CHAPTER 13

Web ベースの認証の設定

この章では、Web ベースの認証の設定方法を説明します。この章で説明する内容は、次のとおりです。

（注） この章で使用しているスイッチ コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

Web ベースの認証の概要

Web ベースの認証機能（*Web 認証プロキシ*）を使用して、IEEE 802.1x サプリカントを実行していないホスト システムでエンド ユーザを認証します。

（注） Web ベースの認証はレイヤ 2 およびレイヤ 3 インターフェイスに設定できます。

HTTP セッションを開始すると、Web ベースの認証は、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。ユーザがそれぞれのクレデンシャルを入力すると、Web ベースの認証機能はそれらのクレデンシャルを Authentication、Authorization、Accounting（AAA; 認証、認可、アカウンティング）サーバに送信して認証します。

認証が成功すると、Web ベースの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。

認証に失敗すると、Web ベースの認証はログイン失敗 HTML ページをユーザに転送し、ユーザにログインの再試行を求めるメッセージを表示します。ユーザが最大試行回数を超えると、Web ベースの認証は、ログイン期限切れ HTML ページをホストに転送し、ユーザは待機期間の間ウォッチ リストに置かれます。

次の項では、AAA の一部としての Web ベースの認証の役割について説明します。

- 「Web 認証のカスタマイズ可能 Web ページ」（P.13-6）
- 「Web ベースの認証と他の機能との相互作用」（P.13-7）

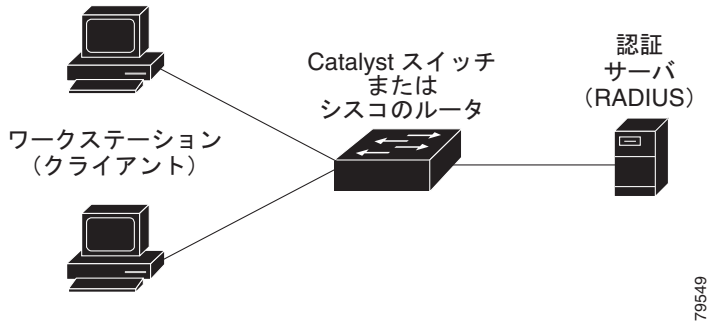
装置の役割

Web ベースの認証では、ネットワーク内の装置は次の特定の役割を持ちます。

- *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装置（ワークステーション）。ワークステーションでは、Java スクリプトがイネーブルの HTML ブラウザを実行し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 ID を検証し、クライアントが LAN およびスイッチ サービスへのアクセスが許可されたこと、またはクライアントが拒否されたこと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的な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の間の仲介装置（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 13-1 に、ネットワークでのこれらの装置の役割を示します。

図 13-1　Web ベースの認証装置の役割



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 IP 装置追跡テーブルを維持します。

（注）　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 ベースの認証を使用するには、IP 装置追跡機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスの場合、Web ベースの認証は次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：Address Resolution Protocol（ARP; アドレス解決プロトコル）リダイレクト Access Control List（ACL; アクセス制御リスト）を使用すると、Web ベースの認証は、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 Dynamic Host Configuration Protocol（DHCP）バインディング エントリを作成すると、Web ベースの認証に通知されます。

セッションの作成

Web ベースの認証で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。

- 例外リストの確認

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

- 認可バイパスの確認

  ホスト IP が例外リストにない場合、Web ベースの認証では、nonresponsive-host（NRH; 非応答ホスト）要求がサーバに送信されます。

  サーバの応答が *access accepted* である場合、このホストの認可はバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL の設定

  NRH 要求に対するサーバの応答が *access rejected* である場合、HTTP インターセプト ACL がアクティブになり、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 ベースの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て、認可が開始されます。スイッチがログイン ページをユーザに送信します。ユーザがユーザ名とパスワードを入力すると、スイッチは認証サーバにエントリを送信します。
- 認証に成功すると、スイッチは認証サーバからユーザのアクセス ポリシーをダウンロードして、アクティブにします。ログイン成功ページがユーザに送信されます。
- 認証に失敗すると、スイッチはログイン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。最大試行回数だけ失敗すると、スイッチはログイン期限切れページを送信し、ホストはウォッチ リストに置かれます。ウォッチ リストが時間切れになったあと、ユーザは認証プロセスを再試行できます。
- 認証サーバがスイッチに応答しない場合、および 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アクセス失敗ポリシーを適用します。ログイン成功ページがユーザに送信されます（「ローカルの Web 認証バナー」（P.13-4）を参照）。
- スイッチは、ホストがレイヤ 2 インターフェイスで ARP プローブに応答しない場合、またはレイヤ 3 インターフェイスでホストがアイドル タイムアウト内にトラフィックを送信しない場合に、クライアントを再認証します。
- この機能では、ダウンロードされたタイムアウトまたはローカルで設定されたセッション タイムアウトが適用されます。
- 終端アクションが RADIUS である場合、この機能では、非応答ホスト（NRH）要求がサーバに送信されます。終端アクションは、サーバからの応答に含まれます。
- 終端アクションがデフォルトである場合、セッションは終了し、適用されたポリシーは削除されます。

ローカルの Web 認証バナー

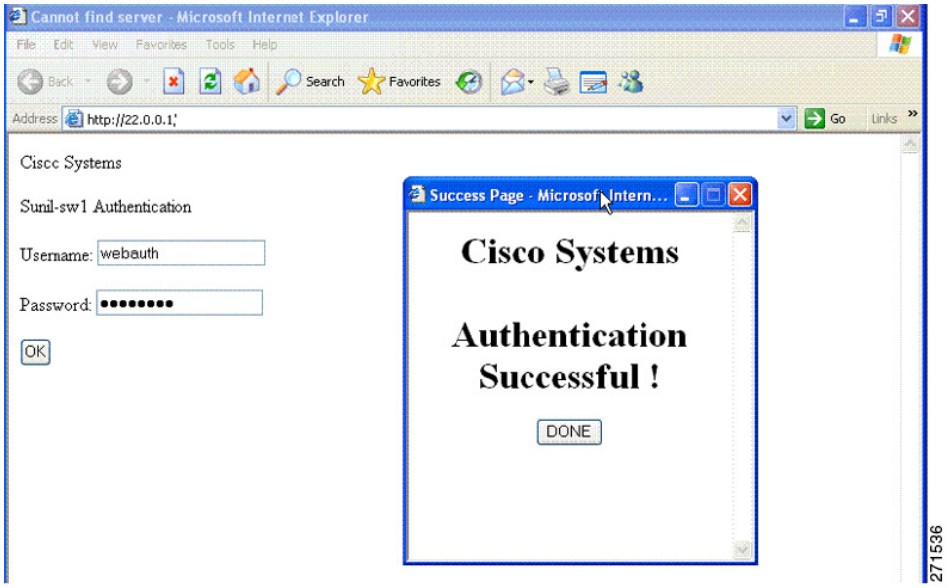
Web 認証を使用してスイッチにログインするときに表示されるバナーを作成できます。

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。

- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

ip admission auth-proxy-banner http グローバル コンフィギュレーション コマンドを使用して、バナーを作成できます。デフォルトのバナー「*Cisco Systems*」および「*Switch host-name Authentication*」はログイン ページに表示されます。「*Cisco Systems*」は認証結果のポップアップ ページに表示されます（図 13-2 を参照）。

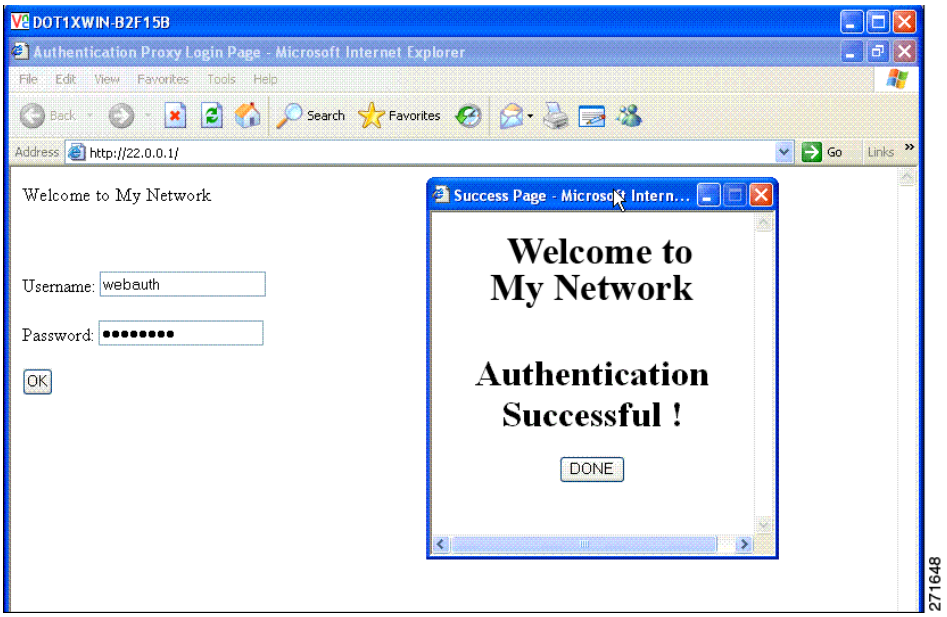
図 13-2　Authentication Successful バナー



また、バナーをカスタマイズすることもできます（図 13-3 を参照）。

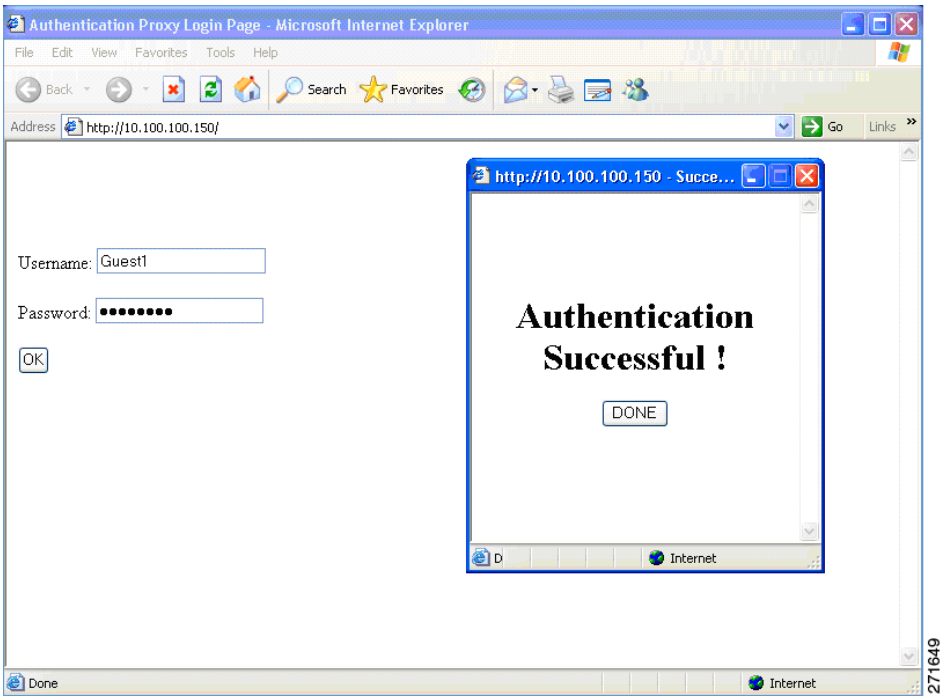
- スイッチ、ルータ、または会社名をバナーに追加するには、**ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用します。
- ロゴまたはテキスト ファイルをバナーに追加するには、**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。

図 13-3　カスタマイズされた Web バナー



バナーをイネーブルにしない場合、図 13-4 に示すように、スイッチへのログイン時に Web 認証の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、バナーは表示されません。

図 13-4　バナーのないログイン画面



詳細については、『Cisco IOS Security Command Reference』および「Web 認証ローカル バナーの設定」（P.13-16）を参照してください。

Web 認証のカスタマイズ可能 Web ページ

Web ベースの認証プロセス中、スイッチの内部 HTTP サーバが、4 つの HTML ページをホストして、認証するクライアントに配信します。サーバはこれらのページを使用して、次の 4 つの認証プロセスのステートを通知します。

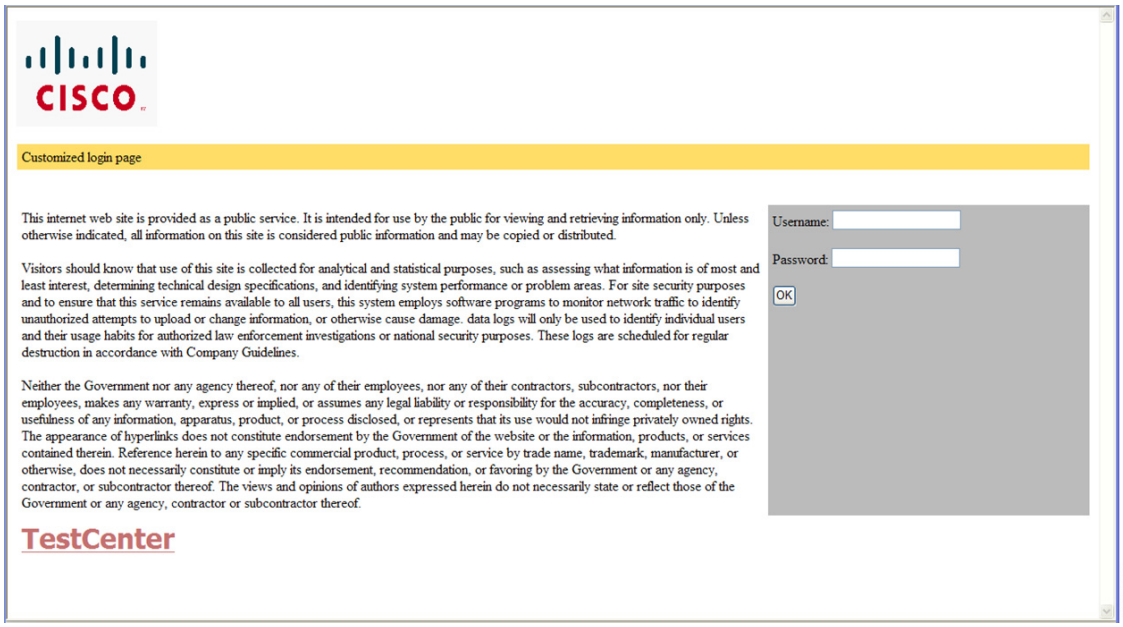
- ログイン：クレデンシャルが要求されています。
- 成功：ログインが成功しました。
- 失敗：ログインが失敗しました。
- 期限切れ：ログインに何度も失敗しているため、ログイン セッションの期限が切れました。

注意事項

- デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます。
- *ログイン*、*成功*、*失敗*、および*期限切れ* Web ページでロゴを使用したり、テキストを指定したりできます。
- バナー ページでは、ログイン ページのテキストを指定できます。
- ページは HTML 形式になります。
- 成功ページに、特定の URL にアクセスするための HTML リダイレクト コマンドを含める必要があります。
- URL ストリングは有効な URL（http://www.cisco.com など）にする必要があります。不完全な URL を指定すると、*page not found* などのエラーが Web ブラウザに表示される場合があります。
- HTTP 認証用に Web ページを設定する場合は、適切な HTML コマンド（ページのタイムアウトを設定したり、非表示パスワードを設定したり、同じページが 2 回送信されていないか確認したりするなど）を含める必要があります。
- ユーザを特定の URL にリダイレクトする CLI（コマンドライン インターフェイス）コマンドは、設定されたログイン フォームがイネーブルな場合は使用できません。管理者は、Web ページにリダイレクションが設定されていることを確認する必要があります。
- 認証が行われたあとにユーザを特定の URL にリダイレクトする CLI コマンドが入力されてから、Web ページを設定するコマンドが入力されると、ユーザを特定の URL にリダイレクトする CLI コマンドは無効になります。
- 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。
- 設定されたページには、スタック マスターまたはメンバー上のフラッシュからアクセスできます。
- ログイン ページは 1 つのフラッシュに格納でき、成功ページと失敗ページは別のフラッシュ（たとえば、スタック マスターまたはメンバーのフラッシュ）に格納できます。
- 4 つのページをすべて設定する必要があります。
- バナー ページは Web ページで設定されている場合、無効です。
- システム ディレクトリ（flash、disk0、または disk）に格納され、ログイン ページに表示する必要のあるすべてのロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）では、ファイル名として *web_auth_<filename>* を使用する必要があります。
- 設定された認証プロキシ機能は、HTTP と Secure Socket Layer（SSL）の両方をサポートします。

デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます（図 13-5（P.13-7）を参照）。また、認証が行われたあとにユーザがリダイレクトされる URL を指定することもできます。この URL は内部の成功ページを置き換えます。

図 13-5　認証ページのカスタマイズ



詳細については、「認証プロキシ Web ページのカスタマイズ」（P.13-13）を参照してください。

Web ベースの認証と他の機能との相互作用

- 「ポート セキュリティ」（P.13-7）
- 「LAN ポート IP」（P.13-7）
- 「ゲートウェイ IP」（P.13-8）
- 「ACL」（P.13-8）
- 「コンテキスト ベースのアクセス制御」（P.13-8）
- 「802.1x 認証」（P.13-8）
- 「EtherChannel」（P.13-8）

ポート セキュリティ

Web ベースの認証とポート セキュリティは、同じポートに設定できます。Web ベースの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 Media Access Control（MAC; メディア アクセス制御）アドレスを含むすべての MAC アドレスのネットワーク アクセスを管理します。そのあと、ポートを介してネットワークにアクセスできるクライアントの数またはグループを制限できます。

ポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。

LAN ポート IP

LAN Port IP（LPIP; LAN ポート IP）およびレイヤ 2 の Web ベースの認証は、同じポートに設定できます。ホストは最初に Web ベースの認証を使用して認証され、そのあとに LPIP ポスチャ検証が行われます。LPIP ホスト ポリシーは、Web ベースの認証ホスト ポリシーよりも優先されます。

Web ベースの認証のアイドル タイマーが時間切れになると、Network Admission Control（NAC）ポリシーが削除されます。ホストが認証され、ポスチャが再検証されます。

ゲートウェイ IP

Web ベースの認証が VLAN 内のスイッチ ポートのいずれかに設定されている場合、レイヤ 3 インターフェイスに Gateway IP（GWIP; ゲートウェイ IP）を設定することはできません。

Web ベースの認証は、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。ソフトウェアでは両方の機能のホスト ポリシーが適用されます。GWIP ポリシーは、Web ベースの認証ホスト ポリシーよりも優先されます。

ACL

インターフェイスに VLAN ACL または Cisco IOS ACL を設定している場合は、Web ベースの認証ホスト ポリシーの適用後に限り ACL がホスト トラフィックに適用されます。

レイヤ 2 の Web ベースの認証の場合は、ポートに接続されているホストからの入力トラフィックに対するデフォルトのアクセス ポリシーとして Port ACL（PACL; ポート ACL）を設定する必要があります。認証後、Web ベースの認証ホスト ポリシーは、PACL よりも優先されます。

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

アクセス VLAN が VACL キャプチャに設定されているポートには、Web ベースの認証を設定できません。

コンテキスト ベースのアクセス制御

Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）がポート VLAN のレイヤ 3 VLAN インターフェイスに設定されている場合、Web ベースの認証をレイヤ 2 ポートに設定することはできません。

802.1x 認証

フォールバック認証方式を除き、802.1x 認証と同じポートに Web ベースの認証を設定することはできません。

EtherChannel

レイヤ 2 EtherChannel インターフェイスに Web ベースの認証を設定できます。Web ベースの認証設定は、すべてのメンバー チャネルに適用されます。

Web ベースの認証の設定

Web ベースの認証のデフォルト設定

表 13-1 に、Web ベースの認証のデフォルト設定を示します。

表 13-1　Web ベースの認証のデフォルト設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 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 ベースの認証設定時の注意事項および制約事項

- Web ベースの認証は、入力だけの機能です。
- Web ベースの認証は、アクセス ポートにだけ設定できます。Web ベースの認証は、トランク ポート、EtherChannel メンバー 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ません。
- Web ベースの認証を設定する前に、インターフェイスにデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスの場合はポート ACL を設定し、レイヤ 3 インターフェイスの場合は Cisco IOS ACL を設定します。
- スタティック ARP キャッシュ 割り当てを使用するレイヤ 2 インターフェイスではホストを認証できません。これらのホストは ARP メッセージを送信しないため、Web ベースの認証機能で検出されません。
- 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 ベースの認証を使用するには、IP 装置追跡機能をイネーブルにする必要があります。
- スイッチの HTTP サーバを実行する 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、各ホストの IP アドレスに到達するためのルートを設定する必要もあります。HTTP サーバは HTTP ログイン ページをホストに送信します。

- Spanning Tree Protocol（STP; スパニング ツリー プロトコル）トポロジの変更によってホストのトラフィックが別のポートに届いた場合、複数のホップ先にあるホストではトラフィックが中断される場合があります。このようなトラフィックの中断は、レイヤ 2（STP）トポロジが変更されたあとに、ARP と DHCP の更新が送信できない場合があるために生じます。
- Web ベースの認証は、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ません。
- Web ベースの認証は、IPv6 トラフィックでサポートされません。

Web ベースの認証設定のタスク リスト

認証のルールとインターフェイスの設定

	コマンド	目的
ステップ 1	**ip admission name** *name* **proxy http**	Web ベースの認可の認証ルールを設定します。
ステップ 2	**interface** *type slot/port*	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 ベースの認証で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 3	**ip access-group** *name*	デフォルトの ACL を適用します。
ステップ 4	**ip admission** *name*	指定したインターフェイスに Web ベースの認証を設定します。
ステップ 5	**exit**	コンフィギュレーション モードに戻ります。
ステップ 6	**ip device tracking**	IP 装置追跡テーブルをイネーブルにします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip admission configuration**	設定を表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポート FastEthernet 5/1 で Web ベースの認証をイネーブルにする例を示します。

```
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 configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name webauth1
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 認証の設定

	コマンド	目的
ステップ 1	**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 group** {*tacacs+* | *radius*}	ログイン時に認証方式のリストを定義します。
ステップ 3	**aaa authorization auth-proxy default group** {*tacacs+* | *radius*}	Web ベースの認可の認可方式のリストを作成します。
ステップ 4	**tacacs-server host** {*hostname* | *ip_address*}	AAA サーバを指定します。RADIUS サーバについては、「スイッチと RADIUS サーバ間の通信設定」（P.13-11）を参照してください。
ステップ 5	**tacacs-server key** {*key-data*}	スイッチと TACACS サーバとの間で使用する認証キーおよび暗号キーを設定します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、AAA をイネーブルにする例を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group tacacs+
Switch(config)# aaa authorization auth-proxy default group tacacs+
```

スイッチと RADIUS サーバ間の通信設定

RADIUS セキュリティ サーバは次のもので識別されます。

- 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、同じ IP アドレスのサーバ上にある複数の 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（認証など）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には、次の作業を実行します。

	コマンド	目的
ステップ 1	**ip radius source-interface** *interface_name*	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 2	**radius-server host** {*hostname* | *ip-address*} **test username** *username*	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* オプションを指定すると、RADIUS サーバ接続の自動テストがイネーブルになります。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** オプションでは、スイッチと RADIUS サーバとの間で使用する認証キーおよび暗号キーを指定します。 複数の RADIUS サーバを使用するには、サーバごとにこのコマンドを再入力します。
ステップ 3	**radius-server key** *string*	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キーおよび暗号キーを設定します。
ステップ 4	**radius-server vsa send authentication**	RADIUS サーバからの ACL のダウンロードをイネーブルにします。この機能は、Cisco IOS Release 12.2(50)SG でサポートされます。
ステップ 5	**radius-server dead-criteria tries** *num-tries*	サーバが非アクティブと見なされるまでの RADIUS サーバに対する非応答送信メッセージの数を指定します。*num-tries* に指定できる値の範囲は 1 ～ 100 です。

RADIUS サーバ パラメータを設定するには、次の手順を実行します。

- 別のコマンドラインには、**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キーおよび暗号キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。
- **key** *string* を指定する場合、キーの途中および末尾の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。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。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 retransmit**、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、次の URL の 『*Cisco IOS Security Configuration Guide*』*Release 12.2* および『*Cisco IOS Security Command Reference*』*Release 12.2* を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

（注）　RADIUS サーバには、スイッチ IP アドレス、サーバとスイッチの両方で共有するキー文字列、Downloadable ACL（DACL; ダウンロード可能 ACL）などのいくつか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。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2
```

HTTP サーバの設定

Web ベースの認証を使用するには、スイッチ内で HTTP サーバをイネーブルにする必要があります。HTTP または HTTPS のいずれかに対してサーバをイネーブルにできます。

	コマンド	目的
ステップ 1	**ip http server**	HTTP サーバをイネーブルにします。Web ベースの認証機能では、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 2	**ip http secure-server**	HTTPS をイネーブルにします。

カスタムの認証プロキシ Web ページを設定するか、ログインの成功を示すリダイレクション URL を指定できます。

（注）　**ip http secure-secure** コマンドの入力時にセキュアな認証を行うために、ユーザが HTTP 要求を送信する場合でも、ログイン ページは常に HTTPS（セキュア HTTP）形式になります。

- 「認証プロキシ Web ページのカスタマイズ」
- 「ログインの成功を示すリダイレクション URL の設定」

認証プロキシ Web ページのカスタマイズ

Web ベースの認証の実行時にスイッチのデフォルト HTML ページの代わりとなる 4 つの HTML ページが表示されるように、Web 認証を設定できます。

カスタムの認証プロキシ Web ページの使用を指定するには、まずカスタムの HTML ファイルをスイッチのフラッシュ メモリに格納し、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	**ip admission proxy http login page file** *device:login-filename*	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の HTML ファイルのスイッチ メモリ ファイル システムにおける場所を指定します。*device:* はフラッシュ メモリです。
ステップ 2	**ip admission proxy http success page file** *device:success-filename*	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の HTML ファイルの場所を指定します。

	コマンド	目的
ステップ 3	**ip admission proxy http failure page file** *device:fail-filename*	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の HTML ファイルの場所を指定します。
ステップ 4	**ip admission proxy http login expired page file** *device:expired-filename*	デフォルトのログイン期限切れページの代わりに使用するカスタムの HTML ファイルの場所を指定します。

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

- カスタムの Web ページ機能をイネーブルにするには、4 つのカスタム HTML ファイルをすべて指定します。4 つよりも少ない数のファイルを指定すると、内部のデフォルト HTML ページが使用されます。
- 4 つのカスタム HTML ファイルは、スイッチのフラッシュ メモリに格納する必要があります。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページのイメージはすべてアクセス可能な HTTP サーバに格納する必要があります。アドミッション ルール内でインターセプト ACL を設定します。
- カスタム ページからの外部リンクには、アドミッション 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。
- 有効な Domain Name System（DNS; ドメイン ネーム システム）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、アドミッション 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。
- カスタムの Web ページ機能がイネーブルの場合、設定された auth-proxy-banner は使用されません。
- カスタムの Web ページ機能がイネーブルの場合、ログイン成功機能のリダイレクション URL は使用できません。
- カスタム ファイルの指定を削除するには、このコマンドの **no** 形式を使用します。

カスタムのログイン 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点に注意してください。

- ログイン フォームはユーザ名とパスワードのユーザ エントリを受け入れる必要があります。また、それらのユーザ名とパスワードは **uname** および **pwd** として表示される必要があります。
- カスタムのログイン ページは、ページ タイムアウト、非表示パスワード、冗長な送信の回避など、Web フォームのベスト プラクティスに従う必要があります。

次に、カスタムの認証プロキシ Web ページを設定する例を示します。

```
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
```

次に、カスタムの認証プロキシ Web ページの設定を検証する例を示します。

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

ログインの成功を示すリダイレクション URL の設定

認証後にユーザがリダイレクトされる URL を指定できます。この URL は内部の*成功* HTML ページを置き換えます。

コマンド	目的
ip admission proxy http success redirect *url-string*	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。

ログインの成功を示すリダイレクション URL を設定する場合は、次の点に注意してください。

- カスタムの認証プロキシ Web ページ機能がイネーブルの場合、リダイレクション URL 機能はディセーブルになり、CLI で使用できません。カスタムのログイン成功ページでリダイレクションを実行できます。
- リダクレイション URL 機能がイネーブルの場合、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 の指定を削除するには、このコマンドの **no** 形式を指定します。

次に、ログインの成功を示すリダクレイション URL を設定する例を示します。

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

次に、ログインの成功を示すリダクレイション URL を検証する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 失敗ポリシーの設定

	コマンド	目的
ステップ 1	**ip admission name** *rule-name* **proxy http event timeout aaa policy identity** *identity_policy_name*	AAA 失敗ルールを作成し、AAA サーバに到達できない場合にセッションに適用されるアイデンティティ ポリシーを関連付けます。 **（注）** ルールを削除するには、**no ip admission name** *rule-name* **proxy http event timeout aaa policy identity** 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。
ステップ 2	**ip admission ratelimit aaa-down** *number_of_sessions*	（任意）AAA ダウン ステートでのホストからの認証試行回数をレート制限して、サービスに戻るときの AAA サーバのフラッディングを回避します。

次に、AAA 失敗ポリシーを適用する例を示します。

```
Switch(config)# ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy
identity GLOBAL_POLICY1
```

次に、接続されているホストが AAA ダウン ステートかどうかを確認する例を示します。

```
Switch# show ip admission cache
Authentication Proxy Cache
 Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

次に、ホスト IP アドレスに基づいて特定のセッションに関する詳細情報を表示する例を示します。

```
Switch# show ip admission cache 209.165.201.11
Address             : 209.165.201.11
MAC Address         : 0000.0000.0000
Interface           : Vlan333
Port                : 3999
Timeout             : 60
Age                 : 1
State               : AAA Down
AAA Down policy     : AAA_FAIL_POLICY
```

Web ベースの認証パラメータの設定

クライアントが待機期間にウォッチ リストに置かれるまでのログイン失敗最大試行回数を設定できます。

	コマンド	目的
ステップ 1	**ip admission max-login-attempts** *number*	ログイン失敗最大試行回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルト値は 5 です。
ステップ 2	**end**	特権 EXEC モードに戻ります。
ステップ 3	**show ip admission configuration**	認証プロキシ設定を表示します。
ステップ 4	**show ip admission cache**	認証エントリのリストを表示します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ログイン失敗最大試行回数を 10 に設定する例を示します。

```
Switch(config)# ip admission max-login-attempts 10
```

Web 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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 admission auth-proxy-banner http** [*banner-text* | *file-path*]	ローカル バナーをイネーブルにします。 （任意）*C banner-text C* を入力してカスタム バナーを作成します。ここで、*C* はデリミタを示します。または、file-path でバナーに表示されるファイル（ロゴやテキスト ファイルなど）を指定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、カスタム メッセージ「*My Switch*」を含むローカル バナーを設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

ip auth-proxy auth-proxy-banner コマンドの詳細については、Cisco.com にある『*Cisco IOS Security Command Reference*』の「Authentication Proxy Commands」を参照してください。

Web ベースの認証キャッシュ エントリの削除

コマンド	目的
clear ip auth-proxy cache {* | *host ip address*}	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するには、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、特定の IP アドレスを入力します。
clear ip admission cache {* | *host ip address*}	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するには、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、特定の IP アドレスを入力します。

次に、IP アドレス 209.165.201.1 にあるクライアントの Web ベースの認証セッションを削除する例を示します。

```
Switch# clear ip auth-proxy cache 209.165.201.1
```

Web ベースの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の Web ベースの認証設定を表示するには、次の作業を実行します。

	コマンド	目的
ステップ 1	**show authentication sessions** [**interface** *type slot/port*]	Web ベースの認証設定を表示します。 type = fastethernet、gigabitethernet または tengigabitethernet （任意）特定のインターフェイスの Web ベースの認証設定を表示するには、**interface** キーワードを使用します。

次に、グローバルな Web ベースの認証ステータスだけを表示する例を示します。

```
Switch# show authentication sessions
```

次に、ギガビット インターフェイス 3/27 の 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
```