CHAPTER 11

Web ベース認証の設定

この章では、Catalyst 3750-E または 3560-E スイッチで 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。

（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、このリリースのコマンド リファレンスを参照してください。

Web ベース認証の概要

Web ベース認証機能は、*Web 認証プロキシ*とも呼ばれ、IEEE 802.1x サプリカントが実行されていないホスト システムでエンド ユーザを認証するために使用されます。

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

HTTP セッションを開始すると、ホストから着信した HTTP パケットが Web ベース認証によって代行受信され、HTML ログイン ページがユーザに送信されます。ユーザが自分の資格情報を入力すると、その情報が Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバに送信され、認証されます。

認証が成功すると、ログイン成功の HTML ページがホストに送信され、AAA サーバから返されたアクセス ポリシーが適用されます。

認証が失敗すると、ログイン失敗の HTML ページがユーザに転送され、ログインの再入力をユーザに要求するプロンプトが表示されます。ユーザの試行回数が最大数を超えると、ログイン失効の HTML ページがホストに転送され、そのユーザは待機時間のウォッチ リストに配置されます。

ここでは、AAA の一部として Web ベース認証が果たす役割について説明します。

- 「Web ベース認証と他の機能の相互作用」（P.11-7）

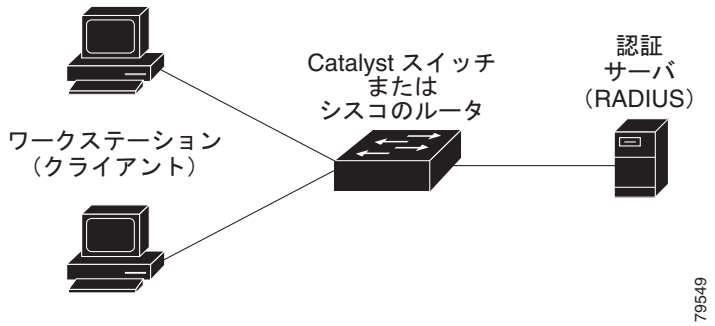
デバイスの役割

Web ベース認証では、ネットワーク上のデバイスにそれぞれ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）。ワークステーションは、Java スクリプトがイネーブルになっている 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べきかどう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 11-1 に、ネットワーク内のデバイスの役割を示します。

図 11-1　Web ベース認証におけるデバイスの役割



ホストの検出

スイッチは、検出したホストの情報を格納するために IP デバイス トラッキング テーブルを保持します。

（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なっています。Web ベース認証を使用するには、IP デバイス 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 インターフェイスの場合、Web ベース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 トリガー：Web ベース認証では、ARP リダイレクト ACL によって固定 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 ベース認証で新しいホストが検出されると、次のようにしてセッションが作成されます。

- 例外リストを確認します。

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

- 許可バイパスを確認します。

  ホスト IP が例外リストに含まれていない場合は、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* である場合は、このホストの許可がバイパスされます。セッションが確立されます。

- HTTP 代行受信 ACL を設定します。

  NRH 要求に対するサーバの応答が *access rejected* である場合は、HTTP 代行受信 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、許可が開始されます。スイッチからユーザにログイン ページが送信されます。ユーザがユーザ名とパスワードを入力すると、その入力内容がスイッチから認証サーバに送信されます。
- 認証が成功すると、ユーザのアクセス ポリシーが認証サーバからスイッチにダウンロードされ、アクティブになります。ログイン成功ページがユーザに送信されます。
- 認証が失敗すると、スイッチからログイン失敗ページが送信されます。ユーザがログインを再試行します。最大試行回数を超過すると、スイッチからログイン失効ページが送信され、ホストがウォッチ リストに配置されます。ウォッチ リストがタイムアウトすると、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や、AAA 失敗ポリシーが設定されている場合は、スイッチによって失敗アクセス ポリシーがホストに適用されます。ログイン成功ページがユーザに送信されます（「ローカル Web 認証バナー」（P.11-4）を参照）。
- ホストがレイヤ 2 インターフェイスの ARP プローブに応答しない場合や、ホストがレイヤ 3 インターフェイスでアイドル タイムアウトまでにトラフィックを送信しない場合は、スイッチによってクライアントが再認証されます。
- この機能は、ダウンロードされたタイムアウトやローカルに設定されたセッション タイムアウトに適用されます。
- 終了アクションが RADIUS の場合は、nonresponsive host（NRH）要求がサーバに送信されます。終了アクションはサーバからの応答に含まれています。
- 終了アクションがデフォルトの場合は、セッションが破棄され、適用されたポリシーが削除されます。

ローカル Web 認証バナー

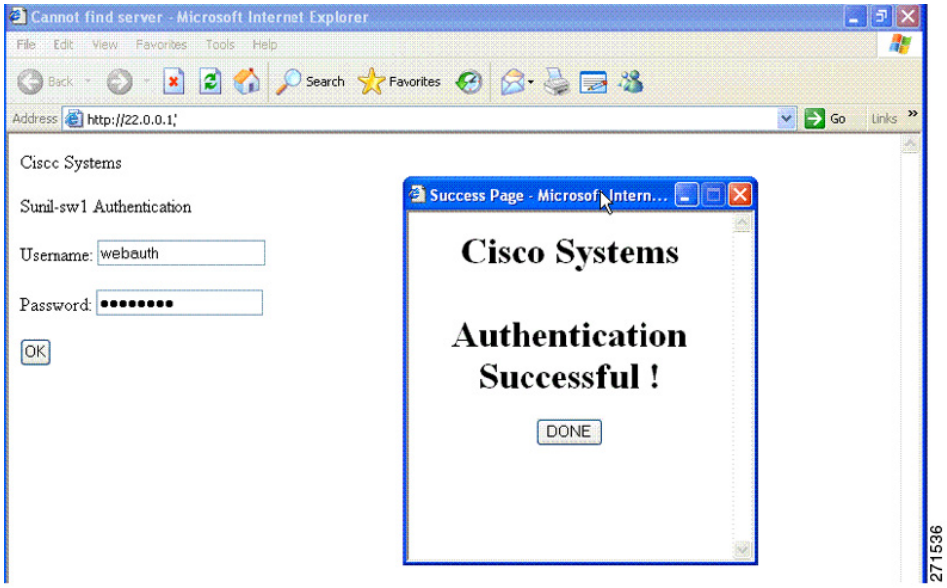
Web 認証を使用してスイッチにログインするときに表示するバナーを作成できます。

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である *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* は認証結果ポップアップ ページに表示されます（図 11-2 を参照）。

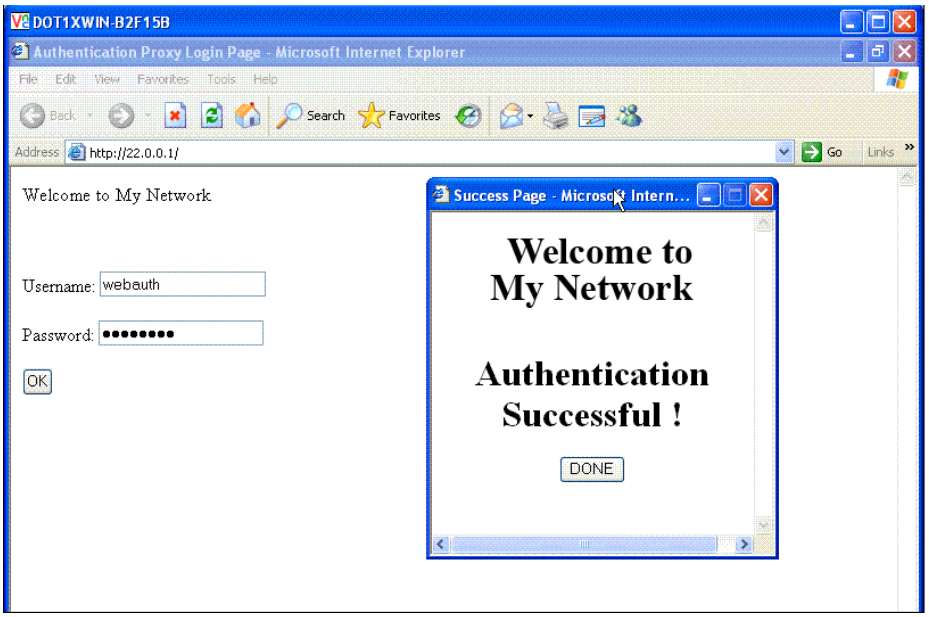
図 11-2　Authentication Successful のバナー



このバナーを図 11-3 のようにカスタマイズすることもできます。

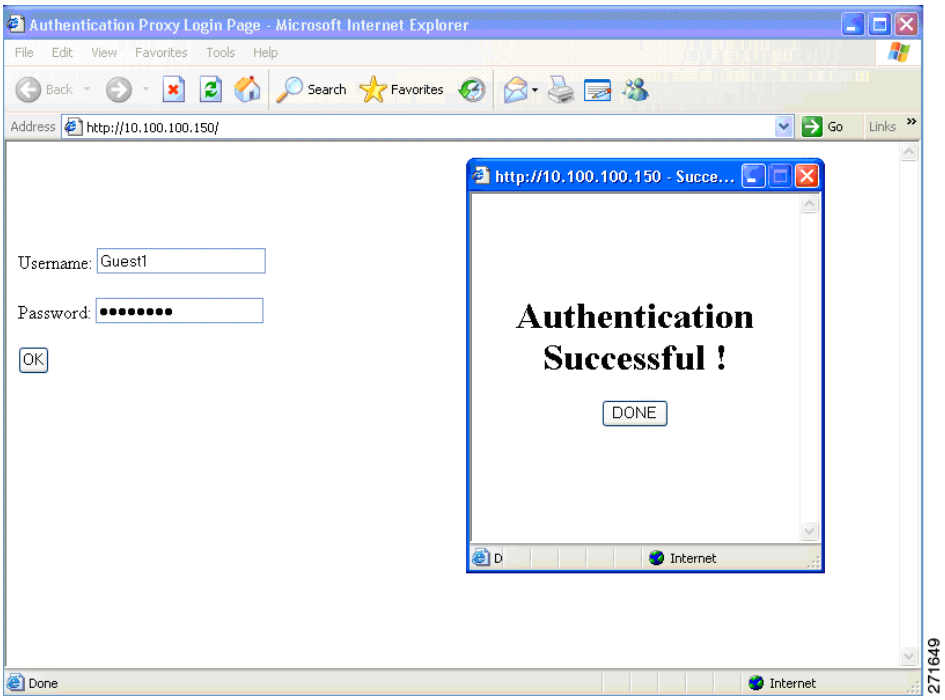
- **ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用して、スイッチ、ルータ、または会社名をバナーに追加します。
- **ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用して、ロゴまたはテキスト ファイルをバナーに追加します。

図 11-3　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と、ユーザ名およびパスワード ダイアログボックスだけが Web 認証ログイン画面に表示され、スイッチにログインしてもバナーは表示されません（図 11-4 を参照）。

図 11-4　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.11-16）を参照してください。

Web 認証の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 サーバが認証対象のクライアントに配信する 4 つの HTML ページを提供します。このサーバは、これらのページを使用して次の 4 つの認証プロセス状態をユーザに通知します。

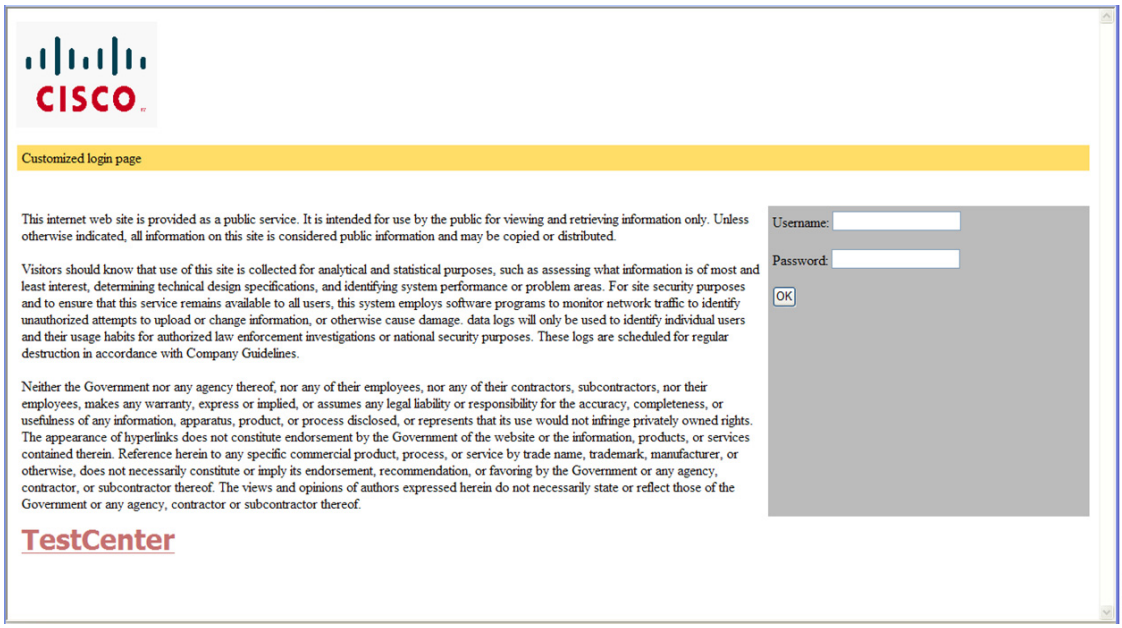
- ログイン：ユーザの資格情報が要求されます。
- 成功：ログインが成功しました。
- 失敗：ログインが失敗しました。
- 失効：ログインの失敗回数が多すぎるため、ログイン セッションが失効しました。

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 ページを使用できます。
- *ログイン*、*成功*、*失敗*、*失効*の各 Web ページには、ロゴを使用したり、テキストを指定できます。
- バナー ページには、ログイン ページのテキストを指定できます。
- 各ページは HTML 形式で記述します。
- 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 コマンドを含める必要があります。
- この URL 文字列は、有効な URL（たとえば、http://www.cisco.com など）である必要があります。不完全な URL を指定すると、Web ブラウザ上で *page not found* などのエラーが発生することがあります。
- HTTP 認証用の Web ページを設定する場合は、Web ページに適切な HTML コマンドを含める必要があります。たとえば、ページのタイムアウトを設定するコマンド、非表示パスワードを設定するコマンド、同じページが 2 回送信されていないことを確認するコマンドなどです。
- 設定したログイン フォームがイネーブルになっている場合は、ユーザを特定の URL にリダイレクトする CLI コマンドを使用できません。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確認する必要があります。
- 認証の実行後にユーザを特定の URL にリダイレクトする CLI コマンドを入力し、次に Web ページを設定するコマンドを入力すると、ユーザを特定の URL にリダイレクトする CLI コマンドが無効になります。
- 設定した 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 つのフラッシュに格納し、成功および失敗ページを別のフラッシュ（スタック マスターやスタック メンバーのフラッシュなど）に格納することもできます。
- 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 ページで設定しても影響を受けません。
- システム ディレクトリ（flash、disk0、disk など）に格納され、ログイン ページに表示する必要があるすべてのロゴ ファイル（イメージ、フラッシュ、音声、ビデオなど）は、ファイル名を *web_auth_<filename>* とする必要があります。
- 設定済みの認証プロキシ機能は、HTTP と SSL の両方をサポートします。

デフォルトの内部 HTML ページの代わりに、図 11-5（P.11-7）に示すような独自の HTML ページを使用できます。また、認証の実行後にユーザをリダイレクトする宛先 URL を指定して、内部の成功ページを置き換えることもできます。

図 11-5　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.11-13）を参照してください。

Web ベース認証と他の機能の相互作用

- 「ポート セキュリティ」（P.11-7）
- 「LAN ポート IP」（P.11-7）
- 「ゲートウェイ IP」（P.11-8）
- 「ACL」（P.11-8）
- 「コンテキストベースのアクセス制御」（P.11-8）
- 「802.1x 認証」（P.11-8）
- 「EtherChannel」（P.11-8）

ポート セキュリティ

Web ベース認証とポート セキュリティを同じポートに設定できます。Web ベース認証によってポートが認証され、ポート セキュリティによってクライアントを含むすべての MAC アドレスのネットワーク アクセスが管理されます。この場合、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とグループを制限できます。

ポート セキュリティのイネーブル化の詳細については、「ポート セキュリティの設定」（P.26-9）を参照してください。

LAN ポート IP

LAN ポート IP（LPIP）とレイヤ 2 の Web ベース認証を同じポートに設定できます。最初に Web ベース認証を使用してホストが認証され、その後 LPIP ポスチャ検証が実行されます。LPIP ホスト ポリシーは、Web ベース認証ホスト ポリシーを上書きします。

Web ベース認証アイドル タイマーが満了すると、NAC ポリシーが削除されます。ホストが認証され、ポスチャが再び検証されます。

ゲートウェイ IP

Web ベース認証が VLAN のスイッチ ポートに設定されている場合は、レイヤ 3 VLAN インターフェイスにゲートウェイ IP（GWIP）を設定できません。

ゲートウェイ IP と同じレイヤ 3 インターフェイスに Web ベース認証を設定できます。ソフトウェア内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 ベース認証ホスト ポリシーを上書きします。

ACL

インターフェイスに VLAN ACL または Cisco IOS ACL を設定すると、Web ベース認証ホスト ポリシーが適用されてからホスト トラフィックに ACL が適用されます。

レイヤ 2 Web ベース認証の場合は、ポートに接続されたホストからの入力トラフィックのデフォルト アクセス ポリシーとしてポート ACL（PACL）を設定する必要があります。認証後、Web ベース認証ホスト ポリシーは PACL を上書きします。

MAC ACL と Web ベース認証は同じインターフェイスに設定できません。

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 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は、Web ベース認証をレイヤ 2 ポートに設定できません。

802.1x 認証

Web ベース認証は、フォールバック認証方式として設定する場合を除き、802.1x 認証と同じポートには設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイスに設定できます。Web ベース認証の設定は、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

表 11-1 に、デフォルトの Web ベース認証の設定を示します。

表 11-1　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	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 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 ベース認証設定時の注意事項および制限事項

- Web ベースの認証は入力専用の機能です。
- Web ベース認証を設定できるのはアクセス ポートだけです。トランク ポート、EtherChannel メンバー ポート、ダイナミック トランク ポートでは Web ベース認証はサポートされません。
- Web ベース認証を設定する前に、デフォルト ACL をインターフェイスに設定する必要があります。レイヤ 2 インターフェイスのポート ACL を設定するか、レイヤ 3 インターフェイスの Cisco IOS ACL を設定します。
- レイヤ 2 インターフェイスでは、スタティック ARP キャッシュが割り当てられている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 デバイス トラッキング機能はディセーブルになっています。Web ベース認証を使用するには、IP デバイス トラッキング機能をイネーブルにする必要があります。

- スイッチの HTTP サーバを実行するには、少なくとも 1 つの IP アドレスを設定する必要があります。各ホスト IP アドレスに到達するためのルートも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。
- STP トポロジの変更によってホスト トラフィックが別のポートに着信すると、2 ホップ以上離れたホストでトラフィックが中断されることがあります。この現象は、レイヤ 2（STP）トポロジーの変更後に ARP と DHCP のアップデートが送信されない場合があるためです。
- Web ベース認証では、VLAN 割り当てはダウンロード可能なホスト ポリシーとしてサポートされません。
- IPv6 トラフィックでは Web ベース認証はサポートされません。

Web ベース認証の設定作業リスト

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 モードに移行し、Web ベース認証のためにイネーブルにするレイヤ 2 またはレイヤ 3 入力インターフェイスを指定します。 *type* には fastethernet、gigabitethernet、または tengigabitethernet を指定します。
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*	指定し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**	設定を表示します。
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、ファスト イーサネット 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式リストを定義します。
ステップ 3	**aaa authorization auth-proxy default group** {*tacacs+* | *radius*}	Web ベース認証用の許可方式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、「スイッチおよび RADIUS サーバ間の通信の設定」（P.11-11）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 サーバの間で使用す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+
```

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは次の項目を識別します。

- 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 番目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 サーバのパラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**ip radius source-interface** *interface_name*	指定したインターフェイスの IP アドレスを RADIUS パケットに含めるように指定します。
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 サーバとの接続が自動的にテストされます。指定する *username* は有効なユーザ名でなくてもかまいません。 **key** オプションは、スイッチと RADIUS サーバの間で使用する認証および暗号鍵を指定します。 複数の RADIUS サーバを使用する場合は、サーバごとにこのコマンドを繰り返し入力します。
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 デーモンの間で使用する認証および暗号鍵を指定します。
ステップ 4	**radius-server vsa send authentication**	RADIUS サーバから ACL をダウンロードをできるようにします。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** *num-tries*	RADIUS サーバから応答がない場合に、サーバが非アクティブであると見なすまでに送信するメッセージの数を指定します。指定できる *num-tries* の範囲は 1 ～ 100 です。

RADIUS サーバのパラメータを設定するときは、次の注意事項に留意してください。

- **key** *string* は別のコマンド行に指定します。
- **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 ストリングでなければなりません。
- **key** *string* を指定するときは、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。
- タイムアウト、再送信回数、および暗号鍵の値をすべての RADIUS サーバに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）　スイッチの IP アドレス、サーバとスイッチで共有するキー ストリング、ダウンロード可能 ACL（DACL）など、RADIUS サーバのいくつかの値を設定する必要があります。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、スイッチ上で RADIUS サーバの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 ベース認証を使用するには、スイッチ内部の 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 のサーバをイネーブルにすることができます。

	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ユーザ認証に関するやり取りを行います。
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 ページを設定したり、ログイン成功時のリダイレクト URL を指定したりできます。

（注）　**ip http secure-server** コマンドの入力時にセキュア認証を確保するため、ユーザが HTTP 要求を送信した場合でも、ログイン ページは常に HTTPS（セキュア HTTP）で動作します。

- 「認証プロキシ Web ページのカスタマイズ」
- 「ログイン成功時のリダイレクト URL の指定」

認証プロキシ Web ページのカスタマイズ

Web ベース認証では、ユーザに対してスイッチのデフォルト HTML ページの代わりに 4 つの代替 HTML ページを表示するように 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 HTML ファイルが格納されたスイッチのメモリ ファイル システム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 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 HTML ファイルが格納された場所を指定します。

	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 HTML ファイルが格納された場所を指定します。
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失効ページの代わりに使用するカスタム HTML ファイルが格納された場所を指定します。

カスタマイズした認証プロキシ Web ページを設定するときは、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、4 つのカスタム HTML ファイルをすべて指定してください。指定したファイルが 4 つ未満の場合は、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 ページ上のイメージは、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 ルールの内部に代行受信 ACL を設定してください。
- カスタム ページで外部リンクを使用するには、アドミッション ルールの内部に代行受信 ACL を設定する必要があります。
- 有効な DNS サーバにアクセスするには、外部リンクやイメージに必要な名前解決のために、アドミッション ルールの内部に代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能をイネーブルにすると、設定済みの認証プロキシ用バナーが使用されません。
- カスタム Web ページ機能をイネーブルにすると、ログイン成功時のリダイレクト URL を使用できません。
- 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 ログイン ページは公開される Web フォームであるため、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、それらを **uname** および **pwd** として表示する必要があります。
- カスタム ログイン ページは、ページのタイムアウト、非表示パスワード、重複送信の防止など、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、カスタム認証プロキシ Web ページの設定を確認する例を示します。

```
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
```

ログイン成功時のリダイレクト URL の指定

認証後にユーザをリダイレクトする宛先 URL を指定できます。この URL は、実質的に内部の*成功* HTML ページの代わりになります。

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なる、ユーザをリダイレクトする宛先 URL を指定します。

ログイン成功時のリダイレクト URL を指定するときは、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 ページ機能をイネーブルにすると、リダイレクト URL 機能がディセーブルになり、CLI で使用できなくなります。リダイレクトはカスタム ログイン成功ページで実行できます。
- リダイレクト URL 機能をイネーブルにすると、設定済みの認証プロキシ用バナーが使用されません。
- リダイレクト URL 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。

次に、ログイン成功時のリダイレクト 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、ログイン成功時のリダイレクト URL を確認する例を示します。

```
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 サーバが到達不能な場合に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）稼動状態に戻った AAA サーバに対するフラッディングを回避するため、AAA ダウン状態のホストからの認証試行回数を制限します。

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、接続しているホストが AAA ダウン状態かどうかを判定する例を示します。

```
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

クライアントが待機時間のウォッチ リストに配置されるまでのログイン試行失敗の最大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*	ログイン試行失敗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 回です。
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**	認証プロキシの設定を表示します。
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。

次に、ログイン試行失敗の最大回数を 10 回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。

	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。*C* はデリミタです。file-path はバナーで表示されるファイル（たとえば、ロゴやテキスト ファイル）を示します。

	コマンド	目的
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。

次に、カスタム メッセージ *My Switch* を使用して、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 の『*Cisco IOS Security Command Reference*』の「Authentication Proxy Commands」を参照してください。

Web ベース認証のキャッシュ エントリの削除

コマンド	目的
clear ip auth-proxy cache {* | *host ip address*}	認証プロキシのエントリを削除します。アスタリスクを使用すると、すべてのキャッシュ エントリが削除されます。特定の IP アドレスを入力すると、1 つのホストのエントリが削除されます。
clear ip admission cache {* | *host ip address*}	認証プロキシのエントリを削除します。アスタリスクを使用すると、すべてのキャッシュ エントリが削除されます。特定の IP アドレスを入力すると、1 つのホストのエントリが削除されます。

次に、IP アドレスが 209.165.201.1 であるクライアントの 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 ベース認証のステータスの表示

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 ベース認証の設定を表示するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**show authentication sessions** [**interface** *type slot/port*]	Web ベース認証の設定を示します。 type には fastethernet、gigabitethernet、または tengigabitethernet を指定します。 （任意）特定のインターフェイスに対する Web ベース認証の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 ベース認証の設定を表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet 3/27
```