# Web-Authentifizierung auf Wireless LAN-Controllern (WLC)

## Inhalt


Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Interne Prozesse der Webauthentifizierung
Position der Webauthentifizierung als Sicherheitsmerkmal
Funktionsweise von WebAuth
So führen Sie eine interne (lokale) WebAuth-Funktion mit einer internen Seite aus
Konfigurieren einer benutzerdefinierten lokalen WebAuth mit einer benutzerdefinierten Seite
Globale Konfigurationsmethode überschreiben
Umleitungsproblem
So führen Sie eine externe (lokale) Webauthentifizierung mit einer externen Seite durch
Web-Passthrough
Bedingte Webumleitung
Webumleitung für Splash-Seite
WebAuth bei MAC-Filterfehler
Zentrale Webauthentifizierung
Authentifizierung externer Benutzer (RADIUS)
Einrichten eines Wired Guest WLAN
Zertifikate für die Anmeldeseite
Hochladen eines Zertifikats für die Webauthentifizierung des Controllers
Zertifizierungsstelle und andere Zertifikate auf dem Controller
Wie das Zertifikat mit der URL übereinstimmt
Fehlerbehebung bei Zertifikatproblemen
Überprüfen
Zu überprüfende Elemente
Andere Problemsituationen
HTTP-Proxy-Server und Funktionsweise
Webauthentifizierung über HTTP anstelle von HTTPS
Zugehörige Informationen


## Einleitung

Dieses Dokument beschreibt die Prozesse für die Webauthentifizierung auf Wireless LAN Controllern (WLC).

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie Grundkenntnisse der WLC-Konfiguration haben.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen WLC-Hardwaremodellen.

**Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.**

# Interne Prozesse der Webauthentifizierung

## Position der Webauthentifizierung als Sicherheitsmerkmal

Web-Authentifizierung (WebAuth) ist Layer-3-Sicherheit. Es ermöglicht eine benutzerfreundliche Sicherheit, die auf jeder Station funktioniert, die einen Browser führt.

Sie kann mit jeder PSK-Sicherheit (Pre-Shared Key) kombiniert werden (Layer-2-Sicherheitsrichtlinie).

Obwohl die Kombination aus WebAuth und PSK den benutzerfreundlichen Teil reduziert, hat es den Vorteil, den Client-Datenverkehr zu verschlüsseln.

WebAuth ist eine Authentifizierungsmethode ohne Verschlüsselung.

WebAuth kann erst dann mit 802.1x/RADIUS (Remote Authentication Dial-In User Service) konfiguriert werden, wenn WLC Softwareversion 7.4 gleichzeitig installiert und konfiguriert wurde.

Clients müssen sowohl dot1x- als auch die Webauthentifizierung durchlaufen. Es soll ein Webportal für Mitarbeiter (die 802.1x verwenden) und nicht für Gäste eingerichtet werden.

Es gibt keine All-in-One Service Set Identifier (SSID) für dot1x für Mitarbeiter oder ein Webportal für Gäste.

## Funktionsweise von WebAuth

Der 802.11-Authentifizierungsprozess ist offen, sodass Sie sich problemlos authentifizieren und eine Verbindung herstellen können. Anschließend werden Sie zugeordnet, jedoch nicht im WLC. **RUN** status.

Wenn die Webauthentifizierung aktiviert ist, bleiben Sie **WEBAUTH_REQD** wo Sie auf keine Netzwerkressource zugreifen können.

Sie müssen eine DHCP-IP-Adresse mit der Adresse des DNS-Servers in den Optionen erhalten.

Geben Sie eine gültige URL in Ihren Browser ein. Der Client löst die URL über das DNS-Protokoll auf. Der Client sendet dann seine HTTP-Anfrage an die IP-Adresse der Website.

Der WLC fängt diese Anforderung ab und sendet die **webauth** Anmeldeseite, die die Website-IP-Adresse nachahmt. Bei einer externen WebAuth antwortet der WLC mit einer HTTP-Antwort, die Ihre Website-IP-Adresse enthält und angibt, dass die Seite verschoben wurde.

Die Seite wurde auf den vom WLC verwendeten externen Webserver verschoben. Nach der Authentifizierung erhalten Sie Zugriff auf alle Netzwerkressourcen und werden standardmäßig zur ursprünglich angeforderten URL umgeleitet (es sei denn, auf dem WLC wurde eine erzwungene Umleitung konfiguriert).

Zusammenfassend lässt sich sagen, dass der WLC dem Client ermöglicht, den DNS aufzulösen und automatisch eine IP-Adresse in **WEBAUTH_REQD** status.

Um einen anderen Port anstelle von Port 80 anzuzeigen, verwenden Sie **config network web-auth-port** um eine Umleitung auch auf diesem Port zu erstellen.

Ein Beispiel ist die ACS-Webschnittstelle (Access Control Server) auf Port 2002 oder anderen ähnlichen Anwendungen.

> **Hinweis zur HTTPS-Umleitung**: Standardmäßig hat der WLC keinen HTTPS-Datenverkehr umgeleitet. Das bedeutet, dass bei Eingabe einer HTTPS-Adresse in den Browser nichts passiert. Sie müssen eine HTTP-Adresse eingeben, um zur Anmeldeseite weitergeleitet zu werden, die über HTTPS bereitgestellt wurde.
>
> In Version 8.0 und höher können Sie die Umleitung von HTTPS-Datenverkehr mit dem CLI-Befehl aktivieren. **config network web-auth https-redirect enable.**
>
> Für den Fall, dass viele HTTPS-Anfragen versendet werden, werden für den WLC viele Ressourcen benötigt. Es ist nicht ratsam, diese Funktion vor WLC Version 8.7 zu verwenden, wo die Skalierbarkeit dieser Funktion verbessert wurde. Beachten Sie auch, dass eine Zertifikatswarnung in diesem Fall unvermeidbar ist. Wenn der Client eine URL anfordert (z. B. https://www.cisco.com), stellt der WLC weiterhin sein eigenes Zertifikat für die IP-Adresse der virtuellen Schnittstelle bereit. Dies entspricht nie der vom Client angeforderten URL/IP-Adresse, und das Zertifikat ist nicht vertrauenswürdig, es sei denn, der Client erzwingt die Ausnahme in seinem Browser.

Indikativer Leistungsabfall der WLC-Softwareversion vor 8.7 gemessen:

| Webauth | Erzielte Leistung |
|---|---|
| 3 URLs - HTTP | 140/Sekunde |
| 1. URL - HTTP<br>2. und 3. URLs - HTTPS | 20/Sekunde |
| 3 URLs - HTTPS (große Bereitstellung) | <1/s |
| 3 URLs - HTTPS (max. 100 Clients) | 10/Sekunde |

In dieser Performance-Tabelle werden die drei URLs als:

- Die vom Endbenutzer eingegebene ursprüngliche URL
- Die URL, an die der WLC den Browser umleitet
- Die endgültige Einreichung der Anmeldeinformationen

Die Leistungstabelle gibt die WLC-Leistung an, wenn alle drei URLs HTTP sind, wenn alle drei URLs HTTPS sind oder wenn der Client von HTTP zu HTTPS wechselt (typisch).

# So führen Sie eine interne (lokale) WebAuth-Funktion mit einer internen Seite aus

Um ein WLAN mit einer dynamischen Betriebsschnittstelle zu konfigurieren, erhalten die Clients über DHCP auch eine IP-Adresse des DNS-Servers.

Vor jeder **webauth** , gesetzt ist, überprüfen, ob WLAN ordnungsgemäß funktioniert, DNS-Anfragen aufgelöst werden können (**nslookup**), und Webseiten können durchsucht werden.

Legen Sie die Webauthentifizierung als Layer-3-Sicherheitsfunktionen fest. Erstellen Sie Benutzer in der lokalen Datenbank oder auf einem externen RADIUS-Server.

Weitere Informationen finden Sie im Dokument Wireless LAN Controller Web Authentication Configuration Example.

## Konfigurieren einer benutzerdefinierten lokalen WebAuth mit einer benutzerdefinierten Seite

Benutzerdefiniert **webauth** kann wie folgt konfiguriert werden: **redirectUrl** von **Security** aus. Dadurch wird eine Umleitung zu einer bestimmten Webseite erzwungen, die Sie eingeben.

Wenn der Benutzer authentifiziert wird, überschreibt er die ursprüngliche URL, die der Client angefordert hat, und zeigt die Seite an, der die Umleitung zugewiesen wurde.

Mit der benutzerdefinierten Funktion können Sie eine benutzerdefinierte HTML-Seite anstelle der Standardanmeldeseite verwenden. Laden Sie Ihr HTML- und Image-Dateipaket auf den Controller hoch.

Suchen Sie auf der Upload-Seite nach **webauth bundle** im TAR-Format. PicoZip erstellt Teere, die kompatibel mit dem WLC arbeiten.

Ein Beispiel für ein WebAuth-Paket finden Sie auf der Seite Software herunterladen für Wireless Controller WebAuth-Pakete. Wählen Sie die entsprechende Version für Ihren WLC aus.

Es wird empfohlen, ein vorhandenes Paket anzupassen. kein neues Paket erstellen.

Es gibt einige Einschränkungen hinsichtlich **custom webauth** die je nach Version und Bugs variieren.

- die .tar-Datei (nicht mehr als 5 MB)
- Die Anzahl der Dateien in der .tar
- die Dateinamenlänge der Dateien (nicht mehr als 30 Zeichen)

Wenn das Paket nicht funktioniert, versuchen Sie ein einfaches benutzerdefiniertes Paket. Fügen Sie Dateien und Komplexität einzeln hinzu, um das Paket zu erreichen, das der Benutzer zu verwenden versuchte. Dies hilft, das Problem zu identifizieren.

Informationen zum Konfigurieren einer benutzerdefinierten Seite finden Sie unter Creating a Customized Web Authentication Login Page (Benutzerdefinierte Web-Authentifizierungs-Anmeldeseite erstellen), einem Abschnitt im Cisco Wireless LAN Controller Configuration Guide, Release 7.6.

### Globale Konfigurationsmethode überschreiben

Konfigurieren Sie den Befehl **override global config**, und legen Sie einen WebAuth-Typ für jedes WLAN fest. Dadurch wird eine interne/standardmäßige WebAuth mit einer benutzerdefinierten internen/standardmäßigen WebAuth für ein anderes WLAN zugelassen.

Dies ermöglicht die Konfiguration verschiedener benutzerdefinierter Seiten für jedes WLAN.

Alle Seiten im selben Paket zusammenfassen und auf den WLC hochladen.

Legen Sie Ihre benutzerdefinierte Seite mit dem Befehl **override global config** in jedem WLAN fest, und wählen Sie aus allen Dateien im Paket aus, welche Datei die Anmeldeseite ist.

Wählen Sie für jedes WLAN eine andere Anmeldeseite innerhalb des Pakets aus.

### Umleitungsproblem

Es gibt eine Variable innerhalb des HTML-Pakets, die die Umleitung ermöglicht. Legen Sie die URL für die erzwungene Umleitung nicht dort ab.

Bei Umleitungsproblemen in benutzerdefinierter WebAuth empfiehlt Cisco, das Paket zu überprüfen.

Wenn Sie eine Umleitungs-URL mit **+=** in die WLC-GUI eingeben, kann diese die im Paket definierte URL überschreiben *oder* hinzufügen.

In der WLC-GUI kann beispielsweise der **redirectURL** auf "www.cisco.com" gesetzt; Im Paket wird jedoch Folgendes angezeigt: **redirectURL+=** '(Website-URL)'. += leitet Benutzer an eine ungültige URL um.

## So führen Sie eine externe (lokale) Webauthentifizierung mit einer externen Seite durch

Die Nutzung eines externen WebAuth-Servers ist nur ein externes Repository für die Anmeldeseite. Die Benutzeranmeldeinformationen werden weiterhin vom WLC authentifiziert. Der externe Webserver lässt nur eine spezielle oder eine andere Anmeldeseite zu.

Schritte für eine externe WebAuth:

1. Der Client (Endbenutzer) öffnet einen Webbrowser und gibt eine URL ein.

2. Wenn der Client nicht authentifiziert wird und eine externe Webauthentifizierung verwendet wird, leitet der WLC den Benutzer zur externen Webserver-URL um. Der WLC sendet eine HTTP-Umleitung mit der imitierten IP-Adresse an den Client und verweist auf die IP-Adresse des externen Servers. Die externe Anmelde-URL für die Webauthentifizierung wird mit Parametern wie dem **AP_Mac_Address**,Die Fehlermeldung **client_url** (URL-Adresse des Clients) und **action_URL** erforderlich, um den Switch-Webserver zu kontaktieren.

3. Die externe Webserver-URL sendet den Benutzer an eine Anmeldeseite. Der Benutzer kann

eine Zugriffskontrollliste vor der Authentifizierung verwenden, um auf den Server zuzugreifen.

4. Die Anmeldeseite sendet die Anforderung der Benutzeranmeldeinformationen zurück an das **action_URLZ**. B. http://192.0.2.1/login.html des WLC-Webservers ein. Dieser wird als Eingabeparameter für die Umleitungs-URL bereitgestellt, wobei 192.0.2.1 die virtuelle Schnittstellenadresse auf dem Switch ist.

5. Der WLC-Webserver sendet den Benutzernamen und das Kennwort zur Authentifizierung ein.

6. Der WLC initiiert die RADIUS-Serveranforderung oder verwendet die lokale Datenbank auf dem WLC und authentifiziert dann den Benutzer.

7. Bei erfolgreicher Authentifizierung leitet der WLC-Webserver den Benutzer entweder an die konfigurierte Umleitungs-URL oder an die vom Client eingegebene URL weiter.

8. Wenn die Authentifizierung fehlschlägt, leitet der WLC-Webserver den Benutzer zurück zur Anmelde-URL des Benutzers.

   **Hinweis**: In diesem Dokument wird 192.0.2.1 als Beispiel für eine virtuelle IP verwendet. Der 192.0.2.x-Bereich sollte für virtuelle IP-Adressen verwendet werden, da diese nicht geroutet werden können. Eine ältere Dokumentation verweist möglicherweise auf "1.1.1.x" oder ist noch immer das, was in Ihrem WLC konfiguriert ist, da dies die Standardeinstellung war. Beachten Sie jedoch, dass diese IP nun eine gültige routbare IP-Adresse ist und daher stattdessen das Subnetz 192.0.2.x empfohlen wird.

Wenn sich die Access Points (APs) im FlexConnect-Modus befinden, **preauth** ACL ist irrelevant. Flex ACLs können verwendet werden, um nicht authentifizierten Clients den Zugriff auf den Webserver zu ermöglichen.

Weitere Informationen finden Sie im Konfigurationsbeispiel für die externe Webauthentifizierung mit Wireless LAN-Controllern.

## Web-Passthrough

Web-Passthrough ist eine Variante der internen Web-Authentifizierung. Es wird eine Seite mit einer Warnung oder einer Warnmeldung angezeigt, aber es werden keine Anmeldeinformationen angefordert.

Der Benutzer klickt dann auf **OK**. Aktivieren Sie die E-Mail-Eingabe, und der Benutzer kann seine E-Mail-Adresse eingeben, die zu seinem Benutzernamen wird.

Wenn der Benutzer verbunden ist, überprüfen Sie die Liste der aktiven Clients und ob der Benutzer mit der E-Mail-Adresse aufgeführt ist, die er als Benutzername eingegeben hat.

Weitere Informationen finden Sie im Konfigurationsbeispiel für den WLAN-Controller 5760/3850 Web-Passthrough.

# Bedingte Webumleitung

Wenn Sie eine bedingte Webumleitung aktivieren, wird der Benutzer nach erfolgreicher 802.1x-Authentifizierung bedingt auf eine bestimmte Webseite umgeleitet.

Sie können die Umleitungsseite und die Bedingungen angeben, unter denen die Umleitung auf dem RADIUS-Server erfolgt.

Zu den Bedingungen kann das Kennwort gehören, wenn es das Ablaufdatum erreicht oder wenn der Benutzer eine Rechnung für die weitere Nutzung/den Zugriff bezahlen muss.

Wenn der RADIUS-Server das Cisco AV-Paar zurückgibt **url-redirect**wird der Benutzer zum angegebenen URL umgeleitet, wenn er einen Browser öffnet.

Wenn der Server auch das Cisco AV-Paar zurückgibt, **url-redirect-acl**wird die angegebene ACL als Pre-Authentication-ACL für diesen Client installiert.

Der Client gilt derzeit als nicht vollständig autorisiert und kann nur den Datenverkehr weiterleiten, der von der ACL vor der Authentifizierung zugelassen wurde. Nachdem der Client einen bestimmten Vorgang unter der angegebenen URL abgeschlossen hat (z. B. eine Passwortänderung oder Rechnungszahlung), muss er sich erneut authentifizieren.

Wenn der RADIUS-Server keine **url-redirect**ist, gilt der Client als vollständig autorisiert und darf Datenverkehr weiterleiten.

> **Anmerkung:** Die Funktion für bedingte Web-Umleitungen steht nur für WLANs zur Verfügung, die für die Sicherheit von 802.1x oder WPA+WPA2 Layer 2 konfiguriert wurden.

Konfigurieren Sie nach der Konfiguration des RADIUS-Servers die bedingte Web-Umleitung auf dem Controller über die grafische Benutzeroberfläche (GUI) oder CLI des Controllers. Lesen Sie die folgenden schrittweisen Anleitungen: Konfigurieren der Webumleitung (GUI) und Konfigurieren der Webumleitung (CLI).

# Webumleitung für Splash-Seite

Wenn Sie die Splash-Page-Webumleitung aktivieren, wird der Benutzer nach erfolgreicher 802.1x-Authentifizierung auf eine bestimmte Webseite umgeleitet. Nach der Umleitung hat der Benutzer vollen Zugriff auf das Netzwerk.

Sie können die Umleitungsseite auf dem RADIUS-Server angeben. Wenn der RADIUS-Server das Cisco AV-Paar zurückgibt **url-redirect**wird der Benutzer zum angegebenen URL umgeleitet, wenn er einen Browser öffnet.

Der Client wird zu diesem Zeitpunkt als vollständig autorisiert angesehen und kann Datenverkehr weiterleiten, selbst wenn der RADIUS-Server keine **url-redirect**.

> **Anmerkung:** Die Splash Page Redirect-Funktion steht nur für WLANs zur Verfügung, die für 802.1x- oder WPA+WPA2 Layer 2-Sicherheit konfiguriert sind.

Konfigurieren Sie nach der Konfiguration des RADIUS-Servers die Splash-Page-Webumleitung auf dem Controller über die grafische Benutzeroberfläche oder Kommandozeile des Controllers.

### WebAuth bei MAC-Filterfehler

Eine WebAuth auf MAC Filter FaFailure erfordert die Konfiguration von MAC-Filtern im Sicherheitsmenü von Layer 2.

Wenn die Benutzer erfolgreich mit ihren MAC-Adressen validiert wurden, können sie direkt **run** status.

Ist dies nicht der Fall, gehen sie zum **WEBAUTH_REQD** und die normale Web-Authentifizierung erfolgt.

> **Anmerkung:** Web-Passthrough wird nicht unterstützt.Weitere Informationen finden Sie in der Aktivität zu Erweiterungsanfrage Cisco Bug-ID CSCtw73512.

## Zentrale Webauthentifizierung

Die zentrale Web-Authentifizierung bezieht sich auf ein Szenario, in dem der WLC keine Dienste mehr hostet. Der Client wird direkt an das ISE-Webportal gesendet und durchläuft nicht 192.0.2.1 auf dem WLC. Die Anmeldeseite und das gesamte Portal werden externalisiert.

Die zentrale Web-Authentifizierung erfolgt, wenn in den erweiterten Einstellungen der WLAN- und MAC-Filter die RADIUS-NAC (Network Admission Control) aktiviert ist.

Der WLC sendet eine RADIUS-Authentifizierung (in der Regel für den MAC-Filter) an die ISE, die mit dem **redirect-url** Attributwertpaar (AV).

Anschließend wird der Benutzer **POSTURE_REQD** bis die ISE die Autorisierung mit einer Anforderung zur Autorisierungsänderung erteilt. Dasselbe Szenario tritt in Posture (Status) oder Central WebAuth (Zentrale WebAuth) auf.

Central WebAuth ist nicht mit WPA-Enterprise/802.1x kompatibel, da das Gastportal keine Sitzungsschlüssel für die Verschlüsselung zurückgeben kann, wie dies bei Extensible Authentication Protocol (EAP) der Fall ist.

## Authentifizierung externer Benutzer (RADIUS)

Die externe Benutzerauthentifizierung (RADIUS) ist nur für die lokale WebAuth gültig, wenn der WLC die Anmeldeinformationen verarbeitet oder wenn eine Layer-3-Webrichtlinie aktiviert ist. Benutzer lokal oder auf dem WLC oder extern über RADIUS authentifizieren.

Es gibt eine Reihenfolge, in der der WLC nach den Anmeldeinformationen des Benutzers sucht.

1. In jedem Fall sucht es zuerst in seiner eigenen Datenbank.
2. Findet er dort keine Benutzer, wird er an den im Gast-WLAN konfigurierten RADIUS-Server weitergeleitet (falls ein Server konfiguriert ist).
3. Anschließend wird die globale RADIUS-Serverliste mit den RADIUS-Servern abgeglichen,

auf denen **network user** ist aktiviert.

Mit diesem dritten Punkt wird die Frage derjenigen beantwortet, die RADIUS nicht für dieses WLAN konfigurieren. Beachten Sie jedoch, dass RADIUS auch dann mit RADIUS abgeglichen wird, wenn der Benutzer nicht auf dem Controller gefunden wird.

Das liegt daran, **network user** wird mit Ihren RADIUS-Servern in der globalen Liste abgeglichen.

WLC kann Benutzer mithilfe des Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) oder EAP-MD5 (Message Digest5) am RADIUS-Server authentifizieren.

Dies ist ein globaler Parameter, der über die GUI oder CLI konfiguriert werden kann:

Über GUI: navigieren zu **Controller > Web RADIUS Authentication**

Aus CLI: eingeben **config custom-web RADIUSauth**

> Hinweis: Der NAC-Gastserver verwendet nur PAP.

# Einrichten eines Wired Guest WLAN

Eine WLAN-Konfiguration für kabelgebundene Gäste ähnelt einer Konfiguration für Wireless-Gäste. Es kann mit einem oder zwei Controllern konfiguriert werden (nur wenn einer automatisch verankert wird).

Wählen Sie ein VLAN als VLAN für kabelgebundene Gastbenutzer aus, z. B. in VLAN 50. Wenn ein kabelgebundener Gast Zugriff auf das Internet wünscht, verbinden Sie den Laptop mit einem Port an einem für VLAN 50 konfigurierten Switch.

Dieses VLAN 50 muss zugelassen und auf dem Pfad durch den WLC-Trunk-Port vorhanden sein.

Bei zwei WLCs (ein Anker und ein Foreign) muss dieses kabelgebundene Gast-VLAN zum Foreign WLC (namens WLC1) und nicht zum Anker führen.

WLC1 übernimmt dann den Datenverkehrstunnel zum DMZ-WLC (der Anker heißt WLC2), der den Datenverkehr im gerouteten Netzwerk freigibt.

Nachfolgend sind die fünf Schritte zum Konfigurieren des kabelgebundenen Gastzugriffs aufgeführt:

1. **Konfigurieren Sie eine dynamische Schnittstelle (VLAN) für den kabelgebundenen Gastbenutzerzugriff.**

   Erstellen Sie auf WLC1 eine dynamische Schnittstelle VLAN50. Im **interface configuration** Seite, überprüfen Sie **Guest LAN** Box. Anschließend können Felder wie **IP address** und **gateway** verschwinden. Der WLC muss erkennen, dass der Datenverkehr von VLAN 50 geroutet wird. Diese Clients sind verkabelte Gäste.

2. **Erstellen Sie ein kabelgebundenes LAN für den Gastbenutzerzugriff.**

Auf einem Controller wird eine Schnittstelle verwendet, wenn sie einem WLAN zugeordnet ist. Erstellen Sie anschließend ein WLAN auf den Controllern der Hauptniederlassung. Navigieren Sie zu **WLANs** und klicke auf **New**. In **WLAN Type**, wählen **Guest LAN**.

Geben Sie in **Profile Name** and **WLAN SSID (Profilname** und **WLAN-SSID**) einen Namen ein, der das WLAN identifiziert. Diese Namen können unterschiedlich sein, dürfen jedoch keine Leerzeichen enthalten. Der Begriff "WLAN" wird verwendet, aber dieses Netzwerkprofil steht in keinem Zusammenhang mit dem Wireless-Netzwerkprofil.

Die Fehlermeldung **General** bietet zwei Dropdown-Listen: **Ingress** und **Egress**. "Ingress" (Eingang) ist das VLAN, von dem Benutzer kommen (VLAN 50). Der Ausgang ist das VLAN, an das Sie sie senden.

für **Ingress**, wählen **VLAN50**.

für **Egress**ist es anders. Wenn Sie nur einen Controller haben, erstellen Sie eine weitere dynamische Schnittstelle, **standard** einmal (nicht in einem Gast-LAN) und senden Sie kabelgebundene Benutzer an diese Schnittstelle. Senden Sie sie in diesem Fall an den DMZ-Controller. Daher **Egress** Schnittstelle auswählen, **Management Interface**.

Die Fehlermeldung **Security** -Modus für dieses Gast-LAN "WLAN" ist WebAuth, was akzeptabel ist. Klicken Sie auf **Ok** um zu validieren.

3. **Konfigurieren Sie den ausländischen Controller (Hauptniederlassung).**

Über die **WLAN list**,Klicken Sie auf **Mobility Anchor** am Ende des **Guest LAN** und wählen Sie Ihren DMZ-Controller aus. Dabei wird davon ausgegangen, dass sich beide Controller gegenseitig erkennen. Wenn dies nicht der Fall ist, besuchen Sie **Controller** > **Mobility Management** > **Mobility group**, und fügen Sie **DMZWLC** auf WLC1 hinzu. Dann fügen Sie **WLC1** auf DMZ hinzu. Beide Controller müssen nicht Teil derselben Mobilitätsgruppe sein. Andernfalls werden grundlegende Sicherheitsregeln nicht eingehalten.

4. **Konfigurieren Sie den Anker-Controller (den DMZ-Controller).**

Der Controller der Hauptniederlassung ist bereit. Bereiten Sie jetzt Ihren DMZ-Controller vor. Öffnen Sie eine Webbrowsersitzung für Ihren DMZ-Controller, und navigieren Sie zu **WLANs**. Erstellen Sie ein neues WLAN. In **WLAN Type**, wählen **Guest LAN**.

In **Profile Name** und **WLAN SSID**einen Namen ein, der dieses WLAN identifiziert. Verwenden Sie die gleichen Werte, die Sie auf dem Controller der Hauptniederlassung eingegeben haben.

Die Fehlermeldung **Ingress** Schnittstelle **None**. Dies spielt keine Rolle, da der Datenverkehr über den Ethernet over IP (EoIP)-Tunnel empfangen wird. Es muss keine Eingangsschnittstelle angegeben werden.

Die Fehlermeldung **Egress** Schnittstelle, an die die Clients gesendet werden sollen. Beispielsweise **DMZ VLAN** ist VLAN 9. Erstellen Sie eine standardmäßige dynamische

Schnittstelle für VLAN 9 auf Ihrem DMZWLC, und wählen Sie dann **VLAN 9** als Egress-Schnittstelle.

Konfigurieren Sie das Ende des Mobility Anchor-Tunnels. Wählen Sie in der **WLAN-Liste** Folgendes aus: **Mobility Anchor for Guest LAN**. Senden Sie den Datenverkehr an den lokalen Controller **DMZWLC**. Beide Seiten sind nun bereit.

5. **Feinabstimmung des Gast-LANs**

   Sie können die WLAN-Einstellungen auch an beiden Enden anpassen. Die Einstellungen müssen auf beiden Seiten identisch sein. Wenn Sie beispielsweise in der **WLAN Advanced** Registerkarte, **Allow AAA override** Aktivieren Sie auf WLC1 dasselbe Kontrollkästchen für DMZWLC. Bei Abweichungen des WLAN auf beiden Seiten wird der Tunnel unterbrochen. DMZWLC lehnt den Datenverkehr ab. können Sie sehen, wenn Sie **run debug mobility**.

   Beachten Sie, dass alle Werte tatsächlich von DMZWLC erhalten werden: IP-Adressen, VLAN-Werte usw. Konfigurieren Sie die WLC1-Seite identisch, sodass die Anforderung an die WLCDMZ weitergeleitet wird.

# Zertifikate für die Anmeldeseite

In diesem Abschnitt werden die Prozesse beschrieben, mit denen Sie ein eigenes Zertifikat auf der WebAuth-Seite platzieren oder die WebAuth-URL 192.0.2.1 ausblenden und eine benannte URL anzeigen können.

## Hochladen eines Zertifikats für die Webauthentifizierung des Controllers

Über die Benutzeroberfläche (**WebAuth > Certificate**) oder CLI (Transfertyp) **webauthcert**) können Sie ein Zertifikat auf den Controller hochladen.

Unabhängig davon, ob es sich um ein mit Ihrer Zertifizierungsstelle (Certificate Authority, CA) erstelltes Zertifikat oder ein offizielles Zertifikat eines Drittanbieters handelt, muss es im Format .pem vorliegen.

Vor dem Senden müssen Sie auch den Schlüssel des Zertifikats eingeben.

Nach dem Upload muss das Zertifikat neu gestartet werden. Rufen Sie nach dem Neustart die WebAuth-Zertifikatsseite in der grafischen Benutzeroberfläche auf, um die Details des von Ihnen hochgeladenen Zertifikats (Gültigkeit usw.) zu finden.

Das wichtige Feld ist der Common Name (CN), d. h. der für das Zertifikat ausgestellte Name. Dieses Feld wird in diesem Dokument im Abschnitt "Zertifizierungsstelle und andere Zertifikate auf dem Controller" behandelt.

Nach dem Neustart und der Überprüfung der Zertifikatdetails wird das neue Controller-Zertifikat auf der WebAuth-Anmeldeseite angezeigt. Es kann jedoch zwei Situationen geben.

1. Wenn Ihr Zertifikat von einer der wenigen Haupt-Stammzertifizierungsstellen ausgestellt wurde, denen jeder Computer vertraut, dann ist es in Ordnung. Ein Beispiel ist VeriSign, aber

normalerweise werden Sie von einer Verisign-Unterzertifizierungsstelle signiert und nicht von der Stammzertifizierungsstelle. Sie können den Zertifikatsspeicher Ihres Browsers einchecken, wenn die dort erwähnte Zertifizierungsstelle als vertrauenswürdig angezeigt wird.

2. Wenn Sie Ihr Zertifikat von einem kleineren Unternehmen/einer kleineren Zertifizierungsstelle erhalten haben, vertrauen ihnen nicht alle Computer. Geben Sie das Firmen-/Zertifizierungsstellenzertifikat auch an den Client weiter, und eine der Stammzertifizierungsstellen stellt dann dieses Zertifikat aus. Schließlich haben Sie eine Kette wie "Zertifikat wurde von CA ausgestellt x > CA x Zertifikat wurde von CA ausgestellt y > CA y Zertifikat wurde von dieser vertrauenswürdigen Stammzertifizierungsstelle ausgestellt". Das Endziel besteht darin, eine Zertifizierungsstelle zu erreichen, der der Client vertraut.

## Zertifizierungsstelle und andere Zertifikate auf dem Controller

Um die Warnung "Dieses Zertifikat ist nicht vertrauenswürdig" zu entfernen, geben Sie das Zertifikat der Zertifizierungsstelle ein, die das Controller-Zertifikat auf dem Controller ausgestellt hat.

Anschließend präsentiert der Controller beide Zertifikate (das Controller-Zertifikat und sein CA-Zertifikat). Das Zertifizierungsstellenzertifikat muss eine vertrauenswürdige Zertifizierungsstelle sein oder über die Ressourcen zum Überprüfen der Zertifizierungsstelle verfügen. Sie können eine Kette von Zertifizierungsstellenzertifikaten erstellen, die zu einer vertrauenswürdigen Zertifizierungsstelle führt.

Platzieren Sie die gesamte Kette in derselben Datei. Die Datei enthält dann Inhalte wie dieses Beispiel:

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

## Wie das Zertifikat mit der URL übereinstimmt

Die WebAuth URL wird auf 192.0.2.1 gesetzt, um sich zu authentifizieren und das Zertifikat wird ausgestellt (dies ist das CN-Feld des WLC-Zertifikats).

Um die WebAuth-URL in 'myWLC.com' zu ändern, gehen Sie beispielsweise in die **virtual interface configuration** (die Schnittstelle 192.0.2.1). Dort können Sie **virtual DNS hostname**wie myWLC.com.

Dadurch wird 192.0.2.1 in der URL-Leiste ersetzt. Dieser Name muss ebenfalls auflösbar sein. Die Sniffer-Ablaufverfolgung zeigt, wie alles funktioniert. Wenn WLC jedoch die Anmeldeseite sendet, zeigt WLC die myWLC.com-Adresse an, und der Client löst diesen Namen mit seinem DNS auf.

Dieser Name muss als 192.0.2.1 aufgelöst werden. Dies bedeutet, wenn Sie auch einen Namen für die Verwaltung des WLC verwenden, verwenden Sie einen anderen Namen für WebAuth.

Wenn Sie "myWLC.com" verwenden, das der IP-Adresse des WLC zugeordnet ist, müssen Sie einen anderen Namen für WebAuth verwenden, z. B. myWLCwebauth.com.

## Fehlerbehebung bei Zertifikatproblemen

In diesem Abschnitt wird erläutert, wie und was Sie zur Fehlerbehebung bei Zertifikatproblemen überprüfen müssen.

## Überprüfen

Laden Sie OpenSSL herunter (für Windows suchen Sie nach OpenSSL Win32) und installieren Sie es. Ohne Konfiguration können Sie im Verzeichnis bin versuchen, **openssl s_client –connect (your web auth URL):443**,

Wenn diese URL die URL ist, mit der Ihre WebAuth-Seite auf Ihrem DNS verknüpft ist, lesen Sie "Was überprüfen" im nächsten Abschnitt dieses Dokuments.

Wenn Ihre Zertifikate eine private Zertifizierungsstelle verwenden, platzieren Sie das Zertifikat der Stammzertifizierungsstelle in einem Verzeichnis auf einem lokalen Computer, und verwenden Sie die openssl-Option **-CApath**. Wenn Sie über eine Zwischen-CA verfügen, speichern Sie diese ebenfalls im gleichen Verzeichnis.

Um allgemeine Informationen über das Zertifikat zu erhalten und es zu überprüfen, verwenden Sie:

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Es ist auch nützlich, Zertifikate mithilfe von openssl zu konvertieren:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

## Zu überprüfende Elemente

Sie können sehen, welche Zertifikate beim Herstellen der Verbindung an den Client gesendet werden. Gerätezertifikat lesen - Der CN muss die URL sein, über die die Webseite erreichbar ist.

Lesen Sie die Zeile "issued by" (Ausgestellt von) im Gerätezertifikat. Dies muss mit der CN des zweiten Zertifikats übereinstimmen. Dieses zweite Zertifikat, "ausgestellt von", muss mit dem CN des nächsten Zertifikats übereinstimmen usw. Andernfalls bildet es keine echte Kette.

Beachten Sie in der hier gezeigten OpenSSL-Ausgabe, dass **openssl** kann das Gerätezertifikat nicht überprüfen, da sein "ausgestellt von" nicht mit dem Namen des bereitgestellten Zertifizierungsstellenzertifikats übereinstimmt.

## SSL-Ausgabe

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
```

```
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

Ein weiteres mögliches Problem besteht darin, dass das Zertifikat nicht auf den Controller hochgeladen werden kann. In dieser Situation gibt es keine Frage der Gültigkeit, CA, und so weiter.

Um dies zu überprüfen, überprüfen Sie die TFTP-Verbindung (Trivial File Transfer Protocol), und versuchen Sie, eine Konfigurationsdatei zu übertragen. Wenn Sie das **debug transfer all enable** - Befehl, beachten Sie, dass das Problem bei der Installation des Zertifikats liegt.

Dies kann daran liegen, dass der falsche Schlüssel für das Zertifikat verwendet wurde. Möglicherweise hat das Zertifikat auch ein falsches Format oder ist beschädigt.

Cisco empfiehlt, den Zertifikatsinhalt mit einem bekannten, gültigen Zertifikat zu vergleichen. So können Sie sehen, ob ein **LocalkeyID** -Attribut zeigt alle 0s (bereits geschehen). In diesem Fall muss das Zertifikat erneut konvertiert werden.

Es gibt zwei OpenSSL-Befehle, mit denen Sie von .pem nach .p12 zurückkehren und dann eine .pem-Datei mit dem gewünschten Schlüssel erneut ausgeben können.

Wenn Sie eine .pem-Datei erhalten haben, die ein Zertifikat gefolgt von einem Schlüssel enthält, kopieren Sie den Schlüsselteil, und fügen Sie ihn ein: **----BEGIN KEY ---- until ------- END KEY ------** aus der .pem-Datei in "key.pem".

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? Sie werden zur Eingabe einer Taste aufgefordert. eingeben **check123**.
2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123**
   Daraus ergibt sich eine operative .pem mit dem Passwort **check123**.

## Andere Problemsituationen

Der **Mobilitätsanker** wurde in diesem Dokument zwar nicht behandelt. Wenn Sie sich jedoch in einer **verankerten** Gastsituation befinden, stellen Sie sicher, dass der Mobilitätsaustausch ordnungsgemäß erfolgt und dass der Client auf dem Anker ankommt.

Alle weiteren WebAuth-Probleme müssen mit dem Anker behoben werden.

Hier einige häufige Probleme, die Sie beheben können:

- **Benutzer können keine Verbindung zum Gast-WLAN herstellen**.

  Dies bezieht sich nicht auf WebAuth. Überprüfen Sie die Client-Konfiguration, die Sicherheitseinstellungen im WLAN (falls aktiviert), die Funkmodule, die aktiv und betriebsbereit sind usw.

- **Benutzer erhalten keine IP-Adresse**.

  In einer Gastankersituation liegt dies meistens daran, dass das Auslands- und das Ankersystem nicht genau gleich konfiguriert wurden. Überprüfen Sie andernfalls die DHCP-Konfiguration, die Verbindung usw.
- Überprüfen Sie, ob andere WLANs problemlos denselben DHCP-Server verwenden können. Dies hängt immer noch nicht mit WebAuth zusammen.

- **Der Benutzer wird nicht zur Anmeldeseite weitergeleitet**.

  Dies ist das häufigste Symptom, aber präziser. Es gibt zwei mögliche Szenarien.

  Der Benutzer wird nicht umgeleitet (der Benutzer gibt eine URL ein und erreicht nie die WebAuth-Seite). Überprüfen Sie in diesem Fall:

  dass dem Client über DHCP (**ipconfig /all**),

  dass der DNS vom Client aus erreichbar ist (**nslookup (website URL**),

  dass der Benutzer eine gültige URL eingegeben hat, um weitergeleitet zu werden,

  dass der Benutzer eine HTTP-URL auf Port 80 verwendet hat (z. B. zum Erreichen eines ACS mit http://localhost:2002 werden Sie nicht umgeleitet, da Sie auf Port 2002 anstatt auf 80 gesendet haben).

  Der Benutzer wird korrekt zu 192.0.2.1 umgeleitet, aber die Seite selbst wird nicht angezeigt.

  Diese Situation ist höchstwahrscheinlich entweder ein WLC-Problem (Bug) oder ein clientseitiges Problem. Möglicherweise verfügt der Client über eine Firewall, Software oder einen Richtlinienblock. Möglicherweise haben sie auch einen Proxy in ihrem Webbrowser konfiguriert.

**Empfehlung:** Übernehmen Sie eine Sniffer-Ablaufverfolgung auf dem Client-PC. Es ist keine spezielle Wireless-Software erforderlich, sondern nur Wireshark, das auf dem Wireless-Adapter ausgeführt wird und Ihnen anzeigt, ob der WLC antwortet und versucht, eine Umleitung vorzunehmen. Sie haben zwei Möglichkeiten: Entweder gibt es keine Antwort von WLC, oder es stimmt etwas nicht mit dem SSL-Handshake für die WebAuth-Seite. Bei einem SSL-Handshake können Sie überprüfen, ob der Benutzerbrowser SSLv3 zulässt (einige erlauben nur SSLv2) und ob die Zertifikatverifizierung zu aggressiv ist.

Es ist ein gängiger Schritt, http://192.0.2.1 manuell einzugeben, um zu überprüfen, ob die Webseite ohne DNS angezeigt wird. Eigentlich können Sie http://10.0.0.0 eingeben und den gleichen Effekt erzielen. Der WLC leitet alle eingegebenen IP-Adressen um. Wenn Sie daher http://192.0.2.1 eingeben, müssen Sie nicht an der Web-Umleitung arbeiten. Wenn Sie https://192.0.2.1 (sicher) eingeben, funktioniert dies nicht, da WLC den HTTPS-Verkehr nicht umleitet (dies ist in Version 8.0 und höher standardmäßig möglich). Die beste Möglichkeit, die Seite direkt ohne Umleitung zu laden, ist die Eingabe von https://192.0.2.1/login.html.

- **Benutzer können sich nicht authentifizieren**.

  Weitere Informationen finden Sie im Abschnitt dieses Dokuments zur Authentifizierung. Überprüfen Sie die Anmeldeinformationen lokal auf dem RADIUS.

- **Benutzer können sich erfolgreich über WebAuth authentifizieren, haben danach jedoch keinen Internetzugang mehr**.

  Sie können WebAuth aus der Sicherheit des WLAN entfernen, und dann haben Sie ein offenes WLAN. Sie können dann versuchen, auf das Internet, den DNS usw. zuzugreifen. Wenn auch hier Probleme auftreten, entfernen Sie die WebAuth-Einstellungen vollständig, und überprüfen Sie die Konfiguration Ihrer Schnittstellen.

Weitere Informationen finden Sie unter: Problembehandlung bei der Webauthentifizierung auf einem Wireless LAN Controller (WLC).

# HTTP-Proxy-Server und Funktionsweise

Sie können einen HTTP-Proxyserver verwenden. Wenn der Client in seinem Browser eine Ausnahme hinzufügen muss, die besagt, dass 192.0.2.1 nicht über den Proxyserver laufen soll, können Sie den WLC veranlassen, den HTTP-Verkehr auf dem Port des Proxyservers (in der Regel 8080) zu überwachen.

Um dieses Szenario zu verstehen, müssen Sie wissen, was ein HTTP-Proxy tut. Es handelt sich um etwas, das Sie auf der Client-Seite (IP-Adresse und Port) im Browser konfigurieren.

Das übliche Szenario, wenn ein Benutzer eine Website besucht, besteht darin, den Namen in IP mit DNS aufzulösen, und dann fragt er die Webseite an den Webserver. Der Prozess sendet immer die HTTP-Anfrage für die Seite an den Proxy.

Der Proxy verarbeitet ggf. den DNS und leitet ihn an den Webserver weiter (sofern die Seite nicht bereits auf dem Proxy zwischengespeichert ist). Die Diskussion findet nur zwischen Client und Proxy statt. Ob der Proxy die echte Webseite erhält oder nicht, ist für den Kunden irrelevant.

Dies ist der Web-Authentifizierungsprozess:

- Der Benutzer gibt eine URL ein.
- Client PC sendet Daten an den Proxy-Server.
- WLC fängt Proxy-Server-IP ab und imitiert diese. antwortet er dem PC mit einer Umleitung zu 192.0.2.1

Wenn der PC zu diesem Zeitpunkt nicht konfiguriert ist, fordert er den Proxy zur Eingabe der WebAuth-Seite 192.0.2.1 auf, damit diese nicht funktioniert. Der PC muss eine Ausnahme für 192.0.2.1 machen. sendet er eine HTTP-Anforderung an 192.0.2.1 und setzt WebAuth fort.

Bei der Authentifizierung werden alle Kommunikationen erneut über den Proxy geleitet. Eine Ausnahmekonfiguration befindet sich normalerweise im Browser in der Nähe der Konfiguration des Proxyservers. Dann wird die Meldung angezeigt: "Verwenden Sie keinen Proxy für diese IP-Adressen".

Ab WLC Version 7.0 bietet die **webauth proxy redirect** können in den globalen WLC-Konfigurationsoptionen aktiviert werden.

Wenn diese Funktion aktiviert ist, prüft der WLC, ob die Clients für die manuelle Verwendung eines Proxys konfiguriert sind. In diesem Fall leiten sie den Client auf eine Seite um, die ihnen zeigt, wie sie ihre Proxyeinstellungen ändern können, damit alles funktioniert.

Die WebAuth-Proxyumleitung kann für eine Vielzahl von Ports konfiguriert werden und ist mit der zentralen Webauthentifizierung kompatibel.

Ein Beispiel für die WebAuth-Proxy-Umleitung finden Sie unter Web Authentication Proxy on a Wireless LAN Controller Configuration Example.

### Webauthentifizierung über HTTP anstelle von HTTPS

Sie können sich bei der Webauthentifizierung über HTTP anstelle von HTTPS anmelden. Wenn Sie sich über HTTP anmelden, erhalten Sie keine Zertifikatswarnungen.

Bei älteren Versionen als WLC Version 7.2 müssen Sie die HTTPS-Verwaltung des WLC deaktivieren und die HTTP-Verwaltung beibehalten. Dies ermöglicht jedoch nur die Webverwaltung des WLC über HTTP.

Verwenden Sie für den WLC Release 7.2-Code den **config network web-auth secureweb disable** zu deaktivieren. Dies deaktiviert HTTPS nur für die Webauthentifizierung und nicht für die Verwaltung. Beachten Sie, dass hierfür ein Neustart des Controllers erforderlich ist!

Ab WLC Version 7.3 können Sie HTTPS für WebAuth nur über die Benutzeroberfläche und die Kommandozeile aktivieren/deaktivieren.

## Zugehörige Informationen

- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Software für Wireless Controller WebAuth-Pakete herunterladen
- Erstellen einer benutzerdefinierten Anmeldeseite für die Webauthentifizierung
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern

- Konfigurationsbeispiel für den Wireless LAN Controller 5760/3850 Web-Passthrough
- Konfigurieren der Webumleitung (GUI)
- Konfigurieren der Webumleitung (CLI)
- Problembehandlung bei der Webauthentifizierung auf einem Wireless LAN Controller (WLC)
- Webauthentifizierungsproxy auf einem Wireless LAN-Controller - Konfigurationsbeispiel
- Request For Comments (RFCs)
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.