

Dépannage de l'authentification Web sur un contrôleur LAN sans fil (WLC)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Produits connexes](#)

[Authentification Web sur les WLC](#)

[Dépanner l'authentification Web](#)

[Informations connexes](#)

Introduction

Ce document décrit des conseils afin de dépanner les problèmes d'authentification Web dans un environnement de contrôleur de réseau local sans fil (WLC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôle et mise en service des points d'accès sans fil (CAPWAP).
- Comment configurer le point d'accès léger (LAP) et le WLC pour un fonctionnement de base.
- Connaissance de base de l'authentification Web et de la configuration de l'authentification Web sur les WLC.

Pour plus d'informations sur la façon de configurer l'authentification Web sur les WLC, référez-vous à [Exemple de configuration d'authentification Web du contrôleur LAN sans fil](#).

Composants utilisés

Les informations de ce document sont basées sur un WLC 5500 qui exécute la version 8.3.121 du microprogramme.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec ce matériel :


- Contrôleurs sans fil Cisco 5500
- Contrôleurs sans fil Cisco 8500
- Contrôleurs sans fil Cisco 2500
- Contrôleur de réseau local sans fil de la gamme Cisco Airespace 3500
- Contrôleur de réseau local sans fil de la gamme Cisco Airespace 4000
- Contrôleurs sans fil Cisco Flex 7500
- Module de services sans fil Cisco 2 (WiSM2)

Authentification Web sur les WLC

L'authentification Web est une fonctionnalité de sécurité de couche 3 qui empêche le contrôleur d'autoriser le trafic IP, à l'exception des paquets DHCP et des paquets DNS (Domain Name System), à partir d'un client particulier jusqu'à ce que ce client ait correctement fourni un nom d'utilisateur et un mot de passe valides, à l'exception du trafic autorisé via une liste de contrôle d'accès (ACL) de pré-authentification. L'authentification Web est la seule stratégie de sécurité qui permet au client d'obtenir une adresse IP avant l'authentification. Il s'agit d'une méthode d'authentification simple qui ne requiert aucun utilitaire demandeur ou client. L'authentification Web peut être faite localement sur un WLC ou via un serveur RADIUS. L'authentification Web est généralement utilisée par les clients qui veulent déployer un réseau d'accès invité.

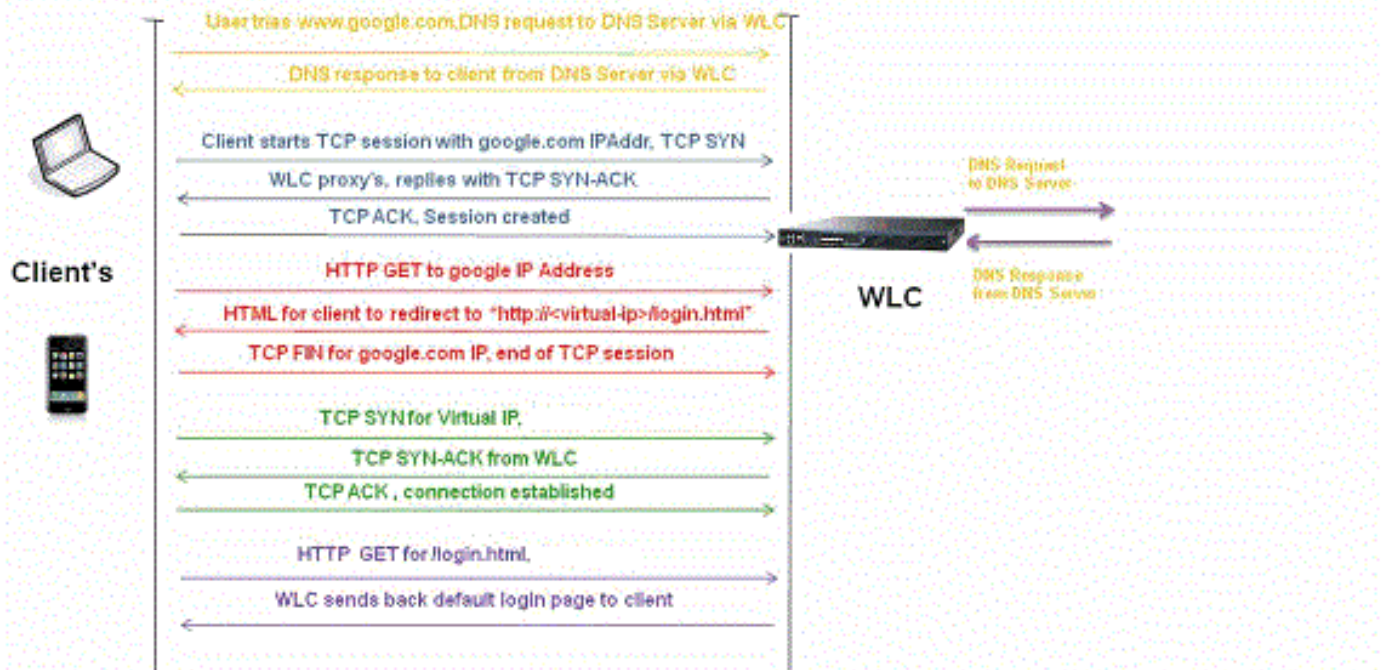
L'authentification Web démarre lorsque le contrôleur intercepte le premier paquet TCP HTTP (port 80) GET du client. Pour que le navigateur Web du client puisse atteindre ce niveau, il doit d'abord obtenir une adresse IP et traduire l'URL en adresse IP (résolution DNS) pour le navigateur Web. Cela permet au navigateur Web de savoir quelle adresse IP envoyer à HTTP GET.

Lorsque l'authentification Web est configurée sur le WLAN, le contrôleur bloque tout le trafic (jusqu'à ce que le processus d'authentification soit terminé) en provenance du client, à l'exception du trafic DHCP et DNS. Lorsque le client envoie le premier HTTP GET au port TCP 80, le contrôleur redirige le client vers <https://192.0.2.1/login.html> (s'il s'agit de l'adresse IP virtuelle configurée) pour traitement. Ce processus fait apparaître la page Web de connexion.

 Remarque : lorsque vous utilisez un serveur Web externe pour l'authentification Web, les plates-formes WLC ont besoin d'une ACL de pré-authentification pour le serveur Web externe.

Cette section explique en détail le processus de redirection de l'authentification Web.

Web-Auth Redirection Process



- Vous ouvrez le navigateur Web et tapez une URL, par exemple, `http://www.example.com`. Le client envoie une demande DNS liée à cet URL afin d'obtenir l'IP pour la destination. WLC transmet la requête DNS au serveur DNS et le serveur DNS répond avec une réponse DNS, qui contient l'adresse IP de la destination `www.example.com` qui à son tour est transmise aux clients sans fil.
- Le client tente alors d'établir une connexion TCP avec l'adresse IP de destination. Il envoie un paquet TCP SYN destiné à l'adresse IP de `www.example.com`.
- Le WLC a configuré des règles pour le client, donc peut agir en tant que serveur mandataire pour `www.example.com`. Il renvoie un paquet TCP SYN-ACK au client, avec l'adresse IP de `www.example.com` comme source. Le client renvoie un paquet TCP ACK afin de terminer la connexion TCP en trois étapes et la connexion TCP est entièrement établie.
- Le client envoie un paquet HTTP GET destiné à `www.example.com`. Le WLC intercepte ce paquet et l'envoie pour redirection. La passerelle d'application HTTP prépare un corps en HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client à se rendre à l'URL de page Web par défaut du WLC, par exemple : `http://<Virtual-Server-IP>/login.html`.
- Le client ferme la connexion TCP avec l'adresse IP, par exemple www.example.com.
- Maintenant, le client veut aller à <http://<virtualip>/login.html> et donc il essaie d'ouvrir une connexion TCP avec l'adresse IP virtuelle du WLC. Il envoie un paquet SYN TCP pour 192.0.2.1 (qui est notre IP virtuelle ici) au WLC.
- Le WLC répond par un TCP SYN-ACK, et le client renvoie un TCP ACK au WLC afin de terminer la liaison.

- Le client envoie une requête HTTP GET pour /login.html destinée à 192.0.2.1 afin de demander la page de connexion.
- Cette requête est autorisée jusqu'au serveur Web du WLC et le serveur répond avec la page de connexion par défaut. Le client reçoit la page de connexion dans la fenêtre du navigateur où l'utilisateur peut poursuivre et se connecter.

Dans cet exemple, l'adresse IP du client est 192.168.68.94. Le client a résolu l'URL vers le serveur Web auquel il a accédé, 10.1.0.13. Comme vous pouvez le voir, le client a effectué la connexion en trois étapes pour démarrer la connexion TCP, puis a envoyé un paquet HTTP GET qui a commencé par le paquet 96 (00 est le paquet HTTP). Cela n'a pas été déclenché par l'utilisateur, mais par les déclencheurs de détection du portail automatisé du système d'exploitation (comme nous pouvons le deviner à partir de l'URL demandée). Le contrôleur intercepte les paquets et répond avec le code 200. Le paquet code 200 contient une URL de redirection :

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://captive.apple.c
</HEAD></HTML>
```

Il ferme ensuite la connexion TCP via la connexion en trois étapes.

Le client démarre alors la connexion HTTPS à l'URL de redirection qui l'envoie à 192.0.2.1, qui est l'adresse IP virtuelle du contrôleur. Le client doit valider le certificat du serveur ou l'ignorer pour activer le tunnel SSL. Dans ce cas, il s'agit d'un certificat auto-signé, donc le client l'a ignoré. La page Web de connexion est envoyée via ce tunnel SSL. Le paquet 112 commence les transactions.

No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 - 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSval=1450324338
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000002000	50755 - 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002281000	80 - 50755 [ACK] Seq=1 Ack=132 Win=30000 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	TCP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 - 50755 [FIN, ACK] Seq=500 Ack=132 Win=30000 Len=0 TSval=1450324342 TSecr=1585208304
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 - 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324342
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 - 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324342
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 - 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=1450324342
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001346000	80 - 50755 [ACK] Seq=501 Ack=133 Win=30000 Len=0 TSval=1450324345 TSecr=1585208304
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 - 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGMP	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGMP	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.004031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.local
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 - 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 - 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1585209337
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 - 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSval=1450325384
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 - 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 - 50756 [ACK] Seq=1 Ack=199 Win=30000 Len=0 TSval=1450325387 TSecr=1585209337
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 - 50756 [ACK] Seq=949 Ack=199 Win=30000 Len=948 TSval=1450325390 TSecr=1585209337
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 - 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=1450325384

Vous avez la possibilité de configurer le nom de domaine pour l'adresse IP virtuelle du WLC. Si vous configurez le nom de domaine pour l'adresse IP virtuelle, ce nom de domaine est retourné dans le paquet HTTP OK du contrôleur en réponse au paquet HTTP GET du client. Vous devez ensuite effectuer une résolution DNS pour ce nom de domaine. Une fois qu'il obtient une adresse

IP à partir de la résolution DNS, il tente d'ouvrir une session TCP avec cette adresse IP, qui est une adresse IP configurée sur une interface virtuelle du contrôleur.

La page Web est ensuite transmise au client via le tunnel et l'utilisateur renvoie le nom d'utilisateur/mot de passe via le tunnel SSL (Secure Sockets Layer).

L'authentification Web est effectuée par l'une des trois méthodes suivantes :

- Utiliser une page Web interne (par défaut).
- Utilisez une page de connexion personnalisée.
- Utilisez une page de connexion à partir d'un serveur Web externe.



Remarques :

- Le bundle d'authentification Web personnalisé peut contenir jusqu'à 30 caractères pour les noms de fichiers. Assurez-vous qu'aucun nom de fichier dans le bundle ne dépasse 30 caractères.

- À partir de la version 7.0 du WLC, si l'authentification Web est activée sur le WLAN et que vous avez également des règles de liste de contrôle d'accès du processeur, les règles d'authentification Web basées sur le client sont toujours prioritaires tant que le client n'est pas authentifié dans l'état WebAuth_Reqd. Une fois que le client passe à l'état EXÉCUTÉ, les règles ACL du processeur sont appliquées.

- Par conséquent, si les ACL de CPU sont activées dans le WLC, une règle d'autorisation pour l'IP d'interface virtuelle est requise (dans n'importe quelle direction) dans ces conditions :

- Lorsque la liste de contrôle d'accès du processeur n'a pas de règle d'autorisation ALL pour les deux directions.

- Lorsqu'il existe une règle d'autorisation ALL, mais qu'il existe également une règle de refus pour le port 443 ou 80 de priorité supérieure.

- La règle d'autorisation pour l'adresse IP virtuelle doit être pour le protocole TCP et le port 80 si secureweb est désactivé, ou le port 443 si secureweb est activé. Ceci est nécessaire afin de permettre l'accès du client à l'adresse IP de l'interface virtuelle après une authentification réussie lorsque les ACL du CPU sont en place.

Dépanner l'authentification Web

Après avoir configuré l'authentification Web et si la fonctionnalité ne fonctionne pas comme prévu, procédez comme suit :

1. Vérifiez si le client obtient une adresse IP. Si ce n'est pas le cas, les utilisateurs peuvent décocher la case DHCP Required sur le WLAN et donner au client sans fil une adresse IP statique. Cela suppose une association avec le point d'accès.

2. L'étape suivante du processus est la résolution DNS de l'URL dans le navigateur Web. Lorsqu'un client WLAN se connecte à un WLAN configuré pour l'authentification Web, il obtient une adresse IP du serveur DHCP. L'utilisateur ouvre un navigateur Web et saisit une adresse de site Web. Le client effectue ensuite la résolution DNS pour obtenir l'adresse IP du site Web. À présent, lorsque le client tente d'atteindre le site Web, le WLC intercepte la session HTTP GET du client et redirige l'utilisateur vers la page de connexion d'authentification Web.
3. Par conséquent, assurez-vous que le client est en mesure d'effectuer une résolution DNS pour que la redirection fonctionne. Dans Microsoft Windows, choisissez Démarrer > Exécuter, entrez CMD afin d'ouvrir une fenêtre de commande, et faites un «nslookup www.cisco.com» et voyez si l'adresse IP revient.

Dans Macs/Linux, ouvrez une fenêtre de terminal et faites une nslookup www.cisco.com et voyez si l'adresse IP revient.

Si vous pensez que le client n'obtient pas de résolution DNS, vous pouvez :

- Saisissez l'adresse IP de l'URL (par exemple, <http://www.cisco.com> est <http://192.168.219.25>).
- Essayez de taper n'importe quelle adresse IP (même inexistante) qui doit être résolue via l'adaptateur sans fil.

Lorsque vous entrez cette URL, la page Web s'affiche-t-elle ? Si oui, il s'agit très probablement d'un problème DNS. Il peut également s'agir d'un problème de certificat. Le contrôleur, par défaut, utilise un certificat auto-signé et la plupart des navigateurs Web mettent en garde contre leur utilisation.

4. Pour l'authentification Web avec une page Web personnalisée, assurez-vous que le code HTML de la page Web personnalisée est approprié.

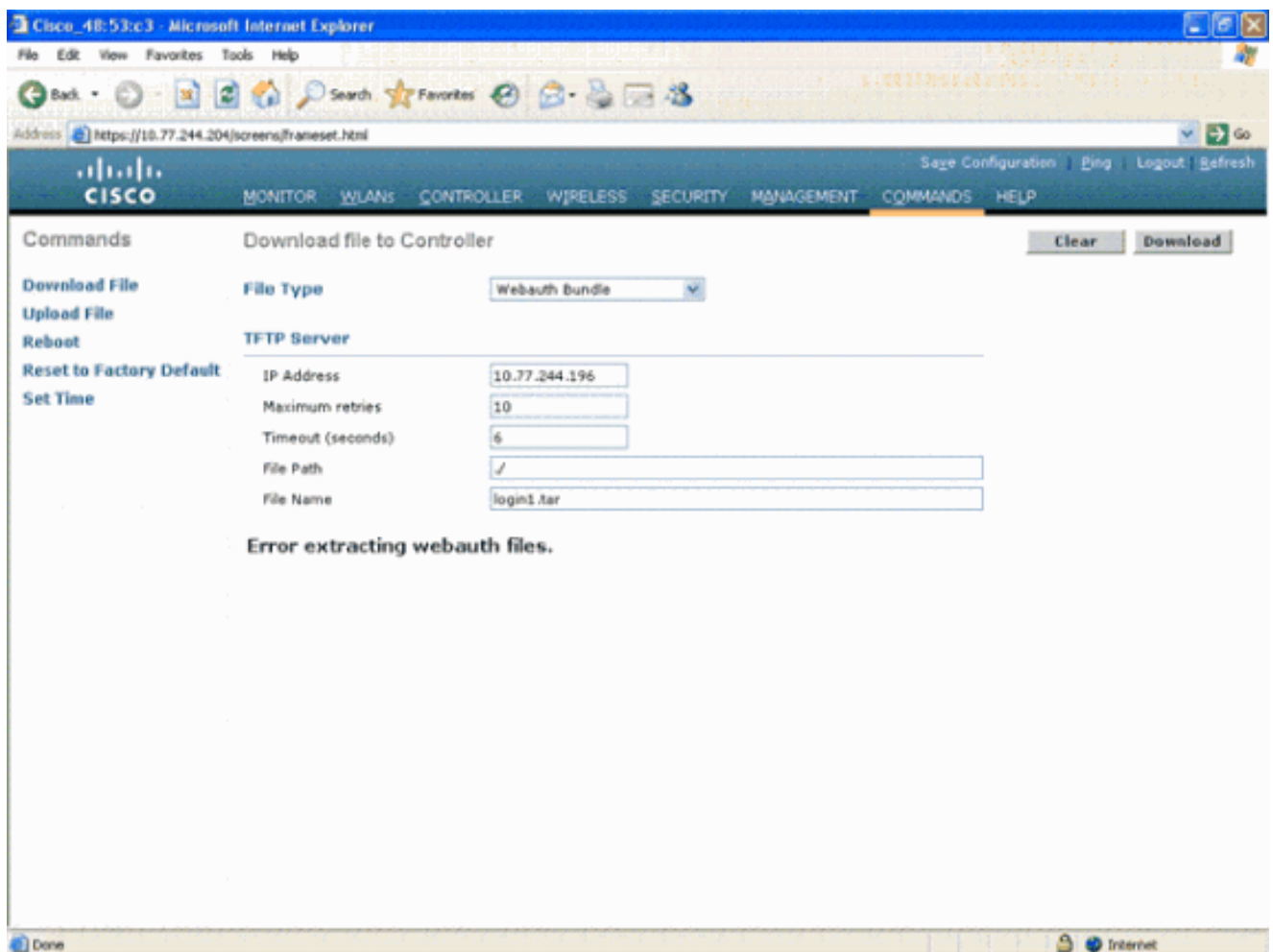
Vous pouvez télécharger un exemple de script d'authentification Web à partir de [Téléchargements de logiciels Cisco](#). Par exemple, pour les contrôleurs 5508, choisissez Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle et téléchargez le fichier webauth_bundle.zip.

Ces paramètres sont ajoutés à l'URL lorsque le navigateur Internet de l'utilisateur est redirigé vers la page de connexion personnalisée :


- ap_mac : adresse MAC du point d'accès auquel l'utilisateur sans fil est associé.
- switch_url : URL du contrôleur vers lequel les informations d'identification de l'utilisateur doivent être publiées.
- redirect : URL vers laquelle l'utilisateur est redirigé une fois l'authentification réussie.
- statusCode : code d'état renvoyé par le serveur d'authentification Web du contrôleur.
- wlan : SSID WLAN auquel l'utilisateur sans fil est associé.

Voici les codes d'état disponibles :

- Code d'état 1 - Vous êtes déjà connecté. Aucune autre action de votre part n'est requise.
 - Code d'état 2 : vous n'êtes pas configuré pour vous authentifier sur le portail Web. Aucune autre action de votre part n'est requise.
 - Code d'état 3 - Le nom d'utilisateur spécifié ne peut pas être utilisé pour le moment. Le nom d'utilisateur est peut-être déjà connecté au système ?
 - Code d'état 4 - Vous avez été exclu.
 - Code d'état 5 - La combinaison du nom d'utilisateur et du mot de passe que vous avez saisie n'est pas valide. Veuillez réessayer.
5. Tous les fichiers et images qui doivent apparaître sur la page Web personnalisée doivent être regroupés dans un fichier .tar avant d'être téléchargés sur le WLC. Assurez-vous que l'un des fichiers inclus dans le bundle .tar est login.html. Vous recevez ce message d'erreur si vous n'incluez pas le fichier login.html :



Référez-vous à la section [Directives pour l'authentification Web personnalisée](#) de [Exemple de configuration de l'authentification Web du contrôleur de réseau local sans fil](#) pour plus d'informations sur la façon de créer une fenêtre d'authentification Web personnalisée.

 Remarque : les fichiers volumineux et les fichiers dont le nom est long peuvent entraîner une erreur d'extraction. Il est recommandé que les images soient au format



.jpg.

6. Assurez-vous que l'option Scripting n'est pas bloquée sur le navigateur client car la page Web personnalisée sur le WLC est fondamentalement un script HTML.
7. Si vous avez un nom d'hôte configuré pour l'interface virtuelle du WLC, assurez-vous que la résolution DNS est disponible pour le nom d'hôte de l'interface virtuelle.



Remarque : accédez au menu Controller > Interfaces à partir de l'interface utilisateur graphique du WLC afin d'attribuer un nom d'hôte DNS à l'interface virtuelle.

8. Parfois, le pare-feu installé sur l'ordinateur client bloque la page de connexion de l'authentification Web. Désactivez le pare-feu avant d'essayer d'accéder à la page de connexion. Le pare-feu peut être réactivé une fois l'authentification Web terminée.
9. Le pare-feu de la topologie/solution peut être placé entre le client et le serveur d'authentification Web, qui dépend du réseau. Comme pour chaque conception/solution réseau implémentée, l'utilisateur final doit s'assurer que ces ports sont autorisés sur le pare-feu réseau.

Protocol	Port
Trafic HTTP/HTTPS	Port TCP 80/443
Trafic de données/contrôle CAPWAP	Port UDP 5247/5246
Trafic de données/contrôle LWAPP (antérieur à rel 5.0)	Port UDP 12222/12223
paquets EOIP	Protocole IP 97
Mobilité	Port UDP 16666 (non sécurisé) Port UDP 16667 (tunnel IPSEC sécurisé)

10. Pour que l'authentification Web se produise, le client doit d'abord s'associer au WLAN approprié sur le WLC. Accédez au menu Monitor > Clients sur la GUI du WLC afin de voir si le client est associé au WLC. Vérifiez si le client dispose d'une adresse IP valide.
11. Désactivez les paramètres proxy sur le navigateur client jusqu'à ce que l'authentification Web soit terminée.
12. La méthode d'authentification Web par défaut est le protocole PAP (Password Authentication Protocol). Assurez-vous que l'authentification PAP est autorisée sur le serveur RADIUS pour que cela fonctionne. Afin de vérifier l'état de l'authentification du client, vérifiez les débogages et les messages de journal du serveur RADIUS. Vous pouvez utiliser la commande debug aaa all sur le WLC afin d'afficher les débogages à partir du serveur RADIUS.
13. Mettez à jour le pilote matériel de l'ordinateur avec le dernier code du site Web du fabricant.
14. Vérifiez les paramètres du demandeur (programme sur ordinateur portable).
15. Lorsque vous utilisez le supplicatif Windows Zero Config intégré à Windows :
 - Vérifiez que l'utilisateur dispose des derniers correctifs installés.
 - Exécutez des débogages sur le demandeur.
16. Sur le client, activez les journaux EAPOL (WPA+WPA2) et RASTLS à partir d'une fenêtre de commande. Choisissez Démarrer > Exécuter > CMD :


```
netsh ras set tracing eapol enable
netsh ras set tracing rastls enable
```

Afin de désactiver les journaux, exécutez la même commande mais remplacez enable par disable. Pour XP, tous les journaux se trouvent dans C:\Windows\tracing.

17. Si vous n'avez toujours pas de page Web de connexion, collectez et analysez ce résultat à partir d'un seul client :

```
debug client <mac_address in format xx:xx:xx:xx:xx:xx>
debug dhcp message enable
debug aaa all enable
debug dot1x aaa enable
debug mobility handoff enable
```

18. Si le problème n'est pas résolu après avoir effectué ces étapes, collectez ces débogages et utilisez [Support Case Manager](#) afin d'ouvrir une demande de service.

```
debug pm ssh-appgw enable
debug pm ssh-tcp enable
debug pm rules enable
debug emweb server enable
debug pm ssh-engine enable packet <client ip>
```

Informations connexes

- [Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil](#)
- [Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil](#)
- [Assistance technique de Cisco et téléchargements](#)

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.