



## IPv6 Web 認証の設定

---

- [IPv6 Web 認証の前提条件, 1 ページ](#)
- [IPv6 Web 認証の制限, 1 ページ](#)
- [IPv6 Web 認証について, 2 ページ](#)
- [IPv6 Web 認証の設定方法, 3 ページ](#)
- [IPv6 Web 認証の確認, 10 ページ](#)
- [その他の参考資料, 11 ページ](#)
- [IPv6 Web 認証の機能情報, 13 ページ](#)

## IPv6 Web 認証の前提条件

次の設定を、IPv6 Web 認証を開始する前に行う必要があります。

- IPv6 デバイス トラッキング
- IPv6 DHCP スヌーピング
- wlan 上の 802.1x タイプのセキュリティをディセーブルにします。
- 各 WLAN には、vlan が関連付けられている必要があります。
- デフォルトの wlan 設定を **shutdown** から **no shutdown** に変更します。

関連トピック

[WLAN のセキュリティのイネーブル化, \(5 ページ\)](#)

## IPv6 Web 認証の制限

次の制限は、IPv6 Web 認証の使用時に適用されます。

## 関連トピック

[WLAN のセキュリティのイネーブル化, \(5 ページ\)](#)

# IPv6 Web 認証について

Web 認証は、レイヤ 3 セキュリティ機能です。スイッチでは、有効なユーザー名とパスワードを入力するまで、特定のクライアントからの IP トラフィック（DHCP および DNS 関連パケットを除く）を拒否します。これはサブリカントまたはクライアントユーティリティを必要としないシンプルな認証方式です。一般に Web 認証は、ゲストアクセス ネットワークを展開する顧客が使用します。HTTP と HTTPS の両方からのトラフィックで、ページがログインページを表示できるようにします。



(注) Web 認証は、データ暗号化を提供せず、通常は、接続が常に重要になるホット スポットまたはキャンパス環境用のシンプルなゲスト アクセスとして使用されます。

WLAN は、Web ベース認証の **security webauth** として設定されます。スイッチは次のタイプの Web ベース認証をサポートしています。

- Web 認証：クライアントが Web ページにクレデンシャルを入力し、次に Wlan コントローラによって検証されます。
- Web 同意：Wlan コントローラは、[Accept/Deny] ボタンが用意されたポリシー ページを提供します。ネットワークにアクセスするには、[Accept] ボタンをクリックします。

一般に Wlan はオープン認証用に設定されます。つまり、レイヤ 2 認証なしで、Web ベースの認証メカニズムが使用されるときに設定されます。

## Web 認証プロセス

次のイベントは、WLAN が Web 認証用に設定されている場合に発生します。

- ユーザは、Web ブラウザを開き、URL アドレスとして、たとえば、*http://www.example.com* を入力します。クライアントは、この URL の DNS 要求を送信して、宛先の IP アドレスを取得します。スイッチは DNS 要求を DNS サーバにバイパスし、サーバは宛先 *www.example.com* の IP アドレスが含まれている DNS 応答で応答します。次にこれがワイヤレスクライアントに転送されます。
- クライアントは、宛先 IP アドレスで TCP 接続を開こうとします。*www.example.com* の IP アドレス宛ての TCP SYN パケットを送信します。
- スイッチにはクライアントに設定されたルールがあり、*www.example.com* のプロキシとして機能できません。*www.example.com* の IP アドレスとしての送信元とともにクライアントに TCP SYN-ACK パケットを戻します。クライアントは、スリーウェイ TCP ハンドシェイクを完了するために TCP ACK パケットを戻し、TCP 接続が完全に確立されます。

- クライアントは、*www.example.com* 宛での HTTP GET パケットを送信します。スイッチはこのパケットをインターセプトし、リダイレクト処理用に送信します。HTTP アプリケーションゲートウェイは、クライアントによって要求された HTTP GET への応答として、HTML 本文を準備し送信します。この HTML では、クライアントはスイッチのデフォルトの Web ページ（たとえば、*http://<Virtual-Server-IP>/login.html*）に転送されます。
- クライアントは、たとえば、*www.example.com* などの IP アドレスとの TCP 接続を閉じます。
- クライアントは仮想 IP に移動する場合に、スイッチの仮想 IP アドレスで TCP 接続を開こうとします。スイッチに、仮想 IP 用の TCP SYN パケットを送信します。
- スイッチは TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK をスイッチに戻します。
- クライアントは、ログインページの要求のために、仮想 IP 宛での */login.html* 用に HTTP GET を送信します。
- この要求は、スイッチの Web サーバで許可され、サーバはデフォルト ログイン ページで応答します。クライアントは、ユーザがログインできるブラウザ ウィンドウでログイン ページを受信します。

#### 関連トピック

- [WPA のディセーブル化, \(3 ページ\)](#)
- [WLAN のセキュリティのイネーブル化, \(5 ページ\)](#)
- [WLAN のパラメータ マップのイネーブル化, \(5 ページ\)](#)
- [WLAN の認証リストのイネーブル化, \(6 ページ\)](#)
- [グローバル Web 認証 WLAN パラメータ マップの設定, \(6 ページ\)](#)
- [WLAN の設定, \(7 ページ\)](#)
- [グローバル コンフィギュレーション モードの IPv6 のイネーブル化, \(9 ページ\)](#)
- [パラメータ マップの確認, \(10 ページ\)](#)
- [認証リストの確認, \(10 ページ\)](#)

## IPv6 Web 認証の設定方法

### WPA のディセーブル化

#### はじめる前に

802.1x をディセーブルにします。一般的な Web 認証では、レイヤ 2 セキュリティを使用しません。レイヤ 2 セキュリティを削除するには、この設定を使用します。

## 手順の概要

1. **configureterminal**
2. **wlan test1 2 test1**
3. **no security wpa**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configureterminal</b>  例： Switch# <b>configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<b>wlan test1 2 test1</b>  例： Switch(config)# wlan test1 2 test1	WLAN を作成し、SSID を割り当てます。
ステップ 3	<b>no security wpa</b>  例： Switch(config-wlan)# no security wpa	Wlan に対して WPA のサポートをディセーブルにします。

## 次の作業

次をイネーブルにします。

- セキュリティ Web 認証
- パラメータ ローカル
- 認証リスト

## 関連トピック

[Web 認証プロセス, \(2 ページ\)](#)

## WLAN のセキュリティのイネーブル化

### 手順の概要

1. `parameter-map type web-auth global`
2. `virtual-ip ipv4 192.0.2.1`
3. `virtual-ip ipv6 2001:db8::24:2`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>parameter-map type web-auth global</b>  例： Switch(config)# parameter-map type web-auth global	すべての Web 認証 wlan にパラメータ マップを適用します。
ステップ 2	<b>virtual-ip ipv4 192.0.2.1</b>  例： Switch(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1	仮想ゲートウェイの IPv4 アドレスを定義します。
ステップ 3	<b>virtual-ip ipv6 2001:db8::24:2</b>  例： Switch(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2	仮想ゲートウェイの IPv6 アドレスを定義します。

### 関連トピック

- [IPv6 Web 認証の前提条件, \(1 ページ\)](#)
- [IPv6 Web 認証の制限, \(1 ページ\)](#)
- [Web 認証プロセス, \(2 ページ\)](#)

## WLAN のパラメータ マップのイネーブル化

### 手順の概要

1. `security web-auth parameter-map <mapname>`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>security web-auth parameter-map &lt;mapname&gt;</b>  例 : Switch(config-wlan)# security web-auth parameter-map webparalocal	wlan 用の Web 認証をイネーブルにし、パラメータ マップを作成します。

## 関連トピック

[Web 認証プロセス, \(2 ページ\)](#)

## WLAN の認証リストのイネーブル化

## 手順の概要

### 1. security web-auth authentication-list webauthlistlocal

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>security web-auth authentication-list webauthlistlocal</b>  例 : Switch(config-wlan)# security web-auth	wlan 用の Web 認証をイネーブルにし、ローカル Web 認証リストを作成します。

## 関連トピック

[Web 認証プロセス, \(2 ページ\)](#)

## グローバル Web 認証 WLAN パラメータ マップの設定

この例を使用して、グローバル Web 認証 WLAN を設定し、パラメータ マップを追加します。

## 手順の概要

1. **parameter-map type webauth global**
2. **virtual-ip ipv6 2001:db8:4::1**
3. **ratelimit init-state-sessions 120**
4. **max-https-conns 70**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>parameter-map type webauth global</b>  例： Switch (config)# parameter-map type webauth global	グローバル Web 認証を設定し、パラメータ マップを追加します。
ステップ 2	<b>virtual-ip ipv6 2001:db8:4::1</b>  例： Switch (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1	認証用のワイヤレス クライアントに表示される仮想 ゲートウェイ IP アドレスを定義します。
ステップ 3	<b>ratelimit init-state-sessions 120</b>  例： Switch (config-params-parameter-map)# ratelimit init-state-sessions 120	グローバル レート制限を設定して、スイッチで Web クライアントが使用できる帯域幅を制限し、オーバーフラッディング攻撃を防止します。
ステップ 4	<b>max-https-conns 70</b>  例： Switch (config-params-parameter-map)# max-http-conns 70	オーバーフラッディング攻撃を防止するため、スイッチで試行される http 接続の最大数を設定します。

## 関連トピック

[Web 認証プロセス, \(2 ページ\)](#)

[WLAN の設定, \(7 ページ\)](#)

## WLAN の設定

## はじめる前に

- WLAN は、Vlan が関連付けられている必要があります。デフォルトでは、新しい Wlan は常に設定要件に応じて変更できる Vlan 1 に関連付けられます。

- WLAN を *no shutdown* に設定して、イネーブルにします。デフォルトでは、Wlan は *shutdown* パラメータで設定され、ディセーブルです。

## 手順の概要

1. **wlan 1**
2. **client vlan interface ID**
3. **security web-auth authentication list webauthlistlocal**
4. **security web-auth parameter-map global**
5. **no security wpa**
6. **no shutdown**
7. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>wlan 1</b>  例： Switch(config-wlan)# wlan 1 name vicweb ssid vicweb	wlan を作成し、SSID を割り当てます。
ステップ 2	<b>client vlan interface ID</b>  例： Switch(config-wlan)# client vlan VLAN0136	クライアントを wlan インターフェイスに割り当てます。
ステップ 3	<b>security web-auth authentication list webauthlistlocal</b>  例： Switch(config-wlan)# security web-auth authentication-list webauthlistlocal	wlan 用の Web 認証を設定します。
ステップ 4	<b>security web-auth parameter-map global</b>  例： Switch(config-wlan)# security web-auth parameter-map global	wlan にパラメータ マップを設定します。
ステップ 5	<b>no security wpa</b>  例： Switch(config-wlan)# no security wpa	wlan のセキュリティポリシーを設定します。これにより wlan がイネーブルになります。
ステップ 6	<b>no shutdown</b>  例： Switch(config-wlan)# no shutdown	Wlan を設定して、イネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。また、 <b>Ctrl+Z</b> キーを押しても、グローバル コンフィギュレーション モードを終了できます。

#### 関連トピック

[グローバル Web 認証 WLAN パラメータ マップの設定, \(6 ページ\)](#)

[Web 認証プロセス, \(2 ページ\)](#)

[グローバル コンフィギュレーション モードの IPv6 のイネーブル化, \(9 ページ\)](#)

## グローバル コンフィギュレーション モードの IPv6 のイネーブル化

Web 認証用にグローバル コンフィギュレーションの IPv6 をイネーブルにします。

#### 手順の概要

1. **configure terminal**
2. **web-auth global**
3. **virtual IPv6**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>web-auth global</b>  例： Switch(config)# <b>parameter-map type</b> <b>webauth global</b>	パラメータ マップのタイプを Web 認証としてグローバルに設定します。
ステップ 3	<b>virtual IPv6</b>  例： Switch(config-params-parameter-map)# <b>virtual-ip ipv6</b>	Web 認証用の仮想 IP として IPv6 を選択します。 (注) Web 認証用の優先 IP として IPv4 を選択することもできます。

## 関連トピック

[WLAN の設定, \(7 ページ\)](#)[Web 認証プロセス, \(2 ページ\)](#)[パラメータ マップの確認, \(10 ページ\)](#)

## IPv6 Web 認証の確認

### パラメータ マップの確認

Wlan に対して設定したパラメータ マップを確認するには、**show running configuration** コマンドを使用します。

## 手順の概要

**1. show running config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>show running config</b>  例： Switchshow running config	スイッチの実行コンフィギュレーション全体を表示します。パラメータマップのグレップを行い結果を表示します。

```
wlan alpha 2 alpha
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauthlistlocal
security web-auth parameter-map webparalocal
```

## 関連トピック

[グローバル コンフィギュレーション モードの IPv6 のイネーブル化, \(9 ページ\)](#)[Web 認証プロセス, \(2 ページ\)](#)[認証リストの確認, \(10 ページ\)](#)

### 認証リストの確認

Wlan に対して設定した認証リストを確認するには、**show running configuration** コマンドを使用します。

## 手順の概要

1. **show running configuration**
2. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>show running configuration</b>  例： Switch#show running-config	Wlan の設定を表示します。  Switch# show running-config
ステップ 2	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。また、 <b>Ctrl+Z</b> キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch#show running-config
.....
.....
.....
wlan alpha 2 alpha
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauthlistlocal
security web-auth parameter-map webparalocal
.....
.....
```

## 関連トピック

[パラメータ マップの確認, \(10 ページ\)](#)

[Web 認証プロセス, \(2 ページ\)](#)

## その他の参考資料

## 関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	<i>IPv6 Command Reference (Catalyst 3850 Switches)</i> <i>IPv6 Command Reference (Cisco WLC 5700 Series)</i>

関連項目	マニュアル タイトル
Web 認証設定	<i>Security Configuration Guide (Catalyst 3850 Switches)</i> <i>Security Configuration Guide (Cisco WLC 5700 Series)</i>

### エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

### MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### シスコのテクニカル サポート

説明	Link
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## IPv6 Web 認証の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 Web 認証機能	Cisco IOS XE 3.2SE	この機能が導入されました。

