Configurer l'authentification invité Active Directory sur WAP125 ou WAP581

Objectif

L'authentification d'invité Active Directory (AD) permet à un client de configurer une infrastructure de portail captif pour utiliser son service Windows Directory interne pour l'authentification. Captive Portal est une fonctionnalité qui permet à un administrateur de bloquer les clients se connectant au réseau du point d'accès sans fil (WAP) jusqu'à ce qu'ils aient accès au réseau. Les clients sont dirigés vers une page Web pour l'authentification et les conditions d'accès avant de pouvoir se connecter au réseau. La vérification du portail captif est destinée aux invités et aux utilisateurs authentifiés du réseau. Cette fonctionnalité utilise le navigateur Web et le transforme en périphérique d'authentification.

Les instances de portail captif sont un ensemble défini de configurations utilisées pour authentifier les clients sur le réseau WAP. Les instances peuvent être configurées pour répondre de différentes manières aux utilisateurs lorsqu'ils tentent d'accéder aux points d'accès virtuels associés. Les portails captifs sont souvent utilisés dans les points d'accès Wi-Fi pour s'assurer que les utilisateurs acceptent les conditions générales et fournissent des informations de sécurité avant d'accéder à Internet.

Pour prendre en charge l'authentification AD, le WAP devra communiquer avec un à trois contrôleurs de domaine Windows pour fournir l'authentification. Il peut prendre en charge plusieurs domaines pour l'authentification en choisissant des contrôleurs de domaine de différents domaines AD.

L'objectif de ce document est de vous montrer comment configurer l'authentification d'invité AD sur WAP125 ou WAP581.

Périphériques pertinents

- WAP125
- WAP581

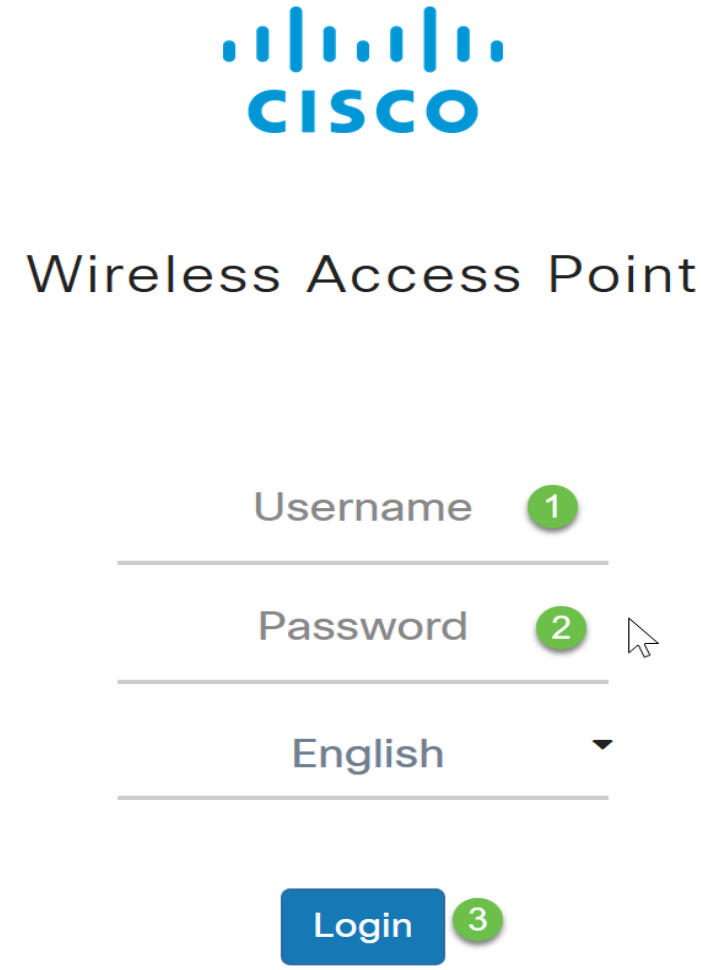
Version du logiciel

- 1.0.1

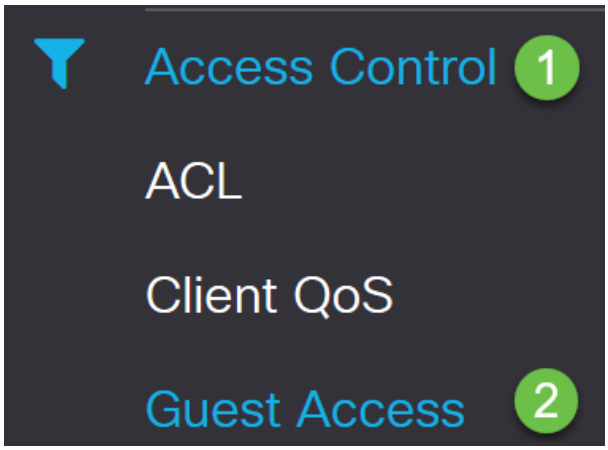
Configurer l'authentification d'invité Active Directory

Étape 1. Connectez-vous à l'utilitaire de configuration Web du WAP en entrant le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe par défaut sont cisco/cisco. Si vous avez configuré un nouveau nom d'utilisateur ou mot de passe, saisissez plutôt les informations d'identification. Cliquez sur **Connexion.**

NOTE: Dans cet article, le WAP125 est utilisé pour démontrer la configuration de l'authentification des invités AD. Les options de menu peuvent varier légèrement selon le modèle de votre périphérique.



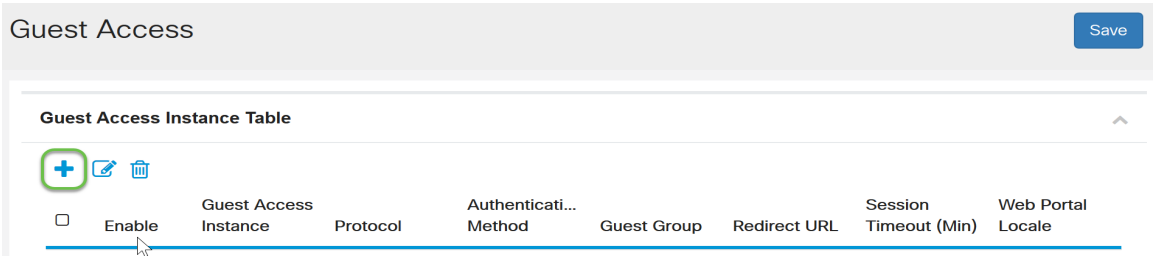
Étape 2. Choisissez **Access Control > Guest Access**.



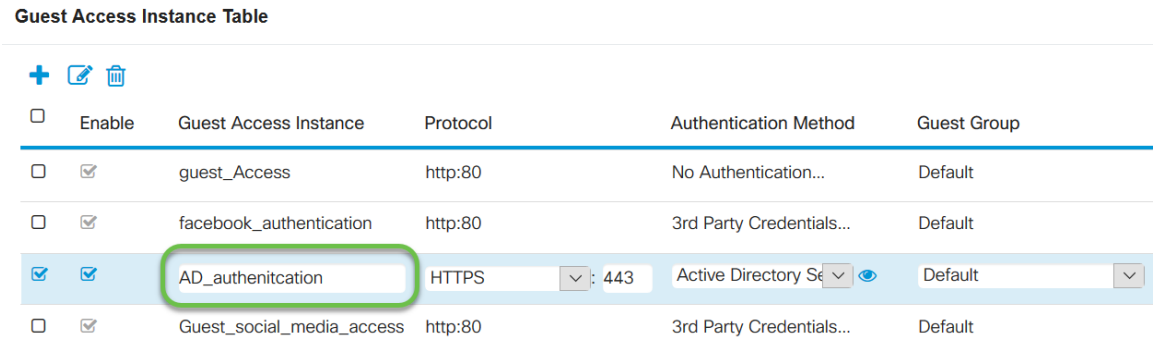
Étape 3. Dans le *tableau Instance d'accès invité*, vous pouvez ajouter une nouvelle *instance d'accès invité* ou modifier une instance existante. La fonctionnalité d'accès invité du point d'accès WAP125 ou WAP581 fournit une connectivité sans fil aux clients sans fil temporaires de la portée du périphérique. Il fonctionne en demandant au point d'accès de diffuser deux SSID différents : l'une pour le réseau principal et l'autre pour le réseau invité. Les invités sont ensuite redirigés vers un portail captif où ils doivent saisir leurs informations d'identification. En effet, le réseau principal reste sécurisé tout en permettant aux invités d'accéder à Internet.

Les paramètres du portail captif sont configurés dans la table d'instances d'accès invité de l'utilitaire Web du WAP. L'accès invité est particulièrement utile dans les halls d'hôtels et de bureaux, les restaurants et les centres commerciaux.

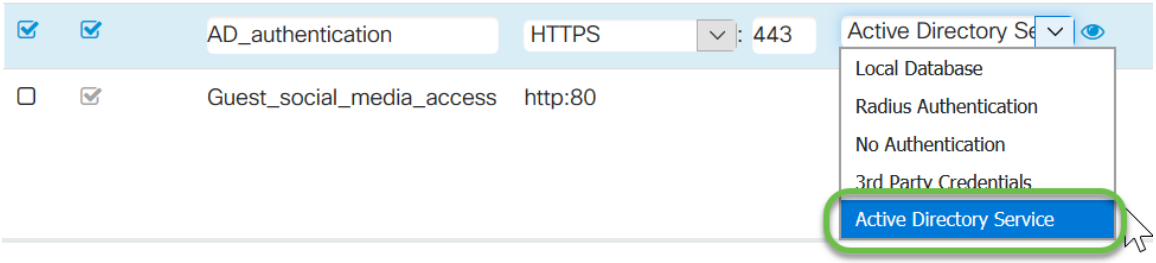
Dans cet exemple, une nouvelle *instance d'accès invité* est ajoutée en cliquant sur l'**icône plus**.



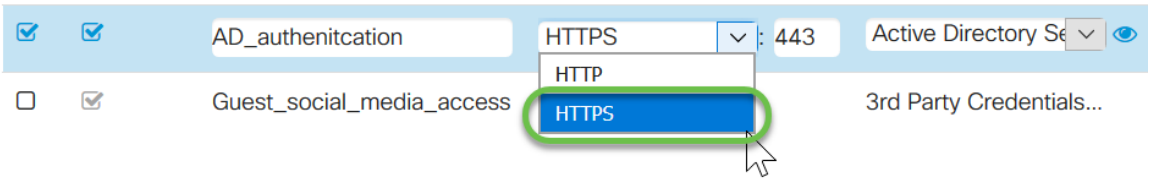
Étape 4. Nommez l'*instance d'accès invité*. Dans cet exemple, il s'appelle **AD_authentication**.



Étape 5. Sélectionnez la *méthode d'authentification* en tant que **service Active Directory**.

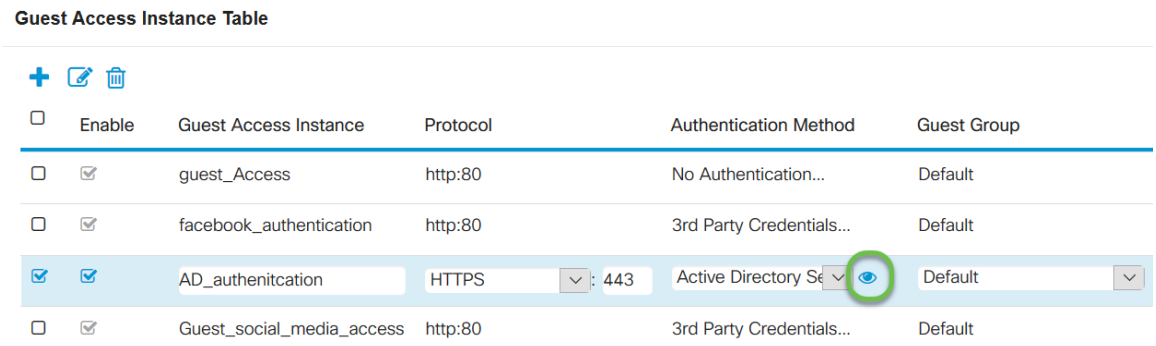


Étape 6. Une fois que vous avez choisi le service Active Directory comme *méthode d'authentification*, le protocole passe du protocole HTTP (Hyper Text Transfer Protocol) au protocole HTTPS (Hyper Text Transfer Protocol Secure).

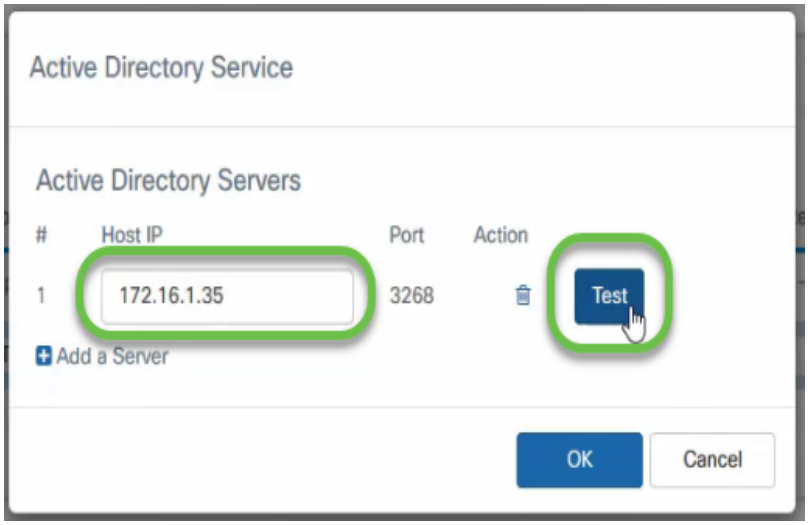


NOTE: Il est très important qu'un client configure la page du portail captif pour utiliser HTTPS et non HTTP, car le premier est plus sécurisé. Si un client choisit HTTP, il peut par inadvertance exposer des noms d'utilisateur et des mots de passe en les transmettant en texte clair non chiffré. Il est recommandé d'utiliser une page de portail HTTPS captive.

Étape 7. Configurez l'adresse IP du serveur AD en cliquant sur l'**icône en forme d'oeil bleu** en regard du service Active Directory dans la colonne *Authentication Method*.

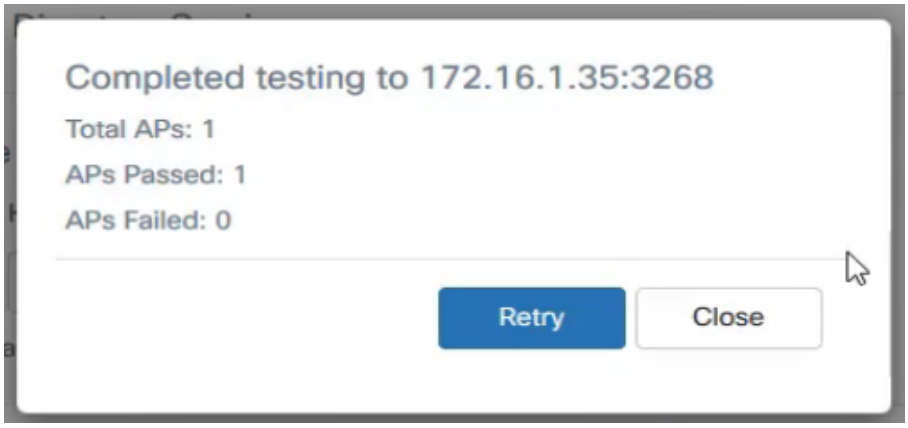


Étape 8. Une nouvelle fenêtre s'ouvrira. Saisissez l'adresse IP du serveur AD. Dans cet exemple, l'adresse IP de l'hôte utilisée est **172.16.1.35**. En option, vous pouvez cliquer sur **Test** pour vérifier sa validité.



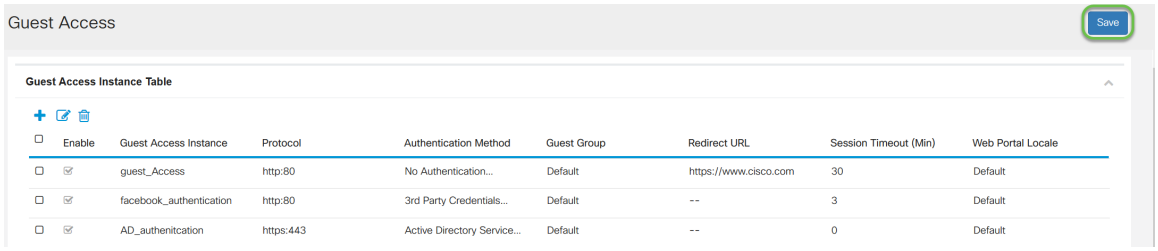
Étape 9. (Facultatif) Une fois que vous avez cliqué sur **Test** à l'étape précédente, une autre fenêtre contextuelle s'ouvre et vous pouvez entrer le *Nom d'utilisateur* et le *Mot* de passe de l'utilisateur dans AD et cliquer sur **Commencer le test**.

S'il est valide, il réussira le test et l'écran suivant s'affiche. Ceci confirme que vous pouvez vous connecter au contrôleur de domaine et vous authentifier.

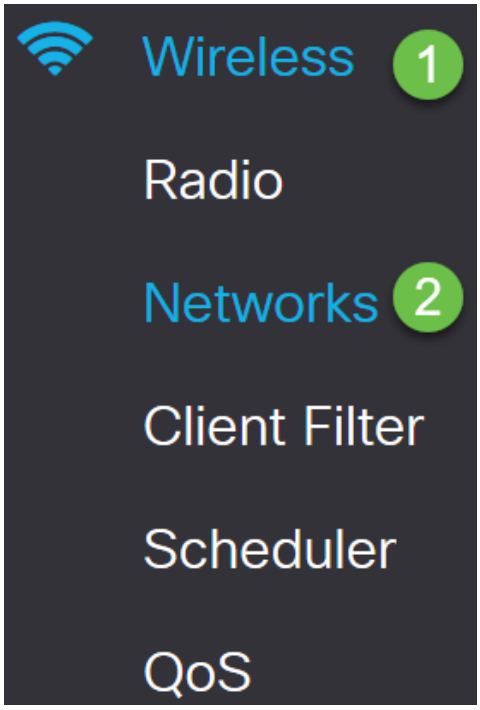


NOTE: Vous pouvez ajouter jusqu'à 3 serveurs AD.

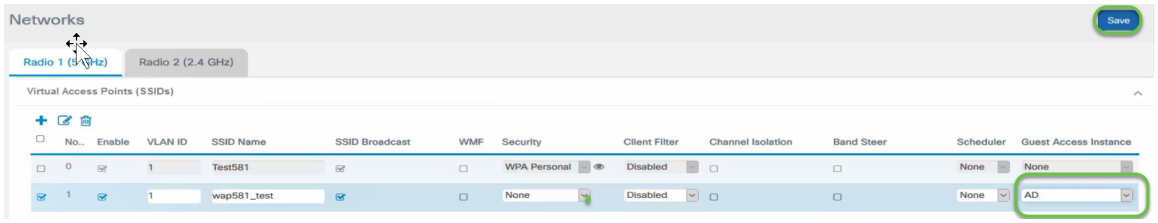
Étape 10. Enregistrez les modifications.



Étape 11. Accédez au menu et choisissez **Wireless > Networks**

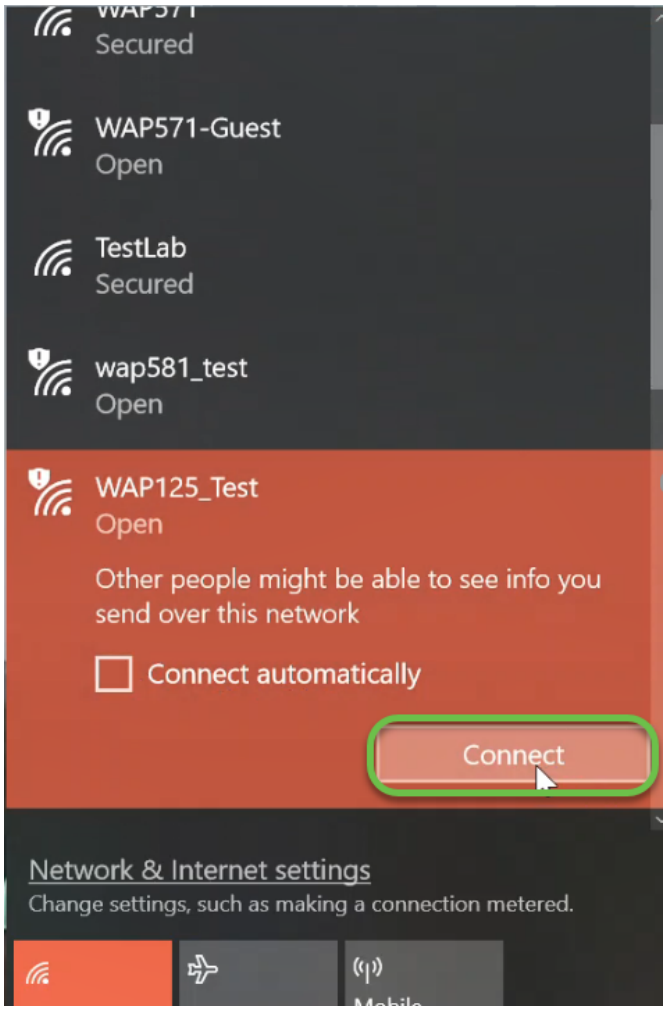


Étape 12. Choisissez le réseau et spécifiez qu'il choisira **AD** comme *instance d'accès invité* pour l'authentification. Click **Save.**

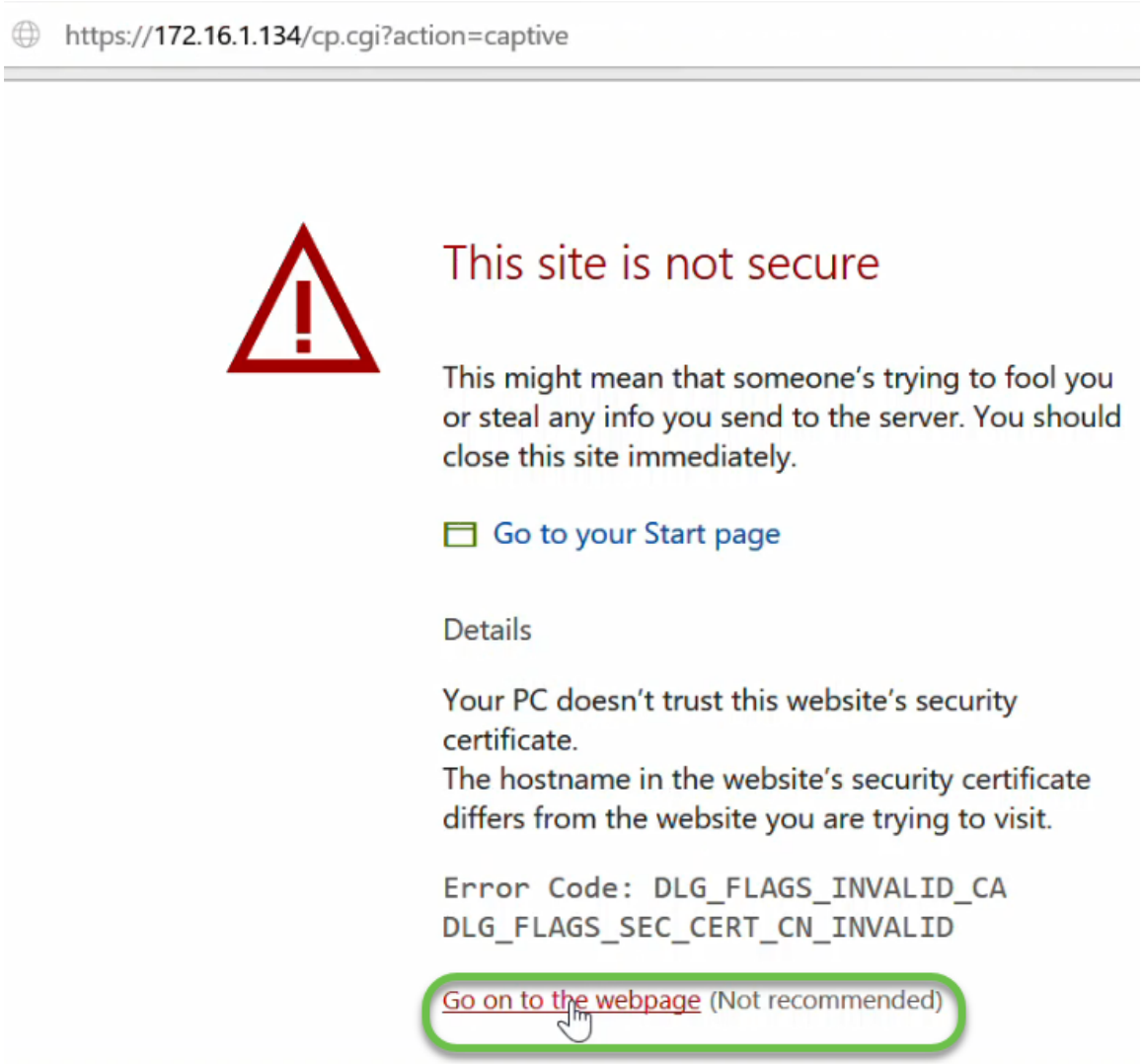


Étape 13. Pour vous connecter au réseau sans fil invité à l'aide de l'authentification AD,

sélectionnez l'option sans fil sur votre ordinateur personnel (PC) et sélectionnez le réseau configuré pour l'authentification AD, puis cliquez sur **Connect.**

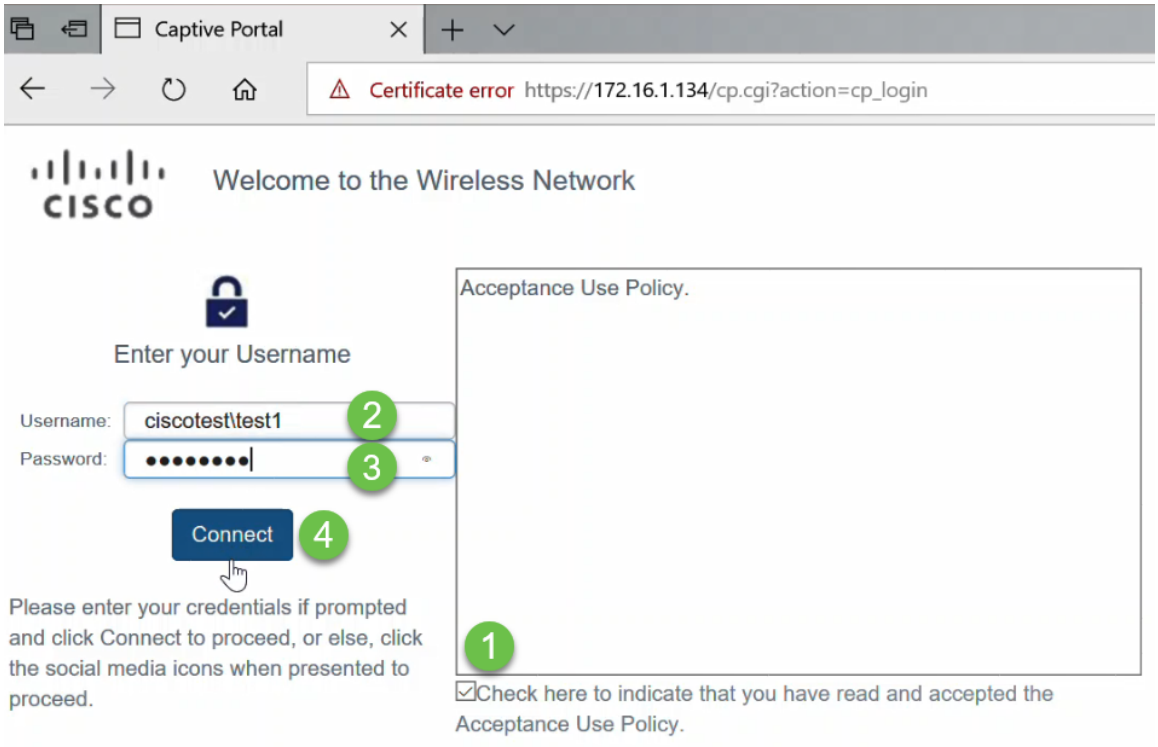


Étape 14. Une fois connecté, une fenêtre de navigateur Web s'ouvre avec l'avertissement de certificat de sécurité standard. Cliquez sur **Aller à la page Web**.



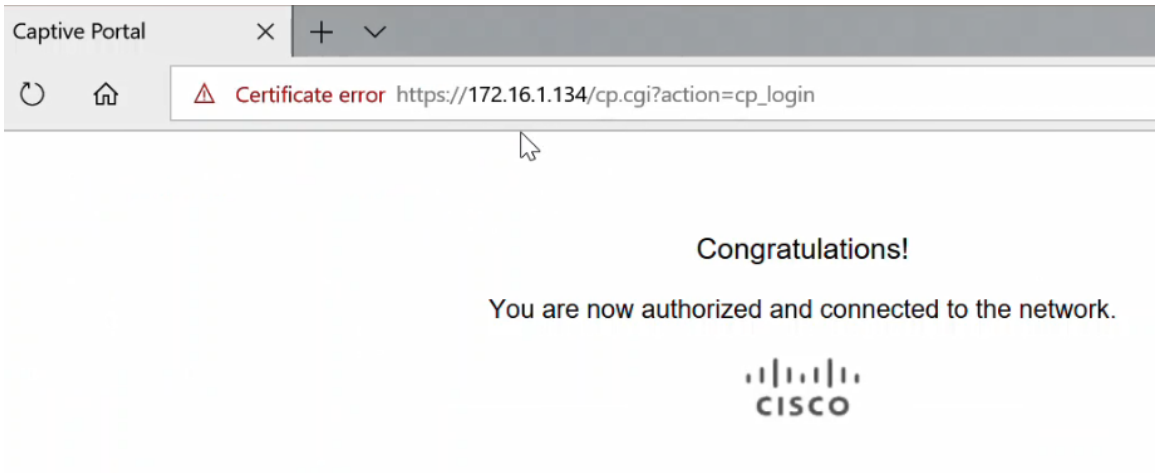
NOTE: L'écran peut apparaître différemment selon le navigateur que vous utilisez.

Étape 15. La page *Captive Portal* est lancée. Cochez la case Acceptance Use Policy pour accepter la stratégie et entrez le *nom d'utilisateur* et le *mot de passe* de l'utilisateur dans AD. Cliquez sur **Connect** pour vous connecter au réseau.



NOTE: S'il existe plusieurs domaines, le nom d'utilisateur inclut le nom de domaine\nom d'utilisateur. Dans cet exemple, il s'agit de ciscotest\test1.

Étape 16. Vous êtes maintenant authentifié et vous avez accès à Internet.



Conclusion

Vous devez maintenant avoir correctement configuré l'authentification d'invité Active Directory sur WAP125 ou WAP581 et vérifié sa fonctionnalité.