le connecteur du capteur d'environnement sur le port SENSOR du dispositif EMX.

Remarque : selon le modèle acheté, le nombre total de ports SENSOR varie.

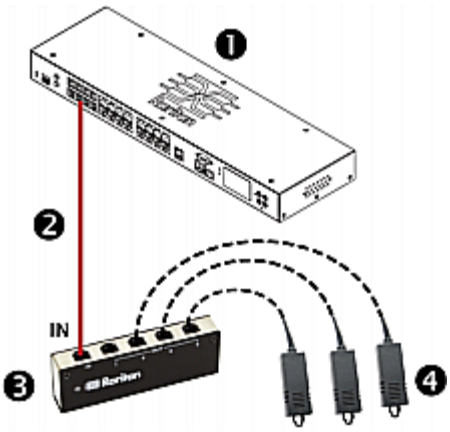
Pour connecter des capteurs d'environnement via un concentrateur de capteurs PX facultatif :

1. Connectez un concentrateur de capteurs Raritan au dispositif EMX.
   a. Branchez une extrémité du câble téléphonique (4 fils, 6 broches, RJ-12) fourni par Raritan dans le port IN (Port 1) du concentrateur.

b. Branchez l'autre extrémité sur un des ports SENSOR du dispositif EMX.

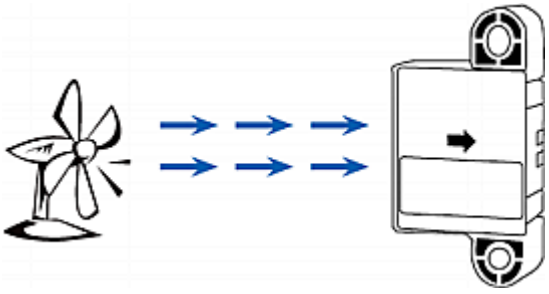
2. Connectez les capteurs d'environnement Raritan à un des quatre ports OUT du concentrateur.

   Les concentrateurs de capteurs Raritan NE PEUVENT PAS être mis en cascade. Il ne peut donc y avoir qu'un seul concentrateur connecté à chaque port SENSOR du dispositif EMX. Le diagramme illustre une configuration avec un concentrateur de capteurs connecté.



❶	Dispositif EMX
❷	Câble téléphonique fourni par Raritan
❸	Concentrateur de capteurs PX Raritan
❹	Capteurs d'environnement Raritan

3. Si des capteurs de flux d'air Raritan sont connectés, assurez-vous qu'ils font face à la source de vent (un ventilateur, par exemple), dans l'orientation appropriée indiquée par la flèche figurant dessus.



4. Configurez le capteur d'environnement. Reportez-vous à ***Configuration des capteurs d'environnement*** (à la page 168).

A propos des capteurs de fermeture de contact

Le capteur de fermeture de contact Raritan (DPX-CC2-TR) peut détecter le statut ouvert-et-fermé des détecteurs/commutateurs connectés.

Pour fonctionner correctement, cette fonctionnalité requiert l'intégration d'un détecteur/commutateur discret (activé/désactivé) au moins. Les types de détecteurs/commutateurs discrets pouvant être branchés sur DPX-CC2-TR incluent ceux destinés à :

- la détection de porte ouverte/fermée ;
- la détection du verrouillage de porte ;
- la détection d'eau à terre ;
- la détection de fumée ;
- la détection de vibrations.

Raritan NE FOURNIT PAS de détecteurs/commutateurs discrets. Il s'agit de sondes tierces que vous devez donc tester avec le dispositif DPX-CC2-TR de Raritan pour vérifier leur fonctionnement correct.

Important : l'intégration et l'essai de détecteurs/commutateurs tiers est à la seule responsabilité du client. Raritan n'assume aucune responsabilité en cas de terminaison incorrecte ou de panne (indirecte ou consécutive) des détecteurs/commutateurs tiers fournis ou installés par les clients. Le non-respect des instructions d'installation et de configuration peut entraîner de fausses alertes ou aucune alerte. Raritan ne déclare ni ne suggère en aucun cas que tous les détecteurs/commutateurs tiers fonctionneront avec DPX-CC2-TR.

Connexion des détecteurs/commutateurs tiers

Il existe deux manières de connecter des détecteurs/commutateurs tiers au dispositif EMX :

- Connectez les détecteurs/commutateurs à DPX-CC2-TR, qui sera branché sur un port SENSOR du dispositif EMX.
- Connectez les détecteurs/commutateurs à la terminaison du capteur de fermeture de contact sur le dispositif EMX s'il s'agit du modèle EMX2-888.

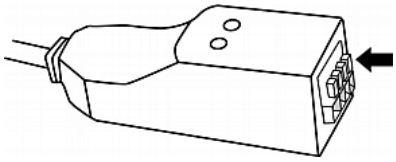
Connexion des détecteurs/commutateurs tiers à DPX-CC2-TR

Une unité DPX-CC2-TR dispose de deux canaux pour la connexion de deux détecteurs/commutateurs tiers. Le corps de DPX-CC2-TR comporte quatre points de terminaison à ressort : les deux à droite sont associés à un canal (comme indiqué par le numéro du voyant) et les deux à gauche, à l'autre canal. Vous devez brancher les détecteurs/commutateurs tiers dans ces points de terminaison.

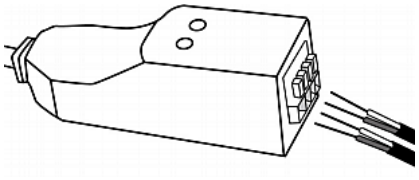
Pour connecter des détecteurs/commutateurs tiers :

1. Dénudez l'isolant sur environ 12 mm de l'extrémité de chaque fil de deux détecteurs/commutateurs tiers.
2. Appuyez sur les petits boutons rectangulaires au-dessus des points de terminaison du corps de DPX-CC2-TR, et maintenez-les enfoncés.

Remarque : chaque bouton contrôle le ressort du point de terminaison correspondant.



3. Insérez entièrement chaque fil des deux détecteurs/commutateurs tiers dans chaque point de terminaison.
   - Branchez les deux fils d'un détecteur/commutateur dans les deux points de terminaison à gauche.
   - Branchez les deux fils d'un autre détecteur/commutateur dans les deux points de terminaison à droite.



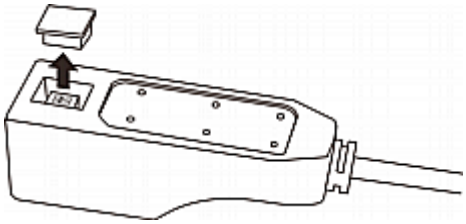
4. Relâchez les petits boutons rectangulaires après avoir inséré les fils correctement.
5. Vérifiez que ces fils sont solidement fixés.

Configuration d'un capteur de fermeture de contact

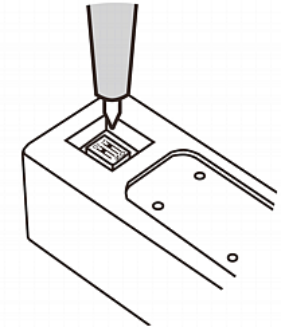
Avant d'utiliser un capteur DPX-CC2-TR afin de détecter le statut de fermeture de contact, la présence d'eau, de fumée ou de vibration, vous devez déterminer l'état normal en réglant un commutateur DIP contrôlant l'état du voyant sur le bâti du capteur DPX-CC2-TR. Un commutateur DIP est associé à un canal.

Pour régler le commutateur DIP :

1. Placez les détecteurs/commutateurs connectés au capteur DPX-CC2-TR à l'endroit où vous souhaitez détecter une situation environnementale particulière.
2. Découvrez le commutateur DIP sur le bâti du capteur DPX-CC2-TR.



3. Pour définir l'état Normal pour le canal 1, repérez le commutateur DIP libellé 1.
4. Utilisez une pointe, telle que celle d'un stylo, pour placer le commutateur à glissière sur l'extrémité libellée NO (Normally Open) ou NC (Normally Closed).
   - Normally Open (Normalement ouvert) : le statut ouvert du détecteur/commutateur connecté est considéré comme normal.
   - Normally Closed (Normalement fermé) : le statut fermé du détecteur/commutateur connecté est considéré comme normal. Il s'agit de la valeur par défaut.



5. Pour définir l'état Normal pour le canal 2, répétez l'étape 4 pour régler l'autre commutateur DIP.
6. Replacez le couvercle sur le commutateur DIP.

Remarque : le commutateur DIP doit être correctement configuré, sinon le voyant du capteur risque d'être allumé de manière erronée à l'état Normal.

Connexion des détecteurs/commutateurs tiers à EMX

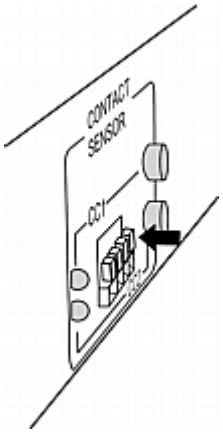
Un modèle EMX spécifique (EMX2-888) offre deux canaux de points de terminaison de capteurs de fermeture de contact, permettant une connexion directe des détecteurs/commutateurs de fermeture de contact tiers.

La compatibilité de tous les détecteurs/commutateurs tiers avec le dispositif EMX n'est pas garantie. Vous devez tester cette compatibilité après les avoir correctement installés.

Pour connecter des détecteurs/commutateurs tiers :

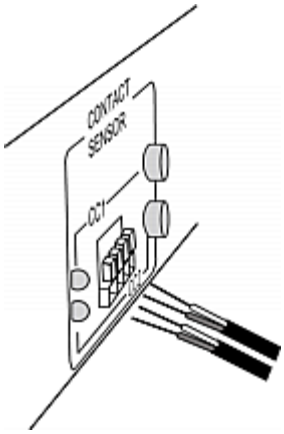
1. Dénudez l'isolant sur environ 12 mm de l'extrémité de chaque fil de deux détecteurs/commutateurs tiers.
2. Appuyez sur les petits boutons rectangulaires situés au-dessus des points de terminaison et maintenez-les enfoncés.

   Remarque : chaque bouton contrôle le ressort du point de terminaison correspondant.



3. Insérez entièrement chaque fil des deux détecteurs/commutateurs tiers dans chaque point de terminaison.
   - Branchez les deux fils d'un détecteur/commutateur dans les deux points de terminaison à gauche.

- Branchez les deux fils d'un autre détecteur/commutateur dans les deux points de terminaison à droite.



4. Relâchez les petits boutons rectangulaires après avoir inséré les fils correctement.
5. Vérifiez que ces fils sont solidement fixés.
6. Par défaut, le statut ouvert du détecteur/commutateur est considéré comme normal. Pour définir le paramètre normal sur fermé, appuyez sur le bouton correspondant adjacent aux points de terminaison.

Voyants de capteur de fermeture de contact

Deux voyants sont situés près des points de terminaison de fermeture de contact du dispositif EMX ou du module de capteur de fermeture de contact Raritan (DPX-CC2-TR). Chaque voyant affiche l'état du canal correspondant.

Le voyant est allumé lorsque le détecteur/commutateur associé est à l'état « anormal », soit l'opposé de l'état Normal.

La signification d'un voyant allumé varie selon les paramètres d'état Normal.

- **Lorsque l'état Normal est défini sur Closed (Fermé) :**

Voyant	Etat du capteur
Non allumé	Fermé
Allumé	Ouvert

- **Lorsque l'état Normal est défini sur Open (Ouvert) :**

Voyant	Etat du capteur
Non allumé	Ouvert

Voyant	Etat du capteur
Allumé	Fermé

Connexion des capteurs de pression d'air différentielle

Vous pouvez connecter un capteur de pression d'air différentielle Raritan au dispositif EMX si vous avez besoin des données correspondantes.

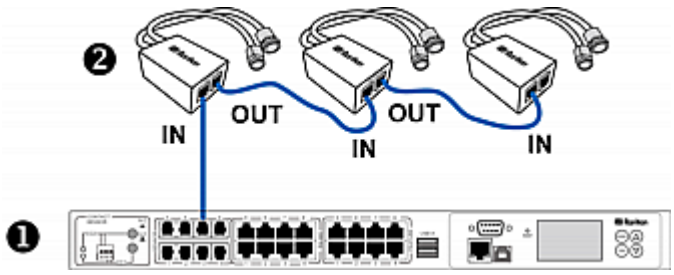
Grâce à ce capteur, la température autour de lui peut également être détectée au moyen d'un capteur de température intégré.

Plusieurs capteurs de pression d'air différentielle peuvent être mis en cascade.

Pour connecter des capteurs de pression d'air différentielle :

1. Branchez une extrémité du câble téléphonique fourni par Raritan dans le port SENSOR du dispositif EMX.
2. Branchez l'autre extrémité de ce câble téléphonique au port IN du capteur de pression d'air différentielle.
3. Pour connecter des capteurs de pression d'air différentielle Raritan supplémentaires, effectuez les opérations suivantes :
   a. Branchez une extrémité d'un câble téléphonique fourni par Raritan au port OUT du capteur de pression d'air différentielle précédent.
   b. Branchez l'autre extrémité de ce câble téléphonique au port IN du nouveau capteur de pression d'air différentielle.
   c. Répétez les étapes a et b pour mettre en cascade des capteurs supplémentaires. Notez que chaque port SENSOR prend en charge 16 capteurs d'environnement maximum.

❶	Dispositif EMX
❷	Capteur de pression d'air différentielle Raritan



Connexion d'une webcam Logitech (facultatif)

EMX prend en charge les webcams Logitech® QuickCam® Pro 9000 qui lui sont connectées et vous permet ainsi de visualiser une vidéo ou des instantanés de la zone autour de la webcam. Le dispositif EMX 888 prend en charge jusqu'à deux webcams, et EMX 111, une. Après avoir connecté une webcam, vous pouvez surveiller les conditions environnementales près du dispositif EMX via l'interface Web, de n'importe où.

Pour plus d'informations sur la webcam QuickCam, consultez la documentation d'utilisation qui l'accompagne.

Pour connecter une webcam :

1. Connectez la webcam au port USB-A du dispositif EMX. EMX détecte automatiquement la webcam.
2. Positionnez correctement la webcam.

Des images statiques ou des vidéos prises par la webcam s'affichent immédiatement dans l'interface Web de EMX. Reportez-vous à ***Webcams*** (à la page 191) pour en savoir plus sur la fonction et à ***Configuration des webcams*** (à la page 191) pour en savoir plus sur la configuration de la webcam après sa connexion.

Remarque : Votre rôle doit disposer de l'autorisation Change Webcam Configuration (Modifier la configuration de la webcam) pour configurer les webcams, et de l'autorisation View Webcam Images and Configuration (Afficher les images et la configuration de la webcam) pour visualiser des images dans EMX.

Connexion d'un échangeur thermique Schroff LHX (facultatif)

Pour surveiller et gérer à distance les échangeurs thermiques Schroff® LHX-20 ou LHX-40 par le biais du dispositif EMX, vous devez établir une connexion entre eux.

Pour plus d'informations sur l'échangeur thermique LHX, consultez la documentation d'utilisation qui accompagne ce produit.

Pour connecter un échangeur thermique LHX :

1. Branchez une extrémité d'un câble UTP Catégorie 5e/6 standard sur le port RS-485 de l'échangeur thermique Schroff LHX.
2. Branchez l'autre extrémité du câble sur un des ports RS-485 disponibles du dispositif EMX.

Pour connecter un échangeur thermique LHX au port FEATURE série à l'aide d'un câble série (fourni par Schroff) :

1. Branchez l'extrémité DB9 du câble dans le port RS232 de l'échangeur thermique Schroff LHX.
2. Branchez l'autre extrémité du câble sur un des ports FEATURE série disponibles du dispositif EMX.

Reportez-vous à ***Echangeurs thermiques Schroff LHX*** (à la page 198) pour apprendre comment surveiller et gérer l'échangeur thermique à l'aide de EMX.

Chapitre 3 Mise en route

Dans ce chapitre

Navigateurs Web pris en charge

Les navigateurs Web ci-après peuvent être utilisés pour accéder à l'interface Web de EMX :

- Internet Explorer® 7 et 8
- Firefox® 3.x
- Safari® 5.1 (MacOS Lion)
- Konqueror
- Google® Chrome® 16.0

Les navigateurs pour téléphone intelligent suivants sont pris en charge :

- Safari sous iOS 5.01
- Dolphin® 3.2.1

Ports de connexion

Selon le modèle acheté, le nombre total de ports disponibles varie.

Le tableau ci-dessous explique la fonction de chaque port.

Port	Utilisation
USB-B	Etablir une connexion USB entre un ordinateur et le dispositif EMX : Ce port sert pour la reprise totale après sinistre du dispositif EMX. Contactez le support technique de Raritan pour obtenir des instructions.
USB-A	Connecter un dispositif USB : Il s'agit d'un port hôte, qui est alimenté, selon les caractéristiques USB 2.0.

Port	Utilisation
FEATURE	Connexion aux capteurs de ressources via un câble Catégorie 5e/6. *Remarque : le dispositif EMX alimente les capteurs de ressources connectées une fois la connexion établie.*
CONSOLE/ MODEM	Etablir une connexion série entre un ordinateur et le dispositif EMX : Il s'agit d'un port DTE RS-232 standard. Vous pouvez utiliser un câble null-modem avec deux connecteurs DB9 aux deux extrémités pour connecter le dispositif EMX à l'ordinateur.
SENSOR	Connexion aux capteurs d'environnement Raritan : Un concentrateur de capteurs Raritan peut être nécessaire si vous souhaitez connecter plusieurs capteurs d'environnement.
ETHERNET	Connexion du dispositif EMX au réseau de votre société : Raccordez un câble UTP Cat5e/6 standard à ce port et connectez l'autre fiche à votre réseau. Cette connexion est nécessaire à l'administration du et à l'accès à distance au dispositif EMX via l'interface Web. Il existe deux petits voyants en regard du port : ▪ Le vert indique un lien physique et de l'activité. ▪ Le jaune indique la communication à des vitesses de 10/100 BaseT. Pour une configuration en cascade USB, la connexion câblée est obligatoire pour le dispositif EMX *maître*. Reportez-vous à Mise en cascade des PDU via USB pour en savoir plus. *Remarque : la connexion à ce port n'est pas nécessaire si le dispositif EMX est connecté à un réseau sans fil.*
RS-485	Connexion à un dispositif électrique avec l'interface RS-485. Actuellement, EMX prend uniquement en charge les échangeurs thermiques Schroff® LHX-20 et LHX-40.

Panneau d'affichage LCD

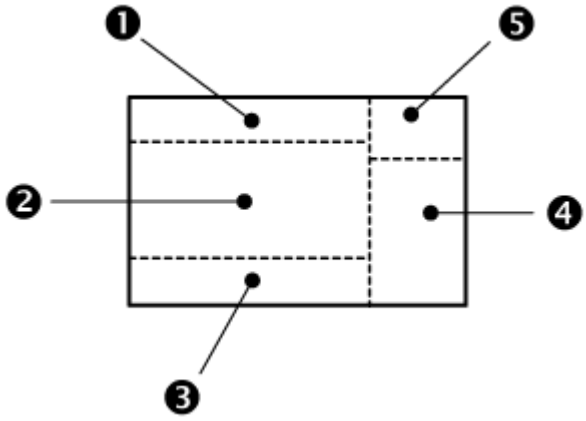
Le panneau d'affichage LCD présente le relevé ou le statut du capteur, les états de gestion des ressources et l'adresse MAC du dispositif.

Il comprend :

- Affichage LCD
- Boutons de contrôle

Affichage LCD

Différents types d'informations sont présents dans les sections de l'affichage LCD. Le diagramme illustre ces sections.



Section	Informations affichées
❶	Suivant la sélection, les informations affichées incluent : • Le capteur d'environnement sélectionné, notamment son numéro d'identification. EMX présente le capteur d'environnement sélectionné de deux façons : ▪ Un capteur dont le numéro d'identification est inférieur à 100 est affiché comme SENSOR X ou SENSOR XX, où X et XX sont des chiffres. ▪ Un capteur dont le numéro d'identification est égal ou supérieur à 100 est affiché comme 1 SENSOR XX, où XX représente les deux derniers chiffres du numéro d'identification. • Le numéro du port FEATURE auquel le capteur de ressources sélectionné est connecté.
❷	Suivant la sélection, les informations affichées incluent : • Le relevé du capteur comprenant des chiffres ou l'état du capteur comprenant des lettres. • Le numéro du port SENSOR auquel le capteur sélectionné est physiquement connecté. • Les coordonnées X, Y ou Z du capteur d'environnement sélectionné. • Le numéro de série du capteur d'environnement sélectionné. • Le numéro de l'unité de rack choisie du capteur de ressources sélectionné. *Remarque : Pour le capteur de ressources Raritan, une unité de rack fait référence à un port d'étiquette.* • L'adresse MAC du dispositif EMX.
❸	Le texte ALARM peut s'afficher pour indiquer l'un des scénarios suivants : • Pour un capteur d'environnement numérique, tel qu'un capteur de température, cela signifie que le relevé du capteur atteint ou dépasse les seuils supérieur ou inférieur s'ils sont activés. • Pour un capteur d'environnement discret (activé/désactivé), tel qu'un capteur de fermeture de contact, cela signifie que le capteur est passé à l'état anormal. • Pour un capteur de ressources, AUCUNE étiquette de gestion des ressources n'est détectée sur l'unité de rack sélectionnée.

Section	Informations affichées
❹	L'unité de mesure pour le capteur d'environnement apparaît. Cette unité dépend du type du capteur : • % est affiché pour un capteur d'humidité. • °C est affiché pour un capteur de température.
❺	Lorsque le terme ASSET apparaît, les informations affichées sont associées aux capteurs de ressources et aux étiquettes de gestion des ressources.

Boutons de contrôle

Le dispositif comporte quatre boutons de contrôle :

- les boutons Up (Haut) et Down (Bas) pour sélectionner un identifiant ou un numéro de port spécifique ;
- le bouton MODE pour passer d'un type d'informations cible à l'autre, comme les informations de capteur d'environnement, de gestion des ressources et l'adresse MAC ;
- le bouton FUNC pour permuter entre les différents types de données pour un capteur d'environnement sélectionné.

Par défaut, le panneau d'affichage présente le premier capteur d'environnement répertorié sur la page External Sensors (Capteurs externes) de l'interface Web jusqu'à ce que vous en sélectionniez un autre ou une cible différente.

Informations sur les capteurs d'environnement

Les informations du capteur d'environnement sont représentées par SENSOR dans l'affichage LCD. Faites fonctionner l'affichage LCD pour consulter les données du capteur d'environnement sélectionné, comme son relevé ou son état, le numéro de son port physique, les coordonnées X, Y, Z et son numéro de série.

Pour afficher les données du capteur d'environnement :

1. Appuyez sur le bouton Up ou Down jusqu'à ce que le numéro d'identification du capteur d'environnement souhaité apparaisse au sommet de l'affichage LCD. Reportez-vous à ***Affichage LCD*** (à la page 43). Par exemple, SENSOR 1 désigne le capteur nº 1 répertorié sur la page External Sensors (Capteurs externes) de l'interface Web.
   - Appuyez sur le bouton △ (UP) pour faire monter d'une sélection.
   - Appuyez sur le bouton ▽ (DOWN) pour faire descendre d'une sélection.

- 1 SENSOR 24 se refère au capteur nº 124.

Remarque : appuyez sur les boutons Up (Haut) ou Down (Bas) et maintenez-les enfoncés au moins deux secondes pour passer plusieurs éléments à la fois.

2. L'affichage LCD présente le relevé ou l'état du capteur sélectionné en son milieu.

   Pour un relevé de capteur numérique, l'unité de mesure appropriée apparaît à droite du relevé.

   - % est affiché pour un capteur d'humidité.
   - °C est affiché pour un capteur de température.

   Pour un capteur discret, un des états de capteur suivants est affiché.

   - on (actif) : le capteur est dans un état anormal.
   - oFF (inactif) : le capteur est dans un état normal.

   Remarque : les capteurs numériques utilisent des valeurs numériques pour indiquer des conditions d'environnement ou internes, alors que les capteurs discrets (activé/désactivé) utilisent des caractères alphabétiques pour indiquer l'état.

3. Si le dispositif EMX dispose de plusieurs ports SENSOR, appuyez sur le bouton FUNC pour afficher le numéro de port physique du capteur d'environnement. Le numéro de port indique P:X, où X est le numéro du port. Pour le capteur de fermeture de contact embarqué, il indique CC1 ou CC2.
4. Appuyez sur le bouton FUNC pour afficher respectivement les coordonnées X, Y et Z du capteur.

   - La coordonnée X est affichée sous la forme x:XX, où XX représente les deux premiers chiffres entrés pour la coordonnée X dans l'interface Web.
   - La coordonnée Y est affichée sous la forme y:XX, où XX représente les deux premiers chiffres entrés pour la coordonnée Y dans l'interface Web.
   - La coordonnée Z est affichée sous la forme z:XX, où XX représente les deux premiers chiffres entrés pour la coordonnée Z dans l'interface Web.

   Si l'un des deux premiers caractères ou les deux d'une coordonnée spécifique sont alphabétiques, un ou deux soulignés sont affichés à la place de ces caractères.

5. Appuyez sur le bouton FUNC à nouveau pour afficher le numéro de série du capteur, présenté sous la forme s:XX, où XX représente les deux caractères du numéro de série. Le LCD affichera les caractères du numéro de série deux par deux, des deux premiers aux deux derniers.

Par exemple, si le numéro de série est AE17A00022, l'affichage LCD présente les données suivantes les unes après les autres :

s:AE --> s:17 --> s:A0 --> s:00 --> s:22

Si aucun bouton n'est activé après des dizaines de secondes, l'affichage LCD retourne au relevé ou à l'état du capteur.

Informations de gestion des ressources

L'affichage LCD peut présenter l'état du capteur de ressources sur chaque port FEATURE ainsi que l'état d'étiquette de gestion des ressources de chaque unité de rack. Pour le capteur de ressources Raritan, une unité de rack fait référence à un port d'étiquette.

Pour afficher les informations de gestion des ressources :

1. Appuyez sur le bouton MODE jusqu'à ce que le mot ASSET apparaisse dans le coin supérieur droit de l'affichage LCD.
2. Appuyez sur le bouton Up ou Down jusqu'à ce que le numéro de port FEATURE souhaité apparaisse au sommet de l'affichage LCD. Reportez-vous à ***Affichage LCD*** (à la page 43).
   - Appuyez sur le bouton △ (UP) pour faire monter d'une sélection.
   - Appuyez sur le bouton ▽ (DOWN) pour faire descendre d'une sélection.

   Si aucun capteur de ressources n'est détecté ou connecté physiquement au port FEATURE sélectionné, le terme nA apparaît.

   Remarque : appuyez sur les boutons Up (Haut) ou Down (Bas) et maintenez-les enfoncés au moins deux secondes pour passer plusieurs éléments à la fois.
3. Appuyez sur le bouton FUNC. Lorsque le symbole de flèche double ◇ clignotant apparaît sur le côté gauche de l'affichage LCD, vous pouvez appuyer sur le bouton Up ou Down pour sélectionner l'unité de rack souhaitée sur le capteur de ressources actuellement activé. Le numéro de l'unité de rack apparaît au milieu de l'affichage LCD.
   - Si le terme ALARM apparaît sous le numéro d'unité de rack, il indique qu'aucune étiquette de gestion des ressources n'est détectée ou connectée physiquement à cette unité de rack.
   - Si le terme ALARM N'APPARAIT PAS, une étiquette de gestion des ressources est détectée sur l'unité de rack.

Adresse MAC

L'adresse MAC du dispositif EMX est disponible via l'affichage LCD. Par le biais des outils de réseau courants, vous pouvez rechercher l'adresse IP du dispositif à l'aide de l'adresse MAC. Adressez-vous à l'administrateur du réseau local pour obtenir de l'aide.

Pour afficher l'adresse MAC :

1. Appuyez sur le bouton MODE jusqu'à ce que le caractère M apparaisse sur le côté gauche de l'affichage LCD.
2. L'adresse MAC est affichée sous la forme M:XX, où XX représente deux caractères de cette adresse. Le LCD affichera les caractères de l'adresse MAC deux par deux, des deux premiers aux deux derniers.

   Par exemple, si l'adresse MAC est 00:0d:5d:03:5E:1A, l'affichage LCD présente les données suivantes les unes après les autres :

   M:00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

Remarque : appuyez sur les boutons Up (Haut) ou Down (Bas) et maintenez-les enfoncés au moins deux secondes pour passer plusieurs éléments à la fois.

IP Address (Adresse IP)

L'adresse IP est également disponible dans l'affichage LCD du dispositif EMX. Utilisez le bouton Mode pour permuter entre les modes capteur, ressource et dispositif. En mode dispositif, un petit d apparaît dans le coin supérieur gauche. L'adresse commence par l'adresse IPv4, indiquée par i4 dans le coin supérieur droit de l'affichage. Utilisez le bouton Function pour passer à l'adresse MAC. Dans ce cas, un M est affiché dans le coin supérieur droit.

Bouton Reset (Réinitialiser)

Le bouton de réinitialisation se trouve à l'intérieur d'un petit orifice libellé RESET.

Le dispositif EMX peut être réinitialisé à ses valeurs par défaut usine à l'aide de ce bouton lorsqu'une connexion série est disponible. Reportez-vous à ***Réinitialisation aux valeurs par défaut usine*** (à la page 100).

Sans connexion série, appuyez sur ce bouton de réinitialisation pour redémarrer le logiciel du dispositif EMX.

Terminaison de capteur de fermeture de contact

Deux canaux de connexion des capteurs de fermeture de contact tiers sont fournis sur le modèle EMX2-888.

Pour plus d'informations, reportez-vous à :

- ***Connexion des détecteurs/commutateurs tiers à EMX*** (à la page 36)
- ***Voyants de capteur de fermeture de contact*** (à la page 37)

Interrupteur d'alimentation

L'interrupteur d'alimentation met sous ou hors tension le dispositif EMX.

Pour effectuer l'alimentation cyclique de EMX, appuyez sur l'interrupteur d'alimentation pour mettre le dispositif hors tension, **patientez au moins 10 secondes**, puis appuyez à nouveau sur l'interrupteur pour le mettre sous tension. Notez qu'une période de mise hors tension d'au moins 10 secondes est nécessaire. Sinon, le dispositif ne démarrera pas correctement.

Connexion

Pour vous connecter à l'interface Web, vous devez entrer un nom d'utilisateur et un mot de passe. Pour la première connexion à EMX, utilisez le nom d'utilisateur (admin) et le mot de passe (raritan) par défaut. Vous êtes ensuite invité à modifier le mot de passe pour des raisons de sécurité.

Exception : si vous avez déjà modifié le mot de passe du compte admin au cours de la configuration initiale du réseau, utilisez le nouveau de passe pour vous connecter à l'interface Web, et EMX NE vous invitera PAS à modifier le mot de passe.

Une fois connecté, vous pouvez créer des profils pour vos autres utilisateurs. Ces profils définissent les noms et les mots de passe de connexion des utilisateurs. Reportez-vous à ***Création d'un profil utilisateur*** (à la page 62).

L'interface Web autorise la connexion simultanée de 16 utilisateurs.

Vous devez activer Java Script dans le navigateur Web pour un fonctionnement correct.

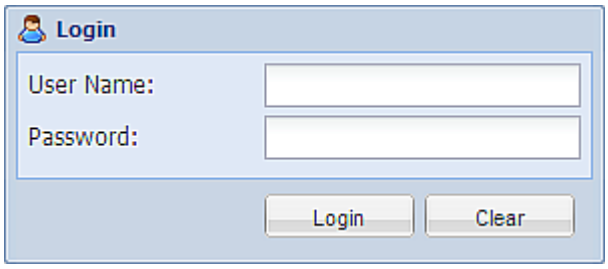
Pour vous connecter à l'interface Web :

1. Ouvrez un navigateur, tel que Microsoft Internet Explorer ou Mozilla Firefox, et tapez cette URL :

   http(s)://<adresse ip>

   où *<adresse ip>* représente l'adresse IP du dispositif EMX.

2. Si un message d'alerte de sécurité apparaît, cliquez sur OK ou sur Yes (Oui) pour accepter. La page de connexion s'ouvre alors.



3. Tapez votre nom d'utilisateur dans le champ User Name et votre mot de passe dans le champ Password.

   Remarque : le nom d'utilisateur et le mot de passe sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules. En cas de faute de frappe, cliquez sur Clear pour effacer la saisie ou le message d'erreur éventuel qui apparaît.

4. Cliquez sur Login (Connexion) ou appuyez sur Entrée. La page EMX s'ouvre.

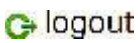
Remarque : selon votre configuration matérielle, les éléments affichés sur la page EMX peuvent différer légèrement de ceux présentés dans cette image.

Déconnexion

Une fois votre travail terminé dans EMX, déconnectez-vous pour empêcher à d'autres d'accéder à l'interface Web.

Pour vous déconnecter de l'interface Web :

1. Effectuez une des opérations suivantes :
   - Cliquez sur logout (déconnexion) dans l'angle supérieur droit de l'interface Web.

   - Fermez le navigateur Web en cliquant sur le bouton Fermer () dans l'angle supérieur droit du navigateur.
   - Fermez le navigateur Web en choisissant File > Close (Fichier > Fermer) ou File > Exit (Fichier > Quitter). La commande varie selon la version de navigateur utilisée.
   - Choisissez la commande Refresh (Actualiser) ou cliquez sur le bouton Refresh du navigateur Web.
2. La page de connexion s'ouvre ou le navigateur se ferme, selon votre choix à l'étape précédente.

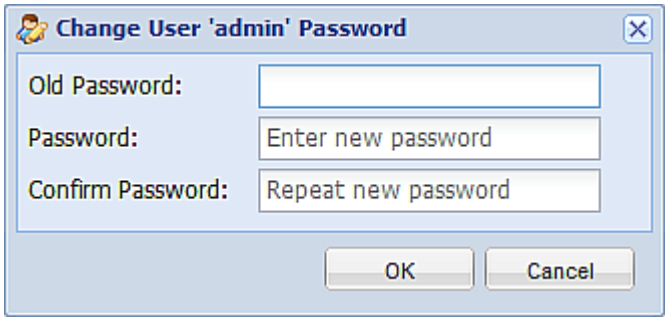
Modification de votre mot de passe

Les utilisateurs de base peuvent modifier leur propre mot de passe s'ils disposent de l'autorisation Change Own Password (Changer son propre mot de passe). Reportez-vous à ***Paramétrage des rôles*** (à la page 69).

Si vous êtes l'administrateur (admin), l'interface Web de EMX vous invite automatiquement à modifier le mot de passe s'il s'agit de la première connexion à EMX. Si vous disposez des privilèges d'administrateur, vous pouvez également modifier le mot de passe des autres utilisateurs. Reportez-vous à ***Modification d'un profil utilisateur*** (à la page 66).

Pour modifier votre mot de passe :

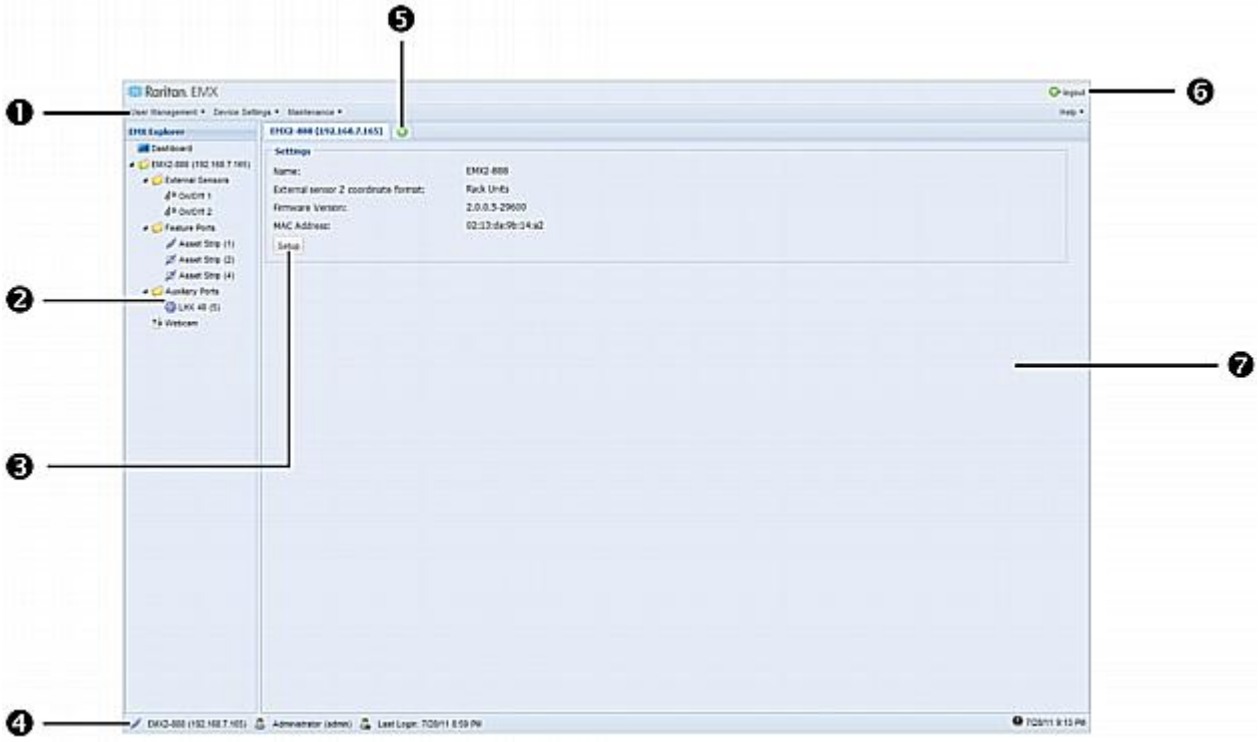
1. Sélectionnez User Management > Change Password (Gestion des utilisateurs > Modifier le mot de passe). La fenêtre Change User Password (Modifier le mot de passe utilisateur) s'affiche.



2. Tapez le mot de passe actuel dans le champ Old Password (Ancien mot de passe).
3. Entrez votre nouveau mot de passe dans les champs Password (Mot de passe) et Confirm Password (Confirmer le mot de passe). Le mot de passe peut comporter de 4 à 64 caractères. Il est sensible à la casse.
4. Cliquez sur OK pour enregistrer les modifications.

Introduction à l'interface Web

Sur chaque page, l'interface Web présente deux volets, une barre de menus, une barre de statut, une icône d'ajout de pages et un bouton de déconnexion.



Numéro	Elément de l'interface Web
❶	Menus
❷	Volet EMX Explorer
❸	Bouton Setup*
❹	Barre de statut
❺	Icône d'ajout de pages
❻	Bouton de déconnexion
❼	Volet de données

* Le bouton Setup n'est pas disponible sur certaines pages, notamment la page *Dashboard* (Tableau de bord).

Reportez-vous aux sections suivantes pour en savoir plus sur ces éléments de l'interface Web.

Menus

Quatre menus sont disponibles pour gérer les différentes tâches ou pour afficher des informations.

- **User Management** (Gestion des utilisateurs) contient des options de menu permettant la gestion des profils utilisateur, des autorisations (rôles) et du mot de passe.
- **Device Settings** (Paramètres du dispositif) concerne les paramètres relatifs au dispositif, tels que son nom, les paramètres réseau, les paramètres de sécurité et l'heure système.
- **Maintenance** présente des outils utiles à la maintenance du dispositif EMX, tels que le journal des événements, les informations sur le matériel, la mise à niveau du firmware, etc.
- **Help** (Aide) affiche des informations relatives au firmware et à tous les progiciels libres intégrés au dispositif EMX. En outre, vous pouvez accéder au manuel d'utilisation à partir de ce menu.

Bouton Setup

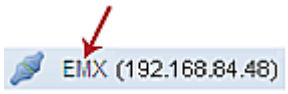
Le bouton Setup (Paramétrer) est disponible pour la plupart des éléments de l'arborescence. Il déclenche l'affichage d'une boîte de dialogue de paramétrage où vous pouvez modifier les paramètres de l'élément de l'arborescence sélectionné.

Barre de statut

La barre de statut présente cinq informations de gauche à droite :

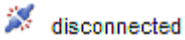
- **Nom du dispositif :**

  Il s'agit du nom attribué au dispositif EMX ; La valeur par défaut est EMX. Reportez-vous à ***Nommage du dispositif EMX*** (à la page 73).



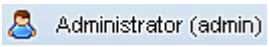
- **Adresse IP :**

  Les chiffres entre parenthèses représentent l'adresse IP affectée au dispositif EMX. Reportez-vous à Configuration initiale du réseau ou ***Modification des paramètres réseau*** (à la page 82).

Conseil : la présence du nom du dispositif et de l'adresse IP dans la barre de statut indique la connexion au dispositif EMX. Si la connexion est perdue,  *s'affiche à la place.*

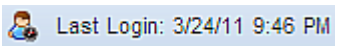
- **Nom de connexion :**

  Il s'agit du nom d'utilisateur ayant servi à la connexion à l'interface Web.

- **Last login time (Dernière heure de connexion) :**

  Ceci indique la date et l'heure auxquelles ce nom de connexion a été utilisé pour la dernière connexion au dispositif EMX.

  Lorsque le pointeur de la souris passe au-dessus de l'heure de la dernière connexion, des informations détaillées sur celle-ci s'affichent, notamment le client d'accès et l'adresse IP.

  Pour la connexion via une connexion série, la mention <local> est affichée à la place d'une adresse IP.

  Il existe différents types de clients d'accès :

  - Web GUI : fait référence à l'interface Web de EMX.
  - CLI : fait référence à l'interface de ligne de commande (CLI). Les informations entre parenthèses suivant CLI indiquent comment cet utilisateur était connecté à l'interface CLI.
    - *Serial* : représente la connexion locale (série ou USB).
    - *SSH* : représente la connexion SSH.
    - *Telnet* : représente la connexion Telnet.

- **Date et heure système :**

  La date, l'année et l'heure actuelles sont affichées sur la droite de la barre. Si vous placez le pointeur de la souris au-dessus de la date et de l'heure système, les informations de fuseau horaire sont également affichées.

Parfois, une icône de drapeau () apparaît tout à droite de la barre lorsqu'une erreur de communication se produit entre le dispositif EMX et l'interface graphique. Lorsque l'icône apparaît, vous pouvez cliquer dessus pour consulter le journal de communications. Reportez-vous à ***Consultation du journal de communication*** (à la page 160).

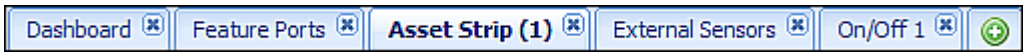
Icône d'ajout de pages

L'icône d'ajout de pages , située au sommet du volet de données, vous permet d'ouvrir les pages de données de plusieurs éléments d'arborescence sans supplanter les pages ouvertes.

Pour ouvrir de nouvelles pages de données :

1. Cliquez sur l'icône d'ajout de pages . Un nouvel onglet avec une page de données vide apparaît.
2. Cliquez sur l'élément d'arborescence dont vous souhaitez ouvrir la page de données. Les données de l'élément sélectionné sont alors affichées sur la page vide.
3. Pour ouvrir des pages de données supplémentaires, répétez les étapes 1 et 2. Tous les onglets représentant des pages ouvertes sont affichés en haut de la page.

   Le diagramme suivant présente un exemple de plusieurs onglets.



4. Lorsque plusieurs pages sont ouvertes, vous pouvez effectuer les actions suivantes :
   - Pour passer à l'une des pages de données ouvertes, cliquez sur l'onglet correspondant.

     Lorsque le nombre d'onglets à afficher est trop important, deux flèches (et) apparaissent sur les bordures gauche et droite du volet. Cliquez sur une des flèches pour parcourir tous les onglets.
   - Pour fermer une page de données, cliquez sur le bouton Fermer () dans l'onglet correspondant.

Volet de données

Le volet de droite affiche la page de données de l'élément de l'arborescence sélectionné. La page de données contient le statut actuel et les paramètres de l'élément, et un bouton Setup (le cas échéant).

Tous les onglets au-dessus du volet représentent les pages de données ouvertes. L'onglet mis en surbrillance indique la sélection en cours.

Vous pouvez modifier la largeur du volet pour agrandir ou réduire la zone.

Pour ajuster la largeur du volet :

1. Déplacez le pointeur de la souris vers la bordure gauche du volet de droite.
2. Lorsque le pointeur de la souris devient une flèche bidirectionnelle, faites glisser la bordure horizontalement pour élargir ou rétrécir le volet.

Icône d'avertissement

Si la valeur que vous avez entrée dans un champ spécifique n'est pas valide, une icône d'avertissement rouge apparaît sur la droite et le champ en question est encadré de rouge, comme le montre cette illustration.

Dans ce cas, placez le pointeur de la souris sur l'icône d'avertissement pour afficher le motif et modifier la valeur entrée en conséquence.

Relevés mis en surbrillance en jaune ou en rouge

Lorsqu'un relevé de capteur numérique dépasse un seuil supérieur ou inférieur, le fond de la rangée entière devient jaune ou rouge pour avertir les utilisateurs.

Pour un capteur discret (activé/désactivé), la rangée change de couleur de fond lorsque le capteur passe en état anormal.

Remarque : les capteurs numériques utilisent des valeurs numériques pour indiquer des conditions d'environnement ou internes, alors que les capteurs discrets (activé/désactivé) utilisent des caractères alphabétiques pour indiquer l'état.

Consultez le tableau pour connaître la signification de chaque couleur :

Couleur	Etat
Blanc	Le fond est blanc dans un des scénarios suivants : • Pour un capteur numérique, aucun seuil n'a été activé. • Si des seuils ont été activés pour un capteur numérique, le relevé de ce dernier se trouve entre les seuils d'avertissement inférieur et supérieur. • Pour un capteur discret (activé/désactivé), l'état est normal. • Le relevé ou l'état du capteur est indisponible.
Jaune	Le relevé descend sous le seuil d'avertissement inférieur ou monte au-dessus du seuil d'avertissement supérieur.
Rouge	La signification de la couleur rouge varie selon le type du capteur : • Pour un capteur numérique, cette couleur indique que le relevé descend sous le seuil critique inférieur ou monte au-dessus du seuil critique supérieur. • Pour un capteur discret (activé/désactivé), cette couleur indique l'état d'alarme. • Pour un échangeur thermique Schroff® LHX (si disponible), cette couleur indique qu'au moins un capteur implémenté sur cet échangeur est en panne. Reportez-vous à ***Echangeurs thermiques Schroff LHX*** (à la page 198).

Pour déterminer la signification exacte de l'alerte, lisez les informations affichées dans la colonne State (Etat) (ou Status (Statut)) :

- below lower critical : le relevé du capteur numérique descend sous le seuil critique inférieur.
- below lower warning : le relevé du capteur numérique descend sous le seuil d'avertissement inférieur.
- above upper critical : le relevé du capteur numérique atteint ou dépasse le seuil critique supérieur.
- above upper warning : le relevé du capteur numérique atteint ou dépasse le seuil d'avertissement supérieur.
- alarmed : le capteur discret N'EST PAS à l'état normal.

Pour obtenir des informations sur les seuils, reportez-vous à ***Configuration des capteurs d'environnement*** (à la page 168).

Menu de raccourcis défini par la navigateur

Un menu de raccourcis, intégré au navigateur Web, peut apparaître lorsque vous cliquez avec le bouton droit n'importe où dans l'interface Web de EMX.

Les fonctions du menu de raccourcis sont définies par le navigateur. Par exemple, la commande Retour du menu de raccourcis d'Internet Explorer® (IE) fonctionne de la même façon que le bouton Retour du navigateur IE. Ces deux fonctions permettent de retourner à la page précédente.

Reportez-vous à l'aide en ligne ou à la documentation accompagnant votre navigateur Web pour en savoir plus sur chaque commande ou option de menu de raccourcis.

Le menu de raccourcis du navigateur IE est illustré ci-dessous. Les commandes ou options de menu disponibles peuvent varier légèrement en fonction de la version de votre navigateur Web.

Affichage du tableau de bord

Lorsque vous vous connectez à l'interface Web, la page Dashboard (Tableau de bord) s'affiche par défaut. Cette page offre un aperçu du statut du dispositif EMX.

La page est divisée en plusieurs sections suivant l'équipement connecté, tel que des capteurs de ressources et d'environnement. Double-cliquez sur un élément de la page Dashboard pour ouvrir la page de données spécifique à celui-ci.

Remarque : si une rangée de relevés de capteur est colorée, ceci signifie qu'un relevé a déjà dépassé un des seuils ou qu'un des capteurs LHX intégré au moins est en panne sur l'échangeur thermique. Reportez-vous à **Relevés mis en surbrillance en jaune ou en rouge (EMX)** *(voir "***Relevés mis en surbrillance en jaune ou en rouge***" à la page 58).*

Si vous cliquez sur une autre icône de l'arborescence hiérarchique, la page Dashboard est supplantée. Pour retourner à la page Dashboard, cliquez sur l'icône correspondante.

Lorsque la page Dashboard est ouverte, vous pouvez effectuer les opérations suivantes pour afficher ou masquer des données spécifiques.

Pour réduire une section :

1. Localisez la section à réduire.
2. Cliquez sur la flèche vers le haut devant le titre de la section. Les données spécifiques de cette section sont masquées.

Pour développer une section réduite :

1. Localisez la section à développer.
2. Cliquez sur la flèche vers le bas devant le titre de la section. Les données spécifiques de cette section apparaissent.

Chapitre 4 Gestion des utilisateurs et des rôles

Dans ce chapitre

Aperçu

A la livraison, EMX intègre un profil utilisateur : **admin**, utilisé pour la connexion et la configuration initiales. Ce profil dispose d'autorisations complètes sur le système et doit être réservé à l'administrateur système. Il ne peut pas être supprimé et ses autorisations ne sont pas configurables par l'utilisateur, hormis l'autorisation SNMP v3.

Tous les utilisateurs doivent disposer d'un profil indiquant un nom et un mot de passe de connexion, et contenant des informations supplémentaires (facultatives) sur l'utilisateur. Chaque profil utilisateur doit disposer d'au moins un rôle pour déterminer les autorisations système de l'utilisateur. Reportez-vous à ***Paramétrage des rôles*** (à la page 69). Pour assurer la gestion des paramètres, vous devez vous connecter au compte d'utilisateur doté des autorisations appropriées.

Par défaut, plusieurs utilisateurs peuvent se connecter simultanément à l'aide du même nom de connexion.

Gestion des utilisateurs

Création d'un profil utilisateur

La création d'utilisateurs ajoute une nouvelle connexion au dispositif EMX.

Pour créer un profil utilisateur :

1. Choisissez User Management > Users (Gestion des utilisateurs > Utilisateurs). La boîte de dialogue Manage Users (Gérer les utilisateurs) apparaît.
2. Cliquez sur New (Nouveau). La boîte de dialogue Create New User (Créer un utilisateur) apparaît.
3. Tapez les informations relatives à l'utilisateur dans les champs correspondants. Notez que les champs User Name (Nom d'utilisateur), Password (Mot de passe) et Confirm Password (Confirmer le mot de passe) sont obligatoires.

Champ	Entrez...
User Name (Nom d'utilisateur)	Nom que l'utilisateur entre pour se connecter à EMX. ▪ Le nom peut comporter de 4 à 32 caractères. ▪ Il est sensible à la casse. ▪ Les espaces NE SONT PAS autorisés.
Full Name (Nom complet)	Prénom et nom de l'utilisateur.
Password (Mot de passe), Confirm Password (Confirmer le mot de passe)	Mot de passe que l'utilisateur doit entrer pour se connecter. Tapez-le d'abord dans le champ Password (Mot de passe), puis de nouveau dans le champ Confirm Password (Confirmer le mot de passe). ▪ Le mot de passe peut comporter de 4 à 32 caractères. ▪ Il est sensible à la casse. ▪ Les espaces sont autorisés.
Telephone Number (Numéro de téléphone)	Un numéro de téléphone auquel l'utilisateur peut être joint.
eMail Address (Adresse électronique)	Adresse électronique à laquelle l'utilisateur peut être joint. ▪ L'adresse électronique peut comporter de 4 à 32 caractères. ▪ Il est sensible à la casse.

4. Cochez la case Enabled (Activé). Sinon, l'utilisateur NE PEUT PAS se connecter au dispositif EMX.
5. Cochez la case Force password change on next login (Exiger la modification du mot de passe à la prochaine connexion) si vous préférez que l'utilisateur modifie le mot de passe à la première connexion après l'activation de cette case à cocher.
6. Cliquez sur l'onglet SNMPv3 pour définir l'autorisation d'accès SNMPv3. L'autorisation est désactivée par défaut.
   a. Pour autoriser l'accès SNMPv3 à cet utilisateur, cochez la case Enable SNMPv3 access (Activer l'accès SNMPv3). Sinon, laissez-la vide.

Remarque : le protocole SNMPv3 doit être activé pour l'accès SNMPv3. Reportez-vous à **Configuration des paramètres SNMP** *(à la page 88).*

b. Définissez les paramètres SNMPv3 si l'autorisation d'accès SNMPv3 est activée.

Champ	Description
Security Level (Niveau de sécurité)	Cliquez sur la flèche déroulante pour sélectionner un niveau de sécurité privilégié dans la liste : ▪ NoAuthNoPriv : pas d'authentification et pas de confidentialité. ▪ AuthNoPriv : authentification et pas de confidentialité. ▪ AuthPriv : authentification et confidentialité. Il s'agit de la valeur par défaut.
Use Password as Authentication Pass Phrase (Utiliser le mot de passe comme phrase passe d'authentification)	*Cette case à cocher n'est configurable que si AuthNoPriv ou AuthPriv est sélectionné.* Lorsque la case est cochée, la phrase passe d'authentification est identique au mot de passe de l'utilisateur. Pour indiquer une phrase passe d'authentification différente, désactivez la case à cocher.
Authentication Pass Phrase (Phrase passe d'authentification)	Tapez la phrase passe d'authentification dans ce champ si la case Use Password as Authentication Pass Phrase (Utiliser le mot de passe comme phrase de passe d'authentification) n'est pas cochée. La phrase passe doit comporter 8 à 32 caractères ASCII imprimables.
Confirm Authentication Pass Phrase (Confirmer la phrase passe d'authentification)	Entrez à nouveau la même phrase passe d'authentification pour la confirmer.
Use Authentication Pass Phrase as Privacy Pass Phrase (Utiliser la phrase passe d'authentification comme phrase de passe de confidentialité)	*Cette case à cocher est modifiable uniquement si AuthPriv est sélectionné.* Lorsque cette case est cochée, la phrase passe de confidentialité est identique à la phrase passe d'authentification. Pour définir une phrase passe de confidentialité différente, décochez la case.

Champ	Description
Privacy Pass Phrase (Phrase passe de confidentialité)	Entrez la phrase passe de confidentialité dans ce champ lorsque la case Use Authentication Pass Phrase as Privacy Pass Phrase (Utiliser la phrase passe d'authentification comme phrase passe de confidentialité) n'est pas cochée. La phrase passe doit comporter 8 à 32 caractères ASCII imprimables.
Confirm Privacy Pass Phrase (Confirmer la phrase passe de confidentialité)	Entrez à nouveau la même phrase passe de confidentialité pour la confirmer.
Protocole d'authentification	Cliquez sur la flèche déroulante et sélectionnez le protocole d'authentification souhaité dans la liste. Deux protocoles sont disponibles : ▪ MD5 ▪ SHA-1 (défaut)
Protocole de confidentialité	Cliquez sur la flèche déroulante et sélectionnez le protocole de confidentialité souhaité dans la liste. Deux protocoles sont disponibles : ▪ DES (défaut) ▪ AES-128

7. Cliquez sur l'onglet SSH pour entrer la clé publique si l'authentification correspondante est activée pour le service SSH. Reportez-vous à ***Modification des paramètres SSH*** (à la page 88).
   a. Ouvrez la clé publique SSH à l'aide d'un éditeur de texte.
   b. Copiez et collez tout le contenu de l'éditeur de texte dans le champ Public Key de l'onglet SSH.
8. Cliquez sur l'onglet Roles (Rôles) pour déterminer les autorisations de l'utilisateur.
9. Sélectionnez un ou plusieurs rôles en cochant les cases correspondantes.
   - Le rôle Admin fournit des autorisations complètes.
   - Le rôle Operator (Opérateur) accorde des autorisations limitées pour les fonctions fréquemment utilisées. Reportez-vous à ***Paramétrage des rôles*** (à la page 69) pour connaître la portée des autorisations. Ce rôle est sélectionné par défaut.
   - Lorsqu'aucun rôle ne répond à vos besoins, vous pouvez :

- *modifier les autorisations d'un rôle existant :* Pour modifier les autorisations d'un rôle, double-cliquez sur le rôle ou mettez-le en surbrillance, puis cliquez sur Edit Role (Modifier le rôle). Reportez-vous à ***Modification d'un rôle*** (à la page 70).
- *créer un rôle en cliquant sur le bouton Manage Roles (Gérer les rôles) :* reportez-vous à ***Création d'un rôle*** (à la page 69).

Remarque : lorsque plusieurs rôles sont sélectionnés, un utilisateur dispose de l'union des autorisations de tous les rôles.

10. Pour changer les unités de mesure affichées dans l'interface Web pour ce nouvel utilisateur, cliquez sur l'onglet Preferences et effectuez une des opérations suivantes :
    - Dans le champ Temperature Unit (Unité de température), sélectionnez °C (Celsius) ou °F (Fahrenheit) comme unité de mesure pour les températures.
    - Dans le champ Length Unit (Unité de longueur), sélectionnez Meter (Mètre) ou Feet (Pieds) comme unité de mesure de longueur ou de hauteur.
    - Dans le champ Pressure Unit (Unité de pression), sélectionnez Pascal ou psi comme unité de mesure de pression.

    Un pascal est égal à un newton par mètre carré. Psi signifie pounds per square inch (livres par pouce carré).

    Remarque : la modification des unités de mesure ne s'applique qu'à l'interface Web et à l'interface de ligne de commande.
11. Cliquez sur OK pour enregistrer les modifications.

Modification d'un profil utilisateur

Vous pouvez changer toutes les informations d'un profil utilisateur à l'exception du nom d'utilisateur.

Pour modifier un profil utilisateur :

1. Choisissez User Management > Users (Gestion des utilisateurs > Utilisateurs). La boîte de dialogue Manage Users (Gérer les utilisateurs) apparaît.
2. Sélectionnez l'utilisateur en cliquant dessus.
3. Cliquez sur Edit (Modifier) ou double-cliquez sur l'utilisateur. La boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX), où XXX est le nom de l'utilisateur.
4. Apportez toutes les modifications nécessaires aux informations affichées.

Pour modifier le mot de passe, entrez-en un nouveau dans les champs Password (Mot de passe) et Confirm Password (Confirmer le mot de passe). Si le champ du mot de passe reste vide, le mot de passe n'est pas modifié.

5. Pour modifier les autorisations d'accès SNMPv3, cliquez sur l'onglet SNMPv3 et effectuez les modifications nécessaires. Reportez-vous à l'étape 6 de ***Création d'un profil utilisateur*** (à la page 62).
6. Pour modifier les autorisations, cliquez sur l'onglet Roles (Rôles) et effectuez une des opérations suivantes :
   - Sélectionnez ou désélectionnez la case à cocher d'un rôle.
   - Pour modifier les autorisations d'un rôle, double-cliquez sur le rôle ou mettez-le en surbrillance, puis cliquez sur Edit Role (Modifier le rôle). Reportez-vous à ***Modification d'un rôle*** (à la page 70).
7. Pour changer l'unité de mesure de température, de longueur ou de pression, cliquez sur l'onglet Preferences, puis sélectionnez une option différente dans la liste déroulante.

   Remarque : la modification des unités de mesure ne s'applique qu'à l'interface Web et à l'interface de ligne de commande.
8. Cliquez sur OK pour enregistrer les modifications.

Suppression d'un profil utilisateur

Supprimez des profils utilisateur obsolètes ou redondants lorsque nécessaire.

Pour supprimer des profils utilisateur :

1. Choisissez User Management > Users (Gestion des utilisateurs > Utilisateurs). La boîte de dialogue Manage Users (Gérer les utilisateurs) apparaît.
2. Sélectionnez l'utilisateur à supprimer en cliquant dessus. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
3. Cliquez sur Delete (Supprimer).
4. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.

Modification de la vue de la liste d'utilisateurs

Vous pouvez modifier le nombre de colonnes affichées ou l'ordre de tri de la liste pour améliorer l'affichage des données. Reportez-vous à Modification de la vue d'une liste.

Affichage des utilisateurs connectés

Vous pouvez voir les utilisateurs connectés au dispositif EMX et leur statut. Si vous disposez des privilèges d'administrateur, vous pouvez mettre fin à la connexion au dispositif EMX de n'importe quel utilisateur.

Pour voir les utilisateurs connectés :

1. Choisissez Maintenance > Connected Users (Utilisateurs connectés). La boîte de dialogue Connected Users s'affiche, qui présente la liste des utilisateurs connectés et les données suivantes :

Colonne	Description
User Name (Nom d'utilisateur)	Nom de connexion utilisé par chaque utilisateur connecté.
IP Address (Adresse IP)	Adresse IP de l'hôte de chaque utilisateur. Pour la connexion via une connexion série, la mention <local> est affichée à la place d'une adresse IP.
Client Type (Type de client)	Interface par laquelle l'utilisateur est connecté à EMX. ▪ Web GUI : fait référence à l'interface Web de EMX. ▪ CLI : fait référence à l'interface de ligne de commande (CLI). Les informations entre parenthèses suivant CLI indiquent comment cet utilisateur était connecté à l'interface CLI. - *Serial* : représente la connexion locale (série ou USB). - *SSH* : représente la connexion SSH. - *Telnet* : représente la connexion Telnet.
Idle Time (Délai d'inactivité)	Durée pendant laquelle l'utilisateur reste inactif. L'unité min représente les minutes.

1. Pour déconnecter n'importe quel utilisateur, cliquez sur le bouton Disconnect correspondant.
   a. La boîte de dialogue qui apparaît vous invite à confirmer l'opération.
   b. Cliquez sur Yes pour déconnecter l'utilisateur ou sur No pour abandonner l'opération. Si vous cliquez sur Yes, l'utilisateur est forcé de se déconnecter.
2. Vous pouvez modifier l'ordre de tri de la liste, si nécessaire. Reportez-vous à Modification du tri.
3. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Gestion des rôles

Paramétrage des rôles

Pour assurer la gestion des paramètres, vous devez vous connecter au compte d'utilisateur doté des autorisations appropriées. Un rôle définit les opérations et fonctions qu'un utilisateur est autorisé à effectuer ou auxquelles il peut accéder. Chaque utilisateur doit être associé à un rôle au moins.

EMX est livré avec deux rôles intégrés : **Admin** et **Operator**.

- Le rôle Admin fournit des autorisations complètes. Vous ne pouvez ni modifier ni supprimer ce rôle.
- Le rôle Operator (Opérateur) accorde des autorisations limitées pour les fonctions fréquemment utilisées. Vous pouvez modifier ou supprimer ce rôle. Par défaut, le rôle Operator contient ces autorisations :
  - Afficher les paramètres de l'événement
  - Afficher le journal des événements
  - Modifier les paramètres de l'événement
  - Changer son propre mot de passe
  - Modifier la configuration EMD
- Le rôle Operator est affecté à un nouveau profil utilisateur par défaut. Reportez-vous à ***Création d'un profil utilisateur*** (à la page 62).

Création d'un rôle

Créez un rôle lorsque vous avez besoin d'une nouvelle combinaison d'autorisations.

Pour créer un rôle :

1. Choisissez User Management > Roles (Gestion des utilisateurs > Rôles). La boîte de dialogue Manage Roles (Gérer les rôles) apparaît.

   Conseil : vous pouvez également accéder à la boîte de dialogue Manage Roles en cliquant sur le bouton Manage Roles de la boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX).

2. Cliquez sur New (Nouveau). La boîte de dialogue Create New Role (Créer un rôle) apparaît.
3. Tapez le nom du rôle dans le champ Role Name.
4. Tapez une description du rôle dans le champ Description.

5. Cliquez sur l'onglet Privileges pour afficher une ou plusieurs autorisations.
   a. Cliquez sur Add (Ajouter). La boîte de dialogue Add Privileges to new Role (Ajouter des privilèges au nouveau rôle) apparaît.
   b. Sélectionnez l'autorisation souhaitée dans la liste Privileges.
   c. Si l'autorisation sélectionnée contient des définitions d'argument, la liste Arguments s'affiche sur la droite. Sélectionnez ensuite un ou plusieurs arguments.
   d. Cliquez sur Add pour ajouter l'autorisation sélectionnée (et les arguments éventuels).
   e. Répétez les étapes *a* à *d* jusqu'à ce que toutes les autorisations nécessaires soient ajoutées.
6. Cliquez sur OK pour enregistrer les modifications.

Vous pouvez maintenant affecter le nouveau rôle à des utilisateurs. Reportez-vous à ***Création d'un profil utilisateur*** (à la page 62) ou ***Modification d'un profil utilisateur*** (à la page 66).

Modification d'un rôle

Vous pouvez modifier les paramètres d'un rôle existant, mais pas son nom.

Pour modifier un rôle :

1. Choisissez User Management > Roles (Gestion des utilisateurs > Rôles). La boîte de dialogue Manage Roles (Gérer les rôles) apparaît.

   Conseil : vous pouvez également accéder à la boîte de dialogue Manage Roles en cliquant sur le bouton Manage Roles de la boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX).

2. Sélectionnez le rôle à modifier en cliquant dessus.
3. Cliquez sur Edit (Modifier) ou double-cliquez sur le rôle. La boîte de dialogue Edit Role XXX (Modifier le rôle XXX) s'affiche, où XXX est le nom du rôle.

   Conseil : vous pouvez également accéder à la boîte de dialogue Edit Role XXX en cliquant sur le bouton Edit Role de la boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX).

4. Le cas échéant, modifiez le texte affiché dans le champ Description.
5. Pour modifier les autorisations, cliquez sur l'onglet Privileges.

   Remarque : vous ne pouvez pas modifier les autorisations du rôle Admin.

6. Pour supprimer des autorisations, procédez comme suit :
   a. Sélectionnez l'autorisation à supprimer en cliquant dessus. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
   b. Cliquez sur Delete (Supprimer).
7. Pour ajouter des autorisations, procédez comme suit :
   a. Cliquez sur Add (Ajouter). La boîte de dialogue Add Privileges to Role XXX (Ajouter des privilèges au rôle XXX) s'affiche, où XXX est le nom du rôle.
   b. Sélectionnez l'autorisation souhaitée dans la liste Privileges.
   c. Si l'autorisation sélectionnée contient des définitions d'argument, la liste Arguments s'affiche sur la droite. Sélectionnez ensuite un ou plusieurs arguments.
   d. Cliquez sur Add pour ajouter l'autorisation sélectionnée (et les arguments éventuels).
   e. Répétez les étapes *a* à *d* jusqu'à ce que toutes les autorisations nécessaires soient ajoutées.
8. Pour modifier les arguments d'une autorisation spécifique, procédez comme suit :
   a. Sélectionnez l'autorisation en cliquant dessus.
   b. Cliquez sur Edit (Modifier). La boîte de dialogue Edit arguments of privilege XXX (Modifier les arguments du privilège XXX), où XXX est le nom du privilège.

   Remarque : si l'autorisation sélectionnée ne contient aucun argument, le bouton Edit (Modifier) est désactivé.

   c. Sélectionnez l'argument souhaité. Vous pouvez effectuer plusieurs sélections.
   d. Cliquez sur OK.
9. Cliquez sur OK pour enregistrer les modifications.

Suppression d'un rôle

Vous pouvez supprimer tous les rôles à l'exception du rôle Admin.

Pour supprimer un rôle :

1. Choisissez User Management > Roles (Gestion des utilisateurs > Rôles). La boîte de dialogue Manage Roles (Gérer les rôles) apparaît.

   Conseil : vous pouvez également accéder à la boîte de dialogue Manage Roles en cliquant sur le bouton Manage Roles de la boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX).

2. Sélectionnez le rôle à supprimer en cliquant dessus. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
3. Cliquez sur Delete (Supprimer).
4. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.

Chapitre 5 Gestion du dispositif EMX

Dans ce chapitre

Aperçu

Vous trouverez ci-après des informations concernant le paramétrage et la gestion du dispositif EMX après son installation.

Eventuellement, si vous avez déjà installé et configuré un dispositif EMX et en configurez un autre, vous pouvez utiliser la fonction de configuration en bloc pour faciliter cette opération. Reportez-vous à ***Paramétrage d'un dispositif EMX à l'aide de la configuration en bloc*** (à la page 92).

Nommage du dispositif EMX

Le nom par défaut d'un dispositif EMX est *EMX*. Ce nom peut être changé, le cas échéant.

Pour modifier le nom du dispositif :

1. Dans le volet de navigation gauche, cliquez sur le dossier EMX. La page Settings (Paramètres) s'ouvre.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur Setup (Paramétrer) dans la page Settings. La boîte de dialogue EMX Setup (Paramétrage du dispositif EMX) apparaît.

3. Entrez un nouveau nom dans le champ Device Name (Nom du dispositif).
4. Cliquez sur OK pour enregistrer les modifications.

Affichage des informations de dispositif

La boîte de dialogue Device Information (Informations sur le dispositif) présente des données spécifiques au dispositif EMX auquel vous accédez, telles que des identifiants et des versions de protocoles de capteurs de ressources.

Pour afficher les informations sur le dispositif :

1. Sélectionnez Maintenance > Device Information (Informations sur le dispositif). La boîte de dialogue Device Information s'affiche.
2. Cliquez sur l'onglet contenant les informations que vous souhaitez consulter.

Onglet	Informations affichées
Device Information (Informations sur le dispositif)	Informations générales sur le dispositif, telles que nom du modèle, numéro de série, version de firmware, révision matérielle, etc.
Bandeaux des ressources	Identifiant, version de démarrage, d'application et de protocole de chaque capteur de ressources.

3. Agrandissez la boîte de dialogue si nécessaire.
4. Vous pouvez retrier la liste ou modifier les colonnes affichées.
5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Conseil : la version du firmware est également disponible en cliquant sur le dossier EMX dans le volet EMX Explorer.

Paramétrage de la date et de l'heure

Réglez manuellement l'horloge interne du dispositif EMX ou reliez-vous à un serveur NTP (Network Time Protocol) et laissez-le définir la date et l'heure.

Pour définir la date et l'heure :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Date/Time (Date/heure). La fenêtre Configure Date/Time Settings (Configurer les paramètres date/heure) s'affiche.
2. Dans le champ Timezone (Fuseau horaire), cliquez sur la flèche déroulante et sélectionnez votre fuseau horaire dans la liste.

3. Si l'heure d'été s'applique à votre fuseau horaire, assurez-vous que la case Automatic Daylight Saving Time Adjustment (Passage automatique à l'heure d'été) est cochée.

   Si les règles d'heure d'été ne sont pas disponibles pour le fuseau horaire sélectionné, la case à cocher n'est pas configurable.

4. Choisissez une des méthodes suivantes pour définir la date et l'heure :

   - Pour personnaliser la date et l'heure, sélectionnez la case d'option User Specified Time (Heure spécifiée par l'utilisateur), puis entrez la date et l'heure dans les champs appropriés. Utilisez le format aaaa-mm-jj pour la date et hh:mm:ss pour l'heure.
     - Pour définir la date, supprimez les chiffres existants du champ Date et tapez-en de nouveaux, ou cliquez sur l'icône de calendrier pour sélectionner une date.
     - L'heure est mesurée au format de 24 heures. Vous pouvez entrer l'heure en supprimant les chiffres existants des champs d'heure, de minutes et de secondes et en en tapant de nouveaux, ou en cliquant sur les flèches pour ajuster chaque nombre.
   - Pour laisser un serveur NTP régler la date et l'heure, sélectionnez la case d'option Synchronize with NTP Server (Synchroniser avec le serveur NTP). Il existe deux manières d'affecter les serveurs NTP.
     - Pour utiliser les serveurs NTP affectés par DHCP, assurez-vous que la case Always use the servers below and ignore DHCP-provided servers (Utiliser systématiquement les serveurs ci-dessous et ignorer les serveurs fournis par DHCP) n'est pas cochée. Cette méthode n'est utilisable que lorsque DHCP IPv4 ou IPv6 est activé.
     - Pour utiliser les serveurs NTP précisés manuellement, cochez la case Always use the servers below and ignore DHCP-provided servers, et indiquez le serveur NTP principal dans le champ First Time Server (Premier serveur d'horloge). Un serveur NTP secondaire est facultatif.

   Remarque : si l'adresse IP du dispositif EMX est affectée via DHCP IPv4 ou IPv6, les serveurs NTP peuvent être automatiquement détectés. Dans ce cas, les données entrées dans les champs des premier et second serveurs d'horloge seront supplantées.

5. Cliquez sur OK pour enregistrer les modifications.

Définition de l'altitude du dispositif

Vous devez indiquer l'altitude au-dessus du niveau de la mer du dispositif EMX si un capteur de pression d'air différentielle est branché. En effet, l'altitude du dispositif est associée au facteur de correction pour l'altitude. Reportez-vous à ***Facteurs de correction pour l'altitude*** (voir "***Facteurs de correction pour l'altitude (EMX)***" à la page 327).

L'unité de mesure de l'altitude est par défaut le mètre. Vous pouvez faire varier l'unité de mesure entre mètre et pied suivant les informations d'identification des utilisateurs. Reportez-vous à ***Modification des unités de mesure*** (à la page 76).

Pour définir l'altitude du dispositif EMX :

1. Dans le volet de navigation gauche, cliquez sur le dossier EMX. La page Settings (Paramètres) s'ouvre.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur Setup (Paramétrer) dans la page Settings. La boîte de dialogue EMX Setup (Paramétrage du dispositif EMX) apparaît.
3. Entrez un nombre entier dans le champ Altitude. Suivant l'unité de mesure affichée, la fourchette de nombres valides varie.
   - Pour les mètres (m), les valeurs sont comprises entre 0 et 3000.
   - Pour les pieds (ft), la valeur est comprise entre 0 et 9842.
4. Cliquez sur OK pour enregistrer les modifications.

Modification des unités de mesure

Par défaut, les unités de mesure suivantes sont appliquées à toutes les données présentées dans l'interface Web de EMX :

- Température : degrés en Celsius (°C)
- Longueur ou hauteur : mètres (m)
- Pression d'air : pascal (pa)

L'interface Web de EMX présente différentes unités de mesure suivant le nom de connexion utilisateur. C'est-à-dire que les utilisateurs peuvent voir des unités de mesure différentes affichées en fonction de leurs préférences. Les alternatives de chaque unité de mesure sont les suivantes :

- Température : degrés en Fahrenheit (°F)
- Longueur ou hauteur : pieds (ft)

- Pression d'air : psi

Déterminez l'unité de mesure désirée lors de la création des profils utilisateur. Reportez-vous à ***Création d'un profil utilisateur*** (à la page 62). Pour modifier les unités de mesure définies, vous devez disposer des privilèges d'administrateur.

Pour définir les unités de mesure privilégiées :

1. Choisissez User Management > Users (Gestion des utilisateurs > Utilisateurs). La boîte de dialogue Manage Users (Gérer les utilisateurs) apparaît.
2. Sélectionnez l'utilisateur en cliquant dessus.
3. Cliquez sur Edit (Modifier) ou double-cliquez sur l'utilisateur. La boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX), où XXX est le nom de l'utilisateur.
4. Cliquez sur l'onglet Preferences.
5. Pour modifier l'unité de température, sélectionnez l'option désirée dans le champ Temperature Unit.
   - °C : Cette option affiche la température en Celsius.
   - °F : Cette option affiche la température en Fahrenheit.
6. Pour modifier l'unité de longueur ou de hauteur, sélectionnez l'option désirée dans le champ Length Unit.
   - Meter (Mètre) : Cette option affiche la longueur ou la hauteur en mètres.
   - Feet (Pieds) : Cette option affiche la longueur ou la hauteur en pieds.
7. Pour modifier l'unité de pression, sélectionnez l'option désirée dans le champ Pressure Unit.
   - Pascal : Cette option affiche la valeur de pression en Pascals (Pa). Un pascal est égal à un newton par mètre carré.
   - psi : Cette option affiche la valeur de pression en psi. Psi signifie pounds per square inch (livres par pouce carré).
8. Cliquez sur OK pour enregistrer les modifications.

Définition du mode d'affichage des éléments d'arborescence

Par défaut, l'interface Web de EMX affiche les dispositifs connectés dans l'arborescence uniquement si des dispositifs sont physiquement connectés aux ports FEATURE et RS-485 (auxiliaires) et n'affiche rien si aucun dispositif n'est connecté.

L'interface Web de EMX permet de définir quand et comment afficher les icônes des dispositifs connectés et déconnectés dans l'arborescence.

Comment afficher des capteurs de ressources

Il existe deux manières d'afficher les capteurs de ressources connectés dans l'arborescence de l'interface Web :

- Les capteurs de ressources sont affichés uniquement lorsqu'ils sont connectés physiquement.
- Les capteurs de ressources sont toujours affichés qu'ils soient physiquement connectés ou non, mais leur icône change pour indiquer le statut de connexion.

Pour déterminer comment afficher les capteurs de ressources connectés :

1. Cliquez sur le dossier Feature Ports (Ports de fonction). La page correspondante s'ouvre dans le volet de droite et affiche tous les ports FEATURE.
2. Sélectionnez le numéro du port que vous souhaitez configurer et cliquez sur Setup (Paramétrer). Vous pouvez également double-cliquer sur ce numéro de port. La boîte de dialogue Feature Port Setup (Paramétrage du port de fonction) apparaît.
3. Dans le champ Detection Mode (Mode de détection), sélectionnez le mode d'affichage des capteurs de ressources connectés.
   - Disabled (Désactivé) : lorsqu'appliqué, désactive vers le port et aucun objet connecté au port n'est détecté.
   - Auto : une icône est affichée pour ce port uniquement lorsque le dispositif EMX détecte la connexion physique du capteur à ce port. Sinon, rien n'est affiché. Il s'agit de l'approche par défaut.
   - Pinned (A broche) : une icône est affichée pour ce port à tout moment mais son image varie suivant le statut de connexion. Lorsque la connexion d'un capteur de ressources est détectée sur un port Feature particulier, l'icône  est affichée sur ce dernier. Si elle n'est pas détectée, l'icône  apparaît à la place. Reportez-vous à ***Définition du mode d'affichage des éléments d'arborescence*** (à la page 77).

     Lorsque la case Pinned est cochée, cliquez sur la flèche déroulante pour sélectionner le type de dispositif à afficher. Sélectionnez Asset Strip (Bandeau de ressources) pour les capteurs de ressources.
4. Cliquez sur OK pour enregistrer les modifications.

Dans l'arborescence, l'icône, le cas échéant, est suivie du nom du dispositif, si disponible, de son type et du numéro de port.

Comment afficher les échangeurs thermiques LHX

Il existe deux manières d'afficher les échangeurs thermiques Schroff® LHX connectés dans l'arborescence de l'interface Web :

- Les échangeurs thermiques LHX sont affichés uniquement lorsqu'ils sont connectés physiquement.
- Les échangeurs thermiques LHX sont toujours affichés qu'ils soient physiquement connectés ou non, mais leur icône change pour indiquer le statut de connexion.

EMX prend en charge les modèles LHX-20 et LHX-40.

Remarque : la prise en charge de Schroff LHX doit être activée pour que le LHX soit affiché. Reportez-vous à **Activation et désactivation de la prise en charge de l'échangeur thermique Schroff LHX** *(à la page 199).*

Pour déterminer comment afficher les échangeurs thermiques LHX :

1. Cliquez sur le dossier Auxiliary Ports (Ports auxiliaires) ou Feature Ports (Ports de fonction) suivant le port auquel vous souhaitez relier le capteur.
2. Sélectionnez le numéro du port que vous souhaitez configurer et cliquez sur Setup (Paramétrer). Vous pouvez également double-cliquer sur ce numéro de port. La boîte de dialogue Auxiliary Port Setup (Paramétrage des ports auxiliaires) apparaît.
3. Dans le champ Detection Mode (Mode de détection), sélectionnez le mode d'affichage des échangeurs thermiques LHX connectés.
   - Disabled (Désactivé) : lorsqu'appliqué, désactive vers le port et aucun objet connecté au port n'est détecté.
   - Auto : une icône est affichée pour ce port uniquement lorsque le dispositif EMX détecte la connexion physique de l'échangeur thermique à ce port. Sinon, rien n'est affiché. Il s'agit de l'approche par défaut.
   - Pinned (A broche) : une icône est affichée pour ce port à tout moment mais son image varie suivant le statut de connexion. Reportez-vous à ***Etats de dispositifs et variations des icônes*** (à la page 202).

     Lorsque la case Pinned est cochée, cliquez sur la flèche déroulante pour sélectionner le type de dispositif approprié pour ce port : LHX 20 ou LHX 40.
4. Cliquez sur OK pour enregistrer les modifications.

Dans l'arborescence, l'icône, si elle est présente, est suivie du nom du dispositif, si disponible, de son type et du numéro de port ou du port FEATURE (le cas échéant).

Modification de la configuration réseau

Par l'interface Web, vous pouvez modifier les paramètres réseau suivants : câblés, sans fil, IPv4 et/ou IPv6.

Modification des paramètres de l'interface réseau

EMX prend en charge deux types d'interfaces réseau : câblée et sans fil. Configurez les paramètres d'interface réseau selon le mode de mise en réseau applicable. Reportez-vous à ***Connexion du dispositif EMX au réseau*** (à la page 14).

Paramètres de réseau câblé

La vitesse et le mode bidirectionnel de l'interface LAN (réseau local) ont été définis au cours du processus d'installation et de configuration. Reportez-vous à Configuration initiale du réseau.

Par défaut, la vitesse et le mode bidirectionnel de l'interface LAN sont définis sur Auto (automatique), ce qui fonctionne dans presque tous les scénarios. Vous pouvez les modifier en cas d'exigences locales spéciales.

Pour modifier les paramètres de l'interface réseau :

1. Sélectionnez Device Settings > Network (Paramètres du dispositif > Réseau). La boîte de dialogue Network Configuration (Configuration du réseau) apparaît.
2. L'onglet Interface Settings (Paramètres de l'interface) aurait dû être sélectionné. S'il ne l'est pas, cliquez dessus.
3. Dans le champ Network Interface (Interface réseau), cliquez sur la flèche déroulante et sélectionnez Wired (Câblée) dans la liste.
4. Pour modifier la vitesse de l'interface LAN, cliquez sur la flèche déroulante du champ Speed (Vitesse) et sélectionnez une option dans la liste.
   - Auto : Le système détermine la vitesse optimale du réseau local par négociation automatique.
   - 10 Mbit/s : La vitesse du réseau local est toujours de 10 Mbps.
   - 100 Mbit/s : La vitesse du réseau local est toujours de 100 Mbps.
5. Pour modifier le mode bidirectionnel, cliquez sur la flèche déroulante du champ Duplex et sélectionnez une option dans la liste.
   - Auto : EMX sélectionne le mode de transmission optimal par négociation automatique.
   - Full (Bidirectionnel simultané) : Les données sont transmises dans les deux sens simultanément.

- Half (Bidirectionnel non simultané) : Les données sont transmises dans une direction (vers ou depuis le dispositif EMX) à la fois.

6. Cliquez sur OK pour enregistrer les modifications.

Conseil : vous pouvez vérifier le statut du réseau local dans le champ Current State, notamment la vitesse et le mode bidirectionnel.

Paramètres de réseau sans fil

Les paramètres sans fil SSID, PSK et BSSID ont été définis pendant l'installation et la configuration. Reportez-vous à Configuration initiale du réseau. Vous pouvez les modifier via l'interface Web.

Pour modifier les paramètres de l'interface sans fil :

1. Sélectionnez Device Settings > Network (Paramètres du dispositif > Réseau). La boîte de dialogue Network Configuration (Configuration du réseau) apparaît.
2. L'onglet Interface Settings (Paramètres de l'interface) aurait dû être sélectionné. S'il ne l'est pas, cliquez dessus.
3. Dans le champ Network Interface (Interface réseau), cliquez sur la flèche déroulante et sélectionnez Wireless (Sans fil) dans la liste.
4. Vérifiez dans le champ Hardware State (Etat du matériel) que le dispositif EMX a détecté un adaptateur LAN USB sans fil. Sinon, vérifiez que l'adaptateur LAN USB est fermement connecté ou s'il est pris en charge. Reportez-vous à ***Connexion du dispositif EMX au réseau*** (à la page 14).
5. Entrez le nom du point d'accès (AP) sans fil dans le champ SSID.
6. Si l'identificateur BSSID est disponible, cochez la case Force AP BSSID (Forcer le BSSID du point d'accès) et entrez l'adresse MAC dans le champ BSSID.

Remarque : BSSID se réfère à l'adresse MAC d'un point d'accès dans le réseau sans fil.

7. Dans le champ Authentication (Authentification), cliquez sur la flèche déroulante et sélectionnez une option appropriée dans la liste.

Option	Description
No Authentication (Aucune authentification)	Sélectionnez cette option lorsqu'aucune donnée d'authentification n'est requise.
PSK	Une clé prépartagée (PSK) est requise pour cette option. ▪ Dans le champ Pre-Shared, entrez la chaîne PSK.

Option	Description
EAP - PEAP	PEAP désigne le protocole PEAP (Protected Extensible Authentication Protocol). Les données d'authentification suivantes sont requises : ▪ Inner Authentication (Authentification interne) : seul Challenge Authentication Protocol Version 2 (MSCHAPv2) de Microsoft est pris en charge, permettant l'authentification dans les bases de données acceptant MSCHAPv2. ▪ Identity : entrez votre nom d'utilisateur pour l'authentification EAP. ▪ Password (Mot de passe) : entrez votre mot de passe pour l'authentification EAP. ▪ CA Certificate : un certificat d'une autorité de certification tierce doit être fourni pour l'authentification EAP. Cliquez sur Browse (Parcourir) pour sélectionner un fichier de certificat valide. - Pour afficher le contenu du fichier de certificat sélectionné, cliquez sur Show (Afficher). - Si le fichier de certificat sélectionné n'est pas valide, cliquez sur Remove (Supprimer). Sélectionnez ensuite un nouveau fichier.

1. Cliquez sur OK pour enregistrer les modifications.

Modification des paramètres réseau

Le dispositif EMX a été configuré pour la connectivité réseau au cours du processus d'installation et de configuration. Reportez-vous à ***Configuration de EMX*** (voir "***Configuration du dispositif EMX***" à la page 11) Le cas échéant, vous pouvez modifier les paramètres réseau depuis l'interface Web.

Sélection du protocole Internet

Le dispositif EMX prend en charge deux types de protocoles Internet : IPv4 et IPv6. Vous pouvez activer ces deux protocoles ou l'un d'entre eux. Après l'activation, tous les protocoles ci-après, entre autres, seront compatibles avec les protocoles Internet choisis :

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

Pour sélectionner le protocole Internet approprié :

1. Sélectionnez Device Settings > Network (Paramètres du dispositif > Réseau). La boîte de dialogue Network Configuration (Configuration du réseau) apparaît.
2. Cliquez sur l'onglet IP Protocol (Protocole IP).
3. Cochez une case selon les protocoles Internet que vous souhaitez activer :
   - IPv4 only (IPv4 uniquement) : Active uniquement IPv4 sur toutes les interfaces. Il s'agit de la valeur par défaut.
   - IPv6 only (IPv6 uniquement) : Active uniquement IPv6 sur toutes les interfaces.
   - IPv4 and IPv6 : Active IPv4 et IPv6 sur toutes les interfaces.
4. Si vous avez coché la case IPv4 and IPv6 à l'étape précédente, vous devez déterminer l'adresse IP utilisée lorsque le résolveur DNS retourne des adresses IPv4 et IPv6.
   - Adresse IPv4 : Utilisez les adresses IPv4 renvoyées par le serveur DNS.
   - Adresse IPv6 : Utilisez les adresses IPv6 renvoyées par le serveur DNS.
5. Cliquez sur OK pour enregistrer les modifications.

Modification des paramètres IPv4

Vous devez activer le protocole IPv4 avant de modifier les paramètres réseau correspondants. Reportez-vous à ***Sélection du protocole Internet*** (à la page 83).

Pour modifier les paramètres IPv4 :

1. Sélectionnez Device Settings > Network (Paramètres du dispositif > Réseau). La boîte de dialogue Network Configuration (Configuration du réseau) apparaît.
2. Cliquez sur l'onglet IPv4 Settings (Paramètres IPv4).
3. Dans le champ IP Auto Configuration (Configuration automatique IP), cliquez sur la flèche déroulante et sélectionnez l'option souhaitée dans la liste.

Option	Description
DHCP	Pour configurer EMX automatiquement, sélectionnez DHCP. Si vous sélectionnez DHCP, vous pouvez entrer un nom d'hôte DHCP privilégié (facultatif). Tapez le nom d'hôte dans le champ Preferred Hostname (Nom d'hôte privilégié). Le nom d'hôte : ▪ se compose de caractères alphanumériques et/ou de tirets ; ▪ ne peut pas débuter ni finir par un tiret ; ▪ ne peut pas contenir plus de 63 caractères ; ▪ ne peut pas contenir de signes de ponctuation, d'espaces et autres symboles. Le cas échéant, cochez la case Specify DNS server manually (Indiquer le serveur DNS manuellement). Tapez ensuite l'adresse du serveur DNS principal dans le champ Primary DNS Server. Le serveur DNS secondaire et le suffixe DNS sont facultatifs.
Static	Pour affecter manuellement une adresse IP, sélectionnez Static et entrez les informations suivantes dans les champs correspondants : ▪ l'adresse IP ▪ le masque réseau ▪ la passerelle ▪ le serveur DNS principal

Option	Description
	▪ le serveur DNS secondaire (facultatif) ▪ le suffixe DNS (facultatif)

4. Cliquez sur OK pour enregistrer les modifications.

Remarque : EMX prend en charge trois serveurs DNS au maximum. Si deux serveurs DNS IPv4 et deux serveurs DNS IPv6 sont disponibles, EMX n'utilise que les serveurs DNS IPv4 et IPv6 principaux.

Modification des paramètres IPv6

Vous devez activer le protocole IPv6 avant de modifier les paramètres réseau correspondants. Reportez-vous à ***Sélection du protocole Internet*** (à la page 83).

Pour modifier les paramètres IPv6 :

1. Sélectionnez Device Settings > Network (Paramètres du dispositif > Réseau). La boîte de dialogue Network Configuration (Configuration du réseau) apparaît.
2. Cliquez sur l'onglet IPv6 Settings (Paramètres IPv6).
3. Dans le champ IP Auto Configuration (Configuration automatique IP), cliquez sur la flèche déroulante et sélectionnez l'option souhaitée dans la liste.

Option	Description
Automatic	Pour configurer EMX automatiquement, sélectionnez Automatic. Lorsque cette option est sélectionnée, vous pouvez entrer un nom d'hôte DHCP privilégié (facultatif). Tapez le nom d'hôte dans le champ Preferred Hostname (Nom d'hôte privilégié). Le nom d'hôte : ▪ se compose de caractères alphanumériques et/ou de tirets ; ▪ ne peut pas débuter ni finir par un tiret ; ▪ ne peut pas contenir plus de 63 caractères ; ▪ ne peut pas contenir de signes de ponctuation, d'espaces et autres symboles. Le cas échéant, cochez la case Specify DNS server manually (Indiquer le serveur DNS manuellement). Tapez ensuite l'adresse du serveur DNS principal dans le champ Primary DNS Server. Le serveur DNS secondaire et le

Option	Description
	suffixe DNS sont facultatifs.
Static	Pour affecter manuellement une adresse IP, sélectionnez Static et entrez les informations suivantes dans les champs correspondants : ▪ l'adresse IP ▪ la passerelle ▪ le serveur DNS principal ▪ le serveur DNS secondaire (facultatif) ▪ le suffixe DNS (facultatif)

4. Cliquez sur OK pour enregistrer les modifications.

Remarque : EMX prend en charge trois serveurs DNS au maximum. Si deux serveurs DNS IPv4 et deux serveurs DNS IPv6 sont disponibles, EMX n'utilise que les serveurs DNS IPv4 et IPv6 principaux.

Rôle d'un serveur DNS

Etant donné que les communications Internet sont réalisées sur la base des adresses IP, des paramètres de serveur DNS appropriés sont nécessaires pour le mappage des noms de domaine (noms d'hôte) aux adresses IP correspondantes. Sinon, la tentative de connexion de EMX à l'hôte donné risque d'échouer.

Aussi, les paramètres de serveur DNS sont importants pour l'authentification LDAP. Avec les paramètres DNS appropriés, EMX peut résoudre le nom du serveur LDAP en adresse IP afin d'établir une connexion. Si le *chiffrement SSL* est activé, les paramètres du serveur DNS deviennent critiques car seul le nom de domaine complet peut être utilisé pour indiquer le serveur LDAP.

Pour en savoir plus sur l'authentification LDAP, reportez-vous à ***Paramétrage de l'authentification LDAP*** (à la page 124).

Modification des paramètres des services réseau

EMX prend en charge ces services de communication réseau : HTTPS, HTTP, Telnet et SSH.

HTTPS et HTTP permettent l'accès à l'interface Web, et Telnet et SSH, à l'interface de ligne de commande.

Par défaut, SSH est activé, Telnet désactivé, et tous les ports TCP des services pris en charge sont définis sur ports standard. Au besoin, vous pouvez modifier les paramètres par défaut.

Remarque : l'accès Telnet est désactivé par défaut car la communication s'effectue en clair et n'est donc pas sécurisée.

En outre, EMX prend également en charge le protocole SNMP.

Modification des paramètres HTTP(S)

HTTPS constitue un protocole plus sûr que HTTP car il utilise la technologie SSL (Secure Sockets Layer) pour chiffrer tout le trafic vers et depuis le dispositif EMX.

Par défaut, l'accès à EMX via HTTP est automatiquement redirigé vers HTTPS. Reportez-vous à ***Chiffrement HTTPS imposé*** (à la page 102).

Pour modifier les paramètres de port HTTP ou HTTPS :

1. Sélectionnez Device Settings > Network Services > HTTP (Paramètres du dispositif > Services réseau > HTTP). La boîte de dialogue HTTP Settings (Paramètres HTTP) s'affiche.
2. Pour utiliser un port différent pour HTTP ou HTTPS, tapez un nouveau numéro de port dans le champ correspondant. La plage valide est comprise entre 1 et 65535.

   Avertissement : différents services réseau ne peuvent pas partager le même port TCP.
3. Cliquez sur OK pour enregistrer les modifications.

Configuration des paramètres SNMP

Vous pouvez activer ou désactiver la communication SNMP entre un gestionnaire SNMP et le dispositif EMX. L'activation de la communication SNMP permet au gestionnaire d'extraire le statut du dispositif EMX.

De plus, il vous faudra peut-être configurer les destinations SNMP si l'option intégrée System SNMP Trap Rule (Règle de traps SNMP système) est activée et que la destination de trap n'a pas encore été définie. Reportez-vous à ***Règles et actions d'événement*** (à la page 131).

Pour configurer la configuration SNMP :

1. Sélectionnez Device Settings > Network Services > SNMP (Paramètres du dispositif > Services réseau > SNMP). La boîte de dialogue SNMP Settings (Paramètres SNMP) s'affiche.
2. Entrez les données relatives aux destinations de traps s'appliquant à l'un des types de traps ou aux deux.
3. Recherchez le fichier MIB à télécharger et sélectionnez-le. Le fichier MIB SNMP de votre dispositif EMX est utilisé par le gestionnaire SNMP.
4. Cliquez sur OK.

Modification des paramètres SSH

Vous pouvez activer ou désactiver l'accès SSH à l'interface de ligne de commande, ou modifier le port TCP par défaut pour le service SSH. En outre, vous pouvez décider de vous connecter à l'aide du mot de passe ou de la clé publique via la connexion SSH.

Pour modifier les paramètres de service SSH :

1. Sélectionnez Device Settings > Network Services > SSH (Paramètres du dispositif > Services réseau > SSH). La boîte de dialogue SSH Settings (Paramètres SSH) s'affiche.
2. Pour utiliser un port différent, tapez un nouveau numéro de port dans le champ. La plage valide est comprise entre 1 et 65535.
3. Pour activer l'application SSH, cochez la case Enable SSH (Activer SSH). Pour la désactiver, décochez la case.
4. Pour sélectionner une méthode d'authentification différente, cochez une des cases.
   - Allow password authentication only (Autoriser l'authentification par mot de passe uniquement) : Active la connexion par mot de passe uniquement.

- Allow public key authentication only (Autoriser l'authentification par clé publique uniquement) : Active la connexion par clé publique uniquement.
- Allow password and public key authentication (Autoriser l'authentification par mot de passe et clé publique) : Active la connexion par mot de passe et par clé publique. Il s'agit de la valeur par défaut.

5. Cliquez sur OK pour enregistrer les modifications.

Si l'authentification par clé publique est sélectionnée, vous devez entrer une clé publique SSH valide pour établir une connexion SSH pour chaque profil utilisateur. Reportez-vous à ***Création d'un profil utilisateur*** (à la page 62).

Modification des paramètres Telnet

Vous pouvez activer ou désactiver l'accès Telnet à l'interface de ligne de commande, ou modifier le port TCP par défaut pour le service Telnet.

Pour modifier les paramètres de service Telnet :

1. Sélectionnez Device Settings > Network Services > Telnet (Paramètres du dispositif > Services réseau > Telnet). La boîte de dialogue Telnet Settings (Paramètres Telnet) s'affiche.
2. Pour utiliser un port différent, tapez un nouveau numéro de port dans le champ. La plage valide est comprise entre 1 et 65535.
3. Pour activer l'application Telnet, cochez la case Enable Telnet Access (Activer l'accès Telnet). Pour la désactiver, décochez la case.
4. Cliquez sur OK pour enregistrer les modifications.

Activation de la publication des services

EMX publie tous les services activés accessibles à l'aide du réseau IP. Cette fonctionnalité utilise DNS-SD (Domain Name System-Service Discovery, Système de noms de domaine-Détection de services) et mDNS (DNS multidiffusion). Les services publiés sont détectés par les clients ayant mis en œuvre DNS-SD et mDNS.

Les services publiés sont les suivants :

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

Cette fonctionnalité est activée par défaut.

Pour activer l'option Service Advertisement :

1. Cliquez sur Device Settings > Network Services > Service Advertisement (Paramètres du dispositif > Services réseau > Publication des services).
2. Cliquez sur Yes dans la boîte de dialogue de confirmation Changing Service Advertisement (Modification de la publication des services). Cette fonction est activée et la case Service Advertisement est cochée dans le menu.

Pour désactiver l'option Service Advertisement :

1. Cliquez sur Device Settings > Network Services > Service Advertisement (Paramètres du dispositif > Services réseau > Publication des services).
2. Cliquez sur No dans la boîte de dialogue de confirmation Changing Service Advertisement (Modification de la publication des services). Cette fonction est désactivée et la case Service Advertisement est décochée dans le menu.

Configuration des paramètres SMTP

Le dispositif EMX peut être configuré pour envoyer des alertes ou des messages d'événement par courriel à un administrateur spécifique. Pour ce faire, il vous faut configurer les paramètres SMTP et entrer une adresse IP pour votre serveur SMTP et l'adresse électronique de l'expéditeur.

Remarque : reportez-vous à **Configuration des règles d'événement** *(voir "***Règles et actions d'événement***" à la page 131) pour en savoir plus sur la création de règles d'événement pour l'envoi de notifications par courriel.*

Pour définir les paramètres de serveur SMTP :

1. Choisissez Device Settings > SMTP Server (Paramètres du dispositif > Serveur SMTP). La boîte de dialogue SNMP Server Settings (Paramètres du serveur SNMP) s'affiche.
2. Tapez le nom ou l'adresse IP du serveur de messagerie dans le champ Server Name (Nom du serveur).
3. Tapez le numéro du port du serveur SMTP dans le champ Port. La valeur par défaut est 25.
4. Renseignez le champ Sender Email Address (Adresse électronique de l'expéditeur).
5. Tapez le nombre de tentatives d'envoi de courriels dans le champ Number of Sending Retries (Nombre de tentatives d'envoi). La valeur par défaut est 2 tentatives.
6. Tapez l'intervalle entre les tentatives d'envoi dans le champ Time Interval Between Sending Retries (in minutes) (Intervalle entre les tentatives d'envoi (en minutes)). L'intervalle est mesuré en minutes. La valeur par défaut est 2 minutes.
7. Si votre serveur SMTP requiert l'authentification par mot de passe, procédez comme suit :
   a. Cochez la case Server Requires Authentication (Serveur requiert l'authentification).
   b. Tapez un nom d'utilisateur dans le champ User Name.
   c. Tapez un mot de passe dans le champ Password.
8. Maintenant que vous avez défini les paramètres SMTP, vous pouvez effectuer un test pour vous assurer que tout fonctionne correctement. Procédez comme suit :
   a. Tapez l'adresse électronique du destinataire dans le champ Recipient Email Addresses. Utilisez une virgule pour séparer ces adresses.
   b. Cliquez sur Send Test Email (Envoyer un courriel de test).

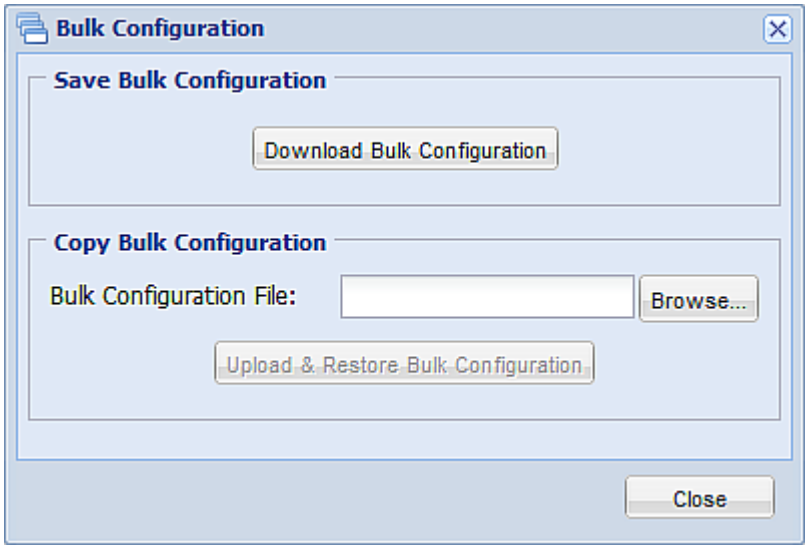
9. Cliquez sur OK pour enregistrer les modifications.
10. Vérifiez que les destinataires ont bien reçu le courriel.

Paramétrage d'un dispositif EMX à l'aide de la configuration en bloc

Utilisez cette fonction si vous avez déjà défini un dispositif EMX et en paramétrez un autre. La fonction Bulk Configuration (Configuration en bloc) vous permet d'enregistrer sur votre PC les paramètres d'un dispositif EMX configuré. Vous pouvez utiliser ce fichier de configuration pour :

- copier cette configuration sur d'autres dispositifs EMX des mêmes modèle et version de firmware ;
- rétablir les paramètres du même dispositif EMX à la configuration précédente.

Vous devez disposer des privilèges d'administrateur pour enregistrer et copier les configurations EMX.



Enregistrement d'une configuration EMX

Un dispositif source est un dispositif EMX déjà configuré qui est utilisé pour créer un fichier de configuration contenant les paramètres pouvant être partagés entre dispositifs EMX. Ces paramètres comprennent les configurations d'utilisateur et de rôle, les règles d'événement, les paramètres de sécurité, etc.

Ce fichier NE CONTIENT PAS d'informations spécifiques au dispositif, comme :

- Nom du dispositif
- Paramètres réseau (adresse IP, passerelle, masque réseau, etc.)
- Journaux des dispositifs
- Noms des capteurs d'environnement
- Etats et valeurs des capteurs d'environnement
- Certificat SSL
- Noms des capteurs de gestion des ressources et des unités de rack
- Nom, emplacement et contact SNMP
- Entrées d'écrans de serveur

Comme les paramètres de date et d'heure sont enregistrés dans le fichier de configuration, les utilisateurs doivent faire attention lorsqu'ils distribuent ce fichier aux dispositifs EMX opérant dans un fuseau horaire différent de celui du dispositif source.

Pour enregistrer un fichier de configuration :

1. Choisissez Maintenance > Bulk Configuration (Configuration en bloc). La boîte de dialogue Bulk Configuration apparaît.
2. Cliquez sur Download Bulk Configuration (Télécharger la configuration en bloc).
3. Lorsque le navigateur Web vous invite à ouvrir ou à enregistrer le fichier de configuration, cliquez sur Save (Enregistrer). Choisissez un emplacement approprié et enregistrez le fichier de configuration sur votre PC.

Le fichier est enregistré au format XML et son contenu est chiffré à l'aide de l'algorithme de chiffrement AES-128.

Copie d'une configuration EMX

Un dispositif cible est un dispositif EMX qui charge le fichier de configuration d'un autre dispositif EMX.

La copie de la configuration d'un EMX à un dispositif cible ajuste les paramètres de ce dernier pour qu'ils correspondent à ceux du dispositif EMX source. Pour copier la configuration d'un dispositif EMX :

- L'utilisateur doit être l'utilisateur Admin. Ou le rôle Admin est affecté à l'utilisateur.
- Le dispositif EMX cible doit être du même type de modèle que le dispositif EMX source.
- Le dispositif EMX cible doit exécuter la même version de firmware que le dispositif EMX source.

Pour copier une configuration EMX :

1. Connectez-vous à l'interface Web du dispositif cible.
2. Si la version du firmware du dispositif cible est différente de celle du dispositif source, mettez à jour le firmware de la cible. Reportez-vous à ***Mise à niveau du firmware*** (à la page 94).
3. Choisissez Maintenance > Bulk Configuration (Configuration en bloc). La boîte de dialogue Bulk Configuration apparaît.
4. Dans la section Copy Bulk Configuration (Copier la configuration en bloc), cliquez sur Browse (Parcourir) et sélectionnez le fichier de configuration stocké sur votre PC.
5. Cliquez sur Upload & Restore Bulk Configuration (Téléverser & Restaurer la configuration en bloc) pour copier le fichier.
6. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer l'opération.
7. Attendez que le dispositif EMX se réinitialise et que la page Login (Connexion) réapparaisse, indiquant que la configuration est copiée.

Mise à niveau du firmware

Vous pouvez mettre à niveau le dispositif EMX pour bénéficier des dernières améliorations et fonctions.

Les fichiers de firmware de EMX sont disponibles dans la section ***Firmware and Documentation*** (***http://www.raritan.com/support/firmware-and-documentation/***) du site Web de Raritan.

Mise à jour du firmware

Vous devez être l'administrateur système ou vous connecter au profil utilisateur doté de l'autorisation Firmware Update (Mise à jour du firmware) pour mettre à jour le firmware du dispositif EMX.

Selon votre modèle, téléchargez le dernier fichier de firmware du site Web de Raritan, lisez les notes de version, puis commencez la mise à niveau. Si vous avez des questions ou des inquiétudes concernant cette opération, contactez le support technique Raritan AVANT la mise à niveau.

Avertissement : N'EFFECTUEZ PAS la mise à niveau du firmware via une connexion sans fil.

Pour mettre à jour le firmware :

1. Choisissez Maintenance > Update Firmware (Maintenance > Mettre à jour le firmware). La boîte de dialogue Firmware Update (Mise à jour du firmware) apparaît.
2. Dans le champ Firmware File (Fichier de firmware), cliquez sur Browse (Parcourir) pour sélectionner un fichier de firmware approprié.
3. Cliquez sur Upload (Téléverser). Une barre de progression apparaît pour indiquer le statut du téléversement.
4. Lorsque le téléversement est terminé, les informations de version du firmware existant et du firmware téléversé sont affichées, vous offrant une dernière possibilité d'abandonner la mise à jour.
5. Pour afficher le certificat du firmware téléversé, cliquez sur View Certificate. **Facultatif.**
6. Pour continuer la mise à jour, cliquez sur Update Firmware (Mettre à jour le firmware). La mise à jour peut prendre plusieurs minutes.

   Avertissement : NE METTEZ PAS le dispositif EMX hors tension pendant la mise à jour.

   Au cours de la mise à jour du firmware :

   - Une barre de progression indiquant le statut de la mise à jour apparaît dans l'interface Web.
   - Aucun utilisateur ne peut se connecter à EMX.
   - Dans l'interface Web, tous les utilisateurs connectés voient le message de déconnexion automatique de EMX et l'état disconnected (déconnecté) apparaît dans la barre de statut.
   - L'opération de gestion des utilisateurs, le cas échéant, est forcée de s'interrompre.

7. Lorsque la mise à jour est terminée, un message apparaît, indiquant que la mise à jour a abouti.
8. Le dispositif EMX est réinitialisé et la page de connexion réapparaît. Vous pouvez maintenant vous connecter et reprendre votre opération.

Remarque 1 : la session des autres utilisateurs connectés est également interrompue lorsque la mise à jour du firmware est terminée.

Remarque 2 : si vous utilisez EMX avec un gestionnaire SNMP, il est recommandé de télécharger à nouveau le fichier MIB EMX après la mise à jour du firmware. Ainsi, votre gestionnaire SNMP dispose du fichier MIB correspondant à la version la plus récente que vous utilisez. Reportez-vous à **Utilisation de SNMP** *(à la page 205).*

Affichage de l'historique de la mise à jour du firmware

L'historique de la mise à niveau du firmware, le cas échéant, est stocké de manière permanente sur le dispositif EMX.

Cet historique indique quand l'événement de mise à niveau du firmware a eu lieu, les versions précédente et nouvelle associées à l'événement et le résultat de la mise à niveau.

Pour afficher l'historique de la mise à jour du firmware :

1. Choisissez Maintenance > View Firmware Update History (Historique de la mise à jour du firmware). La boîte de dialogue Firmware Update History (Historique de la mise à jour du firmware) apparaît et affiche les données suivantes :
   - la date et l'heure de l'événement de mise à niveau du firmware ;
   - la version précédente du firmware ;
   - la version de mise à jour du firmware ;
   - le résultat de la mise à niveau du firmware.
2. Vous pouvez modifier le nombre de colonnes affichées ou l'ordre de tri de la liste pour améliorer l'affichage des données. Reportez-vous à Modification de la vue d'une liste.
3. Pour afficher les détails d'un événement de mise à niveau du firmware, sélectionnez-le et cliquez sur Details, ou double-cliquez simplement sur l'événement. La boîte de dialogue Firmware Update Details (Détails de la mise à jour du firmware) qui apparaît présente des données détaillées sur l'événement sélectionné.
4. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Reprise totale après sinistre

Si la mise à niveau du firmware échoue et qu'à cause de cet échec, le dispositif EMX cesse de fonctionner, vous pouvez le récupérer à l'aide d'un utilitaire spécial au lieu de retourner le dispositif à Raritan.

Contactez le support technique de Raritan pour obtenir l'utilitaire de reprise, qui fonctionne sous Windows XP/Vista/7 et Linux. De plus, un fichier de firmware EMX est requis dans la procédure de reprise.

Mise à jour du firmware du capteur de ressources

Une fois le capteur de ressources connecté au dispositif EMX, ce dernier compare automatiquement la version de son propre firmware à celle du firmware de capteur stocké dans son firmware. Si deux versions sont différentes, le capteur de ressources télécharge automatiquement le nouveau firmware du dispositif EMX afin de mettre à niveau le sien.

Au cours de la mise à niveau du firmware, les événements suivants se produisent :

- Le capteur de ressources est entièrement allumé et les voyants clignotants passent du rouge au vert.
- Un processus de mise à niveau du firmware est indiqué dans l'interface Web de EMX.
- Un trap SNMP est envoyé pour indiquer l'événement de mise à niveau du firmware.

Diagnostics du réseau

L'interface Web de EMX offre les outils suivants pour le diagnostic de problèmes de réseau éventuels.

- Ping
- Trace Route (Traçage de route)
- List TCP Connections (Liste des connexions TCP)

Conseil : ces outils de diagnostic du réseau sont également disponibles via l'interface CLI. Reportez-vous à **Dépannage du réseau** *(à la page 319).*

Test ping d'un hôte

L'outil Ping est utile pour vérifier si un hôte est accessible via le réseau ou Internet.

Pour effectuer le test ping d'un hôte :

1. Choisissez Maintenance > Network Diagnostics (Diagnostics du réseau) > Ping. La boîte de dialogue Ping Network Host (Test ping de l'hôte du réseau) apparaît.
2. Dans le champ Host Name, tapez le nom ou l'adresse IP de l'hôte à vérifier.
3. Dans le champ Number of Requests (Nombre de requêtes), tapez un nombre inférieur ou égal à 10 ou cliquez sur l'une des flèches pour ajuster la valeur. Ce nombre détermine la quantité de paquets envoyés pour le test ping de l'hôte.
4. Cliquez sur Run Ping (Exécuter le test ping) pour lancer le test ping de l'hôte. La boîte de dialogue qui apparaît affiche les résultats du test ping.
5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Traçage de la route du réseau

Trace Route vous permet de découvrir la route via le réseau entre deux hôtes ou systèmes.

Pour tracer la route d'un hôte :

1. Choisissez Maintenance > Network Diagnostics > Trace Route (Maintenance > Diagnostics du réseau > Traçage de la route). La boîte de dialogue Trace Route to Host (Tracer la route jusqu'à l'hôte) apparaît.
2. Dans le champ Host Name, tapez l'adresse IP ou le nom de l'hôte dont vous souhaitez vérifier la route.
3. Cliquez sur Run (Exécuter). La boîte de dialogue qui apparaît affiche les résultats du traçage de la route.
4. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Liste des connexions TCP

Vous pouvez utiliser List TCP Connections pour afficher la liste des connexions TCP.

Pour tracer la route d'un hôte :

1. Choisissez Maintenance > Network Diagnostics > List TCP Connections (Maintenance > Diagnostics du réseau > Liste des connexion TCP). La boîte de dialogue des connexions TCP apparaît.
2. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Téléchargement des données de diagnostic

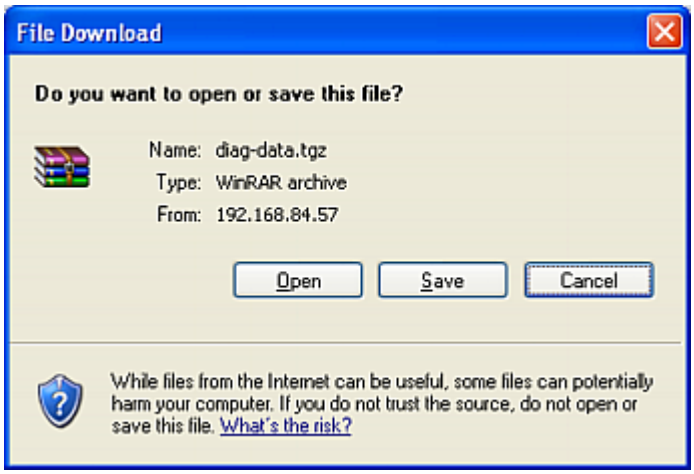
Important : Cette fonction est destinée à l'usage des inspecteurs de maintenance Raritan ou du client si le support technique Raritan le lui demande.

Vous pouvez télécharger le fichier de diagnostic du dispositif EMX à une machine cliente. Le fichier est compressé en fichier .tgz et doit être envoyé au support technique Raritan pour être interprété.

Cette fonction est accessible uniquement aux utilisateurs disposant de privilèges d'administration.

Pour extraire un fichier de diagnostic :

1. Sélectionnez Maintenance > Download Diagnostic Information (Télécharger les données de diagnostic). La boîte de dialogue File Download (Téléchargement de fichier) apparaît.



2. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) apparaît.
3. Accédez au répertoire désiré et cliquez sur Save (Enregistrer).

4. Envoyez ce fichier par courriel selon les instructions du support technique Raritan.

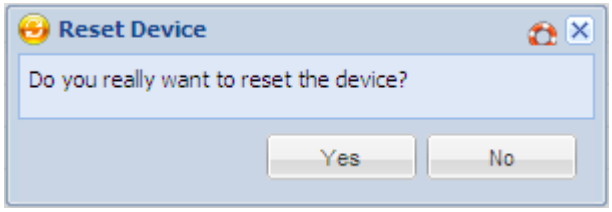
Redémarrage du dispositif EMX

Vous pouvez redémarrer le dispositif EMX à distance via l'interface Web. Cette opération ne réinitialise pas la configuration du dispositif comme pendant la réinitialisation aux valeurs par défaut usine.

Remarque : le redémarrage du dispositif EMX efface les instantanés pris par une webcam.

Pour redémarrer le dispositif :

1. Choisissez Maintenance > Unit Reset (Maintenance > Réinitialisation de l'unité). La boîte de dialogue Reset Device (Réinitialiser le dispositif) s'affiche.



2. Cliquez sur Yes (Oui) pour réinitialiser EMX.
3. Un message apparaît avec un indicateur effectuant le compte à rebours du temps restant pour l'opération. Elle dure environ une minute.
4. Une fois la réinitialisation terminée, la page Login (Connexion) s'ouvre. Vous pouvez à présent vous reconnecter au dispositif EMX.

Remarque : si vous n'êtes pas redirigé vers la page de connexion à la fin de la réinitialisation, cliquez sur le texte souligné this link (ce lien) dans le message.

Réinitialisation aux valeurs par défaut usine

Pour des raisons de sécurité, le dispositif EMX ne peut être réinitialisé aux valeurs par défaut usine que depuis la console locale.

Important : la réinitialisation aux valeurs par défaut usine d'un dispositif EMX doit être effectuée avec précaution. Cette opération efface toutes les données existantes et les paramètres personnalisés, tels que les profils utilisateur, les valeurs de seuil, etc.

Vous pouvez utiliser le bouton de réinitialisation ou l'interface de ligne de commande (CLI) pour réinitialiser EMX.

Pour rétablir les valeurs par défaut usine à l'aide du bouton Reset :

1. Connectez un ordinateur au dispositif EMX. Reportez-vous à ***Connexion du dispositif EMX à un ordinateur*** (à la page 12).
2. Lancez un programme d'émulation de terminal, tel qu'HyperTerminal, Kermit ou PuTTY, puis ouvrez une fenêtre sur EMX.
3. Enfoncez (et relâchez) le bouton Reset (Réinitialiser) du dispositif EMX tout en appuyant plusieurs fois rapidement sur la touche Echap du clavier. Une invite (=>) doit apparaître après environ une seconde.
4. Entrez *defaults* pour rétablir les valeurs par défaut usine du dispositif EMX.
5. Patientez jusqu'à l'apparition de l'invite Username (Nom d'utilisateur) indiquant que la réinitialisation est terminée.

Remarque : HyperTerminal est disponible dans les systèmes d'exploitation Windows avant Windows Vista. Pour Windows Vista ou les versions ultérieures, utilisez PuTTY, programme gratuit téléchargeable depuis Internet. Reportez-vous à la documentation de PuTTY pour en savoir plus sur la configuration.

Chapitre 6 Security (Sécurité)

Dans ce chapitre

Contrôle de sécurité d'accès

EMX fournit des outils pour contrôler l'accès. Vous pouvez exiger le chiffrement HTTPS, activer le pare-feu interne et créer des règles le concernant, et limiter le nombre de connexions.

Conseil : vous pouvez également créer et installer le certificat, ou paramétrer des serveurs d'authentification externes pour contrôler n'importe quel accès. Reportez-vous à **Configuration d'un certificat SSL** *(à la page 118) et* **Paramétrage de l'authentification LDAP** *(à la page 124).*

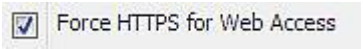
Chiffrement HTTPS imposé

HTTPS constitue un protocole plus sûr que HTTP car il utilise la technologie SSL (Secure Sockets Layer) pour chiffrer tout le trafic vers et depuis le dispositif EMX.

Vous pouvez obliger les utilisateurs à accéder à l'interface Web EMX par l'intermédiaire du protocole HTTPS uniquement. Par défaut, ce protocole est activé.

Pour forcer l'accès HTTPS à l'interface Web :

1. Choisissez Device Settings > Security > Force HTTPS for Web Access (Paramètres du dispositif > Sécurité > Forcer HTTPS pour l'accès Web).
2. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes pour exécuter le service HTTPS.
3. Choisissez Device Settings > Security (Paramètres du dispositif > Sécurité) pour vérifier que la case Force HTTPS for Web Access (Forcer HTTPS pour l'accès Web) est cochée comme illustré dans le schéma.



Si la case n'est pas cochée, répétez ces étapes.

Après l'activation du protocole HTTPS, toutes les tentatives d'accès à l'aide d'HTTP sont redirigées automatiquement vers HTTPS.

Configuration du pare-feu

Le dispositif EMX est doté d'un pare-feu configurable pour interdire son accès à des adresses IP et à des plages d'adresses IP spécifiques. Par défaut, le pare-feu est désactivé.

Pour configurer le pare-feu :

1. Activez le pare-feu. Reportez-vous à ***Activation du pare-feu*** (à la page 103).
2. Définissez la stratégie par défaut. Reportez-vous à ***Modification de la stratégie par défaut*** (à la page 104).
3. Créez des règles de pare-feu indiquant les adresses à accepter et à refuser. Reportez-vous à ***Création des règles de pare-feu*** (à la page 105).

Les modifications apportées aux règles du pare-feu prennent immédiatement effet. Les activités IP non autorisées cessent instantanément.

Remarque : la désactivation du pare-feu par défaut a pour but d'empêcher les utilisateurs de bloquer accidentellement leur accès au dispositif.

Activation du pare-feu

Les règles de pare-feu éventuelles ne prennent effet qu'après l'activation du pare-feu.

Pour activer le pare-feu du dispositif EMX :

1. Choisissez Device Settings > Security > IP Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès par IP). La boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) apparaît.
2. Pour activer le pare-feu IPv4, cliquez sur l'onglet IPv4 et cochez la case Enable IPv4 Access Control (Activer le contrôle d'accès IPv4).
3. Pour activer le pare-feu IPv6, cliquez sur l'onglet IPv6 et cochez la case Enable IPv6 Access Control (Activer le contrôle d'accès IPv6).
4. Cliquez sur OK pour enregistrer les modifications.

Modification de la stratégie par défaut

Après l'activation du pare-feu, la stratégie par défaut consiste à accepter le trafic de toutes les adresses IP. Ceci signifie que seules les adresses IP rejetées par une règle spécifique NE SERONT PAS autorisées à accéder à EMX.

Vous pouvez remplacer la stratégie par défaut par Drop (Refuser) ou Reject (Rejeter) ; le trafic de toutes les adresses IP est alors annulé, hormis les adresses IP acceptées par une règle spécifique.

Pour modifier la stratégie par défaut :

1. Choisissez Device Settings > Security > IP Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès par IP). La boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) apparaît.
2. Pour déterminer la stratégie par défaut pour les adresses IPv4 :
   a. Le cas échéant, cliquez sur l'onglet IPv4.
   b. Assurez-vous que la case Enable IPv4 Access Control (Activer le contrôle d'accès IPv4) est cochée.
   c. La stratégie par défaut apparaît dans le champ Default Policy. Pour la modifier, sélectionnez une stratégie différente dans la liste déroulante.
      - Accept : accepte le trafic de toutes les adresses IPv4.
      - Drop : refuse le trafic de toutes les adresses IPv4 sans envoyer de notification d'échec à l'hôte source.
      - Reject : refuse le trafic de toutes les adresses IPv4 et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec.
3. Pour déterminer la stratégie par défaut pour les adresses IPv6 :
   a. Cliquez sur l'onglet IPv6.
   b. Assurez-vous que la case Enable IPv6 Access Control (Activer le contrôle d'accès IPv6) est cochée.
   c. La stratégie par défaut apparaît dans le champ Default Policy. Pour la modifier, sélectionnez une stratégie différente dans la liste déroulante.

- Accept : accepte le trafic de toutes les adresses IPv6.
- Drop : refuse le trafic de toutes les adresses IPv6 sans envoyer de notification d'échec à l'hôte source.
- Reject : refuse le trafic de toutes les adresses IPv6 et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec.

4. Cliquez sur OK pour enregistrer les modifications. La nouvelle stratégie par défaut est appliquée.

Création des règles de pare-feu

Les règles du pare-feu déterminent si le trafic destiné à EMX doit être accepté ou refusé, en fonction de l'adresse IP de l'hôte émetteur. Lors de la création des règles du pare-feu, gardez les principes suivants à l'esprit :

- **L'ordre des règles est important.**

  Lorsque le trafic parvient au dispositif EMX, les règles sont exécutées dans l'ordre numérique. Seule la première règle correspondant à l'adresse IP détermine si le trafic est accepté ou refusé. Les règles suivantes correspondant à l'adresse IP sont ignorées par EMX.

- **Subnet mask may be required. (Un masque de sous-réseau peut être requis.)**

  Lors de la saisie de l'adresse IP, vous devez ou non indiquer l'adresse ET un masque de sous-réseau. Le masque de sous-réseau par défaut est /32 (c'est-à-dire, 255.255.255.255). Vous devez indiquer un masque de sous-réseau uniquement lorsqu'il est différent de la valeur par défaut. Par exemple, pour indiquer une adresse unique dans un réseau de classe C, utilisez le format suivant :

  x.x.x.x/24

  où */24* = un masque de sous-réseau de 255.255.255.0.

  Pour indiquer un sous-réseau entier ou une plage d'adresses, modifiez le masque de sous-réseau en conséquence.

Remarque : les adresses IP valides sont comprises entre 0.0.0.0 et 255.255.255.255. Assurez-vous que les adresses IP saisies figurent dans cette plage.

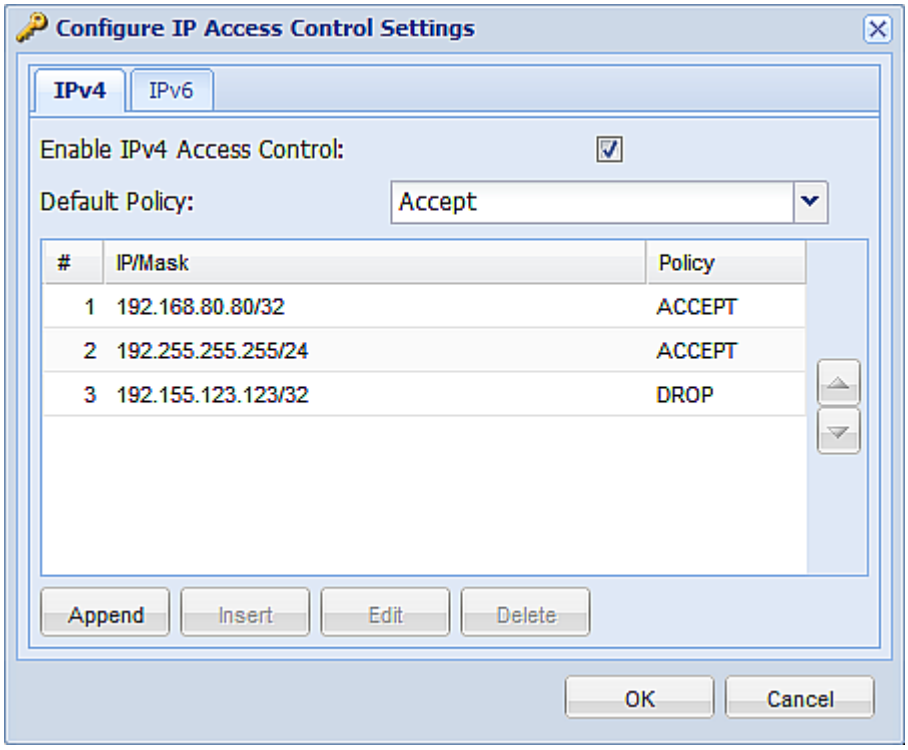
Pour créer des règles de pare-feu :

1. Choisissez Device Settings > Security > IP Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès par IP). La boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) apparaît.
2. Cliquez sur l'onglet IPv4 pour créer des règles de pare-feu, ou sur l'onglet IPv6 pour créer des règles de pare-feu IPv6.

3. Assurez-vous que la case Enable IPv4 Access Control (Activer le contrôle d'accès IPv4) ou Enable IPv6 Access Control (Activer le contrôle d'accès IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Créez des règles spécifiques. Reportez-vous au tableau pour différentes opérations.

Action	Procédure
Ajouter une règle à la fin de la liste des règles	▪ Cliquez sur Append (Ajouter). La boîte de dialogue Append new Rule (Ajouter la nouvelle règle) apparaît. ▪ Entrez une adresse IP et un masque de sous-réseau dans le champ IP/Mask (IP/Masque). ▪ Sélectionnez Accept (Accepter), Drop (Refuser) ou Reject (Rejeter) dans la liste déroulante du champ Policy (Stratégie). ▪ Accept : Accepte le trafic des adresses IP indiquées. ▪ Drop : Refuse le trafic des adresses IP indiquées, sans envoyer de notification d'échec à l'hôte source. ▪ Reject : Refuse le trafic des adresses IP indiquées et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec. ▪ Cliquez sur OK pour enregistrer les modifications. Le système numérote automatiquement la règle.
Insérer une règle entre deux autres	▪ Sélectionnez la règle au-dessus de laquelle vous souhaitez insérer une nouvelle règle. Par exemple, pour insérer une règle entre les règles 3 et 4, entrez 4. ▪ Cliquez sur Insert (Insérer). La boîte de dialogue Insert new Rule (Insérer la nouvelle règle) apparaît. ▪ Entrez une adresse IP et un masque de sous-réseau dans le champ IP/Mask (IP/Masque). ▪ Sélectionnez Accept (Accepter), Drop (Refuser) ou Reject (Rejeter) dans la liste déroulante du champ Policy (Stratégie). ▪ Accept : Accepte le trafic des adresses IP indiquées. ▪ Drop : Refuse le trafic des adresses IP indiquées, sans envoyer de notification d'échec à l'hôte source. ▪ Reject : Refuse le trafic des adresses IP indiquées et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec. ▪ Cliquez sur OK pour enregistrer les modifications. Le système insère la règle et renumérote automatiquement les règles suivantes.

5. Lorsque vous avez terminé, les règles apparaissent dans la boîte de dialogue Configure IP Access Control (Configurer le contrôle d'accès par IP).



6. Cliquez sur OK pour enregistrer les modifications. Les règles sont appliquées.

Modification des règles de pare-feu

Lorsqu'une règle de pare-feu existante nécessite la mise à jour des fourchettes d'adresses IP et/ou de stratégie, modifiez-les en conséquence.

Pour modifier une règle de pare-feu :

1. Choisissez Device Settings > Security > IP Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès par IP). La boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) apparaît.
2. Pour modifier les règles de pare-feu IPv4, cliquez sur l'onglet IPv4. Pour modifier les règles de pare-feu IPv6, cliquez sur l'onglet IPv6.
3. Assurez-vous que la case Enable IPv4 Access Control (Activer le contrôle d'accès IPv4) ou Enable IPv6 Access Control (Activer le contrôle d'accès IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.

4. Dans la liste de règles, sélectionnez la règle à modifier.
5. Cliquez sur Edit (Modifier) ou double-cliquez sur la règle. La fenêtre Edit Rule (Modifier la règle) s'affiche.
6. Modifiez les informations affichées.
7. Cliquez sur OK pour enregistrer les modifications.
8. Cliquez sur OK pour quitter la boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) sinon les modifications seront perdues.

Tri des règles de pare-feu

L'ordre des règles détermine celle des règles correspondant à une même adresse IP qui sera exécutée.

Pour trier les règles de pare-feu :

1. Choisissez Device Settings > Security > IP Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès par IP). La boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) apparaît.
2. Pour trier les règles de pare-feu IPv4, cliquez sur l'onglet IPv4. Pour trier les règles de pare-feu IPv6, cliquez sur l'onglet IPv6.
3. Assurez-vous que la case Enable IPv4 Access Control (Activer le contrôle d'accès IPv4) ou Enable IPv6 Access Control (Activer le contrôle d'accès IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Sélectionnez une règle particulière en cliquant dessus.
5. Cliquez sur  ou sur  pour faire monter ou descendre la règle sélectionnée jusqu'à ce qu'elle atteigne l'emplacement souhaité.
6. Cliquez sur OK pour enregistrer les modifications.

Suppression des règles de pare-feu

Lorsque des règles de pare-feu deviennent obsolètes ou inutiles, supprimez-les de la liste des règles.

Pour supprimer une règle de pare-feu :

1. Choisissez Device Settings > Security > IP Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès par IP). La boîte de dialogue Configure IP Access Control Settings (Configurer les paramètres de contrôle d'accès par IP) apparaît.
2. Pour supprimer les règles de pare-feu IPv4, cliquez sur l'onglet IPv4. Pour supprimer les règles de pare-feu IPv6, cliquez sur l'onglet IPv6.

3. Assurez-vous que la case Enable IPv4 Access Control (Activer le contrôle d'accès IPv4) ou Enable IPv6 Access Control (Activer le contrôle d'accès IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Sélectionnez la règle que vous souhaitez supprimer. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
5. Cliquez sur Delete (Supprimer).
6. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes pour retirer les règles sélectionnées de la liste.
7. Cliquez sur OK pour enregistrer les modifications.

Paramétrage des contrôles de connexion des utilisateurs

Vous pouvez paramétrer des contrôles de connexion pour empêcher les pirates d'accéder à EMX et aux dispositifs branchés dessus. Vous pouvez choisir de bloquer des individus après un nombre spécifique d'échecs de connexion, limiter le nombre d'utilisateurs connectés simultanément à l'aide du même nom d'utilisateur et obliger les utilisateurs à créer des mots de passe forts.

Activation du blocage des utilisateurs

Le blocage des utilisateurs détermine le nombre de fois où un utilisateur peut tenter de se connecter à EMX et où l'authentification peut échouer avant que l'utilisateur ne soit bloqué.

Notez que cette fonction s'applique uniquement à l'authentification locale plutôt qu'à l'authentification via des serveurs AA externes.

Remarque : si un événement de blocage se produit, vous pouvez débloquer manuellement l'utilisateur concerné en utilisant la commande CLI unblock via une connexion série. Reportez-vous à **Déblocage d'un utilisateur** *(à la page 317).*

Pour activer le blocage des utilisateurs :

1. Choisissez Device Settings > Security > Login Settings (Paramètres du dispositif > Sécurité > Paramètres de connexion). La boîte de dialogue Login Settings s'affiche.
2. Accédez à la section User Blocking (Blocage des utilisateurs).
3. Pour activer la fonction de blocage des utilisateurs, cochez la case Block user on login failure (Bloquer l'utilisateur en cas d'échec de connexion).
4. Entrez un nombre dans le champ Maximum number of failed logins (Nombre maximum d'échecs de connexion). Il s'agit du nombre maximum d'échecs de connexion autorisé à l'utilisateur avant que l'accès à EMX ne soit bloqué à ses données de connexion.

5. Pour déterminer la durée de blocage de la connexion, sélectionnez la durée souhaitée dans la liste déroulante du champ Block timeout (Délai de blocage). Les options disponibles sont décrites ci-après.
   - Infinite : cette option n'impose aucune limite de temps au blocage de la connexion.
   - X min : ce type d'option fixe le délai à X minutes, où X est un nombre.
   - X h : ce type d'option fixe le délai à X heures, où X est un nombre.
   - 1 d : cette option fixe le délai à 1 jour.

   Conseil : si l'option de durée souhaitée ne figure pas dans la liste, vous pouvez la taper dans ce champ. Par exemple, vous pouvez taper 4 min pour définir la durée sur 4 minutes.

6. Cliquez sur OK pour enregistrer les modifications.

Activation des limites de connexion

Les limites de connexion déterminent si plusieurs personnes peuvent utiliser simultanément le même nom de connexion et combien de temps les utilisateurs sont autorisés à rester inactifs avant d'être déconnectés de force.

Pour activer les limites de connexion :

1. Choisissez Device Settings > Security > Login Settings (Paramètres du dispositif > Sécurité > Paramètres de connexion). La boîte de dialogue Login Settings s'affiche.
2. Accédez à la section Login Limitations (Limites de connexion).
3. Pour empêcher à plusieurs personnes d'utiliser les mêmes données de connexion simultanément, cochez la case Prevent concurrent login with same username (Empêcher la connexion simultanée avec le même nom d'utilisateur).
4. Pour ajuster le délai pendant lequel les utilisateurs peuvent rester inactifs avant d'être déconnectés de force par EMX, sélectionnez une option dans le champ Idle Timeout Period (Période d'inactivité). La valeur par défaut est 10 minutes.
   - X min : ce type d'option fixe le délai à X minutes, où X est un nombre.
   - X h : ce type d'option fixe le délai à X heures, où X est un nombre.
   - 1 d : cette option fixe le délai à 1 jour.

Conseil : si l'option de durée souhaitée ne figure pas dans la liste, vous pouvez la taper dans ce champ. Par exemple, vous pouvez taper 4 min pour définir la durée sur 4 minutes.

5. Cliquez sur OK pour enregistrer les modifications.

Conseil : gardez le délai d'inactivité à 20 minutes ou moins si possible. Ceci réduit le nombre de sessions connectées inactives et le nombre de commandes simultanées envoyées à EMX.

Activation des mots de passe forts

L'utilisation de mots de passe forts empêche aux intrus de découvrir les mots de passe des utilisateurs et d'accéder au dispositif EMX. Par défaut, les mots de passe forts doivent comporter au moins huit caractères, contenir des lettres majuscules et minuscules, des chiffres et des caractères spéciaux (tels que @ ou &).

Pour obliger les utilisateurs à créer des mots de passe forts :

1. Choisissez Device Settings > Security > Password Policy (Paramètres du dispositif > Sécurité > Stratégie en matière de mot de passe). La boîte de dialogue Password Policy s'affiche.
2. Cochez la case Strong Passwords (Mots de passe forts) pour activer la fonction de mots de passe forts. Les paramètres par défaut sont les suivants :

Longueur minimum	= 8 caractères
Longueur maximum	= 32 caractères
Au moins un caractère en minuscule	= Obligatoire
Au moins un caractère en majuscules	= Obligatoire
Au moins un caractère numérique	= Obligatoire
Au moins un caractère spécial	= Obligatoire
Nombre de mots de passe interdits dans l'historique	= 5

Remarque : la longueur maximum de mot de passe acceptée par EMX est de 32 caractères.

3. Apportez les modifications nécessaires aux paramètres par défaut.
4. Cliquez sur OK pour enregistrer les modifications.

Activation du vieillissement des mots de passe

Le vieillissement des mots de passe indique si les utilisateurs doivent obligatoirement modifier leur mot de passe à intervalles réguliers. L'intervalle par défaut est de 60 jours.

Pour forcer les utilisateurs à changer régulièrement de mot de passe :

1. Choisissez Device Settings > Security > Password Policy (Paramètres du dispositif > Sécurité > Stratégie en matière de mot de passe). La boîte de dialogue Password Policy s'affiche.
2. Cochez la case Password Aging (Vieillissement des mots de passe) pour activer la fonction correspondante.
3. Pour indiquer à quelle fréquence les utilisateurs doivent changer de mot de passe, sélectionnez un nombre de jours dans le champ Password Aging Interval (Intervalle de vieillissement des mots de passe). Les utilisateurs doivent modifier leur mot de passe chaque fois que le nombre de jours est écoulé.

   Conseil : si l'option de durée souhaitée ne figure pas dans la liste, vous pouvez la taper dans ce champ. Par exemple, vous pouvez taper 9 d pour définir le délai de vieillissement des mots de passe sur 9 jours.

4. Cliquez sur OK pour enregistrer les modifications.

Paramétrage des règles de contrôle d'accès basé rôle

Les règles de contrôle d'accès basé rôle sont similaires aux règles de pare-feu, hormis le fait qu'elles sont applicables aux membres partageant un rôle particulier. Ceci vous permet d'accorder des autorisations système à un rôle précis, suivant l'adresse IP.

Pour paramétrer des règles de contrôle d'accès basé rôle :

1. Activez la fonction. Reportez-vous à ***Activation de la fonction*** (à la page 113).
2. Définissez la stratégie par défaut. Reportez-vous à ***Modification de la stratégie par défaut*** (à la page 113).
3. Créez des règles spécifiant les adresses à accepter et celles à rejeter lorsqu'elles sont associées à un rôle spécifique. Reportez-vous à ***Création des règles de contrôle d'accès basé rôle*** (voir "***Création de règles de contrôle d'accès basé rôle***" à la page 114).

Les modifications apportées n'affectent les utilisateurs actuellement connectés qu'à l'ouverture de session suivante.

Activation de la fonction

Vous devez activer cette fonction de contrôle d'accès pour permettre l'entrée en vigueur des règles pertinentes.

Pour activer les règles de contrôle d'accès basé rôle :

1. Choisissez Device Settings > Security > Role Based Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès basé rôle). La boîte de dialogue Configure Role Based Access Control Settings (Configurer les paramètres de contrôle d'accès basé rôle) apparaît.
2. Pour activer le pare-feu IPv4, cliquez sur l'onglet IPv4 et cochez la case Enable Role Based Access Control for IPv4 (Activer le contrôle d'accès basé rôle pour IPv4).
3. Pour activer le pare-feu IPv6, cliquez sur l'onglet IPv6 et cochez la case Enable Role Based Access Control for IPv6 (Activer le contrôle d'accès basé rôle pour IPv6).
4. Cliquez sur OK pour enregistrer les modifications.

Modification de la stratégie par défaut

La stratégie par défaut est d'accepter la totalité du trafic provenant de toutes les adresses IP quel que soit le rôle attribué à l'utilisateur.

Pour modifier la stratégie par défaut :

1. Choisissez Device Settings > Security > Role Based Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès basé rôle). La boîte de dialogue Configure Role Based Access Control Settings (Configurer les paramètres de contrôle d'accès basé rôle) apparaît.
2. Pour déterminer la stratégie par défaut pour les adresses IPv4 :
   a. Le cas échéant, cliquez sur l'onglet IPv4.
   b. Assurez-vous que la case Enable Role Based Access Control for IPv4 (Activer le contrôle d'accès basé rôle pour IPv4) est cochée.
   c. Sélectionnez l'action souhaitée dans la liste déroulante Default Policy (Stratégie par défaut).
      - Allow (Autoriser) : accepte le trafic de toutes les adresses IPv4 indépendamment du rôle de l'utilisateur.
      - Deny (Refuser) : refuse le trafic de toutes les adresses IPv4 indépendamment du rôle de l'utilisateur.
3. Pour déterminer la stratégie par défaut pour les adresses IPv6 :
   a. Cliquez sur l'onglet IPv6.

b. Assurez-vous que la case Enable Role Based Access Control for IPv6 (Activer le contrôle d'accès basé rôle pour IPv6) est cochée.

c. Sélectionnez l'action souhaitée dans la liste déroulante Default Policy (Stratégie par défaut).

- Allow (Autoriser) : accepte le trafic de toutes les adresses IPv6 indépendamment du rôle de l'utilisateur.
- Deny (Refuser) : refuse le trafic de toutes les adresses IPv6 indépendamment du rôle de l'utilisateur.

4. Cliquez sur OK pour enregistrer les modifications.

Création de règles de contrôle d'accès basé rôle

Les règles de contrôle d'accès basé rôle acceptent ou refusent le trafic, suivant le rôle et l'adresse IP de l'utilisateur. Comme pour les règles de pare-feu, l'ordre des règles est important car elles sont exécutées dans l'ordre numérique.

Pour créer des règles de contrôle d'accès basé rôle :

1. Choisissez Device Settings > Security > Role Based Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès basé rôle). La boîte de dialogue Configure Role Based Access Control Settings (Configurer les paramètres de contrôle d'accès basé rôle) apparaît.
2. Cliquez sur l'onglet IPv4 pour créer des règles de pare-feu, ou sur l'onglet IPv6 pour créer des règles de pare-feu IPv6.
3. Assurez-vous que la case Enable Role Based Access Control for IPv4 (Activer le contrôle d'accès basé rôle pour IPv4) ou Enable Role Based Access Control for IPv6 (Activer le contrôle d'accès basé rôle pour IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Créez des règles spécifiques :

Action	Procédure
Ajouter une règle à la fin de la liste des règles	▪ Cliquez sur Append (Ajouter). La boîte de dialogue Append new Rule (Ajouter la nouvelle règle) apparaît. ▪ Entrez une adresse IP de début dans le champ Starting IP Address. ▪ Entrez la dernière adresse IP dans le champ Ending IP Address (Adresse IP de fin). ▪ Dans la liste déroulante du champ Role, sélectionnez un rôle. Cette règle ne s'applique qu'aux membres de ce rôle.

Action	Procédure
	▪ Sélectionnez Allow (Autoriser) ou Deny (Refuser) dans la liste déroulante du champ Policy (Stratégie). ▪ Allow (Autoriser) : Accepte le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié. ▪ Deny (Refuser) : Refuse le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié. ▪ Cliquez sur OK pour enregistrer les modifications. Le système numérote automatiquement la règle.
Insérer une règle entre deux autres	▪ Sélectionnez la règle au-dessus de laquelle vous souhaitez insérer une nouvelle règle. Par exemple, pour insérer une règle entre les règles 3 et 4, entrez 4. ▪ Cliquez sur Insert (Insérer). La boîte de dialogue Insert new Rule (Insérer une nouvelle règle) apparaît. ▪ Entrez une adresse IP de début dans le champ Starting IP Address. ▪ Entrez la dernière adresse IP dans le champ Ending IP Address (Adresse IP de fin). ▪ Dans la liste déroulante du champ Role, sélectionnez un rôle. Cette règle ne s'applique qu'aux membres de ce rôle. ▪ Sélectionnez Allow (Autoriser) ou Deny (Refuser) dans la liste déroulante du champ Policy (Stratégie). ▪ Allow (Autoriser) : Accepte le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié. ▪ Deny (Refuser) : Refuse le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié. ▪ Cliquez sur OK pour enregistrer les modifications. Le système insère la règle et renumérote automatiquement les règles suivantes.

5. Cliquez sur OK pour enregistrer les modifications.

Modification de règles de contrôle d'accès basé rôle

Vous pouvez modifier des règles existantes lorsqu'elles ne répondent pas à vos besoins.

Pour modifier une règle de contrôle d'accès basé rôle :

1. Choisissez Device Settings > Security > Role Based Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès basé rôle). La boîte de dialogue Configure Role Based Access Control Settings (Configurer les paramètres de contrôle d'accès basé rôle) apparaît.
2. Pour modifier les règles de pare-feu IPv4, cliquez sur l'onglet IPv4. Pour modifier les règles de pare-feu IPv6, cliquez sur l'onglet IPv6.
3. Assurez-vous que la case Enable Role Based Access Control for IPv4 (Activer le contrôle d'accès basé rôle pour IPv4) ou Enable Role Based Access Control for IPv6 (Activer le contrôle d'accès basé rôle pour IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Dans la liste de règles, sélectionnez la règle à modifier.
5. Cliquez sur Edit (Modifier) ou double-cliquez sur la règle. La fenêtre Edit Rule (Modifier la règle) s'affiche.
6. Modifiez les informations affichées.
7. Cliquez sur OK pour enregistrer les modifications.

Tri des règles de contrôle d'accès basé rôle

Comme pour les règles de pare-feu, l'ordre des règles de contrôle d'accès basé rôle détermine laquelle des règles correspondant à la même adresse IP est exécutée.

Pour trier les règles de contrôle d'accès basé rôle :

1. Choisissez Device Settings > Security > Role Based Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès basé rôle). La boîte de dialogue Configure Role Based Access Control Settings (Configurer les paramètres de contrôle d'accès basé rôle) apparaît.
2. Pour trier les règles de pare-feu IPv4, cliquez sur l'onglet IPv4. Pour trier les règles de pare-feu IPv6, cliquez sur l'onglet IPv6.
3. Assurez-vous que la case Enable Role Based Access Control for IPv4 (Activer le contrôle d'accès basé rôle pour IPv4) ou Enable Role Based Access Control for IPv6 (Activer le contrôle d'accès basé rôle pour IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Sélectionnez une règle particulière en cliquant dessus.

5. Cliquez sur  ou sur  pour faire monter ou descendre la règle sélectionnée jusqu'à ce qu'elle atteigne l'emplacement souhaité.
6. Cliquez sur OK pour enregistrer les modifications.

Suppression des règles de contrôle d'accès basé rôle

Lorsqu'une règle de contrôle d'accès devient inutile ou obsolète, supprimez-la.

Pour supprimer une règle de contrôle d'accès basé rôle :

1. Choisissez Device Settings > Security > Role Based Access Control (Paramètres du dispositif > Sécurité > Contrôle d'accès basé rôle). La boîte de dialogue Configure Role Based Access Control Settings (Configurer les paramètres de contrôle d'accès basé rôle) apparaît.
2. Pour supprimer les règles de pare-feu IPv4, cliquez sur l'onglet IPv4. Pour supprimer les règles de pare-feu IPv6, cliquez sur l'onglet IPv6.
3. Assurez-vous que la case Enable Role Based Access Control for IPv4 (Activer le contrôle d'accès basé rôle pour IPv4) ou Enable Role Based Access Control for IPv6 (Activer le contrôle d'accès basé rôle pour IPv6) est cochée dans l'onglet IPv4 ou IPv6 respectivement.
4. Sélectionnez la règle à supprimer dans la liste de règles. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
5. Cliquez sur Delete (Supprimer).
6. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.
7. Cliquez sur OK pour enregistrer les modifications.

Configuration d'un certificat SSL

L'objet d'un certificat numérique X.509 est d'assurer que les deux parties d'une connexion SSL sont authentiques.

Pour obtenir un certificat pour EMX, créez une demande de signature de certificat et soumettez-la à une autorité de certification. Une fois les données de la demande traitée par l'autorité, un certificat vous est fourni et vous devez l'installer sur le dispositif EMX.

Remarque : reportez-vous à **Chiffrement HTTPS imposé** *(à la page 102) pour savoir comment imposer aux utilisateurs l'emploi de SSL lors de la connexion à EMX.*

Une demande de signature de certificat n'est pas obligatoire dans les cas suivants :

- Vous décidez de générer un certificat *auto-signé* sur le dispositif EMX.
- Des fichiers de certificat et de clé valables sont disponibles.

Demande de signature de certificat

Lorsque des fichiers de certificat et de clé valables pour EMX NE SONT PAS disponibles, une des solutions consiste à créer une demande de signature de certificat et une clé privée sur le dispositif EMX, puis à envoyer la demande à une autorité de certification pour qu'elle signe le certificat.

Création d'une demande de signature de certificat

Suivez cette procédure pour créer la demande de signature de certificat du dispositif EMX.

Pour créer une demande de signature de certificat :

1. Choisissez Device Settings > Security > SSL Certificate (Paramètres du dispositif > Sécurité > Certificat SSL). La boîte de dialogue Manage SSL Certificate (Gérer le certificat SSL) apparaît.
2. Cliquez sur l'onglet New SSL Certificate (Nouveau certificat SSL).
3. Donnez les informations demandées.
   - Dans la section Subject (Objet) :

Champ	Tapez ces données
Country (ISO Code) (Pays (code ISO))	Le pays où se situe votre société. Utilisez le code de pays ISO standard. Pour obtenir la liste des codes ISO, consultez le ***site Web de l'ISO*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province (Etat ou Province)	Le nom complet de l'Etat ou de la province où se situe votre société.
Locality (Localité)	La ville où se situe votre société.
Organization (Organisation)	Le nom officiel de votre société.
Organizational Unit (Unité organisationnelle)	Le nom de votre service.
Common Name (Nom courant)	Le nom de domaine complet du dispositif EMX.
Email address (Adresse électronique)	Une adresse électronique à laquelle vous ou un autre utilisateur administratif pouvez être joint.

Remarque : tous les champs de la section Subject (Objet) sont obligatoires, sauf Organization, Organizational Unit et Email Address. Si vous générez une demande de signature de certificat avec les champs obligatoires vides, vous ne pouvez pas obtenir de certificats tiers.

- Dans la section Key Creation Parameters (Paramètres de création de clé) :

Champ	Procédure
Key Length (Longueur de clé)	Sélectionnez la longueur de clé (bits) dans la liste déroulante de ce champ. Une longueur de clé plus importante améliore la sécurité mais ralentit la réponse du dispositif EMX.
Self Sign (Signature automatique)	**Pour demander un certificat signé par l'autorité de certification, vérifiez que cette case N'EST PAS cochée.**
Challenge (Mot de passe de demande d'accès)	Entrez un mot de passe. Le mot de passe est utilisé pour protéger le certificat ou la demande de signature de certificat. Cette information est facultative et la valeur doit comporter 4 à 64 caractères. Le mot de passe est sensible à la casse, veillez à mettre les bonnes lettres en majuscules.
Confirm Challenge (Confirmer le mot de passe de demande d'accès)	Entrez à nouveau le même mot de passe pour le confirmer.

4. Cliquez sur Create New SSL Key (Créer une clé SSL) pour créer la demande de signature de certificat et la clé privée. L'opération peut prendre plusieurs minutes.
5. Pour télécharger la nouvelle demande sur votre ordinateur, cliquez sur Download Certificate Signing Request (Télécharger la demande de signature de certificat).
   a. Vous êtes invité à ouvrir ou à enregistrer le fichier. Cliquez sur Save pour l'enregistrer sur votre ordinateur.
   b. Une fois le fichier stocké sur votre ordinateur, soumettez-le à une autorité de certification pour obtenir le certificat numérique.
   c. Si vous le souhaitez, cliquez sur Delete Certificate Signing Request (Supprimer la demande de signature de certificat) pour supprimer définitivement le fichier de la demande du dispositif EMX.
6. Pour stocker la clé privée que vous venez de créer sur votre ordinateur, cliquez sur Download Key (Télécharger la clé). Vous êtes invité à ouvrir ou à enregistrer le fichier. Cliquez sur Save pour l'enregistrer sur votre ordinateur.
7. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Installation d'un certificat signé par une autorité de certification

Une fois que l'autorité de certification a fourni un certificat signé en fonction de la demande soumise, vous devez installer celui-ci sur le dispositif EMX.

Pour installer le certificat :

1. Choisissez Device Settings > Security > SSL Certificate (Paramètres du dispositif > Sécurité > Certificat SSL). La boîte de dialogue Manage SSL Certificate (Gérer le certificat SSL) apparaît.
2. Cliquez sur l'onglet New SSL Certificate (Nouveau certificat SSL).
3. Dans le champ Certificate File (Fichier de certificat), cliquez sur Browse (Parcourir) pour sélectionner le fichier de certificat fourni par l'autorité de certification.
4. Cliquez sur Upload (Téléverser). Le certificat est installé sur le dispositif EMX.

   Conseil : pour vérifier si le certificat a été installé correctement, cliquez ultérieurement sur l'onglet Active SSL Certificate (Certificat SSL actif).

5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Création d'un certificat auto-signé

Lorsqu'aucun fichier de certificat et de clé valable pour le dispositif EMX n'est disponible, la solution, outre l'envoi d'une demande à l'autorité de certification, consiste à générer une certificat auto-signé.

Pour créer et installer un certificat auto-signé :

1. Choisissez Device Settings > Security > SSL Certificate (Paramètres du dispositif > Sécurité > Certificat SSL). La boîte de dialogue Manage SSL Certificate (Gérer le certificat SSL) apparaît.
2. Cliquez sur l'onglet New SSL Certificate (Nouveau certificat SSL).
3. Donnez les informations demandées.

Champ	Tapez ces données
Country (ISO Code) (Pays (code ISO))	Le pays où se situe votre société. Utilisez le code de pays ISO standard. Pour obtenir la liste des codes ISO, consultez le ***site Web de l'ISO*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province (Etat ou Province)	Le nom complet de l'Etat ou de la province où se situe votre société.
Locality (Localité)	La ville où se situe votre société.
Organization (Organisation)	Le nom officiel de votre société.
Organizational Unit (Unité organisationnelle)	Le nom de votre service.
Common Name (Nom courant)	Le nom de domaine complet du dispositif EMX.
Email address (Adresse électronique)	Une adresse électronique à laquelle vous ou un autre utilisateur administratif pouvez être joint.
Key Length (Longueur de clé)	Sélectionnez la longueur de clé (bits) dans la liste déroulante de ce champ. Une longueur de clé plus importante améliore la sécurité mais ralentit la réponse du dispositif EMX.
Self Sign (Signature automatique)	**Vérifiez que cette case est cochée, ce qui indique que vous créez un certificat auto-signé.**
Validity in days (Jours de validité)	Ce champ apparaît lorsque la case Self Sign est cochée. Entrez le nombre de jours de validité du certificat auto-signé dans ce champ.

Remarque : tous les champs de la section Subject (Objet) sont obligatoires, sauf Organization, Organizational Unit et Email Address.

aucun mot de passe n'est nécessaire pour un certificat auto-signé alors les champs Challenge et Confirm Challenge disparaissent après que la case Self Sign est cochée.

4. Cliquez sur Create New SSL Key (Créer une clé SSL) pour créer le certificat auto-signé et la clé privée. L'opération peut prendre plusieurs minutes.
5. Vous pouvez également effectuer une des opérations suivantes :
   - Cliquez sur Install Key and Certificate (Installer la clé et le certificat) pour installer immédiatement le certificat auto-signé et la clé privée. Lorsque des messages de confirmation et de sécurité apparaissent, cliquez sur Yes pour continuer.

   Conseil : pour vérifier si le certificat a été installé correctement, cliquez ultérieurement sur l'onglet Active SSL Certificate (Certificat SSL actif).

   - Pour télécharger le certificat auto-signé ou la clé privée, cliquez sur Download Certificate (Télécharger le certificat) ou Download Key (Télécharger la clé). Vous êtes invité à ouvrir ou à enregistrer le fichier. Cliquez sur Save pour l'enregistrer sur votre ordinateur.
   - Pour supprimer définitivement le certificat auto-signé et la clé privée du dispositif EMX, cliquez sur Delete Key and Certificate (Supprimer la clé et le certificat).
6. Si vous avez installé le certificat auto-signé à l'étape 5, une fois l'installation terminée, le dispositif EMX est réinitialisé et la page de connexion s'ouvre à nouveau.

Installation des fichiers de clé et de certificat existants

Si les fichiers de certificat SSL et de clé privée sont déjà disponibles, vous pouvez les installer directement sans passer par le processus de création d'une demande de signature de certificat ou d'un certificat auto-signé.

Pour installer les fichiers de clé et de certificat existants :

1. Choisissez Device Settings > Security > SSL Certificate (Paramètres du dispositif > Sécurité > Certificat SSL). La boîte de dialogue Manage SSL Certificate (Gérer le certificat SSL) apparaît.
2. Cliquez sur l'onglet New SSL Certificate (Nouveau certificat SSL).
3. Cochez la case Upload Key and Certificate (Téléverser la clé et le certificat). Les champs Key File (Fichier de clé) et Certificate File (Fichier de certificat) apparaissent.
4. Dans le champ Key File, cliquez sur Browse (Parcourir) pour sélectionner le fichier de clé privée.

5. Dans le champ Certificate File, cliquez sur Browse (Parcourir) pour sélectionner le fichier de certificat.
6. Cliquez sur Upload (Téléverser). Les fichiers sélectionnés sont installés sur le dispositif EMX.

Conseil : pour vérifier si le certificat a été installé correctement, cliquez ultérieurement sur l'onglet Active SSL Certificate (Certificat SSL actif).

7. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Téléchargement des fichiers de clé et de certificat

Vous pouvez télécharger les fichiers de clé et de certificat actuellement installés sur le dispositif EMX pour la sauvegarde ou d'autres opérations. Par exemple, vous pouvez installer les fichiers sur un dispositif EMX de remplacement, ajouter le certificat à votre navigateur, etc.

Pour télécharger les fichiers de certificat et de clé depuis un dispositif EMX :

1. Choisissez Device Settings > Security > SSL Certificate (Paramètres du dispositif > Sécurité > Certificat SSL). La boîte de dialogue Manage SSL Certificate (Gérer le certificat SSL) apparaît.
2. L'onglet Active SSL Certificate (Certificat SSL actif) doit être ouvert. Sinon, cliquez dessus.
3. Cliquez sur Download Key (Télécharger la clé) pour télécharger le fichier de clé privée installé sur le dispositif EMX. Vous êtes invité à ouvrir ou à enregistrer le fichier. Cliquez sur Save pour l'enregistrer sur votre ordinateur.
4. Cliquez sur Download Certificate (Télécharger le certificat) pour télécharger le fichier de certificat installé sur le dispositif EMX. Vous êtes invité à ouvrir ou à enregistrer le fichier. Cliquez sur Save pour l'enregistrer sur votre ordinateur.
5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Paramétrage de l'authentification LDAP

Pour des raisons de sécurité, les utilisateurs tentant de se connecter à EMX doivent être authentifiés. EMX prend en charge l'accès à l'aide d'un des mécanismes d'authentification suivants :

- Base de données locale des profils utilisateur sur le dispositif EMX
- Protocole LDAP (Lightweight Directory Access Protocol)

Par défaut, le dispositif EMX est configuré pour une authentification locale. Si vous conservez cette méthode, il vous suffit de créer des profils pour chaque utilisateur autorisé. Si vous préférez utiliser un serveur LDAP externe, effectuez les opérations suivantes :

- Fournissez à EMX les données concernant le serveur LDAP.
- Créez des profils pour les utilisateurs authentifiés en externe car un profil utilisateur sur le dispositif EMX détermine les rôles appliqués à l'utilisateur et de fait, les autorisations accordées à ce dernier.

Si l'authentification LDAP est configurée, tous les utilisateurs EMX doivent avoir un compte sur le serveur LDAP. Les utilisateurs à authentification locale uniquement n'auront pas accès à EMX, à l'exception de l'administrateur qui a accès à EMX en permanence.

Rassemblement des informations LDAP

La configuration de EMX pour l'authentification LDAP nécessite la connaissance du serveur LDAP et des paramètres de répertoire. Si vous n'êtes pas familiarisé avec les paramètres, demandez l'aide de votre administrateur LDAP.

Pour configurer l'authentification LDAP, vous devez vérifier :

- l'adresse IP ou le nom d'hôte du serveur LDAP ;
- si le protocole LDAP sécurisé (LDAP sur SSL) est utilisé ;
  - Si tel est le cas, demandez le fichier de certificat de l'AC à l'administrateur LDAP.
- le port réseau utilisé par le serveur LDAP ;
- le type de serveur LDAP, généralement l'une des options suivantes :
  - *OpenLDAP*
    - Si vous utilisez un serveur OpenLDAP, consultez l'administrateur LDAP pour obtenir le ND et le mot de passe de liaison.
  - *Microsoft Active Directory® (AD)*

  - Si vous utilisez un serveur Microsoft Active Directory, demandez à l'administrateur AD le nom du domaine Active Directory.
- le ND et le mot de passe de liaison (si la liaison anonyme N'EST PAS utilisée) ;
- le ND de base du serveur (utilisé pour rechercher des utilisateurs) ;
- l'attribut de nom de connexion (ou AuthorizationString) ;
- la classe d'objets d'entrée d'utilisateur ;
- le sous-filtre de recherche des utilisateurs (ou BaseSearch).

Ajout des paramètres de serveur LDAP

Pour activer et utiliser l'authentification de serveur LDAP/LDAPS, activez l'authentification LDAP et entrez les informations rassemblées pour les serveurs LDAP/LDAPS.

Remarque : un serveur LDAPS se réfère à un serveur LDAP sécurisé SSL.

Pour ajouter les paramètres de serveur LDAP/LDAPS :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Sélectionnez la case d'option LDAP pour activer l'authentification de serveur LDAP/LDAPS à distance.
3. Cliquez sur New (Nouveau) pour ajouter un serveur LDAP/LDAPS pour authentification. La boîte de dialogue Create new LDAP Server Configuration (Créer une configuration de serveur LDAP) apparaît.
4. IP Address / Hostname : entrez l'adresse IP ou le nom d'hôte de votre serveur d'authentification LDAP/LDAPS.

   Important : si le chiffrement SSL n'est pas activé, vous pouvez taper le nom de domaine ou l'adresse IP dans ce champ. S'il est activé, vous devez taper le nom de domaine complet.
5. Type de serveur LDAP/LDAPS externe. Sélectionnez-le parmi les options disponibles :
   - OpenLDAP
   - Microsoft Active Directory. Active Directory est une implémentation des services d'annuaires LDAP/LDAPS par Microsoft à utiliser dans les environnements Windows.
6. LDAP over SSL (LDAP sur SSL) : cochez cette case si vous souhaitez utiliser SSL. SSL (Secure Sockets Layer) est un protocole cryptographique qui permet à EMX de communiquer en toute sécurité avec le serveur LDAP/LDAPS.

7. Port : le port par défaut est 389. Utilisez le port LDAP TCP standard ou spécifiez un autre port.
8. SSL Port (Port SSL) : la valeur par défaut est 636. Utilisez le port par défaut ou spécifiez un autre port. Ce champ est activé lorsque la case LDAP over SSL (LDAP sur SSL) est cochée.
9. Use only trusted LDAP Server Certificates (Utiliser uniquement des certificats de serveur LDAP de confiance) : cochez cette case si vous souhaitez utiliser un fichier de certificat de serveur LDAP de confiance, c'est-à-dire signé par l'autorité de certification. Lorsque cette case N'EST PAS cochée, vous pouvez utiliser tous les certificats de serveur LDAP/LDAPS, même un fichier de certificat auto-signé. Un fichier de certificat est nécessaire après l'activation de cette option.
10. Server Certificate (Certificat de serveur) : consultez l'administrateur de serveur d'authentification pour obtenir un fichier de certificat de l'autorité de certification pour le serveur LDAP/LDAPS. Utilisez le bouton Browse (Parcourir) pour localiser le fichier du certificat. Ce fichier est obligatoire lorsque la case Use only trusted LDAP Server Certificates (Utiliser uniquement des certificats de serveur LDAP de confiance) est cochée.

   Conseil : vous pouvez d'abord téléverser le certificat CA pour une utilisation future avant de cocher la case Use only trusted LDAP Server Certificates, puis cochez cette dernière lorsque vous avez besoin du fichier de certificat.

11. Anonymous Bind (Liaison anonyme) : pour OpenLDAP, utilisez cette case à cocher pour activer ou désactiver une liaison anonyme.
    - Pour utiliser une liaison anonyme, cochez cette case.
    - Lorsqu'un ND et un mot de passe de liaison sont nécessaires pour effectuer la liaison au serveur LDAP/LDAPS externe, décochez cette case.
12. Use Bind Credentials (Utiliser les informations d'identification de liaison) : Pour Microsoft Active Directory, utilisez cette case à cocher pour activer ou désactiver la liaison anonyme.
    - Pour utiliser une liaison anonyme, décochez cette case. Par défaut, elle est décochée.
    - Lorsqu'un ND et un mot de passe de liaison sont nécessaires pour effectuer la liaison au serveur LDAP/LDAPS externe, cochez cette case.
13. Bind DN (ND de liaison) : indiquez le ND de l'utilisateur qui est autorisé à rechercher le répertoire LDAP dans la base de recherche définie. Cette information est requise uniquement lorsque la case Use Bind Credentials est cochée.

14. Bind Password (Mot de passe de liaison) et Confirm Bind Password (Confirmer le mot de passe de liaison) : entrez tout d'abord le mot de passe de liaison dans le champ Bind Password, puis dans le champ Confirm Bind Password. Cette information est requise uniquement lorsque la case Use Bind Credentials est cochée.
15. Base DN for Search (ND de base pour recherche) : entrez le nom à soumettre à l'authentification LDAP/LDAPS (31 caractères au plus) et l'emplacement dans la base de données où doit débuter la recherche du DN de base spécifié. Exemple de valeur de recherche de base : `cn=Users,dc=raritan,dc=com`. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ces champs.
16. Entrez les valeurs suivantes dans les champs correspondants : LDAP a besoin de ces informations pour vérifier les noms d'utilisateur et les mots de passe.
    - Attribut de nom de connexion (également appelé AuthorizationString)
    - Classe d'objets d'entrée d'utilisateur
    - Sous-filtre de recherche des utilisateurs (également appelé BaseSearch)

    Remarque : EMX alimentera l'attribut de nom de connexion et la classe d'objets d'entrée d'utilisateur avec des valeurs par défaut qui ne devront être modifiées que si nécessaire.
17. Domaine Active Directory : entrez le nom du domaine Active Directory. Par exemple, testradius.com. Consultez l'administrateur Active Directory pour obtenir un nom de domaine spécifique.
18. Pour vérifier si la configuration LDAP/LDAPS est correcte, vous pouvez cliquer sur Test Connection (Tester la connexion) pour vous assurer que EMX peut se connecter au serveur LDAP/LDAPS.

    Conseil : pour cela, vous pouvez également utiliser le bouton Test Connection (Tester la connexion) dans la boîte de dialogue Authentication Settings (Paramètres d'authentification).
19. Cliquez sur OK pour enregistrer les modifications. Le nouveau serveur LDAP figure dans la boîte de dialogue Authentication Settings (Paramètres d'authentification).
20. Pour ajouter des serveurs LDAP/LDAPS, répétez les étapes 3 à 19.
21. Cliquez sur OK pour enregistrer les modifications. L'authentification LDAP est maintenant en place.

Remarque : si les horloges de EMX et du serveur LDAP ne sont pas synchrones, les certificats sont considérés comme expirés et les utilisateurs ne peuvent pas s'authentifier à l'aide de LDAP. Pour assurer une synchronisation correcte, il est recommandé que les administrateurs configurent EMX et le serveur LDAP pour qu'ils utilisent le même serveur NTP.

Informations supplémentaires sur la configuration AD

Pour en savoir plus sur la configuration LDAP à l'aide de Microsoft Active Directory, reportez-vous à ***Illustration de la configuration LDAP*** (à la page 330).

Tri de l'ordre d'accès LDAP

L'ordre de la liste LDAP détermine la priorité d'accès des serveurs LDAP/LDAPS distants. EMX tente en premier lieu d'accéder au serveur LDAP/LDAPS au sommet de la liste pour authentification, puis au serveur suivant si l'accès au premier échoue, etc. jusqu'à ce que le dispositif EMX se connecte à un des serveurs LDAP/LDAPS de la liste.

Remarque : après s'être connecté à un serveur LDAP/LDAPS, EMX N'ESSAIE PLUS d'accéder aux serveurs LDAP/LDAPS de la liste quel que soit le résultat de l'authentification de l'utilisateur.

Pour trier à nouveau la liste d'accès des serveurs LDAP :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Sélectionnez le serveur LDAP/LDAPS dont vous souhaitez changer la priorité.
3. Cliquez sur Move up (Vers le haut) ou Move down (Vers le bas) jusqu'à ce que le serveur sélectionné atteigne la position souhaitée dans la liste.
4. Cliquez sur OK pour enregistrer les modifications.

Test de la connexion des serveurs LDAP

Vous pouvez tester la connexion vers n'importe quel serveur LDAP/LDAPS afin de vérifier l'accessibilité de ce serveur ou la validité des paramètres d'authentification.

Pour tester la connexion vers un serveur LDAP/LDAPS :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.

2. Sélectionnez le serveur LDAP/LDAPS que vous souhaitez tester.
3. Cliquez sur Test Connection (Tester la connexion) pour démarrer le test de connexion.

Modification des paramètres de serveur LDAP

Si la configuration d'un serveur LDAP/LDAPS a été modifiée, comme le numéro de port, les ND et mot de passe de liaison, vous devez modifier les paramètres LDAP/LDAPS sur le dispositif EMX en conséquence ou l'authentification échoue.

Pour modifier la configuration de l'authentification LDAP :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Sélectionnez le serveur LDAP/LDAPS que vous souhaitez modifier.
3. Cliquez sur Edit (Modifier). La boîte de dialogue Edit LDAP Server Configuration (Modifier la configuration du serveur LDAP) apparaît.
4. Apportez les modifications nécessaires aux informations affichées.
5. Cliquez sur OK pour enregistrer les modifications.

Suppression des paramètres de serveur LDAP

Vous pouvez supprimer les paramètres d'authentification d'un serveur LDAP/LDAPS particulier lorsque ce serveur n'est pas disponible ou utilisé pour l'authentification à distance.

Pour supprimer un ou plusieurs serveurs LDAP/LDAPS :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Sélectionnez le serveur LDAP/LDAPS que vous souhaitez supprimer. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
3. Cliquez sur Delete (Supprimer).
4. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.
5. Cliquez sur OK pour enregistrer les modifications.

Désactivation de l'authentification LDAP

Lorsque le service d'authentification à distance est désactivé, EMX authentifie les utilisateurs à l'aide de la base de données locale stockée sur le dispositif EMX.

Pour désactiver le service d'authentification LDAP :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Sélectionnez la case d'option Local Authentication (Authentification locale).
3. Cliquez sur OK pour enregistrer les modifications.

Activation des services d'authentification LDAP et locale

Pour que l'authentification fonctionne correctement à tout moment, même lorsque l'authentification externe n'est pas disponible, vous pouvez activer les services d'authentification locale et distante.

Lorsque ces deux services d'authentification sont activés, EMX suit les règles d'authentification suivantes :

- Lorsque n'importe lequel des serveurs LDAP/LDAPS de la liste d'accès est disponible, EMX effectue l'authentification sur le serveur LDAP/LDAPS connecté uniquement.
- Lorsque la connexion échoue pour tous les serveurs LDAP/LDAPS, EMX autorise l'authentification sur la base de données locale.

Pour activer les deux services d'authentification :

1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Vérifiez que la case d'option LDAP est sélectionnée.
3. Cochez la case Use Local Authentication if Remote Authentication service is not available (Utiliser l'authentification locale si le service d'authentification distante n'est pas disponible).
4. Cliquez sur OK pour enregistrer les modifications.

Chapitre 7 Règles et actions d'événement, et journaux d'applications

Dans ce chapitre

Règles et actions d'événement

L'un des avantages de l'intelligence du produit réside dans sa capacité à vous avertir d'une modification des conditions et à y réagir. Cette notification d'événement ou réaction est une règle d'événement.

EMX est livré avec deux règles d'événement intégrées qui ne peuvent pas être supprimées.

- System Event Log Rule (Règle de journal des événements système) : cette règle entraîne l'enregistrement de N'IMPORTE QUEL événement se produisant sur EMX dans le journal interne. Cette règle est activée par défaut.
- System SNMP Trap Rule (Règle de traps SNMP système) : cette règle entraîne l'envoi des traps SNMP à des adresses IP ou hôtes indiqués lorsque N'IMPORTE QUEL événement se produit sur EMX. Cette règle est désactivée par défaut.

Si ces deux règles ne répondent pas à vos besoins, vous pouvez créer des règles supplémentaires pour répondre à différents événements.

Remarque : Internet Explorer® 8 (IE8) n'utilise pas de script JAVA compilé. Lorsque vous utilisez IE8 pour créer ou modifier des règles d'événement, les performances du processeur peuvent se dégrader, provoquant l'apparition du message de temporisation de la connexion. Lorsque cela se produit, cliquez sur Ignore pour continuer.

Composants d'une règle d'événement

Une règle d'événement définit ce que EMX fait dans certaines situations ; elle est composée de deux parties :

- Evénement : il s'agit de la situation où EMX ou une partie répond à une certaine condition ; par exemple, le capteur de température dépasse le seuil d'avertissement.
- Action : il s'agit de la réponse à l'événement. Par exemple, EMX avertit l'administrateur système de l'événement et consigne ce dernier dans le journal.

Remarque : les règles d'événement de gestion des ressources doivent être créées à nouveau après une mise à niveau du firmware du dispositif EMX.

Création d'une règle d'événement

Le meilleur moyen de créer un jeu de règles d'événement, en séquence, consiste à :

- créer des actions pour répondre à un ou plusieurs événements ;
- créer des règles afin de déterminer les actions à effectuer lorsque ces événements se produisent.

Création des règles

Lorsque les actions nécessaires sont disponibles, vous pouvez créer des règles d'événement afin de déterminer les actions à effectuer pour répondre à des événements particuliers.

Par défaut, EMX fournit deux règles d'événement intégrées : System Event Log Rule (Règle de journal des événements système) et System SNMP Trap Rule (Règle de traps SNMP système). Si les règles intégrées ne répondent pas à vos besoins, créez-en d'autres.

Pour créer des règles d'événement :

1. Choisissez Device Settings > Event Rules (Paramètres du dispositif > Règles d'événement). La fenêtre Event Rule Settings (Paramètres des règles d'événement) s'affiche.
2. Dans l'onglet Rules (Règles), cliquez sur New Rule (Nouvelle règle).
3. Dans le champ Rule name (Nom de la règle), entrez un nouveau nom pour identifier la règle. Le nom par défaut est New Rule <number> (Nouvelle règle numéro), où <numéro> est un numéro séquentiel.
4. Cochez la case Enabled (Activée) pour activer cette règle d'événement.

5. Cliquez sur Event (Evénement) pour sélectionner un événement pour lequel vous souhaitez déclencher une action. Un menu déroulant présentant tous les types d'événements s'affiche.
   - Sélectionnez le type d'événement souhaité dans le menu déroulant, et si un sous-menu apparaît, continuez la navigation jusqu'à ce que l'événement souhaité soit sélectionné.

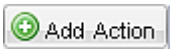
Remarque : l'option <Any sub-event> fait référence à tous les événements/éléments répertoriés sur le même sous-menu, <Any slot>, à toutes les fentes, <Any server>, à tous les serveurs, et <Any user> à tous les utilisateurs.

6. Selon l'événement sélectionné à l'étape précédente, le champ Trigger condition (Condition de déclenchement) contenant trois cases d'option apparaît ou non.

Types d'événements	Cases d'option
Evénements de dépassement d'un seuil de capteur numérique, ou connexions ou déconnexions d'étiquettes de gestion des ressources	Les cases d'option disponibles sont Asserted (Affirmé), Deasserted (Infirmé) et Both (Les deux). ▪ Asserted (Affirmée) : EMX n'intervient que lorsque l'événement se produit. Ceci signifie que le statut de l'événement décrit passe de FALSE à TRUE. ▪ Deasserted (Infirmée) : EMX n'intervient que lorsque la condition d'événement disparaît. Ceci signifie que le statut de l'événement décrit passe de TRUE à FALSE. ▪ Both (Les deux) : EMX intervient lorsque l'événement a lieu (affirme) et lorsque la condition d'événement disparaît (infirme).
Changement d'état du capteur discret (activé/désactivé)	Les cases d'option disponibles sont Alarmed (Alarme), No longer alarmed (Plus d'alarme) et Both (Les deux). ▪ Alarmed : EMX n'intervient que lorsque le capteur choisi passe à l'état alarmed, soit à l'état anormal. ▪ No longer alarmed : EMX n'intervient que lorsque le capteur choisi retourne à l'état normal. ▪ Both : EMX intervient lorsque le capteur passe à l'état alarmed ou le quitte.

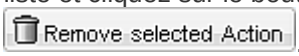
Types d'événements	Cases d'option
Disponibilité des capteurs	Les cases d'option disponibles sont Unavailable (Indisponible), Available (Disponible) et Both (Les deux). ▪ Unavailable : EMX n'intervient que lorsque le capteur choisi N'EST PAS détecté et devient indisponible. ▪ Available : EMX n'intervient que lorsque le capteur choisi est détecté et devient disponible. ▪ Both : EMX intervient lorsque le capteur choisi devient indisponible ou disponible.
Etat de liaison de l'interface réseau	Les cases d'option disponibles sont Link state is up (Etat de liaison actif), Link state is down (Etat de liaison inactif) et Both (Les deux). ▪ Link state is up : EMX n'intervient que lorsque l'état de la liaison réseau passe d'inactif à actif. ▪ Link state is down : EMX n'intervient que lorsque l'état de la liaison réseau passe d'actif à inactif. ▪ Both : EMX intervient chaque fois que l'état de la liaison réseau change.
Fonction activée ou désactivée	Les cases d'option disponibles sont Enabled (Activé), Disabled (Désactivé) et Both (Les deux). ▪ Enabled : EMX n'intervient que lorsque la fonction choisie est activée. ▪ Disabled : EMX n'intervient que lorsque la fonction choisie est désactivée. ▪ Both : EMX intervient lorsque la fonction choisie est activée ou désactivée.
Connexion ou déconnexion des utilisateurs	Les cases d'option disponibles sont Logged in (Connecté), Logged out (Déconnecté) et Both (Les deux). ▪ Logged in : EMX n'intervient que lorsque l'utilisateur sélectionné se connecte. ▪ Logged out : EMX n'intervient que lorsque l'utilisateur sélectionné se déconnecte. ▪ Both : EMX intervient lorsque l'utilisateur sélectionné se connecte et se déconnecte.

Types d'événements	Cases d'option
Evénement de surveillance des serveurs	Les cases d'option disponibles sont Monitoring started (Surveillance démarrée), Monitoring stopped (Surveillance arrêtée) et Both (Les deux). ▪ Monitoring started : EMX n'intervient que lorsque la surveillance d'un serveur indiqué démarre. ▪ Monitoring stopped : EMX n'intervient que lorsque la surveillance d'un serveur indiqué s'arrête. ▪ Both : EMX intervient lorsque la surveillance d'un serveur indiqué démarre ou s'arrête.
Accessibilité des serveurs	Les cases d'option disponibles sont Unreachable (Inaccessible), Reachable (Accessible) et Both (Les deux). ▪ Unreachable : EMX n'intervient que lorsque le serveur indiqué devient inaccessible. ▪ Reachable : EMX n'intervient que lorsque le serveur indiqué devient accessible. ▪ Both : EMX intervient lorsque le serveur indiqué devient inaccessible ou accessible.

1. Dans le champ Actions, cliquez sur la flèche déroulante et sélectionnez dans la liste l'action souhaitée. Cliquez ensuite sur le bouton 

pour ajouter l'action.

   L'action ajoutée apparaîtra dans la zone de liste à droite du champ Actions.

2. Pour ajouter des actions supplémentaires, répétez l'étape 7.
3. Pour supprimer une action ajoutée, sélectionnez-la dans la zone de liste et cliquez sur le bouton Remove selected Action 

.
4. Cliquez sur Save (Enregistrer) pour enregistrer la nouvelle règle d'événement.

   Remarque : si vous ne cliquez pas sur Save (Enregistrer) avant de quitter la page de paramètres active, un message apparaît. Cliquez alors sur Yes pour enregistrer les modifications, sur Discard (Refuser) pour les abandonner ou sur Cancel (Annuler) pour retourner sur la page des paramètres active.

5. Répétez les étapes 2 à 10 pour créer des règles d'événement supplémentaires.
6. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Remarque : les règles d'événement de gestion des ressources doivent être créées à nouveau après une mise à niveau du firmware du dispositif EMX.

Création des actions

EMX est livré avec deux actions intégrées :

- System Event Log Action (Action de journal des événements système) : cette action enregistre l'événement sélectionné dans le journal interne lorsqu'il se produit.
- System SNMP Trap Action (Action de traps SNMP système) : cette action envoie des traps SNMP à une ou plusieurs adresses IP après que l'événement sélectionné se produit.

Remarque : aucune adresse IP n'est indiquée par défaut pour l'action de traps SNMP système (System SNMP Trap Action) ; vous devez donc spécifier des adresses IP avant d'appliquer cette action à une règle d'événement quelconque.

Les actions intégrées ne peuvent pas être supprimées. Si ces actions ne répondent pas à vos besoins, créez-en d'autres.

Pour créer des actions :

1. Cliquez sur l'onglet Actions.
2. Cliquez sur New Action (Nouvelle action).
3. Dans le champ Action name (Nom de l'action), entrez un nouveau nom pour l'action. Le nom par défaut est New Action <number> (Nouvelle action numéro), où <numéro> est un numéro séquentiel.
4. Dans le champ Action, cliquez sur la flèche déroulante et sélectionnez l'action souhaitée dans la liste. Vous trouverez des descriptions ci-après.
5. Cliquez sur Save (Enregistrer).

   Remarque : si vous ne cliquez pas sur Save (Enregistrer) avant de quitter la page de paramètres active, un message apparaît. Cliquez alors sur Yes pour enregistrer les modifications, sur Discard (Refuser) pour les abandonner ou sur Cancel (Annuler) pour retourner sur la page des paramètres active.

6. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Option	Description
Execute an action group (Exécuter un groupe d'actions)	Cette option permet de sélectionner l'action qui sera exécutée lorsqu'un événement est déclenché. • SMS • System Event Log Action (Action de journal des événements système) • System SNMP Trap Action (Action de traps SNMP système) *Remarque : Un modem Cinterion® GSM MC52i doit être branché sur EMX pour permettre l'envoi de SMS.*
Log event message (Consigner un message de l'événement)	Cette option enregistre les événements sélectionnés dans le journal interne.

Option	Description
Send Snapshots via Email (Envoyer des instantanés par courriel)	Cette option prévient une ou plusieurs personnes des événements sélectionnés en leur envoyant des instantanés ou des vidéos pris par une webcam Logitech® QuickCam® Pro 9000 connectée (s'il y a lieu). ▪ Renseignez le champ Recipients email addresses (Adresses électroniques des destinataires). Utilisez une virgule pour séparer ces adresses. ▪ Pour utiliser le serveur SMTP indiqué dans la boîte de dialogue SMTP Server Settings (Paramètres du serveur SMTP), cochez la case Use Default SMTP Server (Utiliser le serveur SMTP par défaut). Pour utiliser un autre serveur SMTP, cochez la case Use Custom SMTP Settings (Utiliser des paramètres SMTP personnalisés). Si les paramètres du serveur SMTP ne sont pas encore configurés, cliquez sur Configure (Configurer). Reportez-vous à ***Configuration des paramètres SMTP*** (à la page 91) pour en savoir plus sur chaque champ. ▪ Sélectionnez la webcam qui prend les images que vous souhaitez envoyer dans le courriel. ▪ Dans le champ Number of Snapshots (Nombre d'instantanés), entrez le nombre de clichés à inclure dans la séquence d'images prises lorsque l'événement se produit. Par exemple, vous pouvez indiquer que 10 images seront prises lorsque l'événement déclenche l'action. ▪ Dans le champ Snapshots/Mail (Instantanés/Courriel), entrez le nombre maximum d'instantanés de la séquence à envoyer en même temps dans le courriel. ▪ Dans le champ Time before first Snapshot(s): (Temps écoulé avant les premiers instantanés), entrez le nombre de secondes qui doit s'écouler entre le déclenchement de l'événement et le moment où la webcam commence à prendre des clichés. ▪ Dans le champ Time between Snapshots(s): (Durée entre les instantanés), entrez le temps qui doit s'écouler entre la prise de chaque cliché.

Option	Description
Send EMail (Envoyer un courriel)	Cette action envoie un courriel aux destinataires indiqués pour les prévenir qu'un événement s'est produit. • Renseignez le champ Recipients email addresses (Adresses électroniques des destinataires). Utilisez une virgule pour séparer ces adresses. • Pour utiliser le serveur SMTP indiqué dans la boîte de dialogue SMTP Server Settings (Paramètres du serveur SMTP), cochez la case Use Default SMTP Server (Utiliser le serveur SMTP par défaut). Pour utiliser un autre serveur SMTP, cochez la case Use Custom SMTP Settings (Utiliser des paramètres SMTP personnalisés). Si les paramètres du serveur SMTP ne sont pas encore configurés, cliquez sur Configure (Configurer). Reportez-vous à ***Configuration des paramètres SMTP*** (à la page 91) pour en savoir plus sur chaque champ. Des messages par défaut sont envoyés selon l'événement. Reportez-vous à ***Messages de journaux par défaut*** (à la page 143) pour obtenir la liste des messages de journaux par défaut et des événements qui les déclenchent. • Le cas échéant, cochez la case Use Custom Log Message (Utiliser un message de journal personnalisé), puis créez un message personnalisé dans le champ fourni. Reportez-vous à ***Création de courriels personnalisés*** (à la page 141).
Send SNMP trap (Envoyer un trap SNMP)	Cette option envoie des traps SNMP à un ou plusieurs gestionnaires SNMP. • Vous pouvez définir jusqu'à trois destinations de traps SNMP dans les champs Host *x* (Hôte x), où *x* est un nombre de 1 à 3. • Indiquez un numéro de port pour chaque destination dans les champs Port *x*, où *x* est un nombre de 1 à 3. • Indiquez une chaîne de communauté pour chaque destination dans les champs Community *x* (Communauté x), où *x* est un nombre de 1 à 3.

Option	Description
Syslog message (Message syslog)	Cette option force EMX à transmettre automatiquement des messages d'événement au serveur syslog indiqué. ▪ Dans le champ Syslog server, indiquez l'adresse IP à laquelle le message syslog est transmis. ▪ Dans le champ Port, indiquez un numéro de port approprié.
Send SMS message (Envoyer un SMS)	Envoie un texto au téléphone mobile désigné. Un modem Cinterion® GSM MC52i doit être branché sur EMX pour permettre l'envoi de SMS. *Remarque : EMX ne peut pas recevoir de SMS.* *Remarque : seul l'anglais est pris en charge pour les SMS.* • Entrez le numéro de téléphone dans le champ Recipient's Phone Number (Numéro de téléphone du destinataire).
Record Snapshots to Webcam Storage (Enregistrer des instantanés dans la mémoire de la webcam)	Cette option permet de définir une action laissant une webcam particulière prendre des clichés ou l'en empêchant. ▪ Entrez le nombre total d'instantanés à prendre lorsque l'événement se produit. Le nombre maximum d'instantanés pouvant être stockés dans EMX est de 10. Si vous le définissez sur un nombre supérieur, après la prise et le stockage du dixième instantané, les instantanés sont écrasés. ▪ Dans le champ Time before first Snapshot(s): (Temps écoulé avant les premiers instantanés), entrez le nombre de secondes qui doit s'écouler entre le déclenchement de l'événement et le moment où la webcam commence à prendre des clichés. ▪ Dans le champ Time between Snapshots(s): (Durée entre les instantanés), entrez le temps qui doit s'écouler entre la prise de chaque cliché.

Création de courriels personnalisés

Si vous avez décidé d'envoyer des courriels lorsqu'un événement se produit, vous pouvez personnaliser le message à inclure.

Les messages sont composés de texte libre et de marques de réservation EMX. Celles-ci représentent des données extraites du dispositif EMX et insérées dans le message.

Par exemple :

```
[USERNAME] logged into the device on [TIMESTAMP]
```

devient

```
JQPublic logged into the device on 2012-January-30 21:00
(JQPublic s'est connecté au dispositif le 30 janvier 2012
à 21:00)
```

Reportez-vous à ***Marques de réservation de courriel*** (voir "***Marques de réservation de courriels***" à la page 142) pour obtenir la liste et la définition des variables disponibles.

Pour créer un message personnalisé :

1. Cliquez sur Device Settings > Event Rules (Paramètres du dispositif > Règles d'événement).
2. Cliquez sur l'onglet Actions.
3. Dans le volet gauche, sélectionnez l'événement auquel l'action est associée ou créez une action. Reportez-vous à ***Création des actions*** (à la page 136).
4. Sélectionnez Send EMail (Envoyer un courriel) dans le menu déroulant Actions de la section Action Settings (Paramètres des actions) de la boîte de dialogue.
5. Cochez la case Use Custom Log Message (Utiliser un message de journal personnalisé).
6. Créez le message dans le champ de texte ouvert en entrant des données personnalisées. Le cas échéant, utilisez des marques de réservation dans le message.

   Remarque : cliquez sur l'icône Information pour ouvrir la boîte de dialogue Event Context Information (Données contextuelles d'événement) qui contient la liste des marques de réservation et leur définition.

7. Cliquez sur Save (Enregistrer).

Marques de réservation de courriels

Vous trouverez ci-après les marques de réservation qui peuvent être utilisées dans les courriels d'événements.

Remarque : cliquez sur l'icône Information pour ouvrir la boîte de dialogue Event Context Information (Données contextuelles d'événement) qui contient la liste des marques de réservation et leur définition.

Marque de réservation	Description
[ASSERTION]	Indicateur booléen pour l'entrée (1) dans une condition d'événement ou pour la sortie (0) de cette condition
[EXTSENSORNAME]	Nom d'un capteur externe
[EXTSENSORSLOT]	ID de la fente d'un capteur externe
[IFNAME]	Nom lisible par l'utilisateur d'une interface réseau
[VALUE]	Nouvelle valeur d'un paramètre
[VERSION]	Version de firmware vers laquelle le dispositif est mis à niveau
[OLDVERSION]	Version de firmware à partir de laquelle le dispositif est mis à niveau
[PARAMETER]	Nom d'un paramètre de configuration
[PORTID]	Etiquette du port externe auquel le dispositif déclencheur de l'événement est connecté
[PORTTYPE]	Type du port externe (par exemple, de fonction ou auxiliaire) auquel le dispositif déclencheur de l'événement est connecté
[RECIPIENTS]	Liste des destinataires auxquels un message SMTP a été envoyé
[TARGETROLE]	Nom d'un rôle de gestion des utilisateurs auquel une action a été appliquée
[SERVER]	Nom ou adresse IP d'un serveur
[TARGETUSER]	Utilisateur pour lequel une action a été déclenchée
[TIMESTAMP]	Horodateur de l'occurrence de l'événement
[USERIP]	Adresse IP à partir de laquelle un utilisateur est connecté
[USERNAME]	Utilisateur qui a déclenché une action

[LEDCOLOR]	Couleur du voyant RVB
[LEDMODE]	Mode d'indication du voyant
[LEDOPMODE]	Mode de fonctionnement du voyant
[STATE]	Etat lisible par l'utilisateur d'un bandeau de ressources
[RACKUNIT]	Position de l'unité de rack (verticale) à laquelle une action s'applique
[RACKSLOT]	Position de la fente (horizontale) à laquelle une action s'applique
[STRIPNAME]	Nom d'un bandeau de ressources
[STRIPID]	ID numérique d'un bandeau de ressources
[TAGID]	ID d'étiquette de gestion des ressources
[LDAPERRORDESC]	Une erreur LDAP s'est produite
[LHXFANID]	ID d'un ventilateur connecté à un LHX
[LHXPOWERSUPPLYID]	ID de l'alimentation d'un LHX
[LHXSENSORID]	ID de la sonde d'un capteur LHX
[INLETPOLE]	Identifiant d'une ligne d'alimentation d'entrée
[INLETSENSOR]	Nom d'un capteur d'entrée
[INLET]	Etiquette de l'entrée d'alimentation
[OCPSENSOR]	Nom du capteur du dispositif de protection contre les surintensités
[OCP]	Etiquette du dispositif de protection contre les surintensités
[OUTLETPOLE]	Identifiant de la ligne d'alimentation de sortie
[OUTLETSENSOR]	Nom d'un capteur de sortie
[OUTLET]	Etiquette de la sortie
[POLESENSOR]	Nom du capteur d'une ligne d'alimentation particulière

Messages de journaux par défaut

Vous trouverez ci-après les messages de journaux par défaut déclenchés et envoyés par courriel aux destinataires définis lorsque des événements EMX se produisent (TRUE) ou, dans certains cas, ne se produisent pas (FALSE). Reportez-vous à ***Règles et actions d'événement*** (à la page 131) pour en savoir plus sur la configuration des courriels à envoyer lorsque des événements définis se produisent.

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
Dispositif > Système démarré	System started. (Système démarré.)	
Dispositif > Système réinitialisé	System reset performed by user '[USERNAME]' from host '[USERIP]'. (Réinitialisation du système effectuée par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Dispositif > Echec de la validation du firmware	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'. (Echec de la validation du firmware par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Device > Mise à jour du firmware démarrée	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (Mise à niveau du firmware démarrée de la version [OLDVERSION] à la version [VERSION] par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Dispositif > Mise à jour du firmware terminée	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (Firmware mis à niveau de la version [OLDVERSION] à la version [VERSION] par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Dispositif > Echec de la mise à jour du firmware	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (Echec de la mise à niveau du firmware de la version [OLDVERSION] à la version [VERSION] par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Dispositif > Identification du dispositif modifiée	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'. (Paramètre de configuration [PARAMETER] remplacé par [VALUE] par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Dispositif > Journal des	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
événements effacé	(Journal des événements effacé par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Dispositif > Configuration en bloc enregistrée	Bulk configuration saved from host '[USERIP]'. (Configuration en bloc enregistrée depuis l'hôte [USERIP].)	
Dispositif > Configuration en bloc copiée	Bulk configuration copied from host '[USERIP]'. (Configuration en bloc copiée depuis l'hôte [USERIP].)	
Dispositif > Etat de la liaison d'interface réseau est actif	The [IFNAME] network interface link is now up. (La liaison d'interface réseau [IFNAME] est maintenant active.)	The [IFNAME] network interface link is now down. (La liaison d'interface réseau [IFNAME] est maintenant inactive.)
Dispositif > Echec de l'envoi du message SMTP	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed. (L'envoi du message SMTP à [RECIPIENTS] par le biais du serveur [SERVER] a échoué.)	
Dispositif > Une erreur LDAP s'est produite	An LDAP error occured: [LDAPERRORDESC]. (Une erreur LDAP s'est produite : [LDAPERRORDESC].)	
Dispositif > Esclave USB connecté	USB slave connected. (L'esclave USB est connecté.)	USB slave disconnected. (L'esclave USB est déconnecté.)
Dispositif > Fonctions > Prise en charge de Schroff LHX	Schroff LHX support enabled. (La prise en charge de Schroff LHX est activée.)	Schroff LHX support disabled. (La prise en charge de Schroff LHX est désactivée.)
Administration des utilisateurs > Utilisateur ajouté	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'. (Utilisateur [TARGETUSER] ajouté par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Utilisateur modifié	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'. (Utilisateur [TARGETUSER] modifié par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Utilisateur supprimé	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'. (Utilisateur [TARGETUSER] supprimé	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
	par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Mot de passe modifié	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'. (Mot de passe de l'utilisateur [TARGETUSER] modifié par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Paramètres de mot de passe modifiés	Password settings changed by user '[USERNAME]' from host '[USERIP]'. (Paramètres de mot de passe modifiés par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Rôle ajouté	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'. (Rôle [TARGETROLE] ajouté par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Rôle modifié	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'. (Rôle [TARGETROLE] modifié par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Administration des utilisateurs > Rôle supprimé	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'. (Rôle [TARGETROLE] supprimé par l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Activité d'utilisateur > * > Utilisateur connecté	User '[USERNAME]' from host '[USERIP]' logged in. (Utilisateur [USERNAME] de l'hôte [USERIP] connecté.)	User '[USERNAME]' from host '[USERIP]' logged out. (Utilisateur [USERNAME] de l'hôte [USERIP] déconnecté.)
Activité d'utilisateur > * > Echec d'authentification	Authentication failed for user '[USERNAME]' from host '[USERIP]'. (Echec de l'authentification de l'utilisateur [USERNAME] depuis l'hôte [USERIP].)	
Activité d'utilisateur > * > Utilisateur bloqué	User '[USERNAME]' from host '[USERIP]' was blocked. (L'utilisateur [USERNAME] de l'hôte [USERIP] a été bloqué.)	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
Activité d'utilisateur > * > Expiration de session	Session of user '[USERNAME]' from host '[USERIP]' timed out. (La session de l'utilisateur [USERNAME] depuis l'hôte [USERIP] a expiré.)	
Dispositif de protection contre les surintensités > * > Capteur > * > Indisponible	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable. (Capteur [OCPSENSOR] du dispositif de protection contre les surintensités [OCP] indisponible.)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available. (Capteur [OCPSENSOR] du dispositif de protection contre les surintensités [OCP] disponible.)
Fente de capteur externe > * > Capteur numérique > Indisponible	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (Capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] indisponible.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (Capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] disponible.)
Fente de capteur externe > * > Capteur numérique > Au-dessus du seuil critique supérieur	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] affirmé au-dessus du seuil critique supérieur.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] infirmé au-dessus du seuil critique supérieur.)
Fente de capteur externe > * > Capteur numérique > Au-dessus du seuil d'avertissement supérieur	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] affirmé au-dessus du seuil d'avertissement supérieur.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] infirmé au-dessus du seuil d'avertissement supérieur.)
Fente de capteur externe > * > Capteur numérique > Au-dessous du seuil d'avertissement inférieur	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] affirmé au-dessous du seuil d'avertissement inférieur.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] infirmé au-dessous du seuil d'avertissement inférieur.)
Fente de capteur externe > * >	External sensor '[EXTSENSORNAME]'	External sensor

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
Capteur numérique > Au-dessous du seuil critique inférieur	in slot '[EXTSENSORSLOT]' asserted 'below lower critical'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] affirmé au-dessous du seuil critique inférieur.)	'[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'. (Capteur externe [EXTSENSORNAME] dans la fente [EXTSENSORSLOT] infirmé au-dessous du seuil critique inférieur.)
Fente de capteur externe > * > Capteur d'état > Indisponible	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (Capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] indisponible.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (Capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] disponible.)
Fente de capteur externe > * > Capteur d'état > Fermé	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is closed. (Le capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] est fermé.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is open. (Le capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] est ouvert.)
Fente de capteur externe > * > Capteur d'état > Actif	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on. (Le capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] est activé.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is off. (Le capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] est désactivé.)
Fente de capteur externe > * > Capteur d'état > Alarme	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is alarmed. (Le capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] est en état d'alarme.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is no longer alarmed. (Le capteur externe [EXTSENSORNAME] de la fente [EXTSENSORSLOT] n'est plus en état d'alarme.)
Surveillance des serveurs > * > Surveillé	Server '[SERVER]' is now being monitored. (Le serveur [SERVER] est maintenant surveillé.)	Server '[SERVER]' is no longer being monitored. (Le serveur [SERVER] n'est plus surveillé.)
Surveillance des serveurs > * > Inaccessible	Server '[SERVER]' is unreachable. (Le serveur [SERVER] est inaccessible.)	Server '[SERVER]' is reachable. (Le serveur [SERVER] est accessible.)
Gestion des ressources > Etat	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'. (L'état du bandeau des	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
	ressources [STRIPID] ([STRIPNAME]) est devenu [STATE].)	
Gestion des ressources > Unité de rack > * > Etiquette connectée	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (Etiquette de bandeau de ressources avec l'ID [TAGID] connectée à l'unité de rack [RACKUNIT], fente [RACKSLOT] du bandeau de ressources [STRIPID] ([STRIPNAME]).)	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (Etiquette de bandeau de ressources avec l'ID [TAGID] déconnectée de l'unité de rack [RACKUNIT], fente [RACKSLOT] du bandeau de ressources [STRIPID] ([STRIPNAME]).)
Gestion des ressources > Unité de rack > * > Extension de lame connectée	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (Extension de lame avec l'ID [TAGID] connectée à l'unité de rack [RACKUNIT] du bandeau de ressources [STRIPID] ([STRIPNAME]).)	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (Extension de lame avec l'ID [TAGID] déconnectée de l'unité de rack [RACKUNIT] du bandeau de ressources [STRIPID] ([STRIPNAME]).)
Gestion des ressources > Mise à jour du firmware	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'. (Mise à jour du firmware pour le bandeau de ressources [STRIPID] ([STRIPNAME]) : statut est devenu [STATE].)	
Gestion des ressources > Configuration du dispositif modifiée	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'. (Paramètre de configuration [PARAMETER] du bandeau de ressources [STRIPID] ([STRIPNAME]) remplacé par [VALUE] par l'utilisateur [USERNAME].)	
Gestion des ressources > Configuration de l'unité de rack modifiée	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]' (Configuration de l'unité de rack [RACKUNIT] du bandeau de ressources [STRIPID] ([STRIPNAME])	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
	modifiée par l'utilisateur [USERNAME] comme suit : Mode de fonctionnement du voyant [LEDOPMODE], Couleur du voyant [LEDCOLOR], Mode du voyant [LEDMODE])	
Gestion des ressources > Dépassement de capacité d'extension de lame	Blade extension overflow occured on strip [STRIPID] ('[STRIPNAME]'). (Un dépassement de capacité de l'extension de lame s'est produit sur le bandeau [STRIPID] ([STRIPNAME]).)	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]'). (Dépassement de capacité de l'extension de lame corrigé sur le bandeau [STRIPID] ([STRIPNAME]).)
Gestion des ressources > Composition de bandeau de ressources composite modifiée	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]'). (Composition modifiée sur le bandeau de ressources composite [STRIPID] ([STRIPNAME]).)	
**LHX > Connecté	LHX has been connected to [PORTTYPE] port [PORTID]. (LHX a été connecté au port [PORTID] de type [PORTTYPE].)	LHX has been disconnected to [PORTTYPE] port [PORTID]. (LHX a été disconnecté du port [PORTID] de type [PORTTYPE].)
**LHX > Etat fonctionnel	LHX connected to [PORTTYPE] port [PORTID] has been switched on. (LHX connecté au port [PORTID] de type [PORTTYPE] a été mis sous tension.)	LHX connected to [PORTTYPE] port [PORTID] has been switched off. (LHX connecté au port [PORTID] de type [PORTTYPE] a été mis hors tension.)
**LHX > Capteur > Indisponible	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] indisponible.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] disponible.)
**LHX > Capteur > Au-dessus du seuil critique supérieur	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] affirmé au-dessus du seuil critique supérieur.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] infirmé au-dessus du seuil critique supérieur.)
**LHX > Capteur > Au-dessus du seuil d'avertissement supérieur	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'. (Capteur [LHXSENSORID] sur LHX au port

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
	affirmé au-dessus du seuil d'avertissement supérieur.)	[PORTID] de type [PORTTYPE] infirmé au-dessus du seuil d'avertissement supérieur.)
**LHX > Capteur > Au-dessous du seuil d'avertissement inférieur	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] affirmé au-dessous du seuil d'avertissement inférieur.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] infirmé au-dessous du seuil d'avertissement inférieur.)
**LHX > Capteur > Au-dessous du seuil critique inférieur	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] affirmé au-dessous du seuil critique inférieur.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'. (Capteur [LHXSENSORID] sur LHX au port [PORTID] de type [PORTTYPE] infirmé au-dessous du seuil critique inférieur.)
**LHX > Système de refroidissement de secours	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated. (Le système de refroidissement de secours sur LHX au port [PORTID] de type [PORTTYPE] a été activé.)	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated. (Le système de refroidissement de secours sur LHX au port [PORTID] de type [PORTTYPE] a été désactivé.)
**LHX > Demande de refroidissement maximum	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'. (Un refroidissement maximum a été demandé pour LHX au port [PORTID] de type [PORTTYPE].)	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'. (Un refroidissement maximum n'est plus demandé pour LHX au port [PORTID] de type [PORTTYPE].)
**LHX > Perte de données de paramètre	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'. (Une perte de données dans la mémoire de paramètre a été détectée sur LHX au port [PORTID] de type [PORTTYPE].)	
**LHX > Erreur de communication ST-Bus	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'. (Une erreur de communication ST-Bus a été détectée sur LHX au port [PORTID] de type [PORTTYPE].)	
**LHX > Défaillance collective	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'. (Une défaillance collective s'est produite sur	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
	LHX au port [PORTID] de type [PORTTYPE].)	
**LHX > Contact de porte	The door of LHX at [PORTTYPE] port '[PORTID]' was opened. (La porte de LHX au port [PORTID] de type [PORTTYPE] a été ouverte.)	The door of LHX at [PORTTYPE] port '[PORTID]' was closed. (La porte de LHX au port [PORTID] de type [PORTTYPE] a été fermée.)
**LHX > Panne de capteur	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'. (Une panne de capteur (rupture ou court-circuit) s'est produite sur LHX au port [PORTID] de type [PORTTYPE], au niveau du capteur [LHXSENSORID].)	
**LHX > Panne de ventilateur	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'. (Une panne de moteur de ventilateur s'est produite sur LHX au port [PORTID] de type [PORTTYPE], au niveau du ventilateur [LHXFANID].)	
**LHX > Panne d'alimentation	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'. (Une panne d'alimentation s'est produite sur LHX au port [PORTID] de type [PORTTYPE], au niveau de l'alimentation [LHXPOWERSUPPLYID].)	
**LHX > Seuil d'humidité	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (Le seuil d'humidité sur LHX au port [PORTID] de type [PORTTYPE] a été franchi.)	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (L'humidité sur LHX au port [PORTID] de type [PORTTYPE] est dans les limites de seuil.)
**LHX > Panne du refroissement par eau externe	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'. (Une panne du refroissement par eau externe s'est produite sur LHX au port [PORTID] de type [PORTTYPE].)	

Evénement/contexte	Message d'affirmation par défaut quand Evénement = TRUE	Message d'affirmation par défaut quand Evénement = FALSE*
**LHX > Fuite d'eau	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'. (Une fuite d'eau a été détectée sur LHX au port [PORTID] de type [PORTTYPE].)	

**Remarque : Non défini pour les événements déclencheurs (voir [ASSERTION] ctx)*

***Remarque : les événements LHX sont disponibles uniquement si l'option Schroff LHX Support (Prise en charge de Schroff LHX) est activée.*

Exemples de règles d'événement

Exemple de règle d'événement au niveau de la gestion des ressources

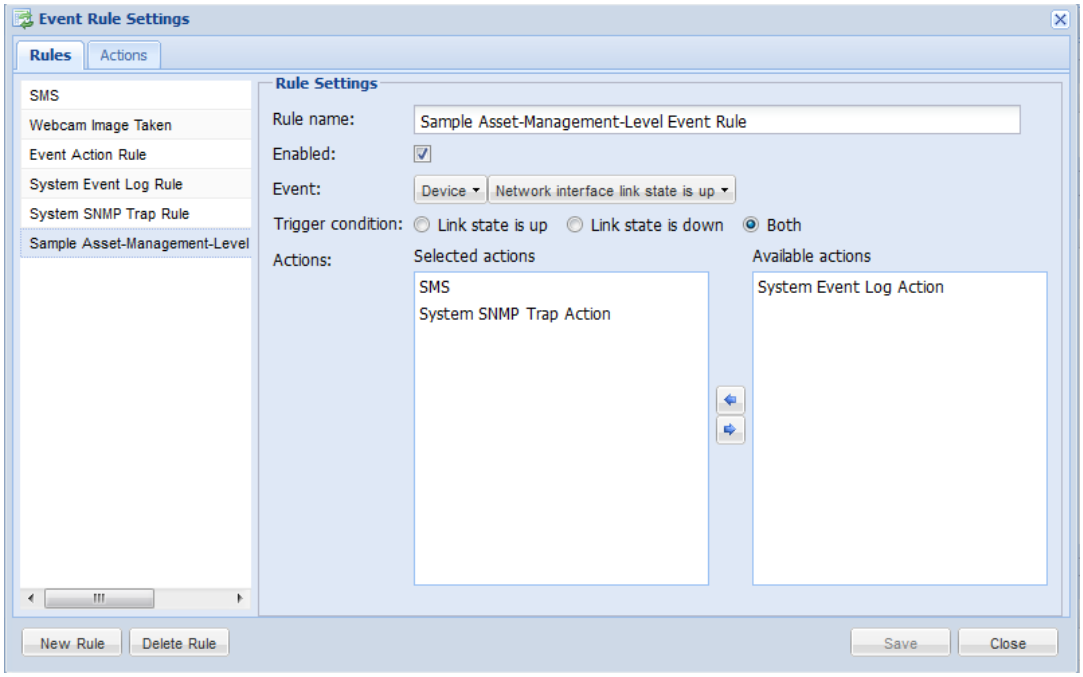
Dans cet exemple, nous voulons que EMX enregistre dans le journal interne l'état actif ou inactif d'une liaison réseau de capteur de ressources. La règle d'événement se présente comme suit :

- Evénement : Device > Network interface link state is up (Dispositif > Etat de la liaison d'interface réseau est actif)
- Trigger condition (Condition de déclenchement) : Both (Les deux)
- Actions : System Event Log Action (Action de journal des événements système)

Pour créer la règle d'événement précédente :

1. Entrez le nom de la règle.
2. Cochez la case Enabled (Activée) pour activer cette règle.
3. Dans le menu déroulant Event, sélectionnez Device > Network interface link state is up. Ces sélections indiquent que nous définissons un événement concernant la gestion des capteurs de ressources et que nous souhaitons que le dispositif EMX réponde à l'événement relatif à des connexions et/ou à des déconnexions physiques.
4. Sélectionnez la case d'option Both (Les deux) puisque nous souhaitons l'enregistrement des actions de connexion et de déconnexion lorsqu'une de ces actions se produit.

5. Sélectionnez System Event Log Action (Action de journal des événements système) puisque nous souhaitons enregistrer cet événement dans le journal interne lorsque les événements spécifiés se produisent.



Exemple de règle d'événement au niveau du capteur

Dans cet exemple, nous souhaitons que le dispositif EMX envoie des traps SNMP au gestionnaire SNMP lorsque le relevé du capteur de température connecté au port nº 1 dépasse un seuil ou lorsque le capteur n'est pas disponible. Pour cela, nous paramétrons la règle d'événement suivante :

- Evénement : External sensor slot > Slot 1 > Numeric Sensor > Any sub-event (Fente de capteur externe > Fente 1 > Capteur numérique > N'importe quel sous-événement)
- Actions : System SNMP Trap Action (Action de traps SNMP système)

Pour créer la règle d'événement précédente :

1. Sélectionnez External sensor slot dans le champ Event pour indiquer que nous définissons un événement au niveau du capteur d'environnement.
2. Sélectionnez Slot 1 dans le sous-menu car nous sommes intéressés par le capteur connecté au port de capteur nº 1.

3. Sélectionnez Numeric Sensor pour indiquer qu'il s'agit d'un capteur numérique.

   Remarque : un capteur numérique utilise des valeurs numériques pour indiquer des conditions d'environnement, alors qu'un capteur discret (activé/désactivé) utilise des caractères alphabétiques pour indiquer l'état.

4. Sélectionnez <Any sub-event> car nous souhaitons inclure tous les événements relatifs au capteur connecté au port nº 1, notamment l'état de non disponibilité du capteur et les dépassements de seuil, Above upper critical (Au-dessus du seuil critique supérieur), Above upper warning (Au-dessus du seuil d'avertissement supérieur), Below lower warning (Sous le seuil d'avertissement inférieur) et Below lower critical (Sous le seuil critique inférieur).
5. Sélectionnez System SNMP Trap Action pour envoyer des traps SNMP afin de répondre aux événements indiqués lorsqu'ils se produisent.

Exemple de règle d'événement au niveau de l'activité de l'utilisateur

Dans cet exemple, nous souhaitons que EMX enregistre un événement d'activité de l'utilisateur dans le journal interne lorsqu'un utilisateur se connecte ou se déconnecte. La règle d'événement est définie comme suit :

- Evénement : User activity > Any user > User logged in (Activité d'utilisateur > N'importe quel utilisateur > Utilisateur connecté)
- Trigger condition (Condition de déclenchement) : Both (Les deux)
- Actions : System Event Log Action (Action de journal des événements système)

Pour créer la règle d'événement précédente :

1. Sélectionnez User Activity dans le champ Event afin d'indiquer que nous définissons un événement concernant une activité d'utilisateur.
2. Sélectionnez <Any user> dans le sous-menu car nous souhaitons enregistrer l'activité de tous les utilisateurs.
3. Sélectionnez User logged in pour sélectionner les événements liés à la connexion des utilisateurs.
4. Sélectionnez la case d'option Both puisque nous souhaitons l'enregistrement des actions de connexion et de déconnexion lorsqu'un de ces événements se produit.
5. Sélectionnez System Event Log Action (Action de journal des événements système) puisque nous souhaitons enregistrer cet événement dans le journal interne lorsque les événements spécifiés se produisent.

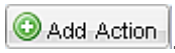
Modification d'une règle d'événement

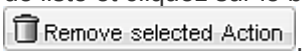
Vous pouvez modifier l'événement, l'action et la condition de déclenchement et d'autres paramètres d'une règle d'événement.

Exception : les événements et les actions sélectionnés dans les règles d'événement intégrées ne sont pas modifiables, notamment System Event Log Rule et System SNMP Trap Rule.

Pour modifier une règle d'événement :

1. Choisissez Device Settings > Event Rules (Paramètres du dispositif > Règles d'événement). La fenêtre Event Rule Settings (Paramètres des règles d'événement) s'affiche.
2. Dans l'onglet Rules (Règles), sélectionnez la règle d'événement que vous souhaitez modifier dans le volet de gauche.
3. Pour désactiver la règle d'événement, désélectionnez la case à cocher Enabled (Activé).
4. Pour modifier l'événement, cliquez sur l'onglet souhaité du champ Event (Evénement) et sélectionnez un élément différent dans le menu ou sous-menu déroulant.

   Par exemple, dans une règle d'événement d'activité pour l'utilisateur admin, vous pouvez cliquer sur l'onglet admin pour afficher un sous-menu déroulant présentant tous les noms d'utilisateur, puis sélectionner un nom d'utilisateur différent ou tous les noms d'utilisateur (option <*Any user*> (N'importe quel utilisateur)).
5. Si des cases d'option sont disponibles, vous pouvez modifier la sélection actuelle pour changer la condition de déclenchement de la règle.
6. Pour modifier les actions, effectuez une des opérations suivantes dans le champ Actions :
   - Pour ajouter une nouvelle action, cliquez sur la flèche déroulante, sélectionnez l'action dans la liste et cliquez sur le bouton Add Action (Ajouter l'action) 

.
   - Pour supprimer une action ajoutée, sélectionnez-la dans la zone de liste et cliquez sur le bouton Remove selected Action 

.
7. Cliquez sur Save pour enregistrer les modifications.

Remarque : si vous ne cliquez pas sur Save (Enregistrer) avant de quitter la page de paramètres active, un message apparaît. Cliquez alors sur Yes pour enregistrer les modifications, sur Discard (Refuser) pour les abandonner ou sur Cancel (Annuler) pour retourner sur la page des paramètres active.

8. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Modification d'une action

Une action existante peut être modifiée afin que toutes les règles d'événement dans laquelle cette action est impliquée changent leur comportement en conséquence.

Exception : l'action intégrée System Event Log Action ne peut pas être modifiée par l'utilisateur.

Pour modifier une action :

1. Choisissez Device Settings > Event Rules (Paramètres du dispositif > Règles d'événement). La fenêtre Event Rule Settings (Paramètres des règles d'événement) s'affiche.
2. Cliquez sur l'onglet Actions.
3. Sélectionnez l'action que vous souhaitez modifier dans la liste de gauche.
4. Apportez les modifications nécessaires aux informations affichées.
5. Cliquez sur Save pour enregistrer les modifications.

   Remarque : si vous ne cliquez pas sur Save (Enregistrer) avant de quitter la page de paramètres active, un message apparaît. Cliquez alors sur Yes pour enregistrer les modifications, sur Discard (Refuser) pour les abandonner ou sur Cancel (Annuler) pour retourner sur la page des paramètres active.

6. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Suppression d'une règle ou d'une action d'événement

Lorsqu'une règle ou une action d'événement est obsolète, il vous suffit de la retirer.

Remarque : vous ne pouvez pas supprimer les règles et les actions d'événement intégrées.

Pour supprimer une règle ou une action d'événement :

1. Choisissez Device Settings > Event Rules (Paramètres du dispositif > Règles d'événement). La fenêtre Event Rule Settings (Paramètres des règles d'événement) s'affiche.
2. Pour supprimer une règle d'événement :
   a. Vérifiez que l'onglet Rules (Règles) est sélectionné. Sinon, cliquez dessus.
   b. Sélectionnez la règle souhaitée dans la liste à gauche, puis cliquez sur Delete Rule (Supprimer la règle).

c. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.

3. Pour supprimer une action :

   a. Cliquez sur l'onglet Actions.

   b. Sélectionnez la règle souhaitée dans la liste à gauche, puis cliquez sur Delete Action (Supprimer l'action).

   c. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.

4. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Remarque à propos des règles non déclenchées

Dans certains cas, une mesure dépasse un seuil et provoque la génération d'une alerte par EMX. La mesure retourne ensuite à une valeur respectant le seuil, mais EMX ne génère pas d'alerte pour l'événement d'infirmation. Ces scénarios peuvent se produire en raison du suivi d'hystérésis utilisé par EMX. Reportez-vous à ***Hystérésis d'infirmation : définition*** (à la page 178).

Journalisation des événements

Par défaut, EMX capture certains événements système et les enregistre dans un journal des événements local (interne).

Consultation du journal local des événements

Vous pouvez afficher jusqu'à 2 000 événements historiques qui se sont produits sur le dispositif EMX dans le journal local des événements.

Lorsque le journal contient déjà 2 000 entrées, chaque nouvelle entrée remplace l'entrée la plus ancienne.

Pour afficher le journal local :

1. Choisissez Maintenance > View Event Log (Maintenance > Afficher le journal des événements). La boîte de dialogue Event Log (Journal des événements) apparaît.

   Chaque entrée d'événement du journal local comprend :

   - la date et l'heure de l'événement ;
   - le type de l'événement ;
   - une description de l'événement.
   - le numéro d'identification de l'événement.

2. La boîte de dialogue affiche la dernière page par défaut. Vous pouvez :

- alterner entre différentes pages en effectuant une des opérations suivantes :

  - Cliquez sur ⏮ ou sur ⏭ pour aller à la première ou à la dernière page.

  - Cliquez sur ◀ ou sur ▶ pour aller à la page précédente ou à la suivante.

  - Tapez un nombre dans la zone de texte Page et appuyez sur Entrée pour aller à une page spécifique.

- Sélectionnez une entrée de journal dans la liste et cliquez sur Show Details (Afficher les détails), ou double-cliquez simplement sur l'entrée pour afficher des informations détaillées.

Remarque : si la boîte de dialogue est trop étroite, il arrive parfois que l'icône » remplace le bouton Show Details. Dans ce cas, cliquez sur » et sélectionnez Show Details pour afficher les détails.

- Cliquez sur ⏭ pour consulter les derniers événements.

3. Agrandissez la boîte de dialogue si nécessaire.
4. Vous pouvez retrier la liste ou modifier les colonnes affichées.
5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Effacement des entrées d'événement

S'il n'est pas nécessaire de conserver l'historique des événements, vous pouvez le retirer entièrement du journal local.

Pour supprimer toutes les entrées d'événement :

1. Choisissez Maintenance > View Event Log (Maintenance > Afficher le journal des événements). La boîte de dialogue Event Log (Journal des événements) apparaît.
2. Cliquez sur Clear Event Log (Effacer le journal des événements).
3. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Consultation du journal de communication

EMX permet d'inspecter toutes les communications qui se sont produites entre le dispositif EMX et son interface utilisateur graphique (GUI). Les données sont généralement utiles pour les ingénieurs du support technique uniquement et vous n'aurez sans doute pas besoin de les consulter.

Cette fonction est accessible uniquement aux utilisateurs disposant de privilèges d'administration.

Pour afficher le journal de communication :

1. Choisissez Maintenance > View Communication Log (Afficher le journal de communication). La boîte de dialogue Communication Log (Journal de communication) apparaît.
2. La boîte de dialogue affiche la dernière page par défaut. Vous pouvez :
   - alterner entre différentes pages en effectuant une des opérations suivantes :

     - Cliquez sur ⏮ ou sur ⏭ pour aller à la première ou à la dernière page.

     - Cliquez sur ◀ ou sur ▶ pour aller à la page précédente ou à la suivante.

     - Tapez un nombre dans la zone de texte Page et appuyez sur Entrée pour aller à une page spécifique.
   - Sélectionnez une entrée de journal dans la liste et cliquez sur Show Details (Afficher les détails), ou double-cliquez simplement sur l'entrée pour afficher des informations détaillées.

   Remarque : si la boîte de dialogue est trop étroite, il arrive parfois que l'icône » remplace le bouton Show Details. Dans ce cas, cliquez sur » et sélectionnez Show Details pour afficher les détails.
3. Pour mettre immédiatement à jour le journal de communication, cliquez sur .
4. Pour enregistrer le journal de communication sur votre ordinateur, cliquez sur .
5. Agrandissez la boîte de dialogue si nécessaire.
6. Vous pouvez retrier la liste ou modifier les colonnes affichées.
7. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Chapitre 8 Gestion des dispositifs externes

Dans ce chapitre

Aperçu

EMX permet de surveiller les dispositifs et les conditions dans votre centre de données, telles que le statut des serveurs, les conditions d'environnement, etc. à l'aide de capteurs et de dispositifs tiers.

Vous pouvez également utiliser une webcam pour visualiser l'activité du centre de données et un modem GSM pour envoyer des SMS lorsqu'un événement particulier se produit.

Accessibilité du serveur

Vous pouvez surveiller l'activité de dispositifs informatiques spécifiques en définissant l'exécution continue par le dispositif EMX de tests ping. La réponse d'un dispositif informatique aux commandes ping indique qu'il est toujours actif et accessible à distance.

Cette fonction est particulièrement utile lorsque vous vous trouvez dans une zone sans connectivité Internet.

Ajout de dispositifs informatiques pour la surveillance par test ping

Vous pouvez charger EMX de surveiller l'accessibilité d'un équipement informatique, tel que des serveurs de base de données et des serveurs d'authentification à distance.

Pour ajouter un équipement informatique à la surveillance par test ping :

1. Choisissez Device Settings > Server Reachability (Paramètres du dispositif > Accessibilité du serveur). La boîte de dialogue Server Reachability apparaît.
2. Cliquez sur New (Nouveau). La boîte de dialogue Add New Server (Ajouter un nouveau serveur) apparaît.

3. Par défaut, la case Enable Ping Monitoring for this Server (Activer la surveillance par test ping pour ce serveur) est cochée. Si ce n'est pas le cas, cochez-la pour activer la fonction de surveillance par test ping.
4. Donnez les informations demandées.

Champ	Description
IP Address/Hostname (Adresse IP/Nom d'hôte)	Adresse IP ou nom d'hôte de l'équipement informatique dont vous souhaitez surveiller l'accessibilité.
Number of Successful Pings to Enable Feature (Nombre de tests ping réussis pour activer la fonction)	Nombre de tests ping réussis nécessaires pour activer cette fonction. La plage valide est comprise entre 0 et 200.
Wait Time (in seconds) after Successful Ping (Délai (en secondes) après un test ping réussi)	Le délai d'attente avant l'envoi de la commande ping suivante si la précédente a reçu une réponse. La plage valide est comprise entre 5 et 600 (secondes).
Wait Time (in seconds) after Unsuccessful Ping (Délai (en secondes) après l'échec d'un test ping)	Le délai d'attente avant l'envoi de la commande ping suivante si la précédente n'a pas reçu de réponse. La plage valide est comprise entre 3 et 600 (secondes).
Number of Consecutive Unsuccessful Pings for Failure (Nombre de tests pings consécutifs sans réponse pour indiquer une panne)	Nombre de tests ping consécutifs sans réponse pour déclarer l'équipement informatique inactif. La plage valide est comprise entre 1 et 100.
Wait Time (in seconds) before Resuming Pinging (Délai (en secondes) avant la reprise des tests ping)	Délai avant la reprise des tests ping après qu'un équipement informatique a été déclaré inactif. La plage valide est comprise entre 1 et 1200 (secondes).

5. Cliquez sur OK pour enregistrer les modifications.
6. Pour ajouter des dispositifs informatiques supplémentaires, répétez les étapes 2 à 5.

7. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Modification des paramètres de surveillance par test ping

Vous pouvez apporter à tout moment les modifications nécessaires aux paramètres de surveillance par test ping pour n'importe quel dispositif informatique.

Pour modifier les paramètres de surveillance par test ping d'un dispositif informatique :

1. Choisissez Device Settings > Server Reachability (Paramètres du dispositif > Accessibilité du serveur). La boîte de dialogue Server Reachability apparaît.
2. Sélectionnez le dispositif informatique dont vous souhaitez modifier les paramètres en cliquant dessus.
3. Cliquez sur Edit (Modifier) ou double-cliquez sur le dispositif informatique. La boîte de dialogue Edit Server 'XXX' (Modifier le serveur XXX, où XXX représente l'adresse IP ou le nom d'hôte du dispositif informatique.
4. Modifiez les informations affichées.
5. Cliquez sur OK pour enregistrer les modifications.

Suppression des paramètres de surveillance par test ping

Lorsque la surveillance de l'accessibilité d'un dispositif informatique n'est pas nécessaire, il vous suffit de la supprimer.

Pour supprimer les paramètres de surveillance par test ping d'un dispositif informatique :

1. Choisissez Device Settings > Server Reachability (Paramètres du dispositif > Accessibilité du serveur). La boîte de dialogue Server Reachability apparaît.
2. Sélectionnez le dispositif informatique dont vous souhaitez supprimer les paramètres de surveillance par test ping en cliquant dessus. Pour effectuer plusieurs sélections, appuyez sur Ctrl+cliquez ou sur Maj+cliquez pour mettre en surbrillance plusieurs éléments.
3. Cliquez sur Delete (Supprimer).
4. Le message qui s'affiche vous invite à confirmer l'opération. Cliquez sur Yes (Oui) pour confirmer la suppression.
5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Vérification des états de surveillance des serveurs

Les résultats de la surveillance des serveurs sont disponibles dans la boîte de dialogue Server Reachability (Accessibilité des serveurs) après la définition des serveurs à surveiller par le dispositif EMX.

Pour vérifier les états et les résultats de la surveillance des serveurs :

1. Choisissez Device Settings > Server Reachability (Paramètres du dispositif > Accessibilité du serveur). La boîte de dialogue Server Reachability apparaît.
2. La colonne libellée Ping Enabled (Ping activé) indique si la surveillance du serveur correspondant est activée.
   - : cette icône indique que la surveillance du serveur correspondant est activée.
   - : cette icône indique que la surveillance du serveur correspondant est désactivée.
3. La colonne libellée Status (Statut) indique l'accessibilité de chaque serveur surveillé.

Statut	Description
Accessible	Le serveur est accessible.
Inaccessible	Le serveur est inaccessible.
En attente de connexion fiable	La connexion entre le dispositif EMX et le serveur n'est pas encore établie.

4. Vous pouvez modifier l'ordre de tri de la liste, si nécessaire. Reportez-vous à Modification du tri.
5. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Capteurs d'environnement

EMX peut contrôler les conditions d'environnement, telles que la température et l'humidité, à l'endroit où les capteurs d'environnement sont placés.

Pour ajouter des capteurs d'environnement :

1. Connectez physiquement des capteurs d'environnement au dispositif EMX. Reportez-vous à ***Connexion de capteurs d'environnement (facultatif)*** (à la page 31).
2. Connectez-vous à l'interface Web de EMX. EMX devrait avoir détecté les capteurs connectés et les afficher dans l'interface Web.

3. Identifiez chaque capteur par son numéro de série. Reportez-vous à ***Identification des capteurs d'environnement*** (à la page 165).
4. EMX devrait automatiquement gérer les capteurs détectés. Vérifiez si c'est le cas. Sinon, paramétrez leur gestion. Reportez-vous à ***Gestion des capteurs d'environnement*** (à la page 166).
5. Configurez les capteurs. Reportez-vous à ***Configuration des capteurs d'environnement*** (à la page 168). Les étapes sont les suivantes :
   a. Nommez le capteur.
   b. Si le capteur connecté est un capteur de fermeture de contact Raritan, indiquez un type de capteur approprié.
   c. Marquez l'emplacement physique du capteur dans le rack ou dans la salle.
   d. Pour un capteur numérique, configurez les paramètres de seuil, d'hystérésis et de délai d'affirmation.

Remarque : les capteurs numériques utilisent des valeurs numériques pour indiquer des conditions d'environnement ou internes, alors que les capteurs discrets (activé/désactivé) utilisent des caractères alphabétiques pour indiquer l'état. Seuls les capteurs numériques utilisent des paramètres de seuil.

Identification des capteurs d'environnement

Le câble d'un capteur d'environnement comporte une étiquette avec un numéro de série.

Le numéro de série de chaque capteur est répertorié dans l'interface Web après la détection de chaque capteur par EMX.

#.	Port	Serial Number	Type	Channel	Name	Reading	State
1		PRB1390001	Air Flow		Air Flow 1		unavailable
2	5	AEI8850019	Temperature		Temperature 1	25.8 °C	normal
3	5	AEI8850019	Humidity		Humidity 1	45 %	normal
4	CC1	PRC1600001	Contact (On/Off)	1	On/Off 1		normal
5	CC2	PRC1600001	Contact (On/Off)	2	On/Off 2		normal

Faites correspondre le numéro de série de l'étiquette à ceux répertoriés dans le tableau des capteurs.

Notez que les informations des colonnes # et Port sont différentes.

Colonne	Informations
#	Numéro d'identification attribué à chaque capteur d'environnement.
Port	Numéro du port SENSOR auquel chaque capteur d'environnement sélectionné est physiquement connecté. CC1 et CC2 se rapportent à la terminaison du capteur de fermeture de contact embarqué.

Gestion des capteurs d'environnement

EMX commence à extraire le relevé et/ou l'état d'un capteur d'environnement et consigne les transitions d'état après que le capteur passe sous sa gestion.

Lorsqu'un concentrateur de capteurs Raritan est utilisé, vous pouvez connecter jusqu'à 16 capteurs d'environnement par port SENSOR. C'est-à-dire,

- Sur EMX2-111, qui n'a qu'un port SENSOR, 16 capteurs d'environnement au plus peuvent être connectés.
- Sur EMX2-888, qui a huit ports SENSOR, 128 capteurs d'environnement au plus peuvent être connectés. Comme le dispositif EMX2-888 est mis en œuvre avec deux canaux de terminaison de fermeture de contact embarqué, il prend en charge jusqu'à 130 capteurs d'environnement.
- Chaque port SENSOR peut uniquement prendre en charge un maximum de deux capteurs de fermeture de contact Raritan, qui utilise l'intervalle de mise à jour le plus court de tous les capteurs Raritan. Reportez-vous à ***Informations sur l'intervalle de mise à jour*** (à la page 172).

Lorsque le nombre total de capteurs gérés n'a pas atteint le maximum, EMX assure automatiquement la gestion des capteurs d'environnement détectés. Vous n'aurez à gérer un capteur manuellement que s'il n'est pas sous gestion.

Pour gérer manuellement un capteur d'environnement :

1. Si le dossier EMX est réduit, développez-le pour afficher tous les composants.

Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur le dossier External Sensors (Capteurs externes) dans le volet EMX Explorer et la page External Sensors s'ouvre dans le volet de droite.
3. Cliquez sur le capteur à gérer sur la page External Sensors (Capteurs externes).

Remarque : pour identifier tous les capteurs détectés, reportez-vous à **Identification des capteurs d'environnement** *(à la page 165).*

4. Cliquez sur Manage (Gérer). La boîte de dialogue Manage sensor (Gérer le capteur) <numéro de série> (<type de capteur>) apparaît, où <numéro de série> indique le numéro de série du capteur et <type de capteur>, le type du capteur.

Remarque : Pour un capteur de fermeture de contact, un numéro de canal est ajouté à la fin du <type de capteur>.

5. Il existe deux manières de gérer le capteur :
   - Pour gérer ce capteur en laissant EMX lui attribuer un numéro, sélectionnez Automatically assign a sensor number (Attribuer un numéro de capteur automatiquement). Cette méthode ne libère aucun capteur géré.
   - Pour gérer ce capteur en lui attribuant le numéro de votre choix, sélectionnez Manually select a sensor number (Sélectionner manuellement un numéro de capteur). Cliquez ensuite sur la flèche déroulante pour sélectionner un numéro.

     Si le numéro que vous avez sélectionné est déjà attribué à un capteur, ce dernier est libéré après avoir perdu ce numéro d'identification.

Conseil : les informations entre parenthèses après chaque numéro d'identification indique si ce nombre a été attribué à un capteur. Si tel est le cas, le numéro de série du capteur est affiché. Sinon, le terme unused (inutilisé) apparaît.

6. Cliquez sur OK. EMX démarre le suivi et l'affichage du relevé et/ou de l'état du capteur géré.
7. Pour gérer des capteurs supplémentaires, répétez les étapes 3 à 6.

Remarque : lorsque le nombre de capteurs gérés atteint le maximum, vous NE POUVEZ gérer des capteurs supplémentaires que si vous supprimez ou remplacez des capteurs gérés. Pour supprimer un capteur, reportez-vous à **Annulation de la gestion des capteurs d'environnement** *(à la page 177).*

Configuration des capteurs d'environnement

Vous pouvez modifier le nom par défaut pour identifier facilement le capteur géré et décrire son emplacement à l'aide des coordonnées X, Y et Z.

Pour configurer des capteurs d'environnement :

1. Si le dossier EMX est réduit, développez-le pour afficher tous les composants.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur le dossier External Sensors (Capteurs externes) dans le volet EMX Explorer et la page External Sensors s'ouvre dans le volet de droite.
3. Sélectionnez le capteur que vous souhaitez configurer.
4. Cliquez sur Setup (Paramétrer). La boîte de dialogue Setup of external sensor (Paramétrage du capteur externe) <numéro de série> (<type de capteur>) apparaît, où <numéro de série> indique le numéro de série du capteur et <type de capteur>, son type.

   Conseil : vous pouvez également ouvrir cette boîte de dialogue de paramétrage en sélectionnant l'icône du capteur d'environnement souhaité dans l'arborescence, puis en cliquant sur Setup (Paramétrer) sur la page du capteur ouverte dans le volet de droite.

5. Si le capteur d'environnement sélectionné est le capteur de fermeture de contact Raritan connecté à un détecteur/commutateur tiers, sélectionnez le type de capteur approprié dans le champ Binary Sensor Subtype (Sous-type de capteur binaire).
   - Contact : le détecteur/commutateur est conçu pour détecter le statut porte verrouillée ou porte fermée/ouverte.
   - Smoke Detection (Détection de fumée) : le détecteur/commutateur est conçu pour détecter la présence de fumée.
   - Water Detection (Détection d'eau) : le détecteur/commutateur est conçu pour détecter la présence d'eau à terre.
   - Vibration : le détecteur/commutateur est conçu pour détecter les vibrations du sol.
6. Tapez un nouveau nom dans le champ Name (Nom).
7. Décrivez l'emplacement du capteur en affectant des valeurs alphanumériques aux coordonnées X, Y et Z. Reportez-vous à ***Description de l'emplacement des capteurs*** (à la page 170).

8. Si le capteur d'environnement sélectionné est un capteur numérique, ses paramètres de seuil sont affichés dans la boîte de dialogue. Cliquez sur Edit (Modifier) ou double-cliquez sur le tableau Threshold Configuration (Configuration des seuils) pour ajuster les paramètres de seuil, d'hystérésis d'infirmation et de délai d'affirmation.
   - Pour activer un seuil, sélectionnez la case à cocher correspondante. Pour désactiver un seuil, décochez la case.
   - Après l'activation d'un seuil, tapez une valeur numérique appropriée dans la zone de texte correspondante.
   - Pour activer l'hystérésis d'infirmation pour tous les seuils, tapez une valeur numérique différente de zéro dans le champ Deassertion Hysteresis. Reportez-vous à ***Hystérésis d'infirmation : définition*** (à la page 178).
   - Pour activer le délai d'affirmation pour tous les seuils, tapez une valeur numérique différente de zéro dans le champ Assertion Timeout (samples) (Délai d'affirmation (échantillons)). Reportez-vous à ***Délai d'affirmation : définition*** (à la page 179).

   Les valeurs Upper Critical (critique supérieur) et Lower Critical (critique inférieur) sont des points auxquels le dispositif EMX considère que l'environnement d'exploitation est critique et en dehors de la plage du seuil acceptable.
9. Cliquez sur OK pour enregistrer les modifications.

Définition du format de la coordonnée Z

Vous pouvez utiliser le nombre d'unités de rack ou un texte descriptif pour indiquer les emplacements verticaux (coordonnées Z) des capteurs d'environnement.

Pour déterminer le format de la coordonnée Z :

1. Dans le volet de navigation gauche, cliquez sur le dossier EMX. La page Settings (Paramètres) s'ouvre.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*
2. Cliquez sur Setup (Paramétrer) dans la page Settings. La boîte de dialogue EMX Setup (Paramétrage du dispositif EMX) apparaît.
3. Dans le champ External sensors Z coordinate format (Format de la coordonnée Z des capteurs externes), cliquez sur la flèche déroulante et sélectionnez une option dans la liste.

- Rack Units (Unités de rack) : la hauteur de la coordonnée Z est mesurée en unités de rack standard. Lorsque cette option est sélectionnée, vous pouvez taper une valeur numérique dans l'unité de rack afin de décrire la coordonnée Z d'un capteur d'environnement.
- Free-Form (Forme libre) : une chaîne alphanumérique quelconque peut être utilisée pour spécifier la coordonnée Z.

4. Cliquez sur OK pour enregistrer les modifications.

Description de l'emplacement des capteurs

Utilisez les coordonnées X, Y et Z pour décrire l'emplacement physique de chaque capteur. Vous pouvez utiliser ces valeurs d'emplacement pour assurer le suivi des enregistrements des conditions d'environnement dans des endroits fixes autour de votre équipement informatique. Les valeurs X, Y et Z servent d'attributs supplémentaires et ne sont pas liées à un schéma de mesure spécifique. Si vous le souhaitez, vous pouvez utiliser des valeurs sans mesure. Par exemple :

X = *Rangée de l'armoire marron*

Y = *Troisième rack*

Z = *Haut de l'armoire*

Les valeurs des coordonnées X, Y et Z peuvent comporter :

- Pour X et Y : une combinaison quelconque de caractères alphanumériques. La valeur de la coordonnée peut contenir 0 à 24 caractères.
- Pour Z lorsque le format de la coordonnée Z est défini sur *Rack Units*, n'importe quelle valeur comprise entre 0 et 60.
- Pour Z lorsque le format de la coordonnée Z est défini sur *Free-Form*, de 0 à 24 caractères alphanumériques.

Conseil : pour configurer et extraire ces valeurs de coordonnées via SNMP, consultez le fichier MIB de EMX. Pour configurer et extraire ces valeurs dans l'interface CLI, reportez-vous à Utilisation de l'interface de ligne de commande.

Définition de la consignation de données

EMX peut stocker 120 mesures pour chaque capteur dans une mémoire tampon. Cette mémoire tampon est appelée journal de données. Les relevés de capteur du journal de données peuvent être récupérés à l'aide de SNMP.

Vous pouvez configurer la fréquence d'inscription des mesures dans le journal des données à l'aide du champ Measurements Per Log Entry (Mesures par entrée de journal). Etant donné que les capteurs internes sont mesurés chaque seconde, la définition de la valeur 60, par exemple, entraîne l'inscription des mesures dans le journal des données toutes les minutes. Comme il existe 120 mesures en mémoire par capteur, la définition de la valeur 60 signifie que le journal peut stocker les deux dernières heures de mesures avant l'écrasement de la plus ancienne.

Même si les capteurs d'environnement sont mesurés par seconde, leurs relevés ne sont pas forcément mis à jour toutes les secondes. Reportez-vous à ***Informations sur l'intervalle de mise à jour*** (à la page 172). L'intervalle de mise à jour varie selon le nombre de capteurs d'environnement connectés au dispositif EMX et le type du capteur. Plus le nombre de capteurs d'environnement connectés est élevé, plus l'intervalle de mise à jour est long. Aussi, tapez un nombre élevé dans le champ Measurements Per Log Entry (Mesures par entrée de journal) lorsqu'un nombre important de capteurs d'environnement sont connectés.

Lorsque des mesures sont consignées dans le journal, trois valeurs pour chaque capteur sont inscrites : moyenne, minimum et maximum. Par exemple, si des mesures sont inscrites chaque minute, la moyenne de toutes les mesures survenues au cours des 60 secondes précédentes, ainsi que les valeurs minimum et maximum sont enregistrées dans le journal.

Remarque : l'agent SNMP du dispositif EMX doit être activé pour permettre cette fonction. Reportez-vous à **Activation de SNMP** *(à la page 205) pour en savoir plus. En outre, l'utilisation d'un serveur d'horloge assure des mesures horodatées exactement.*

Activation de la consignation de données

Par défaut, la consignation de données est désactivée. Seuls les utilisateurs dotés des autorisations Administrator ou Change Data Logging Settings (Modification des paramètres de consignation de données) peuvent activer ou désactiver cette fonction. Reportez-vous à ***Paramétrage des rôles*** (à la page 69).

Pour configurer la fonction de consignation de données :

1. Choisissez Device Settings > Data Logging (Paramètres du dispositif > Consignation des données). La boîte de dialogue Data Logging Options (Options de consignation de données) s'affiche.
2. Pour activer la fonction de consignation de données, cochez la case enable (activer) dans le champ Enable Data Logging (Activer la consignation de données).
3. Entrez un nombre dans le champ Measurements Per Log Entry (Mesures par entrée de journal). La fourchette valide est comprise entre 1 et 600. La valeur par défaut est 60.
4. Sélectionnez les capteurs d'environnement dont vous souhaitez activer la consignation des données.
   - Pour sélectionner une partie des capteurs, cochez la case correspondant aux capteurs souhaités dans la colonne Logging Enabled (Consignation activée).
   - Pour les sélectionner tous, cliquez sur Enable All (Tout activer) ou Enable All in Page (Tout activer sur la page).
   - Pour les désélectionner tous, cliquez sur Disable All (Tout désactiver) ou Disable All in Page (Tout désactiver sur la page).
5. Cliquez sur OK pour enregistrer les modifications.

Informations sur l'intervalle de mise à jour

Les capteurs d'environnement Raritan peuvent être divisés en deux catégories en fonction de l'intervalle de mise à jour du relevé ou de l'état du capteur.

- Type Normal : les relevés ou les états du capteur sont mis à jour à un intervalle plus long qui varie entre 3 et 40 secondes selon le nombre total de capteurs d'environnement connectés. La plupart des capteurs d'environnement Raritan sont de ce type, notamment les capteurs de température ou d'humidité.
- Type High priority (prioritaire) : les relevés ou états de capteur sont mis à jour à un intervalle plus court, inférieur ou égal à 3 secondes. Les capteurs de fermeture de contact Raritan sont de ce type.

Consultation des données des capteurs

Les relevés des capteurs d'environnement s'affichent dans l'interface Web après que ces capteurs sont correctement connectés et gérés.

La page Dashboard (Tableau de bord) présente les informations concernant les capteurs d'environnement gérés uniquement, alors que la page External Sensors (Capteurs externes) présente les informations concernant les capteurs gérés et non gérés.

si une rangée de relevés de capteur est colorée, ceci signifie qu'un relevé a déjà dépassé un des seuils ou qu'un des capteurs LHX intégré au moins est en panne sur l'échangeur thermique. Reportez-vous à ***Relevés mis en surbrillance en jaune ou en rouge (EMX)*** (voir "***Relevés mis en surbrillance en jaune ou en rouge***" à la page 58).

Pour consulter les capteurs d'environnement uniquement :

1. Cliquez sur l'icône Dashboard (Tableau de bord) dans le volet EMX Explorer et la page Dashboard s'ouvre dans le volet de droite.
2. Recherchez la section External Sensors de la page Dashboard. La section présente :
   - Le nombre total de capteurs gérés
   - Le nombre total de capteurs non gérés
   - Les informations sur chaque capteur géré, notamment :
     - Le nom
     - Le relevé
     - L'état

Pour consulter les capteurs d'environnement gérés et non gérés :

1. Si le dossier EMX est réduit, développez-le pour afficher tous les composants.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur le dossier External Sensors (Capteurs externes) dans le volet EMX Explorer et la page External Sensors s'ouvre dans le volet de droite.

   Des informations détaillées pour chaque capteur connecté sont affichées, notamment :

   - Libellé (numéro)
   - Numéro de série
   - Type de capteur

- Nom
- Relevé
- Etat
- Canal (pour un capteur de fermeture de contact uniquement)

Exactitude des mesures des capteurs

Les capteurs d'environnement Raritan utilisent les spécifications usine suivantes. Le calibrage n'est pas nécessaire pour les capteurs d'environnement.

- Température : +/-2%
- Humidité : +/-5%
- Pression d'air différentielle : +/-1,5 %
- Flux d'air : +/- 6,5 %

Etats des capteurs gérés

Un capteur d'environnement indique l'état après être passé sous gestion.

Les états de capteur disponibles varient selon le type du capteur : numérique ou discret. Par exemple, un capteur de fermeture de contact est un capteur discret ; il n'alterne qu'entre trois états : unavailable, alarmed et normal.

Remarque : les capteurs numériques utilisent des valeurs numériques pour indiquer des conditions d'environnement ou internes, alors que les capteurs discrets (activé/désactivé) utilisent des caractères alphabétiques pour indiquer l'état.

Etat du capteur	Concerne
unavailable (indisponible)	Tous les capteurs
alarmed	Capteurs discrets
normal	Tous les capteurs
below lower critical	Capteurs numériques
sous l'avertissement inférieur	Capteurs numériques
au-dessus de l'avertissement supérieur	Capteurs numériques
above upper critical	Capteurs numériques

Etat « unavailable »

L'état *unavailable* (indisponible) signifie que la connectivité au capteur est perdue.

EMX effectue des tests ping de tous les capteurs gérés à intervalles réguliers, en secondes. S'il ne détecte pas un capteur particulier au cours de trois balayages consécutifs, l'état *unavailable* est affiché pour ce capteur.

Lorsque la communication avec le processeur d'un capteur de fermeture de contact est perdue, tous les détecteurs (c'est-à-dire, tous les commutateurs) connectés au même module de capteur affichent l'état unavailable.

Remarque : lorsque le capteur est considéré indisponible, la configuration de capteur existante reste inchangée. Par exemple, le numéro d'identification affecté au capteur lui reste associé.

EMX continue d'effectuer des tests ping sur le capteur indisponible et annule l'état *unavailable* après avoir détecté le capteur au cours de deux balayages consécutifs.

Etat « normal »

Cet état indique que le capteur est à l'état normal.

Pour un capteur de fermeture de contact, il s'agit de l'état normal que vous avez défini.

- Si l'état normal est défini sur Normally Closed (Normalement fermé), l'état *normal* signifie que le commutateur de fermeture de contact est fermé.
- Si l'état normal est défini sur Normally Open (Normalement ouvert), l'état *normal* signifie que le commutateur de fermeture de contact est ouvert.

Remarque : reportez-vous à **Configuration d'un capteur de fermeture de contact** *(à la page 35) pour définir l'état normal. Pour la terminaison du capteur de fermeture de contact embarqué, reportez-vous à* **Connexion des détecteurs/commutateurs tiers à EMX** *(à la page 36) pour apprendre à définir l'état normal.*

Pour un capteur numérique, cet état signifie que le relevé du capteur figure dans la plage acceptable comme indiqué ci-dessous :

Seuil d'avertissement inférieur <= Relevé < Seuil d'avertissement supérieur

---

Remarque : le symbole <= signifie inférieur à (<) ou égal à (=).

Etat « alarmed »

Cet état signifie qu'un capteur discret (activé/désactivé) est à l'état « anormal ».

Pour un capteur de fermeture de contact, la signification de cet état varie suivant le paramètre d'état normal du capteur.

- Si l'état normal est défini sur Normally Closed (Normalement fermé), l'état *alarmed* signifie que le commutateur de fermeture de contact est ouvert.
- Si l'état normal est défini sur Normally Open (Normalement ouvert), l'état *alarmed* signifie que le commutateur de fermeture de contact est fermé.

Remarque : reportez-vous à **Configuration d'un capteur de fermeture de contact** *(à la page 35) pour définir l'état normal. Pour la terminaison du capteur de fermeture de contact embarqué, reportez-vous à* **Connexion des détecteurs/commutateurs tiers à EMX** *(à la page 36) pour apprendre à définir l'état normal.*

Conseil : le voyant d'un capteur de fermeture de contact est allumé après son passage à l'état alarmed*. Si le module de capteur comporte deux canaux pour la connexion de deux commutateurs, deux voyants sont disponibles. Vérifiez quel commutateur de fermeture de contact est au statut anormal selon le numéro de canal du voyant.*

Etat « below lower critical »

Cet état signifie que le relevé d'un capteur numérique est sous le seuil critique inférieur comme indiqué ci-dessous :

Reading < Lower Critical Threshold (*Relevé < Seuil critique inférieur*)

Etat « Sous l'avertissement inférieur »

Cet état signifie que le relevé d'un capteur numérique est au-dessous du seuil d'avertissement inférieur comme indiqué ci-dessous :

Seuil critique inférieur <= Relevé < Seuil d'avertissement inférieur

---

Remarque : le symbole <= signifie inférieur à (<) ou égal à (=).

Etat « au-dessus de l'avertissement supérieur »

Cet état signifie que le relevé d'un capteur numérique est au-dessus du seuil d'avertissement supérieur comme indiqué ci-dessous :

Seuil d'avertissement supérieur <= Relevé < Seuil critique supérieur

---

Remarque : le symbole <= signifie inférieur à (<) ou égal à (=).

Etat « above upper critical »

Cet état signifie que le relevé d'un capteur numérique est au-dessus du seuil critique supérieur comme indiqué ci-dessous :

Upper Critical Threshold <= *Reading* (*Seuil critique supérieur* <= *Relevé*)

Remarque : le symbole <= signifie inférieur à (<) ou égal à (=).

Annulation de la gestion des capteurs d'environnement

Lorsqu'il est nécessaire de surveiller un facteur d'environnement particulier, vous pouvez annuler la gestion du capteur d'environnement correspondant ou le libérer afin que le dispositif EMX cesse d'extraire le relevé et/ou l'état du capteur.

Pour libérer un capteur géré :

1. Si le dossier EMX est réduit, développez-le pour afficher tous les composants.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur le dossier External Sensors (Capteurs externes) dans le volet EMX Explorer et la page External Sensors s'ouvre dans le volet de droite.
3. Cliquez sur le capteur dont vous souhaitez annuler la gestion sur la page External Sensors (Capteurs externes).
4. Cliquez sur Release (Libérer).

Après le retrait d'un capteur de la gestion, le numéro d'identification qui lui était affecté est libéré et peut être automatiquement attribué à un capteur qui vient d'être détecté.

Informations sur les seuils

La définition et l'activation de seuils provoquent la génération par le dispositif EMX de notifications d'alerte lorsqu'il détecte que l'état d'un capteur dépasse ces seuils.

Chaque capteur dispose de quatre seuils : critique inférieur, d'avertissement inférieur, d'avertissement supérieur et critique supérieur.

- Les seuils d'avertissement supérieurs et inférieurs indiquent que le relevé du capteur se situe dans la plage d'avertissement avant le seuil critique.
- Les seuils critiques supérieurs et inférieurs indiquent que le relevé du capteur se situe à un niveau critique.

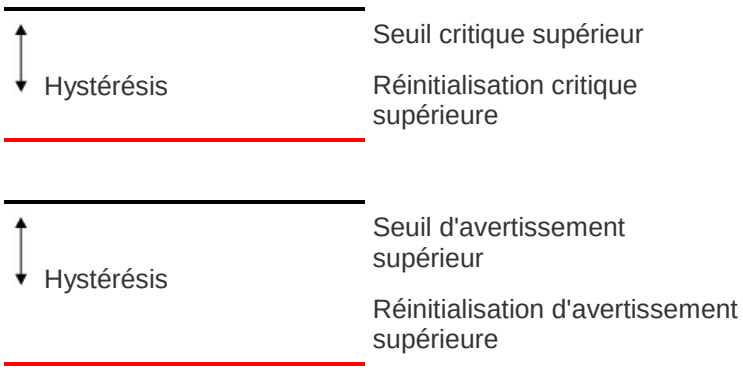
Pour éviter la génération d'un grand nombre d'événements d'alerte, l'hystérésis d'infirmation est activée pour chaque seuil. Vous pouvez changer la valeur d'hystérésis par défaut, le cas échéant. Pour en savoir plus sur l'hystérésis d'infirmation, reportez-vous à ***Hystérésis d'infirmation : définition*** (à la page 178)

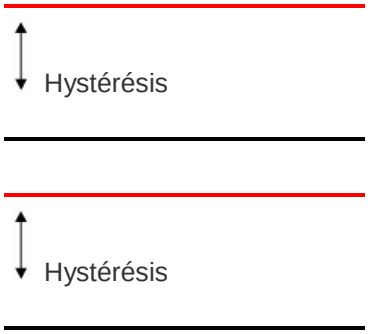
Remarque : après avoir défini les seuils, vous devez configurer les règles d'événement. Reportez-vous à **Configuration des règles d'événement** *(voir "***Règles et actions d'événement***" à la page 131).*

Pour plus d'informations sur la configuration du seuil d'un capteur d'environnement, reportez-vous à ***Configuration des capteurs d'environnement*** (à la page 168). Pour plus d'informations sur la configuration des seuils d'un échangeur thermique Schroff LHX, reportez-vous à ***Configuration des seuils de température et de ventilateur*** (à la page 200).

Hystérésis d'infirmation : définition

Le paramètre d'hystérésis détermine quand une condition de seuil est réinitialisée. Ce diagramme illustre le rapport des valeurs d'hystérésis et des seuils :





Les valeurs d'hystérésis définissent un seuil de réinitialisation. Pour les seuils supérieurs, la mesure doit descendre au-dessous de ce seuil de réinitialisation avant la génération d'un événement d'infirmation. Pour les seuils inférieurs, la mesure doit monter au-dessus de ce seuil de réinitialisation avant la génération d'un événement d'infirmation.

Délai d'affirmation : définition

Lorsque le délai d'affirmation est activé, le dispositif EMX affirme une condition d'avertissement ou critique uniquement lorsqu'un nombre particulier d'échantillons consécutifs dépassant un certain seuil sont générés. Ceci empêche la génération d'un nombre d'alertes de seuil si les mesures reviennent immédiatement à la normale après être montées au-dessus d'un seuil supérieur ou descendues au-dessous d'un seuil inférieur.

Capteurs de ressources et étiquettes de gestion des ressources

Un port Feature (Fonction) est identifié par une combinaison du nom Asset Strip et du numéro de port.

Après avoir connecté un capteur de ressources, vous devez fournir le nombre total d'unités de rack (ports d'étiquette) dont dispose le capteur de ressources connectées sur le dispositif EMX.

Si nécessaire, vous pouvez également modifier manuellement les paramètres de couleur de voyant pour une unité de rack spécifique sur le capteur de ressources afin que le voyant se comporte différemment des autres voyants.

La connexion en guirlande de capteurs de ressources AMS-M2-Z est prise en charge par EMX. Reportez-vous à ***Restrictions de la connexion en guirlande des capteurs AMS-M2-Z*** (à la page 185) pour en savoir plus sur les limites de cette connexion. Une fois connecté, EMX reconnaît chaque capteur de ressources AMS-M2-Z appartenant à la guirlande. Les extensions de lames peuvent être connectées à chaque capteur de ressources AMS-M2-Z de la guirlande, le cas échéant. Lorsque les capteurs de ressources AMS-M2-Z sont ajoutés ou retirés de la guirlande, des événements sont générés dans EMX.

Configuration du capteur de ressources

EMX NE PEUT PAS détecter le nombre d'unités de rack (ports d'étiquette) prises en charge par un capteur de ressources connectées, vous devez donc entrer cette information manuellement.

En outre, vous pouvez nommer le capteur de ressources ou déterminer la méthode de numérotation de toutes les unités de rack dans l'interface Web. De plus, vous pouvez fournir une description afin d'identifier chaque capteur de ressources.

Le nom personnalisé est suivi du libellé entre parenthèses.

Remarque : dans ce contexte, l'étiquette se réfère au numéro du port auquel le capteur de ressources est connecté.

Pour configurer un capteur de ressources :

1. Le cas échéant, connectez le capteur de ressources à EMX. Reportez-vous à ***Connexion des capteurs de ressources à EMX*** (à la page 24).
2. Cliquez sur le dossier Feature Ports (Ports de fonction) dans l'arborescence pour le développer.

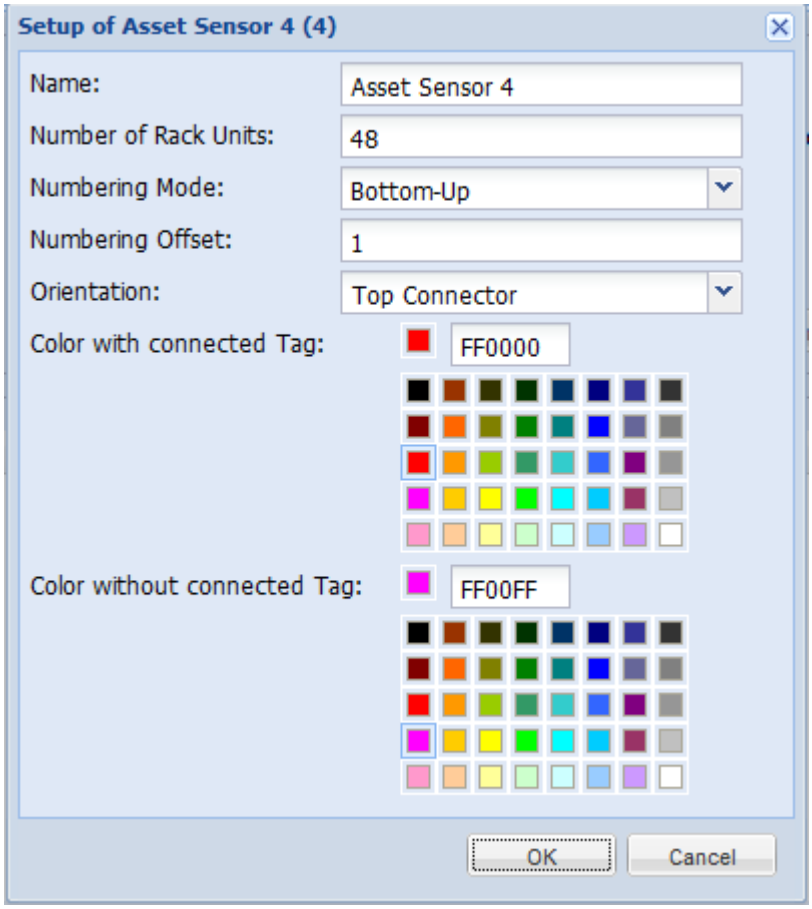
3. Cliquez sur le capteur de ressources désiré. La page spécifique à ce capteur s'ouvre dans le volet droit et affiche les paramètres et informations de capteur de ressources pour toutes les unités de rack (ports d'étiquette).

   Remarque : vous pouvez également accéder à cette boîte de dialogue en double-cliquant sur le capteur de ressources présenté sur la page Dashboard.

4. Cliquez sur Setup (Paramétrer) dans la section Settings (Paramètres). La boîte de dialogue Setup of Asset Strip (Paramétrage d'un bandeau de ressources) apparaît.
5. Entrez le nom de capteur de ressources.
6. Entrez le nombre total d'unités de rack indiqué dans le champ Number of Rack Units du capteur de ressources sélectionné. Ce champ indique 48 par défaut.
7. Déterminez comment numéroter toutes les unités de rack sur le capteur de ressources en sélectionnant une option dans Numbering Mode.
   - Top-Down (Haut-Bas) : Les unités de rack sont numérotées en ordre croissant de l'unité de rack la plus haute à la plus basse.
   - Bottom-Up (Bas-Haut) : Les unités de rack sont numérotées en ordre décroissant de l'unité de rack la plus haute à la plus basse.
8. Dans le champ Numbering Offset (Décalage de numérotation), sélectionnez le numéro de début. Par exemple, si vous sélectionnez 3, la première unité de rack est numérotée 3, la seconde, 4, la troisième, 5, et ainsi de suite jusqu'au numéro final.
9. Indiquez comment le capteur de ressources est monté dans le rack dans le champ Orientation. L'unité de rack la plus proche du connecteur RJ-45 du capteur de ressources sera marquée du numéro d'index 1 dans l'interface Web.

   Pour la dernière version de capteurs de ressources intégrant un détecteur d'inclinaison, il N'EST PAS nécessaire de configurer le paramètre d'orientation manuellement. Le dispositif EMX peut détecter l'orientation des capteurs de ressources et la configurer automatiquement.
   - Connecteur supérieur : Cette option indique que le capteur de ressources est monté à l'aide du connecteur RJ-45 situé en haut.
   - Connecteur inférieur : Cette option indique que le capteur de ressources est monté à l'aide du connecteur RJ-45 situé en bas.
10. Pour modifier la couleur de voyant indiquant la présence d'une étiquette connectée, cliquez sur une couleur dans la palette correspondante ou tapez la valeur RVB hexadécimale de la couleur dans le champ Color with connected Tag (Couleur pour étiquette connectée).

11. Pour modifier la couleur de voyant indiquant l'absence d'une étiquette connectée, cliquez sur une couleur dans la palette correspondante ou tapez la valeur RVB hexadécimale de la couleur dans le champ Color without connected Tag (Couleur sans étiquette connectée).
12. Cliquez sur OK pour enregistrer les modifications.



Modification des paramètres de couleur d'un voyant spécifique

Dans l'interface Web du dispositif EMX, une unité de rack fait référence à un port d'étiquette sur le capteur de ressources. Vous pouvez nommer une unité de rack spécifique, ou modifier ses paramètres de couleur de voyant afin que ce dernier se comporte différemment des autres du même capteur de ressources.

Pour modifier les paramètres d'un voyant :

1. Le cas échéant, connectez le capteur de ressources à EMX. Reportez-vous à ***Connexion des capteurs de ressources à EMX*** (à la page 24).

2. Cliquez sur le dossier Feature Ports (Ports de fonction) dans l'arborescence pour le développer.
3. Cliquez sur le capteur de ressources désiré. La page spécifique à ce capteur s'ouvre dans le volet droit et affiche les paramètres et informations de capteur de ressources pour toutes les unités de rack (ports d'étiquette).

   Remarque : vous pouvez également accéder à cette boîte de dialogue en double-cliquant sur le capteur de ressources présenté sur la page Dashboard.

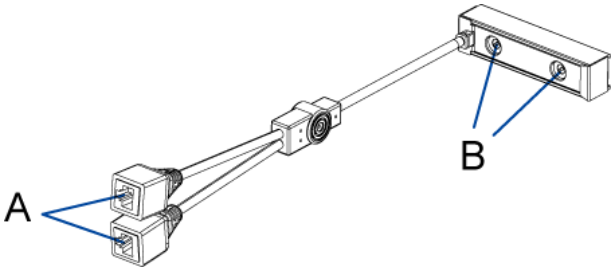
4. Sélectionnez l'unité de rack pour laquelle vous souhaitez modifier les paramètres de voyant.
5. Cliquez sur Configure Rack Unit (Configurer l'unité de rack) ou double-cliquez sur l'unité de rack choisie. La boîte de dialogue de paramétrage de cette unité apparaît.
6. Dans le champ Name, tapez un nom permettant d'identifier cette unité de rack.
7. Sélectionnez Auto ou Manual Override (Automatique ou Supplantation manuelle) comme mode de voyant de l'unité de rack.
   - Auto (suivant l'étiquette) : il s'agit du paramètre par défaut. Lorsque cette option est sélectionnée, le voyant suit les paramètres généraux de couleur de voyant.
   - Manual Override (Supplantation manuelle) : cette option différencie le comportement du voyant. Une fois cette option choisie, vous devez sélectionner un mode de voyant et/ou une couleur de voyant pour l'unité de rack concernée.
     - LED Mode (Mode de voyant) : sélectionnez On pour que le voyant reste allumé, Off pour qu'il reste éteint, Slow blinking pour qu'il clignote lentement ou Fast blinking pour qu'il clignote rapidement.
     - LED Color (Couleur de voyant) : si vous sélectionnez On, Slow blinking ou Fast blinking dans le champ LED Mode, sélectionnez une couleur de voyant en cliquant sur la couleur choisie dans la palette des couleurs ou en entrant la valeur RVB hexadécimale d'une couleur dans la zone de texte associée.
8. Cliquez sur OK pour enregistrer les modifications.

Connexion des capteurs de ressources AMS-M2-Z (facultatif)

AMS-M2-Z est un type spécial de capteur de ressources fonctionnant de la même façon que les capteurs de ressources MAITRES, hormis les différences suivantes.

- Il est doté de deux connecteurs RJ-45.
- Plusieurs capteurs de ressources AMS-M2-Z peuvent être connectés en guirlande.
- Seuls deux ports d'étiquette sont disponibles sur chaque AMS-M2-Z ; deux étiquettes de gestion des ressources seulement peuvent donc être connectées.

Ce produit est particulièrement utile pour le suivi de dispositifs importants, tels que des boîtiers SAN dans une armoire.



Elément	Description
A	Connecteurs RJ-45
B	Ports d'étiquette

Pour connecter les capteurs de ressources AMS-M2-Z au dispositif EMX :

1. Connectez l'AMS-M2-Z à EMX via un câble Catégorie 5e/6.
   a. Connectez une extrémité du câble au port RJ-45 libellé Input (Entrée) sur l'AMS-M2-Z.
   b. Connectez l'autre extrémité du câble au port FEATURE du dispositif EMX.
2. Apposez une étiquette de gestion des ressources au dispositif informatique et connectez-la à l'AMS-M2-Z en branchant son connecteur sur le port d'étiquette de l'AMS-M2-Z. Reportez-vous à ***Connexion des capteurs de ressources à EMX*** (à la page 24) pour en savoir plus.
3. Au besoin, connectez en guirlance plusieurs AMS-M2-Z pour effectuer le suivi de plus de deux dispositifs informatiques via ce dispositif EMX.

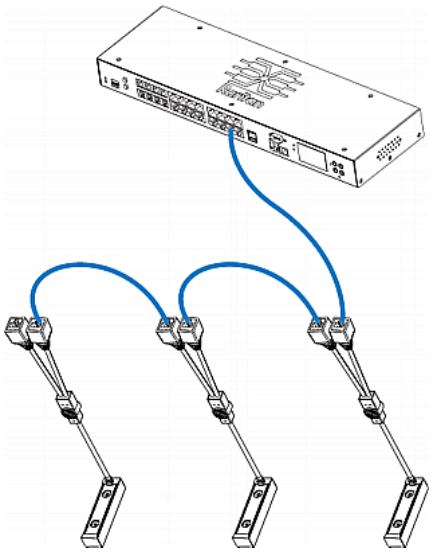
a. Vérifiez que la longueur du câble Catégorie 5e/6 respecte les limites. Reportez-vous à ***Restrictions de la connexion en guirlande des capteurs AMS-M2-Z*** (à la page 185) pour obtenir ces limites de longueur.

b. Branchez une extrémité du câble Catégorie 5e/6 sur le connecteur RJ-45 libellé Output (Sortie) de l'AMS-M2-Z à relier à EMX.

c. Connectez l'autre extrémité du câble au port RJ-45 libellé Input (Entrée) sur un autre AMS-M2-Z.

d. Répétez les étapes précédentes pour connecter en guirlande des AMS-M2-Z supplémentaires. Reportez-vous à ***Restrictions de la connexion en guirlande des capteurs AMS-M2-Z*** (à la page 185) pour connaître le nombre maximum de capteurs de ressources AMS-M2-Z pris en charge.

e. Il est fortement recommandé d'utiliser des attaches de câble pour supporter le poids de tous les câbles de connexion.



4. Répétez l'étape 2 pour connecter des dispositifs informatiques à l'autre AMS-M2-Z de la guirlande au moyen d'étiquettes de gestion des ressources.

Restrictions de la connexion en guirlande des capteurs AMS-M2-Z

La connexion en guirlande des capteurs de ressources AMS-M2-Z entraîne certaines restrictions qui varient selon le modèle du produit Raritan connecté au premier capteur AMS-M2-Z.

Modèles	Restrictions de la connexion en guirlande
Toutes les PDU dont le	• Jusqu'à 4 capteurs AMS-M2-Z peuvent être connectés en guirlande.

Modèles	Restrictions de la connexion en guirlande
nom de modèle débute par PX2	• La longueur de câble maximum entre chaque capteur AMS-M2-Z de la chaîne est de 2 mètres.
EMX2-111	• Jusqu'à 2 capteurs AMS-M2-Z peuvent être connectés en guirlande. • La longueur de câble maximum entre chaque capteur AMS-M2-Z de la chaîne est de 2 mètres.
EMX2-888	• Jusqu'à 6 capteurs AMS-M2-Z peuvent être connectés en guirlande. • La longueur de câble maximum entre chaque capteur AMS-M2-Z de la chaîne est de 3 mètres.

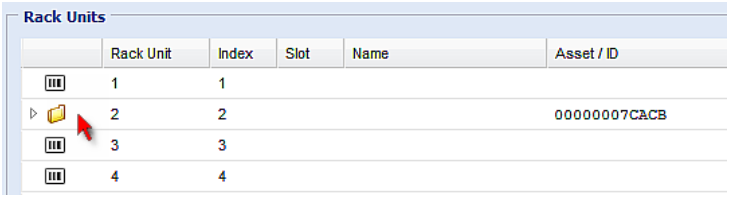
Développement d'un bandeau d'extension de lame

Un bandeau d'extension de lame, comme un capteur de ressources, comporte plusieurs ports d'étiquette. Après sa connexion à un capteur de ressources particulier, il s'affiche sous forme de dossier sur la page de ce capteur.

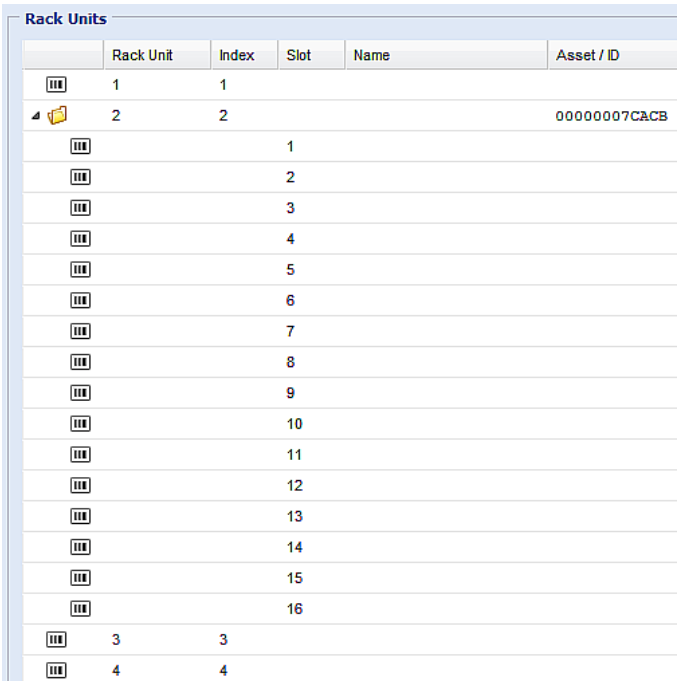
Remarque : si vous devez déconnecter temporairement le connecteur d'étiquette du bandeau d'extension de lame, patientez au moins une seconde avant de le reconnecter, ou le dispositif EMX risque de ne pas le détecter.

Pour développer le dossier d'un bandeau d'extension de lame :

1. Cliquez sur le capteur de ressources souhaité dans le volet gauche. La page du capteur sélectionné s'ouvre dans le volet droit.
2. Recherchez l'unité de rack (port d'étiquette) à laquelle le bandeau d'extension de lame est connecté.



3. Double-cliquez sur cette unité de rack ou cliquez sur la flèche blanche ▷ placée avant l'icône de dossier. La flèche se transforme en flèche de gradient noire ◢ et tous les ports d'étiquette apparaissent sous le dossier.



Pour réduire un bandeau d'extension de lame :

- Double-cliquez sur le dossier du bandeau d'extension de lame ou cliquez sur la flèche de gradient noir ◢ placée avant l'icône du dossier. Tous les ports d'étiquette du dossier sont masqués.

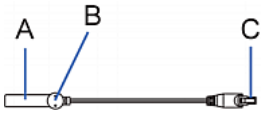
Connexion des bandeaux d'extension de lame

Vous pouvez effectuer le suivi des serveurs lames, figurant sur un même châssis, à l'aide d'un bandeau d'extension de lame.

Le bandeau d'extension de lame Raritan fonctionne de manière similaire à un capteur de ressources Raritan, mais requiert un câble de connecteur d'étiquette pour le branchement sur un port d'étiquette du capteur de ressources standard ou de l'AMS-M2-Z. Le bandeau d'extension de lame contient 4 à 16 ports d'étiquette, selon le modèle acheté.

Le diagramme illustre un câble de connecteur d'étiquette et le bandeau d'extension de lame comportant 16 ports d'étiquette.

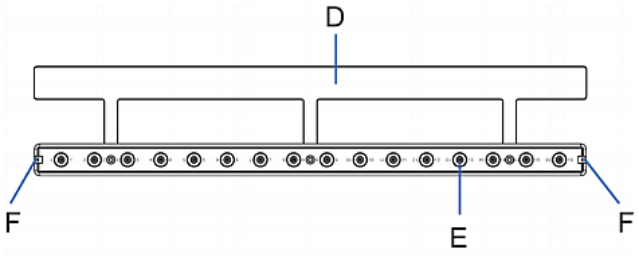
Câble de connecteur d'étiquette



Elément	Description
A	Code à barres (numéro d'identification) pour le câble de connecteur d'étiquette
B	Connecteur d'étiquette
C	Connecteur de câble pour la connexion du bandeau d'extension de lame

Remarque : un câble de connecteur d'étiquette est doté d'un code à barres unique, affiché dans l'interface Web du dispositif EMX pour identifier chaque bandeau d'extension de lame là où il est connecté.

Bandeau d'extension de lame



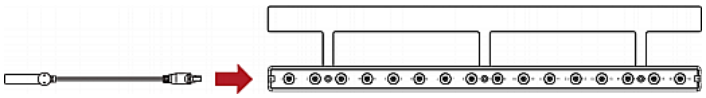
Elément	Description
D	Section en mylar avec la bande adhésive
E	Ports d'étiquette

Elément	Description
F	Prise(s) de câble pour la connexion du câble de connecteur d'étiquette

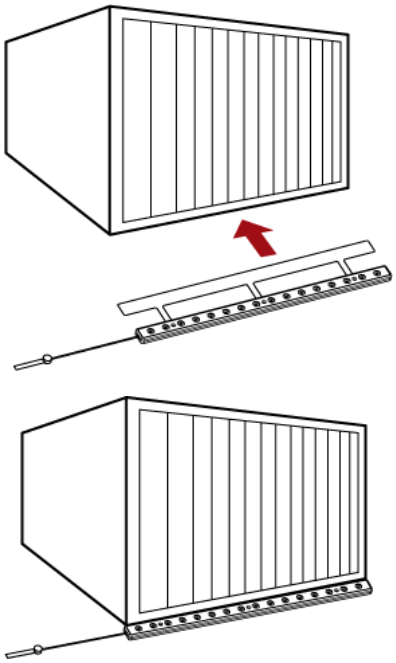
Remarque : chaque port d'étiquette du bandeau d'extension de lame est libellé d'un numéro, affiché comme numéro de fente dans l'interface Web du dispositif EMX.

Pour installer un bandeau d'extension de lame :

1. Branchez le câble du connecteur d'étiquette sur le bandeau d'extension de lame.
   - Branchez le connecteur du câble dans la prise à l'une des extrémités du bandeau d'extension de lame.



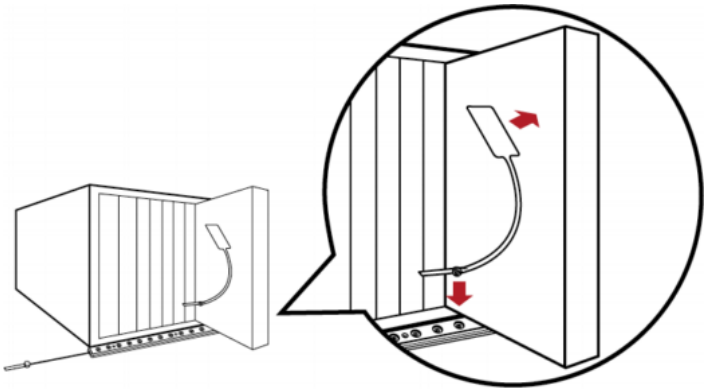
2. Déplacez le bandeau d'extension de lame vers le bas du châssis de lame jusqu'à ce que sa section en mylar se trouve entièrement sous le châssis. Vérifiez ensuite que le bandeau ne se détache pas facilement. Au besoin, vous pouvez utiliser la bande adhésive au dos de la section en mylar pour maintenir le bandeau en place.



3. Connectez une extrémité d'une étiquette de gestion des ressources à un serveur lame et l'autre, au bandeau d'extension de lame.

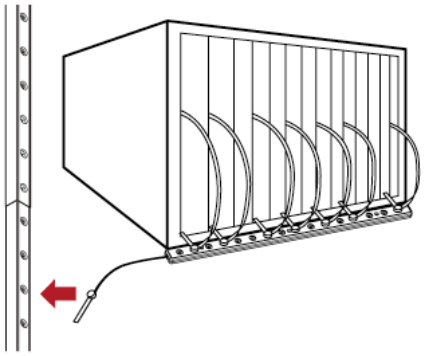
a. Apposez la partie adhésive de l'étiquette de gestion des ressources à un côté d'un serveur lame.

b. Branchez le connecteur de l'étiquette de gestion des ressources sur le port d'étiquette du bandeau d'extension de lame.



4. Répétez l'étape précédente jusqu'à ce que tous les serveurs lames du châssis soient connectés au bandeau d'extension de lame au moyen d'étiquettes de gestion des ressources.

5. Branchez le connecteur d'étiquette du bandeau d'extension de lame sur le port d'étiquette le plus proche de l'assemblage de capteurs de ressources ou du capteur AMS-M2-Z du rack.



Remarque : si vous devez déconnecter temporairement le connecteur d'étiquette du bandeau d'extension de lame, patientez au moins une seconde avant de le reconnecter, ou le dispositif EMX risque de ne pas le détecter.

Webcams

EMX prend en charge les webcams Logitech® QuickCam® Pro 9000 qui lui sont connectées et vous permet ainsi de visualiser une vidéo ou des instantanés de la zone autour de la webcam. Le dispositif EMX 888 prend en charge jusqu'à deux webcams, et EMX 111, une. Après avoir connecté une webcam, vous pouvez surveiller les conditions environnementales près du dispositif EMX via l'interface Web, de n'importe où.

Pour plus d'informations sur la webcam QuickCam, consultez la documentation d'utilisation qui l'accompagne. Pour en savoir plus sur le branchement d'une webcam à EMX, reportez-vous à ***Connexion d'une webcam Logitech (facultatif)*** (à la page 39).

Les instantanés ou les vidéos pris par la webcam sont affichés dans le volet droit de l'interface Web de EMX lorsqu'une webcam est sélectionnée dans l'arborescence de navigation. Ils peuvent également être affichés en mode Live Preview (Prévisualisation en temps réel) dans la fenêtre Primary Standalone Live Preview (Prévisualisation en temps réel autonome principale) en cliquant sur l'icône Live Preview  .

EMX permet de prendre et de stocker des instantanés de chaque webcam. Reportez-vous à ***Prise, consultation et gestion des instantanés de webcam*** (à la page 194) pour en savoir plus.

Des liens vers la vidéo prise par une webcam peuvent être envoyés par courriel ou par message instantané. Reportez-vous à ***Envoi de vidéos par courriel ou par message instantané*** (à la page 196).

Les événements qui déclenchent les courriels contenant les instantanés d'une webcam peuvent être créés. Des événements peuvent être définis pour chaque webcam. Reportez-vous à ***Règles et actions d'événement*** (à la page 131).Votre rôle doit disposer de l'autorisation Change Webcam Configuration (Modifier la configuration de la webcam) pour configurer les webcams, et de l'autorisation View Webcam Images and Configuration (Afficher les images et la configuration de la webcam) pour visualiser des images dans EMX.

Configuration des webcams

Avant de configurer une webcam, vous devez la connecter à EMX. Reportez-vous à ***Connexion d'une webcam Logitech (facultatif)*** (à la page 39).

Pour configurer une webcam :

1. Dans l'arborescence de navigation, cliquez sur le dossier Webcam Management (Gestion de la webcam). La page correspondante s'ouvre.

2. Cliquez sur la webcam que vous souhaitez configurer, puis cliquez sur Setup (Paramétrer) en bas à droite de la page. La boîte de dialogue Webcam Setup (Paramétrage de la webcam) s'ouvre.
3. Entrez le nom de la webcam. 64 caractères au plus sont pris en charge.
4. Sélectionnez une résolution pour la webcam.
5. Sélectionnez un mode. Ceci peut être modifié selon les besoins une fois la webcam configurée.
   a. Video : la webcam est en mode vidéo. Entrez un nombre de secondes dans le champ Framerate (Nombre d'images).
   b. Snapshot : la webcam prend des images. Entrez un nombre de secondes dans le champ Time Between Image(s) (Durée entre les images).
6. Cliquez sur OK. L'image ou la vidéo de la webcam est maintenant disponible dans EMX lorsque vous cliquez sur la webcam dans l'arborescence de navigation.

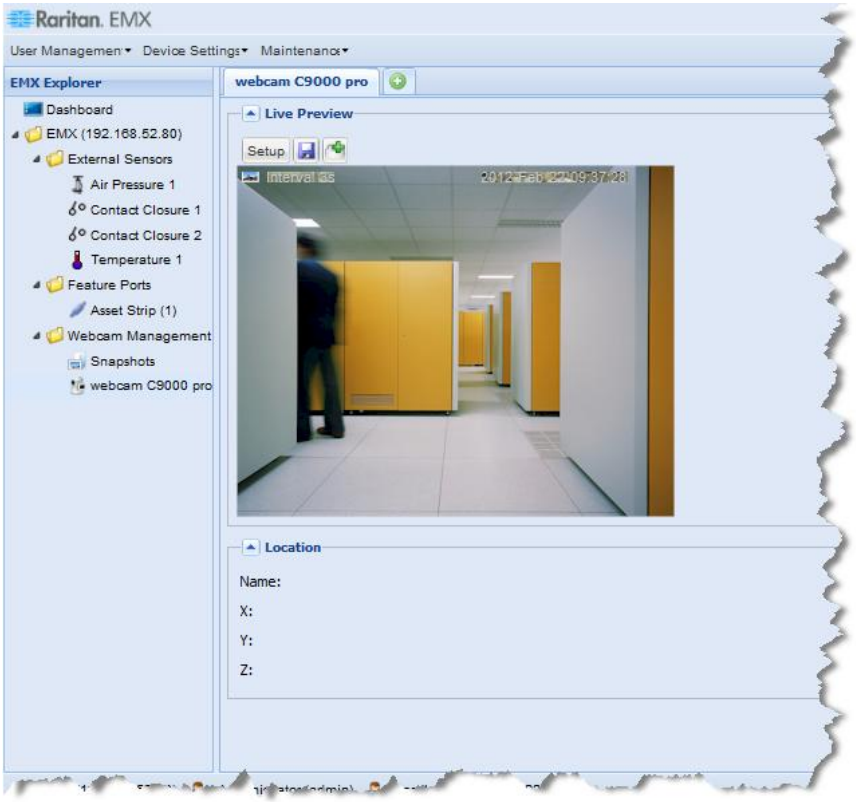
Pour modifier la configuration d'une webcam :

1. Dans l'arborescence de navigation, cliquez sur le dossier Webcam Management (Gestion de la webcam). La page correspondante s'ouvre.
2. Double-cliquez sur la webcam à modifier. L'image ou la vidéo de la webcam s'ouvre dans un nouvel onglet.
3. Cliquez sur Setup (Paramétrer).
4. Modifiez les données si besoin est. La modification apportée à la résolution ne s'applique pas aux images existantes stockées ; elle ne concerne que les images et vidéos prises après le changement.
5. Cliquez sur OK.

Consultation des instantanés et des vidéos de webcam

Par défaut, lorsqu'une webcam est reliée, elle est programmée pour prendre des instantanés toutes les cinq secondes. Modifiez les paramètres de la webcam et/ou alternez entre des instantanés et une vidéo en temps réel dans la boîte de dialogue Webcam Setup (Paramétrage de la webcam) en cliquant sur une webcam dans l'arborescence de navigation, puis sur le bouton Setup du volet Live Preview. Reportez-vous à ***Configuration des webcams*** (à la page 191).

Les instantanés ou les vidéos pris par une webcam sont affichés dans le volet droit de l'interface Web de EMX lorsque cette webcam est sélectionnée dans l'arborescence de navigation.



En mode instantané, l'icône  apparaît dans le coin supérieur gauche de l'image, accompagnée du nombre d'images que la webcam doit prendre par seconde. En mode vidéo, l'icône  apparaît dans le coin supérieur gauche de l'image. Pour permuter entre le mode Snapshot et le mode Video, cliquez sur Setup et sélectionnez la case d'option Image ou Video.

Un horodateur est également affiché sur chaque instantané. L'emplacement de la webcam est affiché dans le volet Location sous l'image, ainsi que les libellés appliqués à la webcam. Reportez-vous à ***Configuration des webcams*** (à la page 191).

Cinq sessions Live Preview au plus peuvent être affichées simultanément dans des onglets différents de l'interface EMX ou dans des fenêtres Live Preview distinctes accessibles en cliquant sur l'icône Live Preview  située au-dessus de l'image ou de la vidéo.

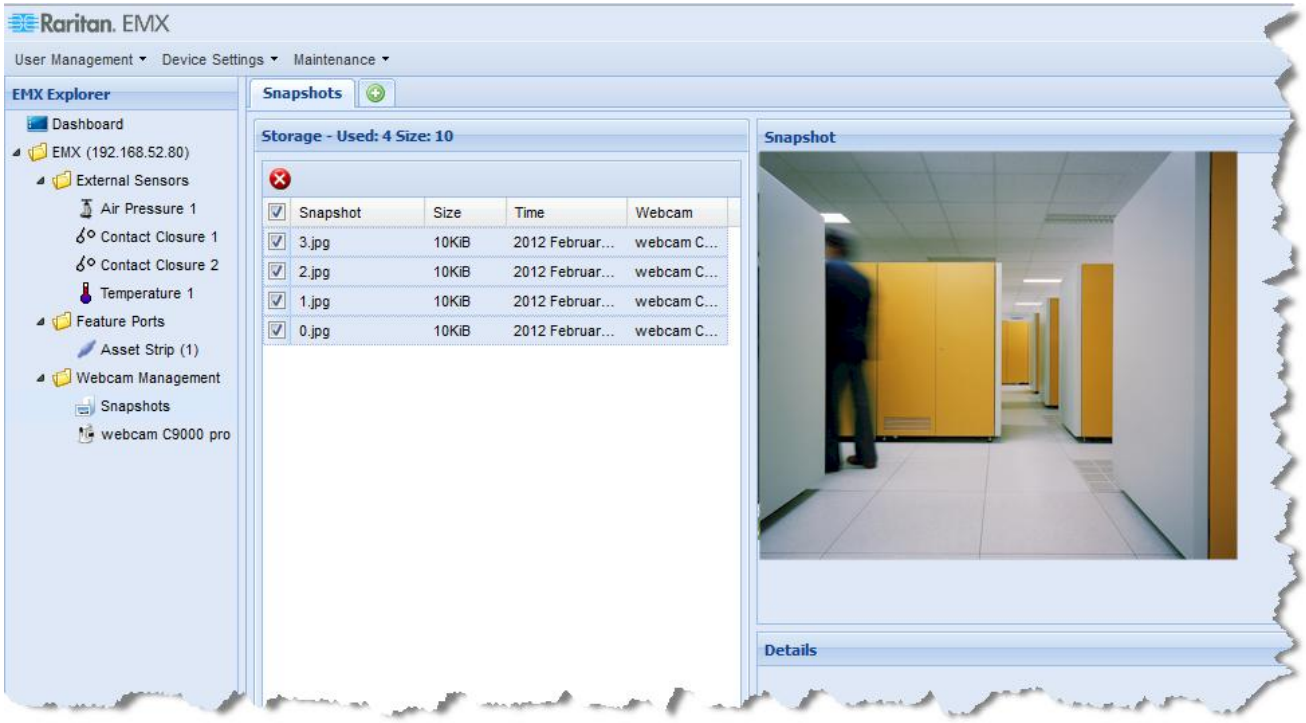
Remarque : pour les sessions Live Preview à distance, auxquelles vous avez accédé, par exemple, au moyen d'un lien dans un courriel ou un message instantané, trois sessions simultanées au maximum sont prises en charge : celle de l'origine dans l'interface EMX et deux sessions distantes au maximum.

Les différents instantanés pris par une webcam sont visibles en cliquant sur Snapshots (Instantanés) sous Webcam Management (Gestion de la webcam) dans l'arborescence de navigation. Lorsque cette option est sélectionnée, l'onglet Snapshots s'ouvre dans le volet droit. Reportez-vous à ***Prise, consultation et gestion des instantanés de webcam*** (à la page 194) et Consultation et gestion des instantanés stockés pour en savoir plus.

Prise, consultation et gestion des instantanés de webcam

Lorsqu'un instantané est pris à l'aide de la fonction Store Snapshot to Webcam Storage (Stocker l'instantané dans la mémoire de la webcam), il est stocké dans EMX. EMX peut conserver jusqu à 10 instantanés à la fois. Si les instantanés ne sont pas supprimés manuellement, le plus ancien est automatiquement effacé du dispositif lorsque le total dépasse 10.

Les fichiers d'instantanés sont enregistrés au format JPG. Les fichiers sont nommés d'après le numéro que porte l'instantané en commençant par 1. Le premier instantané pris se nomme 1.jpg, le second, 2.jpg etc.



Pour prendre un instantané depuis la webcam :

1. Dans l'arborescence de navigation, cliquez sur la webcam que vous souhaitez utiliser. L'image de la webcam apparaît dans le volet droit.

   La webcam doit être en mode instantané pour prendre des images. Si elle est en mode vidéo, cliquez sur Setup (Paramétrer) dans le volet droite au-dessus de l'image vidéo pour ouvrir la boîte de dialogue Webcam Setup (Paramétrage de la webcam), puis sélectionnez la case d'option Snapshot (Instantané).

2. Lorsque l'image de l'instantané à prendre par la webcam sélectionnée est affiché dans le volet droit, cliquez sur l'icône Store Snapshot to Webcam Storage au-dessus de l'image pour prendre l'instantané. Le dispositif peut conserver jusqu à 10 instantanés à la fois.

Pour consulter les instantanés existants :

1. Dans l'arborescence de navigation, cliquez sur Snapshot sous le dossier Webcam Management (Gestion de la webcam). Les instantanés sont affichés dans le volet droit de la section Storage (Mémoire) de la page.

2. Consultez chaque instantané en cliquant sur son fichier dans la section Storage de la page.

   La taille de chaque fichier, les date et heure de prise de chaque instantané et la webcam qui a servi pour chacun sont affichées lors que la consultation des instantanés.

Des détails, tels que l'emplacement et/ou les libellés de la webcam, le cas échéant, sont affichés dans la section Details sous l'instantané dans le volet droit. Ces données sont définies lors de la configuration initiale de la webcam. Reportez-vous à ***Configuration des webcams*** (à la page 191).

Pour supprimer manuellement des instantanés :

- Cochez la case placée à côté de l'instantané que vous souhaitez supprimer, puis cliquez sur l'icône Delete (Supprimer) en haut de la section. Pour sélectionner et supprimer tous les instantanés en même temps, cochez la case dans l'en-tête de la colonne des cases à cocher, puis cliquez sur l'icône Delete.

Envoi de vidéos par courriel ou par message instantané

Vous pouvez envoyer par courriel ou par message instantané à deux destinataires au plus un lien vers les webcams reliées à EMX. Ces utilisateurs peuvent alors cliquer sur ces liens et regarder les instantanés ou les vidéos.

Remarque : pour les sessions Live Preview à distance, auxquelles vous avez accédé, par exemple, au moyen d'un lien dans un courriel ou un message instantané, trois sessions simultanées au maximum sont prises en charge : celle de l'origine dans l'interface EMX et deux sessions distantes au maximum.

Remarque : pour cette rubrique, l'expéditeur du message est l'utilisateur A et le destinataire, l'utilisateur B.

Le destinataire peut accéder à l'image vidéo via le lien tant que l'une des conditions suivantes est respectée :

- La vidéo reste ouverte en mode Live Preview (Prévisualisation en temps réel) dans l'interface EMX de l'utilisateur A et que ce dernier ne se déconnecte pas de l'interface et que la session n'expire pas.

  Ou

- La vidéo reste ouverte dans une fenêtre Live Preview secondaire de l'interface EMX de l'utilisateur A. Tant que la fenêtre Live Preview secondaire est ouverte dans l'interface de l'utilisateur A, même si ce dernier se déconnecte ou que la session expire, le lien demeure disponible.

Meilleure pratique

Pour une meilleure pratique, dans l'interface EMX, l'utilisateur A doit ouvrir la vidéo dans une fenêtre Live Preview secondaire et laisser cette dernière ouverte au moins jusqu'à ce que l'utilisateur B ouvre cette vidéo par le biais du lien.

Lorsque l'utilisateur B a ouvert la vidéo, la fenêtre en mode Live Preview secondaire peut être fermée dans l'interface EMX de l'utilisateur A.

L'utilisateur B doit faire savoir manuellement à l'utilisateur A qu'il a ouvert le lien ou ce dernier peut vérifier si l'utilisateur B est actuellement connecté à l'application en cliquant sur Maintenance > Connected Users (Utilisateurs connectés).

Pour envoyer un lien vidéo par courriel ou par message instantané :

1. Dans l'arborescence de navigation, cliquez sur la webcam qui enregistre la vidéo pour laquelle vous souhaitez fournir un lien dans le courriel. La vidéo s'affiche en mode Live Preview dans le volet droit.
2. Cliquez sur l'icône Live Preview  placée au-dessus de la vidéo. Celle-ci s'ouvre dans une fenêtre Live Preview secondaire.
3. Copiez l'URL de la fenêtre Live Preview, collez-la dans l'application du courriel ou du message instantané. Laissez la fenêtre Live Preview ouverte jusqu'à ce que le destinataire ouvre la vidéo au moyen du lien.

Modems GSM

Un modem Cinteron® MC52i/MC55iGSM doit être connecté à EMX pour envoyer des messages d'événement SMS. Reportez-vous à ***Création des actions*** (à la page 136) pour en savoir plus sur les SMS d'événement.

Remarque : EMX ne peut pas recevoir de SMS.

Pour connecter le modem GSM :

1. Connectez le modem GSM au port série DB9 du dispositif EMX.
2. Configurez le modem GSM selon les besoins. Consultez l'aide accompagnant le modem GSM pour en savoir plus sur la configuration de celui-ci.

Echangeurs thermiques Schroff LHX

Après la connexion de l'échangeur thermique Schroff® LHX au dispositif EMX via le port Feature ou RS-485, EMX détecte LHX. L'échangeur LHX est visible dans le dossier Feature (Fonction) ou Auxiliary Port (Port auxiliaire) de l'arborescence de navigation, suivant le port auquel il est connecté.

Remarque : si vous connectez LHX au port Feature, utilisez le câble série fourni avec ce produit.

Depuis EMX, vous pouvez effectuer les opérations suivantes à distance :

- nommer un échangeur thermique LHX connecté ;
- configurer le point de contrôle de la température de sortie d'air ;
- configurer les seuils de température de sortie d'air ;
- configurer les seuils de température d'admission d'air ;
- configurer les seuils de température d'entrée d'eau ;
- configurer les seuils de vitesse de ventilateur ;
- surveiller la température d'admission d'air ;
- surveiller la température de sortie d'air ;
- surveiller la vitesse du ventilateur ;
- configurer les paramètres de base de l'échangeur thermique connecté, tels que les seuils de capteur.

Remarque : Ces paramètres sont stockés sur le port EMX où l'échangeur thermique est connecté, et sont perdus lorsque ce dernier est placé sur un port différent.

Reportez-vous à ***Connexion d'un échangeur thermique Schroff LHX (facultatif)*** (à la page 39) pour apprendre comment connecter l'échangeur thermique.

Activation et désactivation de la prise en charge de l'échangeur thermique Schroff LHX

Par défaut, la prise en charge de l'échangeur thermique Schroff LHX est désactivée. La prise en charge doit donc être activée avant que le dispositif n'apparaisse dans l'arborescence de navigation ou sur le tableau de bord. De plus, la prise en charge de l'échangeur thermique Schroff LHX doit être activée pour que LHX-MIB soit accessible via SNMP.

Pour activer l'échangeur thermique Schroff LHX :

1. Sélectionnez Device Settings > Features (Paramètres du dispositif > Fonctions), puis cochez la case Schroff Heat Exchanger dans le menu.
2. Cliquez sur Yes pour confirmer.
3. Redémarrez EMX.

Nommage d'un échangeur thermique

Pour permettre l'identification d'un échangeur thermique LHX dans l'interface Web de EMX, attribuez-lui un nom. Le nom personnalisé de l'échangeur personnalisé LHX est suivi du type de dispositif et du numéro de port RS-485 entre parenthèses.

L'interface Web fournit deux types de boîtes de dialogue de paramétrage pour le nommage d'un échangeur thermique LHX spécifique.

Pour nommer un échangeur thermique à l'aide de la boîte de dialogue Auxiliary Port Setup (Paramétrage des ports auxiliaires) :

1. Connectez l'échangeur thermique LHX à EMX si ce n'est pas encore fait.
2. Si le dossier EMX est réduit, développez-le pour afficher tous les composants.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif.
   Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*
3. Cliquez sur le dossier Auxiliary Ports (Ports auxiliaires). La page correspondante s'ouvre dans le volet de droite et affiche tous les ports RS-485.
4. Sélectionnez le port auquel l'échangeur thermique souhaité est connecté sur la page Auxiliary Ports (Ports auxiliaires) et cliquez sur Setup (Paramétrer). Ou double-cliquez simplement sur ce port. La boîte de dialogue Auxiliary Ports Setup (Paramétrage des ports auxiliaires) apparaît.

5. Tapez le nom de l'échangeur thermique dans le champ Name.
6. Cliquez sur OK pour enregistrer les modifications.

Pour nommer un échangeur thermique à l'aide de la boîte de dialogue de paramétrage correspondante :

1. Le cas échéant, développez le dossier Auxiliary Ports (Ports auxiliaires) de manière à afficher tous les dispositifs connectés aux ports RS-485.
2. Cliquez sur l'échangeur thermique souhaité dans le volet EMX Explorer. La page spécifique à cet échangeur s'ouvre dans le volet droit.
3. Cliquez sur Setup (Paramétrer) dans la section Settings (Paramètres).
4. Tapez le nom de l'échangeur thermique dans le champ Name.
5. Cliquez sur OK pour enregistrer les modifications.

Configuration des seuils de température et de ventilateur

Un échangeur thermique LHX est mis en œuvre avec divers capteurs pour détecter la température de l'air, celle de l'eau et la vitesse du ventilateur. Vous pouvez définir des seuils pour ces capteurs afin que EMX vous prévienne lorsque les relevés de capteur approchent une condition critique. Ces paramètres sont stockés sur le port EMX où l'échangeur thermique est connecté, et sont perdus lorsque ce dernier est placé sur un port différent.

Pour configurer les seuils d'un capteur :

1. Connectez l'échangeur thermique LHX à EMX si ce n'est pas encore fait.
2. Le cas échéant, développez le dossier Auxiliary Ports (Ports auxiliaires) de manière à afficher tous les dispositifs connectés aux ports RS-485.
3. Cliquez sur l'échangeur thermique souhaité dans le volet EMX Explorer. La page spécifique à cet échangeur s'ouvre dans le volet droit.
4. Sélectionnez le capteur souhaité dans le tableau Sensors et cliquez sur Setup Thresholds (Paramétrage des seuils), ou double-cliquez simplement sur le capteur concerné. La boîte de dialogue de paramétrage du capteur sélectionné apparaît.
5. Ajustez les paramètres de seuil et d'hystérésis d'infirmation. Les valeurs Upper Critical (critique supérieur) et Lower Critical (critique inférieur) sont des points auxquels le dispositif EMX considère que l'environnement d'exploitation est critique et en dehors de la plage du seuil acceptable.

- Pour activer un seuil, sélectionnez la case à cocher correspondante. Pour désactiver un seuil, décochez la case.
- Après l'activation d'un seuil, tapez une valeur numérique appropriée dans la zone de texte correspondante.
- Pour activer l'hystérésis d'infirmation pour tous les seuils, tapez une valeur numérique différente de zéro dans le champ Deassertion Hysteresis. Reportez-vous à ***Hystérésis d'infirmation : définition*** (à la page 178).

6. Cliquez sur OK pour enregistrer les modifications.

Surveillance de l'échangeur thermique

L'interface Web de EMX vous permet de surveiller le statut de chaque échangeur thermique LHX connecté, ainsi que celui de chaque capteur LHX intégré.

Affichage du récapitulatif

Les pages Dashboard (Tableau de bord) et Auxiliary Ports (Ports auxiliaires) affichent toutes les deux le récapitulatif de tous les échangeurs thermiques LHX connectés, notamment le numéro du port RS-485 auquel chaque échangeur est connecté, et le statut de chacun.

Si un échangeur thermique LHX est mis en surbrillance en rouge dans le récapitulatif, ceci signale une panne de capteur LHX sur cet échangeur. Consultez la colonne State (Etat) ou Status (Statut) pour identifier les capteurs défaillants.

Pour afficher le récapitulatif LHX sur la page Dashboard :

1. Cliquez sur l'icône Dashboard dans le volet EMX Explorer. La page correspondante s'ouvre dans le volet droit.
2. Repérez la section LHX Heat Exchanger où apparaît une liste des échangeurs thermiques LHX connectés.

Pour afficher le récapitulatif LHX sur la page Auxiliary Ports :

1. Si le dossier EMX est réduit, développez-le pour afficher tous les composants.

   Remarque : Le dossier EMX est nommé EMX par défaut. Le nom change après la personnalisation du nom du dispositif. Reportez-vous à **Nommage du dispositif EMX** *(à la page 73).*

2. Cliquez sur le dossier Auxiliary Ports (Ports auxiliaires). La page correspondante s'ouvre dans le volet de droite et affiche tous les ports RS-485.

Affichage des détails

La page d'un échangeur thermique LHX présente des informations détaillées, notamment :

- les données et paramètres du dispositif, tels que le numéro du port RS-485 et le nom du dispositif ;
- la température de sortie d'air ;
- les relevés et états de tous les capteurs LHX intégrés ;
- le cumul des heures de fonctionnement ;
- les erreurs, telles que les capteurs LHX défaillants et l'activation du système de refroidissement de secours.

Pour afficher les détails d'un échangeur thermique LHX spécifique :

1. Le cas échéant, développez le dossier Auxiliary Ports (Ports auxiliaires) de manière à afficher tous les dispositifs connectés aux ports RS-485.

   Cliquez sur l'échangeur thermique souhaité dans le volet EMX Explorer. La page spécifique à cet échangeur s'ouvre dans le volet droit.

Si un relevé de capteur LHX atteint ou dépasse le seuil critique ou d'avertissement, la rangée de ce relevé est mise en surbrillance en rouge ou en jaune. Reportez-vous à ***Relevés mis en surbrillance en jaune ou en rouge*** (à la page 58).

Etats de dispositifs et variations des icônes

L'interface Web de EMX change les icônes afin de représenter les différents statuts de chaque échangeur thermique LHX connecté.

Icônes	Statut du dispositif
	L'échangeur thermique est SOUS tension et fonctionne normalement.
	L'échangeur thermique est HORS tension.
	L'échangeur thermique est SOUS tension mais passe à un état critique à cause d'une panne d'un capteur LHX.
	Un des relevés de capteurs LHX au moins a franchi le seuil d'avertissement supérieur ou inférieur.
	AUCUN dispositif n'est détecté sur ce port RS-485.

Pour identifier la cause de l'état critique, consultez au choix :

- la section LHX Heat Exchanger (Echangeur thermique LHX) de la page Dashboard. Reportez-vous à ***Surveillance de l'échangeur thermique*** (à la page 201).
- La page Auxiliary Ports. Reportez-vous à ***Surveillance de l'échangeur thermique*** (à la page 201).
- La section Alert States (Etats d'alerte) de la page de l'échangeur thermique LHX. Reportez-vous à ***Etats d'alerte et journal d'événements LHX*** (à la page 203).

Etats d'alerte et journal d'événements LHX

Lorsque l'échangeur thermique LHX est connecté physiquement au dispositif EMX, une section intitulée Alert States (Etats d'alerte) apparaît sur sa page. La section Alert States présente des informations indiquant les capteurs LHX actuellement en panne.

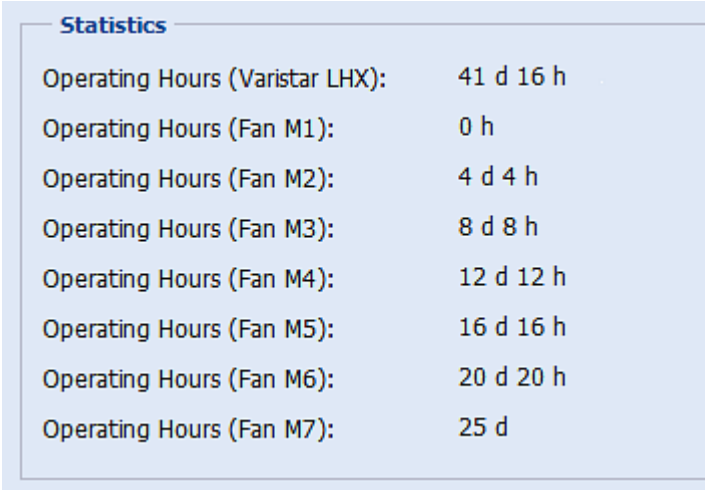
Conseil : les pages Dashboard et Auxiliary Ports répertorient également les capteurs défaillants. Reportez-vous à **Surveillance de l'échangeur thermique** *(à la page 201).*

Un bouton libellé Show Event Log (Afficher le journal d'événements) se trouve dans la section Alert States. Pour consulter les événements associés à EMX, cliquez sur ce bouton.

Heures de fonctionnement

Les heures de fonctionnement indiquent le temps accumulé depuis la connexion de l'échangeur thermique LHX au dispositif EMX et sa mise sous tension.

L'interface Web de EMX affiche les heures de fonctionnement de l'échangeur thermique et de ses ventilateurs. Les données d'heures de fonctionnement sont indiquées dans la section Statistics (Statistiques) de la page de chaque échangeur thermique.



Les unités de temps utilisées pour les heures de fonctionnement sont les suivantes :

- h : heure(s)
- d : jour(s)

Par exemple, 3d 5h indique que la période de fonctionnement totale est de 3 jours et 5 heures.

Contrôle de l'échangeur thermique

EMX permet de mettre sous tension et hors tension à distance un échangeur thermique connecté.

Pour contrôler un échangeur thermique LHX :

1. Le cas échéant, développez le dossier Auxiliary Ports (Ports auxiliaires) de manière à afficher tous les dispositifs connectés aux ports RS-485.

   Cliquez sur l'échangeur thermique souhaité dans le volet EMX Explorer. La page spécifique à cet échangeur s'ouvre dans le volet droit.

2. Recherchez la section Information.
   - Pour mettre hors tension l'échangeur thermique LHX, cliquez sur Switch Off.
   - Pour mettre sous tension l'échangeur thermique LHX, cliquez sur Switch On.
3. Si vous avez cliqué sur Switch Off à l'étape précédente, une boîte de dialogue apparaît, vous invitant à confirmer l'opération. Cliquez sur Yes pour mettre hors tension ou sur No pour abandonner l'opération.

L'icône de l'échangeur thermique affichée dans l'interface Web change après la mise sous ou hors tension. Reportez-vous à ***Etats de dispositifs et variations des icônes*** (à la page 202).

Chapitre 9 Utilisation de SNMP

Cette section SNMP vous indique comment paramétrer EMX pour l'utiliser avec un gestionnaire SNMP. EMX peut être configuré pour envoyer des traps à un gestionnaire SNMP, et pour recevoir des commandes GET et SET afin de récupérer un statut et de configurer certains paramètres de base.

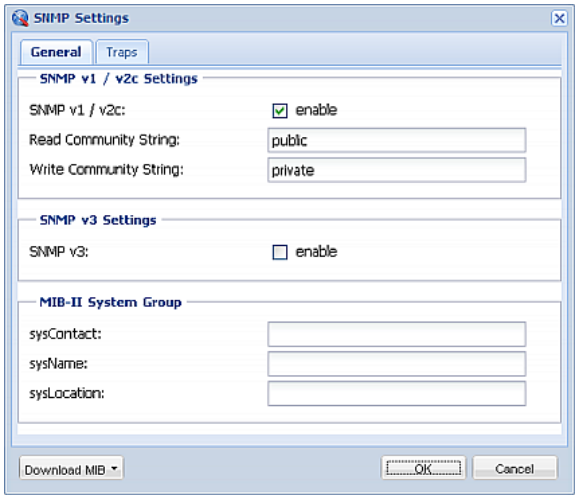
Dans ce chapitre

Activation de SNMP

Pour communiquer avec un gestionnaire SNMP, vous devez en premier lieu activer l'agent SNMP sur le dispositif EMX.

Pour activer SNMP :

1. Sélectionnez Device Settings > Network Services > SNMP (Paramètres du dispositif > Services réseau > SNMP). La boîte de dialogue SNMP Settings (Paramètres SNMP) s'affiche.



2. Cochez la case enable (activer) dans le champ SNMP v1 / v2c pour permettre la communication avec un gestionnaire SNMP à l'aide du protocole SNMP v1 ou v2c.

- Entrez la chaîne de communauté en lecture seule SNMP dans le champ Read Community String (Chaîne de communauté en lecture). En général, la chaîne est public.
- Entrez la chaîne de communauté en lecture/écriture dans le champ Write Community String (Chaîne de communauté en écriture). En général, la chaîne est private.

3. Cochez la case enable (activer) dans le champ SNMP v3 pour permettre la communication avec un gestionnaire SNMP à l'aide du protocole SNMP v3.

Conseil : vous pouvez autoriser ou interdire l'accès d'un utilisateur à EMX via le protocole SNMP v3. Reportez-vous à **Configuration des utilisateurs pour le protocole SNMP v3 chiffré** *(à la page 206).*

4. Tapez la valeur SNMP MIB-II sysContact dans le champ sysContact.
5. Tapez la valeur SNMP MIB-II sysName dans le champ sysName.
6. Tapez la valeur SNMP MIB-II sysLocation dans le champ sysLocation.
7. Cliquez sur OK pour enregistrer les modifications.

Important : vous devez télécharger le fichier MIB SNMP que votre EMX doit utiliser avec le gestionnaire SNMP. Cliquez sur Download MIB dans cette boîte de dialogue pour télécharger le fichier MIB souhaité. Pour plus d'informations, reportez-vous à *Téléchargement du fichier MIB SNMP* (à la page 208).

Configuration des utilisateurs pour le protocole SNMP v3 chiffré

Le protocole SNMP v3 permet une communication chiffrée. Pour tirer profit de ceci, les utilisateurs doivent disposer d'une phrase passe d'authentification et d'une phrase passe de confidentialité, qui agissent en tant que secrets partagés entre eux et EMX.

Pour configurer des utilisateurs pour la communication SNMP v3 chiffrée :

1. Choisissez User Management > Users (Gestion des utilisateurs > Utilisateurs). La boîte de dialogue Manage Users (Gérer les utilisateurs) apparaît.
2. Sélectionnez l'utilisateur en cliquant dessus.
3. Cliquez sur Edit (Modifier) ou double-cliquez sur l'utilisateur. La boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX), où XXX est le nom de l'utilisateur.
4. Pour modifier les autorisations d'accès SNMPv3, cliquez sur l'onglet SNMPv3 et effectuez les modifications nécessaires. Reportez-vous à l'étape 6 de ***Création d'un profil utilisateur*** (à la page 62).

5. Cliquez sur OK pour enregistrer les modifications. L'utilisateur peut maintenant communiquer à l'aide du protocole SNMP v3 chiffré.

Configuration des traps SNMP

EMX tient automatiquement un journal interne des événements qui se produisent. Reportez-vous à ***Configuration des règles d'événement*** (voir "***Règles et actions d'événement***" à la page 131). Ces événements peuvent également être utilisés pour envoyer des traps SNMP à un gestionnaire tiers.

Pour configurer l'envoi par EMX de traps SNMP :

1. Choisissez Device Settings > Event Rules (Paramètres du dispositif > Règles d'événement). La fenêtre Event Rule Settings (Paramètres des règles d'événement) s'affiche.
2. Dans l'onglet Rules (Règles), sélectionnez System SNMP Trap Rule (Règle de trap SNMP système).
3. Cochez la case Enabled (Activée) pour activer cette règle d'événement.
4. Cliquez sur Save pour enregistrer les modifications.
5. Cliquez sur l'onglet Actions si vous n'avez pas configuré les actions de trap SNMP.
6. Sélectionnez System SNMP Trap Action (Action de trap SNMP système) pour paramétrer les destinations de traps.
7. Entrez une adresse IP dans le champ Host 1 (Hôte 1). Il s'agit de l'adresse à laquelle les traps sont envoyés par l'agent système SNMP.
8. Entrez le numéro du port de communication dans le champ Port 1.
9. Entrez le nom de la communauté SNMP dans le champ Community (Communauté). La communauté est un groupe représentant EMX et toutes les stations de gestion SNMP.
10. Pour définir plusieurs destinations de traps SNMP, répétez les étapes 8 à 10 pour chacune. Trois destinations au plus peuvent être définies.
11. Cliquez sur Save pour enregistrer les modifications.
12. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Remarque : il est recommandé de mettre à jour le fichier MIB utilisé par le gestionnaire SNMP à la mise à jour vers une nouvelle version de EMX. Ainsi, votre gestionnaire SNMP dispose du fichier MIB correspondant à la version que vous utilisez. Reportez-vous à **Téléchargement du fichier MIB SNMP** *(à la page 208).*

Requêtes SNMP Get et Set

Outre l'envoi de traps, EMX peut recevoir des requêtes Get et Set SNMP provenant de gestionnaires SNMP tiers.

- Les requêtes Get servent à extraire des informations concernant EMX, telles que l'emplacement du système.
- Les requêtes Set permettent de configurer un sous-ensemble de ces informations, tel que le nom du système SNMP.

Remarque : le nom du système SNMP est le nom du dispositif EMX. Lorsque vous changez le nom du système SNMP, le nom du dispositif affiché dans l'interface Web est également modifié.

EMX NE PREND PAS EN CHARGE la configuration des paramètres relatifs à IPv6 via des requêtes Set SNMP.

Les objets autorisés pour ces requêtes sont limités à ceux trouvés dans le groupe système SNMP MIB-II et le fichier MIB personnalisé de EMX.

Fichier MIB de EMX

Le fichier MIB SNMP est obligatoire pour utiliser le dispositif EMX avec un gestionnaire SNMP. Un fichier MIB SNMP décrit les fonctions SNMP.

Téléchargement du fichier MIB SNMP

Le fichier MIB SNMP de EMX est facilement téléchargeable depuis l'interface Web. Il existe deux manières de télécharger le fichier MIB SNMP.

Pour télécharger le fichier depuis la boîte de dialogue SNMP Settings (Paramètres SNMP) :

1. Sélectionnez Device Settings > Network Services > SNMP (Paramètres du dispositif > Services réseau > SNMP). La boîte de dialogue SNMP Settings (Paramètres SNMP) s'affiche.
2. Cliquez sur Download MIB (Télécharger le fichier MIB). Un sous-menu de fichiers MIB apparaît.
3. Sélectionnez le fichier MIB souhaité.
   - EMD-MIB : fichier MIB SNMP de gestion du dispositif EMX.
   - ASSETMANAGEMENT-MIB : fichier MIB SNMP de gestion des ressources.
   - LHX-MIB : fichier MIB SNMP de gestion des échangeurs thermiques LHX.

Remarque : la prise en charge Schroff LHX doit être activée pour que LHX-MIB soit disponible. Reportez-vous à **Activation et désactivation de la prise en charge de l'échangeur thermique Schroff LHX** *(à la page 199).*

4. Cliquez sur Save (Enregistrer) pour enregistrer le fichier sur votre ordinateur.

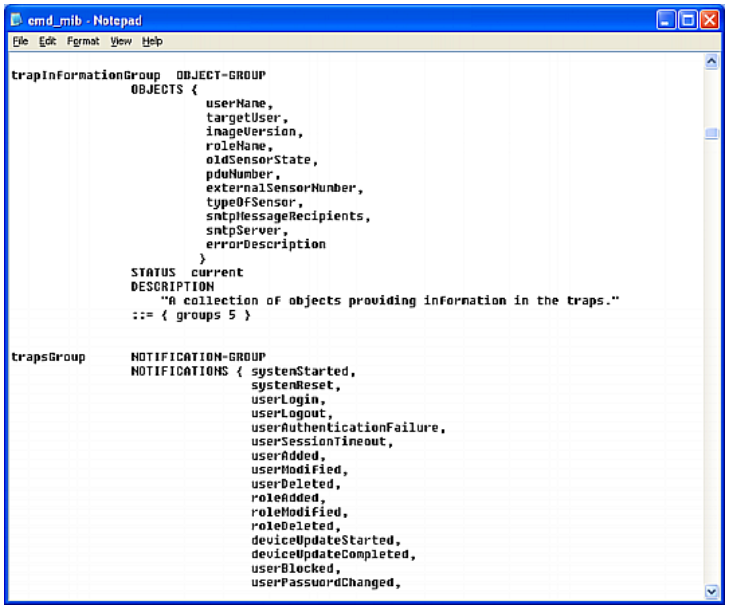
Pour télécharger le fichier depuis la boîte de dialogue Device Information (Informations sur le dispositif) :

1. Sélectionnez Maintenance > Device Information (Informations sur le dispositif). La boîte de dialogue Device Information s'affiche.
2. Cliquez sur le lien de téléchargement dans le champ EMD-MIB, ASSETMANAGEMENT-MIB ou LHX-MIB pour télécharger le fichier MIB SNMP désiré.
3. Cliquez sur Save (Enregistrer) pour enregistrer le fichier sur votre ordinateur.

Présentation

L'ouverture du fichier MIB révèle les objets personnalisés qui décrivent le système EMX.

Généralement, ces objets sont présentés au début du fichier, répertoriés sous leur groupe parent. Ils réapparaissent ensuite individuellement, définis et décrits de manière détaillée.



Par exemple, le groupe measurementsGroup contient des objets pour les capteurs d'environnement connectés au dispositif EMX. Un objet répertorié sous ce groupe, measurementsUnitSensorValue, est décrit plus loin dans le fichier MIB comme The sensor state. boardFirmwareVersion, du groupe configGroup, décrit la version du firmware.

Commandes Set et seuils SNMP

Certains objets peuvent être configurés à partir du gestionnaire SNMP à l'aide de commandes Set SNMP. Les objets configurables ont un niveau MAX-ACCESS en « lecture-écriture » dans le fichier MIB.

Ils comprennent des objets de seuil, ce qui provoque l'émission d'un avertissement par EMX et l'envoi d'un trap SNMP lorsque certains paramètres sont dépassés. Reportez-vous à ***Informations sur les seuils*** (à la page 178) pour obtenir une description du fonctionnement des seuils.

Remarque : lors de la configuration des seuils à l'aide des commandes set SNMP, vérifiez que la valeur du seuil critique supérieur est plus élevé que celle du seuil d'avertissement supérieur.

Chapitre 10 Utilisation de l'interface de ligne de commande

Dans ce chapitre

A propos de l'interface

EMX offre une interface de ligne de commande qui permet aux administrateurs de centres de données d'effectuer certaines tâches de gestion de base.

A l'aide de cette interface, vous pouvez effectuer les opérations suivantes :

- Réinitialiser le dispositif EMX
- Afficher les données de EMX et du réseau, telles que le nom du dispositif, la version du firmware, l'adresse IP, etc.
- Configurer les paramètres de EMX et du réseau.
- Résoudre les problèmes de réseau.

Cette interface est accessible à l'aide d'une connexion série utilisant un programme d'émulation de terminal, tel qu'HyperTerminal, ou via un client Telnet ou SSH comme PuTTY.

Remarque : l'accès Telnet est désactivé par défaut car la communication s'effectue en clair et n'est donc pas sécurisée. Pour activer Telnet, reportez-vous à **Modification des paramètres des services réseau** *(à la page 87).*

Connexion à l'interface CLI

La connexion via HyperTerminal par une connexion locale est un peu différente de la connexion avec SSH ou Telnet.

Avec HyperTerminal

Vous pouvez utiliser un programme d'émulation de terminal quelconque pour accéder localement à l'interface de ligne de commande.

Cette section illustre HyperTerminal, inclus aux systèmes d'exploitation Windows avant Windows Vista.

Pour vous connecter à l'aide d'HyperTerminal :

1. Reliez votre ordinateur au dispositif EMX à l'aide d'une connexion locale.
2. Lancez HyperTerminal sur votre ordinateur et ouvrez une fenêtre de console. Lorsque celle-ci s'ouvre, elle est vide.

   Vérifiez que les paramètres de port COM utilisent la configuration suivante :

   - Bits par seconde = 115200 (115,2Kbps)
   - Bits de données = 8
   - Bits d'arrêt = 1
   - Parité = Néant
   - Contrôle de flux = Néant

   Conseil : pour une connexion USB, vous pouvez déterminer le port COM affecté à EMX en choisissant Panneau de configuration > Système > Matériel > Gestionnaire de périphériques et en repérant la console série Dominion sous le groupe Ports.
3. Appuyez sur Entrée. L'invite Username apparaît.

   ```
   Username: _
   ```
4. Tapez un nom et appuyez sur Entrée. Le nom est sensible à la casse, veillez à mettre les bonnes lettres en majuscules. Vous êtes ensuite invité à saisir un mot de passe.

```
Username: admin
Password: _
```

5. Tapez un mot de passe et appuyez sur Entrée. Le mot de passe est sensible à la casse, veillez à mettre les bonnes lettres en majuscules.

   Après la saisie correcte du mot de passe, # ou l'invite système > apparaît. Reportez-vous à ***Divers modes et invites de l'interface CLI*** (à la page 214) pour en savoir plus.

   Conseil : les données Last Login (Dernière connexion), comprenant les date et heure, sont également affichées si le même profil utilisateur a servi une fois à la connexion à l'interface Web ou à la CLI de EMX.

6. Vous êtes maintenant connecté à l'interface de ligne de commande et pouvez à présent administrer le dispositif EMX.

Avec SSH ou Telnet

Vous pouvez vous connecter à distance à l'interface de ligne de commande à l'aide d'un client SSH ou Telnet, tel que PuTTY.

Remarque : PuTTY est un programme libre téléchargeable depuis Internet. Reportez-vous à la documentation de PuTTY pour en savoir plus sur la configuration.

Pour vous connecter à l'aide de SSH ou de Telnet :

1. Assurez-vous que SSH ou Telnet est activé. Reportez-vous à ***Modification des paramètres des services réseau*** (à la page 87).
2. Lancez un client SSH ou Telnet et ouvrez une fenêtre de console. Une invite de connexion apparaît.

```
login as:
```

3. Tapez un nom et appuyez sur Entrée. Le nom est sensible à la casse, veillez à mettre les bonnes lettres en majuscules.

   Remarque : si vous utilisez le client SSH, le nom NE DOIT PAS dépasser 25 caractères. Sinon, la connexion échoue.

   Vous êtes ensuite invité à saisir un mot de passe.

```
login as: admin
admin@192.168.84.88's password:
```

4. Tapez un mot de passe et appuyez sur Entrée. Le mot de passe est sensible à la casse, veillez à mettre les bonnes lettres en majuscules.
5. Après la saisie correcte du mot de passe, # ou l'invite système > apparaît. Reportez-vous à ***Divers modes et invites de l'interface CLI*** (à la page 214) pour en savoir plus.

   Conseil : les données Last Login (Dernière connexion), comprenant les date et heure, sont également affichées si le même profil utilisateur a servi une fois à la connexion à l'interface Web ou à la CLI de EMX.

6. Vous êtes maintenant connecté à l'interface de ligne de commande et pouvez à présent administrer le dispositif EMX.

Divers modes et invites de l'interface CLI

Suivant votre nom de connexion et le mode utilisé, l'invite système dans l'interface CLI varie.

- Mode utilisateur : lorsque vous vous connectez comme utilisateur normal, qui ne dispose pas des autorisations complètes pour configurer le dispositif EMX, l'invite **>** apparaît.
- Mode administrateur : lorsque vous vous connectez en tant qu'administrateur, qui dispose des autorisations complètes pour configurer EMX, l'invite # apparaît.
- Mode configuration : vous pouvez passer en mode configuration à partir du mode administrateur. Dans ce mode, l'invite devient **config:#** et vous pouvez modifier la configuration du dispositif EMX et du réseau. Reportez-vous à ***Passage en mode configuration*** (à la page 227).
- Mode diagnostic : vous pouvez passer en mode diagnostic à partir du mode administrateur. Dans ce mode, l'invite devient **diag:>** et vous pouvez utiliser les commandes de dépannage du réseau, comme la commande ping. Reportez-vous à ***Passage en mode diagnostic*** (à la page 319).

Fermeture d'une connexion série

Fermez la fenêtre ou le programme d'émulation de terminal lorsque vous avez accédé à un dispositif EMX par la connexion série.

Lorsque vous accédez à ou mettez à jour plusieurs dispositifs EMX, ne transférez pas le câble série d'un dispositif à un autre sans fermer tout d'abord la fenêtre de connexion série.

Commande Help (Aide)

La commande help présente une liste des commandes CLI principales. Ceci est utile lorsque vous n'êtes pas familiarisé avec les commandes.

La syntaxe de la commande help est la suivante :

```
#      help
```

Appuyez sur la touche Entrée après avoir tapé la commande et une liste des commandes principales s'affiche.

Conseil : vous pouvez vérifier les paramètres disponibles pour une commande CLI spécifique en ajoutant un point d'interrogation à la fin de la commande. Reportez-vous à **Recherche des paramètres disponibles pour une commande** *(à la page 323).*

Affichage des données

Vous pouvez utiliser les commandes show pour consulter les paramètres ou le statut actuels du dispositif EMX ou une partie, comme l'adresse IP, le mode de gestion du réseau, la version du firmware, etc.

Certaines commandes show ont deux formats : un avec le paramètre « details » et l'autre, sans. La différence est que la commande sans le paramètre « details » affiche une version abrégée des données alors que l'autre présente des données approfondies.

Après avoir tapé une commande show, appuyez sur Entrée pour l'exécuter.

Remarque : selon votre nom de connexion, l'invite # peut être remplacée par l'invite >.

Configuration du réseau

Cette commande affiche toute la configuration du réseau, notamment l'adresse IP, le mode de mise en réseau et l'adresse MAC.

```
#        show network
```

Configuration IP

Cette commande affiche uniquement la configuration IP, telle qu'une configuration IPv4 et IPv6, les adresses, la passerelle et le masque de sous-réseau.

```
#        show network ip <option>
```

Variables :

- <option> est une des options : *all*, *v4* ou *v6*.

Option	Description
all	Cette option affiche les paramètres IPv4 et IPv6. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
v4	Cette option affiche les paramètres IPv4 uniquement.
v6	Cette option affiche les paramètres IPv6 uniquement.

Paramètres de l'interface LAN

Cette commande affiche uniquement les données de l'interface LAN (réseau local), telles que la vitesse, le mode bidirectionnel et le statut de l'interface LAN courante.

```
#        show network interface
```

Mode de mise en réseau

Cette commande indique si le mode actuel de gestion du réseau est avec fil ou sans fil.

```
#        show network mode
```

Configuration sans fil

Cette commande affiche uniquement la configuration sans fil du dispositif EMX, telle que le paramètre SSID.

```
#        show network wireless
```

Pour afficher des informations détaillées, ajoutez le paramètre « details » à la fin de la commande.

```
#        show network wireless details
```

Paramètres des services réseau

Cette commande affiche uniquement les paramètres des services du réseau, notamment le paramètre Telnet, les ports TCP pour les services HTTP, HTTPS et SSH, et les paramètres SNMP.

```
#        show network services <option>
```

Variables :

- <option> est une des options : *all*, *http*, *https*, *telnet*, *ssh*, *snmp* et *zeroconfig*.

Option	Description
all	Affiche les paramètres de tous les services réseau, notamment HTTP, HTTPS, Telnet, SSH et SNMP. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
http	N'affiche que le port TCP du service HTTP.
https	N'affiche que le port TCP du service HTTPS.
telnet	N'affiche que les paramètres du service Telnet.
ssh	N'affiche que les paramètres du service SSH.
snmp	N'affiche que les paramètres SNMP.
zeroconfig	N'affiche que les paramètres de publication sans configuration.

Paramètres des capteurs de ressources

Cette commande affiche les paramètres du capteur de ressources, tels que le nombre total d'unités de rack (ports d'étiquette), l'état du capteur, le mode de numérotation, l'orientation, les étiquettes disponibles et les paramètres de couleurs des voyants.

```
#        show assetStrip <n>
```

Variables :

- <n> est une des options : *all* ou un numéro.

Option	Description
all	Affiche les informations de tous les capteurs de ressources. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
Un numéro de capteur de ressources spécifique	Affiche les paramètres du capteur de ressources connecté au numéro de port FEATURE indiqué. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro correct est toujours 1.

Cette syntaxe de commande définit la couleur des voyants de toutes les unités de rack sur le(s) capteur(s) de ressources connecté(s) pour indiquer l'absence d'une étiquette de gestion des ressources connectées.

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables :

- <color> est la valeur RVB hexadécimale d'une couleur au format HTML. La variable <color> est comprise entre #000000 et #FFFFFF.

Informations sur les capteurs d'environnement

Cette syntaxe de commande affiche des informations sur le capteur d'environnement indiqué.

```
#        show sensor externalsensor <n>
```

Pour afficher des informations détaillées, ajoutez le paramètre « details » à la fin de la commande.

```
#        show sensor externalsensor <n> details
```

Variables :

- <n> est le numéro du capteur d'environnement. Le numéro de capteur d'environnement est le numéro d'identification affecté au capteur. Ce numéro est indiqué sur la page External Sensors (Capteurs externes) de l'interface Web de EMX.

Informations affichées :

- Sans le paramètre « details », seuls les paramètres de relevé, de seuil, d'hystérésis d'infirmation et de délai d'affirmation du capteur d'environnement spécifié sont affichés.
- Avec le paramètre « details », des informations supplémentaires sur les capteurs sont affichées, comme la précision et la portée.

Remarque : pour un capteur discret (activé/désactivé), les données relatives au seuil et à la précision NE SONT PAS disponibles.

Informations sur les capteurs d'environnement

Cette syntaxe de commande affiche les informations sur les capteurs d'environnement.

```
#        show externalsensors <n>
```

Pour afficher des informations détaillées, ajoutez le paramètre « details » à la fin de la commande.

```
#        show externalsensors <n> details
```

Variables :

- <n> est une des options : *all* ou un numéro.

Option	Description
all	Affiche les informations de tous les capteurs d'environnement. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
Un numéro de capteur d'environnement spécifique*	Affiche les informations concernant le capteur d'environnement indiqué uniquement.

* Le numéro de capteur d'environnement est le numéro d'identification affecté au capteur. Ce numéro est indiqué sur la page External Sensors (Capteurs externes) de l'interface Web de EMX.

Informations affichées :

- Sans le paramètre « details », seuls l'ID du capteur, son type et son relevé sont affichés.

  Remarque : un capteur discret (activé/désactivé) affiche l'état du capteur au lieu du relevé.

- Avec le paramètre « details », des informations supplémentaires sont affichées en plus du numéro d'identification et du relevé du capteur d'environnement, notamment le numéro de série et les coordonnées X, Y et Z.

Informations sur les seuils des capteurs d'environnement

Cette syntaxe de commande affiche les informations relatives aux seuils du capteur d'environnement indiqué.

```
#        show sensor externalsensor <n>
```

Pour afficher des informations détaillées, ajoutez le paramètre « details » à la fin de la commande.

```
#        show sensor externalsensor <n> details
```

Variables :

- <n> est le numéro du capteur d'environnement. Le numéro de capteur d'environnement est le numéro d'identification affecté au capteur. Ce numéro est indiqué sur la page External Sensors (Capteurs externes) de l'interface Web de EMX.

Informations affichées :

- Sans le paramètre « details », seuls les paramètres de relevé, de seuil, d'hystérésis d'infirmation et de délai d'affirmation du capteur d'environnement spécifié sont affichés.
- Avec le paramètre « details », des informations supplémentaires sur les capteurs sont affichées, comme la précision et la portée.

Remarque : pour un capteur discret (activé/désactivé), les données relatives au seuil et à la précision NE SONT PAS disponibles.

Security Settings (Paramètres de sécurité)

Cette commande affiche les paramètres de sécurité du dispositif EMX.

```
#        show security
```

Pour afficher des informations détaillées, ajoutez le paramètre « details » à la fin de la commande.

```
#        show security details
```

Informations affichées :

- Sans le paramètre « details », les informations comprenant le contrôle d'accès IP, le contrôle d'accès basé rôle, la stratégie en matière de mot de passe et le chiffrement HTTPS sont affichées.
- Avec le paramètre « details », des informations de sécurité supplémentaires sont affichées, notamment la durée de blocage et le délai d'inactivité des utilisateurs.

Profils utilisateur existants

Cette commande affiche les données d'un ou de tous les profils utilisateur existants.

```
#        show user <user_name>
```

Pour afficher des informations détaillées, ajoutez le paramètre « details » à la fin de la commande.

```
#        show user <user_name> details
```

Variables :

- <user_name> est le nom de l'utilisateur dont vous souhaitez interroger le profil. La variable peut être une de ces options : *all* ou un nom d'utilisateur.

Option	Description
all	Cette option affiche tous les profils utilisateur existants. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*

Option	Description
le nom d'un utilisateur spécifique	Cette option affiche le profil de l'utilisateur indiqué uniquement.

Informations affichées :

- Sans le paramètre « details », seules quatre informations utilisateur sont affichées : nom d'utilisateur, statut « activé », privilèges d'accès SNMP v3 et rôles.
- Avec le paramètre « details », des informations utilisateur supplémentaires sont affichées, telles que le numéro de téléphone, l'adresse électronique, l'unité de température privilégiée, etc.

Rôles existants

Cette commande affiche les données d'un ou de tous les rôles existants.

```
#        show roles <role_name>
```

Variables :

- <role_name> est le nom du rôle dont vous souhaitez interroger les autorisations. La variable peut être une des options suivantes :

Option	Description
all	Cette option affiche tous les rôles existants. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
le nom d'un rôle spécifique	Cette option affiche les données du rôle indiqué uniquement.

Informations affichées :

- Les paramètres du rôle sont affichés, notamment sa description et les privilèges.

Paramètres d'unités de rack d'un capteur de ressources

Pour le capteur de ressources Raritan, une unité de rack fait référence à un port d'étiquette. Cette commande affiche les paramètres d'une unité de rack spécifique ou de toutes les unités de rack d'un capteur de ressources, tels que la couleur et le mode des voyants d'une unité de rack.

```
#        show rackUnit <n> <rack_unit>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <rack_unit> est une des options : *all* ou le numéro d'index d'une unité de rack spécifique.

Option	Description
all	Affiche les paramètres de toutes les unités de rack d'un capteur de ressources indiqué. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
Un nombre spécifique	Affiche les paramètres d'une unité de rack spécifique du capteur de ressources indiqué. Utilisez le numéro d'index pour indiquer l'unité de rack. Le numéro d'index de chaque unité de rack est disponible sur la page Asset Strip (Bandeau de ressources) de l'interface Web.

Paramètres des bandeaux d'extensions de lames

Cette commande présente les données d'un bandeau d'extension de lame, notamment le nombre total de ports d'étiquette, et si disponible, le numéro d'identification (code à barres) de n'importe quelle étiquette connectée.

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <rack_unit> est le numéro d'index de l'unité de rack (port d'étiquette) souhaitée sur le capteur de ressources sélectionné. Le numéro d'index de chaque unité de rack est disponible sur la page Asset Strip (Bandeau de ressources) de l'interface Web.
- <blade_slot> est une de ces options : *all* ou le numéro d'un port d'étiquette particulier sur le bandeau d'extension de lame.

Option	Description
all	Affiche les données de tous les ports d'étiquette sur le bandeau d'extension de lame indiqué, connecté à une unité de rack particulière. *Conseil : vous pouvez également entrer la commande sans ajouter cette option all pour obtenir les mêmes données.*
Un nombre spécifique	Affiche les données du port d'étiquette indiqué sur le bandeau d'extension de lame connecté à une unité de rack particulière. Le numéro de chaque port d'étiquette sur le bandeau d'extension de lame est disponible sur la page Asset Strip (Bandeau de ressources).

Historique des commandes

Cette syntaxe de commande affiche l'historique des commandes de la session de connexion en cours.

```
#       show history
```

Informations affichées :

- Une liste des commandes entrées précédemment au cours de la session active est affichée.

Longueur de la mémoire tampon d'historique

Cette syntaxe de commande affiche la longueur de la mémoire tampon stockant les commandes d'historique.

```
#       show history bufferlength
```

Informations affichées :

- La longueur de la mémoire tampon d'historique actuelle est affichée.

Exemples

Cette section présente des exemples de la commande show.

Exemple 1 - Informations de base de la sécurité

Le schéma présente le résultat de la commande *show security*.

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Exemple 2 - Informations approfondies de la sécurité

Des informations supplémentaires sont affichées lorsque vous entrez la commande *show security details*.

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Configuration du dispositif EMX et du réseau

Pour configurer le dispositif EMX ou les paramètres du réseau à l'aide de l'interface CLI, vous devez vous connecter en tant qu'administrateur.

Passage en mode configuration

Vous devez passer en mode configuration puisque les commandes de configuration ne fonctionnent qu'ici.

Pour passer en mode configuration :

1. Assurez-vous que vous êtes passé en mode administrateur et que l'invite # est affichée.

   Remarque : si vous passez en mode configuration depuis le mode utilisateur, vous disposerez peut-être d'autorisations limitées pour modifier la configuration. Reportez-vous à **Divers modes et invites de l'interface CLI** *(à la page 214).*

2. Tapez `config` et appuyez sur Entrée. L'invite config:# apparaît, indiquant que vous êtes passé en mode de configuration.

   ```
   config:# _
   ```

3. Vous pouvez maintenant entrer n'importe quelle commande de configuration et appuyer sur Entrée pour modifier les paramètres.

Important : pour appliquer de nouveaux paramètres de configuration, vous devez émettre la commande d'application apply

avant de fermer le programme d'émulation de terminal. La fermeture du programme n'enregistre pas les modifications de configuration. Reportez-vous à *Fermeture du mode configuration* (à la page 317).

Commandes de configuration de dispositif

Une commande de configuration de dispositif débute par *emd*. Vous pouvez utiliser ces commandes pour modifier les paramètres qui s'appliquent à tout le dispositif EMX.

Les commandes sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules.

Modification du nom du dispositif

Cette syntaxe de commande modifie le nom du dispositif EMX.

```
config:#    emd name "<name>"
```

Variables :

- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII. La variable <name> doit être entourée de guillemets lorsqu'elle contient des espaces.

Exemple

La commande suivante attribue le nom my emx888 au dispositif EMX.

```
config:#    emd name "my emx888"
```

Définition du format de la coordonnée Z pour les capteurs d'environnement

Cette syntaxe de commande active ou désactive l'utilisation d'unités de rack pour définir la hauteur (coordonnée Z) des capteurs d'environnement.

```
config:#    emd externalSensorsZCoordinateFormat <option>
```

Variables :

- <option> est une des options : *rackUnits* ou *freeForm*.

Option	Description
rackUnits	la hauteur de la coordonnée Z est mesurée en unités de rack standard. Lorsque cette option est sélectionnée, vous pouvez taper une valeur numérique dans l'unité de rack afin de décrire la coordonnée Z d'un capteur d'environnement.
freeForm	une chaîne alphanumérique quelconque peut être utilisée pour spécifier la coordonnée Z.

Remarque : après avoir déterminé le format de la coordonnée Z, vous pouvez lui définir une valeur. Reportez-vous à **Définition de la coordonnée Z** *(à la page 282).*

Exemple

La commande suivante détermine que l'unité de rack sert à définir la coordonnée Z des capteurs d'environnement.

```
config:#    emd externalSensorsZCoordinateFormat rackUnits
```

Activation ou désactivation de la consignation de données

Cette syntaxe de commande active ou désactive la fonction de consignation de données.

```
config:#    emd dataRetrieval <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Active la fonction de consignation de données.
disable	Désactive la fonction de consignation de données.

Pour plus d'informations, reportez-vous à ***Définition de la consignation de données*** (à la page 171).

Exemple

La commande suivante active la fonction de consignation de données.

```
config:#    emd dataRetrieval enable
```

Définition des mesures de consignation de données par entrée

Cette syntaxe de commande définit le nombre de mesures accumulées par entrée de journal.

```
config:#    emd measurementsPerLogEntry <number>
```

Variables :

- <number> est un nombre entier compris entre 1 et 600. La valeur par défaut est de 60 échantillons par entrée de journal.

Pour plus d'informations, reportez-vous à ***Définition de la consignation de données*** (à la page 171).

Exemple

La commande suivante détermine que 66 mesures sont accumulées par entrée de journal par les capteurs, c'est-à-dire, 66 secondes.

```
config:#    emd measurementsPerLogEntry 66
```

Commandes de configuration de réseau

Plusieurs paramètres de réseau peuvent être modifiés à l'aide de l'interface CLI, tels que l'adresse IP, la vitesse de transmission, le mode bidirectionnel, etc.

Définition du mode de gestion du réseau

Si le dispositif EMX est mis en œuvre avec des mécanismes de mise en réseau câblés et sans fil, vous devez déterminer le mécanisme activé pour la connectivité avant de configurer davantage les paramètres réseau.

Cette syntaxe de commande active le mode de mise en réseau câblé ou sans fil.

```
config:#    network mode <mode>
```

Variables :

- <mode> est un des modes : *wired* ou *wireless*.

Mode	Description
wired	Active le mode de mise en réseau câblé.
wireless	Active le mode de mise en réseau sans fil.

Remarque : si vous activez le mode de mise en réseau sans fil et que EMX ne détecte aucun adaptateur de réseau local USB ou que ce dernier n'est pas pris en charge, le message Supported Wireless device not found (Dispositif sans fil pris en charge introuvable) est affiché.

Exemple

La commande suivante active le mode de mise en réseau câblé.

```
config:#    network mode wired
```

Configuration des paramètres de protocole IP

Par défaut, seul le protocole IPv4 est activé. Vous pouvez activer les protocoles IPv4 et IPv6, ou le protocole IPv6 seul pour votre dispositif EMX.

Une commande de configuration du protocole IP débute par *network ip*.

Activation d'IPv4 ou IPv6

Cette syntaxe de commande détermine le protocole IP activé sur EMX.

```
config:#   network ip proto <protocol>
```

Variables :

- <protocol> est une de ces options : *v4Only*, *v6Only* ou *both*.

Mode	Description
v4Only	Active uniquement IPv4 sur toutes les interfaces. Il s'agit de la valeur par défaut.
v6Only	Active uniquement IPv6 sur toutes les interfaces.
both	Active IPv4 et IPv6 sur toutes les interfaces.

Exemple

La commande détermine que les protocoles IPv4 et IPv6 sont activés.

```
config:#   network ip proto both
```

Sélection des adresses IPv4 ou IPv6

Cette syntaxe de commande détermine l'adresse IP utilisée lorsque le serveur DNS retourne à la fois des adresses IPv4 et IPv6. Vous ne devez configurer ce paramètre qu'après l'activation des protocoles IPv4 et IPv6 sur EMX.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variables :

- <resolver> est une de ces options : *preferV4* ou *preferV6*.

Option	Description
preferV4	Utilisez les adresses IPv4 renvoyées par le serveur DNS.
preferV6	Utilisez les adresses IPv6 renvoyées par le serveur DNS.

Exemple

La commande détermine que seules les adresses IPv4 retournées par le serveur DNS sont utilisées.

```
config:#   network ip dnsResolverPreference preferV4
```

Définition des paramètres sans fil

Vous devez configurer des paramètres sans fil, dont le nom du réseau sans fil (SSID), la méthode d'authentification, la clé prépartagée (PSK) et l'identificateur BSSID après l'activation du mode de mise en réseau sans fil.

Une commande de configuration sans fil débute par *network wireless*.

Remarque : si le mode actuel de mise en réseau n'est pas sans fil, les valeurs SSID, PSK et BSSID ne seront appliquées que lorsque le mode deviendra sans fil. En outre, un message apparaît indiquant que l'interface réseau active n'est pas sans fil.

Les commandes sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules.

Définition du nom de réseau sans fil

Cette syntaxe de commande définit la chaîne SSID.

```
config:#    network wireless SSID <ssid>
```

Variables :

- <ssid> est le nom du point d'accès sans fil qui comporte :
  - 32 caractères ASCII au plus
  - Aucun espace
  - Des codes ASCII 0x20 ~ 0x7E

Exemple

La commande suivante affecte myssid en tant que SSID.

```
config:#    network wireless SSID myssid
```

Définition de la méthode d'authentification

Cette syntaxe de commande définit la méthode d'authentification sur PSK ou EAP (Extensible Authentication Protocol).

```
config:#    network wireless authMethod <method>
```

Variables :

- <method> est une de ces méthodes d'authentification : *PSK* ou *EAP*.

Méthode	Description
PSK	La méthode d'authentification sans fil est définie sur PSK.
EAP	La méthode d'authentification sans fil est définie sur EAP.

Exemple

La commande suivante définit la méthode d'authentification sans fil sur PSK.

```
config:#    network wireless authMethod PSK
```

Définition de la clé prépartagée (PSK)

Si la méthode d'authentification Clé prépartagée (PSK) est sélectionnée, vous devez affecter une phrase passe en utilisant cette syntaxe de commande.

```
config:#   network wireless PSK <psk>
```

Variables :

- <psk> est une chaîne ou phrase passe qui comprend :

  - 32 caractères ASCII au plus

  - Aucun espace

  - Des codes ASCII 0x20 ~ 0x7E

Exemple

Cette commande affecte encryp-key comme clé prépartagée.

```
config:#   network wireless PSK encryp-key
```

Définition des paramètres du protocole EAP

Lorsque la méthode d'authentification sans fil est définie sur EAP, vous devez configurer des paramètres d'authentification EAP, notamment authentification externe, authentification interne, identité EAP, mot de passe et certificat d'autorité de certification.

Définition de l'authentification externe

Cette syntaxe de commande détermine le protocole d'authentification externe pour EAP.

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

Variables :

- La valeur d'<outer_auth> est *PEAP* car EMX ne prend en charge que le protocole PEAP (Protected Extensible Authentication Protocol) pour l'authentification externe.

Exemple

La commande suivante détermine que le protocole d'authentification externe pour l'authentification EAP est PEAP (Protected Extensible Authentication Protocol).

```
config:#   network wireless eapOuterAuthentication PEAP
```

Définition de l'authentification interne

Cette syntaxe de commande détermine le protocole d'authentification interne pour EAP.

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

Variables :

- La valeur d'<inner_auth> est *MSCHAPv2* car EMX ne prend en charge que Challenge Authentication Protocol Version 2 (MSCHAPv2) de Microsoft pour l'authentification interne.

Exemple

La commande suivante détermine que le protocole d'authentification interne pour l'authentification EAP est MSCHAPv2.

```
config:#   network wireless eapInnerAuthentication MSCHAPv2
```

Définition de l'identité EAP

Cette syntaxe de commande détermine l'identité EAP.

```
config:#   network wireless eapIdentity <identity>
```

Variables :

- <identity> représente votre nom d'utilisateur pour l'authentification EAP.

Exemple

La commande suivante définit l'identité EAP sur eap_user01.

```
config:#   network wireless eapIdentity eap_user01
```

Définition du mot de passe EAP

Cette syntaxe de commande détermine le mot de passe EAP.

```
config:#   network wireless eapPassword
```

Variables :

- <password> représente votre mot de passe pour l'authentification EAP.

Exemple

La commande suivante définit le mot de passe EAP sur user01_password.

```
config:#   network wireless eapPassword user01_password
```

Production du certificat d'autorité de certification pour EAP

Il vous faudra peut-être fournir un certificat d'autorité de certification tierce pour l'authentification EAP.

Pour fournir un certificat d'autorité de certification :

1. Tapez la commande de certificat d'autorité de certification comme indiqué ci-après et appuyez sur Entrée.

   ```
   config:#   network wireless eapCACertificate
   ```

2. Le système vous invite à entrer le contenu du certificat d'autorité de certification. Effectuez les opérations suivantes pour entrer le contenu :

   a. Ouvrez le certificat d'autorité de certification à l'aide d'un éditeur de texte.

   b. Copiez le contenu figurant entre les lignes --- BEGIN CERTIFICATE --- et --- END CERTIFICATE --- dans un certificat.

   c. Collez le contenu du certificat dans le terminal.

   d. Appuyez sur Entrée.

   Conseil : pour supprimer un certificat d'autorité de certification existant, appuyez sur Entrée sans rien taper ni coller lorsque le système vous invite à entrer le contenu du certificat.

3. Si le certificat est valide, le système affiche à nouveau l'invite de commande `config:#`. Dans le cas contraire, il affiche un message indiquant que le certificat n'est pas valide.

Exemple

Cette section fournit un exemple de certificat d'autorité de certification uniquement. Le contenu du vôtre devrait être différent de celui affiché dans cet exemple.

Pour fournir un certificat d'autorité de certification :

1. Assurez-vous que vous êtes passé en mode configuration. Reportez-vous à ***Passage en mode configuration*** (à la page 227).
2. Tapez la commande suivante et appuyez sur Entrée.

   ```
   config:#   network wireless eapCACertificate
   ```

3. Le système vous invite à entrer le contenu du certificat d'autorité de certification.
4. Ouvrez un certificat d'autorité de certification à l'aide d'un éditeur de texte. Le contenu du certificat devrait être similaire à ce qui suit.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Sélectionnez et copiez le contenu figurant entre la ligne de début BEGIN CERTIFICATE et la ligne de fin END CERTIFICATE comme illustré ci-dessous.

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Collez le contenu dans le terminal.
7. Appuyez sur Entrée.
8. Assurez-vous que le système affiche l'invite de commande suivante, indiquant que le certificat d'autorité de certification fourni est valide.

   ```
   config:#
   ```

Définition de l'identificateur BSSID

Cette syntaxe de commande définit la chaîne BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables :

- <bssid> représente l'adresse MAC du point d'accès sans fil.

Exemple

La commande indique que l'identificateur BSSID est 00:14:6C:7E:43:81.

```
config:#   network wireless BSSID 00:14:6C:7E:43:81
```

Configuration des paramètres IPv4

Une commande de configuration IPv4 débute par *network ipv4*.

Les commandes sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules.

Définition du mode de configuration IPv4

Cette syntaxe de commande détermine le mode de configuration IP.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variables :

- <mode> est un des modes : *dhcp* ou *static*.

Mode	Description
dhcp	Le mode de configuration IPv4 est défini sur DHCP.
static	Le mode de configuration IPv4 est défini sur l'adresse IP statique.

Exemple

La commande suivante active le mode de configuration IP statique.

```
config:#   network ipv4 ipConfigurationMode static
```

Définition du nom de l'hôte privilégié

Après avoir sélectionné DHCP comme mode de configuration IPv4, vous pouvez définir le nom de l'hôte privilégié, qui est facultatif. La syntaxe de la commande est la suivante :

```
config:#   network ipv4 preferredHostName <name>
```

Variables :

- <name> est le nom de l'hôte qui :
  - se compose de caractères alphanumériques et/ou de tirets ;
  - ne peut pas débuter ni finir par un tiret ;
  - ne peut pas contenir plus de 63 caractères ;
  - ne peut pas contenir de signes de ponctuation, d'espaces et autres symboles.

Exemple

La commande suivante définit my-host comme nom de l'hôte privilégié.

```
config:#   network ipv4 preferredHostName my-host
```

Définition de l'adresse IPv4

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour affecter une adresse IP permanente au dispositif EMX.

```
config:#   network ipv4 ipAddress <ip address>
```

Variables :

- <ip address> est l'adresse IP affectée au dispositif EMX. Les plages de valeurs sont comprises entre 0.0.0.0 et 255.255.255.255.

Exemple

La commande suivante affecte l'adresse IPv4 statique 192.168.84.222 au dispositif EMX.

```
config:#   network ipv4 ipAddress 192.168.84.222
```

Définition du masque de sous-réseau IPv4

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir le masque de sous-réseau.

```
config:#   network ipv4 subnetMask <netmask>
```

Variables :

- <netmask> est l'adresse du masque de sous-réseau. Les plages de valeurs sont comprises entre 0.0.0.0 et 255.255.255.255.

Exemple

La commande suivante définit le masque de sous-réseau sur 192.168.84.0.

```
config:#   network ipv4 subnetMask 192.168.84.0
```

Définition de la passerelle IPv4

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir la passerelle.

```
config:#   network ipv4 gateway <ip address>
```

Variables :

- <ip address> est l'adresse IP de la passerelle. Les plages de valeurs sont comprises entre 0.0.0.0 et 255.255.255.255.

Exemple

La commande suivante définit la passerelle IPv4 sur 255.255.255.0.

```
config:#   network ipv4 gateway 255.255.255.0
```

Définition du serveur DNS principal IPv4

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir le serveur DNS principal.

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variables :

- <ip address> est l'adresse IP du serveur DNS principal. Les plages de valeurs sont comprises entre 0.0.0.0 et 255.255.255.255.

Exemple

La commande suivante détermine que le serveur DNS principal est 192.168.84.30.

```
config:#   network ipv4 primaryDNSServer 192.168.84.30
```

Définition du serveur DNS secondaire IPv4

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir le serveur DNS secondaire.

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variables :

- <ip address> est l'adresse IP du serveur DNS secondaire. Les plages de valeurs sont comprises entre 0.0.0.0 et 255.255.255.255.

Remarque : EMX prend en charge trois serveurs DNS au maximum. Si deux serveurs DNS IPv4 et deux serveurs DNS IPv6 sont disponibles, EMX n'utilise que les serveurs DNS IPv4 et IPv6 principaux.

Exemple

La commande suivante détermine que le serveur DNS secondaire est 192.168.84.33.

```
config:#   network ipv4 secondaryDNSServer 192.168.84.33
```

Remplacement du serveur DNS IPv4 affecté par DHCP

Après avoir indiqué le serveur DNS principal/secondaire, vous pouvez utiliser cette commande pour remplacer le serveur DNS affecté par DHCP par celui que vous avez défini.

```
config:#   network ipv4 overrideDNS <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Cette option remplace le serveur DNS affecté par DHCP par le serveur DNS principal/secondaire que vous affectez.
disable	Cette option permet de reprendre l'utilisation du serveur DNS affecté par DHCP.

Exemple

La commande ci-après remplace le serveur DNS affecté par DHCP par celui que vous avez indiqué.

```
config:#   network ipv4 overrideDNS enable
```

Configuration des paramètres IPv6

Une commande de configuration IPv6 débute par *network ipv6*.

Les commandes sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules.

Définition du mode de configuration IPv6

Cette syntaxe de commande détermine le mode de configuration IP.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variables :

- <mode> est un des modes : *automatic* ou *static*.

Mode	Description
automatic	Le mode de configuration IPv6 est défini sur automatic.
static	Le mode de configuration IPv6 est défini sur l'adresse IP statique.

Exemple

La commande suivante définit le mode de configuration IP sur le mode d'adresse IP statique.

```
config:#   network ipv6 ipConfigurationMode static
```

Définition de l'adresse IPv6

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour affecter une adresse IP permanente au dispositif EMX.

```
config:#   network ipv6 ipAddress <ip address>
```

Variables :

- <ip address> est l'adresse IP affectée au dispositif EMX. Cette valeur utilise le format d'adresse IPv6.

Exemple

La commande suivante affecte l'adresse IPv6 statique `3210:4179:0:8:0:800:200C:417A` au dispositif EMX.

```
config:#   network ipv6 ipAddress 3210:4179:0:8:0:800:200C:417A
```

Définition de la passerelle IPv6

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir la passerelle.

```
config:#   network ipv6 gateway <ip address>
```

Variables :

- <ip address> est l'adresse IP de la passerelle. Cette valeur utilise le format d'adresse IPv6.

Exemple

La commande suivante définit la passerelle sur 500:0:330:0:4:9:3:2.

```
config:#   network ipv6 gateway 500:0:330:0:4:9:3:2
```

Définition du serveur DNS principal IPv6

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir le serveur DNS principal. Elle est obligatoire pour activer le remplacement du serveur DNS affecté automatiquement avant la définition manuelle des serveurs DNS. Reportez-vous à ***Remplacement du serveur DNS IPv6 affecté par DHCP*** (à la page 247).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variables :

- <ip address> est l'adresse IP du serveur DNS principal. Cette valeur utilise le format d'adresse IPv6.

Exemple

La commande suivante détermine que le serveur DNS principal est 2103:288:8201:1::14.

```
config:#   network ipv6 primaryDNSServer 2103:288:8201:1::14
```

Définition du serveur DNS secondaire IPv6

Après avoir sélectionné le mode de configuration IP statique, vous pouvez utiliser la syntaxe de cette commande pour définir le serveur DNS secondaire. Elle est obligatoire pour activer le remplacement du serveur DNS affecté automatiquement avant la définition manuelle des serveurs DNS. Reportez-vous à ***Remplacement du serveur DNS IPv6 affecté par DHCP*** (à la page 247).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variables :

- <ip address> est l'adresse IP du serveur DNS secondaire. Cette valeur utilise le format d'adresse IPv6.

Remarque : EMX prend en charge trois serveurs DNS au maximum. Si deux serveurs DNS IPv4 et deux serveurs DNS IPv6 sont disponibles, EMX n'utilise que les serveurs DNS IPv4 et IPv6 principaux.

Exemple

La commande suivante détermine que le serveur DNS secondaire est 2103:288:8201:1::700.

```
config:#   network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

Remplacement du serveur DNS IPv6 affecté par DHCP

Après avoir indiqué le serveur DNS principal/secondaire, vous pouvez utiliser cette commande pour remplacer le serveur DNS affecté par DHCP par celui que vous avez défini.

```
config:#   network ipv6 overrideDNS <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Cette option remplace le serveur DNS affecté par DHCP par le serveur DNS principal/secondaire que vous affectez.
disable	Cette option permet de reprendre l'utilisation du serveur DNS affecté par DHCP.

Exemple

La commande ci-après remplace le serveur DNS affecté par DHCP par celui que vous avez indiqué.

```
config:#   network ipv6 overrideDNS enable
```

Définition des paramètres de l'interface LAN

Une commande de configuration de l'interface LAN débute par *network interface*.

Les commandes sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules.

Modification de la vitesse de l'interface LAN

Cette syntaxe de commande détermine la vitesse de l'interface LAN.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variables :

- <option> est une des options : *auto*, *10Mbps* et *100Mbps*.

Option	Description
auto	Le système détermine la vitesse optimale du réseau local par négociation automatique.
10Mbps	La vitesse du réseau local est toujours de 10 Mbps.
100Mbps	La vitesse du réseau local est toujours de 100 Mbps.

Exemple

La commande ci-après laisse EMX déterminer la vitesse d'interface LAN optimale par le biais de la négociation automatique.

```
config:#   network interface LANInterfaceSpeed auto
```

Modification du mode bidirectionnel LAN

Cette syntaxe de commande détermine le mode bidirectionnel de l'interface LAN.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variables :

- <mode> est un des modes : *auto*, *half* ou *full*.

Option	Description
auto	EMX sélectionne le mode de transmission optimal par négociation automatique.
half	Semi-bidirectionnel : Les données sont transmises dans une direction (vers ou depuis le dispositif EMX) à la fois.

Option	Description
full	Bidirectionnel simultané : Les données sont transmises dans les deux sens simultanément.

Exemple

La commande ci-après laisse EMX déterminer le mode de transmission optimal par le biais de la négociation automatique.

```
config:#   network interface LANInterfaceDuplexMode auto
```

Définition des paramètres des services du réseau

Une commande de service de réseau débute par *network services*.

Modification du port HTTP

Cette syntaxe de commande modifie le port HTTP.

```
config:#   network services http <n>
```

Variables :

- <n> est un numéro de port TCP compris entre 1 et 65535. Le port HTTP par défaut est 80.

Exemple

La commande suivante définit le port HTTP sur 81.

```
config:#   network services http 81
```

Modification du port HTTPS

Cette syntaxe de commande modifie le port HTTPS.

```
config:#   network services https <n>
```

Variables :

- <n> est un numéro de port TCP compris entre 1 et 65535. Le port HTTPS par défaut est 443.

Exemple

La commande suivante définit le port HTTPS sur 333.

```
config:#   network services https 333
```

Modification de la configuration Telnet

Vous pouvez activer ou désactiver le service Telnet, ou modifier son port TCP à l'aide des commandes CLI.

Une commande Telnet débute par *network services telnet*.

Activation ou désactivation de Telnet

Cette syntaxe de commande active ou désactive le service Telnet.

```
config:#   network services telnet enabled <option>
```

Variables :

- <option> est une des options : *true* ou *false*.

Option	Description
true	Le service Telnet est activé.
false	Le service Telnet est désactivé.

Exemple

La commande suivante active le service Telnet.

```
config:#   network services telnet enabled true
```

Modification du port Telnet

Cette syntaxe de commande modifie le port Telnet.

```
config:#   network services telnet port <n>
```

Variables :

- <n> est un numéro de port TCP compris entre 1 et 65535. Le port Telnet par défaut est 23.

Exemple

La syntaxe de commande ci-après définit le port TCP pour Telnet sur 44.

```
config:#   network services telnet port 44
```

Modification de la configuration SSH

Vous pouvez activer ou désactiver le service SSH, ou modifier son port TCP à l'aide des commandes CLI.

Une commande SSH débute par *network services ssh*.

Activation ou désactivation de SSH

Cette syntaxe de commande active ou désactive le service SSH.

```
config:#   network services ssh enabled <option>
```

Variables :

- <option> est une des options : *true* ou *false*.

Option	Description
true	Le service SSH est activé.
false	Le service SSH est désactivé.

Exemple

La commande suivante active le service SSH.

```
config:#   network services ssh enabled true
```

Modification du port SSH

Cette syntaxe de commande modifie le port SSH.

```
config:#   network services ssh port <n>
```

Variables :

- <n> est un numéro de port TCP compris entre 1 et 65535. Le port SSH par défaut est 22.

Exemple

La syntaxe de commande suivante définit le port TCP pour SSH sur 555.

```
config:#   network services ssh port 555
```

Définition de la méthode d'authentification SSH

Cette syntaxe de commande détermine la méthode d'authentification SSH.

```
config:#   network services ssh authentication <auth_method>
```

Variables :

- <option> est une des options : *passwordOnly*, *publicKeyOnly* ou *passwordOrPublicKey*.

Option	Description
passwordOnly	Active la connexion par mot de passe uniquement.
publicKeyOnly	Active la connexion par clé publique uniquement.
passwordOrPublicKey	Active la connexion par mot de passe et par clé publique. Il s'agit de la valeur par défaut.

Si l'authentification par clé publique est sélectionnée, vous devez entrer une clé publique SSH valide pour établir une connexion SSH pour chaque profil utilisateur. Reportez-vous à ***Définition de la clé publique SSH*** (à la page 300).

Exemple

La commande ci-après oblige les utilisateurs à entrer un mot de passe pour la connexion SSH. L'utilisation d'une clé publique SSH n'est pas autorisée.

```
config:#   network services ssh authentication passwordOnly
```

Définition de la configuration SNMP

Vous pouvez activer ou désactiver l'agent SNMP v1/v2c ou v3, configurer les chaînes de communauté en lecture et écriture, ou définir les paramètres MIB-II, tels que sysContact, à l'aide des commandes CLI.

Une commande SNMP débute par *network services snmp*.

Activation ou désactivation de SNMP v1/v2c

Cette syntaxe de commande active ou désactive le protocole SNMP v1/v2c.

```
config:#   network services snmp v1/v2c <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Le protocole SNMP v1/v2c est activé.
disable	Le protocole SNMP v1/v2c est désactivé.

Exemple

La commande suivante active le protocole SNMP v1/v2c.

```
config:#   network services snmp v1/v2c enable
```

Activation ou désactivation de SNMP v3

Cette syntaxe de commande active ou désactive le protocole SNMP v3.

```
config:#   network services snmp v3 <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Le protocole SNMP v3 est activé.
disable	Le protocole SNMP v3 est désactivé.

Exemple

La commande suivante active le protocole SNMP v3.

```
config:#   network services snmp v3 enable
```

Définition de la communauté en lecture SNMP

Cette syntaxe de commande définit la chaîne de communauté en lecture seule SNMP.

```
config:#   network services snmp readCommunity <string>
```

Variables :

- <string> est une chaîne comprenant 4 à 64 caractères imprimables ASCII.
- La chaîne NE PEUT PAS comporter d'espace.

Exemple

Cette syntaxe de commande définit la chaîne de communauté en lecture seule SNMP sur public.

```
config:#   network services snmp readCommunity public
```

Définition de la communauté en écriture SNMP

Cette syntaxe de commande définit la chaîne de communauté en lecture/écriture SNMP.

```
config:#   network services snmp writeCommunity <string>
```

Variables :

- <string> est une chaîne comprenant 4 à 64 caractères imprimables ASCII.
- La chaîne NE PEUT PAS comporter d'espace.

Exemple

La commande suivante définit la chaîne de communauté en lecture/écriture SNMP sur private.

```
config:#   network services snmp writeCommunity private
```

Définition de la valeur sysContact

Cette syntaxe de commande définit la valeur MIB-II sysContact SNMP.

```
config:#   network services snmp sysContact <value>
```

Variables :

- <string> est une chaîne comprenant 0 à 255 caractères alphanumériques.

Exemple

La commande suivante définit la valeur MIB-II sysContact SNMP sur John_Krause.

```
config:#   network services snmp sysContact John_Krause
```

Définition de la valeur sysName

Cette syntaxe de commande définit la valeur MIB-II sysName SNMP.

```
config:#   network services snmp sysName <value>
```

Variables :

- <string> est une chaîne comprenant 0 à 255 caractères alphanumériques.

Exemple

La commande suivante définit la valeur MIB-II sysName SNMP sur Win7_system.

```
config:#   network services snmp sysName Win7_system
```

Définition de la valeur sysLocation

Cette syntaxe de commande définit la valeur MIB-II sysLocation SNMP.

```
config:#   network services snmp sysLocation <value>
```

Variables :

- <string> est une chaîne comprenant 0 à 255 caractères alphanumériques.

Exemple

La commande suivante définit la valeur MIB-II sysLocation SNMP sur New_TAIPEI.

```
config:#   network services snmp sysLocation New_TAIPEI
```

Commandes de configuration de la sécurité

Une commande de configuration de la sécurité débute par *security*.

Contrôle du pare-feu

Vous pouvez gérer les fonctions de contrôle du pare-feu via l'interface CLI. Le contrôle du pare-feu vous permet de paramétrer les règles autorisant ou interdisant l'accès au dispositif EMX à partir d'une adresse IP spécifique ou d'une plage d'adresses IP.

- Une commande de configuration de pare-feu IPv4 débute par *security ipAccessControl ipv4*.
- Une commande de configuration de pare-feu IPv6 débute par *security ipAccessControl ipv6*.

Modification des paramètres de contrôle du pare-feu

Il existe différentes commandes pour modifier les paramètres de contrôle du pare-feu.

- **Commandes IPv4**

Pour activer ou désactiver la fonction de contrôle du pare-feu IPv4, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv4 enabled <option>
```

Pour déterminer la stratégie de contrôle de pare-feu IPv4 par défaut, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv4 defaultPolicy <policy>
```

- **Commandes IPv6**

Pour activer ou désactiver la fonction de contrôle du pare-feu IPv6, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv6 enabled <option>
```

Pour déterminer la stratégie de contrôle de pare-feu IPv6 par défaut, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv6 defaultPolicy <policy>
```

Variables :

- <option> est une des options : *true* ou *false*.

Option	Description
true	Active la fonction de contrôle d'accès IP.
false	Désactive la fonction de contrôle d'accès IP.

- <policy> est une de ces options : *accept*, *drop* ou *reject*.

Option	Description
accept	Accepte le trafic de toutes les adresses IP.
drop	Refuse le trafic de toutes les adresses IP, sans envoyer de notification d'échec à l'hôte source.

Option	Description
reject	Refuse le trafic de toutes les adresses IP et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec.

Conseil : vous pouvez combiner les deux commandes pour modifier tous les paramètres de contrôle de pare-feu en même temps. Reportez-vous à **Syntaxe multi-commandes** *(à la page 316).*

Exemple

La commande suivante définit jusqu'à deux paramètres de la fonction de contrôle d'accès IPv4.

```
config:#   security ipAccessControl ipv4 enabled true defaultPolicy accept
```

Résultats :

- La fonction de contrôle d'accès IPv4 est activée.
- La stratégie par défaut est définie sur accept.

Gestion des règles de pare-feu

Vous pouvez ajouter, supprimer ou modifier les règles de pare-feu à l'aide des commandes CLI.

- Une commande de règle de contrôle du pare-feu IPv4 débute par *security ipAccessControl ipv4 rule*.
- Une commande de règle de contrôle du pare-feu IPv6 débute par *security ipAccessControl ipv6 rule*.

Ajout d'une règle de pare-feu

Selon l'endroit où vous souhaitez ajouter la nouvelle règle de pare-feu dans la liste, la syntaxe de commande pour l'ajout d'une règle varie.

- **Commandes IPv4**

Pour ajouter une nouvelle règle au bas de la liste des règles IPv4, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy>
```

Pour ajouter une nouvelle règle IPv4 en l'insérant au-dessus ou au-dessous d'une règle spécifique, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy> <insert>
            <rule_number>
```

-- OU --

```
config:#    security ipAccessControl ipv4 rule add <insert> <rule_number> <ip_mask>
            <policy>
```

- **Commandes IPv6**

Pour ajouter une nouvelle règle au bas de la liste des règles IPv6, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy>
```

Pour ajouter une nouvelle règle IPv6 en l'insérant au-dessus ou au-dessous d'une règle spécifique, utilisez cette syntaxe de commande :

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy> <insert> <rule_number>
```

-- OU --

```
config:#    security ipAccessControl ipv6 rule add <insert> <rule_number> <ip_mask> <policy>
```

Variables :

- <ip_mask> combine les valeurs d'adresse IP et de masque de sous-réseau, séparées par un barre oblique. Par exemple, une combinaison IPv4 se présente comme suit : *192.168.94.222/24*.
- <policy> est une de ces options : *accept*, *drop* ou *reject*.

Stratégie	Description
accept	Accepte le trafic des adresses IP indiquées.
drop	Refuse le trafic des adresses IP indiquées, sans envoyer de notification d'échec à l'hôte source.

Stratégie	Description
reject	Refuse le trafic des adresses IP indiquées et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec.

- <insert> est une des options : *insertAbove* ou *insertBelow*.

Option	Description
insertAbove	Insère la nouvelle règle au-dessus du numéro de règle indiqué. Ensuite : numéro de la nouvelle règle = numéro de règle indiqué
insertBelow	Insère la nouvelle règle au-dessous du numéro de règle indiqué. Ensuite : numéro de la nouvelle règle = numéro de règle indiqué + 1

- <rule_number> est le numéro de la règle existante au-dessus ou au-dessous de laquelle vous souhaitez insérer la nouvelle règle.

Exemple

La commande suivante ajoute une règle de contrôle d'accès IPv4 et indique son emplacement dans la liste.

```
config:#   security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
           insertAbove 5
```

Résultats :

- Une nouvelle règle de contrôle de pare-feu IPv4 est ajoutée, permettant à tous les paquets de l'adresse IPv4 192.168.84.123 d'être acceptés.
- La nouvelle règle est insérée au-dessus de la 5e. C'est-à-dire que la nouvelle règle devient la 5e, et la 5e d'origine devient la 6e.

Modification d'une règle de pare-feu

Selon l'élément à modifier dans une règle existante, la syntaxe de commande varie.

- **Commandes IPv4**

▶ **Syntaxe de commande permettant de modifier l'adresse IP et/ou le masque de sous-réseau d'une règle IPv4 :**

```
config:#  security ipAccessControl ipv4 rule modify <rule_number> ipMask <ip_mask>
```

Syntaxe de commande permettant de modifier la stratégie d'une règle IPv4 :

```
config:#  security ipAccessControl ipv4 rule modify <rule_number> policy <policy>
```

Syntaxe de commande permettant de modifier le contenu d'une règle IPv4 existante :

```
config:#  security ipAccessControl ipv4 rule modify <rule_number> ipMask <ip_mask>
          policy <policy>
```

- **Commandes IPv6**

Syntaxe de commande permettant de modifier l'adresse IP et/ou le masque de sous-réseau d'une règle IPv6 :

```
config:#  security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
```

Syntaxe de commande permettant de modifier la stratégie d'une règle IPv6 :

```
config:#  security ipAccessControl ipv6 rule modify <rule_number> policy <policy>
```

Syntaxe de commande permettant de modifier le contenu d'une règle IPv6 existante :

```
config:#    security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
            policy <policy>
```

Variables :

- <rule_number> est le numéro de la règle existante que vous souhaitez modifier.
- <ip_mask> combine les valeurs d'adresse IP et de masque de sous-réseau, séparées par un barre oblique. Par exemple, une combinaison IPv4 se présente comme suit : *192.168.94.222/24*.
- <policy> est une de ces options : *accept*, *drop* ou *reject*.

Option	Description
accept	Accepte le trafic des adresses IP indiquées.
drop	Refuse le trafic des adresses IP indiquées, sans envoyer de notification d'échec à l'hôte source.
reject	Refuse le trafic des adresses IP indiquées et un message ICMP est envoyé à l'hôte source pour le notifier de l'échec.

Exemple

La commande suivante modifie tout le contenu de la 5e règle IPv4.

```
config:#    security ipAccessControl ipv4 rule modify 5 ipMask 192.168.84.123/24
            policy accept
```

Résultats :

- L'adresse IPv4 est remplacée par 192.168.84.123 et le masque de sous-réseau par 255.255.255.0.
- La stratégie devient maintenant accept.

Suppression d'une règle de pare-feu

Les commandes ci-après retirent une règle IPv4 ou IPv6 particulière de la liste.

- **Commandes IPv4**

```
config:#    security ipAccessControl ipv4 rule delete <rule_number>
```

- **Commandes IPv6**

```
config:#    security ipAccessControl ipv6 rule delete <rule_number>
```

Variables :

- <rule_number> est le numéro de la règle existante que vous souhaitez supprimer.

Exemple

La commande suivante retire la 5e règle de la liste de contrôle d'accès IPv6.

```
config:#    security ipAccessControl ipv6 rule delete 5
```

Accès HTTPS

Cette commande détermine si l'accès HTTPS à l'interface Web de EMX est imposé. Si tel est le cas, toutes les tentatives d'accès HTTP sont automatiquement dirigées vers HTTPS.

```
config:#    security enforceHttpsForWebAccess <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Active l'accès HTTPS à l'interface Web.
disable	Désactive l'accès HTTPS à l'interface Web.

Exemple

La commande suivante désactive la fonction d'accès HTTPS.

```
config:#    security enforceHttpsForWebAccess disable
```

Limite de connexion

La fonction de limite de connexion contrôle les restrictions relatives à la connexion, telles que le vieillissement des mots de passe, les connexions simultanées à l'aide du même nom d'utilisateur et le délai d'inactivité permis avant la déconnexion forcée.

Une commande de limite de connexion débute par *security loginLimits*.

Vous pouvez combiner plusieurs commandes pour modifier tous les paramètres de limite de connexion en même temps. Reportez-vous à ***Syntaxe multi-commandes*** (à la page 316).

Limite de connexion unique

Cette syntaxe de commande active ou désactive la fonction de connexion unique, qui contrôle si plusieurs connexions simultanées à l'aide du même nom de connexion sont autorisées.

```
config:#   security loginLimits singleLogin <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Active la fonction de connexion unique.
disable	Désactive la fonction de connexion unique.

Exemple

La commande suivante désactive la fonction de connexion unique : plusieurs utilisateurs peuvent se connecter simultanément à l'aide d'un même nom d'utilisateur.

```
config:#   security loginLimits singleLogin disable
```

Vieillissement des mots de passe

Cette syntaxe de commande active ou désactive la fonction de vieillissement des mots de passe, qui contrôle si le mot de passe doit être modifié à intervalles réguliers :

```
config:#   security loginLimits passwordAging <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Active la fonction de vieillissement du mot de passe.
disable	Désactive la fonction de vieillissement des mots de passe.

Exemple

La commande suivante active la fonction de vieillissement des mots de passe.

```
config:#   security loginLimits passwordAging enable
```

Intervalle de vieillissement des mots de passe

Cette syntaxe de commande détermine la fréquence de modification du mot de passe.

```
config:#   security loginLimits passwordAgingInterval <value>
```

Variables :

- <value> est une valeur numérique exprimée en jours pour l'intervalle de vieillissement des mots de passe. L'intervalle varie de 7 à 365 jours.

Exemple

La commande suivante définit l'intervalle de vieillissement des mots de passe à 90 jours.

```
config:#   security loginLimits passwordAgingInterval 90
```

Délai d'inactivité

Cette syntaxe de commande détermine la durée pendant laquelle un utilisateur peut rester inactif avant d'être forcé de se déconnecter de l'interface Web de EMX.

```
config:#   security loginLimits idleTimeout <value>
```

Variables :

- <value> est une valeur numérique en minutes définie pour le délai d'inactivité. Le délai varie de 1 à 1440 minutes (24 heures).

Exemple

La commande suivante définit le délai d'inactivité à 10 minutes.

```
config:#   security loginLimits idleTimeout 10
```

Blocage des utilisateurs

Il existe diverses commandes pour modifier différents paramètres de blocage des utilisateurs. Ces commandes débutent par `security userBlocking`.

Pour déterminer le nombre maximum d'échecs de connexion avant le blocage d'un utilisateur, employez cette syntaxe de commande :

```
config:#    security userBlocking maximumNumberOfFailedLogins <value1>
```

- **Pour déterminer la durée pendant laquelle la connexion d'un utilisateur est bloquée, employez cette syntaxe de commande :**

  ```
  config:#    security userBlocking blockTime <value2>
  ```

Variables :

- <value1> est un nombre entier compris entre 3 et 10, ou *unlimited*, qui ne définit aucune limite sur le nombre maximum d'échecs de connexion et désactive donc la fonction de blocage des utilisateurs.
- <value2> est une valeur numérique exprimée en minutes.

Conseil : vous pouvez combiner plusieurs commandes pour modifier tous les paramètres de blocage des utilisateurs en même temps. Reportez-vous à **Syntaxe multi-commandes** *(à la page 316).*

Exemple

La commande suivante définit deux paramètres de blocage des utilisateurs.

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Résultats :

- Le nombre maximum d'échecs de connexion est défini sur 5.
- La durée de blocage des utilisateurs est définie sur 30 minutes.

Mots de passe forts

Les commandes de mot de passe fort déterminent si un mot de passe fort est obligatoire pour la connexion et les caractères qu'il doit au moins contenir.

Une commande de mot de passe fort débute par `security strongPasswords`.

Vous pouvez combiner plusieurs commandes de mot de passe fort pour modifier différents paramètres en même temps. Reportez-vous à ***Syntaxe multi-commandes*** (à la page 316).

Activation ou désactivation des mots de passe forts

Cette syntaxe de commande active ou désactive la fonction de mot de passe fort.

```
config:#   security strongPasswords enabled <option>
```

Variables :

- <option> est une des options : *true* ou *false*.

Option	Description
true	Active la fonction de mot de passe fort.
false	Désactive la fonction de mot de passe fort.

Exemple

Cette syntaxe de commande active la fonction de mot de passe fort.

```
config:#   security strongPasswords enabled true
```

Longueur minimum de mot de passe

Cette syntaxe de commande détermine la longueur minimum du mot de passe.

```
config:#   security strongPasswords minimumLength <value>
```

Variables :

- <value> est un nombre entier compris entre 8 et 32.

Exemple

Cette syntaxe de commande détermine qu'un mot de passe doit comprendre au moins 8 caractères.

```
config:#   security strongPasswords minimumLength 8
```

Longueur maximum de mot de passe

Cette syntaxe de commande détermine la longueur maximum du mot de passe.

```
config:#    security strongPasswords maximumLength <value>
```

Variables :

- <value> est un nombre entier compris entre 16 et 64.

Exemple

Cette syntaxe de commande détermine qu'un mot de passe NE DOIT PAS comprendre plus de 20 caractères.

```
config:#    security strongPasswords maximumLength 20
```

Caractère en minuscule requis

Cette syntaxe de commande détermine si un mot de passe fort inclut au moins un caractère en minuscule.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Au moins un caractère en minuscule est requis.
disable	Aucun caractère en minuscule n'est requis.

Exemple

Cette syntaxe de commande détermine qu'un mot de passe doit inclure au moins un caractère en minuscule.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

Caractère en majuscule requis

Cette syntaxe de commande détermine si un mot de passe fort inclut au moins un caractère en majuscule.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Au moins un caractère en majuscule est requis.
disable	Aucun caractère en majuscule n'est requis.

Exemple

Cette commande détermine qu'un mot de passe doit comprendre au moins un caractère en majuscule.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

Caractère numérique requis

Cette syntaxe de commande détermine si un mot de passe fort inclut au moins un caractère numérique.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Au moins un caractère numérique est requis.
disable	Aucun caractère numérique n'est requis.

Exemple

La commande suivante détermine qu'un mot de passe doit comprendre au moins un caractère numérique.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter enable
```

Caractère spécial requis

Cette syntaxe de commande détermine si un mot de passe fort inclut au moins un caractère spécial.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables :

- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Au moins un caractère spécial est requis.
disable	Aucun caractère spécial n'est requis.

Exemple

La commande suivante détermine qu'un mot de passe doit comprendre au moins un caractère spécial.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

Historique des mots de passe maximum

Cette syntaxe de commande détermine le nombre de mots de passe précédents NE POUVANT PAS être répétés lors de la modification.

```
config:#    security strongPasswords passwordHistoryDepth <value>
```

Variables :

- <value> est un nombre entier compris entre 1 et 12.

Exemple

La commande suivante détermine que les sept mots de passe précédents NE PEUVENT PAS être réutilisés lors de la modification du mot de passe.

```
config:#    security strongPasswords passwordHistoryDepth 7
```

Contrôle d'accès basé rôle

Outre le contrôle d'accès par pare-feu basé sur les adresses IP, vous pouvez configurer d'autres règles de contrôle d'accès basées sur les adresses IP et les rôles des utilisateurs.

- Une commande de contrôle d'accès basé rôle IPv4 débute par *security roleBasedAccessControl ipv4*.
- Une commande de contrôle d'accès basé rôle IPv6 débute par *security roleBasedAccessControl ipv6*.

Modification des paramètres de contrôle d'accès basé rôle

Il existe différentes commandes pour modifier les paramètres de contrôle d'accès basé rôle.

- **Commandes IPv4**

▶ **Pour activer ou désactiver la fonction de contrôle d'accès basé rôle IPv4, utilisez cette syntaxe de commande :**

```
config:#    security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Pour déterminer la stratégie de contrôle d'accès basé rôle IPv4, utilisez cette syntaxe de commande :**

```
config:#    security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- **Commandes IPv6**

▶ **Pour activer ou désactiver la fonction de contrôle d'accès basé rôle IPv6, utilisez cette syntaxe de commande :**

```
config:#    security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Pour déterminer la stratégie de contrôle d'accès basé rôle IPv6, utilisez cette syntaxe de commande :**

```
config:#    security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables :

- <option> est une des options : *true* ou *false*.

Option	Description
true	Active la fonction de contrôle d'accès basé rôle.
false	Désactive la fonction de contrôle d'accès basé rôle.

- <policy> est une de ces options : *allow* ou *deny*.

Stratégie	Description
allow	Accepte le trafic de toutes les adresses IP indépendamment du rôle de l'utilisateur.
deny	Refuse le trafic de toutes les adresses IP indépendamment du rôle de l'utilisateur.

Conseil : vous pouvez combiner les deux commandes pour modifier tous les paramètres de contrôle d'accès basé rôle en même temps. Reportez-vous à **Syntaxe multi-commandes** *(à la page 316).*

Exemple

La commande suivante définit les deux paramètres de la fonction de contrôle d'accès basé rôle IPv4.

```
config:#    security roleBasedAccessControl ipv4 enabled true defaultPolicy allow
```

Résultats :

- La fonction de contrôle d'accès basé rôle IPv4 est activée.
- La stratégie par défaut est définie sur allow.

Gestion des règles de contrôle d'accès basé rôle

Vous pouvez ajouter, supprimer ou modifier des règles de contrôle d'accès basé rôle.

- Une commande de contrôle d'accès basé rôle IPv4 de gestion des règles débute par *security roleBasedAccessControl ipv4 rule*.
- Une commande de contrôle d'accès basé rôle IPv6 de gestion des règles débute par *security roleBasedAccessControl ipv6 rule*.

Ajout d'une règle de contrôle d'accès basé rôle

Selon l'endroit où vous souhaitez ajouter la nouvelle règle dans la liste, la syntaxe de commande pour l'ajout d'une règle varie.

- **Commandes IPv4**

▶ **Pour ajouter une nouvelle règle au bas de la liste des règles IPv4, utilisez cette syntaxe de commande :**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **Pour ajouter une nouvelle règle IPv4 en l'insérant au-dessus ou au-dessous d'une règle spécifique, utilisez cette syntaxe de commande :**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
          <insert> <rule_number>
```

- **Commandes IPv6**

▶ **Pour ajouter une nouvelle règle au bas de la liste des règles IPv6, utilisez cette syntaxe de commande :**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **Pour ajouter une nouvelle règle IPv6 en l'insérant au-dessus ou au-dessous d'une règle spécifique, utilisez cette syntaxe de commande :**

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
           <insert> <rule_number>
```

Variables :

- <start_ip> est l'adresse IP de début.
- <end_ip> est l'adresse IP de fin.
- <role> est le rôle pour lequel vous souhaitez créer une règle de contrôle d'accès.
- <policy> est une de ces options : *allow* ou *deny*.

Stratégie	Description
allow	Accepte le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié.
deny	Refuse le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié.

- <insert> est une des options : *insertAbove* ou *insertBelow*.

Option	Description
insertAbove	Insère la nouvelle règle au-dessus du numéro de règle indiqué. Ensuite : numéro de la nouvelle règle = numéro de règle indiqué
insertBelow	Insère la nouvelle règle au-dessous du numéro de règle indiqué. Ensuite : numéro de la nouvelle règle = numéro de règle indiqué + 1

- <rule_number> est le numéro de la règle existante au-dessus ou au-dessous de laquelle vous souhaitez insérer la nouvelle règle.

Exemple

La commande suivante crée une règle de contrôle d'accès basé rôle IPv4 et indique son emplacement dans la liste.

```
config:#  security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100 admin
          deny insertAbove 3
```

Résultats :

- Une nouvelle règle de contrôle d'accès basé rôle IPv4 est ajoutée, refusant tous les paquets des adresses IPv4 comprises entre 192.168.78.50 et 192.168.90.100 lorsque l'utilisateur est membre du rôle admin.
- La nouvelle règle IPv4 est insérée au-dessus de la 3e. C'est-à-dire que la nouvelle règle devient la 3e, et la 3e d'origine devient la 4e.

Modification d'une règle de contrôle d'accès basé rôle

Selon l'élément à modifier dans une règle existante, la syntaxe de commande varie.

- **Commandes IPv4**

Pour modifier la plage d'adresses IPv4 d'une règle, utilisez cette syntaxe de commande :

```
config:#  security roleBasedAccessControl ipv4 rule modify <rule_number>
          startIpAddress <start_ip> endIpAddress <end_ip>
```

Pour modifier le rôle d'une règle IPv4, utilisez cette syntaxe de commande :

```
config:#  security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

Pour modifier la stratégie d'une règle IPv4, utilisez cette syntaxe de commande :

```
config:#  security roleBasedAccessControl ipv4 rule modify <rule_number> policy
          <policy>
```

Pour modifier tout le contenu d'une règle IPv4 existante, utilisez cette syntaxe de commande :

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- **Commandes IPv6**

Pour modifier la plage d'adresses IPv6 d'une règle, utilisez cette syntaxe de commande :

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

Pour modifier le rôle d'une règle IPv6, utilisez cette syntaxe de commande :

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

Pour modifier la stratégie d'une règle IPv6, utilisez cette syntaxe de commande :

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

Pour modifier tout le contenu d'une règle IPv6 existante, utilisez cette syntaxe de commande :

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variables :

- <rule_number> est le numéro de la règle existante que vous souhaitez modifier.
- <start_ip> est l'adresse IP de début.
- <end_ip> est l'adresse IP de fin.
- <role> est l'un des rôles existants.
- <policy> est une de ces options : *allow* ou *deny*.

Stratégie	Description
allow	Accepte le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié.

Stratégie	Description
deny	Refuse le trafic de la plage d'adresses IP indiquée lorsque l'utilisateur est membre du rôle spécifié.

Exemple

La commande suivante modifie tout le contenu de la 8e règle IPv4.

```
config:#   security roleBasedAccessControl ipv4 rule modify 8
           startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
           policy allow
```

Résultats :

- L'adresse IPv4 de début est remplacée par 192.168.8.8 et l'adresse IPv4 de fin, par 192.168.90.90.
- Le rôle est remplacé par operator.
- La stratégie devient maintenant allow.

Suppression d'une règle de contrôle d'accès basé rôle

Cette commande supprime une règle spécifique de la liste.

- **Commandes IPv4**

```
config:#   security roleBasedAccessControl ipv4 rule delete <rule_number>
```

- **Commandes IPv6**

```
config:#   security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables :

- <rule_number> est le numéro de la règle existante que vous souhaitez supprimer.

Exemple

La commande suivante supprime la 7e règle IPv6.

```
config:#   security roleBasedAccessControl ipv6 rule delete 7
```

Commandes de configuration des capteurs d'environnement

Une commande de configuration de capteur d'environnement débute par *externalsensor*. Vous pouvez configurer les paramètres de nom et d'emplacement d'un capteur d'environnement individuel.

Modification du nom d'un capteur

Cette syntaxe de commande nomme un capteur d'environnement.

```
config:#   externalsensor <n> name "<name>"
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII. La variable <name> doit être entourée de guillemets lorsqu'elle contient des espaces.

Exemple

La commande suivante affecte le nom Cabinet humidity au capteur d'environnement portant l'ID numéro 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Définition du type de capteur

Le capteur de fermeture de contact (DPX-CC2-TR) de Raritan prend en charge la connexion de divers détecteurs/commutateurs tiers, et vous devez indiquer le type de détecteur/commutateur connecté pour assurer un fonctionnement correct. Utilisez cette syntaxe de commande lorsque vous devez indiquer le type de capteur.

```
config:#   externalsensor <n> sensorSubType <type>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <type> est un de ces types : *contact*, *smokeDetection*, *waterDetection* ou *vibration*.

Type	Description
contact	Le détecteur/commutateur connecté sert à la détection du statut porte verrouillée ou porte fermée/ouverte.
smokeDetection	Le détecteur/commutateur connecté sert à détecter la présence de fumée.
waterDetection	Le détecteur/commutateur connecté sert à détecter la présence d'eau.
vibration	Le détecteur/commutateur connecté sert à détecter les vibrations.

Exemple

La commande suivante indique qu'un détecteur de fumée est connecté au capteur de fermeture de contact (DPX-CC2-TR) de Raritan dont le numéro d'identification affiché dans l'interface Web de EMX est 2.

```
config:#   externalsensor 2 sensorSubType smokeDetection
```

Définition de la coordonnée X

Cette syntaxe de commande définit la coordonnée X d'un capteur d'environnement.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <coordinate> est une chaîne comprenant jusqu'à 24 caractères imprimables ASCII et entourée de guillemets.

Exemple

La commande suivante donne la valeur The 2nd cabinet à la coordonnée X du capteur d'environnement portant l'ID numéro 4.

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

Définition de la coordonnée Y

Cette syntaxe de commande définit la coordonnée Y d'un capteur d'environnement.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <coordinate> est une chaîne comprenant jusqu'à 24 caractères imprimables ASCII et entourée de guillemets.

Exemple

La commande suivante donne la valeur The 4th row à la coordonnée Y du capteur d'environnement portant l'ID numéro 4.

```
config:#   externalsensor 4 ylabel "The 4th row"
```

Définition de la coordonnée Z

Cette syntaxe de commande définit la coordonnée Z d'un capteur d'environnement.

config:# externalsensor <n> zlabel "<coordinate>"

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- Selon le format de la coordonnée Z que vous avez défini, il existe deux types de valeurs pour la variable <coordinate> :

Type	Description
Free-Form (Forme libre)	<coordinate> est une chaîne comprenant jusqu'à 24 caractères imprimables ASCII et entourée de guillemets.
Rack Units (Unités de rack)	<coordinate> est un nombre entier en unités de rack.

Remarque : pour définir la coordonnée Z à l'aide des unités de rack, reportez-vous à **Définition du format de la coordonnée Z pour les capteurs d'environnement** *(à la page 229).*

Exemple

La commande suivante donne la valeur The 5th rack à la coordonnée Z du capteur d'environnement portant le numéro d'identification 4 après que le format de cette coordonnée Z est défini sur *freeForm*.

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

Modification de la description d'un capteur

Cette syntaxe de commande fournit la description d'un capteur d'environnement spécifique.

```
config:#   externalsensor <n> description "<description>"
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <description> est une chaîne comprenant jusqu'à 64 caractères imprimables ASCII et entourée de guillemets.

Exemple

La commande suivante affecte la description humidity detection au capteur d'environnement portant le numéro d'identification 4.

```
config:#   externalsensor 4 description "humidity detection"
```

Commandes de configuration des seuils de capteur d'environnement

Une commande de configuration des seuils de capteurs d'environnement débute par *sensor externalsensor*.

Définition du seuil critique supérieur d'un capteur

Cette syntaxe de commande configure le seuil critique supérieur d'un capteur d'environnement numérique.

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <sensor type> est un de ces types de capteurs : *temperature*, *humidity*, *air Pressure* ou *air Flow* (température, humidité, pression d'air ou flux d'air).

Remarque : si le type de capteur indiqué est différent de celui du capteur d'environnement spécifié, le message d'erreur suivant apparaît : Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (Le type de capteur spécifié XXX ne correspond pas au type du capteur (<sensortype>), où XXX représente le type de capteur spécifié et <sensortype>, le type de capteur correct.

- <option> est une des options : *enable*, *disable* ou une valeur numérique.

Option	Description
enable	Active le seuil critique supérieur du capteur d'environnement indiqué.
disable	Désactive le seuil critique supérieur du capteur d'environnement indiqué.
Valeur numérique	Définit une valeur pour le seuil critique supérieur du capteur d'environnement indiqué et active ce seuil en même temps.

Exemple

La commande suivante définit le seuil critique supérieur du capteur de température d'environnement portant le numéro d'identification 2 sur 40 degrés Celsius. Elle active également ce seuil s'il ne l'est pas encore.

```
config:#   sensor externalsensor 2 temperature upperCritical 40
```

Définition du seuil d'avertissement supérieur d'un capteur

Cette syntaxe de commande configure le seuil d'avertissement supérieur d'un capteur d'environnement numérique.

```
config:#    sensor externalsensor <n> <sensor type> upperWarning <option>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <sensor type> est un de ces types de capteurs : *temperature*, *humidity*, *air Pressure* ou *air Flow* (température, humidité, pression d'air ou flux d'air).

Remarque : si le type de capteur indiqué est différent de celui du capteur d'environnement spécifié, le message d'erreur suivant apparaît : Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (Le type de capteur spécifié XXX ne correspond pas au type du capteur (<sensortype>), où XXX représente le type de capteur spécifié et <sensortype>, le type de capteur correct.

- <option> est une des options : *enable*, *disable* ou une valeur numérique.

Option	Description
enable	Active le seuil d'avertissement supérieur du capteur d'environnement indiqué.
disable	Désactive le seuil d'avertissement supérieur du capteur d'environnement indiqué.
Valeur numérique	Définit une valeur pour le seuil d'avertissement supérieur du capteur d'environnement indiqué et active ce seuil en même temps.

Exemple

La commande suivante active le seuil d'avertissement supérieur du capteur de température d'environnement portant le numéro d'identification 4.

```
config:#    sensor externalsensor 4 temperature upperWarning enable
```

Définition du seuil critique inférieur d'un capteur

Cette syntaxe de commande configure le seuil critique inférieur d'un capteur d'environnement numérique.

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <sensor type> est un de ces types de capteurs : *temperature*, *humidity*, *air Pressure* ou *air Flow* (température, humidité, pression d'air ou flux d'air).

Remarque : si le type de capteur indiqué est différent de celui du capteur d'environnement spécifié, le message d'erreur suivant apparaît : Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (Le type de capteur spécifié XXX ne correspond pas au type du capteur (<sensortype>), où XXX représente le type de capteur spécifié et <sensortype>, le type de capteur correct.

- <option> est une des options : *enable*, *disable* ou une valeur numérique.

Option	Description
enable	Active le seuil critique inférieur du capteur d'environnement indiqué.
disable	Désactive le seuil critique inférieur du capteur d'environnement indiqué.
Valeur numérique	Définit une valeur pour le seuil critique inférieur du capteur d'environnement indiqué et active ce seuil en même temps.

Exemple

La commande suivante définit le seuil critique inférieur du capteur d'humidité environnementale portant le numéro d'identification 1 sur 15 %. Elle active également ce seuil s'il ne l'est pas encore.

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

Définition du seuil d'avertissement inférieur d'un capteur

Cette syntaxe de commande configure le seuil d'avertissement inférieur d'un capteur d'environnement numérique.

```
config:#    sensor externalsensor <n> <sensor type> lowerWarning <option>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <sensor type> est un de ces types de capteurs : *temperature*, *humidity*, *air Pressure* ou *air Flow* (température, humidité, pression d'air ou flux d'air).

Remarque : si le type de capteur indiqué est différent de celui du capteur d'environnement spécifié, le message d'erreur suivant apparaît : Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (Le type de capteur spécifié XXX ne correspond pas au type du capteur (<sensortype>), où XXX représente le type de capteur spécifié et <sensortype>, le type de capteur correct.

- <option> est une des options : *enable*, *disable* ou une valeur numérique.

Option	Description
enable	Active le seuil d'avertissement inférieur du capteur d'environnement indiqué.
disable	Désactive le seuil d'avertissement inférieur du capteur d'environnement indiqué.
Valeur numérique	Définit une valeur pour le seuil d'avertissement inférieur du capteur d'environnement indiqué et active ce seuil en même temps.

Exemple

La commande suivante désactive le seuil d'avertissement inférieur du capteur d'humidité environnementale portant le numéro d'identification 3.

```
config:#    sensor externalsensor 3 humidity lowerWarning disable
```

Définition de l'hystérésis d'infirmation d'un capteur

Cette syntaxe de commande configure la valeur d'hystérésis d'infirmation d'un capteur d'environnement numérique.

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <value>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <sensor type> est un de ces types de capteurs : *temperature*, *humidity*, *air Pressure* ou *air Flow* (température, humidité, pression d'air ou flux d'air).

Remarque : si le type de capteur indiqué est différent de celui du capteur d'environnement spécifié, le message d'erreur suivant apparaît : Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (Le type de capteur spécifié XXX ne correspond pas au type du capteur (<sensortype>), où XXX représente le type de capteur spécifié et <sensortype>, le type de capteur correct.

- <value> est une valeur numérique affectée à l'hystérésis du capteur d'environnement indiqué. Reportez-vous à ***Hystérésis d'infirmation : définition*** (à la page 178) pour en savoir plus sur cette fonction.

Exemple

La commande suivante définit l'hystérésis d'infirmation du capteur de température d'environnement portant le numéro d'identification 4 sur 2 degrés Celsius. Cela signifie que la température doit descendre d'au moins 2 degrés Celsius au-dessous du seuil supérieur ou monter d'au moins 2 degrés Celsius au-dessus du seuil inférieur avant que l'événement de dépassement d'un seuil ne soit infirmé.

```
config:#   sensor externalsensor 4 temperature hysteresis 2
```

Définition du délai d'affirmation du capteur

Cette syntaxe de commande configure la valeur du délai d'affirmation d'un capteur d'environnement numérique.

```
config:#    sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

Variables :

- <n> est le numéro d'identification du capteur d'environnement que vous souhaitez configurer. Le numéro d'identification est affecté et affiché dans l'interface Web de EMX. Il s'agit d'un nombre entier compris entre 1 et 16.
- <sensor type> est un de ces types de capteurs : *temperature*, *humidity*, *air Pressure* ou *air Flow* (température, humidité, pression d'air ou flux d'air).

  Remarque : si le type de capteur indiqué est différent de celui du capteur d'environnement spécifié, le message d'erreur suivant apparaît : Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (Le type de capteur spécifié XXX ne correspond pas au type du capteur (<sensortype>), où XXX représente le type de capteur spécifié et <sensortype>, le type de capteur correct.

- <value> est un nombre exprimé en échantillons affecté au délai d'affirmation du capteur d'environnement indiqué. Reportez-vous à ***Délai d'affirmation : définition*** (à la page 179).

Exemple

La commande suivante définit le délai d'affirmation du capteur de température d'environnement portant le numéro d'identification 3 sur 4 échantillons. Cela signifie qu'au moins quatre échantillons consécutifs doivent dépasser un seuil de courant spécifique avant que l'événement de dépassement d'un seuil ne soit infirmé.

```
config:#    sensor externalsensor 3 temperature assertionTimeout 4
```

Commande de configuration des utilisateurs

La plupart des commandes de configuration des utilisateurs débutent par *user* hormis la commande de modification du mot de passe.

Création d'un profil utilisateur

Cette syntaxe de commande crée un profil utilisateur.

```
config:#   user create <name> <option> <roles>
```

Après avoir exécuté la commande de création d'un utilisateur, EMX vous invite à affecter un mot de passe à celui-ci. Ensuite :

1. Tapez le mot de passe et appuyez sur Entrée.
2. Tapez encore le même mot de passe pour le confirmer et appuyez sur Entrée.

Variables :

- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII. La variable <name> NE PEUT PAS contenir d'espace.
- <option> est une des options : *enable* ou *disable*.

Option	Description
enable	Active le profil utilisateur créé.
disable	Désactive le profil utilisateur créé.

- <roles> est un rôle ou une liste de rôles séparés par des virgules, affectés au profil d'utilisateur indiqué.

Exemple

La commande suivante crée un profil utilisateur et définit deux paramètres pour le nouvel utilisateur.

```
config:#   user create May enable admin
```

Résultats :

- Un profil utilisateur May est créé.
- Le nouveau profil utilisateur est activé.
- Le rôle **admin** est affecté au nouveau profil utilisateur.

Modification d'un profil utilisateur

Un profil utilisateur contient divers paramètres que vous pouvez modifier.

Conseil : vous pouvez combiner toutes les commandes pour modifier les paramètres d'un profil utilisateur spécifique en même temps. Reportez-vous à **Syntaxe multi-commandes** *(à la page 316).*

Modification du mot de passe d'un utilisateur

Cette syntaxe de commande vous autorise à modifier le mot de passe d'un utilisateur existant si vous disposez des privilèges d'administrateur.

```
config:#   user modify <name> password
```

Une fois la commande précédente exécutée, EMX vous invite à entrer un nouveau mot de passe. Ensuite :

1. Tapez un nouveau mot de passe et appuyez sur Entrée.
2. Tapez encore le nouveau mot de passe pour le confirmer et appuyez sur Entrée.

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.

Exemple

La procédure suivante illustre comment modifier le mot de passe de l'utilisateur May.

1. Assurez-vous que vous êtes passé en mode configuration. Reportez-vous à ***Passage en mode configuration*** (à la page 227).
2. Tapez la commande suivante pour modifier le mot de passe du profil utilisateur May.

   ```
   config:#   user modify May password
   ```
3. Tapez un nouveau mot de passe à l'invite et appuyez sur Entrée.
4. Tapez le même mot de passe et appuyez sur Entrée.
5. Si la modification du mot de passe aboutit, l'invite config:# apparaît.

Modification des données personnelles d'un utilisateur

Vous pouvez modifier les données personnelles d'un utilisateur, notamment son nom complet; son numéro de téléphone et son adresse électronique.

Pour modifier le nom complet d'un utilisateur, employez cette syntaxe de commande :

```
config:#   user modify <name> fullName "<full_name>"
```

Pour modifier le numéro de téléphone d'un utilisateur, employez cette syntaxe de commande :

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

Pour modifier l'adresse électronique d'un utilisateur, employez cette syntaxe de commande :

```
config:#   user modify <name> eMailAddress <email_address>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <full_name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII. La variable <full_name> doit être entourée de guillemets lorsqu'elle contient des espaces.
- <phone_number> est le numéro de téléphone auquel l'utilisateur indiqué est joignable. La variable <phone_number> doit être entourée de guillemets lorsqu'elle contient des espaces.
- <email_address> est l'adresse électronique de l'utilisateur indiqué.

Conseil : vous pouvez combiner toutes les commandes pour modifier les paramètres d'un profil utilisateur spécifique en même temps. Reportez-vous à **Syntaxe multi-commandes** *(à la page 316).*

Exemple

La commande suivante modifie deux paramètres du profil utilisateur May :

```
config:#   user modify May fullName "May Turner" telephoneNumber 123-4567
```

Résultats :

- May Turner est indiqué comme nom complet.
- Le numéro de téléphone de May est défini sur 123-4567.

Activation ou désactivation d'un profil utilisateur

Cette syntaxe de commande active ou désactive un profil utilisateur. Un utilisateur ne peut se connecter au dispositif EMX qu'après l'activation de son profil utilisateur.

```
config:#   user modify <name> enabled <option>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option> est une des options : *true* ou *false*.

Option	Description
true	Active le profil utilisateur indiqué.
false	Désactive le profil utilisateur indiqué.

Exemple

La commande suivante active le profil utilisateur May.

```
config:#   user modify May enabled true
```

Modification du mot de passe imposé

Cette syntaxe de commande détermine si la modification du mot de passe est imposée à la connexion suivante au profil utilisateur indiqué.

```
config:#    user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option> est une des options : *true* ou *false*.

Option	Description
true	Une modification du mot de passe est imposée à la connexion suivante de l'utilisateur.
false	La modification du mot de passe n'est pas imposée à la connexion suivante de l'utilisateur.

Exemple

La commande suivante impose la modification du mot de passe à la connexion suivante de May.

```
config:#    user modify May forcePasswordChangeOnNextLogin true
```

Modification des paramètres SNMPv3

Il existe différentes commandes pour modifier les paramètres SNMPv3 d'un profil utilisateur spécifique. Vous pouvez combiner toutes les commandes suivantes pour modifier les paramètres SNMPv3 en même temps. Reportez-vous à ***Syntaxe multi-commandes*** (à la page 316).

Pour activer ou désactiver l'accès SNMP v3 à EMX pour l'utilisateur indiqué :

```
config:#    user modify <name> snmpV3Access <option1>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option1> est une des options : *enable* ou *disable*.

Option	Description
enable	Active l'autorisation d'accès SNMP v3 pour l'utilisateur indiqué.
disable	Désactive l'autorisation d'accès SNMP v3 pour l'utilisateur indiqué.

Pour déterminer le niveau de sécurité :

```
config:#    user modify <name> securityLevel <option2>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option2> est une des options : *noAuthNoPriv*, *authNoPriv* ou *authPriv*.

Option	Description
noAuthNoPriv	Pas d'authentification et pas de confidentialité.
authNoPriv	Authentification et pas de confidentialité.
authPriv	Authentification et confidentialité.

Pour déterminer si la phrase passe d'authentification est identique au mot de passe :

```
config:#    user modify <name> userPasswordAsAuthenticationPassPhrase <option3>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option3> est une des options : *true* ou *false*.

Option	Description
true	La phrase passe d'authentification est identique au mot de passe.
false	La phrase passe d'authentification est différente du mot de passe.

Pour déterminer la phrase passe d'authentification :

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <authentication_passphrase> est une chaîne utilisée comme phrase passe d'authentification, comprenant 32 caractères imprimables ASCII au maximum.

Pour déterminer si la phrase passe de confidentialité est identique à la phrase passe d'authentification :

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option4> est une de ces options : *true* ou *false*.

Option	Description
true	La phrase passe de confidentialité est identique à la phrase passe d'authentification.
false	La phrase passe de confidentialité est différente de la phrase passe d'authentification.

Pour déterminer la phrase passe de confidentialité :

```
config:#    user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <privacy_passphrase> est une chaîne utilisée comme phrase passe de confidentialité, comprenant au plus 32 caractères imprimables ASCII.

Pour déterminer le protocole d'authentification :

```
config:#    user modify <name> authenticationProtocol <option5>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option5> est une de ces options : *MD5* ou *SHA-1*.

Option	Description
MD5	Le protocole d'authentification MD5 est appliqué.
SHA-1	Le protocole d'authentification SHA-1 est appliqué.

Pour déterminer le protocole de confidentialité :

```
config:#    user modify <name> privacyProtocol <option6>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option3> est une de ces options : *DES* ou *AES-128*.

Option	Description
DES	Le protocole de confidentialité DES est appliqué.
AES-128	Le protocole de confidentialité AES-128 est appliqué.

Exemple

La commande suivante définit trois paramètres SNMPv3 de l'utilisateur May.

```
config:#    user modify May snmpV3Access enable securityLevel authNoPriv
            userPasswordAsAuthenticationPassPhrase true
```

Résultats :

- L'autorisation d'accès SNMPv3 de l'utilisateur est activée.
- Le niveau de sécurité SNMPv3 concerne l'authentification uniquement, pas la confidentialité.
- La phrase passe d'authentification est identique au mot de passe de l'utilisateur.

Modification des rôles

Cette syntaxe de commande modifie les rôles d'un utilisateur spécifique.

```
config:#    user modify <name> roles <roles>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <roles> est un rôle ou une liste de rôles séparés par des virgules, affectés au profil d'utilisateur indiqué.

Exemple

La commande suivante affecte deux rôles à l'utilisateur May.

```
config:#    user modify May roles admin,tester
```

Résultats :

- L'utilisateur May est doté de l'union de tous les privilèges d'admin et de tester.

Modification des unités de mesure

Vous pouvez modifier les unités de mesure affichées pour les températures, la longueur et la pression pour un profil utilisateur particulier. Des commandes d'unité de mesure différentes peuvent être combinées pour définir toutes les unités de mesure en même temps. Pour combiner toutes les commandes, reportez-vous à ***Syntaxe multi-commandes*** (à la page 316).

Remarque : la modification des unités de mesure ne s'applique qu'à l'interface Web et à l'interface de ligne de commande.

Pour définir l'unité de température privilégiée :

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option1> est une des options : *C* ou *F*.

Option	Description
C	Cette option affiche la température en Celsius.
F	Cette option affiche la température en Fahrenheit.

Pour définir l'unité de longueur privilégiée :

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option2> est une des options : *meter* ou *feet*.

Option	Description
meter	Cette option affiche la longueur ou la hauteur en mètres.
feet	Cette option affiche la longueur ou la hauteur en pieds.

Pour définir l'unité de pression privilégiée :

```
config:#    user modify <name> preferredPressureUnit <option3>
```

Variables :

- <name> est le nom de l'utilisateur dont vous souhaitez modifier les paramètres.
- <option3> est une des options : *pascal* ou *psi*.

Option	Description
pascal	Cette option affiche la valeur de pression en Pascals (Pa).
psi	Cette option affiche la valeur de pression en psi.

Exemple

La commande suivante définit toutes les unités de mesure privilégiées de l'utilisateur May.

```
config:#    user modify May preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

Résultats :

- L'unité de température privilégiée est définie sur Fahrenheit.
- L'unité de longueur privilégiée est définie sur feet (pieds).
- L'unité de pression privilégiée est définie sur psi.

Définition de la clé publique SSH

Si l'authentification par clé SSH est activée, définissez la clé publique SSH pour chaque profil d'utilisateur grâce à la procédure suivante.

Pour définir la clé publique SSH pour un utilisateur particulier :

1. Tapez la commande de clé publique SSH comme indiqué ci-après et appuyez sur Entrée.

   ```
   config:#    user modify <nom> sshPublicKey
   ```

2. Le système vous invite à entrer le contenu de la clé publique SSH. Effectuez les opérations suivantes pour entrer le contenu :

   a. Ouvrez votre clé publique SSH à l'aide d'un éditeur de texte.

b. Copiez tout le contenu dans l'éditeur de texte.

c. Collez le contenu dans le terminal.

d. Appuyez sur Entrée.

Conseil : pour supprimer une clé publique SSH existante, appuyez sur Entrée sans rien taper ni coller lorsque le système vous invite à entrer le contenu.

Exemple

Cette section décrit comment définir une clé publique SSH pour l'utilisateur existant, May, si l'authentification par clé publique SSH est activée. Reportez-vous à ***Définition de la méthode d'authentification SSH*** (à la page 252). Le contenu de votre clé publique SSH devrait être différent de celui affiché dans cet exemple.

Pour définir la clé publique SSH pour l'utilisateur May :

1. Assurez-vous que vous êtes passé en mode configuration. Reportez-vous à ***Passage en mode configuration*** (à la page 227).
2. Tapez la commande suivante et appuyez sur Entrée.

```
config:#   user modify May sshPublicKey
```

1. Le système vous invite à entrer le contenu de la clé publique SSH.
2. Ouvrez la clé publique SSH à l'aide d'un éditeur de texte. Son contenu devrait être similaire au suivant.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDLZMx/ETBqjczWo0uU6JHZ54H7PwIoHyAa
OdeKdCq8i0h59p1VVa6vS4agObxMU8FjHIZ0uQSLknTjWw3wy358BpJVYmyz8HlTOm
QBR59VvIrSjn77cI7U8DbYQOVgqm8NvFami1Fbd7yX/pMXikeSXZCxP4QtonDvqgZ36l
vjQ== May@raritan.com
```

3. Sélectionnez et copiez tout le contenu de la clé publique SSH.
4. Collez le contenu dans le terminal.
5. Appuyez sur Entrée.

Suppression d'un profil utilisateur

Cette syntaxe de commande supprime un profil utilisateur existant.

```
config:#   user delete <name>
```

Exemple

La commande suivante supprime le profil utilisateur May.

```
config:#   user delete May
```

Modification de votre mot de passe

Chaque utilisateur peut modifier son mot de passe via la syntaxe de cette commande s'il dispose du privilèges Change Own Password (Changer son propre mot de passe). Notez que cette commande ne débute pas par *user*.

```
config:#   password
```

Une fois cette commande exécutée, EMX vous invite à entrer le mot de passe actuel et le nouveau respectivement.

Important : une fois le mot de passe modifié, le nouveau prend effet immédiatement que vous tapiez la commande apply ou non pour enregistrer les modifications.

Exemple

Cette procédure modifie votre propre mot de passe :

1. Assurez-vous que vous êtes passé en mode configuration. Reportez-vous à ***Passage en mode configuration*** (à la page 227).
2. Tapez la commande suivante et appuyez sur Entrée.

   ```
   config:#   password
   ```

3. Tapez le mot de passe existant et appuyez sur Entrée lorsque l'invite suivante apparaît.

   ```
   Current password (Mot de passe actuel) :
   ```

4. Tapez le nouveau mot de passe et appuyez sur Entrée lorsque l'invite suivante apparaît.

   ```
   Enter new password (Entrer le nouveau mot de passe) :
   ```

5. Tapez encore le nouveau mot de passe pour le confirmer et appuyez sur Entrée lorsque l'invite suivante apparaît.

   ```
   Re-type new password (Taper encore le nouveau mot de
   passe) :
   ```

Commandes de configuration de rôle

Une commande de configuration de rôle débute par *role*.

Création d'un rôle

Cette syntaxe de commande crée un rôle, avec une liste de privilèges, séparés par des points-virgules, affectés au rôle.

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

Si un privilège spécifique contient des arguments, il doit être suivi de deux-points puis des arguments.

```
config:#    role create "<name>" <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables :

- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII.
- <privilege1>, <privilege2>, <privilege3>, etc. sont les noms des privilèges affectés au rôle. Séparez les privilèges par un point-virgule. Reportez-vous à ***Tous les privilèges*** (à la page 303).
- <argument1>, <argument2>, etc. sont des arguments définis pour un privilège particulier. Séparez le privilège de son argument à l'aide des deux-points.

Tous les privilèges

Le tableau ci-dessous répertorie tous les privilèges.

Privilège	Description
adminPrivilege	Privilèges d'administrateur
changeAssetStripConfiguration	Modifier la configuration du bandeau de ressources
changeAuthSettings	Modifier les paramètres d'authentification
changeDataTimeSettings	Modifier les paramètres de date et d'heure

Privilège	Description
changeEmdConfiguration	Modifier la configuration EMD
changeEventSetup	Modifier les paramètres de l'événement
changeExternalSensorsConfiguration	Modifier la configuration des capteurs externes
changeLhxConfiguration	Modifier la configuration LHX
changeNetworkSettings	Modifier les paramètres réseau
changePassword	Changer son propre mot de passe
changeSecuritySettings	Modifier les paramètres de sécurité
changeSnmpSettings	Modifier les paramètres SNMP
changeUserSettings	Modifier la gestion des utilisateurs locaux
changeWebcamSettings	Modifier la configuration de la webcam
clearLog	Effacer le journal des événements local
firmwareUpdate	Mise à jour du firmware
performReset	Réinitialiser (Démarrage à chaud)
viewEventSetup	Afficher les paramètres de l'événement
viewLog	Afficher le journal des événements
viewSecuritySettings	Afficher les paramètres de sécurité
viewSnmpSettings	Afficher les paramètres SNMP
viewUserSettings	Afficher la gestion des utilisateurs locaux
viewWebcamSettings	Affichage des images et de la configuration de la webcam

Exemple

La commande suivante crée un rôle et lui affecte des privilèges.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Résultats :

- Un rôle tester est créé.
- Deux privilèges lui sont affectés : firmwareUpdate (Mise à jour du firmware) et viewEventSetup (Afficher les paramètres de l'événement).

Modification d'un rôle

Vous pouvez modifier divers paramètres d'un rôle, notamment ses privilèges.

Pour modifier la description d'un rôle :

```
config:#   role modify <name> description <description>
```

Variables :

- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII.
- <description> est une description comprenant des caractères alphanumériques. La variable <description> doit être entourée de guillemets lorsqu'elle contient des espaces.

Pour ajouter des privilèges supplémentaires à un rôle spécifique :

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

Si un privilège spécifique contient des arguments, ajoutez deux-points puis les arguments après lui.

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables :

- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII.
- <privilege1>, <privilege2>, <privilege3>, etc. sont les noms des privilèges affectés au rôle. Séparez les privilèges par un point-virgule. Reportez-vous à ***Tous les privilèges*** (à la page 303).
- <argument1>, <argument2>, etc. sont des arguments définis pour un privilège particulier. Séparez le privilège de son argument à l'aide des deux-points.

Pour supprimer des privilèges spécifiques d'un rôle :

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

Si un privilège spécifique contient des arguments, ajoutez deux-points puis les arguments après lui.

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Remarque : Lorsque vous supprimez des privilèges d'un rôle, assurez-vous que les privilèges et les arguments (éventuels) correspondent exactement à ceux affectés au rôle. Sinon, la commande ne peut pas retirer les privilèges indiqués car ils ne sont pas disponibles.

Variables :

- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII.
- <privilege1>, <privilege2>, <privilege3>, etc. sont les noms des privilèges affectés au rôle. Séparez les privilèges par un point-virgule. Reportez-vous à ***Tous les privilèges*** (à la page 303).
- <argument1>, <argument2>, etc. sont des arguments définis pour un privilège particulier. Séparez le privilège de son argument à l'aide des deux-points.

Exemple

La commande suivante modifie les privilèges du rôle tester.

```
config:#    role modify tester addPrivileges changeAuthSettings removePrivileges
            firmwareUpgrade
```

Résultats :

- Le privilège changeAuthSettings (Modifier les paramètres d'authentification) est ajouté au rôle.
- Le privilège firmwareUpgrade (Mise à niveau du firmware) est supprimé du rôle.

Suppression d'un rôle

Cette syntaxe de commande supprime un rôle existant.

```
config:#    role delete <name>
```

Exemple

La commande suivante supprime un rôle existant.

```
config:#    role delete tester
```

Commandes de gestion des ressources

Vous pouvez utiliser les commandes CLI pour modifier les paramètres du capteur de ressources connectées (le cas échéant) ou ceux des voyants du capteur.

Gestion des capteurs de ressources

Une commande de configuration de gestion des capteurs de ressources débute par `assetStrip`.

Nommage d'un capteur de ressources

Cette syntaxe de commande nomme ou renomme un capteur de ressources connecté au dispositif EMX.

```
config:#   assetStrip <n> name "<name>"
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII. La variable <name> doit être entourée de guillemets lorsqu'elle contient des espaces.

Exemple

Cette syntaxe de commande nomme ou renomme un capteur de ressources connecté au dispositif EMX.

```
config:#   assetStrip 1 name "Red Rack"
```

Définition du nombre d'unités de rack

Cette syntaxe de commande indique le nombre total d'unités de rack sur un capteur de ressources connecté au dispositif EMX.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Remarque : Pour le capteur de ressources Raritan, une unité de rack fait référence à un port d'étiquette.

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <number> est le nombre total d'unités de rack disponibles sur le capteur de ressources connecté. Cette valeur varie entre 8 et 64.

Exemple

La commande suivante définit le nombre total d'unités de rack sur le capteur de ressources nº 1 sur 48.

```
config:#   assetStrip 1 numberOfRackUnits 48
```

Définition du mode de numérotation des unités de rack

Cette syntaxe de commande indique le mode de numérotation des unités de rack sur les capteurs de ressources connectés au dispositif EMX. Le mode de numérotation change le numéro des unités de rack.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <mode> est un de ces modes de numérotation : *topDown* ou *bottomUp*.

Mode	Description
topDown	Les unités de rack sont numérotées en ordre croissant de l'unité de rack la plus haute à la plus basse.
bottomUp	Les unités de rack sont numérotées en ordre décroissant de l'unité de rack la plus haute à la plus basse.

Exemple

La commande ci-après entraîne la numérotation des unités de rack du capteur de ressources nº 1 dans l'ordre croissant en partant de l'unité la plus proche du connecteur RJ-45 du capteur à la plus éloignée. L'unité de rack la plus proche du connecteur RJ-45 est donc numérotée 1.

```
config:#   assetStrip 1 rackUnitNumberingMode topDown
```

Définition du décalage de numérotation des unités de rack

Cette syntaxe de commande indique le numéro de début des unités de rack sur les capteurs de ressources connectés au dispositif EMX.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <number> est le numéro de début des unités de rack sur le capteur de ressources connecté. Cette valeur est un nombre entier.

Exemple

La commande suivante définit le numéro de début des unités de rack sur le capteur de ressources nº 1 sur 5. Les unités de rack sont donc numérotées 5, 6, 7, etc. de la première unité à la dernière sur le capteur de ressources connecté.

```
config:#   assetStrip 1 rackUnitNumberingOffset 5
```

Définition de l'orientation des capteurs de ressources

Cette syntaxe de commande indique l'orientation des capteurs de ressources connectés au dispositif EMX. Cette commande est généralement inutile sauf si les capteurs de ressources sont fournis SANS détecteur d'inclinaison, ce qui rend EMX incapable de détecter l'orientation des capteurs de ressources.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <orientation> est une de ces options : *topConnector* ou *bottomConnector*.

Orientation	Description
topConnector	Cette option indique que le capteur de ressources est monté à l'aide du connecteur RJ-45 situé en haut.
bottomConnector	Cette option indique que le capteur de ressources est monté à l'aide du connecteur RJ-45 situé en bas.

Exemple

La commande suivante indique que le connecteur RJ-45 du capteur de ressources nº 1 est orienté vers le haut.

```
config:#   assetStrip 1 assetStripOrientation topConnector
```

Configuration des unités de rack

Pour le capteur de ressources Raritan, une unité de rack fait référence à un port d'étiquette. Une commande de configuration des unités de rack débute par `rackUnit`.

Nommage d'une unité de rack

Cette syntaxe de commande affecte ou modifie le nom d'une unité de rack du capteur de ressources indiqué.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <rack_unit> est le numéro d'index de l'unité de rack souhaitée. Le numéro d'index de chaque unité de rack est disponible sur la page Asset Strip (Bandeau de ressources) de l'interface Web.
- <name> est une chaîne comprenant jusqu'à 32 caractères imprimables ASCII. La variable <name> doit être entourée de guillemets lorsqu'elle contient des espaces.

Exemple

La commande suivante affecte le nom Linux server à l'unité de rack nº 25 du capteur de ressources nº 1.

```
config:#   rackUnit 1 25 name "Linux server"
```

Définition du mode de fonctionnement des voyants

Cette syntaxe de commande détermine si une unité de rack spécifique sur le capteur de ressources indiqué suit les paramètres globaux de couleur de voyant.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <rack_unit> est le numéro d'index de l'unité de rack souhaitée. Le numéro d'index de chaque unité de rack est disponible sur la page Asset Strip (Bandeau de ressources) de l'interface Web.
- <mode> est un de ces modes de voyant : *automatic* ou *manual*.

Mode	Description
automatic	Avec cette option, le voyant de l'unité de rack indiquée suit les paramètres de couleur de voyant généraux. Reportez-vous à Paramètres généraux de couleur de voyant. Il s'agit de la valeur par défaut.
manual	Cette option active la sélection d'une couleur et d'un mode de voyant différents pour l'unité de rack indiquée. Lorsque cette option est sélectionnée, reportez-vous à ***Définition d'une couleur de voyant pour une unité de rack*** (à la page 314) et ***Définition d'un mode de voyant pour une unité de rack*** (à la page 315) pour définir différents paramètres de voyant.

Exemple

La commande suivante autorise l'unité de rack nº 25 du capteur de ressources nº 1 à disposer de couleur et de mode de voyant différents.

```
config:#   rackUnit 1 25 LEDOperationMode manual
```

Définition de la couleur de déconnexion du voyant

Cette syntaxe de commande définit la couleur des voyants de toutes les unités de rack sur le(s) capteur(s) de ressources connecté(s) pour indiquer l'absence d'une étiquette de gestion des ressources connectées.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Définition d'une couleur de voyant pour une unité de rack

Cette syntaxe de commande définit la couleur de voyant d'une unité de rack spécifique sur le capteur de ressources indiqué. Vous ne devez définir la couleur de voyant d'une unité de rack que lorsque le mode de fonctionnement de ses voyants a été paramétré sur manual.

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <rack_unit> est le numéro d'index de l'unité de rack souhaitée. Le numéro d'index de chaque unité de rack est disponible sur la page Asset Strip (Bandeau de ressources) de l'interface Web.
- <color> est la valeur RVB hexadécimale d'une couleur au format HTML. La variable <color> est comprise entre #000000 et #FFFFFF.

Remarque : le paramètre de couleur de voyant d'une unité de rack supplante le paramètre global défini. Reportez-vous à Paramètres généraux de couleur de voyant.

Exemple

La commande suivante définit la couleur de voyant de l'unité de rack nº 25 du capteur de ressources nº 1 sur ROSE (soit FF00FF).

```
config:#   rackUnit 1 25 LEDColor #FF00FF
```

Définition d'un mode de voyant pour une unité de rack

Cette syntaxe de commande définit le mode de voyant d'une unité de rack spécifique sur le capteur de ressources indiqué. Vous ne devez définir le mode de voyant d'une unité de rack que lorsque le mode de fonctionnement de ses voyants a été paramétré sur manual.

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables :

- <n> est le numéro du port FEATURE auquel le capteur de ressources sélectionné est physiquement connecté. Pour un dispositif EMX n'ayant qu'un seul port FEATURE, le numéro est toujours 1.
- <rack_unit> est le numéro d'index de l'unité de rack souhaitée. Le numéro d'index de chaque unité de rack est disponible sur la page Asset Strip (Bandeau de ressources) de l'interface Web.
- <mode> est un de ces modes de voyant : *on*, *off*, *blinkSlow* ou *blinkFast*.

Mode	Description
on	Dans ce mode, les voyants restent allumés en permanence.
off	Dans ce mode, les voyants restent éteints en permanence.
blinkSlow	Dans ce mode, les voyants clignotent lentement.
blinkFast	Dans ce mode, les voyants clignotent rapidement.

Exemple

La commande suivante provoque le clignotement rapide des voyants de l'unité de rack nº 25 du capteur de ressources nº 1.

```
config:#   rackUnit 1 25 LEDMode blinkFast
```

Définition de la longueur de mémoire tampon d'historique

Cette syntaxe de commande modifie la longueur de la mémoire tampon d'historique. La longueur par défaut est de 25.

```
config:#   history length <n>
```

Variables :

- <n> est un nombre entier compris entre 1 et 250.
- Si vous laissez la variable <n> vide lors de l'utilisation de la commande, la mémoire tampon d'historique est définie sur 25 par défaut.

Syntaxe multi-commandes

Pour réduire la durée de la configuration, vous pouvez réunir plusieurs commandes de configuration dans une seule afin de les exécuter en même temps.

La syntaxe multi-commandes se présente comme suit :

```
<setting 1> <value 1> <setting 2> <value 2> <setting 3>
<value 3> ...
```

Exemple 1 - Combinaison de paramètres IP, de masque de sous-réseau et de passerelle

La syntaxe multi-commande suivante configure simultanément l'adresse IPv4, le masque de sous-réseau et la passerelle pour la connectivité réseau.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
           gateway 192.168.84.0
```

Résultats :

- L'adresse IP est définie sur 192.168.84.225.
- Le masque de sous-réseau est défini sur 255.255.255.0.
- La passerelle est définie sur 192.168.84.0.

Exemple 2 - Combinaison des paramètres SSID et PSK

Cette syntaxe multi-commandes configure les paramètres SSID et PSK simultanément pour la fonction sans fil.

```
config:#    network wireless SSID myssid PSK encryp_key
```

Résultats :

- La valeur SSID est définie sur myssid.
- La valeur PSK est définie sur encryp_key.

Fermeture du mode configuration

Les commandes d'application apply et d'annulation cancel permettent de quitter le mode configuration. La différence réside dans le fait que la commande apply enregistre tous les changements effectués en mode configuration alors que la commande cancel abandonne tous les changements.

▸ **Pour quitter le mode configuration, utilisez une de ces commandes :**

```
config:#    apply
```

-- OU --

```
config:#    cancel
```

L'invite # apparaît après l'activation d'Entrée, indiquant que vous êtes passé en mode administrateur.

Déblocage d'un utilisateur

Si l'accès d'un utilisateur à EMX est bloqué, vous pouvez le débloquer via la console locale.

▸ **Pour débloquer un utilisateur :**

1. Connectez-vous à l'interface CLI à l'aide d'un programme de terminal via une connexion locale. Reportez-vous à ***Avec HyperTerminal*** (à la page 212).
2. A l'invite Username, tapez `unblock` et appuyez sur Entrée.

```
Username: unblock
```

3. Lorsque l'invite Username to unblock (Nom d'utilisateur à débloquer), tapez le nom de connexion de l'utilisateur à débloquer et appuyez sur Entrée.

```
Username to unblock:
```

4. Un message apparaît indiquant que l'utilisateur indiqué est débloqué.

Réinitialisation de EMX

Vous pouvez rétablir les valeurs par défaut usine de EMX ou simplement le redémarrer à l'aide des commandes CLI.

Redémarrage du dispositif

Cette commande redémarre le dispositif EMX. Il ne s'agit pas de la réinitialisation aux valeurs par défaut usine.

Pour redémarrer le dispositif EMX :

1. Assurez-vous que vous êtes passé en mode administrateur et que l'invite # est affichée.
2. Entrez une des commandes suivantes pour redémarrer EMX.

```
#       reset unit
```

-- OU --

```
#       reset unit /y
```

3. Si vous entrez la commande sans `/y` à l'étape 2, un message vous demande de confirmer l'opération. Entrez y pour confirmer la réinitialisation.
4. Patientez jusqu'à l'apparition de l'invite Username (Nom d'utilisateur) indiquant que la réinitialisation est terminée.

Réinitialisation aux valeurs par défaut usine

Cette commande rétablit tous les paramètres du dispositif EMX aux valeurs par défaut usine.

Pour réinitialiser les paramètres EMX, utilisez une des commandes :

```
#       reset factorydefaults
```

-- OU --

```
#       reset factorydefaults /y
```

Reportez-vous à Utilisation de la commande CLI pour en savoir plus.

Dépannage du réseau

EMX offre quatre commandes de diagnostic pour résoudre les problèmes de réseau : *nslookup*, *netstat*, *ping* et *traceroute*. Les commandes de diagnostic fonctionnent de la même manière que les commandes Linux correspondantes et peuvent produire les mêmes résultats.

Passage en mode diagnostic

Les commandes de diagnostic ne fonctionnent qu'en mode diagnostic.

Pour passer en mode diagnostic :

1. Assurez-vous que vous êtes passé en mode administrateur et que l'invite # est affichée.
2. Tapez `diag` et appuyez sur Entrée. L'invite diag> apparaît pour indiquer que vous êtes en mode diagnostic.
3. Vous pouvez maintenant entrer des commandes de diagnostic pour le dépannage.

Commandes de diagnostic

La syntaxe des commandes de diagnostic varie d'une commande à l'autre.

Interrogation des serveurs DNS

Cette syntaxe de commande recherche des données concernant les serveurs de noms de domaine Internet (DNS) d'un hôte réseau.

```
diag>       nslookup <host>
```

Variables :

- <host> est le nom ou l'adresse IP de l'hôte dont vous souhaitez rechercher les données DNS.

Exemple

La commande suivante vérifie les données DNS concernant l'hôte 192.168.84.222.

```
diag>       nslookup 192.168.84.222
```

Affichage des connexions réseau

Cette syntaxe de commande affiche les connexions réseau et/ou le statut des ports.

```
diag>       netstat <option>
```

Variables :

- <option> est une des options : *ports* ou *connections*.

Option	Description
ports	Affiche les ports TCP/UDP.
connections	Affiche les connexions réseau.

Exemple

La commande suivante affiche les connexions serveur au dispositif EMX.

```
diag>       netstat connections
```

Test de la connectivité de réseau

Cette syntaxe de commande envoie le message ICMP ECHO_REQUEST à un hôte de réseau afin de vérifier sa connectivité de réseau. Si le résultat indique que l'hôte répond correctement, la connectivité réseau est bonne ou l'hôte est arrêté ou n'est pas connecté au réseau.

```
diag>       ping <host>
```

Variables :

- <host> est le nom ou l'adresse IP de l'hôte dont vous souhaitez vérifier la connectivité réseau.

Options :

- Vous pouvez inclure certaines ou toutes les options supplémentaires répertoriées ci-dessous dans la commande ping.

Options	Description
count <number1>	Détermine le nombre de messages à envoyer. <number1> est un nombre entier.
size <number2>	Détermine la taille du paquet. <number2> est un nombre entier d'octets.
timeout <number3>	Détermine la période d'attente avant le délai d'inactivité. <number3> est un nombre entier en secondes.

La syntaxe de la commande se présente comme suit lorsqu'elle inclut toutes les options :

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Exemple

La commande suivante vérifie la connectivité de réseau de l'hôte 192.168.84.222 en envoyant le message ICMP ECHO_REQUEST à l'hôte 5 fois.

```
diag>       ping 192.168.84.222 count 5
```

Traçage de route

Cette syntaxe de commande trace la route du réseau entre le dispositif EMX et un hôte réseau.

```
diag>       traceroute <host>
```

Variables :

- <host> est le nom ou l'adresse IP de l'hôte que vous souhaitez suivre.

Exemple

La commande suivante affiche le routage réseau existant pour l'hôte 192.168.84.222.

```
diag>       traceroute 192.168.84.222
```

Fermeture du mode diagnostic

▶ **Pour quitter le mode diagnostic, utilisez cette commande :**

```
diag>       exit
```

L'invite # apparaît après l'activation d'Entrée, indiquant que vous êtes passé en mode administrateur.

Recherche des paramètres disponibles pour une commande

Si vous n'êtes pas certain des commandes ou des paramètres disponibles pour un type particulier de commandes CLI, vous pouvez les afficher dans l'interface en ajoutant un espace, puis un point d'interrogation à la fin de la commande. La liste des paramètres disponibles et leurs descriptions s'affichent.

Voici quelques exemples d'interrogation :

Pour afficher les paramètres disponibles pour la commande show, la syntaxe est :

```
#           show ?
```

Pour afficher les paramètres de configuration du réseau disponibles, la syntaxe est :

```
config:#    network ?
```

Pour afficher les paramètres de configuration de rôles disponibles, la syntaxe est :

```
config:#    role ?
```

Récupération des commandes précédentes

Si vous souhaitez récupérer une des commandes entrées précédemment pendant la même session de connexion, appuyez sur la flèche Haut (↑) du clavier jusqu'à l'affichage de la commande souhaitée.

Chargement automatique d'une commande

Une commande CLI comporte toujours plusieurs mots. Vous pouvez facilement compléter certaines commandes CLI *particulières*, telles que reset, en appuyant sur les touches Tab ou Ctrl+i au lieu de taper la commande entière.

Pour compléter automatiquement une commande particulière :

1. Tapez les premières lettres ou les premiers mots de la commande. Par exemple, tapez le premier mot de la commande `reset factorydefaults`, c'est-à-dire `reset`.
2. Appuyez sur les touches Tab ou Ctrl+i jusqu'à ce que la commande entière apparaisse. Par exemple, même si vous n'avez entré qu'un mot de la commande de réinitialisation, le reste de la commande s'affiche après que vous avez appuyé sur les touches Tab ou Ctrl+i.

Déconnexion de l'interface CLI

Après avoir terminé vos tâches dans l'interface de ligne de commande, déconnectez-vous toujours de celle-ci pour empêcher à d'autres utilisateurs d'accéder à l'interface CLI.

Pour vous déconnecter de l'interface CLI :

1. Assurez-vous que vous êtes passé en mode administrateur et que l'invite # est affichée.
2. Tapez `exit` et appuyez sur Entrée.

Réinitialisation aux valeurs par défaut usine (CLI)

L'interface de ligne de commande (CLI) offre une commande de réinitialisation pour rétablir les valeurs par défaut usine du dispositif EMX. Pour en savoir plus sur CLI, reportez-vous à Utilisation de l'interface de ligne de commande.

Pour rétablir les valeurs par défaut usine à l'aide de la commande CLI :

1. Connectez un ordinateur au dispositif EMX. Reportez-vous à ***Connexion du dispositif EMX à un ordinateur*** (à la page 12).
2. Lancez un programme d'émulation de terminal, tel qu'HyperTerminal, Kermit ou PuTTY, puis ouvrez une fenêtre sur EMX.
3. Connectez-vous à l'interface de ligne de commande en entrant le nom d'utilisateur admin et son mot de passe. Reportez-vous à l'étape 4 de Configuration initiale du réseau.
4. Lorsque l'invite système # apparaît, entrez une des commandes suivantes et appuyez sur Entrée.
5. Type :

```
#    reset factorydefaults
```

OU

```
#   reset factorydefaults /y
```

6. Patientez jusqu'à l'apparition de l'invite Username (Nom d'utilisateur) indiquant que la réinitialisation est terminée.
7. Si vous avez entré la commande sans `/y`, un message vous demande de confirmer l'opération. Entrez y pour confirmer la réinitialisation.

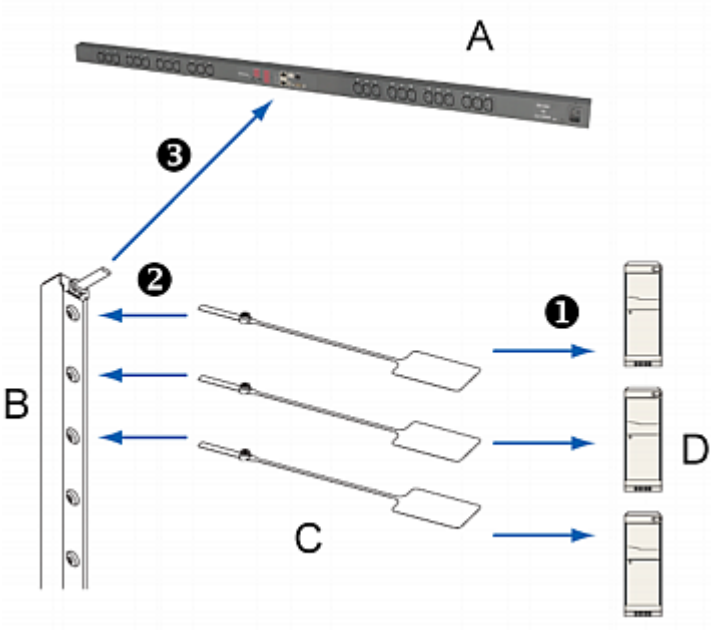
Annexe A Gestion des ressources de Dominion PX

Dans ce chapitre

Aperçu

La PDU PX2 de Raritan prend également en charge des capteurs de ressources pour vous permettre d'assurer le suivi à distance des dispositifs informatiques via l'interface Web de la PDU, tout en surveillant le statut d'alimentation de cette dernière. Seules les PDU dont le nom de modèle commence par PX2 prennent en charge la fonction de gestion des ressources.

Important : lorsque vous manipulez des capteurs de ressources connectés les uns aux autres, ne forcez pas trop sur les joints les reliant afin de ne pas les casser au point de connexion.



Lettre	Elément
A	Dispositif Dominion PX
B	Capteurs de ressources

Lettre	Elément
C	Etiquettes de gestion des ressources
D	Dispositifs informatiques, tels que des serveurs

Pour paramétrer un système de gestion des ressources :

1. Collez le côté adhésif de chaque étiquette de gestion des ressources à chaque dispositif informatique.
2. Branchez le connecteur à l'autre extrémité de chaque étiquette de gestion des ressources dans le port d'étiquette correspondant sur le capteur de ressources.
3. Connectez l'assemblage de capteurs de ressources sur le rack au dispositif Dominion PX en suivant cette procédure :
   a. Branchez une extrémité du câble UTP Catégorie 5e/6 au connecteur RJ-45 sur le capteur de ressources.
   b. Connectez l'autre extrémité du câble au port FEATURE du dispositif Dominion PX.

Pour plus d'informations sur le produit Dominion PX, reportez-vous à la documentation d'accompagnement du dispositif Dominion PX, que vous pouvez télécharger depuis la section ***Firmware and Documentation*** (***http://www.raritan.com/support/firmware-and-documentation/***) du site Web de Raritan. Ou vous pouvez accéder à l'aide en ligne du produit dans la section Product Online Help (http://www.raritan.com/support/online-help/).

Annexe B Spécifications

Dans ce chapitre

Facteurs de correction pour l'altitude (EMX)

Si un capteur de pression d'air différentielle Raritan est relié à votre dispositif, l'altitude entrée peut servir de facteur de correction pour l'altitude. C'est-à-dire que le relevé du capteur de pression d'air différentielle sera multiplié par le facteur de correction pour obtenir un relevé correct.

Ce tableau montre la relation entre les différentes altitudes et les facteurs de correction.

Altitude (mètres)	Altitude (pieds)	Facteur de correction
0	0	0,95
250	820	0,98
425	1394	1,00
500	1640	1,01
740	2428	1,04
1500	4921	1,15
2250	7382	1,26
3000	9842	1,38

Température ambiante d'exploitation maximum (EMX)

La température ambiante d'exploitation maximum (TMA) de EMX est la même pour tous les modèles quelle que soit la norme de certification (CE ou UL).

Spécification	Mesure
Température ambiante	60 degrés Celsius

Spécification	Mesure
maximum	

Broches de port RS-232 série

Définition broche RS-232/de signal			
Broche nº	Signal	Direction	Description
1	DCD	Entrée	Données
2	RxD	Entrée	Réception de données (données en entrée)
3	TxD	Sortie	Transmission de données
4	DTR	Sortie	Terminal prêt
5	GND	—	Signal de mise à la terre
6	DSR	Entrée	Poste de données prêt
7	RTS	Sortie	Demande d'émission
8	CTS	Entrée	Prêt à émettre
9	RI	Entrée	Indicateur de sonnerie

Broches de port RJ-12 du capteur

Définition broche RJ-12/de signal			
Broche nº	Signal	Direction	Description
1	+12V	—	Alimentation (500mA, protégée par fusible)
2	GND	—	Signal de mise à la terre
3	—	—	—
4	—	—	—
5	GND	—	Signal de mise à la terre
6	1 fil		Utilisé pour le port Feature

Broches de port RS-485

Définition broche RS-485/de signal			
Broche nº	Signal	Direction	Description
1	—	—	—
2	—	—	—
3	D+	bidirectionnel	Données +
4	—	—	—
5	—	—	—
6	D-	bidirectionnel	Données -
7	—	—	—
8	—	—	—

Annexe C Illustration de la configuration LDAP

Cette section présente un exemple de LDAP pour illustrer la procédure de configuration à l'aide de Microsoft Active Directory® (AD). Pour configurer l'authentification LDAP, quatre étapes principales sont requises :

a. Déterminer les comptes et les groupes d'utilisateurs conçus pour EMX

b. Créer des groupes d'utilisateurs pour EMX sur le serveur AD

c. Configurer l'authentification LDAP sur le dispositif EMX

d. Configurer des rôles sur le dispositif EMX

Dans ce chapitre

Etape A. Déterminer des comptes et groupes d'utilisateurs

Déterminez les comptes et les groupes d'utilisateurs authentifiés pour accéder à EMX. Dans cet exemple, nous allons créer deux groupes d'utilisateurs disposant d'autorisations différentes. Chaque groupe sera composé de deux comptes d'utilisateur disponibles sur le serveur AD.

Groupes d'utilisateurs	Comptes d'utilisateur (membres)
EMX_User	usera
	emxuser2
EMX_Admin	userb
	emxuser

Autorisations des groupes :

- Le groupe EMX_User ne disposera que d'autorisations en lecture seule.
- Le groupe EMX_Admin disposera d'autorisations complètes sur le système.

Etape B. Configurer des groupes d'utilisateurs sur le serveur AD

Vous devez créer des groupes pour EMX sur le serveur AD, puis transformer les utilisateurs appropriés en membres de ces groupes.

Dans cet exemple, nous supposons les faits suivants :

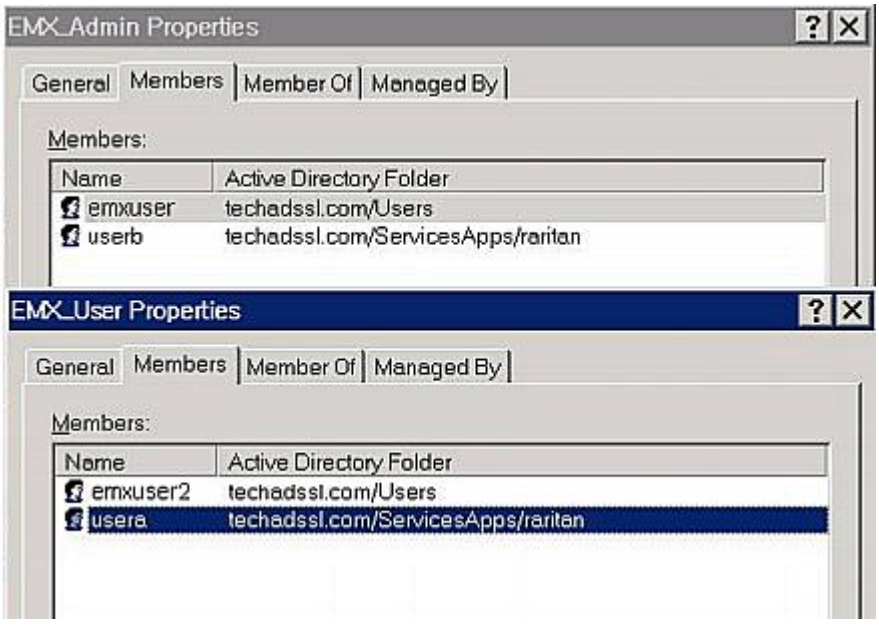
- Les groupes du dispositif EMX sont nommés *EMX_Admin* et *EMX_User*.
- Les comptes d'utilisateur *emxuser*, *emxuser2*, *usera* et *userb* existent déjà sur le serveur AD.

Pour configurer les groupes d'utilisateurs sur le serveur AD :

1. Sur le serveur AD, créez les groupes *EMX_Admin* et *EMX_User*.

   Remarque : consultez la documentation ou l'aide en ligne qui accompagne Microsoft AD pour obtenir des instructions détaillées.

2. Ajoutez les comptes *emxuser2* et *usera* au groupe EMX_User.
3. Ajoutez les comptes *emxuser* et *userb* au groupe EMX_Admin.
4. Vérifiez que chaque groupe comporte les utilisateurs qui conviennent.



Etape C. Configurer l'authentification LDAP sur le dispositif EMX

Vous devez activer et paramétrer correctement l'authentification LDAP sur le dispositif EMX pour utiliser une authentification externe.

Dans cet exemple, nous supposons que :

- Les paramètres du serveur DNS sont configurés correctement. Reportez-vous à ***Modification des paramètres réseau*** (à la page 82) et ***Rôle d'un serveur DNS*** (à la page 86).
- Le nom de domaine du serveur AD est *techadssl.com*, son adresse IP est *192.168.56.3*.
- Le protocole AD N'EST PAS chiffré sur SSL.
- Le serveur AD utilise le port TCP par défaut *389*.
- Une liaison anonyme est utilisée.

Pour configurer l'authentification LDAP :

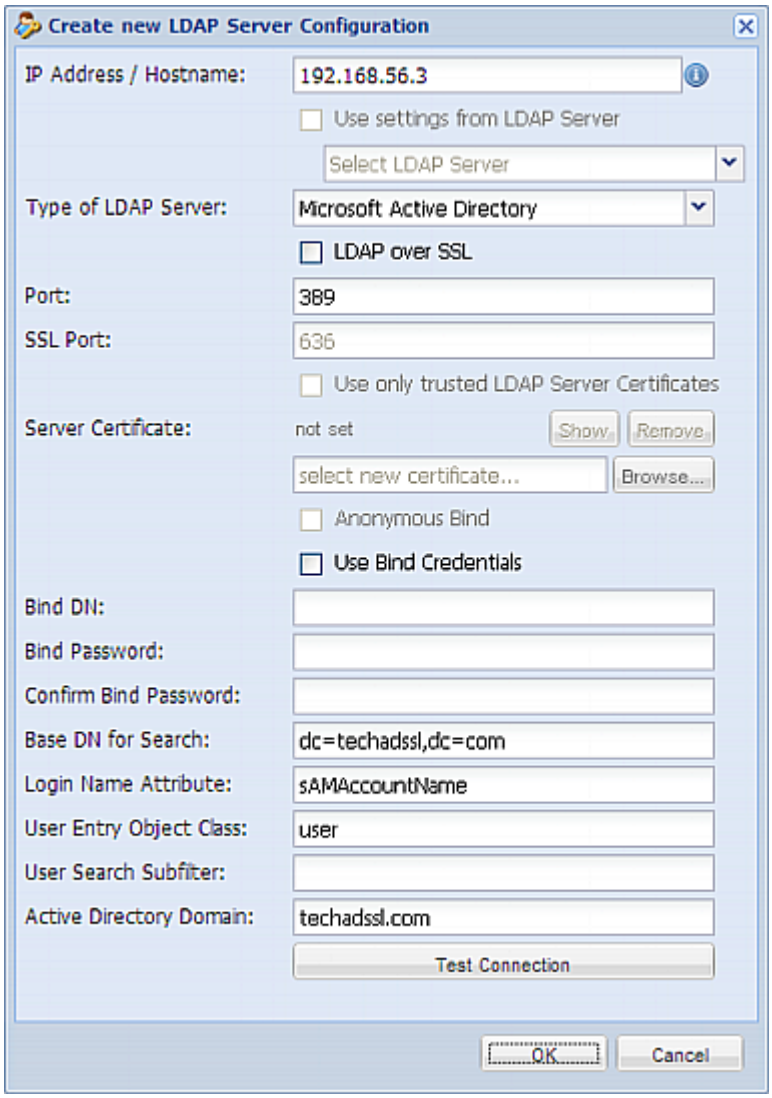
1. Choisissez Device Settings > Security > Authentication (Paramètres du dispositif > Sécurité > Authentification). La boîte de dialogue Authentication Settings (Paramètres d'authentification) s'affiche.
2. Sélectionnez la case d'option LDAP pour activer l'authentification de serveur LDAP/LDAPS à distance.
3. Cliquez sur New (Nouveau) pour ajouter un serveur LDAP/LDAPS pour authentification. La boîte de dialogue Create new LDAP Server Configuration (Créer une configuration de serveur LDAP) apparaît.
4. Fournissez à EMX les données concernant le serveur AD.
   - Adresse IP/Nom d'hôte : tapez le nom de domaine `techadssl.com` ou l'adresse IP `192.168.56.3`.

   Important : si le chiffrement SSL n'est pas activé, vous pouvez taper le nom de domaine ou l'adresse IP dans ce champ. S'il est activé, vous devez taper le nom de domaine complet.

   - Use settings from LDAP server (Utiliser les paramètres du serveur LDAP) : laissez la case à cocher désélectionnée.
   - Type of LDAP Server (Type de serveur LDAP) : sélectionnez Microsoft Active Directory dans la liste déroulante.
   - LDAP over SSL (LDAP sur SSL) : laissez la case à cocher désélectionnée puisque le chiffrement SSL n'est pas appliqué dans cet exemple.
   - Port : vérifiez que le champ est défini sur `389`.
   - SSL Port and Server Certificate (Port SSL et certificat du serveur) : omettez les deux champs puisque le chiffrement SSL n'est pas activé.

- Use Bind Credentials (Utiliser les informations d'identification de liaison) : NE COCHEZ PAS cette case car une liaison anonyme est utilisée.
- Bind DN, Bind Password and Confirm Bind Password (ND de liaison, Mot de passe de liaison et Confirmer mot de passe de liaison) : omettez ces trois champs car une liaison anonyme est utilisée.
- Base DN for Search (ND de base pour recherche) : tapez `dc=techadssl,dc=com` comme point de départ de la recherche sur le serveur AD.
- Login Name Attribute (Attribut de nom de connexion) : vérifiez que ce champ est défini sur `sAMAccountName` puisque le serveur LDAP est Microsoft Active Directory.
- User Entry Object Class (Classe d'objets d'entrée d'utilisateur) : vérifiez que ce champ est défini sur `user` puisque le serveur LDAP est Microsoft Active Directory.
- User Search Subfilter (Sous-filtre de recherche des utilisateurs) : ce champ est facultatif. Les données du sous-filtre sont également utiles pour filtrer les objets supplémentaires dans une structure de répertoire importante. Dans cet exemple, il reste vide.

- Active Directory Domain (Domaine Active Directory) : tapez `techadssl.com`.



Remarque : pour en savoir plus sur la configuration LDAP, reportez-vous à **Paramétrage de l'authentification LDAP** *(à la page 124).*

5. Cliquez sur OK pour enregistrer les modifications. Le serveur LDAP est enregistré.
6. Cliquez sur OK pour enregistrer les modifications. L'authentification LDAP est activée.

Remarque : si les horloges de EMX et du serveur LDAP ne sont pas synchrones, les certificats sont considérés comme expirés et les utilisateurs ne peuvent pas s'authentifier à l'aide de LDAP. Pour assurer une synchronisation correcte, il est recommandé que les administrateurs configurent EMX et le serveur LDAP pour qu'ils utilisent le même serveur NTP.

Etape D. Configurer des groupes d'utilisateurs sur le dispositif EMX

Un rôle sur le dispositif EMX détermine les autorisations sur le système. Vous devez créer des rôles dont les noms sont identiques aux groupes d'utilisateurs créés pour EMX sur le serveur AD ou l'autorisation échouera. Nous allons donc créer les rôles nommés *EMX_User* et *EMX_Admin* sur le dispositif EMX.

Dans cet exemple, nous supposons les faits suivants :

- Les utilisateurs affectés au rôle *EMX_User* ne peuvent qu'accéder au dispositif EMX et afficher les paramètres.
- Les utilisateurs affectés au rôle *EMX_Admin* disposent d'autorisations Administrator (Administrateur) et peuvent donc accéder au dispositif EMX et le configurer.

Pour créer le rôle EMX_User et lui affecter les autorisations appropriées :

1. Choisissez User Management > Roles (Gestion des utilisateurs > Rôles). La boîte de dialogue Manage Roles (Gérer les rôles) apparaît.

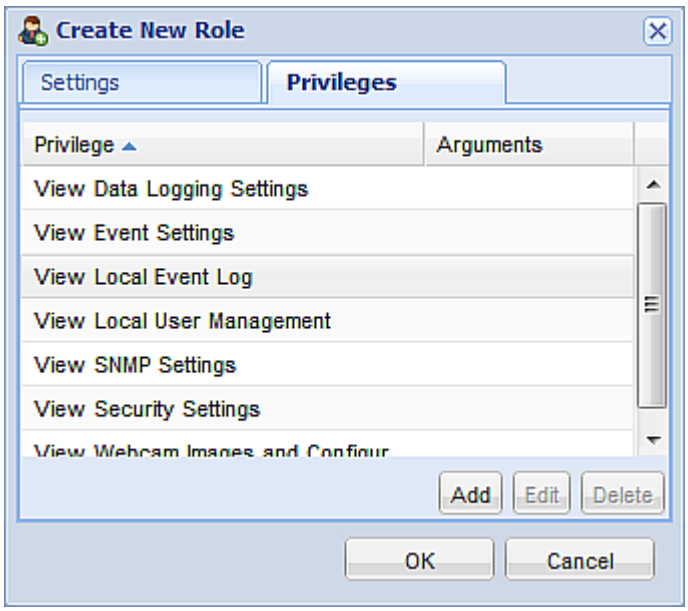
   Conseil : vous pouvez également accéder à la boîte de dialogue Manage Roles en cliquant sur le bouton Manage Roles de la boîte de dialogue Edit User XXX (Modifier l'utilisateur XXX).

2. Cliquez sur New (Nouveau). La boîte de dialogue Create New Role (Créer un rôle) apparaît.
3. Tapez `EMX_User` dans le champ Role Name (Nom du rôle).
4. Tapez une description du rôle EMX_User dans le champ Description. Dans cet exemple, nous entrons : « Le rôle peut uniquement consulter les paramètres EMX » pour décrire le rôle.
5. Cliquez sur l'onglet Privileges (Privilèges) pour sélectionner toutes les autorisations View XXX (Afficher XXX, XXX représentant le nom du paramètre). Une autorisation View XXX permet aux utilisateurs de consulter les paramètres XXX sans pouvoir les configurer ou les modifier.
   a. Cliquez sur Add (Ajouter). La boîte de dialogue Add Privileges to new Role (Ajouter des privilèges au nouveau rôle) apparaît.

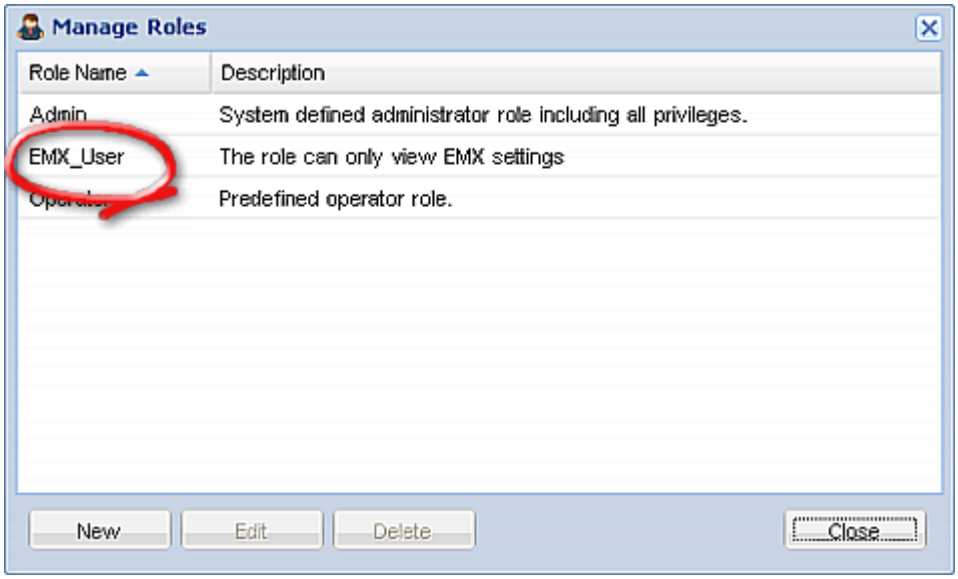
b. Sélectionnez une autorisation commençant par le mot View (Afficher) dans la liste des privilèges, telle que View Event Settings (Afficher les paramètres de l'événement).

c. Cliquez sur Add (Ajouter).

d. Répétez les étapes A à C pour ajouter toutes les autorisations commençant par View.



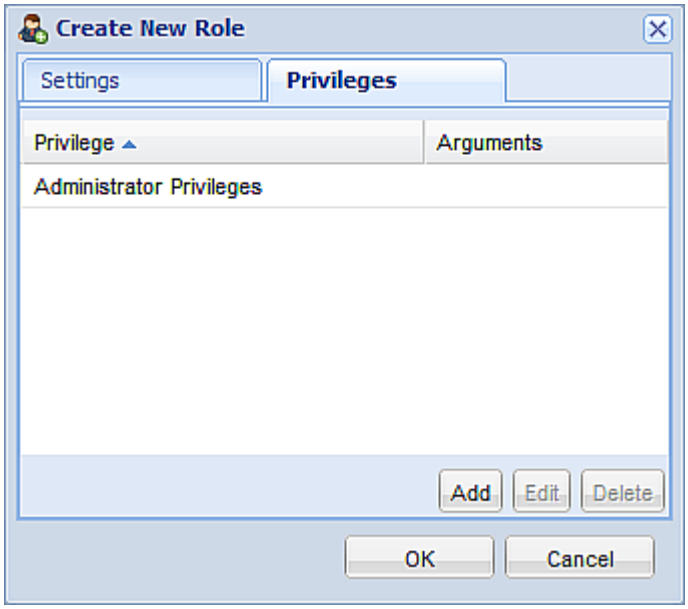
6. Cliquez sur OK pour enregistrer les modifications. Le rôle EMX_User est créé.



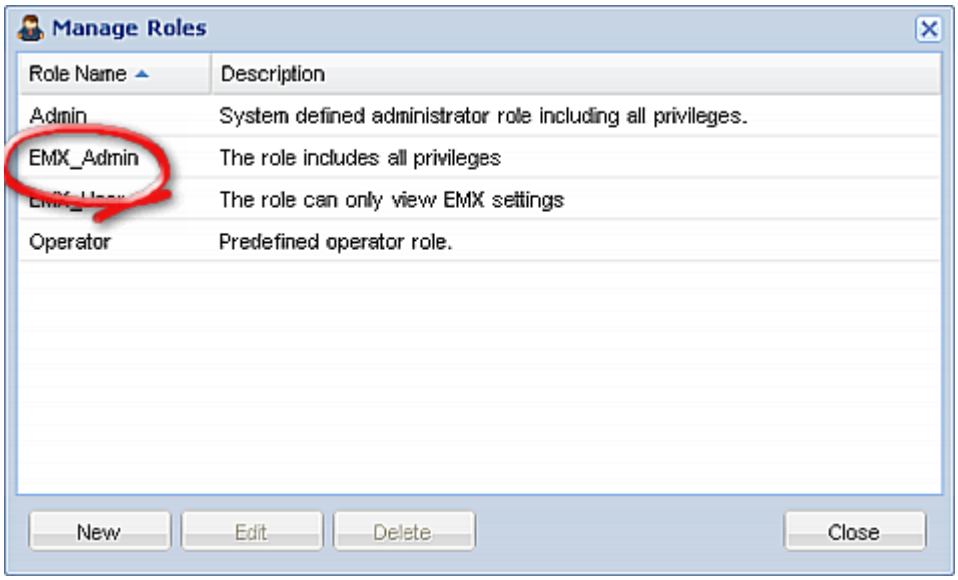
7. Laissez la boîte de dialogue Manage Roles (Gérer les rôles) ouverte pour créer le rôle EMX_Admin.

Pour créer le rôle EMX_Admin et lui affecter des autorisations complètes :

1. Cliquez sur New (Nouveau). La boîte de dialogue Create New Role (Créer un rôle) apparaît.
2. Tapez `EMX_Admin` dans le champ Role Name (Nom du rôle).
3. Tapez une description du rôle EMX_Admin dans le champ Description. Dans cet exemple, nous entrons « Le rôle dispose de tous les privilèges » pour décrire le rôle.
4. Cliquez sur l'onglet Privileges pour sélectionner l'autorisation Administrator. Celle-ci permet aux utilisateurs de configurer ou de modifier tous les paramètres du dispositif EMX.
   a. Cliquez sur Add (Ajouter). La boîte de dialogue Add Privileges to new Role (Ajouter des privilèges au nouveau rôle) apparaît.
   b. Sélectionnez l'autorisation nommée Administrator Privileges (Privilèges de l'administrateur) dans la liste des privilèges.
   c. Cliquez sur Add (Ajouter).



5. Cliquez sur OK pour enregistrer les modifications. Le rôle EMX_Admin est créé.



6. Cliquez sur Close (Fermer) pour quitter la boîte de dialogue.

Index

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W

Etats-Unis/Canada/Amérique latine

Lundi - Vendredi
8h00 - 20h00, heure de la côte Est des Etats-Unis
Tél. : 800-724-8090 ou 732-764-8886
Pour CommandCenter NOC : appuyez sur 6, puis sur 1.
Pour CommandCenter Secure Gateway : appuyez sur 6, puis sur 2.
Fax : 732-764-8887
E-mail pour CommandCenter NOC : tech-ccnoc@raritan.com
E-mail pour tous les autres produits : tech@raritan.com

Chine

Beijing
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-10-88091890

Shanghai
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-21-5425-2499

Guangzhou
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-20-8755-5561

Inde

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +91-124-410-7881

Japon

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5991
E-mail : support.japan@raritan.com

Europe

Europe
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +31-10-2844040
E-mail : tech.europe@raritan.com

Royaume-Uni
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +44-20-7614-77-00

France
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +33-1-47-56-20-39

Allemagne
Lundi - Vendredi
8h30 - 17h30, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0
E-mail : rg-support@raritan.com

Melbourne, Australie

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +61-3-9866-6887

Taiwan

Lundi - Vendredi
9h00 - 18h00, UTC/GMT - Heure normale 5 - Heure avancée 4
Tél. : +886-2-8919-1333
E-mail : support.apac@raritan.com