CHAPTER 5

エンドユーザ クレデンシャルの取得

エンドユーザ クレデンシャルの取得の概要

サーバ タイプ/レルム	認証方式	サポートされるネットワーク プロトコル	注記（Notes）
Active Directory	Kerberos NTLMSSP 基本	HTTP、HTTPS ネイティブ FTP、FTP over HTTP SOCKS（基本認証）	Kerberos は標準モードでのみサポートされます。クラウド コネクタ モードではサポートされません。
LDAP	基本	HTTP、HTTPS ネイティブ FTP、FTP over HTTP SOCKS	—

認証タスクの概要

手順	タスク	関連項目および手順へのリンク
1.	認証レルムを作成する。	• Active Directory 認証レルムの作成（NTLMSSP および基本）（5-15 ページ） • LDAP 認証レルムの作成（5-17 ページ）
2.	グローバル認証を設定する。	• グローバル認証の設定（5-22 ページ）
3.	外部認証を設定する。 外部 LDAP または RADIUS サーバからユーザを認証できます。	• 外部認証（5-11 ページ）
4.	（任意）追加の認証レルムを作成して順序を決定する。 使用する予定の各認証プロトコルとスキームの組み合わせに対して、少なくとも 1 つの認証レルムを作成する。	• 認証シーケンスの作成（5-28 ページ）
5.	（任意）クレデンシャルの暗号化を設定する。	• クレデンシャル暗号化の設定（5-38 ページ）
6.	認証要件に基づいてユーザとクライアント ソフトウェアを分類する識別プロファイルを作成する。	• ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）
7.	識別プロファイルの作成対象となったユーザとユーザ グループからの Web 要求を管理するポリシーを作成する。	• ポリシーによる Web 要求の管理：ベスト プラクティス（10-3 ページ）

認証に関するベスト プラクティス

- できる限り少数の Active Directory レルムを作成します。多数の Active Directory レルムを作成すると、認証で追加のメモリが必要になります。
- NTLMSSP を使用する場合は、Web Security Appliance またはアップストリーム プロキシ サーバを使用してユーザを認証します（両方は使用できません）。（Web Security Appliance を推奨）
- Kerberos を使用する場合は、Web Security Appliance を使用して認証します。
- 最適なパフォーマンスを得るには、1 つのレルムを使用して同じサブネット上のクライアントを認証します。
- 一部のユーザ エージェントには、通常の動作に悪影響を及ぼすマシン クレデンシャルや認証失敗の問題があることが判明されています。これらのユーザ エージェントとの認証をバイパスする必要があります。問題のあるユーザ エージェントの認証のバイパス（5-30 ページ）を参照してください。

認証の計画

- Active Directory/Kerberos（5-3 ページ）
- Active Directory/Basic（5-4 ページ）
- Active Directory/NTLMSSP（5-5 ページ）

- LDAP/基本（5-5 ページ）
- ユーザの透過的識別（5-6 ページ）

Active Directory/Kerberos

明示的な転送	透過、IP ベースのキャッシング	透過、Cookie ベースのキャッシング
利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべてのブラウザ、および他のほとんどのアプリケーションでサポートされている • RFC ベース • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる • パスフレーズが認証サーバに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Web Security Appliance を信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現	**利点：** • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべての主要ブラウザで使用できる • 認証をサポートしていないユーザ エージェントを使用する場合、ユーザはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザが以前に HTTP 要求で認証されている場合は、HTTPS 要求で使用できる	**利点：** • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべての主要ブラウザで使用できる • 認証が、ホストや IP アドレスではなく、ユーザに関連付けられる **欠点：** • Cookie はドメイン固有であるため、新規の各 Web ドメインで認証プロセス全体が必要 • Cookie をイネーブルにする必要がある • HTTPS 要求で使用できない

Active Directory/Basic

明示的な転送	透過、IP ベースのキャッシング	透過、Cookie ベースのキャッシング
利点: • すべてのブラウザ、および他のほとんどのアプリケーションでサポートされている • RFC ベース • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる • パスフレーズが認証サーバに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Web Security Appliance を信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現 欠点: • すべての要求でパスフレーズがクリア テキスト（Base64）として送信される • シングル サインオンなし • 中程度のオーバーヘッド：新規の接続ごとに再認証が必要 • 主に Windows および主要ブラウザでのみサポート	利点: • すべての主要ブラウザで使用できる • 認証をサポートしていないユーザ エージェントを使用する場合、ユーザはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザが以前に HTTP 要求で認証されている場合は、HTTPS 要求で使用できる 欠点: • 認証クレデンシャルが、ユーザではなく、IP アドレスに関連付けられる（Citrix および RDP 環境では使用できず、ユーザが IP アドレスを変更した場合も使用できない） • シングル サインオンなし • パスフレーズがクリア テキスト（Base64）として送信される	利点: • すべての主要ブラウザで使用できる • 認証が、ホストや IP アドレスではなく、ユーザに関連付けられる 欠点: • Cookie はドメイン固有であるため、新規の各 Web ドメインで認証プロセス全体が必要 • Cookie をイネーブルにする必要がある • HTTPS 要求で使用できない • シングル サインオンなし • パスフレーズがクリア テキスト（Base64）として送信される

Active Directory/NTLMSSP

明示的な転送	透過
利点: • パスフレーズが認証サーバに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Web Security Appliance を信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現 **欠点:** • 中程度のオーバーヘッド:新規の接続ごとに再認証が必要 • 主に Windows および主要ブラウザでのみサポート	**利点:** • より柔軟性が高い 透過 NTLMSSP 認証は透過基本認証と似ています。ただし、Web プロキシはクライアントとの通信に、基本的なクリア テキストのユーザ名とパスフレーズではなく、チャレンジ/レスポンス認証を使用します。 透過 NTLM 認証を使用する利点と欠点は、透過基本認証を使用する場合と同様です。ただし、**透過 NTLM 認証には、パスフレーズが認証サーバに送信されないというさらなる利点があり、クライアント アプリケーションが Web Security Appliance を信頼するように設定されている場合はシングル サインオンを実現できます。**

LDAP/基本

明示的な転送	透過
利点: • RFC ベース • NTLM よりも多くのブラウザをサポート • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる **欠点:** • シングル サインオンなし • すべての要求でパスフレーズがクリア テキスト（Base64）として送信される **回避策:** • 認証の失敗（5-30 ページ）	**利点:** • 明示的な転送よりも柔軟。 • NTLM よりも多くのブラウザをサポート • 認証をサポートしていないユーザ エージェントを使用する場合、ユーザはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザが以前に HTTP 要求で認証されている場合は、HTTPS 要求で使用できる **欠点:** • シングル サインオンなし • パスフレーズがクリア テキスト（Base64）として送信される • 認証クレデンシャルが、ユーザではなく、IP アドレスに関連付けられる（Citrix および RDP 環境では使用できず、ユーザが IP アドレスを変更した場合も使用できない） **回避策:** • 認証の失敗（5-30 ページ）

ユーザの透過的識別

従来、ユーザの識別および認証では、ユーザにユーザ名とパスフレーズの入力を求めていました。ユーザが入力したクレデンシャルは認証サーバによって認証され、その後、Web プロキシが、認証されたユーザ名に基づいてトランザクションに適切なポリシーを適用します。

しかし、Web Security Appliance は、ユーザを透過的に認証するように設定することができます。つまり、エンドユーザにクレデンシャルを要求しません。透過的な識別では、別の信頼できるソースによってユーザが認証済みであると想定し、そのソースから取得したクレデンシャルを使用してユーザを認証して、適切なポリシーを適用します。

ユーザを透過的に識別して以下を実行する場合があります。

- ユーザがネットワーク上のプロキシの存在を意識しないように、シングル サイン オン環境を構築する。
- エンド ユーザに認証プロンプトを表示できないクライアント アプリケーションからのトランザクションに、認証ベースのポリシーを適用する。

ユーザの透過的識別は、Web プロキシがユーザ名を取得して識別プロファイルを割り当てる方法にのみ影響を与えます。ユーザ名を取得して識別プロファイルを割り当てた後、Web プロキシは、識別プロファイルの割り当て方法に関係なく、通常どおり他のすべてのポリシーを適用します。

透過認証が失敗した場合、トランザクションを処理する方法を設定できます。ユーザにゲスト アクセスを許可するか、またはユーザに認証プロンプトを表示することができます。

透過的ユーザ ID の失敗によりエンド ユーザに認証プロンプトが表示され、ユーザが無効なクレデンシャルにより認証に失敗した場合、ユーザのゲスト アクセスを許可するかどうかを選択できます。

(注)　再認証をイネーブルにしたが、URL フィルタリングによってトランザクションがブロックされている場合、エンド ユーザ通知ページが表示され、別のユーザとしてログインするオプションが提供されます。ユーザがリンクをクリックすると、認証を求めるプロンプトが表示されます。詳細については、認証の失敗：異なるクレデンシャルによる再認証の許可（5-34 ページ）を参照してください。

透過的ユーザ識別について

透過的ユーザ識別は以下の方式で使用できます。

- [ISE によってユーザを透過的に識別（Transparently identify users with ISE）]：Identity Services Engine（ISE）サービスがイネーブルの場合に使用可能（[ネットワーク（Network）] > [Identity Services Engine]）。これらのトランザクションの場合、ユーザ名と関連するセキュリティ グループ タグは Identity Services Engine サーバから取得されます。ISE サービスを認証および統合するためのタスク（8-4 ページ）を参照してください。
- [ASA によってユーザを透過的に識別（Transparently identify users with ASA）]：ユーザは、Cisco 適応型セキュリティ アプライアンスから受信した現在の IP アドレス対ユーザ名のマッピングによって識別されます（リモート ユーザのみ）。このオプションは、AnyConnect Secure Mobility がイネーブルになっており、ASA と統合されている場合に使用できます。ユーザ名は ASA から取得され、関連するディレクトリ グループは Web Security Appliance で指定された認証レルムまたはシーケンスから取得されます。リモート ユーザ（10-25 ページ）を参照してください。
- [認証レルムによってユーザを透過的に識別（Transparently identify users with authentication realms）]：このオプションは、1 つ以上の認証レルムが、以下のいずれかの認証サーバを使用して透過的識別をサポートするように設定されている場合に使用できます。

- Active Directory：NTLM または Kerberos 認証レルムを作成し、透過的ユーザ識別をイネーブルにします。また、Cisco Context Directory Agent などの Active Directory エージェントを個別に展開する必要があります。詳細については、Active Directory による透過的ユーザ識別（5-7 ページ）を参照してください。
- LDAP：eDirectory として設定した LDAP 認証レルムを作成し、透過的ユーザ識別をイネーブルにします。詳細については、LDAP による透過的ユーザ識別（5-8 ページ）を参照してください。

AsyncOS for Web は eDirectory または Active Directory エージェントと定期的に通信して、認証されたユーザ名と現在の IP アドレスを照合するマッピングを保守します。

Active Directory による透過的ユーザ識別

Active Directory は、Web Security Appliance などの他のシステムから簡単に照会できる形式でユーザ ログイン情報を記録しません。Cisco Context Directory Agent（CDA）などの Active Directory エージェントは、認証済みユーザの情報を Active Directory セキュリティ イベント ログで照会する必要があります。

AsyncOS for Web は Active Directory エージェントと通信して、IP アドレス対ユーザ名のマッピングのローカル コピーを保守します。AsyncOS for Web は IP アドレスをユーザ名に関連付ける必要がある場合、最初にマッピングのローカル コピーをチェックします。一致が見つからない場合、Active Directory エージェントに照会して一致するものを見つけます。

Active Directory エージェントのインストールと設定の詳細については、Web セキュリティ アプライアンスに情報を提供する Active Directory エージェントの設定（5-8 ページ）を参照してください。

Active Directory を使用してユーザを透過的に識別する場合は、以下を考慮してください。

- Active Directory による透過的ユーザ識別は、NTLM または Kerberos 認証スキームでのみ機能します。Active Directory インスタンスに対応する LDAP 認証レルムでは使用できません。
- 透過的ユーザ ID は Active Directory エージェントがサポートする Active Directory のバージョンで動作します。
- 高可用性を実現するために、別のマシンに Active Directory エージェントの 2 番目のインスタンスをインストールできます。その場合、各 Active Directory エージェントは、他方のエージェントとは別個に、独自の IP アドレス対ユーザ名 マッピングを保持します。AsyncOS for Web は、プライマリ エージェントに対する ping の試行が 3 回失敗した後にバックアップとして Active Directory エージェントを使用します。
- Active Directory エージェントは、Web Security Appliance と通信する際にオンデマンド モードを使用します。
- Active Directory エージェントは、Web Security Appliance にユーザのログアウト情報をプッシュします。ただし、ユーザのログアウト情報が Active Directory セキュリティ ログに記録されないことがあります。これは、クライアント マシンがクラッシュしたり、ユーザがログアウトせずにマシンをシャット ダウンした場合に発生します。ユーザのログアウト情報がセキュリティ ログにないと、Active Directory エージェントは、IP アドレスがそのユーザに割り当てられていないことをアプライアンスに通知できません。これを回避するために、Active Directory エージェントからのアップデートがない場合に AsyncOS が IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さを定義できます。詳細については、CLI を使用した透過的ユーザ識別の詳細設定（5-10 ページ）を参照してください。
- Active Directory エージェントは、ユーザ名の一意性を確保するために、特定の IP アドレスからログインする各ユーザの `sAMAccountName` を記録します。

- クライアント マシンが Active Directory サーバに提供するクライアントの IP アドレスと Web Security Appliance は同一である必要があります。
- AsyncOS for Web はユーザが属する上位の親グループだけを検索します。ネストされたグループは検索しません。

Web セキュリティ アプライアンスに情報を提供する Active Directory エージェントの設定

AsyncOS for Web OS は、Active Directory から直接クライアントの IP アドレスを取得できないので、Active Directory エージェントから IP アドレス対ユーザ名のマッピング情報を取得する必要があります。

Web Security Appliance にアクセスでき、表示されるすべての Windows ドメイン コントローラと通信できるネットワーク上のマシンに、Active Directory エージェントをインストールします。最高のパフォーマンスを実現するために、このエージェントは Web Security Appliance に物理的にできるだけ近いところに配置する必要があります。小規模なネットワーク環境では、Active Directory サーバに直接 Active Directory エージェントをインストールすることもできます。

(注)　Web Security Appliance との通信に使用される Active Directory エージェントのインスタンスは、シスコの適応型セキュリティ アプライアンスやその他の Web Security Appliance など、他のアプライアンスもサポートできます。

Cisco Context Directory Agent の取得、インストール、および設定

Cisco Context Directory Agent のダウンロード、インストール、および設定に関する詳細については、http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html を参照してください。

(注)　Web Security Appliance と Active Directory エージェントは、RADIUS プロトコルを使用して相互に通信します。アプライアンスとエージェントは、ユーザのパスフレーズを難読化するために同じ共有秘密キーを使用して設定する必要があります。その他のユーザ属性は難読化されません。

LDAP による透過的ユーザ識別

AsyncOS for Web は、Lightweight Directory Access Protocol（LDAP）レルムとして設定されている eDirectory サーバと通信し、IP アドレス対ユーザ名のマッピングを保守できます。eDirectory クライアントを介してログインする場合、ユーザは eDirectory サーバに対して認証されます。認証に成功すると、ログインしたユーザの属性（`NetworkAddress`）としてクライアントの IP アドレスが eDirectory サーバに記録されます。

LDAP（eDirectory）を使用してユーザを透過的に識別する場合は、以下を考慮してください。

- eDirectory クライアントを各クライアント ワークステーションにインストールし、エンドユーザがそれを使用して eDirectory サーバによる認証を受けるようにする必要があります。
- eDirectory クライアントのログインで使用する LDAP ツリーは、認証レルムに設定されている LDAP ツリーと同一である必要があります。
- eDirectory クライアントが複数の LDAP ツリーを使用する場合は、ツリーごとに認証レルムを作成し、各 LDAP 認証レルムを使用する認証シーケンスを作成します。
- eDirectory として LDAP 認証レルムを設定する場合は、クエリー クレデンシャルのバインド DN を指定する必要があります。
- eDirectory サーバは、ユーザのログイン時にユーザ オブジェクトの `NetworkAddress` 属性を更新するように設定する必要があります。

- AsyncOS for Web はユーザが属する上位の親グループだけを検索します。ネストされたグループは検索しません。
- eDirectory ユーザの `NetworkAddress` 属性を使用して、ユーザの最新のログイン IP アドレスを特定できます。

透過的ユーザ識別のルールとガイドライン

任意の認証サーバで透過的ユーザ ID を使用する場合は、以下のルールとガイドラインを考慮してください。

- DHCP を使用してクライアント マシンに IP アドレスを割り当てる場合は、Web Security Appliance 上の IP アドレス対ユーザ名のマッピングが DHCP リースよりも頻繁に更新されるようにします。`tuiconfig` CLI コマンドを使用して、マッピングの更新間隔を更新します。詳細については、CLI を使用した透過的ユーザ識別の詳細設定（5-10 ページ）を参照してください。
- IP アドレス対ユーザ名のマッピングが Web Security Appliance 上で更新される前に、ユーザがマシンからログアウトし、別のユーザが同じマシンにログインした場合、Web プロキシは前のユーザをクライアントとして記録します。
- 透過的ユーザ ID が失敗したときに、Web プロキシがトランザクションを処理する方法を設定できます。ユーザにゲスト アクセスを許可するか、または認証プロンプトをエンド ユーザに強制的に表示することができます。
- 透過的ユーザ ID の失敗によりユーザに認証プロンプトが表示され、ユーザが無効なクレデンシャルにより認証に失敗した場合、ユーザのゲスト アクセスを許可するかどうかを選択できます。
- 割り当てられた識別プロファイルが、ユーザが存在する複数のレルムを含む認証シーケンスを使用している場合、AsyncOS for Web はシーケンスで示される順序でレルムからユーザ グループを取得します。
- ユーザを透過的に識別するように識別プロファイルを設定する場合、認証サロゲートは IP アドレスでなければなりません。別のサロゲート タイプを選択することはできません。
- ユーザの詳細なトランザクションを表示すると、透過的に識別されたユーザが [Web トラッキング（Web Tracking）] ページに表示されます。
- `%m` および `x-auth-mechanism` カスタム フィールドを使用して、透過的に識別されたユーザをアクセス ログと WC3 ログに記録することができます。`SSO_TUI` のログ エントリは、ユーザ名が、透過的ユーザ識別により認証されたユーザ名をクライアント IP アドレスと照合することによって取得されたことを示しています。（同様に、`SSO_ASA` の値は、ユーザがリモート ユーザであり、ユーザ名が AnyConnect Secure Mobility を使用して Cisco ASA から取得されたことを示しています）。

透過的ユーザ識別の設定

透過的なユーザの識別と認証の設定については、エンドユーザ クレデンシャルの取得（5-1 ページ）に詳しく記載されています。基本的な手順は以下のとおりです。

- 認証レルムを作成して、順序付けます。
- 識別プロファイルを作成し、ユーザおよびクライアント ソフトウェアを分類します。
- 識別されたユーザとユーザ グループからの Web 要求を管理するポリシーを作成します。

CLI を使用した透過的ユーザ識別の詳細設定

AsyncOS for Web は以下の TUI 関連の CLI コマンドを備えています。

- **tuiconfig**：透過的ユーザ識別に関連する詳細設定を設定します。バッチ モードを使用して、複数のパラメータを同時に設定できます。
  - **Configure mapping timeout for Active Directory agent**：AD エージェントからのアップデートがない場合に、AD エージェントによって取得された IP アドレスに対して、IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さ（分単位）。
  - **Configure proxy cache timeout for Active Directory agent**：プロキシ固有の IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さ（秒単位）。有効な値は 5 ～1200 秒です。デフォルト値および推奨値は 120 秒です。より低い値を指定すると、プロキシのパフォーマンスに悪影響を及ぼします。
  - **Configure mapping timeout for Novell eDirectory**：サーバからのアップデートがない場合に、eDirectory サーバから取得された IP アドレスに対して、IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さ（秒単位）。
  - **Configure query wait time for Active Directory agent**：Active Directory エージェントからの応答を待機する時間の長さ（秒単位）。クエリーに要する時間がこのタイムアウト値を上回った場合、透過的ユーザ識別は失敗したと見なされます。これにより、エンド ユーザが体験する認証遅延が限定されます。
  - **Configure query wait time for Novell eDirectory**：eDirectory サーバからの応答を待機する時間の長さ（秒単位）。クエリーに要する時間がこのタイムアウト値を上回った場合、透過的ユーザ識別は失敗したと見なされます。これにより、エンド ユーザが体験する認証遅延が限定されます。

  Active Directory の設定は、透過的ユーザ識別に AD エージェントを使用するすべての AD レルムに適用されます。eDirectory の設定は、透過的ユーザ識別に eDirectory を使用するすべての LDAP レルムに適用されます。

  いずれかのパラメータの検証に失敗した場合は、どの値も変更されません。
- **tuistatus**：このコマンドには、以下のような AD 関連のサブコマンドがあります。
  - **adagentstatus**：すべての AD エージェントの現在のステータス、および Windows ドメイン コントローラとの接続に関する情報を表示します。
  - **listlocalmappings**：Web Security Appliance に保存されているすべての IP アドレス対ユーザ名のマッピングを、AD エージェントによって取得された順序で一覧表示します。このコマンドは、エージェントに保存されているエントリや、現在クエリーが進行中のマッピングを一覧表示しません。

シングル サインオンの設定

透過的にクレデンシャルを取得することにより、シングル サインオン環境を実現できます。透過的ユーザ識別は認証レルムの設定項目の 1 つです。

Internet Explorer の場合は、リダイレクト ホスト名として、完全修飾ドメイン名ではなく、（ドットを含まない）短縮形のホスト名または NetBIOS 名を必ず使用します。または、Internet Explorer の [ローカル イントラネット] ゾーンにアプライアンスのホスト名を追加することができます（[ツール] > [インターネット オプション] > [セキュリティ] タブ）。ただし、この操作をすべてのクライアントで実行する必要があります。これに関する詳細については、『How do I properly set up NTLM with SSO (credentials sent transparently)?』を参照してください。

Firefox およびその他の Microsoft 以外のブラウザでは、パラメータ **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris**、**network.automatic-ntlm-auth.trusted-uris** を透過モードのリダイレクト ホスト名に設定する必要があります。『Firefox is not sending authentication credentials transparently (SSO)』も参照してください。この記事には、Firefox パラメータの変更に関する一般情報が記載されています。

リダイレクト ホスト名については、グローバル認証の設定、または CLI コマンド sethostname を参照してください。

認証レルム

認証レルムによって、認証サーバに接続するために必要な詳細情報を定義し、クライアントと通信するときに使用する認証方式を指定します。AsyncOS は複数の認証レルムをサポートしています。レルムを認証シーケンスにグループ化することにより、認証要件が異なるユーザを同じポリシーで管理することができます。

- 外部認証（5-11 ページ）
- Kerberos 認証方式の Active Directory レルムの作成（5-12 ページ）
- Active Directory 認証レルムの作成（NTLMSSP および基本）（5-15 ページ）
- LDAP 認証レルムの作成（5-17 ページ）
- 認証レルムの削除について（5-22 ページ）
- グローバル認証の設定（5-22 ページ）

関連項目

- RADIUS ユーザ認証（22-9 ページ）
- 認証シーケンス（5-28 ページ）

外部認証

外部 LDAP または RADIUS サーバからユーザを認証できます。

LDAP サーバによる外部認証の設定

はじめる前に

- LDAP 認証レルムを作成し、それに 1 つ以上の外部認証クエリーを設定します。LDAP 認証レルムの作成（5-17 ページ）。

手順 1　アプライアンスで外部認証を有効にします。

a. [システム管理（System Administration）] > [ユーザ（Users）] に移動します。

b. [外部認証（External Authentication）] セクションで [有効（Enable）] をオンにします。

c. 以下のオプションを設定します。

オプション	説明
認証タイプ（Authentication Type）	[LDAP] を選択します。
外部認証キャッシュタイムアウト（External Authentication Cache Timeout）	再認証のために LDAP サーバに再接続するまで、AsyncOS が外部認証クレデンシャルを保存する秒数。デフォルトはゼロ（0）です。
LDAP 外部認証クエリー（LDAP External Authentication Query）	LDAP レルムにより設定されたクエリー。
サーバからの有効なレスポンス待ちタイムアウト（Timeout to wait for valid response from server）	AsyncOS がサーバからのクエリーに対する応答を待機する秒数。
グループ マッピング（Group Mapping）	ディレクトリ内の各グループ名に対して、ロールを割り当てます。

手順 2　変更を送信し、保存します。

RADIUS 外部認証のイネーブル化

その場合は、次のトピックを参照してください。

RADIUS ユーザ認証（22-9 ページ）。

Kerberos 認証方式の Active Directory レルムの作成

はじめる前に

- アプライアンスが（クラウド コネクタ モードではなく）標準モードで設定されていることを確認します。
- Active Directory サーバを準備します。
  - 以下のサーバのいずれかに Active Directory をインストールします：Windows Server 2003、2008、2008R2、2012。
  - ドメイン管理者グループまたはアカウント オペレータ グループのメンバーであるユーザを Active Directory サーバ上に作成します。

    または
  - 次の権限を持つユーザ名を作成します。

    - Active Directory でのパスワード リセット権限

    - servicePrincipalName への検証済み書き込み

    - アカウント制限事項の書き込み

    - dNShost 名の書き込み

    - servicePrincipalName の書き込み

    以上は、アプライアンスをドメインに参加させてアプライアンスが完全機能していることを確認するために、ユーザ名に必要な最小限の Active Directory 権限です。

  - クライアントをドメインに参加させます。サポートされるクライアントは、Windows XP、Windows 7、Mac OS 10.5+ です。
  - Windows Resource Kit の kerbtray ツールを使用して、クライアントの Kerberos チケットを確認します（http://www.microsoft.com/en-us/download/details.aspx?id=17657）。
  - Mac クライアントでは、[メイン メニュー（Main Menu）] > [Keychain Access] で、Ticket Viewer アプリケーションを使用して Kerberos チケットを確認できます。
- 認証元となる Active Directory ドメインに Webセキュリティ アプライアンスを参加させるために必要な、権限とドメイン情報を取得済みであることを確認します。
- Web Security Appliance の現在の時刻と Active Directory サーバの現在時刻を比較して、その差が Active Directory サーバの [コンピュータ クロック同期の最大許容時間（Maximum tolerance for computer clock synchronization）] オプションで指定されている時間を超えていないことを確認します。
- Web Security Appliance がセキュリティ管理アプライアンスで管理されている場合は、異なる Web Security Appliance 上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同一になるように設定しておきます。
- Web Security Appliance の設定
  - 明示的モードでは、WSA ホスト名（sethostname CLI コマンド）をブラウザで設定されているプロキシ名と同じにする必要があります。
  - 透過モードでは、WSA ホスト名をリダイレクト ホスト名と同じにする必要があります（グローバル認証の設定（5-22 ページ）を参照）。さらに、Kerberos レルムを作成する前に、WSA ホスト名とリダイレクト ホスト名を設定する必要があります。
- 新しいレルムを確定すると、レルムの認証プロトコルを変更できなくなるので注意してください。
- シングル サインオン（SSO）をクライアント ブラウザで設定する必要があります（シングル サインオンの設定（5-10 ページ）を参照）。
- ログの使用を簡素化するため、%m のカスタム フィールドのパラメータを使用してアクセス ログをカスタマイズします。アクセス ログのカスタマイズ（21-32 ページ）を参照してください。

手順 1　Cisco Web セキュリティ アプライアンス Web インターフェイスで、[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[レルムを追加（Add Realm）] をクリックします。

手順 3　英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

手順 4　[認証プロトコル（Authentication Protocol）] フィールドで [Active Directory] を選択します。

手順 5　Active Directory サーバの完全修飾ドメイン名または IP アドレスを 3 つまで入力します。

例：`ntlm.example.com`

IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバが Active Directory サーバのホスト名を解決できない場合のみです。

レルムに複数の認証サーバを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバで認証を試みます。

手順 6　アプライアンスをドメインに参加させます。

a.　Active Directory アカウントを設定します。

設定	説明
Active Directory ドメイン（Active Directory Domain）	Active Directory サーバのドメイン名。DNS ドメインまたはレルムとも呼ばれます。
NetBIOS ドメイン名（NetBIOS domain name）	ネットワークで NetBIOS を使用する場合は、ドメイン名を入力します。 ヒント　このオプションを使用できない場合は、setntlmsecuritymode CLI コマンドを使用して、NTLM セキュリティ モードが [ドメイン（domain）] に設定されていることを確認します。
コンピュータ アカウント（Computer Account）	ドメイン上のコンピュータを一意的に識別する Active Directory コンピュータ アカウント（別名「マシン信頼アカウント」）が作成される、Active Directory ドメイン内の場所を指定します。 Active Directory 環境で、コンピュータ オブジェクトが一定の間隔で自動的に削除される場合は、自動削除から保護されているコンテナ内にコンピュータ アカウントの場所を指定します。

b. [ドメインに参加（Join Domain）] をクリックします。

（注） すでに参加しているドメインに参加しようとすると（同じクレデンシャルを使用している場合でも）、Active Directory が新しいキー セットをこの WSA を含む全てのクライアントに送信するため、既存の接続は閉じられます。影響を受けるクライアントは、ログオフしてから再度ログインする必要があります。

c. Active Directory 上のアカウントにログイン クレデンシャル（ユーザ名およびパスフレーズ）を指定し、[アカウントの作成（Create Account）] をクリックします。

手順 7　（任意）透過的ユーザ識別を設定します。

設定	説明
Active Directoryを使用して透過ユーザ識別を有効にする（Enable Transparent User Identification using Active Directory agent）	プライマリ Context Directory エージェントがインストールされているマシンのサーバ名と、それにアクセスするために使用する共有秘密の両方を入力します。 （任意）バックアップ Context Directory エージェントがインストールされているマシンのサーバ名とその共有秘密を入力します。

手順 8　ネットワーク セキュリティを設定します。

設定	説明
クライアントの署名が必須（Client Signing Required）	クライアントの署名を要求するように Active Directory サーバが設定されている場合は、このオプションを選択します。 このオプションを選択した場合、AsyncOS は、Active Directory サーバとの通信時に Transport Layer Security を使用します。

手順 9　（任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。テストの具体的な実行方法については、「•既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。（5-22 ページ）」を参照してください。

手順 10　テスト中に発生した問題をトラブルシューティングします。認証の問題のトラブルシューティング ツールを参照してください

手順 11　変更を送信し、保存します。

次の作業

- Kerberos 認証方式を使用する識別プロファイルを作成します。ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）。

Active Directory 認証レルムの作成（NTLMSSP および基本）

Active Directory 認証レルムの作成の前提条件（NTLMSSP および基本）

- 認証元となる Active Directory ドメインに Web セキュリティ アプライアンスを参加させるために必要な、権限とドメイン情報を取得済みであることを確認します。
- NTLM セキュリティ モードとして「domain」を使用する場合は、ネストした Active Directory グループのみを使用します。Active Directory グループがネストされていない場合は、デフォルト値の「ads」を使用します。このマニュアルの付録「コマンドライン インターフェイス」で setntlmsecuritymode を参照してください。
- Web Security Appliance の現在の時刻と Active Directory サーバの現在時刻を比較して、その差が Active Directory サーバの [コンピュータ クロック同期の最大許容時間（Maximum tolerance for computer clock synchronization）] オプションで指定されている時間を超えていないことを確認します。
- Web Security Appliance がセキュリティ管理アプライアンスで管理されている場合は、異なる Web Security Appliance 上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同一になるように設定しておきます。
- 新しいレルムを確定すると、レルムの認証プロトコルを変更できなくなるので注意してください。
- WSA は、信頼できるすべてのドメインのドメイン コントローラと、NTLM レルムに設定されたドメイン コントローラに接続する必要があります。認証が正しく機能するように、内部ドメインおよび外部ドメインのすべてのドメイン コントローラに対して次のポートを開く必要があります。

  LDAP（389 UDP および TCP）

  Microsoft SMB（445 TCP）

  Kerberos（88 UDP）

  エンドポイント解決：ポート マッパー（135 TCP）Net Log-on 固定ポート
- NTLMSSP の場合は、クライアント ブラウザにシングル サインオン（SSO）を設定できます。シングル サインオンの設定（5-10 ページ）を参照してください。

複数の NTLM レルムとドメインの使用について

以下のルールは、複数の NTLM レルムとドメインを使用する場合に該当します。

- 最大 10 の NTLM 認証レルムを作成できます。
- ある NTLM レルムのクライアント IP アドレスが、別の NTLM レルムのクライアント IP アドレスと重複しないようにする必要があります。
- 各 NTLM レルムは 1 つの Active Directory ドメインにのみ参加できますが、そのドメインが信頼しているあらゆるドメインのユーザを認証できます。この信頼は、同じフォレスト内の他のドメインにデフォルトで適用され、少なくとも一方向の信頼が存在しているフォレスト外部のドメインに適用されます。
- 既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。

Active Directory 認証レルムの作成（NTLMSSP および基本）

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[レルムを追加（Add Realm）] をクリックします。

手順 3　英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

手順 4　[認証プロトコルと方式（Authentication Protocol and Scheme(s)）] フィールドで [Active Directory] を選択します。

手順 5　Active Directory サーバの完全修飾ドメイン名または IP アドレスを 3 つまで入力します。

例：`active.example.com`

IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバが Active Directory サーバのホスト名を解決できない場合のみです。

レルムに複数の認証サーバを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバで認証を試みます。

手順 6　アプライアンスをドメインに参加させます。

a.　Active Directory アカウントを設定します。

設定	説明
Active Directory ドメイン（Active Directory Domain）	Active Directory サーバのドメイン名。 DNS ドメインまたはレルムとも呼ばれます。
NetBIOS ドメイン名（NetBIOS domain name）	ネットワークで NetBIOS を使用する場合は、ドメイン名を入力します。
コンピュータ アカウント（Computer Account）	ドメイン上のコンピュータを一意的に識別する Active Directory コンピュータ アカウント（別名「マシン信頼アカウント」）が作成される、Active Directory ドメイン内の場所を指定します。 Active Directory 環境で、コンピュータ オブジェクトが一定の間隔で自動的に削除される場合は、自動削除から保護されているコンテナ内にコンピュータ アカウントの場所を指定します。

b.　[ドメインに参加（Join Domain）] をクリックします。

(注)　すでに参加しているドメインに参加しようとすると(同じクレデンシャルを使用している場合でも)、Active Directory が新しいキー セットをこの WSA を含む全てのクライアントに送信するため、既存の接続は閉じられます。影響を受けるクライアントは、ログオフしてから再度ログインする必要があります。

c. そのドメインにコンピュータ アカウントを作成する権限を持つ、既存の Active Directory ユーザの sAMAccountName ユーザ名とパスフレーズを入力します。

例:「jazzdoe」(「DOMAIN\jazzdoe」や「jazzdoe@domain」は使用しないでください)。

この情報は、コンピュータ アカウントを確立するために一度だけ使用され、保存されません。

d. [アカウントの作成(Create Account)] をクリックします。

手順 7　(任意)透過的認証を設定します。

設定	説明
Active Directory を使用して透過ユーザ識別を有効にする(Enable Transparent User Identification using Active Directory agent	プライマリ Context Directory エージェントがインストールされているマシンのサーバ名と、それにアクセスするために使用する共有秘密の両方を入力します。 (任意)バックアップ Context Directory エージェントがインストールされているマシンのサーバ名とその共有秘密を入力します。

手順 8　ネットワーク セキュリティを設定します。

設定	説明
クライアントの署名が必須(Client Signing Required)	クライアントの署名を要求するように Active Directory サーバが設定されている場合は、このオプションを選択します。 このオプションを選択した場合、AsyncOS は、Active Directory サーバとの通信時に Transport Layer Security を使用します。

手順 9　(任意)[テスト開始(Start Test)] をクリックします。これにより、ユーザが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。

手順 10　変更を送信し、保存します。

LDAP 認証レルムの作成

はじめる前に

- 組織の LDAP に関する以下の情報を取得します。
  - LDAP のバージョン
  - サーバのアドレス
  - LDAP ポート
- Web Security Appliance がセキュリティ管理アプライアンスで管理されている場合は、異なる Web Security Appliance 上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同じであることを確認します。

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[レルムを追加（Add Realm）] をクリックします。

手順 3　英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

手順 4　[認証プロトコルと方式（Authentication Protocol and Scheme(s)）] フィールドで [LDAP] を選択します。

手順 5　LDAP 認証の設定を入力します。

設定	説明
LDAP のバージョン（LDAP Version）	LDAP のバージョンを選択し、セキュア LDAP を使用するかどうかを選択します。 アプライアンスは、LDAP バージョン 2 および 3 をサポートしています。セキュア LDAP には LDAP バージョン 3 が必要です。 この LDAP サーバが透過的ユーザ識別で使用する Novell eDirectory をサポートしているかどうかを選択します。
LDAP サーバ（LDAP Server）	LDAP サーバの IP アドレスまたはホスト名、およびポート番号を入力します。最大 3 つのサーバを指定できます。 ホスト名は、完全修飾ドメイン名である必要があります。例: `ldap.example.com`。IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバが LDAP サーバのホスト名を解決できない場合のみです。 標準 LDAP のデフォルトのポート番号は 389 です。セキュア LDAP のデフォルトの番号は 636 です。 LDAP サーバが Active Directory サーバの場合は、ドメイン コントローラのホスト名または IP アドレス、およびポートを入力します。可能な限り、グローバル カタログ サーバの名前を入力し、ポート 3268 を使用します。ただし、グローバル カタログ サーバが物理的に離れた場所にあり、ローカル ドメイン コントローラのユーザのみを認証する必要がある場合は、ローカル ドメイン コントローラを使用することもできます。 **注:** レルムに複数の認証サーバを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバで認証を試みます。
LDAP 持続的接続（LDAP Persistent Connections） （[詳細設定（Advanced）] セクションの下）	以下の値のいずれかを選択します。 • [永続的接続の使用（無制限）（Use persistent connections (unlimited)）]。既存の接続を使用します。使用できる接続がない場合は、新しい接続が開かれます。 • [永続的接続の使用（Use persistent connections）]。既存の接続を使用して、指定された数の要求に使用します。最大値に達すると、LDAP サーバへの新しい接続が確立されます。 • [永続的接続を使用しない（Do not use persistent connections）]。必ず、LDAP サーバへの新しい接続を作成します。

設定	説明
ユーザ認証（User Authentication）	以下のフィールドに値を入力します。 [ベース識別名（ベース DN）（Base Distinguished Name (Base DN)] LDAP データベースはツリー型のディレクトリ構造になっており、アプライアンスはベース DN を使用して、LDAP ディレクトリ ツリー内の適切な場所に移動し、検索を開始します。有効なベース DN フィルタ文字列は、`object-value` という形式の 1 つ以上のコンポーネントで構成されます。たとえば、「`dc=companyname, dc=com`」のように入力します。 [ユーザ名属性（User Name Attribute）] 以下の値のいずれかを選択します。 • [uid]、[cn]、[sAMAccountName]。ユーザ名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`UserAccount`」などのカスタム ID。 [ユーザフィルタクエリー（User Filter Query）] ユーザ フィルタ クエリーは、ユーザのベース DN を見つける LDAP 検索フィルタです。これは、ユーザ ディレクトリがベース DN の下の階層にある場合、またはそのユーザのベース DN のユーザ固有コンポーネントにログイン名が含まれていない場合に必要です。 以下の値のいずれかを選択します。 • [なし（none）]。すべてのユーザを抽出します。 • [カスタム（custom）]。ユーザの特定のグループを抽出します。
クエリー クレデンシャル（Query Credentials）	認証サーバが匿名クエリーを受け入れるかどうかを選択します。 認証サーバが匿名クエリーを受け入れる場合は、[サーバは、匿名の質問に対応します（Server Accepts Anonymous Queries）] を選択します。 認証サーバが匿名クエリーを受け入れない場合は、[バインド DN を使用（Use Bind DN）] を選択し、以下の情報を入力します。 • [バインド DN（Bind DN）]。LDAP ディレクトリの検索を許可された外部 LDAP サーバ上のユーザ。通常、バインド DN はディレクトリ全体の検索を許可されます。 • [パスフレーズ（Passphrase）]。[バインドDN（Bind DN）] フィールドに入力するユーザに関連付けられるパスフレーズ。 以下のテキストは、[バインド DN（Bind DN）] フィールドに入力するユーザの例を示しています。 cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. LDAP サーバが Active Directory サーバの場合は、「DOMAIN\username」の形式でバインド DN ユーザ名を入力することもできます。

手順 6　（任意）グループ オブジェクトまたはユーザ オブジェクトを介して [グループ認証（Group Authorization）] をイネーブルにし、選択したオプションを設定します。

グループ オブジェクト設定	説明
グループ オブジェクト内のグループ メンバーシップ属性（Group Membership Attribute Within Group Object）	このグループに属するすべてのユーザをリストする LDAP 属性を選択します。 以下の値のいずれかを選択します。 • [member] および [uniquemember]。グループ メンバを指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`UserInGroup`」などのカスタム ID。
グループ名を含む属性（Attribute that Contains the Group Name）	ポリシー グループの設定で使用できるグループ名を指定する LDAP 属性を選択します。 以下の値のいずれかを選択します。 • [cn]。グループ名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`FinanceGroup`」などのカスタム ID。
オブジェクトがグループかどうかを判別するクエリ文字列（Query string to determine if object is a group）	LDAP オブジェクトがユーザ グループを表しているかどうかを判別する LDAP 検索フィルタを選択します。 以下の値のいずれかを選択します。 • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • [カスタム（custom）]。「`objectclass=person`」などのカスタム フィルタ。 **注:** クエリーによって、ポリシー グループで使用できる一連の認証グループが定義されます。

ユーザ オブジェクト設定	説明
ユーザ オブジェクト内のグループメンバーシップ属性（Group Membership Attribute Within User Object）	このユーザが属するすべてのグループをリストする属性を選択します。 以下の値のいずれかを選択します。 • [memberOf]。ユーザ メンバを指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`UserInGroup`」などのカスタム ID。
グループ メンバーシップ属性は DN（Group Membership Attribute is a DN）	グループ メンバーシップ属性が、LDAP オブジェクトを参照する識別名（DN）であるかどうかを指定します。Active Directory サーバの場合は、このオプションをイネーブルにします。 これをイネーブルにした場合は、以下の設定を指定する必要があります。

ユーザ オブジェクト設定	説明
グループ名を含む属性（Attribute that Contains the Group Name）	グループ メンバーシップ属性が DN である場合に、ポリシー グループ設定でグループ名として使用できる属性を指定します。 以下の値のいずれかを選択します。 • [cn]。グループ名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`FinanceGroup`」などのカスタム ID。
オブジェクトがグループかどうかを判別するクエリ文字列（Query string to determine if object is a group）	LDAP オブジェクトがユーザ グループを表しているかどうかを判別する LDAP 検索フィルタを選択します。 以下の値のいずれかを選択します。 • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • [カスタム（custom）]。「`objectclass=person`」などのカスタム フィルタ。 **注：**クエリーによって、Web Security Manager ポリシーで使用できる一連の認証グループが定義されます。

手順 7　（任意）ユーザに対する外部 LDAP 認証を設定します。

a. [外部認証クエリ（External Authentication Queries）] を選択します。

b. ユーザ アカウントを特定します。

ベース DN（Base DN）	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。

クエリー文字列（Query String）	一連の認証グループを返すクエリー。例：
	`(&(objectClass=posixAccount)(uid={u}))`
	または
	`(&(objectClass=user)(sAMAccountName={u}))`

ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	LDAP 属性（例：`displayName`、`gecos`）。

c. （任意）RFC 2307 アカウント有効期限 LDAP 属性に基づき、有効期限切れのアカウントはログインが拒否されます。

d. ユーザのグループ情報を取得するクエリーを入力します。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。

ベース DN（Base DN）	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。
クエリー文字列（Query String）	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	`gecos`

手順 8　(任意)[テスト開始(Start Test)] をクリックします。これにより、ユーザが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。テストの具体的な実行方法については、「 •既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。(5-22 ページ)」を参照してください。

(注)　変更を送信して確定すると、後でレルムの認証プロトコルを変更できなくなります。

手順 9　変更を送信し、保存します。

次の作業

- Kerberos 認証方式を使用する識別プロファイルを作成します。ユーザおよびクライアント ソフトウェアの分類(6-3 ページ)。

関連項目

- 外部認証(5-11 ページ)

複数の NTLM レルムとドメインの使用

以下のルールは、複数の NTLM レルムとドメインを使用する場合に該当します。

- 最大 10 の NTLM 認証レルムを作成できます。
- ある NTLM レルムのクライアント IP アドレスが、別の NTLM レルムのクライアント IP アドレスと重複しないようにする必要があります。
- 各 NTLM レルムは 1 つの Active Directory ドメインにのみ参加できますが、そのドメインが信頼しているあらゆるドメインのユーザを認証できます。この信頼は、同じフォレスト内の他のドメインにデフォルトで適用され、少なくとも一方向の信頼が存在しているフォレスト外部のドメインに適用されます。
- 既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。

認証レルムの削除について

認証レルムを削除すると関連する ID がディセーブルになり、さらに、関連するポリシーからそれらの ID が削除されます。

認証レルムを削除すると、そのレルムがシーケンスから削除されます。

グローバル認証の設定

認証レルムの認証プロトコルとは別途に、グローバル認証の設定項目を設定してすべての認証レルムに設定を適用します。

Web プロキシの展開モードは、設定できるグローバル認証の設定項目に影響します。明示的な転送モードよりも、透過モードで展開されている場合の方がより多くの設定項目を使用できます。

はじめる前に

- 以下の概念をよく理解しておいてください。
  - 認証の失敗（5-30 ページ）
  - 認証の失敗：異なるクレデンシャルによる再認証の許可（5-34 ページ）

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

手順 3　[グローバル認証設定（Global Authentication Settings）] セクションで、設定を編集します。

設定	説明
認証サーバが利用できない場合のアクション（Action if Authentication Service Unavailable）	以下の値のいずれかを選択します。 • [認証なしでトラフィックの通過を許可（Permit traffic to proceed without authentication）]。処理が、ユーザが認証されたかのように続行されます。 • [認証に失敗した場合にすべてのトラフィックをブロック（Block all traffic if user authentication fails）]。処理が中止され、すべてのトラフィックがブロックされます。
失敗した認証手続き（Failed Authentication Handling）	識別プロファイル ポリシーでユーザにゲスト アクセスを許可する場合は、この設定項目により、Web プロキシがユーザをゲストとして識別してアクセス ログに記録する方法を指定します。 ユーザのゲスト アクセス許可の詳細については、認証失敗後のゲスト アクセスの許可（5-33 ページ）を参照してください。
再認証（Re-authentication） （URL カテゴリまたはユーザ セッションの制限によりエンド ユーザがブロックされた場合に再認証プロンプトをイネーブルにする（Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction）））	制限が厳しい URL フィルタリング ポリシーによって、または別の IP アドレスへのログインの制限によってユーザが Web サイトからブロックされた場合に、ユーザに再認証を許可します。 新しい認証クレデンシャルを入力できるリンクが記載されたブロック ページがユーザに表示されます。より多くのアクセスを許可するクレデンシャルをユーザが入力すると、要求されたページがブラウザに表示されます。 **注：**この設定は、制限が厳しい URL フィルタリング ポリシーまたはユーザ セッションの制限によってブロックされた、認証済みユーザにのみ適用されます。認証されずに、サブネットによりブロックされたトランザクションには適用されません。 詳細については、認証の失敗：異なるクレデンシャルによる再認証の許可（5-34 ページ）を参照してください。
ベーシック認証トークン TTL（Basic Authentication Token TTL）	認証サーバによって再検証されるまで、ユーザのクレデンシャルがキャッシュ内に保管される期間を制御します。これには、ユーザ名とパスフレーズ、およびユーザに関連付けられているディレクトリ グループが含まれます。 デフォルト値は推奨されている設定です。[サロゲート タイムアウト（Surrogate Timeout）] が設定されており、その値が [ベーシック認証トークン TTL（Basic Authentication Token TTL）] よりも大きい場合は、サロゲート タイムアウトの値が優先され、Web プロキシは、サロゲート タイムアウトの期限が切れた後に認証サーバに連絡します。

その他の設定可能な認証設定項目は、Web プロキシが展開されているモード（透過モードまたは明示的な転送モード）に応じて異なります。

手順 4　Web プロキシが透過モードで展開されている場合は、以下の設定項目を編集します。

設定	説明
クレデンシャルの暗号化（Credential Encryption）	クライアントが暗号化 HTTPS 接続を介して Web プロキシにログイン クレデンシャルを送信するかどうかを指定します。 この設定は基本認証方式と NTLMSPP 認証方式の両方に適用されますが、特に基本認証方式の場合に役立ちます。基本認証方式では、ユーザ クレデンシャルがプレーン テキストで送信されるからです。 詳細については、認証の失敗（5-30 ページ）を参照してください。
HTTPS リダイレクト ポート（HTTPS Redirect Port）	HTTPS 接続を介してユーザ認証要求をリダイレクトする場合に使用する TCP ポートを指定します。 これによって、クライアントが HTTPS による Web プロキシへの接続を開始するポートが指定されます。これは、クレデンシャルの暗号化がイネーブルになっている場合や、アクセス コントロールの使用時にユーザに認証を求める場合に発生します。
リダイレクト ホスト名（Redirect Hostname）	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短いホスト名を入力します。 透過モードで展開されているアプライアンスに認証を設定した場合、Web プロキシは、ユーザの認証のためにクライアントに送信するリダイレクション URL でこのホスト名を使用します。 以下の値のいずれかを入力できます。 • [1 語のホスト名（Single word hostname）]。クライアントと Web Security Appliance が DNS 解決可能な 1 語のホスト名を入力できます。これにより、クライアントは、ブラウザ側を設定することなく、Internet Explorer で真のシングル サインオンを実現できます。必ず、クライアントと Web Security Appliance が DNS 解決可能な 1 語のホスト名を入力してください。 たとえば、クライアントがドメイン `mycompany.com` にあり、Web プロキシがリッスンしているインターフェイスの完全なホスト名が `proxy.mycompany.com` である場合は、このフィールドに「`proxy`」と入力する必要があります。クライアントは「`proxy`」に対してルックアップを実行し、`proxy.mycompany.com` を解決できます。 • [完全修飾ドメイン名（FQDN）（Fully qualified domain name (FQDN)）]。このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、その場合、Internet Explorer や Firefox ブラウザで真のシングル サインオンを実現するには、入力する FQDN または IP アドレスが、クライアント ブラウザのクライアント信頼済みサイト リストに追加されていることを確認する必要があります。 デフォルト値は、プロキシ トラフィックに使用されるインターフェイスに応じて、M1 または P1 インターフェイスの FQDN です。

設定	説明
クレデンシャル キャッシュ オプション:（Credential Cache Options:） サロゲート タイムアウト（Surrogate Timeout）	クライアントに認証クレデンシャルを再度要求するまでに、Web プロキシが待機する時間を指定します。クレデンシャルを再度要求するまで、Web プロキシはサロゲートに保存された値（IP アドレスまたは Cookie）を使用します。 一般的に、ブラウザなどのユーザ エージェントでは、ユーザが毎回クレデンシャルを入力する必要がないように、認証クレデンシャルがキャッシュされます。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） クライアント IP アイドル タイムアウト（Client IP Idle Timeout）	IP アドレスを認証サロゲートとして使用する場合は、この設定で、クライアントがアイドル状態のときに、認証クレデンシャルをクライアントに再要求するまで Web プロキシが待機する時間を指定します。 この値がサロゲート タイムアウト値よりも大きい場合、この設定には効力がなく、サロゲート タイムアウトに達した後にクライアントへの認証要求が行われます。 この設定を使用すると、コンピュータの前にいない時間が多いユーザの脆弱性を低減できます。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） キャッシュ サイズ（Cache Size）	認証キャッシュに格納するエントリの数を指定します。この値を設定すると、実際にこのデバイスを使用しているユーザの数に安全に対応できます。デフォルト値は推奨されている設定です。
ユーザ セッション制限（User Session Restrictions）	認証済みユーザが複数の IP アドレスから同時にインターネットにアクセスすることを許可するかどうかを指定します。 ユーザが未認証ユーザと認証クレデンシャルを共有しないように、1 つのマシンへのアクセスを制限できます。ユーザが別のマシンでログインできない場合は、エンド ユーザ通知ページが表示されます。このページの [再認証（Re-authentication）] 設定を使用し、ユーザがボタンをクリックして別のユーザ名でログインできるかどうかを指定することもできます。 この設定をイネーブルにする場合は、制限タイムアウト値を入力します。この値によって、別の IP アドレスでマシンにログインできるようになるまでのユーザの待機時間を指定します。制限タイムアウト値は、サロゲートタイムアウト値よりも大きい値でなければなりません。 `authcache` CLI コマンドを使用して、認証キャッシュから特定のユーザやすべてのユーザを削除できます。
詳細設定（Advanced）	クレデンシャルの暗号化またはアクセス コントロールを使用している場合は、アプライアンスがそれに付属しているデジタル証明書とキー（Cisco IronPort Web セキュリティ アプライアンス デモ証明書）を使用するか、ここでアップロードするデジタル証明書を使用するかを選択できます。

手順 5　Web プロキシが明示的な転送モードで展開されている場合は、以下の設定項目を編集します。

設定	説明
クレデンシャルの暗号化（Credential Encryption）	クライアントが暗号化 HTTPS 接続を介して Web プロキシにログイン クレデンシャルを送信するかどうかを指定します。クレデンシャルの暗号化をイネーブルにするには、[HTTPS リダイレクト（セキュアな）（HTTPS Redirect (Secure)）] を選択します。クレデンシャルの暗号化をイネーブルにすると、認証のためにクライアントを Web プロキシにリダイレクトする方法を設定する追加フィールドが表示されます。 この設定は基本認証方式と NTLMSPP 認証方式の両方に適用されますが、特に基本認証方式の場合に役立ちます。基本認証方式では、ユーザ クレデンシャルがプレーン テキストで送信されるからです。 詳細については、認証の失敗（5-30 ページ）を参照してください。
HTTPS リダイレクト ポート（HTTPS Redirect Port）	HTTPS 接続を介してユーザ認証要求をリダイレクトする場合に使用する TCP ポートを指定します。 これによって、クライアントが HTTPS による Web プロキシへの接続を開始するポートが指定されます。これは、クレデンシャルの暗号化がイネーブルになっている場合や、アクセス コントロールの使用時にユーザに認証を求める場合に発生します。
リダイレクト ホスト名（Redirect Hostname）	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短縮形のホスト名を入力します。 上記の認証モードをイネーブルにすると、Web プロキシは、ユーザの認証のためにクライアントに送信するリダイレクション URL でこのホスト名を使用します。 以下の値のいずれかを入力できます。 • [1 語のホスト名（Single word hostname）]。クライアントと Web Security Appliance が DNS 解決可能な 1 語のホスト名を入力できます。これにより、クライアントは、ブラウザ側を設定することなく、Internet Explorer で真のシングル サインオンを実現できます。必ず、クライアントと Web Security Appliance が DNS 解決可能な 1 語のホスト名を入力してください。 たとえば、クライアントがドメイン `mycompany.com` にあり、Web プロキシがリッスンしているインターフェイスの完全なホスト名が `proxy.mycompany.com` である場合は、このフィールドに「`proxy`」と入力する必要があります。クライアントは「`proxy`」に対してルックアップを実行し、`proxy.mycompany.com` を解決できます。 • [完全修飾ドメイン名（FQDN）（Fully qualified domain name (FQDN)）]。このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、その場合、Internet Explorer や Firefox ブラウザで真のシングル サインオンを実現するには、入力する FQDN または IP アドレスが、クライアント ブラウザのクライアント信頼済みサイト リストに追加されていることを確認する必要があります。 デフォルト値は、プロキシ トラフィックに使用されるインターフェイスに応じて、M1 または P1 インターフェイスの FQDN です。

設定	説明
クレデンシャル キャッシュ オプション:（Credential Cache Options:） サロゲート タイムアウト（Surrogate Timeout）	クライアントに認証クレデンシャルを再度要求するまでに、Web プロキシが待機する時間を指定します。クレデンシャルを再度要求するまで、Web プロキシはサロゲートに保存された値（IP アドレスまたは Cookie）を使用します。 一般的に、ブラウザなどのユーザ エージェントでは、ユーザが毎回クレデンシャルを入力する必要がないように、認証クレデンシャルがキャッシュされます。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） クライアント IP アイドル タイムアウト（Client IP Idle Timeout）	IP アドレスを認証サロゲートとして使用する場合は、この設定で、クライアントがアイドル状態のときに、認証クレデンシャルをクライアントに再要求するまで Web プロキシが待機する時間を指定します。 この値がサロゲート タイムアウト値よりも大きい場合、この設定には効力がなく、サロゲート タイムアウトに達した後にクライアントへの認証要求が行われます。 この設定を使用すると、コンピュータの前にいない時間が多いユーザの脆弱性を低減できます。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） キャッシュ サイズ（Cache Size）	認証キャッシュに格納するエントリの数を指定します。この値を設定すると、実際にこのデバイスを使用しているユーザの数に安全に対応できます。デフォルト値は推奨されている設定です。
ユーザ セッション制限（User Session Restrictions）	認証済みユーザが複数の IP アドレスから同時にインターネットにアクセスすることを許可するかどうかを指定します。 ユーザが未認証ユーザと認証クレデンシャルを共有しないように、1 つのマシンへのアクセスを制限できます。ユーザが別のマシンでログインできない場合は、エンド ユーザ通知ページが表示されます。このページの [再認証（Re-authentication）] 設定を使用し、ユーザがボタンをクリックして別のユーザ名でログインできるかどうかを指定することもできます。 この設定をイネーブルにする場合は、制限タイムアウト値を入力します。この値によって、別の IP アドレスでマシンにログインできるようになるまでのユーザの待機時間を指定します。制限タイムアウト値は、サロゲートタイムアウト値よりも大きい値でなければなりません。 `authcache` CLI コマンドを使用して、認証キャッシュから特定のユーザやすべてのユーザを削除できます。
詳細設定（Advanced）	クレデンシャルの暗号化またはアクセス コントロールを使用している場合は、アプライアンスがそれに付属しているデジタル証明書とキー（Cisco IronPort Web セキュリティ アプライアンス デモ証明書）を使用するか、ここでアップロードするデジタル証明書を使用するかを選択できます。 デジタル証明書とキーをアップロードするには、[参照（Browse）] をクリックして、ローカル マシン上の必要なファイルに移動します。次に、目的のファイルを選択してから、[ファイルのアップロード（Upload Files）] をクリックします。

手順 6　変更を送信し、保存します。

認証シーケンス

認証シーケンスについて

認証シーケンスを使用すると、さまざまな認証サーバやプロトコルで 1 つの ID によってユーザを認証できます。認証シーケンスは、プライマリ認証オプションを使用できなくなった場合にバックアップ オプションを提供する上でも役立ちます。

認証シーケンスは複数の認証レルムの集合です。使用するレルムには、さまざまな認証サーバや認証プロトコルを指定できます。認証レルムの詳細については、認証レルム（5-11 ページ）を参照してください。

2 番目の認証レルムを作成すると、[ネットワーク（Network）] > [認証（Authentication）] に、[すべてのレルム（All Realms）] というデフォルトの認証シーケンスを含む [レルム シーケンス（Realm Sequences）] セクションが自動的に表示されます。[すべてのレルム（All Realms）] シーケンスには、ユーザが定義した各レルムが自動的に含まれます。[すべてのレルム（All Realms）] シーケンス内のレルムの順序は変更できますが、[すべてのレルム（All Realms）] シーケンスを削除したり、そこからレルムを削除することはできません。

複数の NTLM 認証レルムを定義した場合、Web Security Appliance は、各シーケンスの 1 つの NTLM 認証レルムだけを NTLMSSP 認証方式で使用します。[すべてのレルム（All Realms）] シーケンスを含め、各シーケンス内から、NTLMSSP で使用する NTLM 認証レルムを選択できます。複数の NTLM レルムを NTLMSSP で使用するには、各レルムに対して個々に識別プロファイルを定義します。

認証で使用されるシーケンス内の認証レルムは、以下によって決まります。

- 使用される認証方式。通常これは、クライアントに入力したクレデンシャル タイプで指定されます
- シーケンス内でのレルムの順序（1 つの NTLMSSP レルムだけを使用できるので、基本レルムのみ）。

ヒント　最適なパフォーマンスを得るには、1 つのレルムを使用して同じサブネット上のクライアントを認証します。

認証シーケンスの作成

はじめる前に

- 複数の認証レルムを作成します（認証レルム（5-11 ページ）を参照）。
- Web Security Appliance がセキュリティ管理アプライアンスで管理されている場合は、異なる Web Security Appliance 上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同じであることを確認します。
- AsyncOS では、レルムを使用して認証を処理する際に、リストの先頭のレルムから順番に使用されることに注意してください。

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[シーケンスを追加（Add Sequence）] をクリックします。

手順 3　英数字とスペース文字を使用して、シーケンスの一意の名前を入力します。

手順 4　[基本スキームのレルム シーケンス（Realm Sequence for Basic Scheme）] 領域の最初の行で、シーケンスに含める最初の認証レルムを選択します。

手順 5　[基本スキームのレルム シーケンス（Realm Sequence for Basic Scheme）] 領域の 2 番目の行で、シーケンスに含める以下のレルムを選択します。

手順 6　（任意）基本クレデンシャルを使用する他のレルムを追加するには、[行の追加（Add Row）] をクリックします。

手順 7　NTLM レルムを定義したら、[NTLMSSP スキームのレルム（Realm for NTLMSSP Scheme）] フィールドで NTLM レルムを選択します。

Web プロキシは、クライアントが NTLMSSP 認証クレデンシャルを送信するときに、この NTLM レルムを使用します。

手順 8　変更を送信し、保存します。

認証シーケンスの編集および順序変更

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　編集または順序変更するシーケンスの名前をクリックします。

手順 3　レルムを配置するシーケンス内の位置番号に対応する行で、[レルム（Realms）] ドロップダウンリストからレルム名を選択します。

（注）　[すべてのレルム（All Realms）] シーケンスの場合は、レルムの順序のみを変更できます。レルム自体を変更することはできません。[すべてのレルム（All Realms）] シーケンス内のレルムの順序を変更するには、[順序（Order）] 列の矢印をクリックして、該当するレルムの位置を変更します。

手順 4　すべてのレルムをリストして順序付けするまで、必要に応じてステップ 3 を繰り返し、各レルム名が 1 つの行にのみ表示されていることを確認します。

手順 5　変更を送信し、保存します。

認証シーケンスの削除

はじめる前に

- 認証レルムを削除すると関連する ID がディセーブルになり、さらに、関連するポリシーからそれらの ID が削除されるので注意してください。

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　シーケンス名に対応するゴミ箱アイコンをクリックします。

手順 3　[削除(Delete)] をクリックして、シーケンスを削除することを確定します。

手順 4　変更を保存します。

認証の失敗

認証の失敗について

以下の理由により認証に失敗したため、ユーザが Web からブロックされることがあります。

- **クライアント/ユーザ エージェントの制限。**一部のクライアント アプリケーションでは、認証が適切にサポートされないことがあります。認証を必要としない識別プロファイルを設定し、識別プロファイルの基準をそのクライアント(およびアクセスする必要がある URL(任意))に基づかせることで、これらのクライアントの認証をバイパスできます。
- **認証サービスを使用できない。**ネットワークまたはサーバの問題によって、認証サービスを使用できない場合があります。このような状況が生じた場合に未認証トラフィックを許可することを選択できます。
- **クレデンシャルが無効である。**ユーザによっては、適切な認証を得るための有効なクレデンシャルを提供できないことがあります(ビジターやクレデンシャルを待っているユーザなど)。そのようなユーザに制限付きの Web アクセスを許可するかどうかを選択できます。

関連項目

- 問題のあるユーザ エージェントの認証のバイパス(5-30 ページ)
- 認証のバイパス(5-32 ページ)
- 認証サービスが使用できない場合の未認証トラフィックの許可(5-32 ページ)
- 認証失敗後のゲスト アクセスの許可(5-33 ページ)

問題のあるユーザ エージェントの認証のバイパス

一部のユーザ エージェントには、通常の動作に影響する認証問題があることが判明されています。

以下のユーザ エージェント経由で認証をバイパスする必要があります。

- Windows Update エージェント
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient

- Akamai NetSession Interface
- Microsoft CryptoAPI
- NCSI
- MSDW
- Gnotify
- msde
- Google Update

(注)　トラフィックのフィルタリング（URL カテゴリに基づく）とスキャン（McAfee、Webroot）は、引き続き、アクセス ポリシー設定に従い、アクセス ポリシーによって実行されます。

手順 1　指定したユーザ エージェントとの認証をバイパスするように識別プロファイルを設定します。

a. [Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profile）] を選択します。

b. [識別プロファイルの追加（Add Identification Profile）] をクリックします。

c. 情報を入力します。

オプション	値
[名前（Name）]	ユーザ エージェントの AuthExempt 識別プロファイル。
上に挿入（Insert Above）	処理順序の最初のプロファイルに設定します。
サブネット別メンバの定義（Define Members by Subnet）	ブランクのままにします。
認証ごとにメンバを定義（Define Members by Authentication）	認証は不要です。

d. [詳細設定（Advanced）] > [ユーザ エージェント（User Agents）] をクリックします。

e. [選択なし（None Selected）] をクリックします。

f. [カスタムユーザエージェント（Custom User Agents）] で、問題のあるユーザ エージェントの文字列を指定します。

手順 2　アクセス ポリシーの設定

a. [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

b. [ポリシーを追加（Add Policy）] をクリックします。

c. 情報を入力します。

オプション	値
ポリシー名	ユーザ エージェントの認証免除
上記ポリシーを挿入（Insert Above Policy）	処理順序の最初のポリシーに設定します。

オプション	値
識別プロファイル ポリシー（Identification Profile Policy）	ユーザ エージェントの AuthExempt 識別プロファイル。
詳細設定（Advanced）	なし

手順 3　変更を送信し、保存します。

認証のバイパス

手順	詳細情報
1. [詳細設定（Advanced）] プロパティを設定して、影響を受ける Web サイトを含むカスタム URL カテゴリを作成します。	
2. 以下の特性を持つ識別プロファイルを作成します。 – 認証を必要とする ID が特に配置されている。 – カスタム URL カテゴリが含まれている。 – 影響を受けるクライアント アプリケーションが含まれている。 – 認証を必要としない。	ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）
3. 識別プロファイルのポリシーを作成します。	ポリシーの作成（10-7 ページ）

関連項目

- Web プロキシのバイパス

認証サービスが使用できない場合の未認証トラフィックの許可

（注）　この設定は、認証サービスを使用できない場合にのみ適用されます。恒久的に認証をバイパスするわけではありません。代替の方法については、認証の失敗について（5-30 ページ）を参照してください。

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

手順 3　[認証サーバが利用できない場合のアクション（Action if Authentication Service Unavailable）] フィールドで、[認証なしでトラフィックの通過を許可（Permit traffic to proceed without authentication）] をクリックします。

手順 4　変更を送信し、保存します。

認証失敗後のゲスト アクセスの許可

ゲスト アクセスを許可するには、以下の手順を実行する必要があります。

1. ゲスト アクセスをサポートする識別プロファイルの定義（5-33 ページ）
2. ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用（5-33 ページ）
3. （任意）ゲスト ユーザの詳細の記録方法の設定（5-34 ページ）

（注） 識別プロファイルがゲスト アクセスを許可しており、その識別プロファイルを使用しているユーザ定義のポリシーがない場合、認証に失敗したユーザは適切なポリシー タイプのグローバル ポリシーと照合されます。たとえば、MyIdentificationProfile がゲスト アクセスを許可し、MyIdentificationProfile を使用するユーザ定義のアクセス ポリシーがない場合、認証に失敗したユーザはグローバル アクセス ポリシーに一致します。ゲスト ユーザをグローバル ポリシーと照合しない場合は、ゲスト ユーザに適用してすべてのアクセスをブロックするポリシー グループを、グローバル ポリシーよりも上に作成します。

ゲスト アクセスをサポートする識別プロファイルの定義

手順 1 [Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] を選択します。

手順 2 [識別プロファイルの追加（Add Identification Profile）] をクリックして新しい ID を追加するか、使用する既存の ID の名前をクリックします。

手順 3 [ゲスト権限をサポート（Support Guest Privileges）] チェックボックスをオンにします。

手順 4 変更を送信し、保存します。

ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用

手順 1 [Web セキュリティ マネージャ（Web Security Manager）] メニューからポリシー タイプを選択します。

手順 2 ポリシー テーブル内のポリシー名をクリックします。

手順 3 [識別プロファイルおよびユーザ（Identification Profiles And Users）] ドロップダウン リストから、[1 つ以上の識別プロファイルを選択（Select One Or More Identification Profiles）] を選択します（まだ選択していない場合）。

手順 4 [識別プロファイル（Identification Profile）] 列のドロップダウン リストから、ゲスト アクセスをサポートしているプロファイルを選択します。

手順 5 [ゲスト（認証に失敗したユーザ）（Guests (Users Failing Authentication)）] オプション ボタンをクリックします。

（注） このオプションを使用できない場合は、選択した**プロファイル**がゲスト アクセスをサポートするように設定されていないことを示しています。ステップ 4 に戻って別のものを選択するか、ゲスト アクセスをサポートする識別プロファイルの定義（5-33 ページ）を参照して、新しいポリシーを定義してください。

手順 6 変更を送信し、保存します。

ゲスト ユーザの詳細の記録方法の設定

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

手順 3　[失敗した認証手続き（Failed Authentication Handling）] フィールドで、次に示す [ゲスト ユーザのログ方法（Log Guest User By）] のオプション ボタンをクリックします。

オプション ボタン	説明
[IP アドレス（IP Address）]	ゲスト ユーザのクライアント IP アドレスがアクセス ログに記録されます。
エンドユーザが入力したユーザ名（User Name As Entered By End-User）	最初に認証に失敗したユーザ名がアクセス ログに記録されます。

手順 4　変更を送信し、保存します。

認証の失敗：異なるクレデンシャルによる再認証の許可

異なるクレデンシャルによる再認証の許可について

前に使用したクレデンシャルが認証に失敗した場合に、ユーザが別のクレデンシャルを使用して再認証を受けることを許可するには、再認証機能を使用します。ユーザは正常に認証されますが、アクセスが許可されない限り、Web リソースにはアクセスできません。これは、認証は、検証したクレデンシャルをポリシーに渡すためにユーザを識別するだけであり、リソースへのユーザのアクセスを許可（または禁止）するのはポリシーだからです。

再認証を受けるには、ユーザは正常に認証されている必要があります。

- ユーザ定義のエンドユーザ通知ページで再認証機能を使用するには、リダイレクト URL を解析する CGI スクリプトで Reauth_URL パラメータを解析して使用する必要があります。

異なるクレデンシャルによる再認証の許可

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

手順 3　[URL カテゴリまたはユーザ セッションの制限によりエンド ユーザがブロックされた場合に再認証プロンプト（Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction）] チェックボックスをオンにします。

手順 4　[送信（Submit）] をクリックします。

識別済みユーザの追跡

(注)　アプライアンスがクッキー ベースの認証サロゲートを使用するように設定されている場合、アプライアンスは HTTP 要求を介した HTTPS および FTP のクライアントからクッキー情報を取得しません。このため、クッキーからユーザ名を取得できません。

明示的要求でサポートされる認証サロゲート

サロゲート タイプ	クレデンシャルの暗号化がディセーブルの場合			クレデンシャルの暗号化がイネーブルの場合		
[プロトコル（Protocol）]:	**HTTP**	**HTTPS および FTP over HTTP**	**ネイティブ FTP**	**HTTP**	**HTTPS および FTP over HTTP**	**ネイティブ FTP**
サロゲートなし	○	○	○	NA	NA	NA
IP ベース	○	○	○	○	○	○
Cookie ベース	○	○***	○***	○	×/○**	○***

透過的要求でサポートされる認証サロゲート

(注)　ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）の [認証サロゲート（Authentication Surrogates）] オプションの説明も参照してください。

サロゲート タイプ	クレデンシャルの暗号化がディセーブルの場合			クレデンシャルの暗号化がイネーブルの場合		
[プロトコル（Protocol）]:	**HTTP**	**HTTPS**	**ネイティブ FTP**	**HTTP**	**HTTPS**	**ネイティブ FTP**
サロゲートなし	NA	NA	NA	NA	NA	NA
IP ベース	○	×/○*	×/○*	○	×/○*	×/○*
Cookie ベース	○	×/○**	×/○**	○	×/○**	×/○**

* クライアントが HTTP サイトに要求を送信し、認証された後に機能します。その前の動作は、トランザクション タイプによって異なります。

- **ネイティブ FTP トランザクション。**トランザクションが認証をバイパスします。
- **HTTPS トランザクション。**トランザクションがドロップされます。ただし、認証を目的とする最初の HTTPS 要求を復号化するように HTTPS プロキシを設定できます。

** Cookie ベースの認証を使用している場合、Web プロキシは、HTTPS、ネイティブ FTP、および FTP over HTTP の各トランザクションに対してユーザを認証できません。この制限により、すべての HTTPS、ネイティブ FTP、FTP over HTTP の要求が認証をバイパスするため、認証は要求されません。

*** この場合は、Cookie ベースのサロゲートが設定されていても、サロゲートは使用されません。

関連項目

- 識別プロファイルと認証（6-9 ページ）

再認証ユーザの追跡

再認証の場合、より強力な権限を持つユーザが認証を求め承認されると、Web プロキシは、設定されている認証サロゲートに応じた期間だけこのユーザの ID をキャッシュします。

- [セッション Cookie（Session cookie）]。特権ユーザのアイデンティティが、ブラウザを閉じるか、セッションがタイム アウトになるまで使用されます。
- [永続的な Cookie（Persistent cookie）]。特権ユーザのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- [IP アドレス（IP Address）]。特権ユーザのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- [サロゲートなし（No surrogate）]。デフォルトでは、Web プロキシは新しい接続ごとに認証を要求しますが、再認証がイネーブルの場合は新しい要求ごとに認証を要求します。そのため、NTLMSSP を使用すると認証サーバの負荷が増大します。ただし、認証アクティビティの増加はユーザにはわからない場合があります。ほとんどのブラウザでは、ブラウザが閉じられるまで特権ユーザのクレデンシャルがキャッシュされ、再入力を求めることなく認証が行われるからです。また、Web プロキシが透過モードで展開され、[明示的転送要求に同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）] オプションがイネーブルでない場合は、明示的な転送要求に認証サロゲートが使用されず、再認証により負荷が増加します。

（注）　Web Security Appliance が認証サロゲートに Cookie を使用する場合は、クレデンシャルの暗号化をイネーブルにすることを推奨します。

クレデンシャル

認証クレデンシャルは、ユーザのブラウザまたは別のクライアント アプリケーションを介してユーザに認証クレデンシャルの入力を求めることによってユーザから取得されるか、または別のソースから透過的に取得されます。

- セッション中のクレデンシャルの再利用の追跡（5-37 ページ）
- 認証および承認の失敗（5-37 ページ）
- クレデンシャルの形式（5-37 ページ）
- 基本認証のクレデンシャルの暗号化（5-38 ページ）

セッション中のクレデンシャルの再利用の追跡

セッション中に 1 回ユーザを認証した後、認証サロゲートを使用すると、新しい要求ごとにユーザを認証するのでなく、そのセッション全体におけるクレデンシャルの再利用を追跡できます。認証サロゲートは、ユーザのワークステーションの IP アドレスまたはセッションに割り当てられた Cookie に基づくことができます。

Internet Explorer の場合は、リダイレクト ホスト名として、完全修飾ドメイン名ではなく、(ドットを含まない)短縮形のホスト名または NetBIOS 名を必ず使用します。または、Internet Explorer の [ローカル イントラネット] ゾーンにアプライアンスのホスト名を追加することができます([ツール] > [インターネット オプション] > [セキュリティ] タブ)。ただし、この操作をすべてのクライアントで実行する必要があります。これに関する詳細については、『How do I properly set up NTLM with SSO (credentials sent transparently)?』を参照してください。

Firefox およびその他の Microsoft 以外のブラウザでは、パラメータ **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris**、**network.automatic-ntlm-auth.trusted-uris** を透過モードのリダイレクト ホスト名に設定する必要があります。『Firefox is not sending authentication credentials transparently (SSO)』も参照してください。この記事には、Firefox パラメータの変更に関する一般情報が記載されています。

リダイレクト ホスト名については、グローバル認証の設定、または CLI コマンド sethostname を参照してください。

認証および承認の失敗

互換性のないクライアント アプリケーションなど、容認できる理由で認証に失敗した場合は、ゲスト アクセスを許可できます。

認証に成功したが、承認に失敗した場合は、要求したリソースへのアクセスが許可される可能性がある別のクレデンシャル セットによる再認証を許可できます。

関連項目

- 認証失敗後のゲスト アクセスの許可(5-33 ページ)
- 異なるクレデンシャルによる再認証の許可(5-34 ページ)

クレデンシャルの形式

認証方式	クレデンシャルの形式
NTLMSSP	`MyDomain\jsmith`

基本	`jsmith`
	`MyDomain\jsmith`
	(注)　ユーザが Windows ドメインを入力しなかった場合は、Web プロキシによってデフォルトの Windows ドメインが付加されます。

基本認証のクレデンシャルの暗号化

基本認証のクレデンシャルの暗号化について

暗号化した形式でクレデンシャルを HTTPS 経由で送信するには、クレデンシャルの暗号化をイネーブルにします。これによって、基本認証プロセスのセキュリティが向上します。

デフォルトでは、Web Security Appliance は、認証の安全を確保するために、自身の証明書と秘密キーを使用してクライアントとの HTTPS 接続を確立します。ただし、大部分のブラウザでは、この証明書が無効であることがユーザに警告されます。無効な証明書に関するメッセージをユーザに表示しないようにするには、組織で使用している有効な証明書とキーのペアをアップロードします。

クレデンシャル暗号化の設定

はじめる前に:

- IP サロゲートを使用するようにアプライアンスを設定します。
- （任意）証明書と暗号化された秘密キーを取得します。ここで設定した証明書とキーは、アクセス コントロールでも使用されます。

手順 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

手順 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

手順 3　[クレデンシャルの暗号化（Credential Encryption）]フィールドで、[認証には暗号化された HTTPS 接続を使用（Use Encrypted HTTPS Connection For Authentication）] チェックボックスをオンにします。

手順 4　（任意）認証時のクライアントの HTTPS 接続に対して、[HTTPS リダイレクト ポート（HTTPS Redirect Port）] フィールドでデフォルトのポート番号（443）を編集します。

手順 5　（任意）証明書とキーをアップロードします。

a. [詳細設定（Advanced）] セクションを展開します。

b. [証明書（Certificate）] フィールドで [参照（Browse）] をクリックし、アップロードする証明書ファイルを検索します。

c. [キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードする秘密キー ファイルを検索します。

d. [ファイルのアップロード（Upload File）] をクリックします。

手順 6　変更を送信し、保存します。

関連項目

- 証明書の管理（22-26 ページ）

認証に関するトラブルシューティング