

Configuration de l'authentification des médias sociaux sur les périphériques WAP571 et WAP571E

Objectif

Les utilisateurs du réseau se connectent souvent à un point d'accès sans fil pour bénéficier de débits Internet plus rapides que le service de leur opérateur mobile. Un processus de connexion fluide et une navigation facile peuvent garantir une expérience positive pour ces utilisateurs. Vous pouvez configurer votre WAP571 ou WAP571E pour qu'il dispose d'options simples de connexion utilisateur tout en préservant la sécurité de votre réseau. L'authentification tierce via Google ou Facebook est une fonctionnalité disponible avec cette dernière mise à jour. Cet article vous guide dans la configuration de l'authentification tierce sur un point d'accès WAP571 ou WAP71E. Lorsqu'il est utilisé, le compte ^{tiers} de l'utilisateur agit comme un type de « passeport », accordant à l'utilisateur l'accès à votre réseau sans fil. Que vous teniez un café ou un bureau immobilier, les visiteurs pourront accéder facilement à votre réseau et bénéficier d'une expérience exceptionnelle.

Périphériques / Version logicielle

- WAP571 - 1.0.2.6
- WAP571E - 1.0.2.6

Exigences

- Accès Internet aux serveurs d'authentification Facebook ou Google
- Les utilisateurs doivent disposer d'un compte et d'une préférence pour utiliser Google ou Facebook pour accéder aux services réseau

Introduction

Dans ce guide en plusieurs étapes, vous effectuerez de courtes étapes à travers plusieurs emplacements de menu dans l'interface d'administration. Une fois que vous vous connectez à votre appareil, les sections que nous allons utiliser sont toutes contenues dans le menu *Captive Portal* sur le côté gauche de l'écran. Ce guide présente deux fonctionnalités facultatives, notamment la possibilité de personnaliser l'apparence du portail Web et d'afficher les clients connectés. Pour terminer ce guide, nous aborderons quelques notions de base sur la personnalisation du « visage » de votre réseau pour ces utilisateurs, ainsi que la méthode d'affichage des utilisateurs authentifiés.

Configuration globale

Étape 1. Cliquez sur **Captive Portal** dans la barre de menus située sur le côté gauche de l'écran. Par défaut, le navigateur vous dirige vers la configuration globale.



Étape 2. Cochez la case **Enable** en haut du menu.

A screenshot of the 'Global Configuration' page for Captive Portal. The 'Captive Portal Mode' is set to 'Enable' with a checked checkbox, highlighted by a red rectangle. Below this are three input fields: 'Authentication Timeout' (3600), 'Additional HTTP Port' (0), and 'Additional HTTPS Port' (0). Each field has a range and default value in parentheses. At the bottom, there is a 'Save' button and a section for 'Captive Portal Configuration Counters' showing Instance Count: 1, Group Count: 1, and User Count: 0.

Étape 3 : configuration du délai d'authentification et du port HTTP/S supplémentaire Ces options ouvrent des ports supplémentaires au cas où votre réseau les obligerait à accéder à des services. Dans notre cas, nous avons laissé ces options à leurs valeurs par défaut.

Étape 4. Cliquez sur le bouton **Enregistrer**.

Global Configuration

Captive Portal Mode: Enable

Authentication Timeout: Sec (Range: 60 - 3600, Default: 3600)

Additional HTTP Port: (Range:1025-65535 or 80, 0 = Disable, Default: 0)

Additional HTTPS Port: (Range:1025-65535 or 443, 0 = Disable, Default: 0)

Captive Portal Configuration Counters

Instance Count:	1
Group Count:	1
User Count:	0

Groupes/utilisateurs locaux

Cette section gère les paramètres appliqués aux groupes d'utilisateurs en fonction de votre saisie. En d'autres termes, il agit comme un entonnoir pour n'importe quel utilisateur se connectant au réseau, les dirigeant vers l'instance de portail captif de notre choix.

Étape 1. Dans le menu *Captive Portal*, cliquez sur **Local Groups Users**.



Étape 2. Assurez-vous que l'option **Create** est affichée dans la zone déroulante *Captive Portal Groups*.

Local Groups/Users

Local Groups Settings

Captive Portal Groups: ▼

Group Name: (Range: 1 - 32 Characters)

Local Users Settings

Captive Portal Users: ▼

User Name: (Range: 1 - 32 Characters)

Étape 3. Nommez ensuite le **groupe d'utilisateurs**. Dans notre cas, nous avons nommé le *groupe local* « Social_Media_Passport ».

Local Groups/Users

Local Groups Settings

Captive Portal Groups: ▼

Group Name: (Range: 1 - 32 Characters)

Local Users Settings

Captive Portal Users: ▼

User Name: (Range: 1 - 32 Characters)

Étape 4. Cliquez sur le bouton **Add Group**.

Local Groups/Users

Local Groups Settings

Captive Portal Groups:

Group Name: (Range: 1 - 32 Characters)

Local Users Settings

Captive Portal Users:

User Name: (Range: 1 - 32 Characters)

Configuration d'instance

Une instance peut être considérée comme un système unique autour d'un groupe de paramètres appliqués à la demande. Ainsi, un ensemble d'utilisateurs peut être servi à une instance tandis qu'un autre est servi à une instance différente.

Étape 1. Dans le menu *Captive Portal*, cliquez sur **Instance Configuration**.

- ▶ SNMP
- ▼ **Captive Portal**
 - Global Configuration
 - Local Groups/Users
 -
 - Instance Association
 - Web Portal Customization
 - Authenticated Clients
- ▶ Single Point Setup

Étape 2. Assurez-vous que **Create** figure dans la liste déroulante *Captive Portal Instances*.

Instance Configuration

Captive Portal Instances:

Captive Portal Instance Parameters

Instance Name: (Range: 1 - 32 Characters)

Étape 3. **Nommez l'instance**, qui contient entre 1 et 32 caractères alphanumériques.

Instance Configuration

Captive Portal Instances:

Captive Portal Instance Parameters

Instance Name: (Range: 1 - 32 Characters)

Étape 4. Cliquez sur le bouton **Enregistrer**.

Instance Configuration

Captive Portal Instances:

Captive Portal Instance Parameters

Instance Name: (Range: 1 - 32 Characters)

La page sera actualisée et de nouvelles options seront disponibles, comme indiqué ci-dessous.

Instance Configuration

Captive Portal Instances:

Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode: Enable

Protocol:

Verification:

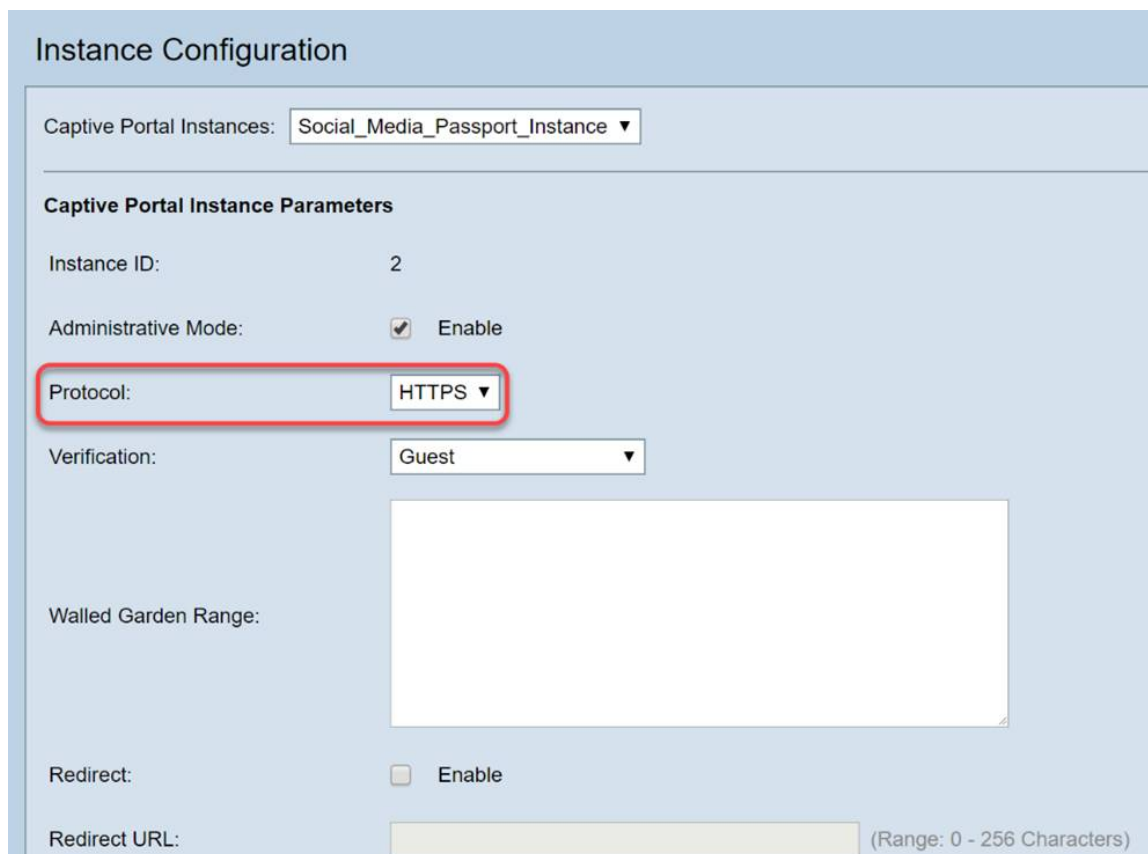
Walled Garden Range:

Redirect: Enable

Redirect URL: (Range: 0 - 256 Characters)

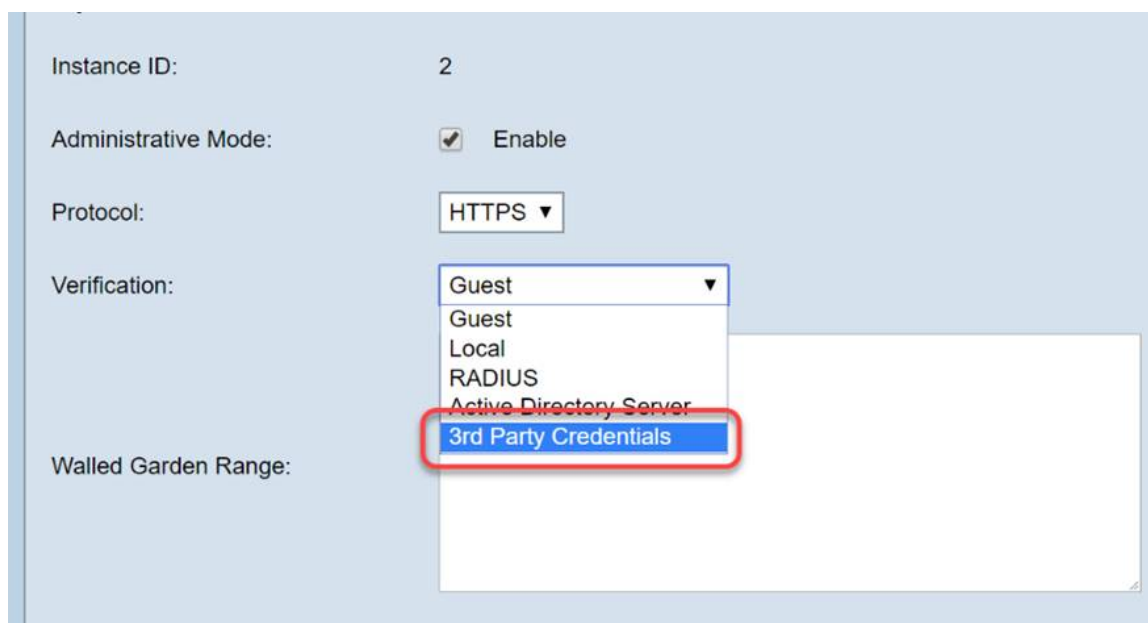
Away Timeout: (Range: 0 - 1440 Min, Default: 60)

Étape 5. (Facultatif) Cliquez sur la liste déroulante Protocol et sélectionnez HTTPS.



The screenshot shows the 'Instance Configuration' page. At the top, 'Captive Portal Instances:' is set to 'Social_Media_Passport_Instance'. Under 'Captive Portal Instance Parameters', 'Instance ID:' is 2, 'Administrative Mode:' is checked and 'Enable', and 'Protocol:' is set to 'HTTPS' (highlighted with a red box). 'Verification:' is set to 'Guest'. Below this is a large empty text area for 'Walled Garden Range:'. 'Redirect:' is unchecked. 'Redirect URL:' is an empty field with '(Range: 0 - 256 Characters)' next to it.

Étape 6. Cliquez sur la liste déroulante Vérification, puis sélectionnez 3rd Party Credentials.



This screenshot is a closer view of the 'Verification:' dropdown menu. The menu is open, showing options: 'Guest', 'Local', 'RADIUS', 'Active Directory Server', and '3rd Party Credentials'. The '3rd Party Credentials' option is highlighted with a blue background and a red box. The other options are in white text on a light blue background.

Pour plus d'informations sur la méthode d'authentification, consultez le tableau ci-dessous.

Méthode d'authentification	Détails
Base de données locale	Utilise la mémoire embarquée du périphérique pour conserver un enregistrement des utilisateurs attendus et des critères de participation au réseau.
Serveur Radius	Contrairement à local, un serveur d'authentification utilisant le protocole RADIUS et est distant du périphérique.
Service Active Directory	Comme pour RADIUS, les services Active Directory sont distants du périphérique.
Identifiants de tiers	Utilise un compte de médias sociaux pour vérifier l'identité et fournir un accès au réseau.

Étape 7. Sélectionnez les services tiers que vous souhaitez utiliser en cochant leurs cases.

Verification: 3rd Party Credentials ▼

Social Login Method: Facebook Google

Walled Garden Range:

- www.msftconnecttest.com,
- facebook.com,
- facebook.net,
- fbcdn.net,
- googleapis.com,
- apis.google.com,
- accounts.google.com,
- googleusercontent.com,
- ssl.gstatic.com,

Étape 8. Faites défiler la page vers le bas jusqu'à ce que vous voyiez *User Group Name*, puis cliquez sur la liste déroulante et sélectionnez le *User Group* créé dans la section précédente de ce guide.

Walled Garden Range:

- fbcdn.net,
- googleapis.com,
- apis.google.com,
- accounts.google.com,
- googleusercontent.com,
- ssl.gstatic.com,
- fonts.gstatic.com,

Redirect: Enable

Redirect URL: (Range: 0 - 256 Characters)

Away Timeout: (Range: 0 - 1440 Min, Default: 60)

Session Timeout: (Range: 0 - 1440 Min, Default: 0)

Maximum Bandwidth Upstream: (Range: 0 - 1300 Mbps, Default: 0)

Maximum Bandwidth Downstream: (Range: 0 - 1300 Mbps, Default: 0)

User Group Name: Social_Media_Passport ▼
Default

RADIUS IP Network: **Social_Media_Passport**

Global RADIUS: Enable

Étape 9. Faites maintenant défiler cette page jusqu'en bas et cliquez sur le bouton **Save**.

Key-3:

Key-4:

Locale Count: 0

Delete Instance:

Save

Association d'instance

Une fois l'instance créée, nous devons soit l'associer à un point d'accès virtuel (VAP), soit la conserver par défaut (VAP 0). Un VAP est une instance synthétique dupliquant l'apparence d'un point d'accès *supplémentaire* pour la connexion des utilisateurs.

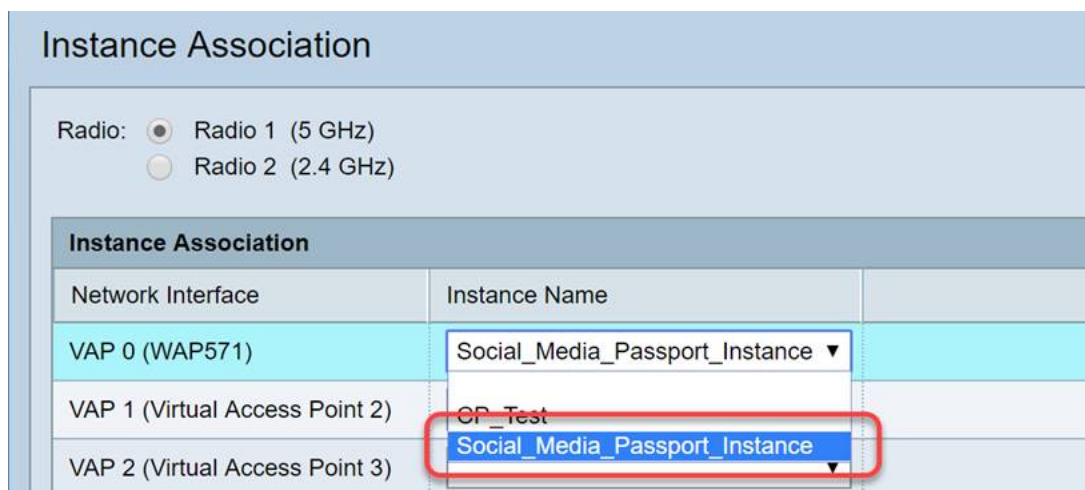
Étape 1. Dans le menu *Captive Portal*, cliquez sur **Instance Association**.



Étape 2. Sélectionnez la case d'option à laquelle vous souhaitez associer une instance. La page prend par défaut la valeur 5.



Étape 3. Cliquez sur la liste déroulante et sélectionnez l'instance que vous avez créée dans la dernière section.



Note: La plupart des utilisateurs devront définir le nom d'instance pour les bandes 5 GHz et 2,4 GHz. Répétez cette étape en cliquant sur la case d'option appropriée mise en surbrillance à l'étape 2.

Étape 4. Cliquez sur Enregistrer.

VAP 14 (Virtual Access Point 15)	<input type="text"/>
VAP 15 (Virtual Access Point 16)	<input type="text"/>

nc. All rights reserved.

Personnalisation du portail Web

Cette section vous permet de personnaliser le « visage » de votre nouveau portail captif. Vous pouvez ajouter et personnaliser le logo de votre entreprise et un accord utilisateur pour vous connecter au réseau.

Étape 1. Dans le menu *Captive Portal*, cliquez sur **Web Portal Customization**.

- ▶ SNMP
- ▼ **Captive Portal**
 - Global Configuration
 - Local Groups/Users
 - Instance Configuration
 - Instance Association
 - Web Portal Customization**
 - Authenticated Clients
- ▶ Single Point Setup

Étape 2. Dans la liste *Captive Portal Web Locale*, assurez-vous que **Create** figure dans la liste déroulante.

Web Portal Customization

Captive Portal Web Locale:

Captive Portal Web Locale Parameters

Web Locale Name: (Range: 1 - 32 Characters)

Captive Portal Instances:

Étape 3. Entrez un nom de paramètres régionaux Web, dans notre cas, nous avons choisi «

Social_Media_Web_Locale ».

Web Portal Customization

Captive Portal Web Locale:

Captive Portal Web Locale Parameters

Web Locale Name: (Range: 1 - 32 Characters)

Captive Portal Instances

Étape 4. Sélectionnez l'instance **Captive Portal** que vous avez créée précédemment.

Captive Portal Instances

- CP_Test
- CP_Test
- Social_Media_Passport_Instance**

Étape 5. Cliquez sur **Save**.

Captive Portal Instances

- CP_Test
- CP_Test
- Social_Media_Passport_Instance**

Comme la page *Instance Configuration*, la page sera actualisée et inclura désormais des points de personnalisation supplémentaires pour votre portail captif. Les options que vous pouvez modifier dans cette section sont nombreuses et explicites dans de nombreux cas.

Web Portal Customization

Captive Portal Web Locale:

Captive Portal Web Locale Parameters

Locale ID: 1

Instance Name: Social_Media_Passport_Instance

Background Image Name:

Logo Image Name:

Foreground Color: (Range: 1 - 32 Characters, Default: #999999)

Background Color: (Range: 1 - 32 Characters, Default: #BFBFBF)

Separator: (Range: 1 - 32 Characters, Default: #BFBFBF)

Locale Label: (Range: 1 - 32 Characters, Default: English)

Locale: (Range: 1 - 32 Characters, Default: en)

Account Image:

Note: Les couleurs sont représentées au format hexadécimal. [Si vous ne les connaissez pas, consultez cet article sur les couleurs Web.](#)

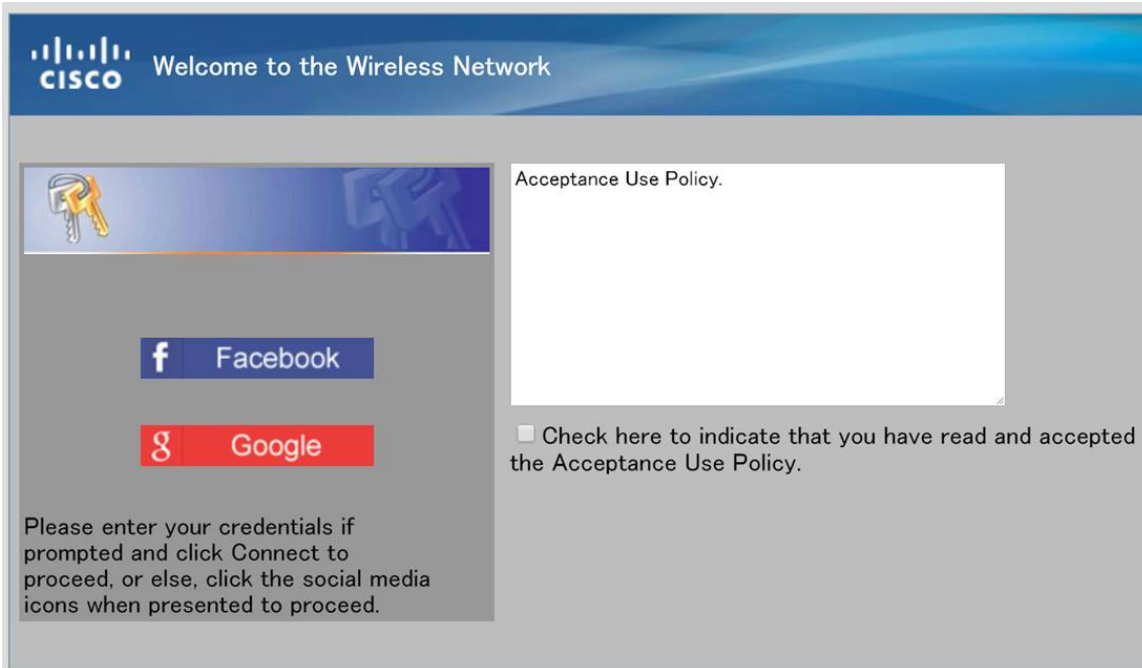
La personnalisation joue un rôle important dans la présentation. Voici quelques-unes des meilleures pratiques à personnaliser :

- Image De Fond
- Image du logo - Mieux si le logo a un arrière-plan transparent
- Couleur de premier plan/arrière-plan
- Politique d'utilisation

Il existe de nombreuses options pour modifier cette page. Prenez donc le temps de modifier ces paramètres.

Étape 6. Lorsque vous êtes satisfait de vos modifications, cliquez sur le bouton **Enregistrer**.

À partir de là, vous pouvez afficher un aperçu de ce que l'utilisateur verrait en cliquant sur le bouton Aperçu au bas de la page *Personnalisation du portail Web*. Voici un aperçu de ce que les utilisateurs verraient avec les options de connexion Google et Facebook en place sur un modèle par défaut.



Clients authentifiés

Lorsque les utilisateurs se sont connectés ou que l'authentification a échoué lors de la connexion à votre WLAN, ils sont détaillés dans cet écran. Pour afficher les invités connectés à votre WLAN, procédez comme suit.

Étape 1. Dans le menu *Captive Portal*, cliquez sur **Authenticated Clients**.



Étape 2. Vérifiez les informations contenues dans cet écran. La capture d'écran ci-dessous ne contient aucun client connecté ou rejeté. Si vous avez des utilisateurs authentifiés via une plateforme tierce, vous verrez des statistiques sur cette page.

Authenticated Clients													
Refresh													
Total Number of Authenticated Clients: 0													
Authenticated Clients													
MAC Address	IP Address	User Name	Protocol	Verification	VAP ID	Radio ID	Captive Portal ID	Session Timeout	Away Timeout	Received Packets	Transmitted Packets	Received Bytes	Transmitted Bytes
Total Number of Fail Authenticated Clients: 0													
Failed Authentication Clients													
MAC Address	IP Address	User Name	Verification	VAP ID	Radio ID	Captive Portal ID	Failure Time						

Conclusion

Bien joué, vous êtes prêt à offrir à vos invités une passerelle facile d'accès à votre réseau. Vous

avez également la possibilité de le personnaliser pour présenter votre marque aux nouveaux utilisateurs. Nous sommes ravis que vous utilisiez cette fonctionnalité et espérons que vous continuerez à construire votre réseau. Il existe encore d'autres fonctionnalités intéressantes pour vous aider à tirer le meilleur parti de votre matériel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.