CHAPTER 42

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。この章の内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

Web ベース認証の概要

Web ベース認証機能（別名 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 ユーザを認証できます。

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

HTTP セッションを開始すると、Web ベース認証がホストからの入力 HTTP パケットを代行受信して、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。Web ベース認証はこのクレデンシャルを認証のために Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバに送信します。

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。

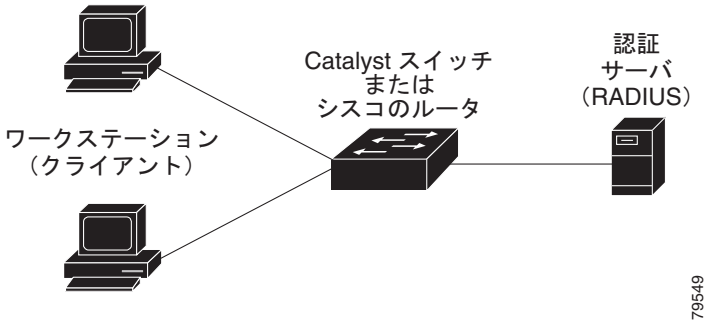
認証に失敗すると、Web ベース認証はログイン失敗 HTML ページをユーザに送信し、ユーザにログインを再試行するように要求します。ユーザが最大試行回数を超えると、Web ベース認証はログイン失効 HTML ページをホストに送信し、ユーザは待機期間の間ウォッチ リストに配置されます。

ここでは、認証、認可、アカウンティング（AAA）システムの一部としての Web ベース認証の役割について説明します。

装置の役割

Web ベース認証では、ネットワーク内の装置にそれぞれ特定の役割があります（図 42-1）。

図 42-1　Web ベース認証装置の役割



役割は次のとおりです。

- *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装置（ワークステーション）。ワークステーションは、Java Script が有効な HTML ブラウザを実行している必要があります。
- *認証サーバ*：クライアントの実際の認証を行います。認証サーバは、クライアントの識別情報を確認し、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を許可されたこと、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間の仲介装置（プロキシ）として機能し、クライアントに識別情報を要求して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。

ホスト検出

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 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、スイッチ上では IP デバイス トラッキング機能はディセーブルです。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 3 インターフェイスの場合、インターフェイス上に Web ベース認証が設定されると（またはインターフェイスがサービス中になると）、Web ベース認証が HTTP 代行受信 Access Control List（ACL; アクセス コントロール リスト）を設定します。

レイヤ 2 インターフェイスの場合、次のメカニズムを使用して Web ベース認証が IP ホストを検出します。

- Address Resolution Protocol（ARP; アドレス解決プロトコル）ベース トリガー：ARP リダイレクト ACL により、Web ベース認証は固定 IP アドレスまたは動的に取得された IP アドレスを持つホストを検出できます。
- Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）
- Dynamic Host Configuration Protocol（Dynamic Host Configuration Protocol）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。

セッション作成

Web ベース認証は新しいホストを検出すると、次のようにセッションを作成します。

- 例外リストをチェックします。

  ホスト IP が例外リストに含まれている場合、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。

- 認証バイパスをチェックします。

  ホスト IP が例外リストにない場合、Web ベース認証は Nonresponsive Host（NRH; 非応答ホスト）要求をサーバに送信します。

  サーバ応答が Access Accepted である場合、このホスト用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応答が Access Rejected である場合、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。スイッチは、ユーザにログイン ページを送信します。ユーザがログイン ページに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そのエントリを送信します。
- クライアント ID が有効で、認証に成功した場合、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。
- 認証に失敗した場合、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。最大試行回数を超えると、スイッチはログイン失効ページを送信し、ホストはウォッチ リストに配置されます。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障害アクセス 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 （「AAA 失敗ポリシー」（P.42-4）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 タイムアウト中にトラフィックを送信しない場合、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。
- 終了処理が Remote Authentication Dial-In User Service（RADIUS）の場合、この機能は非応答ホスト（NRH）要求をサーバに送信します。終了処理は、サーバからの応答に含まれています。
- 終了処理がデフォルトの場合、セッションが停止されて適用されたポリシーが削除されます。

AAA 失敗ポリシー

Cisco IOS Release 12.2(50)SG は AAA 失敗ポリシーをサポートします。このポリシーを使用すると、AAA サーバが使用できない場合に、ネットワークに接続したり、接続状態を維持できます。クライアントの Web ベース認証が必要なときに AAA サーバにアクセスできない場合、ユーザを拒否する（つまり、ネットワークへのアクセスを提供しない）代わりに、管理者はユーザに適用できるデフォルト AAA 失敗ポリシーを設定できます。

このポリシーは次の理由で便利です。

- AAA サーバが使用できない間、アクセスが制限されることがありますが、ネットワークには接続できます。
- AAA サーバが再び使用できるようになると、再確認されて、通常のアクセス ポリシーを AAA サーバからダウンロードできます。

（注）　AAA サーバがダウンすると、関連付けられた既存ポリシーがない場合に限り AAA 失敗ポリシーが適用されます。通常、セッションに再認証が必要なときに AAA サーバが使用できない場合、現在有効なポリシーが保持されます。

AAA 失敗ポリシーが有効な間は、セッション ステートは AAA ダウンとして維持されます。

認証プロキシ Web ページのカスタマイゼーション

Web ベース認証プロセス中、スイッチの内部 HTTP サーバは認証クライアントに提供するために 4 つの HTML ページをホストします。この 4 つのページでは、サーバは認証プロセスの次の 4 つのステートを通知します。

- [Login]：クレデンシャルが要求されます。
- [Success]：ログインに成功しました。
- [Fail]：ログインに失敗しました。
- [Expire]：ログイン試行回数を超えたため、ログイン セッションは期限切れになりました。

Cisco IOS Release 12.2(50)SG では、4 つのデフォルト内部 HTML ページの代わりにカスタム HTML ページを使用したり、認証に成功したあとにリダイレクトされる URL を指定して、内部成功ページを効率的に置き換えることができます。

Web ベース認証と他の機能との相互作用

ここでは、Web ベース認証と他の機能との相互作用について説明します。

- 「ポート セキュリティ」（P.42-5）
- 「LAN ポート IP（LPIP）」（P.42-5）

ポート セキュリティ

同じポート上で Web ベース認証とポート セキュリティを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定します）。ポートでポート セキュリティと Web 認証をイネーブルにすると、Web ベース認証がポートを認証し、ポート セキュリティがクライアントの 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。その後、ポートを介してネットワークにアクセス可能なクライアント数またはクライアント 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、第 43 章「ポート セキュリティの設定」を参照してください。

LAN ポート IP（LPIP）

同じポート上で LAN Port IP（LPIP; LAN ポート IP）とレイヤ 2 Web ベース認証を設定できます。最初にホストが Web ベース認証を使用して認証されて、次に 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 タイマーが期限切れになると、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 ベース認証が VLAN のスイッチ ポートに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 を設定できません。

ゲートウェイ IP と同じレイヤ 3 インターフェイス上に Web ベース認証を設定できます。両方の機能のホスト ポリシーがソフトウェアに適用されます。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

VLAN ACL または Cisco IOS ACL をインターフェイス上に設定する場合、ACL がホスト トラフィックに適用されるのは Web ベース認証ホスト ポリシーが適用されたあとだけです。

レイヤ 2 Web ベース認証の場合、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 Port ACL（PACL; ポート ACL）を設定する必要があります。認証後、Web ベース認証ホスト ポリシーは PACL を上書きします。

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

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 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（CBAC）

Context-based Access Control（CBAC; コンテキストベース アクセス コントロール）がポートの 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

802.1x 認証と同じポート上に Web ベース認証を設定できません。ただし、代替認証方式として設定することは可能です。

EtherChannel

レイヤ 2 EtherChannel インターフェイス上に Web ベース認証を設定できます。Web ベース認証の設定はすべてのメンバ チャネルに適用されます。

スイッチオーバー

Route Processor Redundancy（RPR）モードの冗長スーパーバイザ エンジンを搭載した Catalyst 4500 シリーズ スイッチでは、スイッチオーバー中は現在認証されているホストに関する情報が保持されます。そのため、再認証の必要はありません。

Web ベース認証の設定

ここでは、Web ベース認証を設定する手順について説明します。

Web ベース認証のデフォルト設定

表 42-1 に、Web ベース認証のデフォルト設定を示します。

表 42-1　Web ベース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 • User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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 ベース認証設定時の注意事項および制約事項

Web ベース認証設定時の注意事項および制約事項は次のとおりです。

- Web 認証には、Cisco Attribute-Value（AV）ペア アトリビュートが 2 つ必要です。

  1 つめのアトリビュート priv-lvl=15 は常に 15 に設定する必要があります。これにより、スイッチにログインするユーザの権限レベルが設定されます。

  2 つめのアトリビュートは、Web 認証されるホストに適用されるアクセス リストです。構文は、802.1x ユーザ単位アクセス コントロール リスト（ACL）に似ています。ただし、このアトリビュートは ip:inacl ではなく proxyacl で始まり、各エントリの source フィールドは any でなければなりません　（認証後に、ACL が適用されると any フィールドはクライアント IP アドレスに置き換えられます）。

  次に例を示します。

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

（注）　proxyacl エントリによって、許可されたネットワーク アクセスのタイプが決まります。

- Web ベース認証は入力専用の機能です。
- Web ベース認証はアクセス ポートだけに設定できます。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ません。
- Web ベース認証を設定する前に、インターフェイス上でデフォルト 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 インターフェイス上では、スタティック ARP キャッシュ割り当てのあ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、スイッチ上では IP デバイス トラッキング機能はディセーブルです。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。
- スイッチ上で HTTP サーバを実行するために、IP アドレスを少なくとも 1 つ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場合、2 ホップ以上離れたホストではトラフィックの中断が発生することがあります。これは、レイヤ 2（STP）トポロジの変更後に ARP および DHCP アップデートが送信されないことがあるためです。
- Web ベース認証は、ダウンロード可能ホスト ポリシーとして VLAN 割り当てをサポートしません。
- Cisco IOS Release 12.2(50)SG では、RADIUS サーバからの Downloadable ACL（DACL）がサポートされます。
- Web ベース認証は IPv6 トラフィックではサポートされません。

Web ベース認証設定作業リスト

Web ベース認証機能を設定するには、次の作業を行います。

- 「認証ルールとインターフェイスの設定」（P.42-8）
- 「AAA 認証の設定」（P.42-9）
- 「スイッチ/RADIUS サーバ通信の設定」（P.42-10）
- 「HTTP サーバの設定」（P.42-11）
- 「AAA 失敗ポリシーの設定」（P.42-14）
- 「Web ベース認証パラメータの設定」（P.42-14）
- 「Web ベース認証のキャッシュ エントリの削除」（P.42-15）

認証ルールとインターフェイスの設定

Web ベース認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip admission name` *name* `proxy http`	Web ベース許可の認証ルールを設定します。
	`Switch(config)# no ip admission name` *name*	認証ルールを削除します。
ステップ 2	`Switch(config)# 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* は fastethernet、gigabit ethernet、または tengigabitethernet です。
ステップ 3	`Switch(config-if)# ip access-group` *name*	デフォルト ACL を適用します。
ステップ 4	`Switch(config-if)# ip admission` *name*	指定されたインターフェイス上で Web ベース認証を設定します。
ステップ 5	`Switch(config-if)# exit`	コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	`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 7	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show ip admission configuration`	設定を表示します。

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

Web ベース認証をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# aaa new-model`	AAA 機能をイネーブルにします。
	`Switch(config)# no aaa new-model`	AAA 機能をディセーブルにします。
ステップ 2	`Switch(config)# aaa authentication login default group {tacacs+ | radius}`	ログイン時の認証方式のリストを定義します。
ステップ 3	`Switch(config)# aaa authorization auth-proxy default group {tacacs+ | radius}`	Web ベース許可の許可方式リストを作成します。
	`Switch(config)# no aaa authorization auth-proxy default group {tacacs+ | radius}`	設定されている方式リストを消去します。
ステップ 4	`Switch(config)# tacacs-server host {hostname | ip_address}`	AAA サーバを指定します。RADIUS サーバの場合は、「スイッチ /RADIUS サーバ通信の設定」（P.42-10）を参照してください。
ステップ 5	`Switch(config)# tacacs-server key {key-data}`	スイッチと Terminal Access Controller Access Control System（TACACS）サーバとの間で使用される許可および暗号化キーを設定します。

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/RADIUS サーバ通信の設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- 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り、一意の識別子が作成され、同一 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機能します。RADIUS のホスト エントリは、設定された順序で選択されます。

RADIUS サーバ パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# **ip radius source-interface** *interface_name*	RADIUS パケットに、指定されたインターフェイスの IP アドレスが含まれるように指定します。
	Switch(config)# **no ip radius source-interface**	RADIUS パケットに、以前に指定されたインターフェイスの IP アドレスが含まれないようにします。
ステップ 2	Switch(config)# **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。指定する *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 サーバとの間で使用する認証および暗号化キーを指定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再入力します。
	Switch(config)# **no radius-server host** {*hostname* | *ip-address*}	指定した RADIUS サーバを削除します。
ステップ 3	Switch(config)# **radius-server key** *string*	スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する許可および暗号化キーを設定します。
ステップ 4	Switch(config)# **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	Switch(config)# **radius-server dead-criteria tries** *num-tries*	サーバが非アクティブと判断されるまでの RADIUS サーバへの応答がない送信の回数を指定します。*num-tries* の範囲は 1 ～ 100 です。

RADIUS サーバ パラメータを設定する場合、次の作業を行います。

- 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 サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化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、キーの一部として引用符を使用する場合を除いて、キーを引用符で囲まないでください。このキーは、RADIUS デーモン上で使用する暗号と一致する必要があります。
- **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、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号化キーの値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** のグローバル 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 12.2 および次の URL の『*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 サーバ上で、スイッチの IP アドレス、サーバとスイッチで共有されるキー文字列、Downloadable ACL（DACL）を含む、いくつかの設定を行う必要があります （Cisco IOS Release 12.2(50)SG は DACL をサポートします）。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 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、スイッチ内の HTTP サーバをイネーブルにする必要があります。サーバを HTTP または HTTPS のいずれかにイネーブルにできます。

サーバをイネーブルにするには、次のいずれかの作業を行います。

コマンド	目的
`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、ユーザを認証するために HTTP サーバを使用してホストと通信します。
`Switch(config)# ip http secure-server`	HTTPS をイネーブルにします。

Cisco IOS Release 12.2(50)SG 以降では、任意で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ション URL を指定したりできます。詳細については、以下を参照してください。

- 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ション URL の指定

認証プロキシ Web ページのカスタマイズ

Cisco IOS Release 12.2(50)SG では、Web ベース認証時にスイッチ内部のデフォルト HTML ページの代わりに 4 つの代替 HTML ページをユーザに表示するオプションがあります。

カスタム認証プロキシ Web ページを使用するように指定するには、カスタム HTML ファイルをスイッチの内部ディスクまたはフラッシュ メモリに保存してから、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行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip admission proxy http login page file device:login-filename`	スイッチのメモリ 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 *disk0:* など、ディスクまたはフラッシュ メモリです。
ステップ 2	`Switch(config)# 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 ファイルの場所を指定します。
ステップ 3	`Switch(config)# 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 ファイルの場所を指定します。
ステップ 4	`Switch(config)# 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 ファイルの場所を指定します。

カスタマイズした認証プロキシ Web ページを設定する場合、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 ファイルすべてを指定します。ファイルを 3 つ以下しか指定しないと、内部のデフォルト HTML ページが使用されます。
- この 4 つのカスタム HTML ファイルは スイッチのディスクまたはフラッシュに存在している必要があります。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 サーバ上になければなりません。HTTP サーバにアクセスできるように、アドミッション ルール内に代行受信 ACL を設定する必要があります。
- カスタム ページからの外部リンクには、アドミッション ルール内に代行受信 ACL を設定する必要があります。
- 外部リンクまたはイメージに必要な名前解決には、有効な DNS サーバにアクセスするためにアドミッション ルール内に代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルに設定されている場合、設定済みの 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 ファイルの指定を解除するには、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 形式であるため、このページについて次の注意事項に留意してください。

- ログイン形式では、ユーザ名およびパスワードのユーザ入力を受け入れて、そのデータを **uname** および **pwd** として POST する必要があります。
- カスタム ログイン ページでは、ページ タイムアウト、非表示のパスワード、冗長送信の防止など、Web 形式のベスト 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 disk1:login.htm
```

```
Switch(config)# ip admission proxy http success page file disk1:success.htm
Switch(config)# ip admission proxy http fail page file disk1:fail.htm
Switch(config)# ip admission proxy http login expired page file disk1: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           : disk1:login.htm
 Success page         : disk1:success.htm
 Fail Page            : disk1:fail.htm
 Login expired Page   : disk1: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ション URL の指定

Cisco IOS Release 12.2(50)SG では、ユーザが認証に成功したあとにリダイレクトされる URL を指定するオプションがあり、内部成功 HTML ページを効率的に置き換えることができます。

ログイン成功時のリダイレクション URL を指定するには、次の作業を行います。

コマンド	目的
Switch(config)# **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。

ログイン成功時のリダイレクション 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で、CLI で使用できません。リダイレクションはカスタム ログイン成功ページ内で実行できます。
- 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、設定済みの 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、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、ログイン成功時のリダイレクション 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

Web ベース認証の AAA 失敗ポリシーは Cisco IOS Release 12.2(50)SG でサポートされます。

AAA 失敗ポリシーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# 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 サーバにアクセス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。 スイッチ上の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	`Switch(config)# ip admission ratelimit aaa-down` *number_of_sessions*	（任意）AAA ダウン ステートのホストからの認証試行をレート制限して、AAA サーバがサービスに戻る際に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、AAA ダウン ステートで接続されているホストがあるかどうかを判別する例を示します。

```
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期間の間ウォッチ リストに配置されるまでに可能な失敗ログイン試行の最大回数を設定できます。

Web ベース認証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	`Switch(config)# ip admission max-login-attempts number`	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 です。デフォルトは 5 です。
ステップ 2	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 3	`Switch# show ip admission configuration`	認証プロキシ設定を表示します。
ステップ 4	`Switch# show ip admission cache`	認証エントリのリストを表示します。

次に、失敗ログイン試行の最大回数を 10 に設定する例を示します。

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

Web ベース認証のキャッシュ エントリの削除

既存のセッション エントリを削除するには、次のいずれかの作業を行います。

コマンド	目的
`Switch# 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場合は、アスタリスクを使用します。単一ホストのエントリを削除する場合は、特定の IP アドレスを入力します。
`Switch# 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場合は、アスタリスクを使用します。単一ホストのエントリを削除する場合は、特定の IP アドレスを入力します。

次に、IP アドレスが 209.165.201.1 のクライアントの 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 ベース認証設定を表示するには、次の作業を行います。

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

次に、グローバルな Web ベース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、インターフェイス Gi 3/27 の Web ベース認証設定を表示する例を示します。

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