



CHAPTER 14

Web ベース認証の設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

Web ベース認証設定の前提条件

- 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。
- 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 を設定します。

Web ベース認証の設定に関する制約事項

- 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 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。
- 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。
- 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 ベース認証および Network Edge Access Topology (NEAT) は、相互に排他的です。インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- Web ベース認証は、RADIUS 許可サーバだけをサポートします。TACACS+ サーバまたはローカル許可を使用できません。

Web ベース認証 の設定に関する情報

Web ベース認証

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)

レイヤ 2 インターフェイスで Web ベース認証を設定できます。

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。ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウントिंग (AAA) 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.14-2)
- 「ホストの検出」(P.14-3)
- 「セッションの作成」(P.14-3)
- 「認証プロセス」(P.14-4)
- 「Web 認証カスタマイズ可能な Web ページ」(P.14-6)
- 「その他の機能と Web ベース認証の相互作用」(P.14-8)

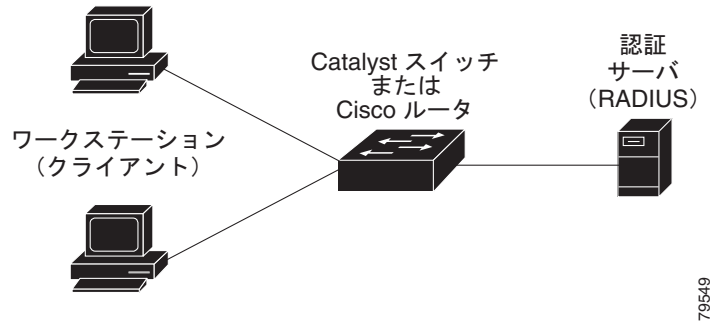
デバイスの役割

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 14-1 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 ベースのトリガー：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 ベース認証は応答しないホスト (NRH) 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.14-4) を参照）。
- ホストがレイヤ 2 インターフェイス上の ARP プロープに回答しなかった場合、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

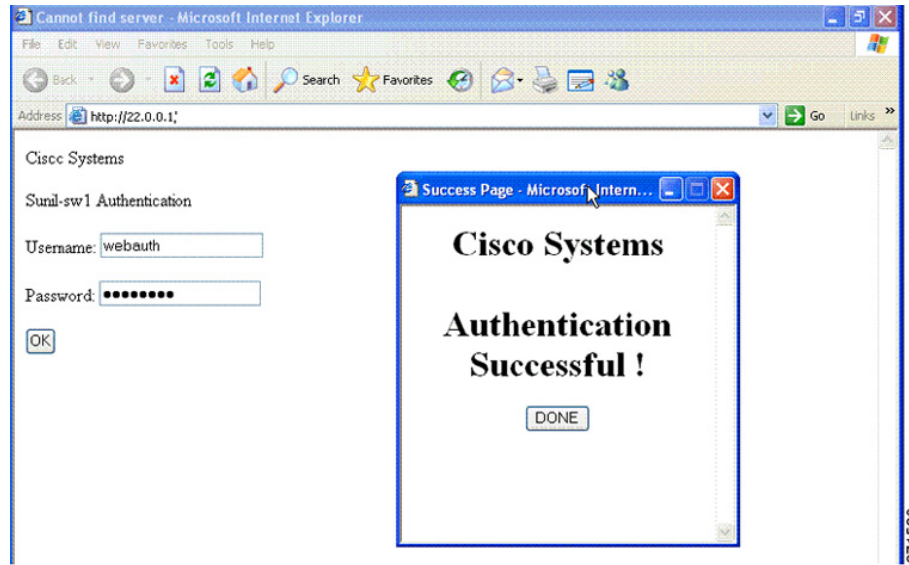
Web 認証を使用してスイッチにログインしたときに表示されるバナーを作成できます。

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

`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。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。認証ポップアップ ページには、Cisco System と表示されず（図 14-2 を参照）。

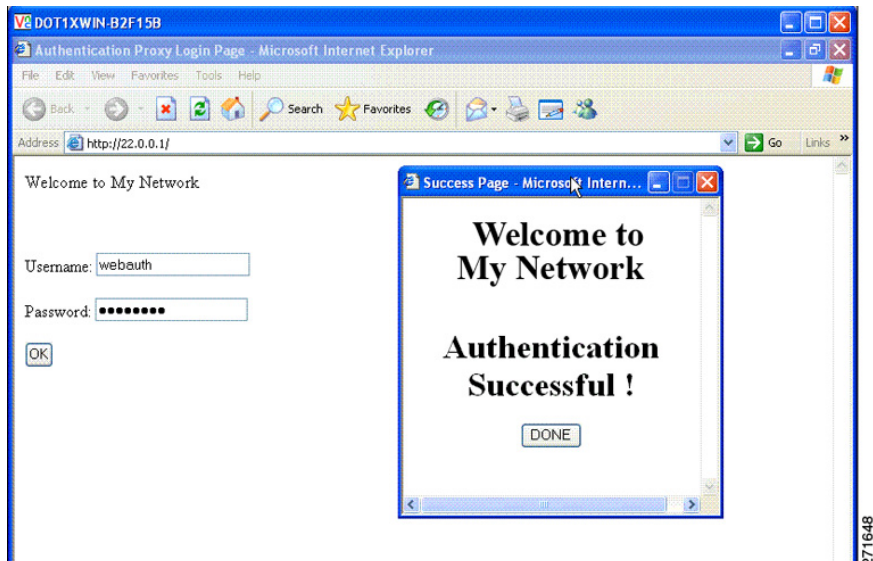
図 14-2 認証成功バナー



また、図 14-3 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。

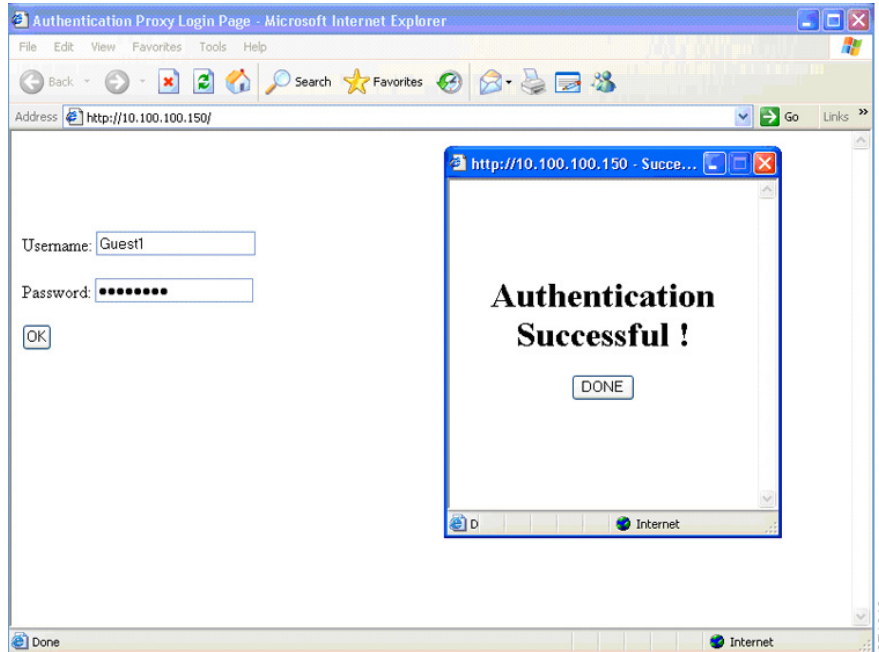
- スイッチ、ルータ、または企業名をバナーに追加するには、**ip admission auth-proxy-banner http banner-text** グローバル コンフィギュレーション コマンドを使用します。
- ロゴ、またはテキスト ファイルをバナーに追加するには、**ip admission auth-proxy-banner http file-path** グローバル コンフィギュレーション コマンドを使用します。

図 14-3 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 14-4 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 14-4 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.14-14)」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：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。

Web 認証時の注意事項

- 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。

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。

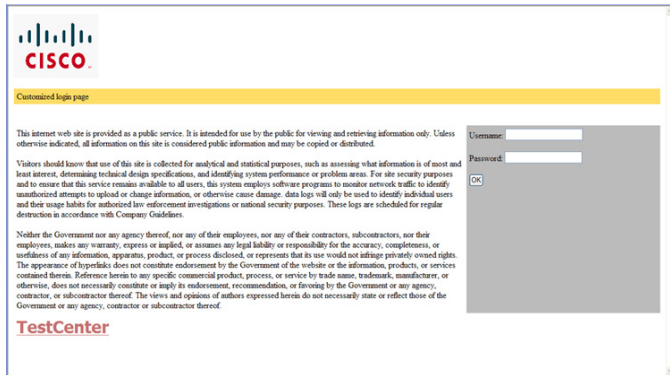
- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個の HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージはすべて、アクセス可能は HTTP サーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL 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。

図 14-5 に示すように、デフォルトの内部 HTML ページを独自の HTML ページで置き換えることができます。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 14-5 カスタマイズ可能な認証ページ



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.14-8)
- 「LAN ポート IP」 (P.14-9)
- 「ゲートウェイ IP」 (P.14-9)
- 「ACL」 (P.14-9)
- 「コンテキストベース アクセス コントロール」 (P.14-9)
- 「802.1X 認証」 (P.14-9)
- 「EtherChannel」 (P.14-9)

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.29-12) 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 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ゲートウェイ IP (GWIP) 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、ポート ACL (PACL) 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。



(注)

プロキシ ACL が Web ベース認証クライアントに設定されると、プロキシ ACL はダウンロードされて、許可プロセスの一部として適用されます。したがって、PACL はプロキシ ACL のアクセス コントロール エントリ (ACE) を表示します。

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

コンテキストベース アクセス コントロール (CBAC) 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 チャンネルに適用されます。

デフォルトの Web ベース認証の設定

表 14-1 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 <ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • キー 	<ul style="list-style-type: none"> • 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

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。

Web ベース認証の設定方法

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 ベース許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 ベースの認証をイネーブルにする入力レイヤ 2 インターフェイスを指定します。 <i>type</i> は、Fast Ethernet、Gigabit Ethernet、10-Gigabit Ethernet があります。
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	設定を表示します。

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 ベース許可の許可方式リストを作成します。
ステップ4	radius-server host {hostname ip-address} test username username	AAA サーバを指定します。 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。
ステップ5	radius-server key string	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。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。

および RADIUS サーバ間の通信の設定

	コマンド	目的
ステップ 1	<code>ip radius source-interface interface_name</code>	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	<code>radius-server host {hostname ip-address} test username username</code>	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 サーバの間で使用される認証と暗号キーを指定します。 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	<code>radius-server key string</code>	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設定します。
ステップ 4	<code>radius-server vsa send authentication</code>	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	<code>radius-server dead-criteria tries num-tries</code>	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 num-tries の範囲は 1 ~ 100 です。

HTTP サーバの設定

	コマンド	目的
ステップ 1	<code>ip http server</code>	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	<code>ip http secure-server</code>	HTTPS をイネーブルにします。

認証プロキシ Web ページのカスタマイズ

はじめる前に

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、代わりに 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。 <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	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	ip admission proxy http login expired page file <i>device:expired-filename</i>	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。

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をリダイレクトする URL を指定します。

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 <i>number</i>	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 回です。デフォルトは 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。

Web 認証ローカル バナーの設定

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>ip admission auth-proxy-banner http [<i>banner-text</i> <i>file-path</i>]</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(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。

Web ベース認証キャッシュ エントリの削除

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。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。

コマンド	目的
<code>clear ip auth-proxy cache {* <i>host ip address</i>}</code>	スイッチから認証プロキシ エントリを消去します。
<code>clear ip admission cache {* <i>host ip address</i>}</code>	スイッチから IP アドミッション キャッシュ エントリを消去します。

Web ベース認証のモニタリングおよびメンテナンス

コマンド	目的
<code>show authentication sessions</code>	Web ベース認証設定を表示します。
<code>show ip admission configuration</code>	認証プロキシの設定を表示します。
<code>show ip admission cache</code>	認証エントリのリストを表示します。

Web ベース認証の設定例

Web ベース認証のイネーブル化と表示 : 例

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 のイネーブル化 : 例

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 radius
Switch(config)# aaa authorization auth-proxy default group radius
```

RADIUS サーバパラメータの設定 : 例

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
```

カスタム認証プロキシ Web ページの設定 : 例

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
```

カスタム認証プロキシ Web ページの確認 : 例

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
```

リダイレクト URL の設定 : 例

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
```

リダイレクト URL の確認 : 例

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
```

ローカル バナーの設定 : 例

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
```

Web ベース認証セッションの削除 : 例

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
```


その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『Cisco IE 2000 Switch Command Reference, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『Cisco IOS Configuration Fundamentals Command Reference』
認証プロキシコマンド RADIUS サーバ コマンド	『Cisco IOS Security Command Reference』
認証プロキシ設定 RADIUS サーバ設定	『Cisco IOS Security Configuration Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html