



Web ベース認証の設定

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

- 「Web ベース認証の概要」(P.10-1)
- 「Web ベース認証の設定」(P.10-9)
- 「Web ベース認証ステータスの表示」(P.10-18)



(注)

この章で使用するスイッチ コマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

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、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。ユーザは証明書を入力します。この証明書は、Web ベース認証機能により、認証のために Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) サーバに送信されます。

認証に成功した場合、Web ベース認証は、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。

ここでは、AAA の一部としての Web ベース認証の役割について説明します。

- 「デバイスの役割」(P.10-2)
- 「ホストの検出」(P.10-2)
- 「セッションの作成」(P.10-3)
- 「認証プロセス」(P.10-3)

- 「Web 認証カスタマイズ可能な Web ページ」(P.10-6)
- 「その他の機能と Web ベース認証の相互作用」(P.10-7)

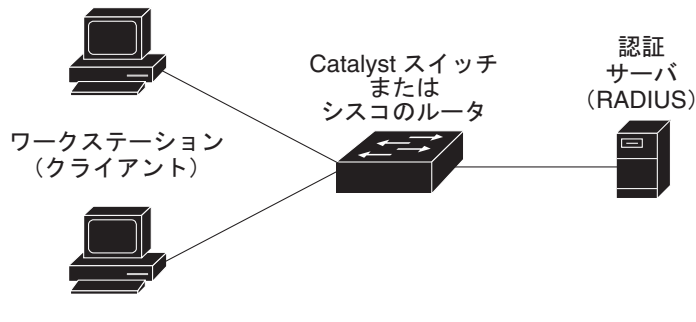
デバイスの役割

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 およびスイッチ 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、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可するか、拒否する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 10-1 は、ネットワークでのこれらのデバイスの役割を示しています。

図 10-1 Web ベース認証デバイスの役割



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ために、IP デバイス トラッキング テーブルを維持します。



(注)

デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。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。

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：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：スイッチにより、このホストに対する DHCP バインディング エントリが作成されると、Web ベース認証に通知が送られます。

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 NonResponsive-Host (NRH; 応答しないホスト) 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しない場合、AAA 失敗ポリシーが設定されていれば、スイッチは失敗アクセス ポリシーにホストを適用します。ログインの成功ページがユーザに送信されます（「ローカル Web 認証バナー」(P.10-4) を参照）。
- ホストがレイヤ 2 インターフェイス上の ARP プロ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。
- 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

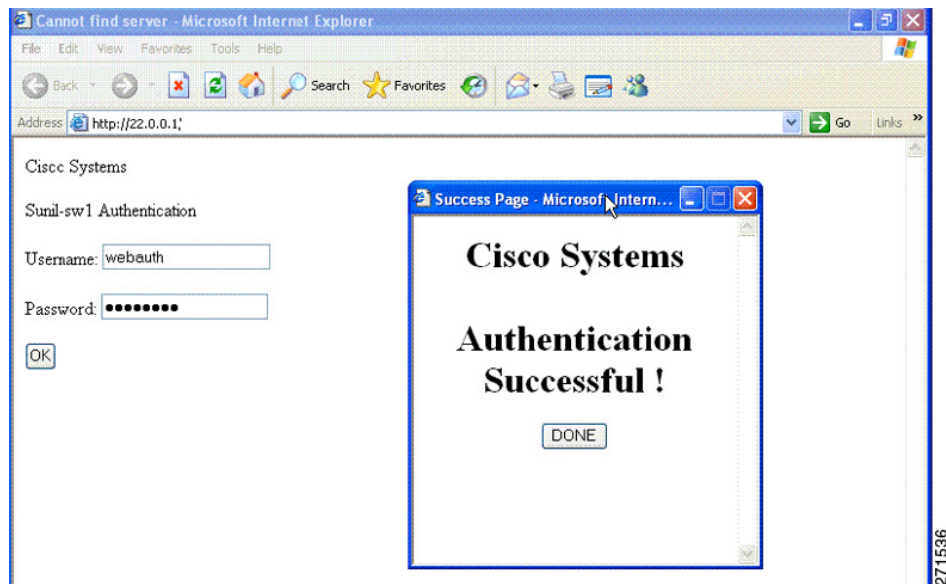
Web 認証を使用してスイッチにログインしたときに表示されるバナーを作成できます。

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。

- 認証成功
- 認証失敗
- 認証期限切れ

バナーを作成するには、**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。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、図 10-2 に示すように、認証結果のポップアップ ページに表示されます。

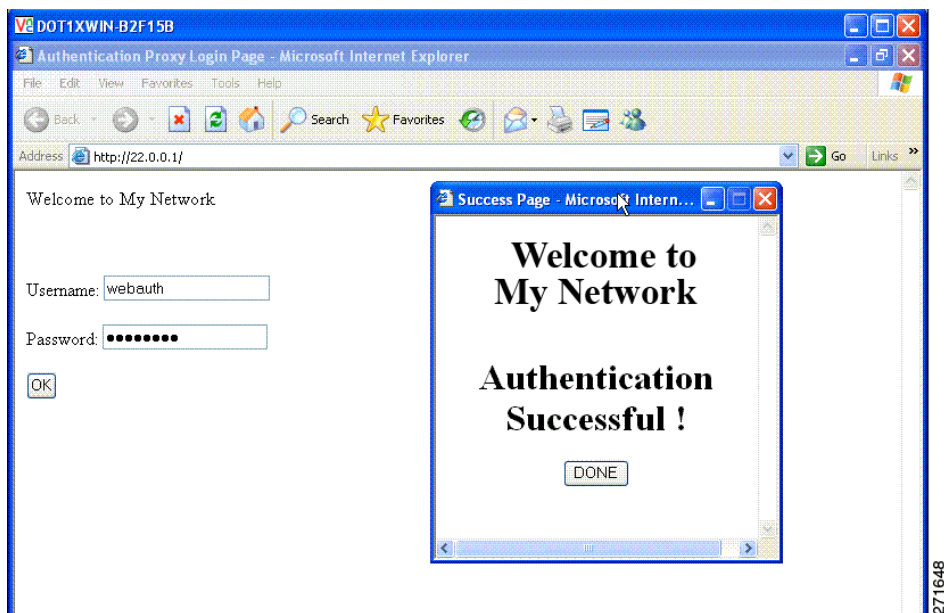
図 10-2 認証成功バナー



また、図 10-3 に示すように、バナーをカスタマイズすることもできます。

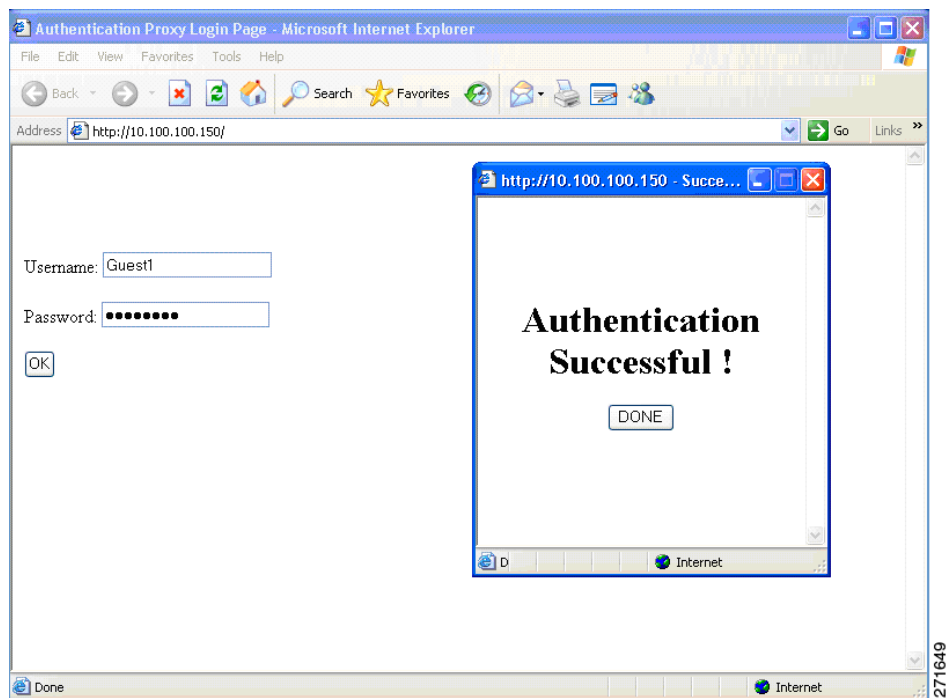
- バナーにスイッチ、ルータ、または会社名を追加するには、**ip admission auth-proxy-banner http banner-text** グローバル コンフィギュレーション コマンドを使用します。
- バナーにロゴ、またはテキスト ファイルを追加するには、**ip admission auth-proxy-banner http file-path** グローバル コンフィギュレーション コマンドを使用します。

図 10-3 カスタマイズされた Web バナー



バナーがイネーブルにされていない場合、図 10-4 に示すように、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 10-4 バナーが表示されていないログイン画面



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.10-17) を参照してください。

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。

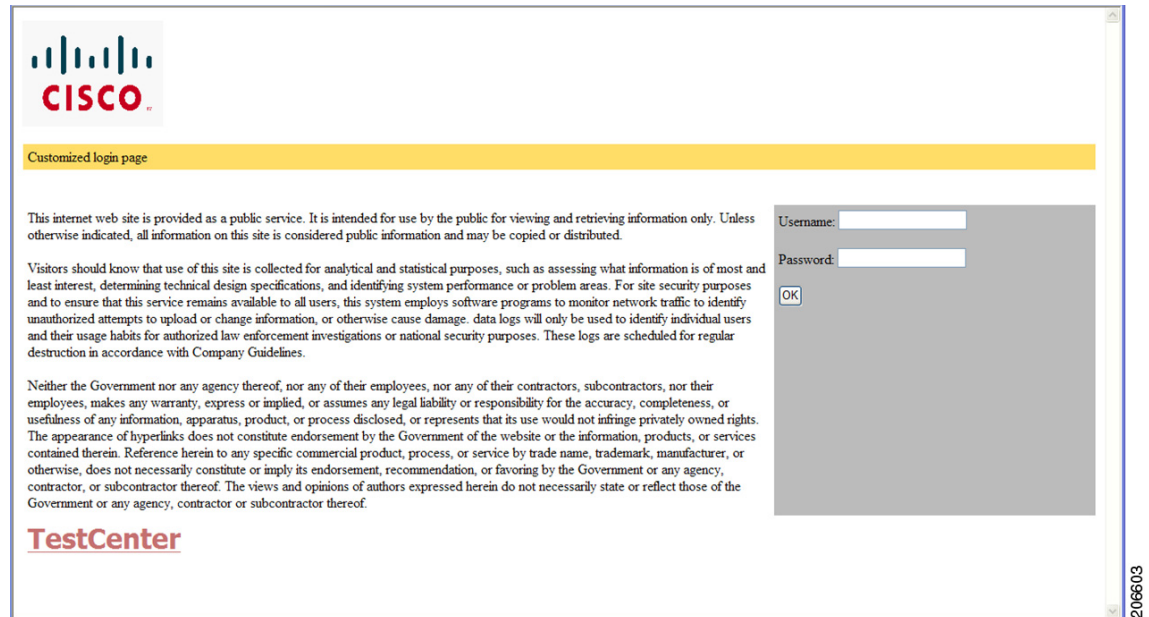
- ログイン：証明書が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになります。

注意事項

- 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。
- 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、またはメンバーのフラッシュ）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。

図 10-5 (P.10-7) に示すとおり、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。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 10-5 カスタマイズ可能な認証ページ



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.10-14) を参照してください。

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」(P.10-7)
- 「LAN ポート IP」(P.10-8)
- 「ゲートウェイ IP」(P.10-8)
- 「ACL」(P.10-8)
- 「コンテキストベース アクセス コントロール」(P.10-8)
- 「802.1x 認証」(P.10-8)
- 「EtherChannel」(P.10-8)

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。

ポート セキュリティをイネーブルにする手順については、「[ポート セキュリティの設定](#)」(P.23-9) を参照してください。

LAN ポート IP

LAN Port IP (LPIP; LAN ポート IP) 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 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入力トラフィックについて、Port ACL (PACL; ポート ACL) をデフォルトのアクセス ポリシーとして設定する必要があります。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。

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

Context-Based Access Control (CBAC; コンテキストベース アクセス コントロール) 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。

802.1x 認証

フォールバック認証メソッドとして設定する場合を除き、Web ベース認証は 802.1x 認証と同じポート上には設定できません。

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、すべてのメンバー チャネルに適用されます。

Web ベース認証の設定

- 「デフォルトの Web ベース認証の設定」 (P.10-9)
- 「Web ベース認証の設定に関する注意事項と制約事項」 (P.10-9)
- 「Web ベース認証の設定タスク リスト」 (P.10-10)
- 「認証ルールとインターフェイスの設定」 (P.10-10)
- 「AAA 認証の設定」 (P.10-11)
- 「スイッチから RADIUS サーバへの通信のコンフィギュレーション」 (P.10-12)
- 「HTTP サーバの設定」 (P.10-13)
- 「Web ベース認証パラメータの設定」 (P.10-16)
- 「Web ベース認証キャッシュ エントリの削除」 (P.10-17)

デフォルトの Web ベース認証の設定

表 10-1 は、デフォルトの Web ベース認証の設定を示しています。

表 10-1 デフォルトの Web ベース認証の設定

機能	デフォルト設定
Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग)	ディセーブル
RADIUS サーバ	
• IP アドレス	• 指定なし
• UDP 認証ポート	• 1812
• 鍵	• 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ていません。
- 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 デバイス トラッキング機能はディセーブルに設定されています。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。
- IPv6 トラフィックについては、Web ベース認証はサポートされていません。

Web ベース認証の設定タスク リスト

- 「認証ルールとインターフェイスの設定」(P.10-10)
- 「AAA 認証の設定」(P.10-11)
- 「スイッチから RADIUS サーバへの通信のコンフィギュレーション」(P.10-12)
- 「HTTP サーバの設定」(P.10-13)
- 「AAA 失敗ポリシーの設定」(P.10-16)
- 「Web ベース認証パラメータの設定」(P.10-16)
- 「Web ベース認証キャッシュ エントリの削除」(P.10-17)

認証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 ベース認証で使用する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 ベースの認証のためにイネーブルにされる入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 <i>type</i> 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 ACL を適用します。
ステップ 4	ip admission name	指定されたインターフェイスに Web ベース認証を設定します。
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 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 7	end	特権 EXEC モードに戻ります。
ステップ 8	show ip admission configuration	コンフィギュレーションを表示します。
ステップ 9	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。

次に、Fast Ethernet ポート 5/1 で Web ベース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}	ログイン時の認証方法のリストを定義します。
ステップ 3	aaa authorization auth-proxy default group {tacacs+ radius}	Web ベースの認証で使用される認証方法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、「スイッチから RADIUS サーバへの通信のコンフィギュレーション」(P.10-12)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 サーバの間で使用される認証および暗号鍵を設定します。
ステップ 6	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。

次の例では、AAA をイネーブルにする方法を示します。

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

スイッチから RADIUS サーバへの通信のコンフィギュレーション

RADIUS セキュリティ サーバの識別情報は次のとおりです。

- ホスト名
- ホスト IP アドレス
- ホスト名および特定の UDP ポート番号
- IP アドレスおよび特定の 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手順は、次のとおりです。

	コマンド	目的
ステップ 1	ip radius source-interface <i>interface_name</i>	RADIUS パケットが、指示されたインターフェイスの IP アドレスを持つことを指定します。
ステップ 2	radius-server host { <i>hostname</i> <i>ip-address</i> } test username <i>username</i>	リモート RADIUS サーバホストのホスト名または IP アドレスを指定します。 test username <i>username</i> 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 <i>username</i> 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鍵を指定します。 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。
ステップ 3	radius-server key <i>string</i>	RADIUS サーバ上で動作するスイッチと RADIUS デーモンの間で使用される認証および暗号鍵を設定します。
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 でサポートされています。
ステップ 5	radius-server dead-criteria tries <i>num-tries</i>	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。

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。

- **key string** は独立したコマンドラインに指定します。
- **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鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト スtring でなければなりません。

- **key string** を指定する場合、鍵の中間、および末尾にスペースを使用します。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵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、および暗号鍵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 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 にある『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 サーバでは、スイッチ IP アドレス、サーバとスイッチで共有される **key string**、および Downloadable ACL (DACL; ダウンロード可能な ACL) 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。

次の例では、スイッチで RADIUS サーバパラメータを設定する方法を示します。

```
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 ベース認証を使用するには、スイッチで 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。

	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 2	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-secure** 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。

- [認証プロキシ Web ページのカスタマイズ](#)
- [成功ログインに対するリダイレクション URL の指定](#)

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、スイッチのデフォルト HTML ページではなく、代替りの 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、まず、カスタム HTML ファイルをスイッチのフラッシュ メモリに保存し、次にグローバル コンフィギュレーション モードでこのタスクを実行します。

	コマンド	目的
ステップ 1	ip admission proxy http login page file <i>device:login-filename</i>	スイッチのメモリ ファイル システムで、デフォルトのログイン ページの代わりに使用されるカスタム HTML ファイルの所在地を指定します。 <i>device:</i> はフラッシュ メモリです。
ステップ 2	ip admission proxy http success page file <i>device:success-filename</i>	デフォルトのログイン成功ページの代わりに使用されるカスタムの HTML ファイルの所在地を指定します。
ステップ 3	ip admission proxy http failure page file <i>device:fail-filename</i>	デフォルトのログイン失敗ページの代わりに使用されるカスタムの HTML ファイルの所在地を指定します。
ステップ 4	ip admission proxy http login expired page file <i>device:expired-filename</i>	デフォルトのログイン期限切れページの代わりに使用されるカスタムの HTML ファイルの所在地を指定します。

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 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。

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
```

次の例では、カスタム認証プロキシ Web ページの設定を確認する方法を示します。

```
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
```

成功ログインに対するリダイレクション URL の指定

認証後に、内部成功 HTML ページを効果的に置き換え、ユーザのリダイレクト先となる URL を指定することができます。

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、ユーザのリダイレクト先となる URL を指定します。

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。
- 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。

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

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 を確認する方法を示します。

```
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 サーバに到達できない場合、AAA 失敗ルールを作成し、セッションに適用される ID 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、ホストからの認証の試行をレート制限し、サービスに戻ってきたときの AAA サーバ 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 ステートであるかどうかを判断する例を示します。

```
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 ベース認証パラメータの設定

失敗できるログイン試行回数の最大値を設定します。失敗した試行回数がこの値を超えると、クライアントは待機期間中、ウォッチ リストに載せられます。

	コマンド	目的
ステップ 1	ip admission max-login-attempts number	失敗できるログイン試行の最高回数を設定します。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	認証プロシキ設定を表示します。
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) コンフィギュレーション ファイルに設定を保存します。

次の例では、失敗ログイン試行の最大回数を 10 に設定する方法を示します。

```
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) <i>C banner-text C</i> と入力して、カスタム バナーを作成します。 ここで、 <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（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	特権 EXEC モードに戻ります。
ステップ 4	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。

次の例では、「*My Switch*」というカスタム メッセージが表示されているローカル バナーを設定する方法を示します。

```
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 の『[Cisco IOS Security Command Reference](#)』にある「Authentication Proxy Commands」セクション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

コマンド	目的
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。
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。

次に、IP アドレス 209.165.201.1 のクライアントに対する Web ベース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。

	コマンド	目的
ステップ 1	show authentication sessions [<i>interface type slot/port</i>]	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。

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
```

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
```