



Web ベース認証

この章では、デバイスで Web ベース認証を設定する方法について説明します。この章の内容は、次のとおりです。

- [認証の概要 \(1 ページ\)](#)
- [ローカル Web 認証の設定方法 \(9 ページ\)](#)
- [無線による管理機能について \(15 ページ\)](#)
- [ローカル Web 認証の設定例 \(16 ページ\)](#)

認証の概要

IEEE 802.1x サプリカントが実行されていないホストシステムでエンドユーザーを認証するには、Web 認証プロキシとして知られている 認証機能を使用します。



(注) Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTPセッションを開始すると、認証は、ホストからの入力HTTPパケットを代行受信し、ユーザーにHTMLログインページを送信します。ユーザーはクレデンシャルを入力します。このクレデンシャルは、認証機能により、認証のために認証、許可、アカウントिंग (AAA) サーバーに送信されます。

認証に成功した場合、認証は、ログインの成功を示すHTMLページをホストに送信し、AAAサーバーから返されたアクセスポリシーを適用します。

認証に失敗した場合、認証は、ログインの失敗を示すHTMLページをユーザーに転送し、ログインを再試行するように、ユーザーにプロンプトを表示します。最大試行回数を超過した場合、認証は、ログインの期限切れを示すHTMLページをホストに転送し、このユーザーは、



- (注) Webauth クライアントの認証試行時に受信する `traceback` には、パフォーマンスや行動への影響はありません。これは、ACL アプリケーションの EPM に FFM が返信したコンテキストがすでにキュー解除済み（タイマーの有効期限切れの可能性あり）で、セッションが「未承認」になった場合にまれに発生します。

Web ページがホストされている場所に基づいて、ローカル Web 認証は次のように分類できます。

- 内部：ローカル Web 認証時に、組み込みワイヤレスコントローラの内部デフォルト HTML ページ（ログイン、成功、失敗、および期限切れ）が使用されます。
- カスタマイズ：ローカル Web 認証時に、カスタマイズされた Web ページ（ログイン、成功、失敗、および期限切れ）が組み込みワイヤレスコントローラにダウンロードされ、使用されます。
- 外部：組み込みまたはカスタム Web ページを使用する代わりに、外部 Web サーバー上でカスタマイズされた Web ページがホストされます。

さまざまな Web 認証ページに基づき、Web 認証のタイプは次のように分類できます。

- *Webauth*：これが基本的な Web 認証です。この場合、組み込みワイヤレスコントローラはユーザー名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザーは正しいクレデンシャルを入力する必要があります。
- *Consent* または *web-passthrough*：この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンが表示されたポリシー ページを提示します。ネットワークにアクセスするには、ユーザーは [Accept] ボタンをクリックする必要があります。
- *Webconsent*：これは *webauth* と *consent* の Web 認証タイプの組み合わせです。この場合、組み込みワイヤレスコントローラは、[Accept] ボタンまたは [Deny] ボタンがあり、ユーザー名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザーは正しいクレデンシャルを入力して [Accept] ボタンをクリックする必要があります。



- (注)
- `webauth` パラメータマップ情報は、`show running-config` コマンドの出力を使用して表示できます。
 - ワイヤレス Web 認証機能は、バイパス タイプをサポートしていません。
 - AP の再接続が発生するまで、Web 認証パラメータマップのリダイレクトログイン URL の変更は発生しません。新しい URL リダイレクションを適用するには、WLAN を有効または無効にする必要があります。



- (注) カスタマイズされた Web 認証ログインページを作成する場合は、シスコのガイドラインに従うことをお勧めします。Google Chrome または Mozilla Firefox ブラウザの最新バージョンにアップグレードした場合は、Web 認証バンドルの login.html ファイルに次の行が含まれていることを確認します。

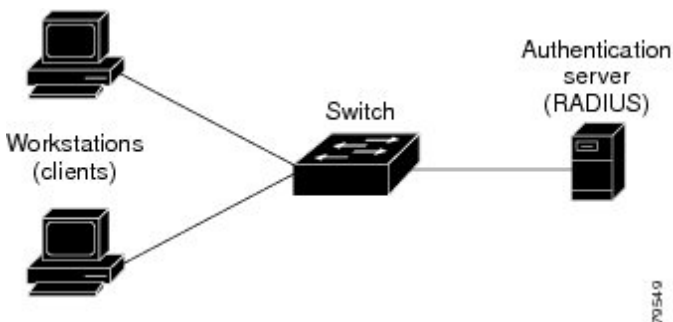
```
<body onload="loadAction();">
```

デバイスのロール

ローカル Web 認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：ネットワークおよびコントローラへのアクセスを要求し、コントローラからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script が有効な HTML ブラウザが実行されている必要があります。
- 認証サーバー：クライアントを認証します。認証サーバーはクライアントの ID を確認し、そのクライアントにネットワークおよびコントローラサービスへのアクセスを許可するか、そのクライアントを拒否するかをコントローラに通知します。
- コントローラ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。コントローラはクライアントと認証サーバーとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、識別情報を認証サーバーで確認し、クライアントに応答をリレーします。

図 1: ローカル Web 認証のデバイスの役割



認証プロセス

ローカル Web 認証を有効にすると、次のイベントが発生します。

- ユーザーが HTTP セッションを開始します。
- HTTP トラフィックが横取りされ、認証が開始されます。スイッチは、ユーザーにログインページを送信します。ユーザーはユーザー名とパスワードを入力します。スイッチはこのエントリを認証サーバーに送信します。

- 認証に成功した場合、スイッチは認証サーバーからこのユーザーのアクセスポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザーに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザーはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期限切れページを送信します。このホストはウォッチリストに入れられます。ウォッチリストのタイムアウト後、ユーザーは認証プロセスを再試行することができます。
- 認証サーバーを利用できない場合、Web 認証が再試行された後、クライアントは除外状態に移行し、クライアントに [Authentication Server is Unavailable] ページが表示されます。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドルタイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- クライアントにはすでに IP アドレスが割り当てられており、VLAN が変更された場合はクライアントの IP アドレスを変更できないため、Web 認証セッションは認証ポリシーの一部として新しい VLAN を適用できません。
- Termination-Action が RADIUS である場合、この機能は、サーバーに NRH 要求を送信します。Termination-Action は、サーバーからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザバナーを作成して、コントローラにログインしたときに表示されるようにできます。

このバナーは、ログインページと認証結果ポップアップページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

- 認証成功
- 認証失敗
- 認証期限切れ

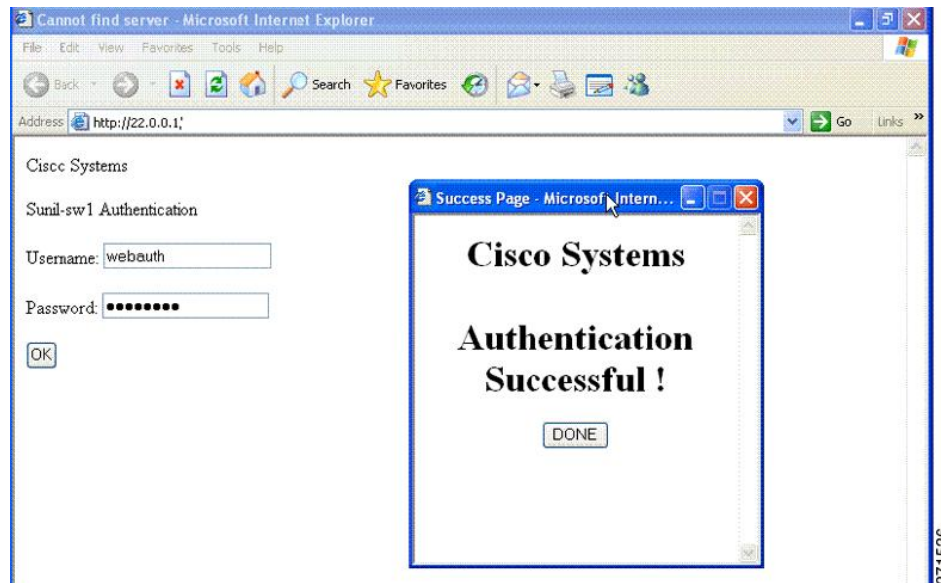
ローカル Web 認証バナーは、次のように設定できます。

- 次のグローバル コンフィギュレーション コマンドを使用します。

```
Device(config)# parameter map type webauth global
Device(config-params-parameter-map)# banner ?
file <file-name>
text <Banner text>
title <Banner title>
```

ログインページには、デフォルトのバナー、Cisco Systems、および Switch host-name Authentication が表示されます。Cisco Systems は認証結果ポップアップ ページに表示されます。

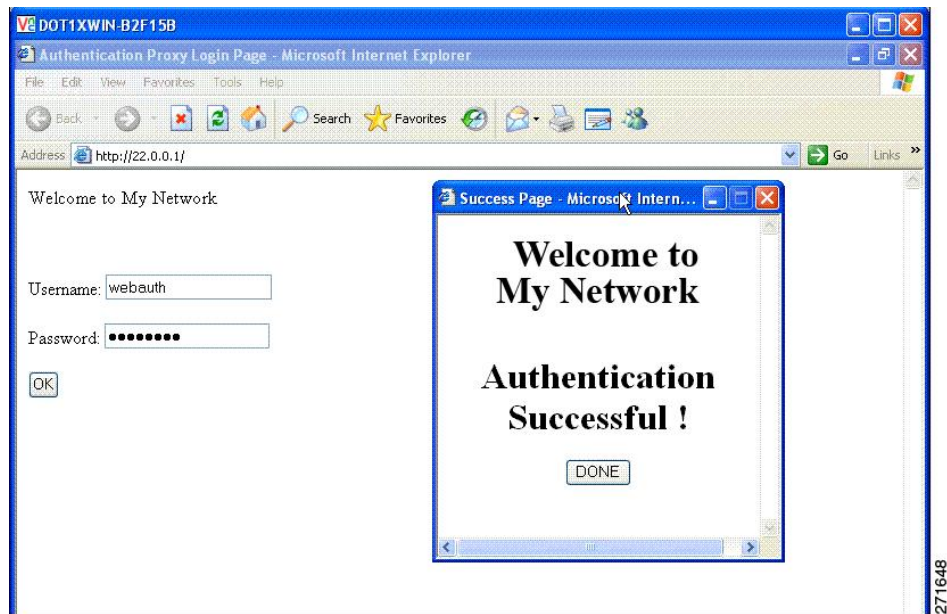
図 2: 認証成功バナー



バナーは次のようにカスタマイズ可能です。

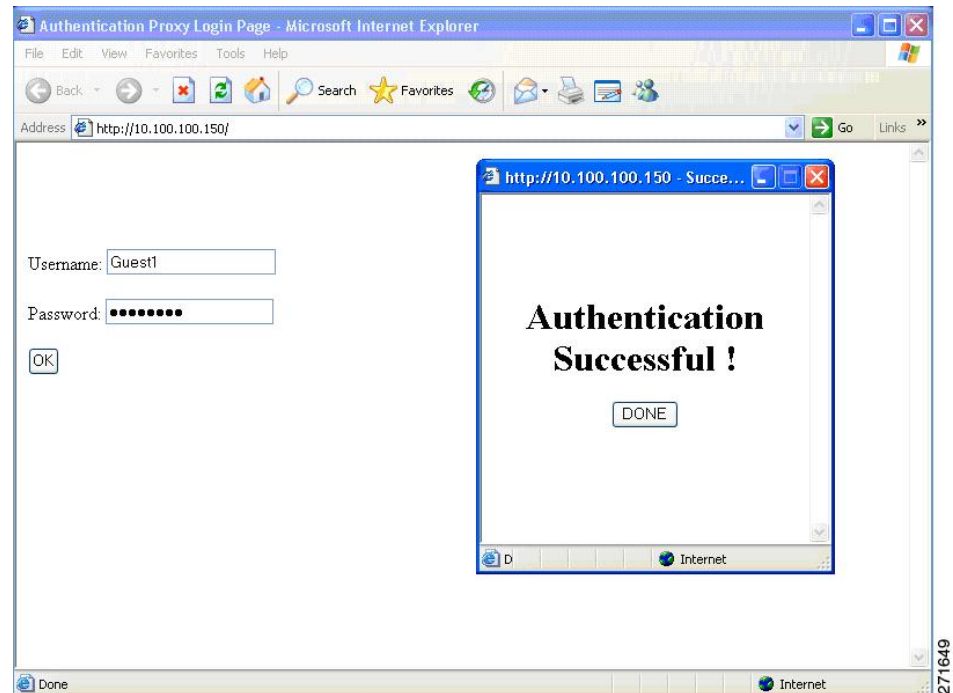
- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
 - 新スタイルモード：次のグローバルコンフィギュレーションコマンドを使用します。
parameter-map type webauth global
banner text <text>
- ログまたはテキスト ファイルをバナーに追加する。
 - 新スタイルモード：次のグローバルコンフィギュレーションコマンドを使用します。
parameter-map type webauth global
banner file <filepath>

図 3: カスタマイズされた Web バナー



バナーが有効にされていない場合、Web 認証ログイン画面にはユーザー名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 4: バナーが表示されていないログイン画面



カスタマイズされたローカル Web 認証

ローカル Web 認証プロセスでは、スイッチ内部の HTTP サーバーは、認証中のクライアントに配信される4種類のHTMLページをホストします。サーバーはこれらのページを使用して、ユーザーに次の4種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになりました。



(注) カスタム Web 認証を設定するには、仮想 IP アドレスが必要です。

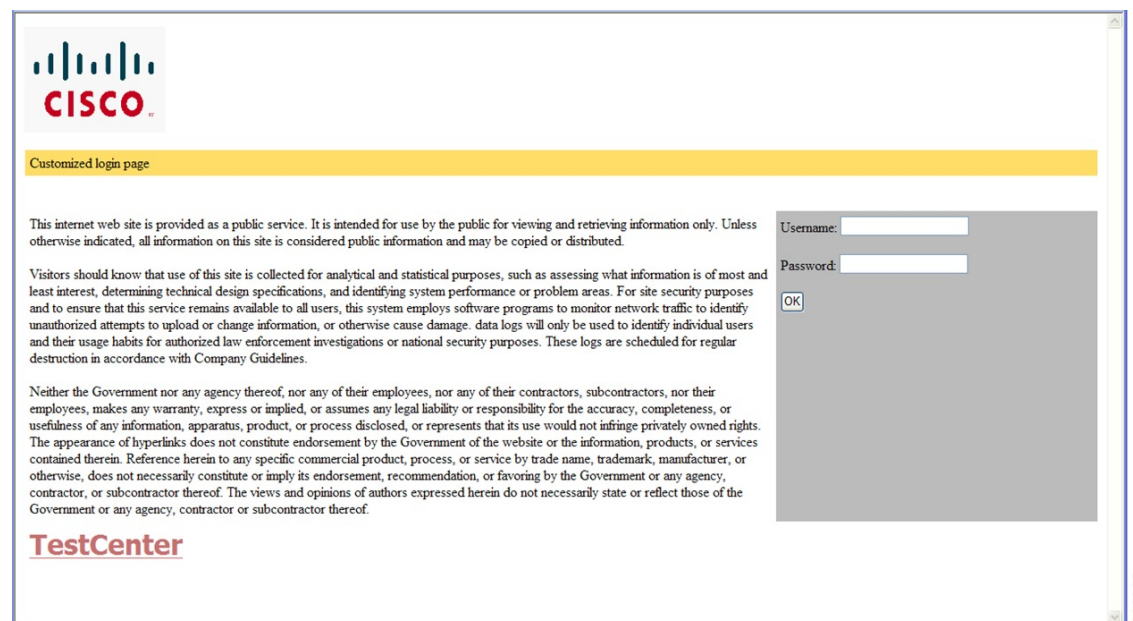
ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL (例: `http://www.cisco.com`) でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド (例: ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが2回送信されていないことの確認など) を記入する必要があります。
- 設定されたログイン フォームが有効な場合、特定の URL にユーザーをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザーをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザーをリダイレクトする CLI コマンドは効力を持ちません。

- 設定された Web ページは、スイッチのブートフラッシュ、またはフラッシュにコピーできます。
- ログインページを任意のフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、アクティブスイッチ、またはメンバスイッチのフラッシュ）に配置できます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システムディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログインページに表示する必要があるロゴファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、`web_auth_<filename>` の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部 HTML ページの代わりに、自分の HTML ページを使用することができます。認証後のユーザーのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 5: カスタマイズ可能な認証ページ



成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。

- リダイレクション URL 機能が有効に設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL (たとえば http://) で開始し、その後に URL 情報が続く必要があります。http://を含まない URL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

ローカル Web 認証の設定方法

デフォルトのローカル Web 認証の設定

次の表に、ローカル Web 認証に必要なデフォルト設定を示します。

表 1: デフォルトのローカル Web 認証の設定

機能	デフォルト設定
AAA	無効
RADIUS サーバ <ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • キー 	<ul style="list-style-type: none"> • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	ディセーブル

AAA 認証の設定 (GUI)



(注) WebUI は、AAA RADIUS サーバグループ設定における ipv6 radius source-interface をサポートしていません。

手順

-
- ステップ 1 [Configuration] > [Security] > [AAA] の順に選択します。
- ステップ 2 [Authentication] セクションで [Add] をクリックします。
- ステップ 3 表示される [Quick Setup: AAA Authentication] ウィンドウに、メソッドリストの名前を入力します。
- ステップ 4 ネットワークへのアクセスを許可する前に実行する認証のタイプを [Type] ドロップダウン リストから選択します。
- ステップ 5 [Group Type] ドロップダウン リストから、サーバーのグループをアクセス サーバーとして割り当てるか、またはローカル サーバーを使用してアクセスを認証するかを選択します。
- ステップ 6 グループ内のサーバーが使用できない場合にフォールバック方式として機能するようにローカル サーバーを設定するには、[Fallback to local] チェックボックスをオンにします。
- ステップ 7 [Available Server Groups] リストで、ネットワークへのアクセスの認証に使用するサーバー グループを選択し、[>] アイコンをクリックして [Assigned Server Groups] リストに移動します。
- ステップ 8 [Save & Apply to Device] をクリックします。
-

AAA 認証の設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	aaa new-model 例 : デバイス(config)# aaa new-model	AAA 機能をイネーブルにします。
ステップ 2	aaa authentication login {default named_authentication_list} group AAA_group_name 例 : デバイス(config)# aaa authentication login default group group1	ログイン時の認証方法のリストを定義します。 named_authentication_list は、31 文字未満の名前を示します。 AAA_group_name はサーバー グループ名を示します。サーバーグループ server_name をその先頭で定義する必要があります。
ステップ 3	aaa authorization network {default named} group AAA_group_name 例 :	Web ベース許可の許可方式リストを作成します。

	コマンドまたはアクション	目的
	<pre>デバイス(config)# aaa authorization network default group group1</pre>	
ステップ 4	<p>tacacs-server host {hostname ip_address}</p> <p>例 :</p> <pre>デバイス(config)# tacacs-server host 10.1.1.1</pre>	AAA サーバーを指定します。

HTTP/HTTPS サーバーの設定 (GUI)

手順

-
- ステップ 1** [Administration] > [Management] > [HTTP/HTTPS/Netconf] の順に選択します。
- ステップ 2** [HTTP/HTTPS Access Configuration] セクションで、[HTTP Access] を有効にして、HTTP 要求をリッスンするポートを入力します。デフォルトのポートは 80 です。有効な値は、80 または 1025 ~ 65535 の値です。
- ステップ 3** デバイスで [HTTPS Access] を有効にし、HTTPS 要求をリッスンする指定ポートを入力します。デフォルトのポートは 1025 です。有効な値は、443 または 1025 ~ 65535 の値です。セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。
- ステップ 4** [Personal Identity Verification] について [enabled] または [disabled] を選択します。
- ステップ 5** [HTTP Trust Point Configuration] セクションで、[Enable Trust Point] を有効にして、認証局サーバーをトラストポイントとして使用します。
- ステップ 6** [Trust Points] ドロップダウンリストから、トラストポイントを選択します。
- ステップ 7** [Timeout Policy Configuration] セクションで、HTTP タイムアウトポリシーを秒単位で入力します。有効な値の範囲は、10 ~ 600 秒です。
- ステップ 8** セッションがタイムアウトするまでに許容される非アクティブな時間 (分数) を入力します。有効な値の範囲は、180 ~ 1200 秒です。
- ステップ 9** サーバーの有効期間を秒単位で入力します。有効値の範囲は、1 ~ 86400 秒です。
- ステップ 10** デバイスが受け取ることのできる要求の最大数を入力します。有効値の範囲は、1 ~ 86400 件です。
- ステップ 11** 設定を保存します。
-

HTTP サーバーの設定 (CLI)

ローカル Web 認証を使用するには、デバイス内で HTTP サーバーを有効にする必要があります。このサーバーは HTTP または HTTPS のいずれかについて有効にできます。



(注) Apple の疑似ブラウザは、**ip http secure-server** コマンドを設定するだけでは開きません。**ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかについてサーバーを有効にするには、次の手順に従います。

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# Device# configure terminal	グローバル設定モードを開始します。
ステップ 2	ip http server 例： Device(config)# ip http server	HTTP サーバーを有効にします。ローカル Web 認証機能は、HTTP サーバーを使用してホストと通信し、ユーザー認証を行います。
ステップ 3	ip http secure-server 例： Device(config)# ip http secure-server	HTTPS を有効にします。 カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。 (注) ip http secure-server コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザーが HTTP 要求を送信した場合でも、ログインページは必ず HTTPS (セキュア HTTP) 形式になるようにします。
ステップ 4	end 例： Device(config)# end	設定モードを終了します。

パラメータマップの作成 (GUI)

手順

- ステップ 1 [Configuration] > [Security] > [Web Auth] の順に選択します。
- ステップ 2 [Add] をクリックします。
- ステップ 3 [Policy Map] をクリックします。
- ステップ 4 [Parameter Name]、[Maximum HTTP connections]、[Init-State Timeout(secs)] を入力し、[Type] ドロップダウンリストで [webauth] を選択します。
- ステップ 5 [Apply to Device] をクリックします。

Web 認証要求の最大再試行回数の設定

最大 Web 認証要求再試行回数を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： デバイス# 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	configure terminal 例： デバイス# 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 3	wireless security web-auth retries number 例： デバイス(config)# wireless security web-auth retries 2	<i>number</i> は Web 認証要求の最大試行回数です。有効な範囲は 0 ~ 20 です。
ステップ 4	end 例： デバイス(config)# end	特権 EXEC モードに戻ります。

Web 認証ページ内のローカル バナーの設定 (GUI)

手順

ステップ 1 [Configuration] > [Security] > [Web Auth] の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [General] タブで、必要なバナー タイプを選択します。

- [Banner Text] を選択した場合は、表示するバナー テキストを入力します。
- [File Name] を選択した場合は、バナー テキストを取得する取得元のファイルのパスを指定します。

ステップ 4 [Update & Apply] をクリックします。

Web 認証ページ内のローカル バナーの設定 (CLI)

Web 認証ページ内のローカル バナーを設定するには、次の手順に従います。

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	parameter-map type webauth param-map 例： Device(config)# parameter-map type webauth param-map	Web 認証パラメータを設定します。パラメータ マップ コンフィギュレーション モードを開始します。
ステップ 3	banner [file banner-text title] 例： Device(config-params-parameter-map)# banner http C My Switch C	ローカル バナーを有効にします。 C banner-text C (C は区切り文字)、バナーに表示されるファイル (ロゴやテキストファイル) の file、またはバナーのタイトルを示す title を入力して、カスタムバナーを作成します。
ステップ 4	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device (config-params-parameter-map) # end	

無線による管理機能について

無線による管理機能を使用すると、ワイヤレスクライアントを使用してローカル組み込みワイヤレスコントローラを監視および設定できます。組み込みワイヤレスコントローラとの間のアップロードおよびダウンロード（転送）を除くすべての管理タスクを実行できます。

無線による管理機能の制限

- 無線による管理機能は、クライアントが中央スイッチングの場合にのみ無効にできます。

無線による管理機能の設定（GUI）

手順

-
- ステップ 1 [Configuration] > [Wireless] > [Wireless Global] を選択します。
- ステップ 2 [Management Via Wireless] チェックボックスをオンにして機能を有効にします。
- ステップ 3 [Apply] をクリックします。
-

無線による管理機能の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： デバイス# 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	[no] wireless mgmt-via-wireless 例： デバイス (config)# wireless mgmt-via-wireless	ワイヤレス クライアント経由の管理アクセスを有効にします。

	コマンドまたはアクション	目的
ステップ 3	end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 4	show running-config include mgmt-via-wireless 例： デバイス# show running-config include mgmt-via-wireless	ワイヤレス クライアント経由の管理アクセスのステータスを確認します。

ローカル Web 認証の設定例

例：Web 認証証明書の手入

次の例は、Web 認証証明書を取得する方法を示しています。

```

デバイス# configure terminal
デバイス(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco

デバイス(config)# end
デバイス# show crypto pki trustpoints cert
Trustpoint cert:
  Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
    Serial Number (hex): 00
  Certificate configured.
デバイス# show crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco

```



```
st=California
c=US
Validity Date:
  start date: 07:35:23 UTC Jan 31 2012
  end   date: 07:35:23 UTC Jan 28 2022
Associated Trustpoints: cert ldap12
Storage: nvram:rkannajrcisc#4.cer

CA Certificate
Status: Available
Certificate Serial Number (hex): 00
Certificate Usage: General Purpose
Issuer:
  e=rkannajr@cisco.com
  cn=sthaliya-lnx
  ou=WNBU
  o=Cisco
  l=SanJose
  st=California
  c=US
Subject:
  e=rkannajr@cisco.com
  cn=sthaliya-lnx
  ou=WNBU
  o=Cisco
  l=SanJose
  st=California
  c=US
Validity Date:
  start date: 07:27:56 UTC Jan 31 2012
  end   date: 07:27:56 UTC Jan 28 2022
Associated Trustpoints: cert ldap12 ldap
Storage: nvram:rkannajrcisc#0CA.cer
```

例 : Web 認証証明書の表示

次の例は、Web 認証証明書を表示する方法を示しています。

```
デバイス# show crypto ca certificate verb
Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 2A9636AC00000000858B
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA
o=Cisco Systems
Subject:
Name: WS-C3780-6DS-S-2037064C0E80
Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
cn=WS-C3780-6DS-S-2037064C0E80
serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca.crl
Validity Date:
start date: 15:43:22 UTC Aug 21 2011
end   date: 15:53:22 UTC Aug 21 2021
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
```

例：デフォルトの Web 認証ログイン ページの選択

```

Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
X509v3 Key Usage: F0000000
    Digital Signature
    Non Repudiation
    Key Encipherment
    Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI

```

例：デフォルトの Web 認証ログイン ページの選択

次の例は、デフォルトの Web 認証ログイン ページを選択する方法を示しています。

```

デバイス# configure terminal
デバイス(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their
CPL control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
デバイス(config)# wlan wlan50
デバイス(config-wlan)# shutdown
デバイス(config-wlan)# security web-auth authentication-list test
デバイス(config-wlan)# security web-auth parameter-map test
デバイス(config-wlan)# no shutdown
デバイス(config-wlan)# end
デバイス# show running-config | section wlan50
wlan wlan50 50 wlan50
  security wpa akm cckm
  security wpa wpa1
  security wpa wpa1 ciphers aes
  security wpa wpa1 ciphers tkip
  security web-auth authentication-list test
  security web-auth parameter-map test
  session-timeout 1800
  no shutdown

デバイス# show running-config | section parameter-map type webauth test
parameter-map type webauth test
  type webauth

```

例：IPv4 外部 Web サーバーでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、IPv4 外部 Web サーバーからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth global
デバイス(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
デバイス(config-params-parameter-map)# parameter-map type webauth test
デバイス(config-params-parameter-map)# type webauth
デバイス(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
デバイス(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：IPv6 外部 Web サーバーでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、IPv6 外部 Web サーバーからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
デバイス# configure terminal
デバイス(config)# parameter-map type webauth global
デバイス(config-params-parameter-map)# virtual-ip ipv6 1:1:1::1
デバイス(config-params-parameter-map)# parameter-map type webauth test
デバイス(config-params-parameter-map)# type webauth
デバイス(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
デバイス(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 1:1:1::1
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：WLAN ごとのログインページ、ログイン失敗ページ、およびログアウト ページの割り当て

次の例は、WLAN ごとのログイン割り当て、ログイン失敗、およびログアウト ページを割り当てる方法を示しています。

```

デバイス# configure terminal
デバイス(config)# parameter-map type webauth test
デバイス(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
デバイス(config-params-parameter-map)# custom-page login expired device
flash:loginexpire.html
デバイス(config-params-parameter-map)# custom-page failure device flash:loginfail.html
デバイス(config-params-parameter-map)# custom-page success device flash:loginsucess.html
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
custom-page login device flash:loginsantosh.html
custom-page success device flash:loginsucess.html
custom-page failure device flash:loginfail.html
custom-page login expired device flash:loginexpire.html

```

例：事前認証 ACL の設定

次の例は、事前認証 ACL を設定する方法を示しています。

```

デバイス# configure terminal
デバイス(config)# wlan fff
デバイス(config-wlan)# shutdown
デバイス(config-wlan)# ip access-group web preauthrule
デバイス(config-wlan)# no shutdown
デバイス(config-wlan)# end
デバイス# show wlan name fff

```

例：Webpassthrough の設定

次の例は、Webpassthrough を設定する方法を示しています。

```

デバイス# configure terminal
デバイス(config)# parameter-map type webauth webparalocal
デバイス(config-params-parameter-map)# type consent
デバイス(config-params-parameter-map)# end
デバイス# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100

```

Web 認証タイプの確認

Web 認証タイプを確認するには、次のコマンドを実行します。

```

Device# show parameter-map type webauth all
Type Name
-----

```

```
Global global
Named webauth
Named ext
Named redirect
Named abc
Named glbal
Named ewa-2
wlc-tunga#sh parameter-map type webauth global
Parameter Map Name : global
Banner:
Text : CisCo
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Enabled
Sleeping-Client timeout : 60 min
Virtual-ipv4 : 1.1.1.1
Virtual-ipv4 hostname :
Webauth intercept https : Disabled
Webauth Captive Bypass : Disabled
Webauth bypass intercept ACL :
Trustpoint name :
HTTP Port : 80
Watch-list:
Enabled : no
Webauth login-auth-bypass:

Device# show parameter-map type webauth name global
Parameter Map Name : global
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Disabled
Webauth login-auth-bypass:
```

