CHAPTER 47

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、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Cisco IOS Command Reference*』と関連資料を参照してください。

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

Web ベース認証について

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。ユーザは資格情報を入力します。Web ベース認証はこの資格情報を認証のために AAA サーバに送信します。

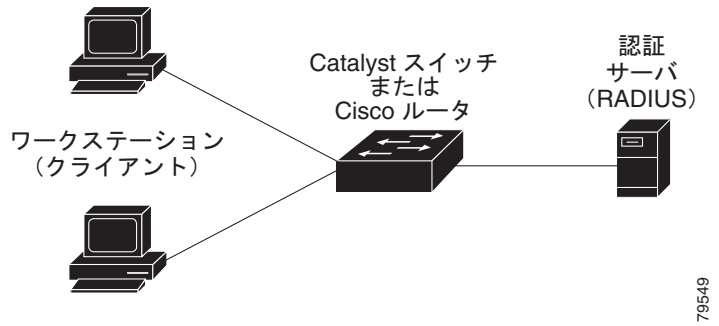
- 認証に成功した場合、Web ベース認証は、ログインの成功を示す HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。
- 認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。ユーザが最大試行回数を超えると、Web ベース認証はログイン失効 HTML ページをホストに送信し、ユーザは待機期間の間ウォッチ リストに配置されます。

ここでは、認証、許可、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。

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（図 47-1）。

図 47-1　Web ベース認証デバイスの役割



ロールには、次のものがあります。

- *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*：実際にクライアントの認証を行います。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。

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 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。

- ARP 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。
- ダイナミック ARP インスペクション（DAI）
- Dynamic Host Configuration Protocol（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。

- 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、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。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。「認証プロキシ Web ページのカスタマイゼーション」（P.47-4）を参照してください。
- 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、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。
- 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。

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。

- 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。

（注）　カスタマイズされた Web ベースの認証ページがスイッチのシステム ディレクトリ（フラッシュ）内にある同じ名前の新しいページ（ファイル）に置き換えられると、新しいページは見られません。古いページが表示されます。リリース 15.0(2)SG 以降では、**ip admission proxy http refresh-all** コマンドを入力するまで新しいページが表示されません。

Cisco IOS Release 12.2(50)SG では、4 枚のデフォルト内部 HTML ページの代わりにカスタム HTML ページを使用したり、認証成功後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たりすることができます。

その他の機能と Web ベース認証の相互作用

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.47-4）
- 「LAN ポート IP」（P.47-5）
- 「ゲートウェイ IP」（P.47-5）
- 「ACL」（P.47-5）
- 「コンテキストベース アクセス コントロール」（P.47-5）
- 「802.1X 認証」（P.47-5）
- 「EtherChannel」（P.47-6）
- 「スイッチオーバー」（P.47-6）

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。（**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 MAC 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。この場合、このポートを使用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 セキュリティのイネーブル化の詳細については、第 48 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

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。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。

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

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

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 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。

デフォルトの Web ベース認証の設定

表 47-1 は、デフォルトの Web ベース認証の設定を示しています。

表 47-1　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 • 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 ベース認証の設定に関する注意事項と制約事項

Web ベース認証を設定する場合、次の注意事項および制約事項を考慮してください。

- Web 認証には、Cisco Attribute-Value（AV）ペア属性が 2 つ必要です。

  1 つめの属性 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 つめの属性は、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、この属性は 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。
- 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。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。
- 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。
- 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

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

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に 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。
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)# ip device tracking [probe {count count | interval interval}]`	（任意）IP デバイス トラッキング テーブルで、これらのパラメータを設定します。 • **count** : スイッチが ARP プローブを送信する回数です。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。 • **interval** : スイッチが ARP プローブを再送する前に、応答を待機する秒数です。指定できる範囲は 30 ～ 300 秒です。デフォルトは 30 秒です。
ステップ 8	`Switch(config)# ip device tracking [probe {delay interval}]`	（任意）IP デバイス トラッキング テーブルに対してオプションのプローブ遅延パラメータを設定します。 • **interval** : スイッチが ARP プローブの送信を遅延する秒数。追跡対象デバイスによるリンク アップおよび ARP プローブの生成により起動されます。指定できる範囲は 1 ～ 120 秒です。デフォルトは 0 秒です。
ステップ 9	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Switch# show ip admission configuration`	設定を表示します。

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

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法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、「スイッチおよび RADIUS サーバ間の通信の設定」（P.47-10）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キーを設定します。

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	`Switch(config)# 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。
	`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* 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 サーバとの間で使用する認証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	`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 でサポートされています。
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。指定できる *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。このキーは RADIUS デーモン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、および暗号キーの値を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、
『*Cisco IOS Security Configuration Guide*, Release 12.2』と
『*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_3/security/command/reference/secur_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。

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、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。
`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」（P.47-12）
- 「成功ログインに対するリダイレクション URL の指定」（P.47-13）

認証プロキシ Web ページのカスタマイズ

Cisco IOS Release 12.2(50)SG を使用すれば、Web ベース認証中にスイッチの内部デフォルト HTML ページの代わりに、ユーザに 4 枚の代替 HTML ページを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、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。
- 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 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
```

成功ログインに対するリダイレクション 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
```

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。デフォルトは 5 です。 **（注）** この値の一般的なカスタム設定は、50 を超えることはありません。
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`	認証プロキシの設定を表示します。
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 ベース認証キャッシュ 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。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。
`Switch# clear ip admission cache {* | host ip address}`	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
Switch# **show authentication sessions** [**interface** *type slot/port*]	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、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
```