

**REVIEW DRAFT - CISCO CONFIDENTIAL**



## **Guide de démarrage rapide de Cisco Business Dashboard & Probe**

**Première publication:** 5 Novembre 2020

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. Tous droits réservés.



Le logo Java est une marque commerciale ou une marque déposée de Sun Microsystems aux États-Unis ou dans d'autres pays.

© 2020 Cisco Systems, Inc. Tous droits réservés.





## TABLE DES MATIÈRES

---

<b>CHAPITRE 1</b>	<b>Présentation de Cisco Business Dashboard</b>	<b>1</b>
	À propos de la solution de Cisco Business Dashboard	1
	Public	1
	Documents connexes	2
	Terminologie	2

---

<b>CHAPITRE 2</b>	<b>Exécuter la configuration initiale du tableau de bord</b>	<b>5</b>
	Exécuter la configuration initiale du tableau de bord	5

---

<b>CHAPITRE 3</b>	<b>Configuration initiale de la sonde</b>	<b>11</b>
	Configuration initiale de la sonde	11

---

<b>CHAPITRE 4</b>	<b>Exécuter la configuration initiale des appareils gérés directement</b>	<b>15</b>
	Exécuter la configuration initiale des appareils gérés directement	15

---

<b>CHAPITRE 5</b>	<b>Configuration du réseau</b>	<b>17</b>
	Configurer le réseau pour Cisco Business Dashboard	17
	Configurer la fonction Plug and Play du réseau	20
	Configurer le réseau	22

---

<b>CHAPITRE 6</b>	<b>Questions fréquentes</b>	<b>25</b>
	Questions fréquentes d'ordre général	25
	Questions fréquentes sur la détection	25
	Questions fréquentes sur la configuration	26
	Questions fréquentes sur la sécurité	26
	Questions fréquentes sur l'accès à distance	29

***REVIEW DRAFT - CISCO CONFIDENTIAL***

Questions fréquentes sur les mises à jour logicielles 30



# CHAPITRE 1

## Présentation de Cisco Business Dashboard

Ce chapitre contient les sections suivantes :

- [À propos de la solution de Cisco Business Dashboard](#) , à la page 1
- [Public](#), à la page 1
- [Documents connexes](#), à la page 2
- [Terminologie](#), à la page 2

### À propos de la solution de Cisco Business Dashboard

Cisco Business Dashboard fournit des outils permettant de contrôler et de gérer votre appareil réseau Cisco Business. Cisco Business Dashboard détecte automatiquement votre réseau, et vous aide à configurer et à contrôler tous les appareils Cisco Business pris en charge, notamment les commutateurs, les routeurs et les points d'accès sans fil. Elle vous signale aussi la disponibilité des mises à jour des microprogrammes et vous indique les appareils qui ne sont plus couverts par la garantie ou un contrat d'assistance.

Cisco Business Dashboard est une application distribuée comprenant deux composants ou applications distincts : l'application principale Cisco Business Dashboard, également appelée *tableau de bord*, et une ou plusieurs instances de Cisco Business Dashboard Probe, également appelées *sonde*.

Une seule instance de Cisco Business Dashboard est installée à un emplacement approprié du réseau. L'interface utilisateur du tableau de bord vous permet d'obtenir une vue générale sur l'état de tous les sites de votre réseau, ou de vous concentrer sur un seul site ou appareil pour afficher des informations spécifiques le concernant.

Une instance de Cisco Business Dashboard Probe est installée sur chaque site du réseau et associée au tableau de bord. La sonde détecte le réseau et communique directement avec chaque appareil géré pour le compte du tableau de bord.

Certains appareils réseau peuvent être directement associés au tableau de bord et gérés en l'absence de sonde. Lorsque les appareils réseau sont gérés directement de cette manière, toutes les fonctions de gestion sont disponibles pour l'appareil, mais il est possible que le processus de découverte du réseau ne soit pas aussi complet qu'en présence d'une sonde.

### Public

Ce guide est principalement destiné aux administrateurs de réseau chargés d'installer et de gérer le logiciel de Cisco Business Dashboard.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Documents connexes

La documentation de Cisco Business Dashboard est composée de plusieurs guides. Notamment :

- **Guide de démarrage rapide (le présent document)** : ce guide explique en détail comment effectuer la configuration initiale de Cisco Business Dashboard à l'aide des options les plus couramment sélectionnées.
- **Guides d'installation**

Le tableau suivant répertorie tous les guides d'installation du logiciel de tableau de bord qui peuvent être déployés sur différentes plates-formes. Consultez les chemins d'accès fournis dans la colonne d'emplacement pour plus de détails :

Plates-formes prises en charge	Lieu
Amazon Web Services	<a href="#">Guide d'installation de Cisco Business Dashboard pour Amazon Web Services</a>
Oracle VirtualBox	<a href="#">Guide d'installation de Cisco Business Dashboard pour Oracle VirtualBox</a>
Microsoft Hyper-V	<a href="#">Guide d'installation de Cisco Business Dashboard pour Microsoft Hyper-V</a>
VMWare vSphere, Workstation et Fusion	<a href="#">Guide d'installation de Cisco Business Dashboard pour VMware</a>
Ubuntu Linux (Dashboard & Probe) et Raspbian Linux (Probe uniquement)	<a href="#">Guide d'installation de Cisco Business Dashboard pour Linux</a>

- **Guide d'administration** : ce guide de référence contient des informations détaillées sur l'ensemble des fonctionnalités et des options fournies par le logiciel, et sur la façon dont elles peuvent être configurées et utilisées. Consultez le [Guide d'administration de Cisco Business Dashboard](#).
- **Liste des appareils pris en charge** : cette liste fournit des informations sur les appareils pris en charge par Cisco Business Dashboard et les fonctionnalités disponibles pour chaque type d'appareil. Pour obtenir la liste de tous les appareils pris en charge par Cisco Business Dashboard, consultez la rubrique [Cisco Business Dashboard – Liste des appareils pris en charge](#).

## Terminologie

Terme	Description
□ Hyper-V	Une plate-forme de virtualisation fournie par Microsoft Corporation.
Open Virtualization Format (OVF)	Une archive TAR contenant une ou plusieurs machines virtuelles au format OVF. Cette méthode indépendante de la plate-forme permet de conditionner et de distribuer des machines virtuelles.



**REVIEW DRAFT - CISCO CONFIDENTIAL**

Terme	Description
Fichier OVA (Open Virtual Appliance ou Application)	Un package qui contient les fichiers suivants utilisés pour décrire une machine virtuelle et sauvegardés dans une archive unique au format .TAR : <ul style="list-style-type: none"> <li>• Fichier de description (.OVF)</li> <li>• Fichiers .MF (Manifest) et de certificat (en option)</li> </ul>
Raspberry Pi	Un ordinateur à carte unique à très faible coût développé par Raspberry Pi Foundation. Pour plus d'informations, consultez le site <a href="https://www.raspberrypi.org/">https://www.raspberrypi.org/</a> .
Raspbian	Une distribution Linux basée sur Debian optimisée pour Raspberry Pi. Pour plus d'informations, consultez le site <a href="https://www.raspbian.org/">https://www.raspbian.org/</a> .
VirtualBox	Une plate-forme de virtualisation fournie par Oracle Corporation.
Disque dur virtuel	Un disque dur virtuel est un format de fichier d'image de disque permettant de stocker tout le contenu d'un disque dur.
Machine virtuelle	Un environnement de traitement informatique virtuel dans lequel peuvent s'exécuter un système d'exploitation invité et un logiciel applicatif associé. Plusieurs machines virtuelles peuvent être exécutées sur le même système hôte simultanément.
<ul style="list-style-type: none"> <li>• VMware ESXi</li> <li>• VMware Fusion</li> <li>• vSphere Server</li> <li>• VMware Workstation</li> </ul>	Une plate-forme de virtualisation fournie par VMware Inc.
vSphere Client	Une interface utilisateur qui permet aux utilisateurs de se connecter à distance à vCenter Server ou VMware ESXi à partir d'un ordinateur Windows. Vous pouvez utiliser l'interface principale pour vSphere Client pour créer, gérer et surveiller des machines virtuelles, leurs ressources et les hôtes. Elle offre également un accès aux machines virtuelles via une console.

***REVIEW DRAFT - CISCO CONFIDENTIAL***



## CHAPITRE 2

# Exécuter la configuration initiale du tableau de bord

---

Ce chapitre contient les sections suivantes :

- [Exécuter la configuration initiale du tableau de bord, à la page 5](#)

## Exécuter la configuration initiale du tableau de bord

Vous devez effectuer quelques tâches de configuration pour vous assurer que le tableau de bord répond à vos exigences.

### Configuration des paramètres système de base sur l'image de machine virtuelle ou l'instance AWS

Pour configurer les paramètres système de base, comme l'adressage IP et les paramètres d'heure du tableau de bord, procédez comme suit :

1. Connectez-vous à la console du tableau de bord à l'aide des outils adaptés à votre hyperviseur en cas d'utilisation d'une machine virtuelle, ou en vous connectant à votre instance AWS dans le cas de SSH.
2. Si vous utilisez une machine virtuelle, connectez-vous avec le nom d'utilisateur et le mot de passe par défaut suivant : `cisco`. Dans le cas d'une instance AWS, utilisez la paire de clés que vous avez spécifiée lors de la création de l'instance et le nom d'utilisateur suivant : `cisco`.

Vous devrez modifier le mot de passe du compte Cisco immédiatement après la connexion. Le nouveau mot de passe doit être un mot complexe qui ne figure pas dans le dictionnaire et qui combine plusieurs types de caractères.

3. Saisissez la commande `sudo config_vm` pour réaliser la configuration initiale. Lorsque vous y serez invité, saisissez le mot de passe du compte Cisco. L'utilitaire `config_vm` vous permet de modifier les paramètres de la plate-forme en plusieurs étapes.
4. Vous devez d'abord modifier le nom d'hôte du tableau de bord. Le nom d'hôte sert à identifier le tableau de bord sur le réseau. Choisissez un nom pertinent ou conservez le nom d'hôte par défaut en ignorant cette étape.



---

#### Remarque

Cette étape n'est pas disponible avec le Cisco Business Dashboard pour AWS.

---

**REVIEW DRAFT - CISCO CONFIDENTIAL**

5. Ensuite, vous serez invité à modifier les ports du serveur web. Si les valeurs par défaut de ces ports sont modifiées, vous devrez sans doute aussi modifier les paramètres du pare-feu sur votre réseau ou les paramètres du groupe de sécurité dans AWS.
6. Vous devrez ensuite configurer l'interface réseau. Vous avez le choix ici entre une adresse IP statique et DHCP (par défaut). Si vous sélectionnez l'adresse IP statique, vous devez fournir des informations concernant l'adresse IP, la passerelle par défaut et les adresses des serveurs DNS. L'interface réseau se réinitialisera si vous apportez des changements ici.

**Remarque**

Cette étape n'est pas disponible avec Cisco Business Dashboard pour AWS. Pour modifier la configuration du réseau, utilisez la console EC2 dans AWS.

7. Ensuite, vous devez configurer les paramètres d'heure du tableau de bord. Vous pouvez choisir de configurer un ou plusieurs serveurs NTP pour la synchronisation de l'heure (recommandé), puis vous devez sélectionner le fuseau horaire.

**Remarque**

Si vous utilisez l'hyperviseur VirtualBox et installez les « guest additions » de VirtualBox sur la machine virtuelle, le service NTP timesyncd ne fonctionne pas.

8. Enfin, vous êtes invité à changer le mot de passe du chargeur d'amorçage. Le nom d'utilisateur et le mot de passe du chargeur d'amorçage peuvent être utilisés dans la console, au démarrage du système, pour modifier le processus de démarrage du système ou pour récupérer les mots de passe perdus du système d'exploitation. Les informations d'identification par défaut du chargeur d'amorçage sont les suivantes : nom d'utilisateur : **root** et mot de passe : **cisco**.

Vous pouvez modifier ces paramètres à tout moment en exécutant à nouveau le script ou via l'interface web sous **Administration > Paramètres de la plate-forme**.

**Lancer l'interface utilisateur du tableau de bord**

1. Lancez un navigateur, tel que **Google Chrome** ou **Microsoft Edge**.
2. Dans le champ **Adresse**, saisissez l'adresse IP ou le nom d'hôte du tableau de bord, puis appuyez sur **Entrée**.
3. Saisissez le nom d'utilisateur par défaut : `cisco` et le mot de passe : `cisco`. Si vous utilisez le Cisco Business Dashboard pour AWS, le mot de passe par défaut correspond à l'ID de l'instance. Vous pouvez afficher l'ID de l'instance dans la console EC2 AWS.
4. Cliquez sur **Connexion**. Vous serez invité à modifier le mot de passe du compte Cisco. Assurez-vous que le nouveau mot de passe comporte au moins 8 caractères issus d'au moins 3 types de caractères différents.
5. Cliquez sur **Next (Suivant)**. Vous découvrirez la manière dont le Cisco Business Dashboard utilise vos données et les informations qu'il partage avec Cisco. Effectuez les modifications nécessaires, puis cliquez sur **Terminer**.

L'interface utilisateur du Cisco Business Dashboard s'affiche.

## REVIEW DRAFT - CISCO CONFIDENTIAL

### Créer des organisations (facultatif)

Les organisations sont utilisées dans le Cisco Business Dashboard pour diviser les réseaux, les utilisateurs et les appareils en groupes qui sont généralement administrés séparément. Chaque réseau ou appareil appartient à une organisation, et chaque utilisateur peut gérer une ou plusieurs organisations. Une organisation peut représenter un client, un service ou une zone géographique, mais l'utilisation d'organisations assure un contrôle plus approfondi sur les utilisateurs autorisés à gérer les différentes parties du réseau. Une seule organisation est créée par défaut lors de l'installation du tableau de bord.

Procédez comme suit pour créer une nouvelle organisation :

1. Accédez à **Administration** > **Organisations**.
2. Cliquez sur le signe **+** (plus) en haut du tableau.
3. Donnez un nom à l'organisation et renseignez les champs requis.
4. Donnez un nom au nouveau groupe d'appareils ; ce nom doit être utilisé comme groupe par défaut pour les appareils nouvellement découverts. Le nouveau groupe d'appareils est créé en même temps que l'organisation.
5. Cliquez sur **Save** (Enregistrer).
6. Répétez les étapes 1 à 5 pour chaque organisation que vous souhaitez créer.

### Créer des utilisateurs et modifier des mots de passe

Le tableau de bord est configuré au départ avec un seul nom d'utilisateur et un mot de passe unique par défaut.

Pour ajouter de nouveaux utilisateurs, procédez comme suit :

1. Accédez à **Administration** > **Utilisateurs**.
2. Cliquez sur le signe **+** (plus) en haut du tableau **Utilisateurs**.
3. Dans la fenêtre **Ajouter un utilisateur** qui s'affiche, saisissez les informations relatives à l'utilisateur à créer. Indiquez si l'utilisateur est un administrateur, un administrateur d'organisation, un opérateur ou un utilisateur en lecture seule. Vous trouverez ci-dessous les privilèges octroyés à chaque type d'utilisateur.
  - Les administrateurs ont accès à toutes les fonctionnalités, notamment la gestion du système
  - Les administrateurs d'organisation ont accès à toutes les fonctionnalités relatives à une ou plusieurs organisations, mais n'ont pas accès aux menus dédiés au système
  - Les opérateurs ont accès à toutes les fonctions disponibles dans les organisations qui leur ont été attribuées, mais ne sont pas en mesure de gérer des utilisateurs. Ils n'ont pas accès aux menus dédiés au système
  - Les utilisateurs en lecture seule ne peuvent pas modifier la configuration et n'ont qu'un accès limité aux menus d'administration. Ils n'ont pas accès aux menus dédiés au système
4. Cliquez sur **Enregistrer** pour créer un nouvel utilisateur.

Vous pouvez également définir les restrictions relatives à la complexité des mots de passe sur la page **Utilisateurs** en sélectionnant l'onglet **Paramètres utilisateur**. Vous devrez configurer de nouveaux mots de passe pour respecter ces restrictions.

Pour changer votre mot de passe, procédez comme suit :

**REVIEW DRAFT - CISCO CONFIDENTIAL**

1. En haut à droite de l'interface utilisateur, cliquez sur votre nom d'utilisateur pour afficher le menu déroulant. Sélectionnez ensuite **Mon profil**. Une page s'affiche.
2. Cliquez sur le lien Réinitialiser le mot de passe.
3. Saisissez votre mot de passe actuel et le nouveau mot de passe dans les champs appropriés
4. Cliquez sur **Enregistrer**.

**Configurer des licences****Remarque**

Cela ne s'applique pas à la version Metered du Cisco Business Dashboard pour AWS.

Cisco Business Dashboard dispose d'une licence pour utiliser Cisco Smart Licensing. Lors de la première installation, le tableau de bord est en mode d'évaluation. Ce mode vous permet de gérer jusqu'à dix appareils réseau sans restriction et vous laisse 90 jours pour obtenir des licences si le nombre d'appareils augmente. Pour appliquer des licences achetées au système, vous devez associer le tableau de bord à un compte Cisco Smart qui contient suffisamment de licences pour votre réseau.

Pour associer le tableau de bord à votre compte Smart, procédez comme suit :

1. Connectez-vous à votre compte Smart à cette adresse <https://software.cisco.com>. Cliquez sur le lien **Smart Software Licensing** situé dans la section **Licence**.
2. Sélectionnez la page **Inventaire** et, si nécessaire, modifiez le compte virtuel sélectionné par défaut. Cliquez ensuite sur l'onglet **Général**.
3. Créez un nouveau Code d'enregistrement d'instance du produit en cliquant sur **Nouveau code**. Ajoutez éventuellement une description et modifiez la valeur **Expire après**. Cliquez sur **Créer le code**.
4. Copiez le code que vous venez de créer dans le presse-papiers en sélectionnant **Copier** dans le menu déroulant **Actions** à droite du code.
5. Accédez à l'interface utilisateur du Cisco Business Dashboard et sélectionnez **Administration** > **Licence**.
6. Cliquez sur le bouton **S'inscrire** et collez le code dans le champ approprié. Cliquez sur **OK**.

Le tableau de bord est enregistré avec Cisco Smart Licensing et demande suffisamment de licences pour le nombre d'appareils réseau à gérer. Si le nombre de licences est insuffisant, un message s'affiche sur l'interface utilisateur et vous aurez 90 jours pour obtenir assez de licences avant de voir les fonctionnalités du système limitées. Pour en savoir plus sur le processus de gestion des licences, consultez le chapitre dédié à la *gestion des licences* du [Guide d'administration de Cisco Business Dashboard](#).

**Désactiver la sonde intégrée dans l'image de machine virtuelle****Remarque**

Cela ne s'applique pas au Cisco Business Dashboard pour AWS.

L'image de machine virtuelle du tableau de bord englobe le logiciel de sonde qui permet de gérer les appareils sur le réseau local vers le tableau de bord. Si vous ne voulez pas gérer le réseau local, vous pouvez désactiver la sonde intégrée en procédant comme suit :

## **REVIEW DRAFT - CISCO CONFIDENTIAL**

1. Accédez à **Système > Sonde locale**.
2. Cliquez sur le bouton pour désactiver la sonde intégrée.
3. Cliquez sur **Enregistrer**.

### **Créer des réseaux (facultatif)**

Vous pouvez prédéfinir des dossiers réseau dans le tableau de bord pour les sondes que vous associez ultérieurement. En général, chaque réseau représente un site distinct, mais vous pouvez avoir plusieurs réseaux sur le même site. Pour créer un nouveau réseau, procédez comme suit :

1. Accédez à **Réseau**.
2. Cliquez sur **Ajouter un réseau** dans la **vue cartographique** ou sur l'icône + (plus) dans la **vue liste**.
3. Indiquez le nom, l'organisation et le groupe d'appareils par défaut pour le réseau.
4. Saisissez l'adresse du réseau dans les champs appropriés. Si vous saisissez une adresse partielle, une liste des résultats potentiels s'affichera. Il vous suffira de choisir l'emplacement dans la liste. Vous pouvez aussi cliquer sur un site sur la carte.
5. Cliquez sur **Enregistrer**.
6. Répétez les étapes 1 à 5 pour chaque réseau que vous souhaitez créer.

***REVIEW DRAFT - CISCO CONFIDENTIAL***





## CHAPITRE 3

# Configuration initiale de la sonde

Ce chapitre contient les sections suivantes :

- [Configuration initiale de la sonde, à la page 11](#)

## Configuration initiale de la sonde

Vous devez effectuer quelques tâches de configuration pour vous assurer que la sonde répond à vos exigences.

### Localiser l'adresse IP de la sonde

Pour trouver l'adresse IP utilisée par la sonde, utilisez l'une des méthodes suivantes :

1. L'adresse IP par défaut de la sonde est configurée à l'aide de DHCP. Assurez-vous que le serveur DHCP est en cours d'exécution et est joignable. Si aucun serveur DHCP n'est disponible, l'adresse IP correspond par défaut à 192.168.1.10.
2. Vous pouvez détecter la sonde et y accéder en utilisant l'**utilitaire de détection de réseau Cisco FindIT** qui vous permet de trouver automatiquement tous les appareils Cisco pris en charge dans le même segment du réseau local que votre PC. Vous pouvez obtenir une vue instantanée de chaque périphérique ou lancer l'utilitaire de configuration du produit pour afficher et configurer les paramètres. Pour obtenir plus d'informations, consultez la section <http://www.cisco.com/go/findit>.
3. La sonde est compatible avec Bonjour et s'annonce automatiquement elle-même en utilisant le protocole Bonjour. Si vous êtes équipé d'un navigateur compatible avec Bonjour, vous pouvez trouver la sonde sur votre réseau local sans connaître son adresse IP.
4. Si vous utilisez une image de machine virtuelle, vous pouvez récupérer l'adresse IP de la sonde à partir de la console de la machine virtuelle. Servez-vous des outils de gestion de votre hyperviseur pour vous connecter à la console de la machine virtuelle en utilisant le nom d'utilisateur par défaut : `cisco` et le mot de passe : `cisco`. Vous devrez modifier le mot de passe immédiatement après la connexion. Le nouveau mot de passe doit être un mot complexe qui ne figure pas dans le dictionnaire et qui combine plusieurs types de caractères. Une bannière s'affichera alors pour vous indiquer l'adresse IP actuelle.

Si vous avez installé la sonde sur votre propre système Ubuntu ou Raspbian, vous pouvez utiliser les outils du système d'exploitation pour détecter l'adresse IP. Par exemple, vous pouvez exécuter la commande `ifconfig` dans une invite de l'interpréteur de commandes pour afficher une liste des interfaces et de leurs adresses.

## REVIEW DRAFT - CISCO CONFIDENTIAL

5. Localisez l'adresse IP attribuée par votre serveur DHCP en accédant à votre routeur ou à votre serveur DHCP. Consultez les instructions du serveur DHCP pour en savoir plus.

### Configurer une sonde logicielle

Une sonde logicielle est une sonde exécutée dans une machine virtuelle ou sur un hôte Linux lorsqu'aucune application de tableau de bord n'est exécutée sur la même machine virtuelle ni sur le même hôte.

Pour configurer une sonde logicielle, procédez comme suit :

1. Lancez un navigateur, tel que **Google Chrome** ou **Microsoft Edge**.
2. Dans le champ **Adresse**, saisissez l'adresse IP attribuée par DHCP et cliquez sur **Entrée**.
3. Saisissez le nom d'utilisateur par défaut : `cisco` et le mot de passe : `cisco`. Cliquez sur **Connexion**.
4. Vous serez invité à modifier le mot de passe du compte Cisco. Assurez-vous que le nouveau mot de passe comporte au moins 8 caractères issus d'au moins 3 types de caractères différents. Cliquez sur **Enregistrer**.
5. Spécifiez l'adresse ou le nom d'hôte d'un tableau de bord auquel vous souhaitez vous connecter, puis cliquez sur **Suivant**.
6. Votre navigateur vous redirige vers l'écran de connexion du tableau de bord. Connectez-vous à l'aide des informations d'identification d'administrateur du tableau de bord, puis votre navigateur vous ramène à nouveau vers la sonde.
7. Vous avez le choix entre créer un nouveau réseau ou sélectionner un réseau existant dans le menu déroulant. Si vous choisissez de créer un nouveau réseau, indiquez le nom et l'emplacement du réseau dans les champs prévus à cet effet.  
  
Vous devez saisir l'adresse du réseau dans les champs appropriés. Si vous saisissez une adresse partielle, une liste des résultats potentiels s'affichera. Il vous suffira de choisir l'emplacement dans la liste. Vous pouvez aussi cliquer sur un site sur la carte.
8. Cliquez sur **Terminer**.

### Configurer une sonde intégrée sur un produit Cisco série 100 à 500

Le processus d'association d'une sonde intégrée au tableau de bord nécessite une configuration explicite sur le tableau de bord et sur la sonde avant la connexion. Ce processus permet à l'appareil qui héberge la sonde intégrée d'être préconfiguré avant l'installation ou d'être configuré automatiquement via un mécanisme de déploiement automatique tel que le réseau prêt à l'emploi.

Pour configurer une sonde intégrée, procédez comme suit :

1. Créez un nouvel enregistrement de réseau pour la sonde intégrée en suivant les étapes décrites dans [Exécuter la configuration initiale du tableau de bord, à la page 5](#). Prenez note du nom de l'entreprise et du nom du réseau.
2. Dans l'interface utilisateur du tableau de bord, accédez à la page **Mon profil** en cliquant sur votre nom d'utilisateur au bas du volet de navigation. Utilisez cette page pour créer une nouvelle **clé d'accès** à l'aide du bouton **Générer une clé d'accès**. Vous pouvez également utiliser une clé d'accès existante si vous préférez.

## REVIEW DRAFT - CISCO CONFIDENTIAL



### Remarque

Il n'est pas nécessaire que la clé d'accès servant à associer une sonde intégrée au tableau de bord soit une clé durable. Cette clé ne doit être valide qu'au moment de l'association initiale. Une fois que la sonde et le tableau de bord sont associés, la connexion est authentifiée avec des informations d'identification de courte durée, en accès limité, propres au réseau et régénérées régulièrement.

3. Dans l'interface utilisateur de l'appareil, accédez à la page de configuration de la sonde et renseignez les champs fournis. Vous devez indiquer au moins l'adresse et le port du tableau de bord, le nom de l'entreprise, le nom du réseau, ainsi que l'ID de la clé d'accès et son mot de passe. Il peut également être nécessaire de configurer le certificat du tableau de bord. Vous trouverez plus d'informations ci-dessous. Vous avez aussi la possibilité d'apporter d'autres modifications.
4. Envoyez les modifications. La sonde se connecte alors au tableau de bord et est associée au réseau créé à l'étape 1.

### Vérifier l'identité du tableau de bord

Lors de l'établissement d'une connexion à la sonde, l'appareil vérifie que le certificat présenté par le tableau de bord est valide et approuvé. Pour assurer la validité du certificat et l'établissement de la connexion, le certificat doit répondre aux conditions suivantes :

- Le certificat doit être signé par une autorité de certification (AC) approuvée, ou doit être ajouté à la configuration de l'appareil en tant que certificat approuvé. Consultez le guide d'administration de l'appareil pour plus d'informations sur l'ajout d'un certificat approuvé.
- Si le tableau de bord est configuré comme une adresse IP, le champ Nom commun ou le champ Sujet-Alt-Nom du certificat doivent contenir cette adresse IP.
- Si le tableau de bord est configuré comme un nom d'hôte, le champ Nom commun ou le champ Sujet-Alt-Nom du certificat doivent contenir ce nom d'hôte.

### Configurer les paramètres système de base sur l'image de machine virtuelle à l'aide de l'interface utilisateur web (facultatif)

Pour configurer les paramètres système de base, comme l'adressage IP et les paramètres d'heure de la sonde à l'aide de l'interface utilisateur web, procédez comme suit :

1. Accédez à **Administration > Paramètres de la plate-forme**.
2. Spécifiez un nom d'hôte pour la sonde. Le nom d'hôte sert à identifier la sonde sur le réseau.
3. Vous pouvez également indiquer les paramètres de l'adresse IP statique dans les champs appropriés. Par défaut, la sonde détermine automatiquement les paramètres IP à l'aide de DHCP.
4. Vous pouvez également imposer à la sonde d'utiliser son horloge interne pour respecter le temps ou alors indiquer vos serveurs NTP préférés. Par défaut, la sonde synchronise son horloge avec les serveurs NTP publics.



### Remarque

Si vous utilisez l'hyperviseur VirtualBox et installez les « guest additions » de VirtualBox sur la machine virtuelle, le service NTP timesyncd ne fonctionne pas.

## REVIEW DRAFT - CISCO CONFIDENTIAL

### Configurer les paramètres système de base sur l'image de machine virtuelle via la ligne de commande (facultatif)

Au lieu d'utiliser l'interface web pour configurer les paramètres système de base, vous pouvez faire appel à la ligne de commande comme suit :

1. Connectez-vous à la console de la machine virtuelle.
2. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe par défaut : `cisco`. Vous devrez modifier le mot de passe immédiatement après la connexion. Le nouveau mot de passe doit être un mot complexe qui ne figure pas dans le dictionnaire et qui combine plusieurs types de caractères.
3. Saisissez la commande `sudo config_vm` pour réaliser la configuration initiale. L'utilitaire `config_vm` vous permet de modifier les paramètres de la plate-forme en plusieurs étapes.
4. Vous devrez d'abord modifier le nom d'hôte de la sonde. Le nom d'hôte sert à identifier la sonde sur le réseau. Choisissez un nom pertinent ou conservez le nom d'hôte par défaut en ignorant cette étape.
5. Ensuite, vous serez invité à modifier les ports du serveur web. Si les valeurs par défaut de ces ports sont modifiées, il est possible que vous deviez modifier les paramètres du pare-feu sur votre réseau.
6. Vous devrez ensuite configurer l'interface réseau. Vous avez le choix ici entre une adresse IP statique et DHCP (par défaut). Si vous sélectionnez l'adresse IP statique, vous devez fournir des informations concernant l'adresse IP, la passerelle par défaut et les adresses des serveurs DNS. L'interface réseau se réinitialisera si vous apportez des changements ici.
7. Ensuite, vous devez configurer les paramètres d'heure de la sonde. Vous pouvez choisir de configurer un ou plusieurs serveurs NTP pour la synchronisation de l'heure (recommandé), puis vous devez sélectionner le fuseau horaire.



#### Remarque

Si vous utilisez l'hyperviseur VirtualBox et installez les « guest additions » de VirtualBox sur la machine virtuelle, le service NTP `timesyncd` ne fonctionne pas.

8. Enfin, vous êtes invité à changer le mot de passe du chargeur d'amorçage. Le nom d'utilisateur et le mot de passe du chargeur d'amorçage peuvent être utilisés dans la console, au démarrage du système, pour modifier le processus de démarrage du système ou pour récupérer les mots de passe perdus du système d'exploitation. Les informations d'identification par défaut du chargeur d'amorçage sont les suivantes : nom d'utilisateur : **root** et mot de passe : **cisco**.

### Configurer les paramètres système de base lorsque la sonde est intégrée à un produit Cisco Business

Si vous utilisez une sonde intégrée dans un produit Cisco Business, l'interface utilisateur de la sonde est accessible via l'interface d'administration de l'appareil. Consultez le Guide d'administration de l'appareil pour découvrir comment associer la sonde au tableau de bord et modifier les paramètres système.

### Configurer les paramètres système de base lorsque la sonde est cohébergée avec Cisco Business Dashboard

Une sonde qui est cohébergée avec Cisco Business Dashboard ne dispose d'aucune interface utilisateur. Elle est entièrement gérée via l'interface utilisateur du tableau de bord.



## CHAPITRE 4

# Exécuter la configuration initiale des appareils gérés directement

Ce chapitre contient les sections suivantes :

- [Exécuter la configuration initiale des appareils gérés directement, à la page 15](#)

## Exécuter la configuration initiale des appareils gérés directement

Les appareils gérés directement sont des appareils réseau qui peuvent être associés directement à un tableau de bord et gérés sans qu'une sonde soit présente sur le réseau. Seuls certains appareils prennent en charge la gestion directe. Reportez-vous à la section [Cisco Business Dashboard – Liste des appareils pris en charge](#) pour obtenir la liste des appareils et des versions logicielles prenant en charge la gestion directe. Les appareils gérés directement détectent les autres appareils du réseau étendu et les ajoutent à l'inventaire du tableau de bord. Cependant, ce processus de détection n'est pas aussi complet que celui effectué par une sonde ; la topologie du réseau qui en résulte peut donc être moins précise.

Le processus d'association d'un appareil géré directement au tableau de bord nécessite une configuration explicite sur le tableau de bord et sur l'appareil avant la connexion. Ce processus permet à l'appareil d'être préconfiguré avant l'installation ou d'être configuré automatiquement via un mécanisme de déploiement automatique tel que la fonction Plug and Play du réseau.

Pour configurer un périphérique géré directement, procédez comme suit :

1. Créez un enregistrement réseau pour le réseau sur lequel l'appareil sera installé en suivant les étapes décrites à la section [Exécuter la configuration initiale du tableau de bord, à la page 5](#). Prenez note du nom de l'entreprise et du nom du réseau.
2. Dans l'interface utilisateur du **tableau de bord**, accédez à la page **Mon profil** en cliquant sur votre nom d'utilisateur au bas du volet de navigation. Utilisez cette page pour créer une nouvelle **clé d'accès** à l'aide du bouton **Générer une clé d'accès**. Vous pouvez également utiliser une clé d'accès existante si vous préférez.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Remarque**

Il n'est pas nécessaire que la clé d'accès servant à associer un appareil géré directement au tableau de bord soit une clé durable. Cette clé ne doit être valide qu'au moment de l'association initiale. Une fois que l'appareil et le tableau de bord sont associés, la connexion est authentifiée avec des informations d'identification de courte durée, en accès limité, propres à l'appareil et régénérées régulièrement.

3. Dans l'interface utilisateur de l'appareil, accédez à la page de configuration de Cisco Business Dashboard et renseignez les champs fournis. Vous devez indiquer au moins l'adresse et le port du tableau de bord, le nom de l'entreprise, le nom du réseau, ainsi que l'ID de la clé d'accès et son mot de passe. Il peut également être nécessaire de configurer le certificat du tableau de bord. Vous trouverez plus d'informations ci-dessous. Pour plus d'informations, reportez-vous au guide d'administration de l'appareil en question.
4. Envoyez les modifications. L'appareil se connecte alors au tableau de bord et est associé au réseau créé à l'étape 1.

Lors de l'établissement d'une connexion au tableau de bord, l'appareil vérifie que le certificat présenté par le tableau de bord est valide et approuvé. Pour assurer la validité du certificat et l'établissement de la connexion, le certificat doit répondre aux conditions suivantes :

- Le certificat doit être signé par une autorité de certification (AC) approuvée, ou doit être ajouté à la configuration de l'appareil en tant que certificat approuvé. Consultez le guide d'administration de l'appareil pour plus d'informations sur l'ajout d'un certificat approuvé.
- Si le tableau de bord est configuré comme une adresse IP, le champ **Nom commun** ou le champ **Sujet-Alt-Nom** du certificat doivent contenir cette adresse IP.
- Si le tableau de bord est configuré comme un nom d'hôte, le champ **Nom commun** ou le champ **Sujet-Alt-Nom** du certificat doivent contenir ce nom d'hôte.



## CHAPITRE 5

# Configuration du réseau

Ce chapitre contient les sections suivantes :

- [Configurer le réseau pour Cisco Business Dashboard, à la page 17](#)
- [Configurer la fonction Plug and Play du réseau, à la page 20](#)
- [Configurer le réseau, à la page 22](#)

## Configurer le réseau pour Cisco Business Dashboard

### Configurer les informations d'identification de l'appareil

Pour que le Cisco Business Dashboard puisse gérer les appareils réseau, vous devez indiquer des informations d'identification adéquates pour autoriser l'accès aux appareils.

Lorsque la sonde détecte un appareil, elle essaie d'abord d'y accéder avec les informations d'identification par défaut, soit le nom d'utilisateur `cisco`, le mot de passe `cisco` et la communauté SNMP définie sur `public`. Cependant, si l'appareil n'utilise pas les informations par défaut, vous devez fournir les bonnes informations d'identification comme expliqué ci-dessous :

1. Accédez à **Administration** > **Informations d'identification de l'appareil**. Le premier tableau de cette page dresse la liste de tous les appareils qui ont été détectés et qui ont besoin des informations d'identification, tandis que le deuxième tableau répertorie tous les appareils détectés qui disposent déjà des informations d'identification.
2. Saisissez un nom d'utilisateur et un mot de passe et/ou des informations d'identification SNMP dans les champs appropriés en haut de la page. Si vous devez indiquer d'autres jeux d'informations d'identification, cliquez sur l'icône + (plus). Vous pouvez dès lors saisir jusqu'à trois jeux de chaque type d'informations.
3. Cliquez sur **Apply** (Appliquer). Les sondes testeront les informations d'identification de chaque appareil qui les exige. Les informations d'identification correctes de chaque appareil sont enregistrées.

Les sondes détectent chaque réseau et génèrent une carte topologique et l'inventaire du réseau après avoir reçu les informations d'identification.

### En savoir plus sur votre réseau

vous donne des informations générales sur votre réseau, sous forme de carte ou de liste. Pour obtenir une vue d'ensemble de tous les réseaux, procédez comme suit :



## REVIEW DRAFT - CISCO CONFIDENTIAL

1. Assurez-vous d'avoir associé vos sondes à Cisco Business Dashboard, conformément aux instructions du chapitre précédent.
2. Cliquez sur **Réseau** dans la zone de navigation du tableau de bord. Cliquez sur le bouton pour passer en mode **carte** ou **liste**.
3. En **mode carte**, vous pouvez cliquer sur la carte et la faire glisser pour la repositionner, puis utiliser les boutons plus et moins pour effectuer des zooms avant et arrière. Chaque réseau sur lequel est installé une Cisco Business Dashboard Probe s'affiche sous forme d'icône sur la carte. Chaque icône contient un chiffre qui indique le nombre de notifications pour ce réseau et sa couleur détermine le niveau de sécurité le plus élevé. Cliquez sur une icône pour en savoir plus sur ce site. Si plusieurs icônes sont trop proches pour bien les distinguer, elles seront remplacées par un marqueur indiquant le nombre d'icônes réseau dans ce groupe. Cliquez sur le marqueur pour faire un zoom sur les sites de ce groupe.  
  
En **mode liste**, vous pouvez cliquer sur l'icône située dans le coin supérieur gauche du tableau pour sélectionner les colonnes à afficher. Par ailleurs, vous pouvez cliquer sur les en-têtes des colonnes pour trier le tableau.
4. Utilisez la zone de recherche pour trouver un réseau spécifique ou le réseau qui contient un appareil en particulier. Vous pouvez saisir le nom, l'adresse ou l'adresse IP d'un réseau dans la zone de recherche, ou le nom, l'adresse IP, l'adresse MAC ou le numéro de série d'un appareil.
5. Lorsque vous cliquez sur un réseau, le panneau **Informations de base** s'affiche pour vous donner plus d'informations sur ce réseau. Vous découvrirez notamment le nom et l'adresse du réseau, et une liste des notifications pour ce réseau.
6. Cliquez sur **Afficher** dans le panneau **Informations de base** pour afficher des informations détaillées sur le réseau, notamment sa topologie et les plans d'étage. Cliquez sur **Plus** pour afficher l'écran **Détails du réseau** qui vous permet de modifier les paramètres de ce réseau et d'afficher tous les appareils détectés sur ce réseau.

Vous pouvez également utiliser l'**Inventaire** pour trouver des informations détaillées sur tous les appareils de votre réseau. La page **Inventaire** dresse la liste de tous les appareils détectés sous forme de tableau. Vous pouvez filtrer cette liste pour limiter le nombre d'appareils affichés, puis cliquer sur chaque appareil pour obtenir plus d'informations à son sujet.

### Personnaliser la carte Topologie (facultatif)

Après avoir fourni des informations d'identification correctes, les **sondes** détecteront chaque réseau et généreront une carte **Topologie**. Vous pouvez ajuster cette carte si nécessaire.

1. Accédez au **Réseau** et sélectionnez le réseau concerné. Cliquez sur **Afficher** pour afficher la topologie.
2. Vous pouvez faire glisser l'icône de chaque appareil pour améliorer la mise en page. Toutes les modifications apportées à la mise en page sont permanentes. La Cisco Business Dashboard ne modifiera plus l'emplacement des icônes. Si vous souhaitez réactiver le placement automatique des icônes, cliquez sur **Remettre en forme la topologie**.
3. Cliquez sur **Superpositions** pour ouvrir le panneau **Superpositions et filtres** et servez-vous des cases à cocher pour restreindre les types d'appareils affichés dans le diagramme topologique.

### Charger les plans d'étage (facultatif)

Vous pouvez télécharger les plans d'étage de chaque réseau et y placer vos appareils réseau afin de déterminer l'emplacement de vos équipements. Les étapes suivantes vous guident tout au long du processus :



## REVIEW DRAFT - CISCO CONFIDENTIAL

1. Lorsque vous affichez le diagramme topologique d'un réseau, cliquez sur **Plan d'étage**.
2. Saisissez le nom du bâtiment et de l'étage, puis faites glisser et déposez un fichier image dans la zone ou cliquez sur le widget pour sélectionner un fichier image sur votre PC. Les fichiers image suivants sont pris en charge : .png, .gif, .jpg
3. Cliquez sur **Enregistrer** pour enregistrer les modifications.
4. Pour placer un appareil sur le plan d'étage, cliquez sur **Ajouter des périphériques** et saisissez son nom ou son adresse IP dans la zone de recherche en bas de l'écran. À mesure que vous écrivez, les appareils correspondants s'affichent. Ceux qui apparaissent grisés ont déjà été placés sur un plan d'étage.
5. Cliquez sur un appareil pour l'ajouter au plan de l'étage, puis faites-le glisser jusqu'au bon emplacement.

### Personnaliser le tableau de bord de surveillance

Vous pouvez adapter le tableau de bord de surveillance à vos exigences en procédant comme suit :

1. Sélectionnez le **Tableau de bord** dans le volet Navigation à gauche de l'écran. Le tableau de bord par défaut s'affiche.
2. Pour déplacer des widgets dans le tableau de bord, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau de bord et sélectionnez l'option **Mode d'édition**. Cliquez sur chaque widget et faites-le glisser vers l'emplacement souhaité. Cliquez sur le bord ou sur l'angle d'un widget et maintenez le bouton enfoncé pour le redimensionner.
3. Pour ajouter un nouveau widget au tableau de bord, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau de bord et sélectionnez un widget dans la liste. Sélectionnez le widget souhaité dans la liste. Pour supprimer un widget du tableau de bord, cliquez sur l'icône **✕ Supprimer le widget** dans le coin supérieur droit du widget en mode d'édition.
4. Une fois le tableau de bord correctement mis en forme, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau de bord et sélectionnez **Mode d'affichage** pour valider les modifications.
5. Pour modifier le comportement d'un widget, cliquez sur l'icône **Modifier la configuration du widget** en haut à droite du widget. Servez-vous de la liste déroulante pour choisir un appareil, une interface ou un réseau spécifique que le widget doit surveiller.

### Configurer les paramètres de messagerie (facultatif)

Cisco Business Dashboard vous préviendra par e-mail si des événements particuliers se produisent sur votre réseau. Pour déterminer les événements qui généreront un e-mail, reportez-vous à la section [Personnaliser l'affichage des notifications](#), à la page 20. Pour configurer les paramètres de messagerie, procédez comme suit :

1. Accédez à **Système > Paramètres de messagerie**.
2. Sur cette page, vous pouvez indiquer le serveur de messagerie et le port à utiliser pour les messages sortants, les paramètres de cryptage et d'authentification ainsi que les adresses e-mail à utiliser.
3. Après avoir terminé la configuration, cliquez sur **Enregistrer**.
4. Cliquez sur **Tester la connectivité** pour tester les modifications que vous avez apportées.

## REVIEW DRAFT - CISCO CONFIDENTIAL

### Personnaliser l'affichage des notifications

Vous pouvez personnaliser le comportement des notifications en suivant ces étapes :

1. Accédez à **Administration > Organisations** et sélectionnez l'organisation dans laquelle vous souhaitez personnaliser le comportement des notifications.
2. Cliquez sur **Notification**.
3. Décochez la case **Hériter des notifications par défaut**. Servez-vous des cases à cocher pour choisir les notifications qui vont déclencher une alerte contextuelle dans l'interface utilisateur et celles qui généreront l'envoi d'un e-mail. Si vous utilisez les notifications par e-mail, vous devez vous assurer que les paramètres de messagerie sont convenablement configurés. Pour obtenir plus d'informations, reportez-vous à la rubrique [Configurer les paramètres de messagerie \(facultatif\)](#), à la page 19.
4. Cliquez sur **Enregistrer**.

Vous pouvez également personnaliser les **Paramètres par défaut des notifications** en accédant à **Administration > Paramètres par défaut des notifications**.

## Configurer la fonction Plug and Play du réseau

Cisco Business Dashboard propose un service Plug and Play de réseau Cisco qui vous permet de centraliser la gestion du microprogramme et des fichiers de configuration de certains appareils Cisco. Pour plus d'informations sur la fonction Plug and Play du réseau, consultez le [Guide de la solution PnP](#).

Pour configurer la fonction Plug and Play du réseau, effectuez les tâches suivantes.

### Télécharger le microprogramme

1. Accédez à **Plug and Play du réseau > Images**.
2. Cliquez sur l'icône **+** (plus).
3. Choisissez une organisation, puis faites glisser un fichier de microprogramme de votre PC pour le déposer à l'emplacement cible dans la fenêtre **Charger le fichier**. Vous pouvez aussi cliquer sur l'emplacement cible et sélectionner l'image de microprogramme à télécharger.
4. Cliquez sur **Charger**.

Vous pouvez désigner une image par défaut pour un ou plusieurs types d'appareils. Pour désigner une image par défaut, procédez comme suit :

1. Cochez la case de l'image dans le tableau **Images** et cliquez sur **Modifier**.
2. Saisissez la liste des ID de produit en les séparant par une virgule dans le champ **Image par défaut pour les ID de produit**. Les ID de produit peuvent contenir des caractères génériques : ? représente un seul caractère et \* représente une chaîne de caractères.
3. Cliquez sur **Enregistrer**.

### Charger les configurations (facultatif)

1. Accédez à **Plug and Play du réseau > Configurations**.

## REVIEW DRAFT - CISCO CONFIDENTIAL

2. Cliquez sur l'icône **+** (plus).
3. Choisissez une organisation, puis faites glisser un fichier de configuration de votre PC et déposez-le à l'emplacement cible dans la fenêtre **Charger le fichier**. Vous pouvez aussi cliquer sur l'emplacement cible et sélectionner le fichier de configuration à télécharger.
4. Cliquez sur **Charger**.

Au lieu de charger des configurations, vous pouvez utiliser les modèles de configuration fournis avec l'application de tableau de bord. Vous pouvez cliquer sur le nom du fichier de configuration pour en voir le contenu.

### Configurer la détection

Pour que les appareils réseau puissent utiliser la fonction **Plug and Play du réseau**, ils doivent d'abord détecter le serveur **Plug and Play du réseau**. Trois mécanismes se tiennent à votre disposition pour fournir ces informations aux appareils :

1. **DHCP** : l'appareil réseau peut récupérer l'adresse du serveur Plug and Play du réseau à l'aide de l'option 43 DHCP. Pour plus d'informations sur cette option, reportez-vous à la section dédiée à la *fonction Plug and Play du réseau* dans le [Guide d'administration de Cisco Business Dashboard](#).
2. **DNS** : si l'appareil réseau ne récupère pas l'adresse du serveur via DHCP, il essaie de rechercher un nom d'hôte bien connu, `pnpserver`, dans le domaine local, par exemple, `pnpserver.example.com`. Vous pouvez configurer votre infrastructure DNS pour vous assurer que ce nom renvoie l'adresse du Cisco Business Dashboard.
3. **Plug and Play Connect** : Cisco propose un service de redirection, **Plug and Play Connect**, que l'appareil interroge s'il ne trouve pas l'adresse du serveur d'une autre manière. Pour configurer le service de redirection pour votre réseau, consultez la section dédiée à la fonction [Plug & Play Connect](#).

### Enregistrer les appareils

Pour enregistrer des appareils sur le point d'être installés, procédez comme suit :

1. Accédez à **Fonction Plug and Play du réseau > Appareils compatibles**.
2. Cliquez sur l'icône **+** (plus).
3. Saisissez le nom, l'ID de produit (PID) et le numéro de série de l'appareil à enregistrer, puis sélectionnez une organisation, un réseau, un groupe d'appareils et un type d'appareil dans les listes déroulantes.
4. Vous pouvez sélectionner une image de microprogramme et/ou un fichier de configuration à utiliser pour cet appareil. Si vous choisissez Image par défaut, l'appareil utilise l'image désignée comme image par défaut pour ce type d'appareil lorsqu'il se connecte au serveur.
5. Cliquez sur **Enregistrer**.

### Demander automatiquement les appareils

Un appareil qui se connecte au serveur et qui ne figure pas dans l'inventaire est considéré comme non demandé. Vous pouvez demander automatiquement les appareils non demandés et les provisionner via le serveur en créant une règle de demande automatique pour cet ID de produit. Pour créer une règle de demande automatique, procédez comme suit :

1. Accédez à **Plug and Play du réseau > Demander automatiquement les appareils**.

## REVIEW DRAFT - CISCO CONFIDENTIAL

2. Cliquez sur l'icône **+** (plus).
3. Saisissez l'ID de produit (PID) pour demander automatiquement l'appareil, puis sélectionnez une organisation, un réseau, un groupe d'appareils et un type d'appareil dans les listes déroulantes.
4. Vous pouvez sélectionner une image de microprogramme et/ou un fichier de configuration à utiliser pour cet ID de produit. Si vous choisissez Image par défaut, les appareils demandés automatiquement utilisent l'image désignée comme image par défaut pour ce type d'appareil lorsqu'ils se connectent au serveur.
5. Cliquez sur **Enregistrer**.

## Configurer le réseau

Si vous installez un nouveau réseau, vous pouvez profiter de l'occasion pour réaliser sa configuration initiale. Vous pouvez par ailleurs modifier la configuration d'un réseau existant à ce moment-là.

### Mettre à jour le microprogramme des appareils (facultatif)

Le tableau de bord vous indique si des mises à jour du microprogramme sont disponibles pour les appareils de votre réseau. De plus, une icône **Mise à niveau du microprogramme** s'affiche pour les appareils concernés à plusieurs endroits de l'interface utilisateur.

Pour mettre à jour le microprogramme d'un seul appareil, procédez comme suit :

1. Cliquez sur l'appareil dans la carte **Topologie** afin d'afficher le panneau **Informations de base**.
2. Ouvrez le panneau **Actions** et cliquez sur le bouton **Mettre à niveau le microprogramme vers la dernière version**. Le tableau de bord télécharge le microprogramme nécessaire auprès de Cisco et applique la mise à jour à l'appareil. L'appareil redémarrera dans le cadre de ce processus.

Vous pouvez également mettre à niveau le microprogramme depuis votre PC en cliquant sur l'option **Mettre à niveau à partir de la version locale** et en indiquant l'image du microprogramme à charger.

3. Vous pouvez suivre la progression de la mise à niveau en cliquant sur l'icône **État de la tâche** en haut à droite de l'interface utilisateur.

Vous pouvez aussi mettre à niveau chaque appareil depuis la vue **Inventaire**. Pour plus d'informations, reportez-vous à la section *Afficher l'inventaire des appareils* du [Guide d'administration de Cisco Business Dashboard](#).

### Mise à jour du microprogramme pour le réseau

Si vous souhaitez mettre à niveau l'intégralité du réseau vers la dernière version du microprogramme disponible, procédez comme suit :

1. Ouvrez la **carte topologique** du réseau à mettre à jour.
2. Cliquez sur **Actions réseau** en haut de la page et sélectionnez l'option **Mise à niveau du microprogramme**. Le tableau de bord télécharge les fichiers nécessaires auprès de Cisco pour chaque appareil pour lequel une mise à jour existe, puis les applique à chaque appareil à tour de rôle. Chaque appareil redémarrera dans le cadre de ce processus.
3. Vous pouvez suivre la progression de la mise à niveau en cliquant sur l'icône **État de la tâche** en haut à droite de l'interface utilisateur.

## REVIEW DRAFT - CISCO CONFIDENTIAL

### Configurer les groupes d'appareils

Le tableau de bord utilise le concept de groupe d'appareils pour vous permettre d'appliquer une configuration à plusieurs appareils en même temps et de vérifier que les paramètres de configuration sont cohérents sur tout le réseau. Pour allouer des appareils à un groupe, procédez comme suit :

1. Accédez à **Administration > Groupes d'appareils**.
2. Cliquez sur l'icône **+** (plus) pour ajouter un nouveau groupe.
3. Spécifiez une organisation, un nom et une description pour le groupe d'appareils. Cliquez sur **Enregistrer**.
4. Pour ajouter des appareils au groupe d'appareils, cliquez sur l'icône **+** (plus) dans le tableau dédié aux **appareils**. Utilisez la zone de recherche pour trouver les appareils à ajouter au groupe. Sélectionnez un ou plusieurs appareils à ajouter au groupe. Chaque appareil ne peut être membre que d'un seul groupe. Si un appareil sélectionné appartient à un autre groupe, vous devez d'abord le supprimer de ce groupe. Si vous voulez supprimer un appareil d'un groupe, cliquez sur l'icône **Annuler** à côté de l'appareil. Ce dernier sera alors déplacé vers le groupe d'appareils **par défaut**. Les groupes peuvent contenir plusieurs types d'appareils.

### Création de profils de configuration

Le tableau de bord vous permet d'appliquer facilement une configuration commune à plusieurs appareils réseau. Vous pouvez utiliser l'**Assistant de configuration du réseau** pour créer des profils de configuration pour chaque section. Vous pouvez aussi créer des profils individuellement. Pour utiliser l'**Assistant de configuration du réseau**, procédez comme suit :

1. Accédez à **Configuration du réseau > Assistant**.
2. Saisissez un nom pour les profils de configuration à créer, puis sélectionnez une organisation et un ou plusieurs groupes d'appareils auxquels appliquer la configuration.
3. Cliquez sur **Next (Suivant)**.
4. Indiquez les paramètres d'heure de ce groupe. Un profil **Gestion du temps** contient les paramètres relatifs au fuseau horaire, à l'heure d'été et à NTP. Si vous ne voulez pas créer de profil **Gestion du temps** pour ce groupe, cliquez sur **Ignorer**, sinon cliquez sur **Suivant**.
5. Indiquez les **paramètres DNS** de ce groupe. Le profil **Résolutions DNS** contient les paramètres concernant le nom de domaine et les serveurs DNS à utiliser. Si vous ne voulez pas créer de profil Résolutions DNS pour ce groupe, cliquez sur **Ignorer**, sinon cliquez sur **Suivant**.
6. Indiquez les paramètres d'authentification de l'utilisateur pour ce groupe. Un profil **Authentification** contient les paramètres relatifs à la base de données d'utilisateurs locaux pour les appareils. Si vous ne voulez pas créer de **profil d'authentification** pour ce groupe, cliquez sur **Ignorer**, sinon cliquez sur **Suivant**.
7. Indiquez les LAN virtuels à créer pour ce groupe. Un profil de VLAN contient les informations relatives à un ou plusieurs VLAN. Si vous ne souhaitez pas créer de profil de VLAN, cliquez sur **Ignorer**. Pour ajouter plusieurs VLAN, cliquez sur **Ajouter** après chaque VLAN. Cliquez sur **Next (Suivant)**.
8. Indiquez les LAN sans fil à créer pour ce groupe. Un profil de LAN sans fil contient les informations relatives à un ou plusieurs SSID. Si vous ne souhaitez pas créer de profil LAN sans fil, cliquez sur **Ignorer**. Pour ajouter plusieurs SSID, cliquez sur **Ajouter** après chaque SSID. Cliquez sur **Next (Suivant)**.

## REVIEW DRAFT - CISCO CONFIDENTIAL

9. Vérifiez les paramètres de configuration que vous avez définis. Si vous voulez apporter des modifications, appuyez sur le bouton **Modifier** ou **Retour** pour revenir à l'écran approprié. Si vous êtes satisfait, cliquez sur **Fin** pour créer les profils et les appliquer aux appareils des groupes sélectionnés.
10. Vous pouvez suivre la progression de la configuration en cliquant sur l'icône **État de la tâche** en haut à droite de l'interface utilisateur.

### Sauvegarde des configurations de l'appareil

Le tableau de bord vous permet de sauvegarder les configurations de vos appareils réseau. Pour sauvegarder la configuration d'un seul appareil, procédez comme suit :

1. Cliquez sur l'appareil dans la carte **Topologie** afin d'afficher le panneau **Informations de base**.
2. Ouvrez le panneau **Actions** et cliquez sur le bouton **Sauvegarder les configurations**. Vous pouvez également ajouter un commentaire décrivant cette sauvegarde dans la fenêtre qui s'ouvre. Le **tableau de bord** copie la configuration de l'appareil.
3. Vous pouvez suivre la progression de la sauvegarde en cliquant sur l'icône **État de la tâche** en haut à droite de l'interface utilisateur.

Vous pouvez également sauvegarder chaque appareil individuellement en cliquant sur **Sauvegarder les configurations** dans la vue **Inventaire**.

Si vous voulez sauvegarder les configurations de tout le réseau, procédez comme suit :

1. Ouvrez la **carte topologique** du réseau à sauvegarder.
2. Cliquez sur **Actions** en haut de la page et sélectionnez l'option **Sauvegarder les configurations**. Vous pouvez également ajouter un commentaire décrivant cette sauvegarde dans la fenêtre qui s'ouvre. Le tableau de bord copie la configuration de chaque appareil.
3. Vous pouvez suivre la progression de la sauvegarde en cliquant sur l'icône **État de la tâche** en haut à droite de l'interface utilisateur.



## CHAPITRE 6

# Questions fréquentes

---

Ce chapitre répond aux questions fréquentes concernant les fonctionnalités de la solution de Cisco Business Dashboard et traite les problèmes que vous pouvez rencontrer. Les sections sont organisées selon les catégories suivantes :

- [Questions fréquentes d'ordre général, à la page 25](#)
- [Questions fréquentes sur la détection, à la page 25](#)
- [Questions fréquentes sur la configuration, à la page 26](#)
- [Questions fréquentes sur la sécurité, à la page 26](#)
- [Questions fréquentes sur l'accès à distance, à la page 29](#)
- [Questions fréquentes sur les mises à jour logicielles, à la page 30](#)

## Questions fréquentes d'ordre général

**Q.** Quelles sont les langues prises en charge par la solution de Cisco Business Dashboard ?

**A.** Cisco Business Dashboard est traduite dans les langues suivantes :

- Chinois
- Français
- Français
- Allemand
- Japonais
- Espagnol

## Questions fréquentes sur la détection

**Q.** Quels protocoles Cisco Business Dashboard utilise-t-il pour gérer mes appareils ?

**A.** Cisco Business Dashboard utilise divers protocoles pour détecter et gérer le réseau. Les protocoles qui seront utilisés pour un appareil particulier dépendent du type de terminal.

Les protocoles suivants peuvent être utilisés :

- Multicast DNS et DNS Service Discovery (soit *Bonjour*, consultez *RFC 6762 et 6763*)

## REVIEW DRAFT - CISCO CONFIDENTIAL

- Protocole CDP (Cisco Discovery Protocol)
- Protocole LLDP (Link Layer Discovery Protocol) (consultez *la spécification IEEE 802.1AB*)
- Protocole SNMP (Simple Network Management Protocol)
- RESTCONF (consultez <https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/>)
- API propriétaires de services web

**Q.** Comment Cisco Business Dashboard découvre-t-il mon réseau ?

**A.** Cisco Business Dashboard Probe crée la liste des appareils du réseau en écoutant les annonces CDP, LLDP et mDNS. Elle se connecte ensuite à chaque appareil via un protocole pris en charge et recueille des informations complémentaires, comme les tables de contiguïté CDP et LLDP, les tables d'adresses MAC et les listes d'appareils associés. Ces informations permettent d'identifier les autres appareils du réseau et le processus se répète jusqu'à ce que tous les appareils soient détectés.

**Q.** Cisco Business Dashboard analyse-t-il le réseau ?

**A.** Cisco Business Dashboard n'analyse pas activement le réseau. La sonde utilise le protocole ARP pour analyser le sous-réseau IP auquel elle est directement rattachée, mais n'essaie pas d'analyser d'autres plages d'adresses. La sonde teste également chaque appareil détecté pour confirmer la présence d'un serveur web et du serveur SNMP sur les ports standard.

## Questions fréquentes sur la configuration

**Q.** Que se passe-t-il si un nouvel appareil est détecté ? Sa configuration sera-t-elle modifiée ?

**A.** Les nouveaux appareils seront ajoutés au groupe d'appareils par défaut. Si des profils de configuration ont été attribués au groupe d'appareils par défaut, cette configuration sera alors appliquée aux appareils qui viennent d'être détectés.

**Q.** Que se passe-t-il si je déplace un appareil d'un groupe d'appareils vers un autre ?

**A.** Les configurations des réseaux locaux virtuels ou sans fil associées aux profils appliqués au groupe d'appareils d'origine, mais qui ne sont pas également appliquées au nouveau groupe d'appareils seront supprimées. Par ailleurs, les configurations des réseaux locaux virtuels ou sans fil associées aux profils appliqués au nouveau groupe, mais qui ne sont pas appliquées au groupe d'origine seront ajoutées à l'appareil. Les paramètres de configuration du système seront remplacés par les profils appliqués au nouveau groupe. Si aucun profil de configuration du système n'est défini pour le nouveau groupe, la configuration système de l'appareil ne changera pas.

## Questions fréquentes sur la sécurité

**Q.** Quelles plages de ports et quels protocoles sont indispensables à Cisco Business Dashboard ?

**A.** Le tableau suivant dresse la liste des protocoles et des ports utilisés par le Cisco Business Dashboard :



**REVIEW DRAFT - CISCO CONFIDENTIAL**

**Tableau 1 : Cisco Business Dashboard – Protocoles et ports**

Port	Direction	Protocole	Utilisation
TCP 22	Entrant	SSH	Accès au tableau de bord via la ligne de commande. SSH est désactivé par défaut sur l'image de machine virtuelle Cisco.
TCP 80	Entrant	HTTP	Accès au tableau de bord en ligne. Redirection vers un serveur web sécurisé (port 443).
TCP 443	Entrant	HTTPS Multiplexage TCP	Accès web sécurisé au tableau de bord Communication entre la sonde et le tableau de bord.
TCP 50000 - 51000	Entrant	HTTPS	Accès à distance aux appareils.
UDP 53	Sortant	DNS	Résolution des noms de domaine.
UDP 123	Sortant	NTP	Synchronisation du temps.
TCP 443	Sortant	HTTPS	Accès aux services web Cisco pour plus d'informations comme les mises à jour logicielles, l'état de l'assistance et les avis de fin de vie. Accès aux services de mise à jour du système d'exploitation et des applications.
UDP 5353	Sortant	mDNS	Les annonces de service Multicast DNS au réseau local qui notifient le tableau de bord.

- Q.** Quelles plages de ports et quels protocoles sont indispensables à Cisco Business Dashboard Probe ?
- A.** Le tableau suivant dresse la liste des protocoles et des ports utilisés par le Cisco Business Dashboard Probe :

**Tableau 2 : Cisco Business Dashboard – Protocoles et ports**

Port	Direction	Protocole	Utilisation
TCP 22	Entrant	SSH	Accès à la sonde via la ligne de commande. SSH est désactivé par défaut sur l'image de machine virtuelle Cisco.
TCP 80	Entrant	HTTP	Accès à la sonde en ligne. Redirection vers un serveur web sécurisé (port 443).
TCP 443	Entrant	HTTPS	Accès web sécurisé à la sonde.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

Port	Direction	Protocole	Utilisation
UDP 5353	Entrant	mDNS	Les annonces de service Multicast DNS du réseau local. Utilisées pour la détection des appareils.
UDP 53	Sortant	DNS	Résolution des noms de domaine.
UDP 123	Sortant	NTP	Synchronisation du temps
TCP 80	Sortant	HTTP	Gestion des appareils sans activer les services web sécurisés.
UDP 161	Sortant	SNMP	Gestion des appareils réseau.
TCP 443	Sortant	HTTPS Multiplexage TCP	Gestion des appareils avec activation des services web sécurisés. Accès aux services web Cisco pour plus d'informations comme les mises à jour logicielles, l'état de l'assistance et les avis de fin de vie.  Accès aux services de mise à jour du système d'exploitation et des applications.  Communication entre la sonde et le tableau de bord.
UDP 5353	Sortant	mDNS	Les annonces de service Multicast DNS au réseau local qui notifient la sonde.

- Q.** Quel est le niveau de protection de la communication entre Cisco Business Dashboard et une sonde ?
- A.** Toutes les communications entre le tableau de bord et la sonde sont chiffrées en utilisant une session TLS 1.2 authentifiée avec des certificats client et serveur. La session est initiée par la sonde en direction du tableau de bord. Lors de l'association initiale entre le tableau de bord et la sonde, l'utilisateur doit se connecter au tableau de bord via la sonde.
- Q.** Cisco Business Dashboard profite-t-il d'un accès à mes appareils via des « portes dérobées » ?
- A.** Non. Lorsque Cisco Business Dashboard détecte un appareil pris en charge, il tente d'y accéder en utilisant les informations d'identification d'usine par défaut de cet appareil, à savoir le nom d'utilisateur et le mot de passe : `cisco` ou la communauté SNMP : `public`. Si la configuration de l'appareil a été modifiée, l'utilisateur doit fournir les bonnes informations d'identification à Cisco Business Dashboard.
- Q.** Quel est le niveau de protection des informations d'identification stockées dans Cisco Business Dashboard ?
- A.** Les informations d'identification qui permettent d'accéder à Cisco Business Dashboard sont hachées de manière irréversible en utilisant l'algorithme SHA512. Les informations d'identification des appareils et

**REVIEW DRAFT - CISCO CONFIDENTIAL**

des autres services, comme **Cisco Active Advisor**, sont chiffrées de manière irréversible à l'aide de l'algorithme AES-128.

- Q.** Comment puis-je récupérer un mot de passe perdu de l'interface utilisateur web ?
- A.** Si vous avez perdu le mot de passe de tous les comptes d'administrateurs de l'interface utilisateur web, vous pouvez le récupérer en vous connectant à la console de la sonde et en exécutant l'outil **cbdprobe recoverpassword**, ou à celle du tableau de bord et en exécutant l'outil **cisco-business-dashboard recoverpassword**. Cet outil rétablit le mot de passe par défaut du compte Cisco ou, si le compte Cisco a été supprimé, il recrée le compte avec le mot de passe par défaut. Vous trouverez ci-dessous un exemple des commandes à fournir pour récupérer le mot de passe à l'aide de cet outil.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```

**Remarque**

Lors de l'utilisation du Cisco Business Dashboard pour AWS, le mot de passe correspond à l'ID d'instance AWS.

- Q.** Quel est le nom d'utilisateur et le mot de passe par défaut du chargeur d'amorçage de la machine virtuelle ?
- A.** Les informations d'identification par défaut du chargeur d'amorçage de la machine virtuelle sont les suivantes : nom d'utilisateur : **root** et mot de passe : **cisco**. Vous pouvez les modifier en exécutant l'outil **config\_vm** et en répondant « Oui » lorsque vous êtes invité à confirmer la modification du mot de passe du chargeur d'amorçage.

## Questions fréquentes sur l'accès à distance

- Q.** Lorsque je me connecte à l'interface d'administration d'un appareil depuis Cisco Business Dashboard, ma session est-elle sécurisée ?
- A.** Cisco Business Dashboard établit un tunnel entre l'appareil et l'utilisateur pour la session d'accès à distance. Le protocole utilisé entre la sonde et l'appareil dépend de la configuration de l'appareil, mais Cisco Business Dashboard ouvre toujours une session via un protocole sécurisé si disponible (par exemple, il privilégiera HTTPS à HTTP). Si l'utilisateur se connecte à l'appareil via le tableau de bord, la session transite par un tunnel chiffré entre le tableau de bord et la sonde, quels que soient les protocoles activés sur l'appareil. La connexion entre le navigateur web de l'utilisateur et le tableau de bord se fait toujours via HTTPS.
- Q.** Pourquoi ma session d'accès à distance avec un appareil se déconnecte-t-elle immédiatement dès que j'ouvre une session d'accès à distance sur un autre terminal ?
- A.** Lorsque vous accédez à un appareil via Cisco Business Dashboard, le navigateur considère que chaque connexion se trouve sur le même serveur web (le tableau de bord) et présente donc les cookies de chaque appareil à tous les autres terminaux. Si plusieurs appareils utilisent le même nom de cookie, il est fort probable que le cookie d'un appareil soit remplacé par un autre terminal. Cette situation est fréquente avec des cookies de session, où le cookie n'est valide que pour l'appareil visité en dernier. Tous les autres

**REVIEW DRAFT - CISCO CONFIDENTIAL**

terminaux qui utilisent le même nom de cookie considéreront le cookie comme étant non valide et vous déconnecteront de la session.

- Q.** Pourquoi ma session d'accès à distance échoue-t-elle en affichant une erreur de ce type ? **Erreur d'accès : entité à l'origine de la demande trop grande Le champ d'en-tête HTTP excède la taille prise en charge**
- A.** Après avoir créé plusieurs sessions d'accès à distance avec différents appareils, le navigateur aura stocké un très grand nombre de cookies pour le domaine du tableau de bord. Pour contourner ce problème, utilisez les contrôles du navigateur pour effacer les cookies du domaine, puis rechargez la page.

## Questions fréquentes sur les mises à jour logicielles

- Q.** Comment puis-je garder le système d'exploitation du tableau de bord à jour ?
- A.** Le tableau de bord utilise la distribution Ubuntu Linux comme système d'exploitation. Les packages et le noyau peuvent être mis à jour à l'aide des processus Ubuntu standard. Par exemple, pour réaliser une mise à jour manuelle, connectez-vous à la console comme un utilisateur cisco et saisissez les commandes `sudo apt-get update` et `sudo apt-get upgrade`. Vous ne devez pas mettre à niveau le système vers une nouvelle version Ubuntu, ni installer des packages autres que ceux inclus dans l'image de machine virtuelle fournie par Cisco, ni ceux installés dans le cadre d'une installation minimale Ubuntu.
- Q.** Comment puis-je mettre à jour Java dans le tableau de bord ?
- A.** Cisco Business Dashboard utilise les packages OpenJDK des référentiels Ubuntu. OpenJDK sera automatiquement mis à jour lors de la mise à jour du système d'exploitation principal.
- Q.** Comment puis-je garder le système d'exploitation de la sonde à jour ?
- A.** Cisco Business Dashboard utilise la distribution Ubuntu Linux comme système d'exploitation. Les packages et le noyau peuvent être mis à jour à l'aide des processus Ubuntu standard. Par exemple, pour réaliser une mise à jour manuelle, connectez-vous à la console comme un utilisateur cisco et saisissez les commandes `sudo apt-get update` et `sudo apt-get upgrade`. Vous ne devez pas mettre à niveau le système vers une nouvelle version Ubuntu, ni installer des packages autres que ceux inclus dans l'image de machine virtuelle fournie par Cisco, ni ceux installés dans le cadre d'une installation minimale Ubuntu.
- Q.** Comment puis-je garder le système d'exploitation de la sonde à jour lors de l'utilisation d'un Raspberry Pi ?
- A.** Vous pouvez mettre à jour les paquets et le noyau Raspbian à l'aide des processus standard utilisés pour les distributions Linux basées sur Debian. Par exemple, pour réaliser une mise à jour manuelle, connectez-vous à la console comme un utilisateur cisco et saisissez les commandes `sudo apt-get update` et `sudo apt-get upgrade`. Le système ne doit pas être mis à niveau vers une nouvelle version majeure de Raspbian. Il est recommandé qu'aucun paquet supplémentaire ne soit installé au-delà de ceux installés dans le cadre de la version 'Lite' de la distribution Raspbian et de ceux qui sont ajoutés par l'installateur de sonde.