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 （8 ページ）
- その他の参考資料 （10 ページ）
- IPv6 Web 認証の機能情報 （11 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 （4 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 （4 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。デバイスでは、有効なユーザ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。これはサプ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。デバイスは次のタイプの 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。

（注） デバイスでサポートされる Web 認証の最大連続セッションは 1 秒間に 40 個です。

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。デバイスは 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。
- デバイス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* 宛ての HTTP GET パケットを送信します。デバイス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、クライアントはデバイスのデフォルトの 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、デバイスの仮想 IP アドレスで TCP 接続を開こうとします。デバイスに、仮想 IP 用の TCP SYN パケットを送信します。
- デバイスは 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 をデバイスに戻します。
- クライアントは、ログイン ページの要求のために、仮想 IP 宛ての */login.html* 用に HTTP GET を送信します。
- この要求は、デバイスの 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 （4 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 （5 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 （6 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 （8 ページ）
パラメータ マップの確認 （8 ページ）
認証リストの確認 （9 ページ）

IPv6 Web 認証の設定方法

WPA のディセーブル化

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	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	**wlan test1 2 test1** 例： `Device(config)# wlan test1 2 test1`	WLAN を作成し、SSID を割り当てます。
ステップ 3	**no security** wpa 例： `Device(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。

次のタスク

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

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type web-auth global** 例： `Device(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	**virtual-ip ipv4 192.0.2.1** 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 3	**virtual-ip ipv6 2001:db8::24:2** 例： `Device(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

	コマンドまたはアクション	目的
ステップ 1	**security web-auth parameter-map <mapname>** 例： `Device(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

	コマンドまたはアクション	目的
ステップ 1	**security web-auth authentication-list webauthlistlocal** 例： `Device(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

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type webauth global** 例： `Device (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	**virtual-ip ipv6 2001:db8:4::1** 例： `Device (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	**ratelimit init-state-sessions 120** 例： `Device (config-params-parameter-map)# ratelimit init-state-sessions 120`	グローバル レート制限を設定して、デバイスで 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	**max-https-conns 70** 例： `Device (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、デバイスで試行される 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 （6 ページ）

WLAN の設定

始める前に

- 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

	コマンドまたはアクション	目的
ステップ 1	**wlan** *1* 例： `Device(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	**client vlan** *interface ID* 例： `Device(config-wlan)# client vlan VLAN0136`	クライアントを vlan インターフェイスに割り当てます。
ステップ 3	**security web-auth authentication list webauthlistlocal** 例： `Device(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	**security web-auth parameter-map global** 例： `Device(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	**no security wpa** 例： `Device(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	**no shutdown** 例： `Device(config-wlan)# no shutdown`	Wlanを設定して、イネーブルにします。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z 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 （8 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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	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	**web-auth global** 例： `Device(config)# parameter-map type webauth global`	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	**virtual IPv6** 例： `Device(config-params-parameter-map)# virtual-ip ipv6`	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 （6 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 （8 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

	コマンドまたはアクション	目的
ステップ 1	**show running config** 例： `Deviceshow running config`	デバイス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 （8 ページ）
Web 認証プロセス （2 ページ）
認証リストの確認 （9 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

	コマンドまたはアクション	目的
ステップ 1	**show running configuration** 例： `Device#show running-config`	Wlan の設定を表示します。 `Device# show running-config`
ステップ 2	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z 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。

```
Device#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 （8 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	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
Web 認証設定	『*Security Configuration Guide (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
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。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/support

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。