Web ベース認証の設定

Web ベース認証機能（別名 Web 認証プロキシ）は、IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

Web ベース認証について

Web ベース認証の概要

IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証するには、Web 認証プロキシと呼ばれる Web ベース認証機能を使用します。

（注） Web ベース認証を設定できるのはレイヤ 2 インターフェイスのみです。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、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、アカウンティング（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）を使用するときに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。

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、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。

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] ボタンまたは [Deny] ボタンがあり、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して [Accept] ボタンをクリックする必要があります。

（注） 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。

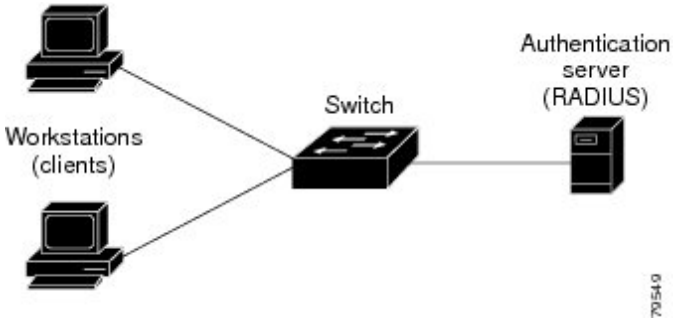
デバイスのロール

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、JavaScriptがイネーブルに設定された 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デバイストラッキング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 インスペクション
- 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す。

- 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 ベース認証をイネーブルにすると、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 トラフィックが代行受信され、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 プローブに応答しない場合、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。

認証プロキシの使用

認証プロキシ機能は、クライアントホスト上でユーザとの対話を必要とします。次の表で、認証プロキシとクライアント ホストの対話について説明します。

表 *1:* 認証プロキシとクライアント ホストの対話

認証プロキシのクライアントとの動作	説明
HTTP 接続の開始	ユーザが現在ファイアウォール ルータで認証済みでない場合、ユーザが HTTP 接続を開始すると認証プロキシが起動されます。ユーザがすでに認証済みの場合、認証プロキシはユーザに対して透過的です。
ログイン ページを使用したログイン	認証プロキシをトリガーすると、HTML ベースのログイン ページが生成されます。ユーザは、AAA サーバで認証されるために、ユーザ名とパスワードを入力する必要があります。How the Authentication Proxy Works モジュールの Authentication Proxy Login Page の図で、認証プロキシのログイン ページを図示しています。

認証プロキシのクライアントとの動作	説明
クライアントでのユーザの認証	ログインの試行の後の認証プロキシの動作は、ブラウザで JavaScript がイネーブルになっているかどうかで変わります。JavaScript が有効なときに認証が成功した場合、認証プロキシは、How the Authentication Proxy Works モジュールの Authentication Proxy Login Status Message の図に示すように、認証のステータスを示すメッセージを表示します。認証ステータスが表示された後、プロキシは自動的に HTTP 接続を完了します。 JavaScript がディセーブルになっており、認証が成功した場合、認証プロキシは、接続を完了するための追加の手順を表示したポップアップウィンドウを生成します。Secure Authentication モジュールの Authentication Proxy Login Status Message with JavaScript Disabled の図を参照してください。 いずれの場合も、認証が成功しなかった場合は、ユーザはログインページから再度ログインする必要があります。

認証プロキシを使用すべき場合

認証プロキシは、次のような状況で使用できます。

- ホストの IP アドレスやグローバル アクセス ポリシーに基づいてアクセス コントロールを設定するのではなく、認証サーバによって提供されているサービスを使用して、個人ごと（ユーザごと）にアクセス権を管理する場合。任意のホスト IP アドレスからのユーザを認証および認可することにより、ネットワーク管理者は、DHCP を使用してホスト IP アドレスを設定できるようにもなります。
- イントラネットやインターネット サービスへのアクセスを許可する前に、ローカル ユーザを認証および認可する場合。
- ローカル サービスへのアクセスを許可する前に、リモート ユーザを認証および認可する場合。
- 特定のエクストラネット ユーザに対するアクセスを制御する場合。たとえば、企業パートナーの財務責任者を、あるアクセス権のセットを使用して認証および認可し、同じパートナーの技術責任者を、別のアクセス権のセットを使用するように認可することができます。
- 認証プロキシを VPN クライアント ソフトウェアとともに使用して、ユーザを検証し、特定のアクセス権を割り当てる場合。
- 認証プロキシを AAA アカウンティングとともに使用して、課金、セキュリティ、またはリソース割り当てのために使用可能な「開始」および「終了」アカウンティング レコードを生成することで、ユーザが認証済みホストからのトラフィックを追跡できるようにする場合。

認証プロキシの適用

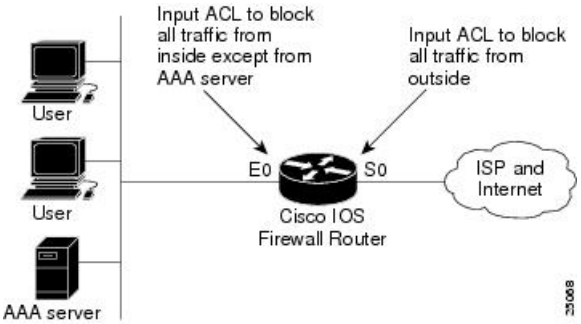
認証プロキシは、ユーザごとの認証と認可を行うルータの任意のインターフェイスで、インバウンド方向に適用します。認証プロキシをインターフェイスでインバウンド方向に適用すると、ユーザからの初期接続要求が、他の処理に渡される前に、認証プロキシによって代行受信されます。ユーザが AAA サーバによる認証に失敗すると、接続要求はドロップされます。

認証プロキシの適用方法は、セキュリティポリシーに依存します。たとえば、インターフェイスを通過するすべてのトラフィックをブロックし、認証プロキシ機能を有効にして、ユーザが開始したすべての HTTP 接続に対して認証と認可を義務付けることができます。ユーザは、AAA サーバで正常に認証されない限り、サービスの利用が認可されません。

認証プロキシ機能では、標準のアクセス リストを使用し、どのホストまたはホスト グループからの初期 HTTP トラフィックに対してプロキシを起動するかを指定できます。

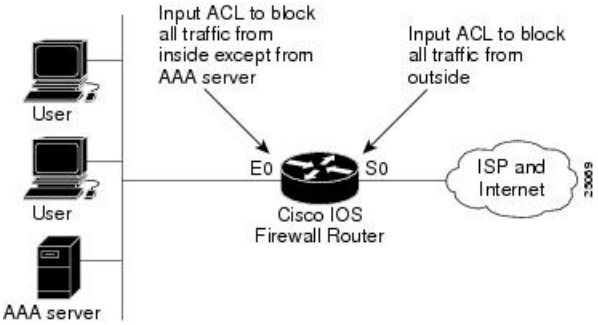
下の図に示す認証プロキシは、LANインターフェイスに適用されており、すべてのネットワーク ユーザは、初期接続時に認証される必要があります（すべてのトラフィックは各インターフェイスでブロックされます）。

図 *2:* ローカル インターフェイスでの認証プロキシの適用



下の図に示す認証プロキシは、ダイヤルイン インターフェイスに適用され、すべてのネットワーク トラフィックが各インターフェイスでブロックされます。

図 *3:* 外部インターフェイスでの認証プロキシの適用



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。

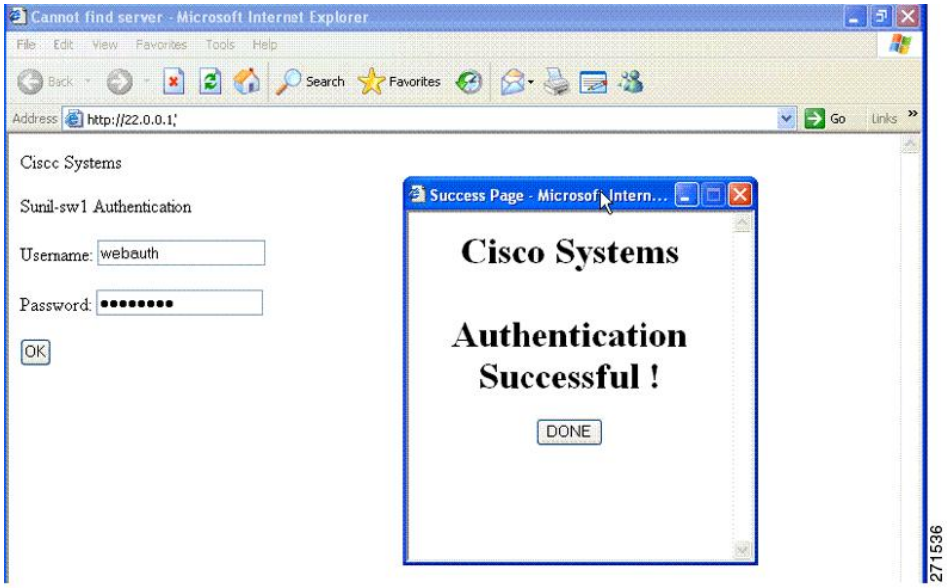
- 認証成功
- 認証失敗
- 認証期限切れ

ローカル ネットワーク認証バナーは、レガシーおよび新スタイル（セッション アウェア）の CLI で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 *4:* 認証成功バナー

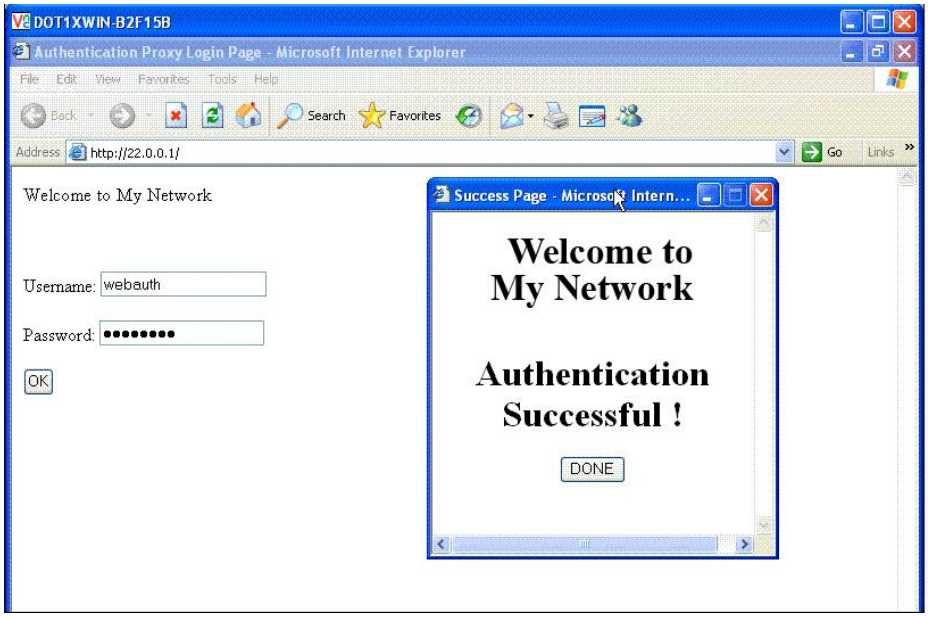


バナーは次のようにカスタマイズ可能です。

- 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。
- ロゴまたはテキスト ファイルをバナーに追加する。

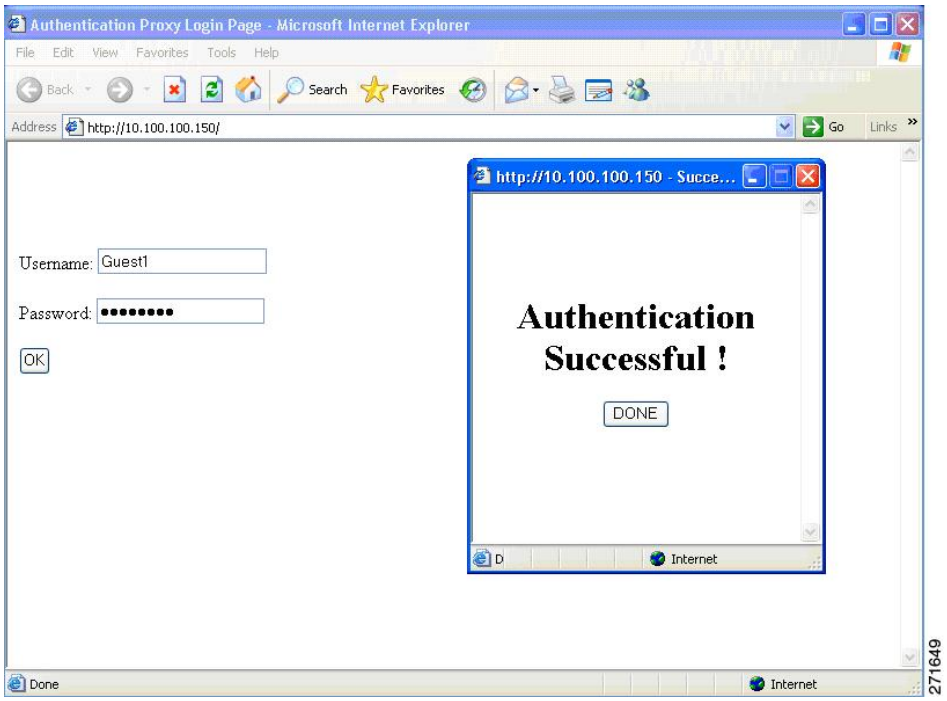
- レガシー モード：**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。
- 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

図 *5*：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 *6:* 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。

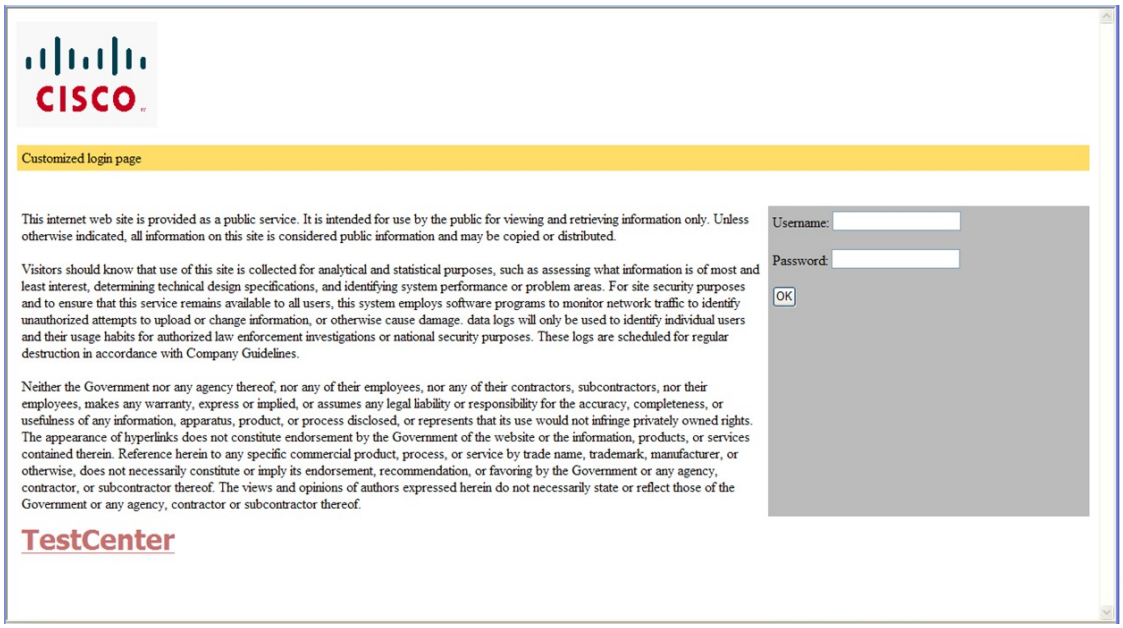
ガイドライン

- 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 フォームがイネーブルにされている場合、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。
- スタック可能なスイッチでは、スタック マスターまたはスタック メンバーのフラッシュから設定済みのページにアクセスできます。
- 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 7: 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 ページ機能をイネーブルにするには、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 ページ機能がイネーブル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 ページ機能がイネーブル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

802.1X 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。
  - スイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。

- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。

認証プロキシによる AAA アカウンティング

認証プロキシを使用して、課金やセキュリティ監査で使用できる十分な情報を含む「開始」および「終了」アカウンティング レコードを生成できます。そうすることで、認証プロキシサービスを使用する認証済みホストの動作をモニタできます。

認証プロキシのキャッシュが満了して削除されると、経過時間などの追加のデータがアカウンティング情報に追加され、「終了」レコードがサーバに送信されます。この時点で、情報がデータ構造から削除されます。

認証プロキシ ユーザ セッションに対するアカウンティング レコードは、キャッシュおよび動的 ACL の使用に関連付けられます。

ACL

Web ベースの認証を行うには、インターフェイスでポート ACL を設定する必要があります。

Web ベースの認証を実行できる十分な TCAM 容量があることを確認します。

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入力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、必須ではないですがより安全です。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。

Gateway 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。

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。

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。

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 *2:* 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 • IP アドレス • UDP 認証ポート • Key	• 指定なし • 1645 • 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	イネーブル

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- 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。
- ポート設定にポート ACL が存在している必要があります。ポート ACL がない場合、intercept ACL を追加できません。

- 必要なトラフィックを認証後に許可できるようポート ACL が適切に設定されている必要があります。これが必要になるのは、このスイッチでダウンロード可能ACL（DACL）がサポートされていないためです。
- スイッチは、すべてのホストモードで、各ポートに1つのWeb認証クライアントをサポートします。複数のクライアントを持つことは、予期せぬ結果を招く可能性があり、推奨されていません。
- DACL がサポートされていないため、Web 認証用認証ルールでポート ACL を設定することは許可されません。
- Web ベース認証を設定する前に、インターフェイスでデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスに対してポート ACL を設定するか、またはレイヤ 3 インターフェイスに対して Cisco IOS ACL を設定します。
- 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 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IPデバイスのトラッキング機能をイネーブルにする必要があります。
- 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もあります。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。
- 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がイネーブルの場合、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。
- Web ベース認証 NRH（応答しないホスト）は、音声デバイスではサポートされません。
- パスワード認証プロトコル（PAP）のみがコントローラの Web ベースの RADIUS 認証でサポートされます。チャレンジハンドシェイク認証プロトコル（CHAP）は、コントローラの Web ベースの RADIUS 認証でサポートされません。
- 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分である場合を除き、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。詳細については、『*Cisco IOS Security Configuration Guide*, Release 12.4』および『*Cisco IOS Security Command Reference*, Release 12.4』を参照してください。

  （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。

- MDA/MA モードでは、IP 電話に接続された PC から Web ベース認証セッションを開始することはできません（ダウンロード可能 ACL がサポートされていないため）。
- スイッチを Web ベース認証クライアント用ゲートウェイとして設定することはできません（スイッチで レイヤ 3 ルックアップが行われないため）。代わりに、アップリンク デバイスのスイッチ仮想インターフェイス（SVI）をゲートウェイとして設定します。
- ASIC による合計 TCAM 領域は、384 までに制限されます。したがって、ポート ACL と Web ベース認証をすべてのポートにわたって設定する場合、セッションの合計数は、スイッチに設定されたアクセス制御エントリ（ACE）によって異なります（Web ベース認証

が設定されているポートは、TCAM で ACL を共有しません。TCAM 領域がポート ACL で一杯になると、Web ベース認証セッションは開始されません）。

- IOS XE リリース 3.6.x および 3.7.x からアップグレードするときに、**radius-server attribute wireless accounting call-station-id macaddress** コマンドを使用して、mac アドレスを設定することを確認します。これは、Cisco IOS XE Denali 16.3.x 以降、アカウンティング デフォルトの call-station-id が mac アドレスから IP アドレスに変更されたためです。

Web ベース認証の設定方法

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。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip admissionname** *name***proxyhttp**
4. **interface** *type slot/port*
5. **ip access-group** *name*
6. **ip admissionname**
7. **exit**
8. **ip device tracking**
9. **end**
10. **show ip admission status**
11. **copy running-config startup-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	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# 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 admissionname** *name***proxyhttp** 例： `Switch(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： `Switch(config)# interface gigabitEthernet1/0/1`	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 ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 *type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 5	**ip access-group** *name* 例： `Switch(config-if)# ip access-group webauthag`	デフォルト ACL を適用します。
ステップ 6	**ip admissionname** 例： `Switch(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： `Switch(config-if)# exit`	コンフィギュレーション モードに戻ります。
ステップ 8	**ip device tracking** 例： `Switch(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip admission status** 例：	設定を表示します。

	コマンドまたはアクション	目的
	`Switch# show ip admission status`	
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA 認証の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login default group** {**tacacs+** | **radius**}
5. **aaa authorization auth-proxy default group** {**tacacs+** | **radius**}
6. **tacacs-server host** {*hostname* | *ip_address*}
7. **tacacs-server key** {*key-data*}
8. **end**
9. **show running-config**
10. **copy running-config startup-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	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# 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	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA 機能を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 4	**aaa authentication login default group** {**tacacs+** | **radius**} 例： `Switch(config)# aaa authentication login default group tacacs+`	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： `Switch(config)# aaa authorization auth-proxy default group tacacs+`	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 host** {*hostname* | *ip_address*} 例： `Switch(config)# tacacs-server host 10.1.1.1`	AAA サーバを指定します。
ステップ 7	**tacacs-server key** {*key-data*} 例： `Switch(config)# tacacs-server key`	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 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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. **configureterminal**
3. **ip radius source-interface vlan** *vlan interface number*
4. **radius-server host** {*hostname* | *ip-address*} **test username** *username*
5. **radius-server key** *string*
6. **radius-server dead-criteria tries** *num-tries*
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： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# 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** *vlan interface number* 例： `Switch(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 host** {*hostname*	*ip-address*} **test username** *username* 例： `Switch(config)# radius-server host 172.120.39.46 test username user1`	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバの間で使用される認証と暗号キーを指定します。 複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。

	コマンドまたはアクション	目的
ステップ 5	**radius-server key** *string* 例： `Switch(config)# radius-server key rad123`	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。
ステップ 6	**radius-server dead-criteria tries** *num-tries* 例： `Switch(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 *num-tries* の範囲は 1 ～ 100 です。
ステップ 7	**end** 例： `Switch(config)# end`	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、Switch で HTTP サーバをイネーブル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イネーブルにできます。

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

HTTP または HTTPS のいずれかでサーバを有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
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：	特権 EXEC モードをイネーブルにします。 • 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
	`Switch> enable`	
ステップ 2	**configureterminal** 例： `Switch# 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： `Switch(config)# ip http server`	HTTP サーバをイネーブルにします。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： `Switch(config)# ip http secure-server`	HTTPS をイネーブルにします。 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： `Switch(config)# end`	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 ベースの認証中に、Switchのデフォルト HTML ページではなく 4 種類の代わりの HTML ページがユーザ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

Switch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. **configureterminal**
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： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# 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： `Switch(config)# ip admission proxy http login page file disk1:login.htm`	Switch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： `Switch(config)# ip admission proxy http success page file disk1:success.htm`	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。
ステップ 5	**ip admission proxy http failure page file** *device:fail-filename* 例： `Switch(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** *device:expired-filename* 例：	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。

	コマンドまたはアクション	目的
	`Switch(config)# ip admission proxy http login expired page file disk1:expired.htm`	
ステップ 7	**end** 例： `Switch(config)# end`	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. **configureterminal**
3. **ip admission max-login-attempts** *number*
4. **end**
5. **show running-config**
6. **copy running-config startup-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	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# 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： `Switch(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。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Web 認証ローカル バナーの設定

この機能のための同等のセッション認識型ネットワーク設定の例については、『*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』マニュアルの「アイデンティティ制御ポリシーの設定」の章の「Web ベース認証のパラメータ マップの設定」の項を参照してください。

Web 認証が設定されたスイッチでローカル バナーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ip auth-proxy auth-proxy-banner http** [*banner-text* | *file-path*]
3. **end**
4. **copy running-config startup-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	**configure terminal** 例： `Switch# 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	**ip auth-proxy auth-proxy-banner http** [*banner-text*	*file-path*]	ローカル バナーを有効にします。

	コマンドまたはアクション	目的
	例： `Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C`	（任意）*C banner-text C* と入力して、カスタム バナーを作成します。ここで、*C* は区切り文字、またはバナーに表示されるファイル（例：ロゴ、またはテキスト ファイル）を示すファイル パスです。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** 例： `Switch(config)# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

中央 Web 認証の設定

中央 Web 認証（CWA）とは、Cisco Identity Services Engine（ISE）などのポリシー サーバを使用して Web 認証によりユーザを一元的に認証するプロセスです。Web 認証のための中枢ポリシー サーバがあると、運用面での実装が容易になります。CWA では、ACL ベースの適用も VLAN ベースの適用もサポートされます。また、RADIUS CoA もサポートされます。これにより、プロファイリングに基づくポスチャ アセスメントおよび適用が可能になります。

（注） CWA は、Cisco IOS リリース 15.2(5) E1 から Catalyst 2960-L スイッチに導入されています。

すべての Catalyst スイッチに関する中央 Web 認証設定方法の詳細については、ドキュメント『Central Web Authentication with a Switch and Identity Services Engine Configuration Example』を参照してください。

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 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： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip admission cache** {* | *host ip address*} 例： `Switch# clear ip admission cache 192.168.4.5`	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 ベース認証ステータスの監視

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 *3:* 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 wireless client mac-address *a.a.a* **detail**	セッション固有のワイヤレス情報とワイヤレス状態を表示します。
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 ベース認証ステータスの表示

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 ベースの認証設定を表示する手順は、次のとおりです。

手順の概要

1. **show authentication sessions** {**interface***type/ slot*}

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show authentication sessions** {**interface***type/ slot*}
	例：
	次に、グローバルな Web ベース認証のステータスだけを表示する例を示します。
	`Switch# show authentication sessions`
	例：
	次に、ギガビット インターフェイス 3/27 に対する Web ベースの認証設定を表示する例を示します。
	`Switch# show authentication sessions interface gigabitethernet 3/27`
		Web ベース認証設定を表示します。
		type には、fastethernet、gigabitethernet、または tengigabitethernet を指定できます。
		（任意）特定のインターフェイスに対する Web ベース認証設定を表示するには、キーワード interface を使用します。

HTTP 認証プロキシのモニタリング

HTTP 認証プロキシの設定をトラブルシューティングするには、次の手順を実行します。

手順の概要

1. **enable**
2. **debugipadmissionall**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugipadmissionall** 例： `Device# debug ip admission all`	Web ベース認証のすべての IP アドミッションのデバッグ情報を表示します。

HTTPS 認証プロキシの確認

HTTPS 認証プロキシの設定を確認するには、オプションで次の手順を実行します。

手順の概要

1. **enable**

2. **showipadmission{ status|cache }**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showipadmission{ status|cache }** 例： `Device# show ip admission cache`	Web認証セッションのネットワーク アドミッション設定ステータスとキャッシュ エントリを表示します。

Web ベース認証の設定例

例：認証ルールとインターフェイスの設定

次の例は、ファスト イーサネット ポート 5/1 で Web ベース認証を有効化する方法を示しています。

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Switch# show ip admission status
IP admission status:
  Enabled interfaces            0
  Total sessions                0
  Init sessions                 0     Max init sessions allowed     100
    Limit reached               0     Hi watermark                  0
  TCP half-open connections     0     Hi watermark                  0
  TCP new connections           0     Hi watermark                  0
  TCP half-open + new           0     Hi watermark                  0
  HTTPD1 Contexts               0     Hi watermark                  0

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured
```

例：AAA の設定

```
aaa new-model
aaa authentication login default group tacacs group radius
! Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default group tacacs group radius
! Define the AAA servers used by the router.
aaa accounting auth-proxy default start-stop group tacacs+
! Set up authentication proxy with accounting.
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
```

例：HTTP サーバの設定

```
! Enable the HTTP server on the router.
ip http server
! Set the HTTP server authentication method to AAA.
ip http authentication aaa
! Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
```

例：認証プロキシ Web ページのカスタマイズ

次の例では、カスタム認証プロキシ Web ページを設定する方法を示します。

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

次の出力には、ホスト IP アドレス、セッション タイムアウト、ポスチャ状態が表示されています。ポスチャ状態が POSTURE ESTAB になっていれば、ホスト検証は成功しています。

```
Switch# show ip admission cache eapoudp
Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

例：ログイン成功時のリダイレクション URL の指定

ログイン成功時のリダイレクション URL の設定

```
Switch(config)# ip admission proxy http success redirect www.cisco.com
```

ログイン成功時のリダイレクション URL の確認

次の例では、成功したログインに対するリダイレクション URL を設定する方法を示します。

```
Switch# show ip admission status
 Enabled interfaces            0
 Total sessions                0
 Init sessions                 0     Max init sessions allowed     100
   Limit reached               0     Hi watermark                  0
 TCP half-open connections     0     Hi watermark                  0
 TCP new connections           0     Hi watermark                  0
 TCP half-open + new           0     Hi watermark                  0
 HTTPD1 Contexts               0     Hi watermark                  0

 Parameter Map: Global
   Custom Pages
     Custom pages not configured
   Banner
     Banner not configured
```

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』
IBNS コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』

シスコのテクニカル サポート

説明	Link
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

Web ベース認証の機能情報

リリース	機能情報
Cisco IOS リリース 15.0(2)EXCisco IOS リリース 15.2(5)E	この機能が導入されます。