エンドユーザー クレデンシャルの取得

この章で説明する内容は、次のとおりです。

エンドユーザー クレデンシャルの取得の概要

サーバー 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
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

ステップ	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）（23 ページ） • LDAP 認証レルムの作成（26 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（33 ページ）
3	外部認証を設定する。 外部 LDAP または RADIUS サーバーからユーザーを認証できます。	• 外部認証（17 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（43 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（54 ページ）
6	認証要件に基づいてユーザーとクライアント ソフトウェアを分類する識別プロファイルを作成する。	• ユーザーおよびクライアント ソフトウェアの分類
7	識別プロファイルの作成対象となったユーザーとユーザー 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

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、 Secure Web 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）。（Secure Web Appliance を推奨）
- Kerberos を使用する場合は、 Secure Web 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。
- 一部のユーザー 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。これらのユーザーエージェントとの認証をバイパスする必要があります。問題のあるユーザー エージェントの認証のバイパス（45 ページ） を参照してください。
- クライアントをアクティブに認証することは、リソースを大量に消費するタスクです。認証サロゲートを使用すると、認証が完了した後、設定された期間（デフォルトは 3600 秒）、**[グローバル認証（Global Authentication）]** > **[サロゲートタイムアウト（Surrogate Timeout）]** で構成可能な認証されたユーザーを記憶することにより、認証パフォーマンスを向上させることができます。アクティブな認証イベントの数を制限するために、可能な場合は常に IP サロゲートを使用する必要があります。

認証の計画

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（再認証は必要ありません） • HTTPS（CONNECT）要求で使用できる • パスフレーズが認証サーバー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 Secure Web 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ー エージェントを使用する場合、ユーザー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 • ユーザーが以前に 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、ユーザーに関連付けられる **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/基本

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ー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 Secure Web 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ーエージェントを使用する場合、ユーザー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 • ユーザーが以前に 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、ユーザーではなく、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、ユーザーが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、ユーザーに関連付けられる **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ー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 Secure Web 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ー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ー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 Secure Web 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 （44 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ー エージェントを使用する場合、ユーザー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 • ユーザーが以前に 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、ユーザーではなく、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、ユーザーが 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 （44 ページ）

ユーザーの透過的識別

従来、ユーザーの識別および認証では、ユーザーにユーザー名とパスフレーズの入力を求めていました。ユーザーが入力したクレデンシャルは認証サーバーによって認証され、その後、Webプロキシが、認証されたユーザー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、 Secure Web 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ー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ーを認証して、適切なポリシーを適用します。

ユーザーを透過的に識別して以下を実行する場合があります。

- ユーザー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 ユーザー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。

ユーザーの透過的識別は、Webプロキシがユーザー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。ユーザー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。ユーザーにゲストアクセスを許可するか、またはユーザーに認証プロンプトを表示することができます。

透過的ユーザー ID の失敗によりエンドユーザーに認証プロンプトが表示され、ユーザーが無効なクレデンシャルにより認証に失敗した場合、ユーザー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、エンドユーザー通知ページが表示され、別のユーザーとしてログインするオプションが提供されます。ユーザー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（49ページ）を参照してください。

透過的ユーザー識別について

透過的ユーザー識別は以下の方式で使用できます。

- [ISEによってユーザーを透過的に識別（Transparently identify users with ISE）]：Identity Services Engine（ISE）サービスまたは Passive Identity Connector（ISE-PIC）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、ユーザー名と関連するセキュリティ グループ タグは Identity Services Engine サーバーから取得されます。ISE-PIC を使用している場合は、ユーザー名と関連する ISE セキュリティ グループが取得されます。ISE/ISE-PIC サービスを統合するためのタスクを参照してください。
- [ASA によってユーザーを透過的に識別（Transparently identify users with ASA）]：ユーザーは、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 アドレス対ユーザー名のマッピングによって識別されます（リモート ユーザーのみ）。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 Secure Web 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。リモートユーザーを参照してください。
- [認証レルムによってユーザーを透過的に識別（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ー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、透過的ユーザー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ー識別 （9 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、透過的ユーザー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ー識別 （11 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、認証されたユーザー名と現在の 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ー識別

Active Directory は、 Secure Web 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、認証済みユーザーの情報を 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。

（注） CDA は、Windows サーバー 2016 では Active Directory によってサポートされていません。Identity Services Engine（ISE）または ISE パッシブ ID コントローラ（ISE-PIC）サービスを使用して、ユーザー情報を受信し、透過的なユーザー ID を取得できます。CDA から ISE/ISE-PIC に切り替える場合は、CDA と ISE/ISE-PIC 情報を使用する識別プロファイル、関連するアクセス ポリシー、復号化ポリシーを設定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 アドレス対ユーザー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 アドレスをユーザー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については、以下の「Secure Web Appliance に情報を提供する Active Directory エージェントの設定」を参照してください。

Active Directory を使用してユーザー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ー識別は、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。
- 透過的ユーザー 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 アドレス対ユーザー名 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、 Secure Web 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、 Secure Web Appliance にユーザのログアウト情報をプッシュします。ただし、ユーザー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、ユーザー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。ユーザー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ー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 アドレス対ユーザー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ー識別の詳細設定 （12 ページ）を参照してください。

- Active Directory エージェントは、ユーザー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ーの `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 Secure Web Applianceは同一である必要があります。
- AsyncOS for Web はユーザー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。

Secure Web Appliance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 アドレス対ユーザー名のマッピング情報を取得する必要があります。

Secure Web 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 Secure Web 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 サーバーに直接 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） Secure Web 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 Secure Web 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） Secure Web 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、ユーザー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。その他のユーザー属性は難読化されません。

LDAP による透過的ユーザー識別

AsyncOS for Web は、Lightweight Directory Access Protocol（LDAP）レルムとして設定されている eDirectory サーバーと通信し、IP アドレス対ユーザー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、ユーザーは eDirectory サーバー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ーの属性（NetworkAddress）としてクライアントの IP アドレスが eDirectory サーバーに記録されます。

LDAP（eDirectory）を使用してユーザー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、エンドユーザーがそれを使用して eDirectory サーバー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 サーバーは、ユーザーのログイン時にユーザー 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 はユーザー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 ユーザーの NetworkAddress 属性を使用して、ユーザーの最新のログイン IP アドレスを特定できます。

透過的ユーザー識別のルールとガイドライン

任意の認証サーバーで透過的ユーザー 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、 Secure Web 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ー識別の詳細設定 （12 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 Secure Web 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。
- 透過的ユーザー識別に失敗した場合に 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。ユーザー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ーに強制的に表示することができます。

- 透過的ユーザー ID の失敗によりユーザーに認証プロンプトが表示され、ユーザーが無効なクレデンシャルにより認証に失敗した場合、ユーザー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、ユーザー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ー グループを取得します。
- ユーザー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。
- ユーザー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ーが [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ーをアクセス 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、ユーザー名が、透過的ユーザー識別により認証されたユーザー名をクライアント 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、ユーザーがリモート ユーザーであり、ユーザー名が 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）。

透過的ユーザー識別の設定

透過的なユーザーの識別と認証の設定については、エンドユーザー クレデンシャルの取得の概要 （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、ユーザーおよびクライアント ソフトウェアを分類します。
- 識別されたユーザーとユーザー 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ー識別の詳細設定

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

- **`tuiconfig`**：透過的ユーザー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 アドレス対ユーザー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 アドレス対ユーザー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**：サーバーからのアップデートがない場合に、eDirectory サーバーから取得された IP アドレスに対して、IP アドレス対ユーザー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、透過的ユーザー識別は失敗したと見なされます。これにより、エンド ユーザーが体験する認証遅延が限定されます。
- **Configure query wait time for Novell eDirectory**：eDirectory サーバー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、透過的ユーザー識別は失敗したと見なされます。これにより、エンドユーザーが体験する認証遅延が限定されます。

Active Directory の設定は、透過的ユーザー識別に 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、透過的ユーザー識別に 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**： Secure Web Appliance に保存されているすべての IP アドレス対ユーザー名のマッピングを、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。透過的ユーザー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名を必ず使用してください。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 （33 ページ）、または CLI コマンド `sethostname` を参照してください。

ハイ アベイラビリティ展開で Kerberos 認証を行うための Windows Active Directory におけるサービス アカウントの作成

Kerberos認証でハイ アベイラビリティに関する問題が発生している場合は、この手順を使用します。ハイ アベイラビリティ展開で Kerberos 認証を使用するときに問題が発生する場所のシナリオは次のとおりです。

- ハイ アベイラビリティのホスト名の servicePrincipalName は、Active Directory 内の複数のコンピュータ アカウントに追加されます。
- Kerberos 認証は servicePrincipalName が Active Directory の 1 つのコンピュータ アカウントに追加されている場合に機能します。異なるアプライアンスノードでは、ケルベロスサービスチケットの復号化に異なる暗号化文字列が使用されるため、プライマリノードが変更されると高可用性に影響を及ぼす可能性があります。

始める前に

- ハイ アベイラビリティで Kerberos 認証に使用するユーザー名を選択します。この目的のためだけに使用する新しいユーザー名を作成することをお勧めします。
- 既存のユーザー名を使用する場合には、次の設定を行います。
  - ユーザー名にパスワードがない場合は、パスワードを設定します。
  - ユーザー アカウントのプロパティ ダイアログボックス（[Active Directory ユーザーとコンピュータ（Active Directory users and computers）]）で、次のことを行います。

    [ユーザーは次回のログオン時にパスワード変更が必要（User must change password at next logon）] チェック ボックスがオフになっていることを確認します。

    [パスワードを無期限にする（Password Never Expires）] チェックボックスをオンにします。

ステップ 1 [Active Directory ユーザーとコンピュータ（Active Directory users and computers）] で新しいユーザー名を作成します。

- パスワードを指定します。
- [ユーザーは次回のログオン時にパスワード変更が必要（User must change password at next logon）] チェックボックスをオフにします。
- [パスワードを無期限にする（Password Never Expires）] チェックボックスをオンにします。

ステップ 2 ハイ アベイラビリティのホスト名の SPN が、作成または選択した Active Directory ユーザー オブジェクトに関連付けられているかどうかを確認します。SPN には、http/ のプレフィックスが付けられ、その後にアプライアンスのハイ アベイラビリティのホスト名が付けられます。クライアントが、ホスト名を解決できることを確認します。

1. Windows の `setspn -q` コマンドを使用して、既存の関連付けをクエリーします。

   例：`setspn -q http/highavail.com`

   この例では、highavail.com は、アプライアンスのハイ アベイラビリティのホスト名です。

2. クエリの結果に応じて、SPN を削除するか、追加します。

（注） ケルベロス HA サービスアカウントのパスワードには、文字、数字、スペース、および特殊文字（~ ! @ # % ^ & ( ) _ - { } ' / [ ] : ; , | + = * ? <>）のみを含めることができます。これらの 3 つの特殊文字 $、`、または " のいずれかがケルベロス HA サービスアカウントのパスワードで使用されている場合、GUI と CLI の両方からの事前認証中にエラーが発生します。ただし、認証はパスワードに使用されるあらゆる種類の文字で成功します。

クエリ結果	操作
「このようなSPNは見つかりませんでした。（No such SPN found.）」	ハイ アベイラビリティのホスト名の SPN を Active Directory ユーザー オブジェクトに関連付けます。 • 次のように `setspn -s` コマンドを使用します。 `setspn -s http/highavail.com hausername` この例で、highavail.com はアプライアンスのハイ アベイラビリティのホスト名で、hausername は作成または選択したユーザー名です。
「既存のSPNが見つかりました。（Existing SPN found!）」 「共通名（CN）は、作成または選択したユーザー名を示しています。（The common name (CN) shows the user name created or chosen.）」 「例: CN＝hausername（Example: CN = hausername）」	Active Directory でこれ以上の作業は必要ありません。

クエリ結果	操作

「既存のSPNが見つかりました。（Existing SPN found!）」
「共通名（CN）によって、作成または選択したユーザー名は表示されません。（The common name (CN) does not show the user name created or chosen.）」
	1. SPN を削除します。
	次のように `setspn -d` コマンドを使用します。
	`setspn -d http/highavail.com johndoe`
	この例で、highavail.com は、アプライアンスのハイ アベイラビリティのホスト名で、johndoe は関連付けを解除するユーザー名です。
	2. SPN を追加します。
	次のように `setspn -s` コマンドを使用します。
	`setspn -s http/highavail.com hausername`
	この例で、highavail.com はアプライアンスのハイ アベイラビリティのホスト名で、hausername は作成または選択したユーザー名です。

（注） 関連する Active Directory レルムで keytab 認証が有効になっていることを確認します。Kerberos 認証方式の Active Directory レルムの作成 （18 ページ）を参照してください。レルムがすでに作成されている場合は、レルムを編集し、keytab 認証を有効にします。

認証レルム

認証レルムによって、認証サーバー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ーを同じポリシーで管理することができます。

認証フェールオーバー

現在のレルム設定では、プライマリ AD または LDAP が 1 つ、バックアップサーバーが 2 つあります。最初のプライマリサーバーに到達できない場合、クエリーは最初のバックアップサーバーに到達します。最初のバックアップサーバーにも到達できない場合、クエリーは2番目のサーバーに到達します。

表 *1 : IPFW* ルールを使用したフェールオーバー時間

フェールオーバー時間	プライマリからセカンダリへのバックアップへのフェールオーバーにかかる時間（秒）
プライマリ AD と Secure Web Applianceの間の接続を切断するまでの時間	75 ～ 80

フェールオーバー時間	プライマリからセカンダリへのバックアップへのフェールオーバーにかかる時間（秒）
プライマリ AD と Secure Web Applianceの間の接続を切断し、かつ最初のバックアップとSecure Web Applianceの間の接続も切断するまでの時間	180 ～ 250
プライマリ AD を再起動するまでの時間	42 秒
プライマリ AD の電源がオフになるまでの時間	75 ～ 80
プライマリ AD と最初のバックアップサーバーの電源がオフになるまでの時間	180 ～ 250

複数のサーバーがダウンしている場合は、動作しているドメインコントローラが見つかるまで、 Secure Web Applianceで接続の確立を再試行します。

- 外部認証 （17 ページ）
- Kerberos 認証方式の Active Directory レルムの作成 （18 ページ）
- Active Directory 認証レルムの作成（NTLMSSP および基本） （23 ページ）
- LDAP 認証レルムの作成 （26 ページ）
- 認証レルムの削除について （32 ページ）
- グローバル認証の設定 （33 ページ）

関連項目

- 認証シーケンス （42 ページ）
- RADIUS ユーザー認証

外部認証

外部 LDAP または RADIUS サーバーからユーザーを認証できます。

LDAP サーバーによる外部認証の設定

始める前に

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 （26 ページ）。

ステップ 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）] > [ユーザー（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
外部認証を有効にする（Enable External Authentication）	—
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 サーバーに再接続するまで、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。
サーバー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 がサーバー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ロールを割り当てます。

ステップ 2 変更を送信し、保存します。

RADIUS 外部認証のイネーブル化

RADIUS を使用した外部認証の有効化 を参照してください。

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

始める前に

- 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。
- 高可用性を設定する場合、**手順 9** で指定した [ケルベロス高可用性（Kerberos High Availability）] セクションの [キータブ認証を使用する（Use keytab authentication）] チェックボックスもオンにしてください。

  アプライアンスが、ロードバランサなどの HTTP/HTTPS トラフィック分散デバイスの背後にある場合は、Active Directory 内のトラフィック分散デバイスの SPN をユーザーアカウントに関連付けて、[ケルベロス高可用性（Kerberos High Availability）] セクションでそ

のユーザーアカウントのログイン情報を入力する必要があります。ネットワーク トポロジで、トラフィックをリダイレクトする最初のデバイスのSPNを追加する必要があります。たとえば、クライアントデバイスの送信ネットワークトラフィックがトラフィックマネージャ、ロードバランサ、および Secure Web Applianceを通過する場合、トラフィックマネージャの SPN を Active Directory のユーザーアカウントに追加し、このセクションでユーザー クレデンシャルを入力する必要があります。これは、トラフィック マネージャがクライアント デバイスのトラフィックを検出する最初のデバイスであるためです。

- Active Directory サーバーを準備します。
  - 次のサーバーのいずれかに Active Directory をインストールします。Windows Server 2003、2008、2008R2、2012、2016（coeus 11.8、12.0、12.5、14.0、14.5）、または 2019（coeus 14.5 のみ）。

    coeus 12.5 用の Active Directory Windows Server 2019 をインストールできます。
  - Active Directory サーバーでユーザーを作成します。
    - 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ーを Active Directory サーバー上に作成します。

      または
    - 次の権限を持つユーザー名を作成します。
      - 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、ユーザー名に必要な最小限の Active Directory 権限です。
  - クライン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 10、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 Secure Web Appliance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。

- Secure Web 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。
- Secure Web 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 Secure Web 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。
- Secure Web Applianceの設定：
  - 明示的モードでは、 Secure Web Applianceのホスト名（`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、 Secure Web Applianceの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 （33 ページ）を参照）。さらに、Kerberos レルムを作成する前に、 Secure Web Applianceの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 （13 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を参照してください。

（注） ケルベロス HA サービスアカウントのパスワードには、文字、数字、スペース、および特殊文字（~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>）のみを含めることができます。これらの 3 つの特殊文字 $、`、または " のいずれかがケルベロス HA サービスアカウントのパスワードで使用されている場合、GUI と CLI の両方からの事前認証中にエラーが発生します。ただし、認証はパスワードに使用されるあらゆる種類の文字で成功します。

ステップ 1 Cisco Secure Web Applianceの 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。

ステップ 2 [レルムを追加（Add Realm）] をクリックします。

ステップ 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。

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

ステップ 5 Active Directory サーバー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 サーバーが Active Directory サーバーのホスト名を解決できない場合だけです。

レルムに複数の認証サーバーを設定した場合、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 つの認証サーバーで認証を試みます。

ステップ 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 サーバーのドメイン名。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。
信頼できるドメインルックアップの有効化	レルムの信頼できるドメインルックアップの動作を制御するために、**[信頼できるドメインのルックアップを有効にする（Enable Trusted Domain Lookup）]** オプションが **[Active Directory アカウント（Active Directory Account）]** セクション（**[ネットワーク（Network）]** > **[認証（Authentication）]** > **[レルムの追加（Add Realm）]**）に追加されました。 このオプションは、デフォルトでは有効になっています。

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 Secure Web Applianceを含むすべてのクライアントに送信するため、既存の接続は閉じます。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。

（注） AWS に展開された Secure Web Applianceのホスト名は一意である必要があります。一意のホスト名を作成するには、ホスト名の最初の文字列を変更する必要があります。

たとえば、「mgmt」が最初の文字列としてホスト名に追加されている場合、「mgmt<*wsa_hostname*>」として変更できます。

c) Active Directory 上のアカウントにログイン クレデンシャル（ユーザー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。

ステップ 7 （任意）透過的ユーザー識別を設定します。

設定	説明
Active Directoryを使用して透過ユーザー識別を有効にする（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ー名と、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ー名とその共有秘密を入力します。

ステップ 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 サーバー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すると、以下の場合に SMB 署名が有効になります。 • アプライアンスが Active Directory に接続するときにデジタル署名を配置する場合。 • 中間者攻撃を防ぐ場合。

ステップ 9 ハイ アベイラビリティを使用する場合は、[Kerberosハイアベイラビリティ（Kerberos High Availability）] セクションで[キータブ認証を使用する（Use keytab authentication）]チェック ボックスをオンにします。

a) [ユーザー名（Username）] と [パスワード（Password）] を入力します。

ハイ アベイラビリティ クラスタの IP アドレスまたはホスト名に対応する SPN に関連付けられている Active Directory ユーザーの名前を入力します。ユーザー名にドメイン名を含めないでください（たとえば、'DOMAIN\johndoe' や 'johndoe@domain' ではなく、「johndoe」と入力します）。ハイ アベイラビリティ展開の認証に使用されるサービス アカウントの作成に関する情報については、ハイ アベイラビリティ展開で Kerberos 認証を行うための Windows Active Directory におけるサービス アカウントの作成 （14 ページ）を参照してください。

b) ハイ アベイラビリティ クラスタ内のすべてのアプライアンスについて、この手順を繰り返します。

（注） アプライアンスが、ロード バランサなどの HTTP/HTTPS トラフィック分散デバイスの背後にある場合は、Active Directory 内のトラフィック分散デバイスの SPN をユーザー アカウントに関連付けて、[Kerberosハイアベイラビリティ（Kerberos High Availability）] セクションでそのユーザー アカウントのクレデンシャルを入力する必要があります。ネットワーク トポロジで、トラフィックをリダイレクトする最初のデバイスの SPN を追加する必要があります。たとえば、クライアントデバイスの送信ネットワークトラフィックがトラフィックマネージャ、ロードバランサ、および Secure Web Applianceを通過する場合、トラフィックマネージャの SPN を Active Directory のユーザーアカウントに追加し、このセクションでユーザークレデンシャルを入力する必要があります。これは、トラフィック マネージャがクライアント デバイスのトラフィックを検出する最初のデバイスであるためです。

ステップ 10 （任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザー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、「複数の NTLM レルムとドメインの使用 （32 ページ）」を参照してください。

ステップ 11 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。

ステップ 12 変更を送信し、保存します。

次のタスク

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

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 Secure Web Appliance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。このガイドの「コマンドライン インターフェイス」のトピックで `setntlmsecuritymode` を参照してください。
- Secure Web 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。
- Secure Web 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Secure Web 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。
- Secure Web Appliance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 TCP）

- 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 （13 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ーを認証できます。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ーを認証するには、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）

始める前に

アプライアンス内の番号の大きなポート（49152 ～ 65535）がファイアウォールでブロックされないことを確認します。これらのポートは、非同期グループルックアップ要求を実行する必要があります。これらのポートをブロックすると、断続的な認証エラーが発生する可能性があります。

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

ステップ 2 [レルムを追加（Add Realm）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 5 Active Directory サーバー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 サーバーが Active Directory サーバーのホスト名を解決できない場合だけです。

レルムに複数の認証サーバーを設定した場合、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 つの認証サーバーで認証を試みます。

ステップ 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 サーバーのドメイン名。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。
信頼できるドメイン ルックアップの有効化	レルムの信頼できるドメインルックアップの動作を制御するために、**[信頼できるドメインのルックアップを有効にする（Enable Trusted Domain Lookup）]** オプションが **[Active Directory アカウント（Active Directory Account）]** セクション（**[ネットワーク（Network）]** > **[認証（Authentication）]** > **[レルムの追加（Add Realm）]**）に追加されました。 このオプションは、デフォルトでは有効になっています。

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 Secure Web Applianceを含むすべてのクライアントに送信するため、既存の接続は閉じます。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。

（注） AWS に展開された Secure Web Applianceのホスト名は一意である必要があります。一意のホスト名を作成するには、ホスト名の最初の文字列を変更する必要があります。

たとえば、「mgmt」が最初の文字列としてホスト名に追加されている場合、「mgmt<*wsa_hostname*>」として変更できます。

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 ユーザーの sAMAccountName ユーザー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。

ステップ 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ー識別を有効にする（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ー名と、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ー名とその共有秘密を入力します。

ステップ 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 サーバー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すると、以下の場合に SMB 署名が有効になります。 • アプライアンスが Active Directory に接続するときにデジタル署名を配置する場合。 • 中間者攻撃を防ぐ場合。

ステップ 9 （任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザー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。

ステップ 10 変更を送信し、保存します。

LDAP 認証レルムの作成

始める前に

- 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
  - サーバーのアドレス
  - LDAP ポート
- Secure Web 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 Secure Web 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。

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

ステップ 2 [レルムを追加（Add Realm）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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 サーバーが透過的ユーザー識別で使用する Novell eDirectory をサポートしているかどうかを選択します。
LDAP サーバー（LDAP Server）	LDAP サーバーの 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 つのサーバーを指定できます。 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 サーバーが LDAP サーバー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 サーバーが Active Directory サーバーの場合は、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 サーバーの名前を入力し、ポート 3268 を使用します。ただし、グローバル カタログ サーバー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ー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ーを設定した場合、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 つの認証サーバーで認証を試みます。 AsyncOS バージョン 11.5 以降では、LDAP/NTLM（ドメインコントローラ通信）の送信元インターフェイスを指定できます。**[送信元インターフェイスの設定（Set Source Interface）]** チェックボックスをオンにし、ドロップダウンから送信元インターフェイスを選択します。
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 サーバー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 サーバーへの新しい接続を作成します。

設定	説明
ユーザー認証（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` 形式の 1 つ以上のコンポーネントから構成されます。たとえば、「`dc=companyname, dc=com`」のように入力します。 （注） このリリースにアップグレードした後で、このフィールドが空の場合、LDAP 認証の [テスト開始（Start Test）] を実行できません。 **[ユーザー名属性（User Name Attribute）]** 以下の値のいずれかを選択します。 • [uid]、[cn]、[sAMAccountName]。 ユーザー名を指定する、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。 **[ユーザーフィルタクエリー（User Filter Query）]** ユーザー フィルタ クエリーは、ユーザーのベース DN を見つける LDAP 検索フィルタです。これは、ユーザー ディレクトリがベース DN の下の階層にある場合、またはそのユーザーのベース DN のユーザー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）]。**すべてのユーザーを抽出します。 • **[カスタム（custom）]。**ユーザーの特定のグループを抽出します。

設定	説明
クエリー クレデンシャル（Query Credentials）	認証サーバーが匿名クエリーを受け入れるかどうかを選択します。 認証サーバーが匿名クエリーを受け入れる場合は、[サーバーは、匿名の質問に対応します（Server Accepts Anonymous Queries）] を選択します。 認証サーバー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 サーバー上のユーザー。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）] フィールドに入力したユーザーに関連付けられているパスフレーズ。 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ー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 サーバーが Active Directory サーバーの場合は、「DOMAIN\username」の形式でバインド DN ユーザー名を入力することもできます。

ステップ 6 （任意）グループ オブジェクトまたはユーザー 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ーをリストする 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。

グループ オブジェクト設定	説明
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ー 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。

ユーザーオブジェクト設定	説明
ユーザーオプ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）	このユーザー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]。**ユーザー 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 サーバーの場合は、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。
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。

ユーザーオブジェクト設定	説明
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ー 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。

ステップ 7 （任意）ユーザーに対する外部 LDAP 認証を設定します。

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

b) ユーザー 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。

クエリ文字列	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) ユーザーのグループ情報を取得するクエリーを入力します。

1 人のユーザーが複数の LDAP グループに属しており、それぞれユーザー 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ーに付与されます。

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。
クエリ文字列	`(&(objectClass=posixAccount)(uid={u}))`

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。
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

ステップ 8 （任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザー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、「複数の NTLM レルムとドメインの使用 （32 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。

ステップ 9 変更を送信し、保存します。

次のタスク

Kerberos 認証方式を使用する識別プロファイルを作成します。ユーザーおよびクライアント ソフトウェアの分類 を参照してください。

関連項目

- 外部認証 （17 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ーを認証できます。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ーを認証するには、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。

始める前に

以下の概念をよく理解しておいてください。

- 認証の失敗 （44 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 （49 ページ）

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

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

ステップ 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
認証サーバー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、ユーザー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 ポリシーでユーザーにゲスト アクセスを許可する場合は、この設定項目により、Web プロキシがユーザー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。 ユーザーのゲスト 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 （48 ページ）を参照してください。

設定	説明
再認証（Re-authentication） （URLカテゴリまたはユーザー セッションの制限によりエンドユーザー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ーがWebサイトからブロックされた場合に、ユーザー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 ページがユーザーに表示されます。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ーが入力すると、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ー セッションの制限によってブロックされた、認証済みユーザー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 （49 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）	認証サーバーによって再検証されるまで、ユーザー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、ユーザー名とパスフレーズ、およびユーザー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ーに連絡します。

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。

ステップ 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、ユーザー 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 （44 ページ）を参照してください。

設定	説明
HTTPS リダイレクト ポート（HTTPS Redirect Port）	HTTPS 接続を介してユーザー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ー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、ユーザー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 Secure Web 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 Secure Web 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。クライアントはプロキシ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ー エージェントでは、ユーザー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ーの脆弱性を低減できます。
ユーザー セッション制限（User Session Restrictions）	認証済みユーザーが複数の 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。 ユーザーが未認証ユーザー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。ユーザーが別のマシンでログインできない場合は、エンド ユーザー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、ユーザーがボタンをクリックして別のユーザー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ー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ーやすべてのユーザーを削除できます。

設定	説明
ヘッダー ベースの認証（Header Based Authentication）	この設定により、Active Directory のヘッダー ベース認証スキームを構成できます。 ヘッダーベース認証のキャッシュ設定： • 認証キャッシュはデフォルトで有効になっています。 • 認証キャッシュのタイムアウトは、サロゲートタイムアウトと同じです。 • キャッシュには、ユーザー名とユーザーグループが保存されます。 （注） ユーザーグループ設定を更新する場合は、認証キャッシュをクリアします。 テキスト エンコーディングとして ASCII を使用し、デフォルト設定の [バイナリのエンコーディングなし（No encoding for Binary）] を使用する [標準ヘッダー（Standard Header）] チェックボックスをオンにします。 着信グループ ヘッダーを考慮するために、[アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタム ヘッダーのグループを使用する（Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies）] チェックボックスをオンにします。カスタム ヘッダー名を設定する場合は、[カスタム ヘッダー名（Custom Header Name）] オプションを使用します。 （注） [アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタムヘッダーのグループを使用する（Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies）] チェックボックスをオンにして、X-Authenticated-Groups ヘッダーを入力しない場合は、アクセス ポリシーの照合が失敗することがあります。有効になっていない場合は、Active Directory から取得されたグループがアクセス ポリシーと照合されます。 出力でヘッダー（ユーザーおよびグループ ヘッダー）を保持するには、[出力に認証詳細を残す（Retain Authentication Details on Egress）] チェックボックスをオンにします。
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。

ステップ 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、ユーザー 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 （44 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ー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ーに認証を求める場合に発生します。

設定	説明
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、ユーザー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 Secure Web 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 Secure Web 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。クライアントはプロキシ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。
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ー エージェントでは、ユーザー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。

設定	説明
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ーの脆弱性を低減できます。
ユーザー セッション制限（User Session Restrictions）	認証済みユーザーが複数の 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。 ユーザーが未認証ユーザー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。ユーザーが別のマシンでログインできない場合は、エンド ユーザー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、ユーザーがボタンをクリックして別のユーザー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ー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ーやすべてのユーザーを削除できます。

設定	説明
ヘッダー ベースの認証（Header Based Authentication）	この設定により、Active Directory のヘッダー ベース認証スキームを構成できます。 ヘッダーベース認証のキャッシュ設定： • 認証キャッシュはデフォルトで有効になっています。 • 認証キャッシュのタイムアウトは、サロゲートタイムアウトと同じです。 • キャッシュには、ユーザー名とユーザーグループが保存されます。 （注） ユーザーグループ設定を更新する場合は、認証キャッシュをクリアします。 テキスト エンコーディングとして ASCII を使用し、デフォルト設定の [バイナリのエンコーディングなし（No encoding for Binary）] を使用する [標準ヘッダー（Standard Header）] チェックボックスをオンにします。 着信グループ ヘッダーを考慮するために、[アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタム ヘッダーのグループを使用する（Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies）] チェックボックスをオンにします。カスタム ヘッダー名を設定する場合は、[カスタム ヘッダー名（Custom Header Name）] オプションを使用します。 （注） [アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタム ヘッダーのグループを使用する（Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies）] チェックボックスをオンにして、X-Authenticated-Groups ヘッダーを入力しない場合は、アクセス ポリシーの照合が失敗することがあります。有効になっていない場合は、Active Directory から取得されたグループがアクセス ポリシーと照合されます。 出力でヘッダー（ユーザーおよびグループ ヘッダー）を保持するには、[出力に認証詳細を残す（Retain Authentication Details on Egress）] チェックボックスをオンにします。

設定	説明
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。

ステップ 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ーやプロトコルで 1 つ の ID によってユーザーを認証できます。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ー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 （16 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、ユーザー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、 Secure Web 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 レルムで NTLMSSP を使用するには、2 つの認証レルムに対して 1 つの識

別プロファイルを設定し、1 つのアイデンティティがすべてのレルムに使用されるようにします。レルム間には相互信頼関係がある必要があります。

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

始める前に

- 複数の認証レルムを作成します（認証レルム （16 ページ）を参照）。
- Secure Web 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 Secure Web 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。

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

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 変更を送信し、保存します。

認証シーケンスの削除

始める前に

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。

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

ステップ 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。

ステップ 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。

ステップ 4 変更を保存します。

認証の失敗

• 認証の失敗：異なるクレデンシャルによる再認証の許可 （49 ページ）

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、ユーザーがWebからブロックされることがあります。

- **クライアント/ユーザー 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ーの問題によって、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。**ユーザーによっては、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ーなど）。そのようなユーザーに制限付きの 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

- 問題のあるユーザー エージェントの認証のバイパス （45 ページ）
- 認証のバイパス （47 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 （47 ページ）
- 認証失敗後のゲスト アクセスの許可 （48 ページ）

問題のあるユーザー エージェントの認証のバイパス

一部のユーザーエージェントには、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。

以下のユーザー 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。

ステップ 1 指定したユーザー 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）	ユーザー 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）] > [ユーザー 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) [カスタムユーザーエージェント（Custom User Agents）] で、問題のあるユーザー エージェントの文字列を指定します。

ステップ 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	ユーザー 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。
識別プロファイル ポリシー（Identification Profile Policy）	ユーザー エージェントの AuthExempt 識別プロファイル。
詳細設定（Advanced）	なし

ステップ 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。	カスタム URL カテゴリの作成および編集
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。	ユーザーおよびクライアント ソフトウェアの分類
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

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 （45 ページ）を参照してください。

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

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

ステップ 3 [認証サーバー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。

ステップ 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 （48 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 （48 ページ）
3. （任意）ゲスト ユーザーの詳細の記録方法の設定 （49 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ー定義のポリシーがない場合、認証に失敗したユーザーは適切なポリシー 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 を使用するユーザー定義のアクセス ポリシーがない場合、認証に失敗したユーザーはグローバル アクセス ポリシーに一致します。ゲスト ユーザーをグローバル ポリシーと照合しない場合は、ゲストユーザー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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 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。

ステップ 2 ポリシー テーブル内のポリシー名をクリックします。

ステップ 3 [識別プロファイルおよびユーザー（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）。

ステップ 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。

ステップ 5 [ゲスト（認証に失敗したユーザー）（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 （48 ページ）を参照して、新しいポリシーを定義してください。

ステップ 6 変更を送信し、保存します。

ゲスト ユーザーの詳細の記録方法の設定

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

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

ステップ 3 [失敗した認証手続き（Failed Authentication Handling）] フィールドで、次に示す [ゲストユーザーのログ方法（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	ゲスト ユーザーのクライアント IP アドレスがアクセス ログに記録されます。
エンドユーザーが入力したユーザー名（User Name As Entered By End-User）	最初に認証に失敗したユーザー名がアクセス ログに記録されます。

ステップ 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、ユーザー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。ユーザー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ーを識別するだけであり、リソースへのユーザーのアクセスを許可（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、ユーザーは正常に認証されている必要があります。

- ユーザー定義のエンドユーザー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

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

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

ステップ 3 [URL カテゴリまたはユーザー セッションの制限によりエンド ユーザー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。

ステップ 4 **[送信（Submit）]** をクリックします。

識別済みユーザーの追跡

（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ー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：	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	対応	対応	対応	NA	NA	NA
IP ベース	対応	対応	対応	対応	対応	対応
Cookie ベース	対応	対応***	対応***	対応	非対応/対応**	対応***

透過的要求でサポートされる認証サロゲート

（注） ユーザーおよびクライアント ソフトウェアの分類 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：	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	対応	非対応/対応*	非対応/対応*	対応	非対応/対応*	非対応/対応*
Cookie ベース	対応	非対応/対応**	非対応/対応**	対応	非対応/対応**	非対応/対応**

*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ーを認証できません。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

再認証ユーザーの追跡

再認証の場合、より強力な権限を持つユーザー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ーの ID をキャッシュします。

- **[セッション Cookie（Session cookie）]。**特権ユーザー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）]。**特権ユーザー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）]。**特権ユーザー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ー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ー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ー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） Secure Web 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。

資格情報

認証クレデンシャルは、ユーザー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ー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ーから取得されるか、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

セッション中に 1 回ユーザーを認証した後、認証サロゲートを使用すると、新しい要求ごとにユーザー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、ユーザー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名を必ず使用してください。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 （33 ページ）、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 （48 ページ）
- 異なるクレデンシャルによる再認証の許可 （50 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） ユーザーが 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、 Secure Web 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ーに警告されます。無効な証明書に関するメッセージをユーザー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

始める前に

- 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。

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

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 変更を送信し、保存します。

次のタスク

関連項目

- 証明書の管理（Certificate Management）。

認証に関するトラブルシューティング

- NTLMSSP に起因する LDAP ユーザーの認証の失敗
- LDAP 参照に起因する LDAP 認証の失敗
- 基本認証の失敗
- エラーによりユーザーがクレデンシャルを要求される
- HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

- 認証をサポートしていない URL にアクセスできない
- クライアント要求がアップストリーム プロキシで失敗する

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。