

Configuration de l'Assistant de configuration sur le WAP561

Objectif

L'Assistant de configuration est un ensemble d'instructions interactives qui vous guide tout au long de la configuration initiale du WAP561. Ces instructions portent sur les configurations de base nécessaires au fonctionnement du WAP561. La fenêtre *Assistant Configuration du point d'accès* apparaît automatiquement la première fois que vous vous connectez au WAP, mais peut également être utilisée à tout moment. Cet article explique comment configurer le WAP561 à l'aide de l'Assistant de configuration.

Périphérique applicable

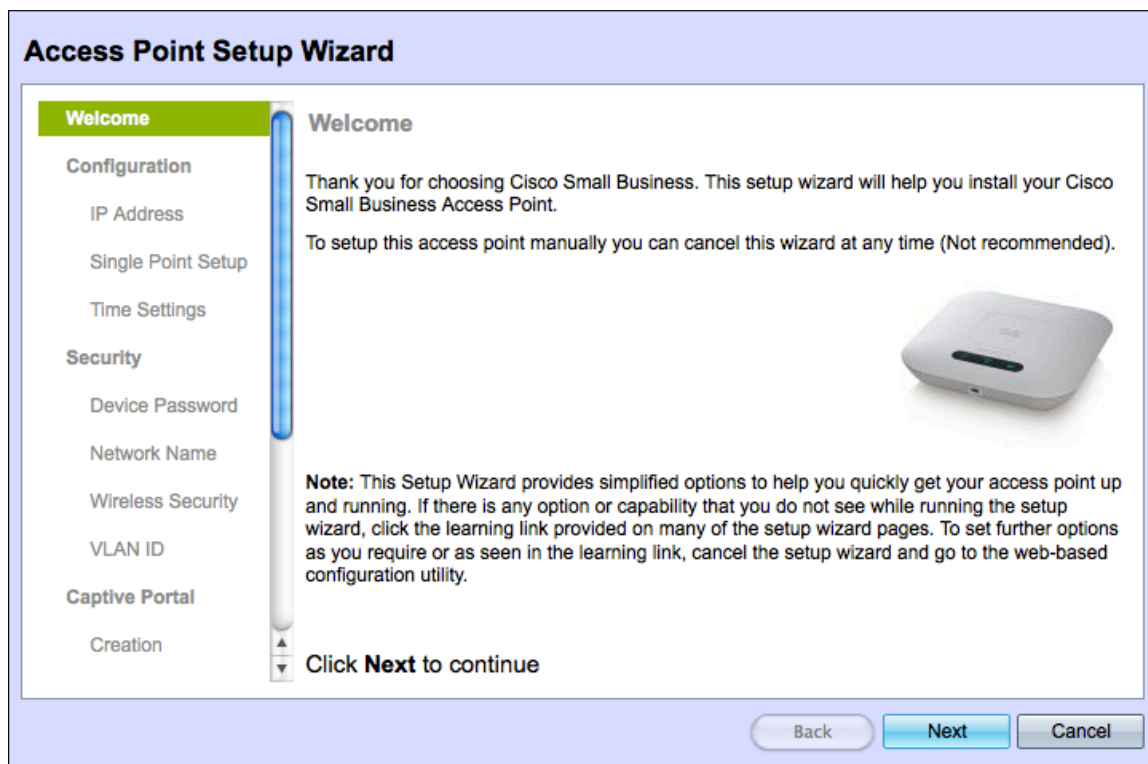
·WAP561

Version du logiciel

•v 1.0.4.2

Assistant Configuration

Étape 1. Connectez-vous à l'utilitaire de configuration Web et sélectionnez **Exécuter l'Assistant de configuration**. La fenêtre *Assistant Configuration du point d'accès* apparaît.



Étape 2. Cliquez sur **Next pour continuer**. La page *Configurer le périphérique - Adresse IP* s'ouvre :

Configure Device - IP Address

Select either Dynamic or Static IP address for your device.

Dynamic IP Address (DHCP) (Recommended)
 Static IP Address

Static IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

DNS: . . .

Secondary DNS (optional): . . .

[? Learn more about the different connection types](#)

Click **Next** to continue

Étape 3. Cliquez sur la case d'option qui correspond à la méthode que vous voulez utiliser pour déterminer l'adresse IP du WAP.

- Dynamic IP Address (DHCP) (Recommandé) : l'adresse IP du WAP est attribuée par un serveur DHCP. Si vous choisissez Dynamic IP Address (Adresse IP dynamique), passez à l'étape 9.

- Static IP Address : permet de créer une adresse IP fixe (statique) pour le WAP. Une adresse IP statique ne change pas.

Étape 4. Dans le champ *Adresse IP statique*, saisissez l'adresse IP du WAP. Cette adresse IP est créée par vous et ne doit pas être utilisée par un autre périphérique du réseau.

Étape 5. Dans le champ *Masque de sous-réseau*, saisissez le masque de sous-réseau de l'adresse IP.

Étape 6. Dans le champ *Default Gateway*, saisissez l'adresse IP de la passerelle par défaut pour le WAP. La passerelle par défaut est généralement l'adresse IP privée attribuée à votre routeur.

Étape 7. (Facultatif) Dans le champ *DNS*, saisissez l'adresse IP du système de noms de domaine principal (DNS). Si vous souhaitez accéder à des pages Web en dehors de votre réseau, l'adresse IP du serveur DNS doit être indiquée par votre fournisseur d'accès Internet (FAI).

Étape 8. (Facultatif) Dans le champ *Secondary DNS*, saisissez l'adresse IP du DNS secondaire.

Étape 9. Cliquez sur **Next pour continuer**. La page *Configuration par point unique - Définir un cluster* s'ouvre :

Single Point Setup – Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than as a series of separate wireless devices.

Create a New Cluster

Recommended for a new deployment environment.

New Cluster Name:

AP Location:

Join an Existing Cluster

Recommended for adding new wireless access points to the existing deployment environment.

Existing Cluster Name:

AP Location:

Do not Enable Single Point Setup

Recommended for single device deployments or if you prefer to configure each device individually.

Click **Next** to continue

Étape 10. Sélectionnez la case d'option correspondant aux paramètres de cluster que vous souhaitez utiliser. Un cluster vous permet de configurer plusieurs points d'accès (AP) en tant que périphérique unique. Si vous choisissez de ne pas utiliser de cluster, vous devez les configurer individuellement.

·Créer un nouveau cluster : créez un nouveau cluster pour les points d'accès.

·Joindre un cluster existant — Rejoint un cluster AP existant dans votre réseau.

·Ne pas activer la configuration par point unique — La configuration par point unique (cluster) n'est pas autorisée. Passez à l'étape 13 si vous avez choisi cette option.

Étape 11. Dans le champ *Nom du cluster*, saisissez un nom de cluster existant ou créez un nouveau nom de cluster en fonction de votre décision à l'étape 10.

Étape 12. Dans le champ *AP Location*, saisissez l'emplacement physique du WAP.

Remarque : si vous avez cliqué sur la case d'option **Joindre un cluster existant**, le WAP configure les autres paramètres en fonction du cluster. Lorsque vous cliquez sur Suivant, une page de confirmation vous demande si vous êtes sûr de vouloir rejoindre le cluster. Cliquez sur **Submit** pour rejoindre le cluster. Une fois la configuration terminée, cliquez sur **Terminer** pour quitter l'Assistant de configuration.

Étape 13. Cliquez sur **Next pour continuer**. La page *Configurer le périphérique - Définir la date et l'heure système* s'ouvre :

Configure Device - Set System Date And Time

Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

NTP Server:

[? Learn more about time settings](#)

Click **Next** to continue

Étape 14. Sélectionnez un fuseau horaire dans la liste déroulante Fuseau horaire.

Étape 15. Cliquez sur la case d'option qui correspond à la méthode que vous souhaitez utiliser pour définir l'heure du WAP.

·Network Time Protocol (NTP) : le WAP obtient l'heure à partir d'un serveur NTP.

·manuellement : l'heure est saisie manuellement dans le WAP. Si vous avez choisi manuellement, passez à l'étape 17.

Étape 16. Dans le champ *Serveur NTP*, saisissez le nom de domaine du serveur NTP qui fournit la date et l'heure. Passez à l'étape 19.

Configure Device - Set System Date And Time

Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

System Date:

System Time: :

[? Learn more about time settings](#)

Click **Next** to continue

Étape 17. Dans les listes déroulantes *Date système*, choisissez le mois, le jour et l'année respectivement.

Étape 18. Dans les listes déroulantes *Heure système*, sélectionnez respectivement l'heure et les minutes.

Étape 19. Cliquez sur **Next pour continuer**. La page *Activer la sécurité - Définir le mot de passe* s'ouvre :

Enable Security - Set Password


The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New Password:

Confirm Password:

Password Strength Meter:  Strong

Password Complexity: Enable

[? Learn more about passwords](#)

Click **Next** to continue

Étape 20. Dans le champ *Nouveau mot de passe*, saisissez un nouveau mot de passe requis pour l'accès administratif sur le WAP.

Étape 21. Dans le champ *Confirmer le mot de passe*, saisissez à nouveau le même mot de passe.

Note: Lorsque vous entrez un mot de passe, le nombre et la couleur des barres verticales changent pour indiquer la force du mot de passe, comme suit :

- rouge : le mot de passe ne répond pas aux exigences minimales de complexité.
- Orange : le mot de passe répond aux exigences minimales en matière de complexité, mais sa puissance est faible.
- Vert : le mot de passe est fort.

Étape 22. (Facultatif) Pour activer la complexité du mot de passe, cochez la case **Activer**. Pour cela, le mot de passe doit comporter au moins 8 caractères et être composé de lettres majuscules et minuscules et de chiffres/symboles.

Étape 23. Cliquez sur **Next pour continuer**. La page *Configure Radio 1 - Name Your Wireless Network* s'affiche. Le WAP561 contient deux radios. Chaque radio fonctionne comme un WAP indépendant et peut contenir 16 points d'accès virtuels. Dans la configuration initiale, vous ne créez qu'un seul point d'accès pour chaque radio.

Configure Radio 1 - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[? Learn more about network names](#)

Click **Next** to continue

Étape 24. Dans le champ *Network Name (SSID)*, saisissez le SSID (Service Set Identification) du réseau sans fil. Le SSID est le nom du réseau local sans fil.

Étape 25. Cliquez sur **Next pour continuer**. La page *Configurer Radio 1 - Sécuriser votre réseau sans fil* s'ouvre.

Configure Radio 1 - Secure Your Wireless Network

Select your network security strength.

- Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
- Better Security (WPA Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Enter a security key with 8-63 characters.

 Strong

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Étape 26. Sélectionnez la case d'option correspondant à la sécurité réseau que vous souhaitez appliquer à votre réseau sans fil.

·sécurité optimale (WPA2 Personal - AES) - WPA2 est la deuxième version de la technologie de sécurité WPA et de contrôle d'accès pour les réseaux sans fil Wi-Fi, qui inclut le cryptage AES-CCMP. Cette version de protocole fournit la meilleure sécurité selon la norme IEEE 802.11i. Toutes les stations clientes du réseau doivent pouvoir prendre en

charge WPA2. WPA2 n'autorise pas l'utilisation du protocole TKIP (Temporal Key Integrity Protocol) qui a des limitations connues.

·sécurité renforcée (WPA Personal - TKIP/AES) : WPA Personal est une norme Wi-Fi Alliance IEEE 802.11i, qui inclut le chiffrement AES-CCMP et TKIP. Il assure la sécurité lorsque des périphériques sans fil plus anciens prennent en charge le WPA d'origine mais ne prennent pas en charge le WPA2 plus récent.

·No Security : le réseau sans fil ne nécessite pas de mot de passe et est accessible à tous. Si vous avez sélectionné No Security (Aucune sécurité), passez à l'étape 29.

Étape 27. Dans le champ *Security Key*, saisissez le mot de passe de votre réseau.

Étape 28. (Facultatif) Pour afficher le mot de passe au fur et à mesure que vous tapez, cochez la case **Afficher la clé en texte clair**.

Étape 29. Cliquez sur **Next pour continuer**. La page *Configure Radio 1 - Assign The VLAN ID For Your Wireless Network* s'affiche.

Configure Radio 1 - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Étape 30. Dans le champ *VLAN ID*, saisissez le numéro d'ID du VLAN auquel vous souhaitez que le WAP appartienne.

Note: L'ID de VLAN doit correspondre à l'un des ID de VLAN pris en charge sur le port du périphérique distant connecté au WAP.

Étape 31. Cliquez sur **Next pour continuer**. La page *Configure Radio 2 - Name Your Wireless Network* s'affiche :

Configure Radio 2 - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[? Learn more about network names](#)

Click **Next** to continue

Étape 32. Dans le champ *Network Name (SSID)*, saisissez le SSID (Service Set Identification) du réseau sans fil.

Étape 33. Cliquez sur **Next pour continuer**. La page *Configurer Radio 2 - Sécuriser votre réseau sans fil* s'ouvre.

Configure Radio 2 - Secure Your Wireless Network

Select your network security strength.

- Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
- Better Security (WPA Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Enter a security key with 8-63 characters.

.....

 Strong

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Étape 34. Sélectionnez la case d'option correspondant à la sécurité réseau que vous souhaitez appliquer à votre réseau sans fil.

·sécurité optimale (WPA2 Personal - AES) : offre la meilleure sécurité et est recommandé si vos périphériques sans fil prennent en charge cette option.

·Meilleure sécurité : assure la sécurité lorsque des périphériques sans fil plus anciens ne

prennent pas en charge WPA2.

·No Security : le réseau sans fil ne nécessite pas de mot de passe et est accessible à tous. Si vous avez sélectionné No Security (Aucune sécurité), passez à l'étape 37.

Étape 35. Dans le champ *Security Key*, saisissez le mot de passe de votre réseau.

Étape 36. (Facultatif) Pour voir le mot de passe au fur et à mesure de votre saisie, cochez la case **Afficher la clé en texte clair** pour voir le mot de passe au fur et à mesure de votre saisie.

Étape 37. Cliquez sur **Next pour continuer**. La page *Configure Radio 2 - Assign The VLAN ID For Your Wireless Network* s'affiche.

Configure Radio 2 - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Étape 38. Dans le champ *VLAN ID*, saisissez le numéro d'ID du VLAN auquel vous souhaitez que le WAP appartienne.

Note: L'ID de VLAN doit correspondre à l'un des ID de VLAN pris en charge sur le port du périphérique distant connecté au WAP.

Étape 39. Cliquez sur **Next pour continuer**. La page *Enable Captive Portal - Create Your Guest Network* s'ouvre :

Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

- Yes
 No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Étape 40. Cliquez sur la case d'option **Oui** si vous souhaitez créer un réseau invité. Un réseau invité nécessite l'authentification des utilisateurs avant de pouvoir utiliser Internet. Aucun réseau invité n'est requis. Sinon, cliquez sur la case d'option **Pas** si vous ne voulez pas créer de réseau invité et passez à l'étape 54.

Étape 41. Cliquez sur **Next pour continuer**. La page *Enable Captive Portal - Name Your Guest Network* s'affiche :

Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Radio: Radio 1
 Radio 2

Guest Network name:
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Étape 42. Sélectionnez la case d'option correspondant à la radio dans laquelle vous souhaitez placer le réseau invité.

Étape 43. Dans le champ *Nom du réseau invité*, saisissez le SSID du réseau invité.

Étape 44. Cliquez sur **Next pour continuer**. La page *Enable Captive Portal - Secure Your Guest Network* s'affiche :

Enable Captive Portal - Secure Your Guest Network


Select your guest network security strength.

Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.

Better Security (WPA Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.

No Security (Not recommended)

Enter a security key with 8-63 characters.

 Strong

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Étape 45. Cochez la case d'option correspondant à la sécurité réseau que vous souhaitez appliquer à votre réseau invité.

·sécurité optimale (WPA2 Personal - AES) : offre la meilleure sécurité et est recommandé si vos périphériques sans fil prennent en charge cette option.

·Meilleure sécurité : assure la sécurité lorsque des périphériques sans fil plus anciens ne prennent pas en charge WPA2.

·No Security : le réseau sans fil ne nécessite pas de mot de passe et est accessible à tous. Si vous avez sélectionné No Security (Aucune sécurité), passez à l'étape 48.

Étape 46. Dans le champ *Security Key*, saisissez le mot de passe du réseau invité.

Étape 47. (Facultatif) Pour afficher le mot de passe au fur et à mesure que vous tapez, cochez la case **Afficher la clé en texte clair**.

Étape 48. Cliquez sur **Next pour continuer**. La page *Enable Captive Portal - Assign The VLAN ID* s'ouvre :

Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Étape 49. Dans le champ *VLAN ID*, saisissez le numéro d'ID du VLAN auquel vous souhaitez que le réseau invité appartienne.

Note: L'ID de VLAN doit correspondre à l'un des ID de VLAN pris en charge sur le port du périphérique distant connecté au WAP.

Étape 50. Cliquez sur **Next pour continuer**. La page *Enable Captive Portal - Enable Redirect URL* s'ouvre :

Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

[? Learn more about redirect urls](#)

Click **Next** to continue

Étape 51. (Facultatif) Pour rediriger les utilisateurs sans fil vers une page Web après s'être connectés au réseau invité, cochez la case **Activer l'URL de redirection**. Si vous ne cochez pas la case **Activer**, passez à l'étape 54.

Étape 52. Dans le champ *Rediriger l'URL*, saisissez la page Web vers laquelle vous souhaitez rediriger les utilisateurs une fois qu'ils se sont connectés au réseau invité.

Étape 53. Cliquez sur **Next pour continuer**. La page *Résumé - Confirmer vos paramètres* s'ouvre :

Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Radio 1

Network Name (SSID):	Network A
Network Security Type:	plain-text
Security Key:	
VLAN ID:	1

Radio 2

Network Name (SSID):	Network B
Network Security Type:	plain-text
Security Key:	
VLAN ID:	2

Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 2
----------------------	---------

Click **Submit** to enable settings on your Cisco Small Business Access Point

Back Submit Cancel


Étape 54. (Facultatif) Si vous souhaitez modifier un paramètre que vous avez défini, cliquez sur **Précédent**.

Étape 55. (Facultatif) Si vous souhaitez quitter l'Assistant de configuration et annuler toutes les modifications apportées, cliquez sur **Annuler**.

Étape 56. Examiner les paramètres réseau et réseau invité. Cliquez sur **Submit** pour activer les paramètres sur le WAP. Une barre de chargement apparaît lorsque le WAP active vos paramètres. Lorsque le WAP est terminé, la page *Terminer* s'ouvre :

Note: L'étape 56 ne s'applique que si vous cliquez sur **Soumettre** dans la page *Confirmer vos paramètres*.

Device Setup Complete

 Congratulations, your access point has been set up successfully. We strongly recommend that you save these settings by writing them down or by copying and pasting them into a text document. You will need these settings later when you add other wireless computers or devices to your network.

Cluster Name:	ciscosb-cluster
Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	



Note: To configure WPS, Click "Run WPS" on the Getting Started page, under Initial Setup.

Click **Finish** to close this wizard.

Back

Finish

Cancel

Étape 57. Cliquez sur **Terminer** pour quitter l'Assistant de configuration.