



Web ベース認証の設定

- [Web ベース認証について \(1 ページ\)](#)
- [Web ベース認証の設定方法 \(11 ページ\)](#)
- [Web ベース認証の確認 \(24 ページ\)](#)
- [Web ベース認証に関するその他の参考資料 \(24 ページ\)](#)

Web ベース認証について

Web ベース認証の概要

IEEE 802.1x サブ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を認証するには、Web 認証プロキシとして知られている Web ベース認証機能を使用します。

HTTP セッションを開始すると、Web ベース認証は、ホストからの受信 HTTP パケットを横取りし、ユーザに HTML ログインページを送信します。ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウントイング (AAA) サーバに送信されます。

認証が成功すると、Web ベース認証はログイン成功 HTML ページをホストに送信し、AAA サーバ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、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザ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、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。



(注) 中央 Web 認証リダイレクト用の HTTPS トラフィック インターセプションはサポートされていません。



(注) グローバルパラメータマップ (method-type、custom、redirect) は、すべてのクライアントおよび SSID で同じ Web 認証方式 (consent、web consent、webauth など) を使用するときのみ使用する必要があります。これにより、すべてのクライアントが同じ Web 認証方式になります。

要件により、1つの SSID に consent、別の SSID に webauth を使用する場合、名前付きパラメータマップを 2 つ使用する必要があります。1 番目のパラメータマップには consent を設定し、2 番目のパラメータマップには webauth を設定する必要があります。



(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、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 サーバ上でカスタマイズされた Web ページがホストされます。



(注) このリリースでは、外部 Web 認証はサポートされていません。

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、コントローラはユーザ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、コントローラは [Accept] ボタンとともにユーザ名とパスワード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。

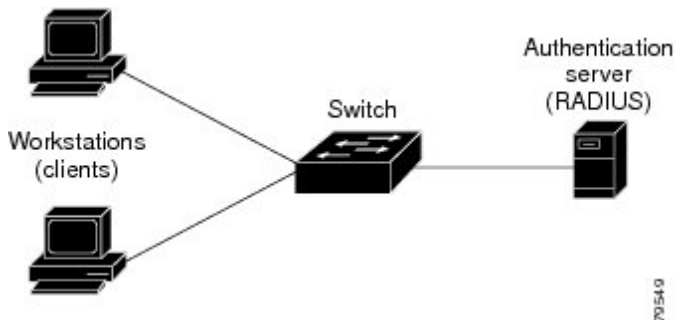
デバイスのロール

Web ベース認証では、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：LAN およびサービスへのアクセスを要求し、スイッチ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：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：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。スイッチはクライアントと認証サーバとの仲介デバイス（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、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 1: Web ベース認証デバイスの役割

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。



ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイス追跡 テーブルを維持します。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP 検査
- DHCP スヌーピング：スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されません。

- 例外リストをレビューします。

ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。

- 認証バイパスをレビューします。

ホスト IP が例外リストに含まれていない場合、Web ベース認証は応答しないホスト (NRH) 要求をサーバに送信します。

サーバの応答が **access accepted** であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL を設定します。

NRH 要求に対するサーバの応答が **access rejected** であった場合、HTTP インターセプト ACL がアクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証を有効にすると、次のイベントが発生します。

- ユーザが 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、ユーザにログイン ページを送信します。ユーザはユーザ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からこのユーザ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。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセスポリシーを適用します。ログインの成功ページがユーザに送信 されます。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに回答しなかった場合、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。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに回答しない場合、スイッチはク ライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信しま す。Termination-Action は、サーバ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、スイッチにログインしたときに表示するようにできます。

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。

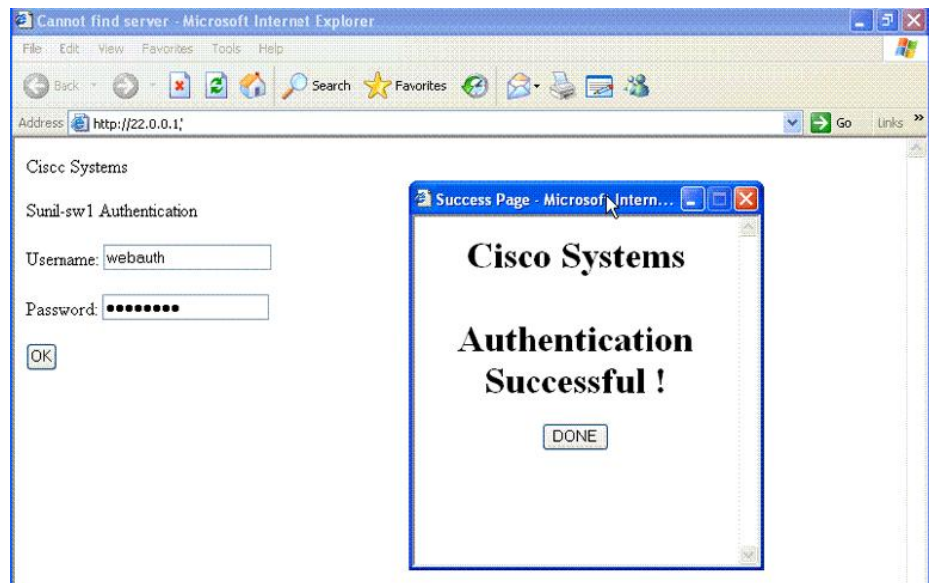
- 認証成功
- 認証失敗
- 認証期限切れ

ローカル Web 認証バナーは、次のように設定できます。

- レガシーモード：**ip admission auth-proxy-banner http** 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。
- 新スタイルモード：**parameter-map type webauth global banner** 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。

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

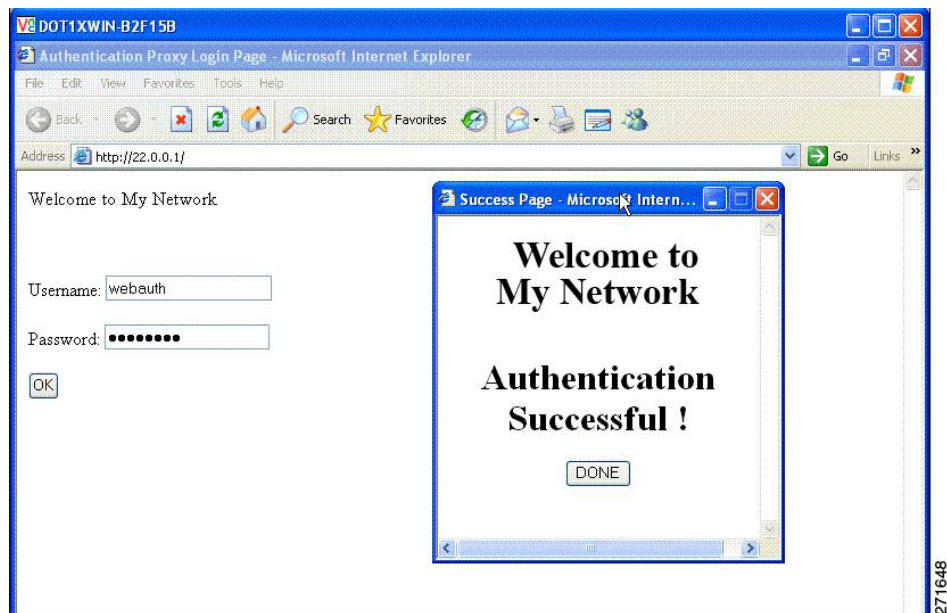


バナーは次のようにカスタマイズ可能です。

- 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。

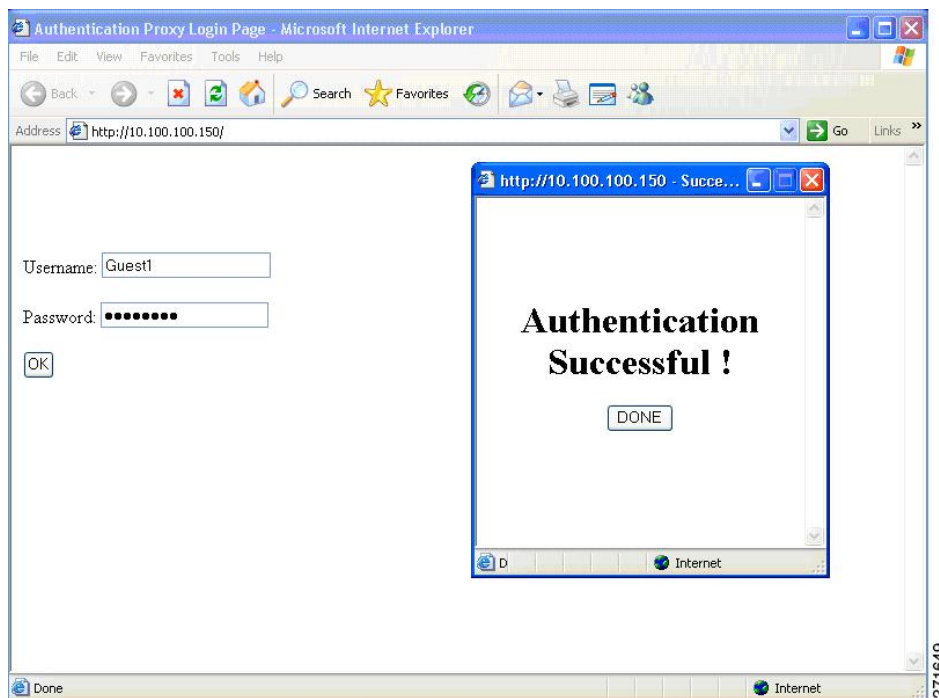
- レガシーモード： **ip admission auth-proxy-banner http banner-text** グローバル コンフィギュレーション コマンドを使用します。
 - 新スタイル モード： **parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。
- ログまたはテキスト ファイルをバナーに追加する。
- レガシーモード： **ip admission auth-proxy-banner http file-path** グローバル コンフィギュレーション コマンドを使用します。
 - 新スタイル モード： **parameter-map type webauth global banner** 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。

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



Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、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。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステータスを通知します。

- 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。

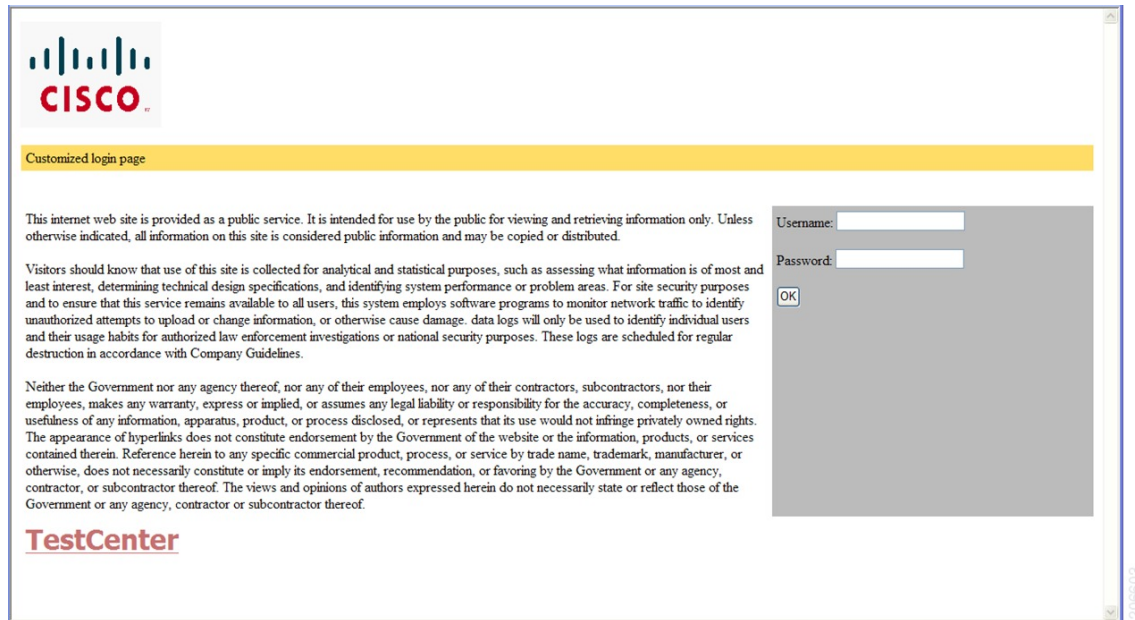
ガイドライン

- 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1つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 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のあるロゴファイル（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



認証プロキシ Web ページの注意事項

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能を有効にするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個のカスタム HTML ファイルは、スイッチのフラッシュメモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタムページ上のイメージはすべて、アクセス可能は HTTP サーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効な DNS サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ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。
- カスタム Web ページ機能が有効に設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイル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。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページタイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベストプラクティスに従う必要があります。

その他の機能と Web ベース認証の相互作用

ポート セキュリティ

Web ベース認証とポートセキュリティは、同じポートに設定できます。Web ベース認証はポートを認証し、ポートセキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

LAN ポート IP

LAN ポート IP (LPIP) とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホストポリシーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポスチャが再度検証されます。

ゲートウェイ IP

VLAN のいずれかのスイッチポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP (GWIP) を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホストポリシーが適用されます。GWIP ホストポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの受信トラフィックについて、ポート ACL (PACL) をデフォルトのアクセスポリシーとして設定することが必須ではないものの、より安全です。認証後、Web ベース認証のホストポリシーは、PACL に優先されます。ポートに設定された ACL がなくても、ポリシー ACL はセッションに適用されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール (CBAC) が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバチャンネルに適用されます。

Web ベース認証の設定方法

デフォルトの Web ベース認証の設定

次の表に、デフォルトの Web ベース認証の設定を示しています。

表 1: デフォルトの Web ベース認証の設定

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 • 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	有効

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は受信時だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランクポート、EtherChannel メンバポート、またはダイナミック トランク ポートではサポートされていません。
- スイッチが特定のホストまたは Web サーバにクライアントをリダイレクトしてログインメッセージを表示する場合、外部 Web 認証はサポートされません。

- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP デバイス追跡機能は無効にされています。Web ベース認証を使用するには、IP デバイス追跡機能を有効にする必要があります。
- Web ベース認証を使用するには、SISF ベースのデバイス追跡を有効にする必要があります。デフォルトでは、SISF ベースのデバイス追跡はスイッチで無効になっています。
- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要があります。HTTP サーバは、ホストに HTTP ログインページを送信します。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホスト トラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。これは、レイヤ 2 (STP) トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。
- Web ベース認証は、ダウンロード可能なホストポリシーとして、VLAN 割り当てをサポートしていません。
- IPv6 Web ベース認証はサポートされていません。
- Web ベース認証および Network Edge Access Topology (NEAT) は、相互に排他的です。インターフェイス上で NEAT が有効の場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- 仮想 IP 設定はサポートされていません。この制限により、ログアウトページはサポートされていません。
- スイッチから RADIUS サーバへの通信の設定に使用される次の RADIUS セキュリティサーバ設定を確認します。
 - ホスト名
 - ホスト IP アドレス
 - ホスト名と特定の UDP ポート番号
 - IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス (たとえば認証) を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

- RADIUS サーバパラメータを設定する場合は、次の点に注意してください。
 - 別のコマンドラインに、**key string** を指定します。

- **key string** には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する、認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。
- **key string** を指定する場合、キーの中間、および末尾にスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
- すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** 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。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server transmit**、および **radius-server key** 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。



(注) RADIUS サーバでは、スイッチの IP アドレス、サーバとスイッチで共有される **key string**、およびダウンロード可能な ACL (DACL) などの設定を行う必要があります。詳細については、RADIUS サーバのマニュアルを参照してください。

認証ルールとインターフェイスの設定

認証ルールおよびインターフェイスを設定するには、次の手順を実行します。

始める前に

SISF ベースのデバイス追跡は、web 認証の前提条件です。デバイス追跡をプログラムまたは手動で有効にしていることを確認します。

詳細については、「*SISF* ベースの追跡の設定」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission name name proxy http**
4. **interface type slot/port**
5. **ip access-group name**
6. **ip admission name**
7. **exit**
8. **show ip admission**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	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 3	ip admission name name proxy http 例： Device(config)# ip admission name webauth1 proxy http	Web ベース許可の認証ルールを設定します。
ステップ 4	interface type slot/port 例： Device(config)# interface gigabitethernet 1/0/1	インターフェイス コンフィギュレーション モードを開始し、Web ベース認証を有効にする受信レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 <i>type</i> には、FastEthernet、GigabitEthernet、または TenGigabitEthernet を指定できます。
ステップ 5	ip access-group name 例： Device(config-if)# ip access-group webauthag	デフォルト ACL を適用します。
ステップ 6	ip admission name 例： Device(config)# ip admission name	インターフェイスの Web ベース認可の認証ルールを設定します。
ステップ 7	exit 例： Device# exit	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 8	show ip admission 例：	ネットワークアドミSSIONのキャッシュエントリと Web 認証セッションに関する情報を表示します。

	コマンドまたはアクション	目的
	Device# <code>show ip admission</code>	

AAA 認証の設定

VTY 回線で方式リストを設定する場合、対応する方式リストを AAA 設定に追加する必要があります。

```
Device(config)# line vty 0 4
Device(config-line)# authorization commands 15 list1
Device(config-line)# exit
Device(config)# aaa authorization commands 15 list1 group tacacs+
```

VTY 回線で方式リストを設定しない場合、デフォルトの方式リストを AAA 設定に追加する必要があります。

```
Device(config)# line vty 0 4
Device(config-line)# exit
Device(config)# aaa authorization commands 15 default group tacacs+
```

AAA 認証を設定するには、次の手順を実行します。

手順の概要

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login default group {tacacs+ | radius}`
5. `aaa authorization auth-proxy default group {tacacs+ | radius}`
6. `tacacs server server-name`
7. `address {ipv4 | ipv6} ip address`
8. `key` 文字列
9. `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	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例：	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。

	コマンドまたはアクション	目的
	Device# <code>configure terminal</code>	
ステップ 3	aaa new-model 例： Device(config)# <code>aaa new-model</code>	AAA 機能を有効にします。
ステップ 4	aaa authentication login default group {tacacs+ radius} 例： Device(config)# <code>aaa authentication login default group tacacs+</code>	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 はサーバグループ名を示します。サーバグループ server_name をその先頭で定義する必要があります。
ステップ 5	aaa authorization auth-proxy default group {tacacs+ radius} 例： Device(config)# <code>aaa authorization auth-proxy default group tacacs+</code>	Web ベース許可の許可方式リストを作成します。
ステップ 6	tacacs server server-name 例： Device(config)# <code>tacacs server yourserver</code>	AAA サーバを指定します。
ステップ 7	address {ipv4 ipv6} ip address 例： Device(config-server-tacacs)# <code>address ipv4 10.0.1.12</code>	TACACS サーバの IP アドレスを設定します。
ステップ 8	key 文字列 例： Device(config-server-tacacs)# <code>key cisco123</code>	スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。
ステップ 9	end 例：	TACACS サーバモードを終了し、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-server-tacacs)# end	

スイッチ/RADIUS サーバ間通信の設定

RADIUS サーバのパラメータを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface vlan** *vlan interface number*
4. **radius server** *server name*
5. **address** {*ipv4* | *ipv6*} *ip address*
6. **key** *string*
7. **exit**
8. **radius-server dead-criteria tries** *num-tries*
9. **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	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	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 3	ip radius source-interface vlan <i>vlan interface number</i> 例： Device(config)# ip radius source-interface vlan 80	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 4	radius server <i>server name</i> 例： Device(config)# radius server rsim address ipv4	(任意) RADIUS サーバの IP アドレスを指定します。

	コマンドまたはアクション	目的
	172.16.0.1	
ステップ 5	address {ipv4 ipv6} ip address 例 : Device(config-radius-server) # address ipv4 10.0.1.2 auth-port 1550 acct-port 1560	RADIUS サーバの IP アドレスを設定します。
ステップ 6	key string 例 : Device(config-radius-server) # key rad123	(任意) RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 7	exit 例 : Device(config-radius-server) # exit	RADIUS サーバモードを終了して、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 8	radius-server dead-criteria tries num-tries 例 : Device(config) # radius-server dead-criteria tries 30	RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。指定できる <i>num-tries</i> の範囲は 1 ~ 100 です。
ステップ 9	end 例 : Device(config) # 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。

HTTP サーバの設定

Web ベース認証を使用するには、device で HTTP サーバを有効にする必要があります。このサーバは 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を有効にするには、次の手順に従います。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http secure-server**
5. **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	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	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 3	ip http server 例： Device(config)# ip http server	HTTP サーバを有効にします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 4	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 5	end 例： Device# 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。

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、のデフォルト HTML ページではなく、代替の HTML ページがユーザーに表示されるように、Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、次の手順を実行してください。

始める前に

device のフラッシュ メモリにカスタム HTML ファイルを保存します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission proxy http login page file device:login-filename**
4. **ip admission proxy http success page file device:success-filename**
5. **ip admission proxy http failure page file device:fail-filename**
6. **ip admission proxy http login expired page file device:expired-filename**
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	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	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 3	ip admission proxy http login page file device:login-filename 例： Device(config)# ip admission proxy http login page file disk1:login.htm	device のメモリ ファイルシステム内で、デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの場所を指定します。device: はフラッシュ メモリです。
ステップ 4	ip admission proxy http success page file device:success-filename 例： Device(config)# ip admission proxy http success	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。

	コマンドまたはアクション	目的
	<code>page file disk1:success.htm</code>	
ステップ 5	ip admission proxy http failure page file <i>device:fail-filename</i> 例 : Device(config)# ip admission proxy http fail page file disk1:fail.htm	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 6	ip admission proxy http login expired page file <i>device:expired-filename</i> 例 : Device(config)# ip admission proxy http login expired page file disk1:expired.htm	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 7	end 例 : Device# 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。

Web ベース認証パラメータの設定

クライアントが待機時間中にウォッチリストに掲載されるまで許容される失敗ログイン試行の最大回数を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission max-login-attempts *number***
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	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 3	ip admission max-login-attempts number 例： Device(config)# ip admission max-login-attempts 10	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ~ 2147483647 回です。デフォルトは 5 分です。
ステップ 4	exit 例： Device# exit	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。

Web ベース認証ローカルバナーの設定

Web 認証が設定されているスイッチにローカルバナーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission auth-proxy-banner http** [*banner-text* | *file-path*]
4. **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	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	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。

	コマンドまたはアクション	目的
ステップ 3	ip admission auth-proxy-banner http [<i>banner-text</i> <i>file-path</i>] 例 : Device(config)# ip admission auth-proxy-banner http C My Switch C	ローカル バナーを有効にします。 (任意) <i>C</i> <i>banner-text C</i> (<i>C</i> は区切り文字)、またはバナーに表示されるファイル (たとえば、ロゴまたはテキストファイル) のファイルパスを入力して、カスタム バナーを作成します。
ステップ 4	end 例 : Device# 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。

Web ベース認証キャッシュ エントリの削除

Web ベース認証キャッシュ エントリを削除するには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear ip auth-proxy cache** {* | *host ip address*}
3. **clear ip admission cache** {* | *host ip address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	clear ip auth-proxy cache {* <i>host ip address</i> }	Delete 認証プロキシエントリを削除します。キャッシュエントリすべてを削除するには、アスタリスクを使用します。シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。
ステップ 3	clear ip admission cache {* <i>host ip address</i> }	Delete 認証プロキシエントリを削除します。キャッシュエントリすべてを削除するには、アスタリスクを使用します。シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。

Web ベース認証の確認

すべてのインターフェイスまたは特定のポートに対する Web ベース認証設定を表示するには、このトピックのコマンドを使用します。

表 2: 特権 EXEC 表示コマンド

コマンド	目的
show authentication sessions method webauth	FastEthernet、ギガビット イーサネット、または 10 ギガビット イーサネットのすべてのインターフェイスに対する Web ベースの認証設定を表示します。
show authentication sessions interface type slot/port[details]	FastEthernet、ギガビット イーサネット、または 10 ギガビット イーサネットの特定のインターフェイスに対する Web ベースの認証設定を表示します。 セッション認識型ネットワーク モードでは、 show access-session interface コマンドを使用します。

Web ベース認証に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『 Cisco IOS Master Command List, All Releases 』

シスコのテクニカル サポート

説明	リンク
<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>	http://www.cisco.com/support