クライアントレス SSL VPN ユーザー

- パスワードの管理 （1 ページ）
- クライアントレス SSL VPN でのシングル サインオンの使用 （3 ページ）
- ユーザー名とパスワードの要件 （22 ページ）
- セキュリティ ヒントの通知 （23 ページ）
- クライアントレス SSL VPN の機能を使用するためのリモート システムの設定 （24 ページ）

パスワードの管理

必要に応じて、パスワードの期限切れが近づいたときにエンドユーザーに警告するようにASAを設定できます。

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネルグループのパスワード管理を設定できます。

パスワード管理を設定すると、ASA はリモート ユーザーのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザーがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザーはそのパスワードを使用してログインし続けることができます。

このコマンドは、この通知をサポートしている AAA サーバーに対して有効です。

ASA のリリース 7.1 以降では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- クライアントレス SSL VPN

RADIUS サーバー（Cisco ACS など）は、認証要求を別の認証サーバーにプロキシする場合があります。ただし、ASA からは RADIUS サーバーとのみ通信しているように見えます。

始める前に

- ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。
- 認証に LDAP ディレクトリ サーバーを使用している場合、パスワード管理は Sun JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。
  - Sun：Sun ディレクトリ サーバーにアクセスするために ASA に設定されている DN が、サーバーのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
  - Microsoft：Microsoft Active Directory でパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。
- MSCHAP をサポートする一部の RADIUS サーバーは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。
- Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポートされません。
- LDAP でパスワードを変更するには、市販の LDAP サーバーごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバーに対してのみ、独自のパスワード管理ロジックを実装しています。
- RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。
- password-management コマンドはパスワードの期限が切れるまでの日数を変更するものではありません。このコマンドは、ASA がパスワードの期限が近いことについてユーザーへの警告を開始する、期限切れ前の日数を変更します。

手順

ステップ 1 一般属性モードに切り替えます。

tunnel-group general-attributes

ステップ 2 パスワードの期限切れが近づいていることをリモート ユーザーに通知します。

password-management password-expire-in-days *days*

例：

```
hostname(config-general)# password-management password-expire-in-days 90
```

- password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。
- 日数を 0 に設定すると、このコマンドはオフになります。

この例では、ASA が有効期限の 90 日前にユーザーへのパスワードの期限切れの警告を開始します。

（注）
password-expire-in-days キーワードが設定されていない場合、ASA は期限切れが近いことをユーザーに通知しませんが、ユーザーは期限が切れた後にパスワードを変更できます。

クライアントレス SSL VPN でのシングル サインオンの使用

SAML 2.0 による SSO

SSO および SAML 2.0 について

ASA は SAML 2.0 をサポートしています。これにより、クライアントレス VPN のエンドユーザーは、クレデンシャルを 1 回だけ入力して、クライアントレス VPN とプライベート ネットワーク外部のその他の SAAS アプリケーションとを切り替えることができるようになります。

たとえば、企業の顧客の場合は、SAML アイデンティティ プロバイダー(IdP）として PingIdentity をイネーブルにして、SAML 2.0 SSO 対応の Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin、または Dropbox のアカウントを持ちます。サービス プロバイダー（SP）として 2.0 SAML SSO をサポートするように ASA を設定すると、エンドユーザーは一度サインインするだけで、クライアントレス VPN などのあらゆるサービスにアクセスできるようになります。

さらに、AnyConnect 4.4 クライアントが SAML 2.0 を使用して SAAS ベースのアプリケーションにアクセスできるように、AnyConnect SAML サポートが追加されました。AnyConnect 4.6 では、組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わります。組み込みブラウザを搭載した新しい拡張バージョンを使用するには、AnyConnect 4.6（またはそれ以降）および ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）へのアップグレードが必要です。

トンネル グループやデフォルト トンネル グループなどの認証方式として SAML が設定されている場合、ASA は SP に対応します。クライアントレス VPN のエンドユーザーは、イネーブルになっている ASA または SAML IdP にアクセスして、シングル サインオンを開始します。以下では、これらの各シナリオについて説明します。

SAML SP によって開始される SSO

エンドユーザーがクライアントレス VPN を使用して ASA アクセスし、ログインを開始した場合、サインオン動作は次のように進行します。

1. クライアントレス VPN のエンドユーザーが SAML 対応のトンネル グループにアクセスするか、またはグループを選択すると、そのユーザーは認証のために SAML idP にリダイレクトされます。グループ URL に直接アクセスしない限り、ユーザーは入力を要求されます。直接アクセスした場合、リダイレクトは行われません。

   ASA は、ブラウザによって SAML IdP にリダイレクトされる SAML 認証要求を生成します。

2. IdP がエンドユーザーのクレデンシャルを確認し、エンドユーザーがログインします。入力されたクレデンシャルは IdP の認証設定に合致していなければなりません。

3. IdP の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

SAML IdP によって開始される SSL

エンドユーザーが IdP にアクセスしてログインを開始した場合、サインオン動作は次のように進行します。

1. エンドユーザーが IdP にアクセスします。IdP は、独自の認証設定に従ってエンドユーザーのクレデンシャルを確認します。エンドユーザーはクレデンシャルを入力し、IdP にログインします。
2. 一般的には、エンドユーザーは、IdP で設定された SAML 対応サービスのリストを取得します。エンドユーザーが ASA を選択します。

3. SAML の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

信頼の輪

ASA と SAML アイデンティティ プロバイダーとの信頼関係は、設定されている証明書（ASA トラストポイント）によって確立されます。

エンドユーザーと SAML アイデンティティ プロバイダーとの信頼関係は、IdP に設定されている認証によって確立されます。

SAML のタイムアウト

SAML アサーションには、次のような NotBefore と NotOnOrAfter があります：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

ASA で設定されている SAML のタイムアウトと NotBefore の合計が NotOnOrAfter よりも早い場合は、そのタイムアウトが NotOnOrAfter よりも優先されます。NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。

タイムアウト後にアサーションによって再利用されないように、タイムアウトにはごく短い時間を設定してください。SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。

プライベート ネットワークでのサポート

SAML 2.0 ベースのサービス プロバイダー IdP は、プライベート ネットワークでサポートされます。SAML IdP がプライベート クラウドに展開されると、ASA およびその他の SAML 対応サービスはピアの位置になり、すべてプライベート ネットワーク内になります。ASA をユーザーとサービス間のゲートウェイとして、IdP の認証は制限された匿名の webvpn セッションで処理され、IdP とユーザー間のすべてのトラフィックは変換されます。ユーザーがログインすると、ASA は対応する属性のセッションを修正し、IdP セッションを保存します。その後は、クレデンシャルを再度入力することなくプライベート ネットワークのサービス プロバイダーを使用できます。

SAML IdP *NameID* 属性は、ユーザーのユーザー名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。

（注） プライベート ネットワークとパブリック ネットワーク間で認証情報を交換することはできません。内部および外部の両方のサービス プロバイダーに同じ IdP を使用する場合、個別に認証する必要があります。内部専用の IdP を外部サービスで使用することはできません。外部専用の IdP は、プライベート ネットワーク内のサービス プロバイダーでは使用できません。

SAML 2.0 に関する注意事項と制約事項

- ASA は、SAML 認証用に次のシグニチャをサポートしています。
  - RSA および HMAC を使用する SHA1
  - RSA および HMAC を使用する SHA2
- ASA は、すべての SAML IdP でサポートされる SAML 2.0 Redirect-POST バインディングをサポートしています。
- ASA は SAML SP としてのみ機能します。ゲートウェイ モードやピア モードでアイデンティティ プロバイダーとして動作することはできません。
- SAML 2.0 SSO は、内部 SAML IdP と SP をサポートしておらず、プライベート ネットワーク外部の SAML IdP と SP のみをサポートしています。
- この SP SAML SSO 機能は相互排他認証方式です。この方式は、AAA や証明書と併用できません。
- ユーザー名/パスワード認証、証明書認証、および KCD に基づく機能はサポートされません。たとえば、ユーザー名/パスワードの事前フィルタリング機能、フォーム ベースの自動サインオン、マクロ置換ベースの自動サインオン、KCD SSO などです。

- DAP 評価で使用可能な SAML 認証属性は（AAA サーバーから RADIUS 認証応答で送信される RADIUS 属性と同様に）サポートされていません。ASA は、DAP ポリシーで SAML 対応トンネルグループをサポートします。ただし、ユーザー名属性は SAML ID プロバイダーによってマスクされるため、SAML 認証の使用中はユーザー名属性を確認できません。
- 既存のクライアントレス VPN のタイムアウト設定は、まだ SAML セッションに適用されます。
- 認証アサーションが適切に処理され、タイムアウトが適切に機能するように、ASA の管理者は、ASA と SAML IdP とのクロック同期を確保する必要があります。
- ASA の管理者は、次の点を考慮して、ASA と IdP の両方で有効な署名証明書を保持する責任があります。
  - ASA に IdP を設定する際には、IdP の署名証明書が必須です。
  - ASA は、IdP から受け取った署名証明書に対して失効チェックを行いません。
- SAML アサーションには、NotBefore と NotOnOrAfter 条件があります。ASA SAML に設定されている**タイムアウト**と、これらの条件との相関関係は次のとおりです。
  - NotBefore とタイムアウトの合計が NotOnOrAfter よりも早い場合は、タイムアウトが NotOnOrAfter に優先します。
  - NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。
  - NotBefore 属性が存在しない場合、ASA はログイン要求を拒否します。NotOnOrAfter 属性が存在せず、SAML タイムアウトが設定されていない場合、ASA はログイン要求を拒否します。
- 二要素認証（プッシュ、コード、パスワード）のチャレンジ/応答中に FQDN が変更されるため、ASA がクライアントとのプロキシを強制的に認証する、内部 SAML を使用した展開では ASA は Duo と連携しません。
- 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。
- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバを IdP NTP サーバと同期する必要があります。

- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- 内部 IdP を使用してログインした後に SSO で内部サーバーにアクセスすることはできません。
- SAML IdP NameID 属性は、ユーザーのユーザー名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。

SAML 2.0 アイデンティティ プロバイダー（IdP）の設定

始める前に

SAML（IdP）プロバイダーのサインイン URL とサインアウト URL を取得します。URL はプロバイダーの Web サイトから取得できます。また、プロバイダーがメタデータ ファイルで情報を提供していることもあります。

手順

ステップ 1 webvpn コンフィギュレーション モードで SAML アイデンティティ プロバイダーを作成し、webvpn で saml-idp サブモードを開始します。

[**no**] **saml idp** *idp-entityID*

idp-entityID：SAML IdP の entityID には 4 ~ 256 文字を指定します。

SAML IdP を削除するには、このコマンドの **no** 形式を使用します。

ステップ 2 IdP URL を設定します。

url [**sign-in** | **sign-out**] *value*

value：IdP にサインインするための URL、または IdP からサインアウトするときにリダイレクトされる URL です。**sign-in** URL は必須ですが、**sign-out** URL はオプションです。url の値には 4 ～ 500 文字を指定します。

ステップ 3 （任意） クライアントレス VPN のベース URL を設定します。

base-url *URL*

この URL は、エンドユーザーを ASA にリダイレクトするために、サードパーティ製 IdP に提供されます。

base-url が設定されている場合、その URL は **show saml metadata** の AssertionConsumerService と SingleLogoutService 属性のベース URL として使用されます。

base-url が設定されていない場合、URL は ASA のホスト名とドメイン名から決定されます。たとえば、ホスト名が `ssl-vpn`、ドメイン名が `cisco.com` の場合は、`https://ssl-vpn.cisco.com` が使用されます。

base-url もホスト名/ドメイン名も設定されていない場合は、**show saml metadata** を入力するとエラーが発生します。

ステップ 4 IdP と SP（ASA）間のトラストポイントを設定します。

trustpoint [**idp** | **sp**] *trustpoint-name*

idp：ASA が SAML アサーションを検証するための IdP 証明書を含むトラストポイントを指定します。

sp ：IdP が ASA（SP）の署名や暗号化 SAML アサーションを検証するための ASA（SP）証明書を含むトラストポイントを指定します。

trustpoint-name：設定されているトラストポイントを指定します。

ステップ 5 （任意） SAML タイムアウトを設定します。

timeout assertion *timeout-in-seconds*

指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。

指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。

（注）
既存の SAML IdP が設定済みのトンネル グループの場合、webvpn での saml idp CLI に対するすべての変更は、SAML がその特定のトンネル グループに再度有効にされたときにのみトンネル グループに適用されます。タイムアウトを設定すると、更新されたタイムアウトはトンネル グループの webvpn 属性の saml アイデンティティ プロバイダー CLI 再発行後にのみ有効になります。

ステップ 6 （任意） SAML 要求の署名をイネーブルまたはディセーブル（デフォルト設定）にします。

signature <value>

（注）
SSO 2.5.1 へのアップグレードに伴い、デフォルトの署名方法は SHA1 から SHA256 に変更します。*value* に rsa-sha1、rsa-sha256、rsa-sha384、または rsa-sha512 を入力すると、希望する署名方法のオプションを設定できます。

ステップ 7 （オプション）IdP が内部ネットワークであることを特定するフラグを設定するには、**internal** コマンドを使用します。ASA はゲートウェイ モードで機能するようになります。

ステップ 8 **show webvpn saml idp** を使用してコンフィギュレーションを表示します。

ステップ 9 SAML 認証要求が発生したときに、以前のセキュリティ コンテキストに依存するのではなくアイデンティティ プロバイダーが直接認証するようにするには、**force re-authentication** を使用します。この設定はデフォルトなので、ディセーブルにする場合は **no force re-authentication** を使用します。

例

次の例では、salesforce_idp という名前の IdP を設定し、事前設定されたトラストポイントを使用します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint  sp asa_trustpoint
```

次の Web ページには、Onelogin の URL の取得方法について例が示されています。

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

次の Web ページには、メタデータを使用して Onelogin から URL を検索する方法について、例が示されています。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

次のタスク

SAML 2.0 サービス プロバイダー（SP）としての ASA の設定 （9 ページ） の説明に従って、SAML 認証を接続プロファイルに適用します。

SAML 2.0 サービス プロバイダー（SP）としての ASA の設定

特定のトンネル グループを SAML SP として設定するには、次の手順を実行します。

（注） AnyConnect 4.4 または 4.5 で SAML 認証を使用していて、ASA バージョン 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）（リリース日付：2018 年 4 月 18 日）を展開している場合、SAML のデフォルトの動作は、AnyConnect 4.4 および 4.5 でサポートされていない組み込みブラウザになります。したがって、AnyConnect 4.4 および 4.5 クライアントが外部（ネイティブ）ブラウザを使用して、SAML で認証するには、トンネル グループ設定で **saml external-browser** コマンドを使用する必要があります。

saml external-browser コマンドは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このコマンド自体がサポートされなくなります。

始める前に

事前に IdP を設定しておく必要があります。SAML 2.0 アイデンティティ プロバイダー（IdP）の設定 （7 ページ）を参照してください。

手順

ステップ 1 tunnel-group webvpn サブモードで、saml identify-provider コマンドを使用して IdP を割り当てます。

saml identity-provider *idp-entityID*

idp-entityID：設定されている既存の IdP のいずれかを指定します。

SAML SP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 2 SAML 認証方式を有効化します。

authentication saml

例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

SAML 2.0 と Onelogin の例

以下の例を実行する際は、Onelogin の情報とネーミングの代わりにサードパーティ製の SAML 2.0 IdP を使用してください。

1. IdP と ASA（SP）間での時刻の同期を設定します。

   ```
   ciscoasa(config)# ntp server 209.244.0.4
   ```

2. サードパーティ製 IdP で指定されている手順に従って、IdP から IdP の SAML メタデータを取得します。

3. トラストポイントに IdP の署名証明書をインポートします。

   ```
   ciscoasa(config)# crypto ca trustpoint onelogin
   ciscoasa(config-ca-trustpoint)# enrollment terminal
   ciscoasa(config-ca-trustpoint)# no ca-check
   ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
   Enter the base 64 encoded CA certificate.
   End with the word "quit" on a line by itself
   quit
   INFO: Certificate has the following attributes:
   ```

```
Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. トラストポイントに SP（ASA）署名 PKCS12 をインポートします

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. SAML IdP を追加します。

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. saml-idp サブモードで属性を設定します。

   IdP サインイン URL とサインアウト URL を設定します。

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   IdP トラストポイントと SP トラストポイントを設定します

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   クライアントレス VPN ベース URL、SAML 要求の署名、および SAML アサーション タイムアウトを設定します。

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. トンネル グループの IdP を設定し、SAML 認証をイネーブルにします。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. ASA の SAML SP メタデータを表示します。

   ASA の SAML SP メタデータは、`https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin` から取得できます。この URL の `cloud_idp_onelogin` は、トンネル グループ名です。

9. サードパーティ製 IdP で指定されている手順に従って、その IdP で SAML SP を設定します。

SAML 2.0 のトラブルシューティング

SAML 2.0 の動作をデバッグするには、**debug webvpn saml***value* を使用します。*value* に応じて次の SAML メッセージが表示されます。

- 8：エラー
- 16：警告およびエラー
- 128 または 255：デバッグ、警告、およびエラー

HTTP Basic 認証または NTLM 認証による SSO の設定

この項では、HTTP Basic 認証または NTLM 認証を使用するシングル サインオンについて説明します。この方法のいずれかまたは両方を使用して SSO を実装するように ASA を設定することができます。**auto-sign-on** コマンドを使用すると、ASA はクライアントレス SSL VPN ユーザーのログインクレデンシャル（ユーザー名およびパスワード）を内部サーバーに自動的に渡すように設定されます。複数の **auto-sign-on** コマンドを入力できます。ASA は複数のコマンドを入力順に処理します（先に入力されたコマンドを優先）。IP アドレスと IP マスク、または URI マスクのいずれかを使用してログインのクレデンシャルを受信するようにサーバーに指定します。

クライアントレス SSL VPN コンフィギュレーション、クライアントレス SSL VPN グループ ポリシー モード、またはクライアントレス SSL VPN ユーザー名モードの 3 つのモードのいずれかで、**auto-sign-on** コマンドを使用します。ユーザー名はグループより優先され、グループはグローバルより優先されます。認証に必要な範囲のモードを選択します。

モード	スコープ
webvpn configuration	クライアントレス SSL VPN ユーザー全員に対するグローバルな範囲
webvpn group-policy configuration	グループ ポリシーで定義されるクライアントレス SSL VPN ユーザーのサブセット
webvpn username configuration	個々のクライアントレス SSL VPN ユーザー

例

- NTLM 認証を使用し、10.1.1.0 ～ 10.1.1.255 の IP アドレス範囲に存在するサーバーに対するすべてのクライアントレス SSL VPN ユーザーからのアクセスに auto-sign-on を設定します。

```
hostname(config-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type
ntlm
```

- 基本の HTTP 認証を使用するすべてのクライアントレス SSL VPN ユーザーに対し、URI マスク https://*.example.com/* で定義されたサーバーへのアクセスに auto-sign-on を設定します。

```
hostname(config-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type
```

- 基本認証または NTLM 認証を使用して、ExamplePolicy グループ ポリシーと関連付けられているクライアントレス SSL VPN セッションに対し、URI マスクで定義されたサーバーへのアクセスに auto-sign-on を設定します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type
 all
```

- *Anyuser* というユーザーが IP アドレス範囲 10.1.1.0 ～ 10.1.1.255 のサーバーに、HTTP 基本認証によって自動サインオンするように設定します。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0
auth-type basic
```

- 特定のポートで自動サインオンを設定し、認証のレルムを設定します。

```
smart-tunnel auto-sign-on host-list [use-domain] [realm realm string] [port port
num] [host host mask | ip address subnet mask]
```

HTTP Form プロトコルによる SSO の設定

この項では、SSO における HTTP Form プロトコルの使用について説明します。HTTP Form プロトコルは、SSO 認証を実行するための手段で、AAA 方式としても使用できます。このプロトコルは、クライアントレス SSL VPN のユーザーおよび認証を行う Web サーバーの間で認証情報を交換するセキュアな方法を提供します。RADIUS サーバーや LDAP サーバーなどの他の AAA サーバーと組み合わせて使用することができます。

ASA は、ここでも認証 Web サーバーに対するクライアントレス SSL VPN ユーザーのプロキシとして機能しますが、この場合は、要求に対して HTTP Form プロトコルと POST 方式を使用します。フォーム データを送受信するように ASA を設定する必要があります。

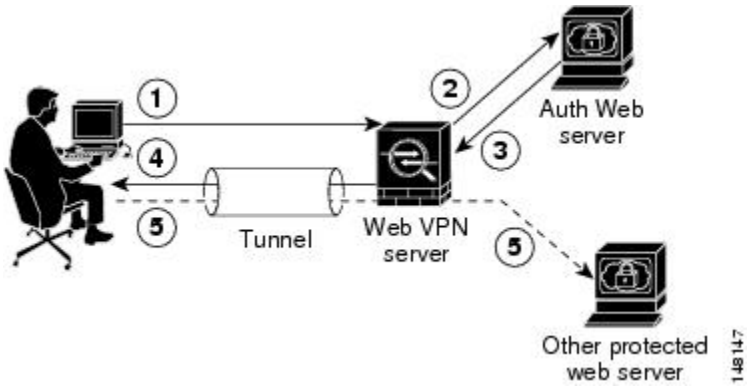
HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

これは、一般的なプロトコルとして、認証に使用する Web サーバー アプリケーションの次の条件に一致する場合にだけ適用できます。

- 認証クッキーは、正常な要求に対して設定され、未許可のログインに対して設定されないようにする必要があります。この場合、ASA は、失敗した認証から正常な要求を識別することはできません。

次の図は、後述する SSO 認証手順を示しています。

図 *1 : HTTP Form* を使用した *SSO* 認証



1. クライアントレス SSL VPN のユーザーは、最初にユーザー名とパスワードを入力して ASA 上のクライアントレス SSL VPN サーバーにログオンします。
2. ユーザーのプロキシとして動作するクライアントレス SSL VPN サーバーは、このフォーム データ（ユーザー名およびパスワード）を、POST 認証要求を使用して認証 Web サーバーに転送します。
3. 認証 Web サーバーがユーザーのデータを承認した場合は、認証クッキーをユーザーの代行で保存していたクライアントレス SSL VPN サーバーに戻します。
4. クライアントレス SSL VPN サーバーはユーザーまでのトンネルを確立します。
5. これでユーザーは、ユーザー名やパスワードを再入力しなくても、保護された SSO 環境内の他の Web サイトにアクセスできるようになります。

ユーザー名やパスワードなどの POST データを ASA によって含めるようにフォーム パラメータを設定しても、Web サーバーに必要な非表示のパラメータが追加されたことに、当初、ユーザーは気づかない可能性があります。認証アプリケーションの中には、ユーザー側に表示されず、ユーザーが入力することもない非表示データを要求するものもあります。ただし、ASA を仲介役のプロキシとして使用せずに、ブラウザから Web サーバーに直接認証要求を行うことによって、認証 Web サーバーに必要な非表示のパラメータを見つけることができます。HTTP ヘッダー アナライザを使用して Web サーバーの応答を分析すると、非表示パラメータが次のような形式で表示されます。

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

非表示パラメータには、必須のパラメータとオプションのパラメータとがあります。Web サーバーが非表示パラメータのデータを要求すると、Web サーバーはそのデータを省略するすべての認証 POST 要求を拒否します。ヘッダーアナライザは、非表示パラメータが必須かオプションかについては伝えないため、必須のパラメータが判別できるまではすべての非表示パラメータを含めておくことをお勧めします。

HTTP Form プロトコルを使用した SSO を設定するには、次を実行する必要があります。

- フォーム データ（**action-uri**）を受信して処理するために、認証 Web サーバーにユニフォーム リソース識別子を設定する。
- ユーザー名パラメータ（**user-parameter**）を設定する。

- ユーザー パスワード パラメータ（**password-parameter**）を設定する。

認証 Web サーバーの要件によっては次のタスクが必要になる場合もあります。

- 認証Webサーバーがログイン前のクッキー交換を必要とする場合は、開始URL（**start-url**）を設定する。
- 認証Webサーバーが必要とするあらゆる非表示認証パラメータ（**hidden-parameter**）を設定する。
- 認証Webサーバーによって設定される認証クッキーの名前（**auth-cookie-name**）を設定する。

手順

ステップ 1 AAA サーバー ホスト コンフィギュレーション モードに切り替えます。

aaa-server-host

ステップ 2 認証 Web サーバーが要求する場合は、認証 Web サーバーから事前ログイン クッキーを取得するための URL を指定します。

start-url

例：

```
hostname(config)# aaa-server testgrp1 protocol http-form
hostname(config)# aaa-server testgrp1 host 10.0.0.2
hostname(config-aaa-server-host)# start-url http://example.com/east/Area.do?Page-Grp1
```

この例では、http://example.com/east/Area.do?Page-Grp1 の URL 認証 Web サーバーを、IP アドレス 10.0.0.2 の testgrp1 サーバー グループに指定します。

ステップ 3 認証 Web サーバー上の認証プログラムの URI を指定します。

action-uri

例：

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433
&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNA
ME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2F
auth.example.com
```

この action URI を指定するには、次のコマンドを入力します。

```
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
```

```
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
```

1 つの URI を連続する複数行にわたって入力することができます。1 行あたりの最大文字数は 255 です。URI 全体の最大文字数は 2048 です。

アクション URI にホスト名とプロトコルを含める必要があります。この例では、これらは http://www.example.com の URI の最初に表示されます。

ステップ 4 HTTP POST 要求の userid ユーザー名パラメータを設定します。

user-parameter

例：

```
hostname(config-aaa-server-host)# user-parameter userid
```

ステップ 5 HTTP POST 要求の user_password ユーザー パスワード パラメータを設定します。

password-parameter

例：

```
hostname(config-aaa-server-host)# password-parameter user_password
```

ステップ 6 認証 Web サーバーと交換するための非表示パラメータを指定します。

hidden-parameter

例：

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
```

この例では、POST 要求から抜粋した非表示パラメータの例を示します。この非表示パラメータには、間を & で区切った 4 つの Form エントリとその値が含まれています。エントリとその値は次のとおりです。

- SMENC、値は ISO-8859-1。
- SMLOCALE、値は US-EN。
- target、値は https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do。
- %3FEMCOPageCode%3DENG。
- smauthreason、値は 0。

ステップ 7 認証クッキーの名前を指定します。

auth-cookie-name *cookie-name*

例：

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
```

この例では、SsoAuthCookie の認証クッキー名を指定します。

ステップ 8 トンネル グループ一般属性コンフィギュレーション モードに切り替えます。

tunnel-group general-attributes

ステップ 9 前の手順で設定された SSO サーバーを使用するためのトンネル グループを設定します。

authentication-server-group

例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#authentication-server-group testgrp1
```

この例では、/testgrp1/ という名前の SSO サーバーを使用するための、/testgroup/ という名前のトンネル グループを設定します。

ステップ 10 AAA サーバー ホスト コンフィギュレーション モードに切り替えます。

aaa-server-host

ステップ 11 認証クッキーの名前を指定します。

auth-cookie-name *cookie-name*

例：

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
```

この例では、SsoAuthCookie の認証クッキー名を指定します。

ステップ 12 トンネル グループ一般属性モードに切り替えます。

tunnel-group general-attributes

ステップ 13 前の手順で設定された SSO サーバーを使用するためのトンネル グループを設定します。

authentication-server-group group

例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#authentication-server-group testgrp1
```

この例では、/testgrp1/ という名前の SSO サーバーを使用するための、/testgroup/ という名前のトンネル グループを設定します。

HTTP Form データの収集

この項では、必要な HTTP Form データを検出および収集する手順を示します。認証 Web サーバーが要求するパラメータが何かわからない場合は、認証交換を分析するとパラメータ データを収集することができます。

始める前に

これらの手順では、ブラウザと HTTP ヘッダー アナライザが必要です。

手順

ステップ 1 ブラウザと HTTP ヘッダー アナライザを起動し、ASA を経由せずに、Web サーバーのログイン ページに直接接続します。

ステップ 2 Web サーバーのログイン ページがユーザーのブラウザにロードされてから、ログイン シーケンスを検証して交換時にクッキーが設定されているかどうか判別します。Web サーバーによってログイン ページにクッキーがロードされている場合は、このログイン ページの URL を *start-URL* として設定します。

ステップ 3 Web サーバーにログオンするためのユーザー名とパスワードを入力して、Enter を押します。この動作によって、ユーザーが検証する認証 POST 要求が HTTP ヘッダー アナライザを使用して生成されます。

次に、ホストの HTTP ヘッダーおよび本文が記載された POST 要求の例を示します。

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c
-ac05-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk
2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.c
om%2Femco%2Fmyemco%2FHTTP/1.1

Host: www.example.com

(BODY)

SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https
%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

ステップ 4 POST 要求を検証してプロトコル、ホストをコピーし、URL を入力して action-uri パラメータを設定します。

ステップ 5 POST 要求の本文を検証して、次の情報をコピーします。

a) ユーザー名パラメータ。上記の例では、このパラメータは *USERID* で、値 *anyuser* ではありません。

b) パスワード パラメータ。上記の例では、このパラメータは *USER_PASSWORD* です。

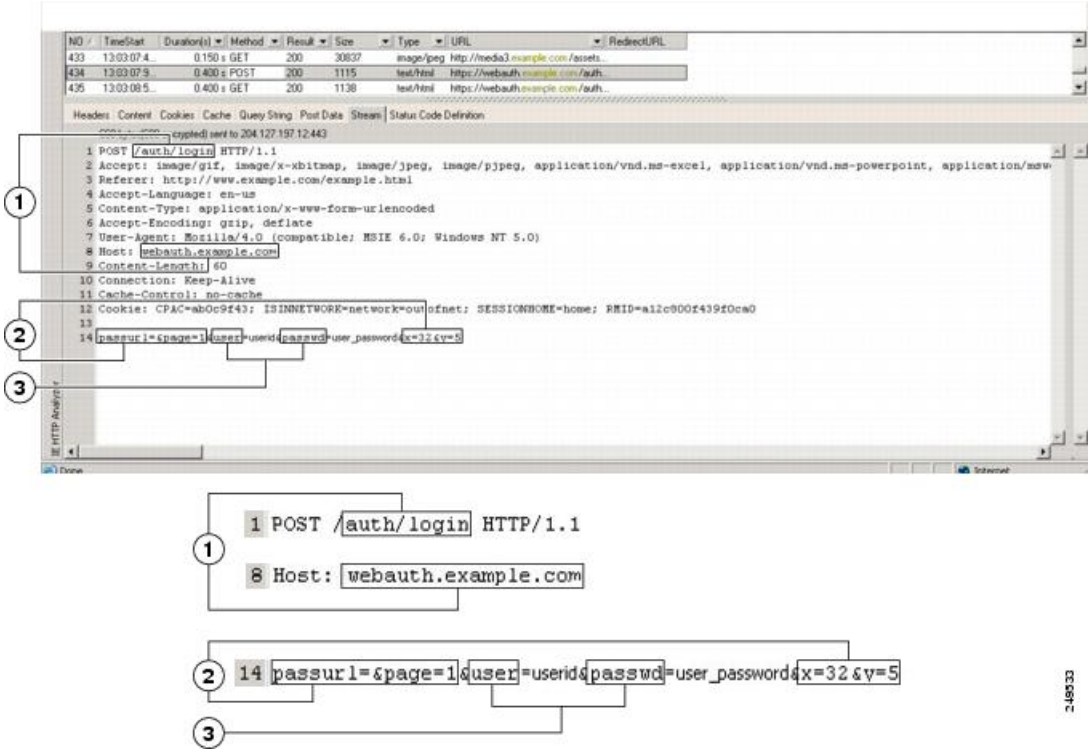
c) 非表示パラメータ。

このパラメータは、POST 本文からユーザー名パラメータとパスワード パラメータを除くすべてです。前の例の非表示パラメータは次のとおりです。

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2
Femco%2Fmyemco%2F&smauthreason=0
```

次の図は、HTTP アナライザの出力例におけるアクション URI、非表示、ユーザー名、パスワードの各種パラメータを強調して示しています。これは一例にすぎません。出力は Web サイトに応じて大きく異なります。

図 *2*: アクション *URI*、非表示、ユーザー名、パスワードの各種パラメータ



1	action URI パラメータ
2	非表示パラメータ
3	ユーザー名パラメータとパスワード パラメータ

ステップ 6 Web サーバーへのログオンに成功したら、HTTP ヘッダーアナライザを使用してサーバーの応答を検証し、サーバーによってブラウザに設定されたセッションクッキーの名前を探します。これは、**auth-cookie-name** パラメータです。

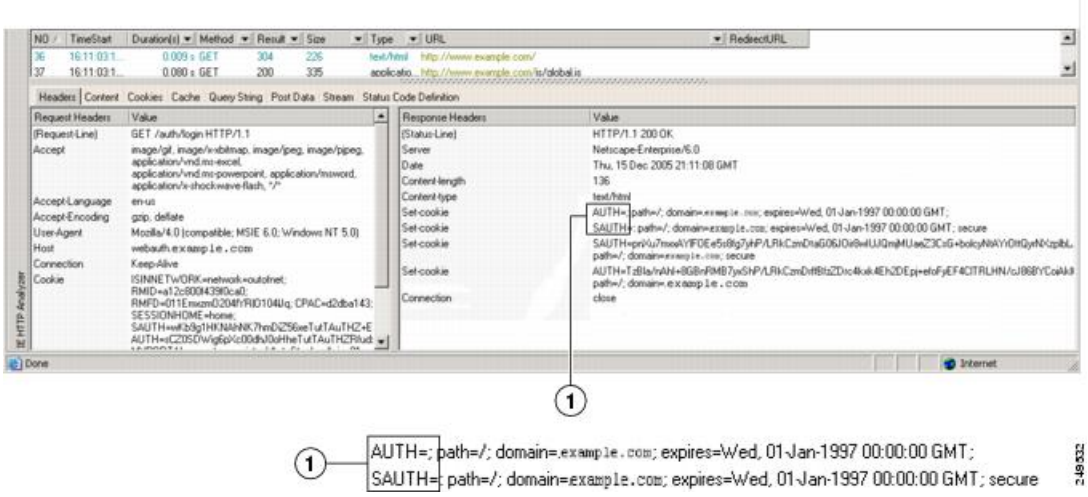
次のサーバー応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZ
PbHIHtWLDKTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0d
SSOSepWvnsCb7IFxCw+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv
+yQzxwfEz2cl7Ef5iMr8LgGcDK7qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGw
pS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0
```

k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9
hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYzVu7EmzMQ+UefYxh4cF2gYD8
RZL2RwmP9JV5148I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41Lx
xaUDhbcmkoHT9ImzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+
0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdah
uq5SxbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdR
Ka5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzu
Q6wApzEp9CUoG8/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/
emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.exa
mple.com;Path=/

次の図は、HTTP アナライザの出力における許可クッキーの例を示しています。これは一例にすぎません。出力は Web サイトに応じて大きく異なります。

図 *3: HTTP* アナライザの出力例における認可クッキー



1	認可クッキー

ステップ 7 場合によっては、認証の成否にかかわらず同じクッキーがサーバーによって設定される可能性があり、このようなクッキーは、SSO の目的上、認められません。クッキーが異なっていることを確認するには、無効なログイン クレデンシャルを使用してステップ 1 ～ 6 を繰り返し、「失敗した」クッキーと「成功した」クッキーを比較します。これで、HTTP Form プロトコルによる SSO を ASA に設定するために必要なパラメータ データを用意できました。

プラグインの SSO の設定

プラグインは、シングルサインオン（SSO）をサポートします。プラグインは、クライアントレス SSL VPN セッションを認証するときに入力したクレデンシャルと同じクレデンシャル（ユーザー名とパスワード）を使用します。プラグインはマクロ置換をサポートしないため、内部ドメイン パスワードなどのさまざまなフィールドや、RADIUS または LDAP サーバーの属性で SSO を実行するオプションはありません。

プラグインに対して SSO サポートを設定するには、プラグインをインストールし、サーバーへのリンクを表示するためのブックマーク エントリを追加します。また、csco_sso=1 パラメー

タを使用してSSOサポートを指定します。次に、SSO用にイネーブルにするプラグインのブックマークの例を示します。

```
ssh://ssh-server/?cisco_sso=1
rdp://rdp-server/?Parameter1=value&Parameter2=value&csco_sso=1
```

マクロ置換による SSO の設定

ここでは、SSO のマクロ置換の使用について説明します。マクロ置換を使用して SSO を設定することで、ブックマークに特定の変数を挿入して動的な値に置換できます。

（注） スマート トンネル ブックマークでは、自動サインオンはサポートされていますが変数置換はサポートされていません。たとえば、スマート トンネル向けに設定された SharePoint ブックマークは、アプリケーションにログオンするために、クライアントレス SSL VPN にログオンするために使用するクレデンシャルと同じユーザー名とパスワードを使用します。（このSSO機能は、クライアントレス VPN にのみ適用され、AnyConnect には適用されません。）変数置換および自動サインオンは同時に、または別々に使用できます。

一部の Web ページでの自動サインオンに、マクロ置換を含むブックマークを使用できるようになりました。以前の POST プラグイン アプローチは、管理者がサインオン マクロを含む POST ブックマークを指定し、POST 要求のポストの前にロードするキックオフ ページを受信できるようにするために作成されました。このPOSTプラグインアプローチでは、クッキーまたはその他のヘッダー項目の存在を必要とする要求は排除されました。現在は、管理者は事前ロード ページおよびURL を決定し、これによってポスト ログイン要求の送信場所が指定されます。事前ロードページによって、エンドポイントブラウザは、クレデンシャルを含むPOST要求を使用するのではなく、Web サーバーまたは Web アプリケーションに送信される特定の情報を取得できます。

次に、ブックマーク内の置換およびフォームベースの HTTP POST 操作が可能な変数（またはマクロ）を示します。

- CSCO_WEBVPN_USERNAME：ユーザーのログイン ID
- CSCO_WEBVPN_PASSWORD：ユーザーのログイン パスワード
- CSCO_WEBVPN_INTERNAL_PASSWORD：ユーザーの内部（または、ドメイン）パスワードこのキャッシュ済みクレデンシャルは、AAA サーバーに対して認証されません。この値を入力すると、セキュリティ アプライアンスは、パスワードまたはプライマリ パスワードの値ではなく、この値を自動サインオンのパスワードとして使用します。

（注） 上記の 3 つの変数は、GET ベースの HTTP（S）ブックマークでは使用できません。これらの値を使用できるのは、POST ベースの HTTP（S）および CIFS ブックマークだけです。

- CSCO_WEBVPN_CONNECTION_PROFILE：ユーザーのログイン グループ ドロップダウン（接続プロファイル エイリアス）
- CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性（VSA）によって設定。LDAP から ldap-attribute-map コマンドをマッピングしている場合、このマクロの Cisco 属性である WebVPN-Macro-Substitution-Value1 を使用します。Active Directory での LDAP 属性マッピングの例については、次の URL を参照してください。http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118

  RADIUS による CSCO_WEBVPN_MACRO1 のマクロ置換は、VSA#223 によって行われます。

表 1 : VSA#223

WebVPN-Macro-Value1	Y	223	文字列	シングル	無制限
WebVPN-Macro-Value2	Y	224	文字列	シングル	無制限

特定の DAP またはグループ ポリシーについて、https://CSCO_WEBVPN_MACRO1 や https://CSCO_WEBVPN_MACRO2 のようにすると、www.cisco.com/email などの値が、クライアントレス SSL VPN ポータルのブックマークに動的に読み込まれます。

- CSCO_WEBVPN_MACRO2：RADIUS-LDAP のベンダー固有属性（VSA）によって設定されます。LDAP から ldap-attribute-map コマンドをマッピングしている場合、このマクロの Cisco 属性である WebVPN-Macro-Substitution-Value2 を使用します。Active Directory での LDAP 属性マッピングの例については、次の URL を参照してください。http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118

  RADIUS による CSCO_WEBVPN_MACRO2 のマクロ置換は、VSA#224 によって行われます。

クライアントレス SSL VPN が（ブックマークの形式または POST 形式の）エンドユーザーの要求内にあるこれらの 6 つの文字列のいずれかを認識するたびに、文字列がユーザー指定の値に置き換えられ、この要求がリモート サーバーに渡されます。

ユーザー名とパスワードのルックアップが ASA で失敗した場合は、空の文字列で置き換えられ、動作は自動サインインが不可の場合の状態に戻されます。

ユーザー名とパスワードの要件

ネットワークによっては、リモートセッション中にユーザーが、コンピュータ、インターネットサービスプロバイダー、クライアントレス SSL VPN、メールサーバー、ファイルサーバー、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザーはさまざまなコンテキストで認証を行うために、固有のユーザー名、パスワード、PIN などさまざまな情報が要求される場合があります。次の表に、クライアントレス SSL VPN ユーザーが理解しておく必要のあるユーザー名とパスワードのタイプを示します。

ログイン ユーザー名/ パスワードのタイプ		入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
Internet Service Provider：インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN の起動
File Server	リモート ファイル サーバーへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバーにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバーへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバー	クライアントレス SSL VPN 経由によるリモート メール サーバーへのアクセス	電子メール メッセージの送受信

セキュリティ ヒントの通知

ユーザーはいつでもツールバーの [Logout] アイコンをクリックして、クライアントレス SSL VPN セッションを閉じることができます（ブラウザ ウィンドウを閉じてもセッションは閉じません）。

クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザーに通知してください。したがって、ユーザーが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバーまでの通信は暗号化されていないため、プライベートではありません。

クライアントレス SSL VPN の機能を使用するためのリモート システムの設定

この項では、クライアントレス SSL VPN を使用するようにリモート システムを設定する方法について説明します。

- クライアントレス SSL VPN について （24 ページ）
- クライアントレス SSL VPN の前提条件 （25 ページ）
- クライアントレス SSL VPN フローティング ツールバーの使用 （25 ページ）
- Web のブラウズ （25 ページ）
- ネットワークのブラウズ（ファイル管理） （26 ページ）
- ポート転送の使用 （27 ページ）
- ポート転送を介した電子メールの使用 （29 ページ）
- Web アクセスを介した電子メールの使用 （29 ページ）
- 電子メール プロキシを介した電子メールの使用 （30 ページ）
- スマート トンネルの使用 （30 ページ）

ユーザー アカウントを別々に設定でき、各ユーザーは異なるクライアントレス SSL VPN の機能を使用できます。

クライアントレス SSL VPN について

次のようなサポートされている接続を使用して、インターネットに接続できます。

- 家庭の DSL、ケーブル、ダイヤルアップ。
- 公共のキオスク。
- ホテルのホットスポット。
- 空港の無線ノード。
- インターネット カフェ。

（注） クライアントレス SSL VPN がサポートしている Web ブラウザのリストについては、『サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ』を参照してください。

クライアントレス SSL VPN の前提条件

- ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
- クライアントレス SSL VPN の URL が必要です。URL は、https:*//address* 形式の https アドレスでなければなりません。*address* は、SSL VPN がイネーブルになっている ASA（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://cisco.example.com などです。
- クライアントレス SSL VPN のユーザー名とパスワードが必要です。

（注） クライアントレス SSL VPN ではローカル印刷がサポートされていますが、VPN 経由による企業ネットワーク上のプリンタへの印刷はサポートされていません。

クライアントレス SSL VPN フローティング ツールバーの使用

フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。

フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[**Close**] ボタンをクリックすると、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。

ヒント テキスト フィールドにテキストを貼り付けるには、Ctrl+V を使用します（クライアントレス SSL VPN セッション中は、表示されるツールバー上での右クリックはオフになっています）。

（注） ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。

Web のブラウズ

クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。セキュリティ ヒントの通知 （23 ページ）を参照してください。

クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザーが使い慣れたものと異なる場合があります。次に例を示します。

- クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。

- Web サイトへのアクセス方法：
  - クライアントレス SSL VPN ホーム ページ上の [Enter Web Address] フィールドに URL を入力する
  - クライアントレス SSL VPN ホーム ページ上にある設定済みの Web サイト リンクをクリックする
  - 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする
  - 保護されている Web サイトのユーザー名とパスワードが必要です。

特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN ホーム ページ上にリンクとして表示されるものに限られる

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN ホーム ページ上にリンクとして表示されるものに限られる

ネットワークのブラウズ（ファイル管理）

ユーザーは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。

（注） コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバーに保存される可能性があります。

重要なポイントは次のとおりです。

- 共有リモート アクセス用にファイル アクセス権を設定する必要があります。
- 保護されているファイル サーバーのサーバー名とパスワードが必要です。
- フォルダとファイルが存在するドメイン、ワークグループ、およびサーバーの名前が必要です。

（注） クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。

Remote File Explorer の使用

ユーザーは、Remote File Explorer を使用して、Web ブラウザから企業ネットワークをブラウズできます。ユーザーが Cisco SSL VPN ポータル ページの [Remote File System] アイコンをクリックすると、ユーザーのシステムでアプレットが起動し、ツリーおよびフォルダ ビューにリモート ファイル システムが表示されます。

（注） この機能を使用するには、ユーザーのマシンに Oracle Java ランタイム環境（JRE）がインストールされ、Web ブラウザで Java がイネーブルになっている必要があります。リモート ファイルの起動には、JRE 8u131 b11、7u141 b11、6u151 b10 以降が必要です。

ユーザーはブラウザで次を実行できます。

- リモート ファイル システムのブラウズ。
- ファイルの名前の変更。
- リモートファイルシステム内、およびリモートとローカルのファイルシステム間でのファイルの移動またはコピー。
- ファイルのバルク アップロードおよびダウンロードの実行。

  ファイルをダウンロードするには、ブラウザでファイルをクリックして、[Operations] > [Download] を選択し、[Save] ダイアログで場所と名前を指定してファイルを保存します。

  ファイルをアップロードするには、宛先フォルダをクリックして、[Operations] > [Upload] を選択し、[Open] ダイアログでファイルの場所と名前を指定します。

  この機能には次の制限があります。

  - ユーザーは、アクセスを許可されていないサブフォルダを表示できません。
  - ユーザーがアクセスを許可されていないファイルは、ブラウザに表示されても移動またはコピーできません。
  - ネストされたフォルダの最大の深さは 32 です。
  - ツリー ビューでは、ドラッグ アンド ドロップのコピーがサポートされていません。
  - Remote File Explorer の複数のインスタンスの間でファイルを移動するときは、すべてのインスタンスが同じサーバーを探索する必要があります（ルート共有）。
  - Remote File Explorer は、1 つのフォルダに最大 1500 のファイルおよびフォルダを表示できます。フォルダがこの制限を超えた場合、フォルダは表示されません。

ポート転送の使用

ポート フォワーディングを使用するには、ローカルにマッピングされたサーバーの IP アドレスとポート番号を使用してクライアント アプリケーションを設定する必要があります。

- アプリケーションを使用した後、ユーザーは [**Close**] アイコンをクリックして必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がオフに切り替わる可能性があります。

始める前に

- macOS では、この機能をサポートしているのは Safari 11 以前のブラウザだけです。
- クライアント アプリケーションがインストールされている必要があります。
- ブラウザでクッキーをイネーブルにする必要があります。
- DNS 名を使用してサーバーを指定する場合、ホスト ファイルの変更に必要になるため、PC に対する管理者アクセス権が必要です。
- Oracle Java Runtime Environment（JRE）をインストールしておく必要があります。

  JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザーに対して使用可能なサイトが示されます。まれに、Java 例外エラーで、ポート フォワーディング アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。

  1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。
  2. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。
  3. Java のインスタンスをすべて閉じます。
  4. クライアントレス SSL VPN セッションを確立し、ポート フォワーディング Java アプレットを起動します。

- ブラウザで javascript をイネーブルにする必要があります。デフォルトでは有効に設定されています。
- 必要に応じて、クライアント アプリケーションを設定する必要があります。

（注） Microsoft Outlook クライアントの場合、この設定手順は不要です。Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] フィールドの値をチェックします。[Remote Server] フィールドにサーバー ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。[Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。

手順

ステップ 1 クライアントレス SSL VPN セッションを開始して、[Home] ページの [Application Access] リンクをクリックします。[Application Access] ウィンドウが表示されます。

ステップ 2 [Name] カラムで、使用するサーバー名を確認し、このサーバーに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。

ステップ 3 この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。

（注）
クライアントレス SSL VPN セッション上で実行しているアプリケーションで URL（電子メールメッセージ内のものなど）をクリックしても、サイトがそのセッションで開くわけではありません。サイトをセッション上で開くには、その URL を [Enter Clientless SSL VPN (URL) Address] フィールドに貼り付けます。

ポート転送を介した電子メールの使用

電子メールを使用するには、クライアントレス SSL VPN のホームページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。

（注） IMAP クライアントの使用中にメール サーバーとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。

アプリケーション アクセスおよびその他のメール クライアントの要件を満たしている必要があります。

Web アクセスを介した電子メールの使用

次の電子メール アプリケーションがサポートされています。

- Microsoft Outlook Web App to Exchange Server 2010

  OWA には、Internet Explorer 11（以降）、または最新の Firefox が必要です。

- Exchange Server 2013 への Microsoft Outlook Web アクセス。

  最適な結果を得るために、Internet Explorer11（以降）または最新の Firefox で OWA を使用してください。

- Louts iNotes

（注） Web ベースの電子メール製品がインストールされており、その他の Web ベースの電子メール アプリケーションも動作する必要がありますが、検証されていません。

電子メール プロキシを介した電子メールの使用

メール アプリケーションの使用方法と例については、「クライアントレス SSL VPN を介した電子メールの使用」を参照してください。

はじめる前に

SSL 対応メール アプリケーションがインストールされている必要があります。

ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。

メール アプリケーションが正しく設定されている必要があります。

その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

スマート トンネルの使用

スマート トンネルの使用に管理権限は必要ありません。

（注） ポート フォワーダの場合と異なり、Java は自動的にダウンロードされません。

- スマート トンネルを使用する場合、Windows では ActiveX または JRE、Mac OS X では Java Web Start が必要です。
- ブラウザでクッキーをイネーブルにする必要があります。
- ブラウザで javascript をイネーブルにする必要があります。
- Mac OS X では、フロントサイド プロキシはサポートされていません。
- サポートされているオペレーティング システムとブラウザだけを使用してください。
- TCP ソケットベースのアプリケーションだけがサポートされています。

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。