SaaS アクセス コントロール

この章で説明する内容は、次のとおりです。

SaaS アクセス コントロールの概要

Secure Web Applianceは、セキュリティ アサーション マークアップ言語（SAML）を使用して、SaaS アプリケーションへのアクセスを許可します。SAML バージョン 2.0 に厳密に準拠している SaaS アプリケーションで動作します。

Cisco SaaS アクセス コントロールによって、以下のことが可能になります。

- SaaS アプリケーションにアクセスできるユーザーおよび場所を制御する。
- ユーザーが組織を退職した時点で、すべての SaaS アプリケーションへのアクセスをただちに無効にする。
- ユーザーに SaaS ユーザー クレデンシャルの入力を求めるフィッシング攻撃のリスクを軽減する。
- ユーザーを透過的にサインインさせるか（シングル サイン オン機能）、ユーザーに認証ユーザー名とパスフレーズの入力を求めるかを選択する。

SaaS アクセスコントロールは、 Secure Web Applianceがサポートしている認証メカニズムを必要とする SaaS アプリケーションでのみ動作します。現在、Web プロキシは「PasswordProtectedTransport」認証メカニズムを使用しています。

SaaS アクセスコントロールをイネーブルにするには、 Secure Web Applianceと SaaS アプリケーションの両方の設定を行う必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Secure Web Applianceを ID プロバイダーとして設定する。	ID プロバイダとしてのアプライアンスの設定 （2 ページ）
ステップ 2	SaaS アプリケーションの認証ポリシーを作成します。	SaaS アプリケーション認証ポリシーの作成 （4 ページ）
ステップ 3	SaaS アプリケーションをシングル サイン オン用に設定します。	シングル サイン オン URL へのエンドユーザー アクセスの設定 （8 ページ）
ステップ 4	（任意）複数の Secure Web Applianceを設定する。	SaaS アクセス コントロールと複数のアプライアンスの使用 （4 ページ）

ID プロバイダとしてのアプライアンスの設定

Secure Web Applianceを ID プロバイダーとして設定する場合、定義する設定は通信するすべての SaaS アプリケーションに適用されます。 Secure Web Applianceは、作成する各 SAML アサーションに署名するために証明書とキーを使用します。

始める前に

- （任意）SAML アサーションに署名するための証明書（PEM 形式）とキーを検索します。
- 各 SaaS アプリケーションに証明書をアップロードします。

ステップ 1 [ネットワーク（Network）] > [SaaS の ID プロバイダ（Identity Provider for SaaS）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [SaaS シングルサインオンサービスを有効にする（Enable SaaS Single Sign-on Service）] をオンにします。

ステップ 4 [アイデンティティ プロバイダのドメイン名（Identity Provider Domain Name）] フィールドに仮想ドメイン名を入力します。

ステップ 5 [アイデンティティ プロバイダのエンティティ ID（Identity Provider Entity ID）] フィールドに、一意のテキスト識別子を入力します（URI 形式の文字列を推奨）。

ステップ 6 証明書とキーをアップロードまたは生成します。

方法	この他の手順
証明書およびキーのアップロード	**1.** [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。 **2.** [証明書（Certificate] フィールドで [参照（Browse）]をクリックし、アップロードするファイルを検索します。 （注） Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルはPEM形式にする必要があります。DER 形式はサポートされていません。 **3.** [キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードするファイルを指定します。 キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。 （注） キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キー ファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。 **4.** [ファイルのアップロード（Upload File）] をクリックします。 **5.** [証明書をダウンロード（Download Certificate）] をクリックして、 Secure Web Applianceが通信する SaaS アプリケーションに転送する証明書のコピーをダウンロードします。
証明書およびキーの生成	**1.** [生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。 **2.** [新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。 **1.** [証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、署名付き証明書に表示する情報を入力します。 （注） [共通名（Common Name）] フィールドには、スラッシュ（/）を除く任意の ASCII 文字を入力できます。 **2.** [生成（Generate）] をクリックします。 **3.** [証明書をダウンロード（Download Certificate）] をクリックして、 Secure Web Applianceが通信する SaaS アプリケーションに証明書を転送します。 **4.** （任意）署名付き証明書を使用するには、[証明書署名要求のダウンロード（Download Certificate Signing Request）]（DCSR）リンクをクリックして、認証局（CA）に要求を送信します。CA から署名付き証明書を受信したら、[参照（Browse）] をクリックし、署名付き証明書の場所に移動します。[ファイルのアップロード（Upload File）] をクリックします。（バグ 37984）

（注） アップロードされた証明書とキーのペアと、生成された証明書とキーのペアの両方がアプライアンスにある場合、アプライアンスは、[署名証明書（Signing Certificate）] セクションで現在選択されている証明書とキーのペアのみを使用します。

ステップ 7 アプライアンスを ID プロバイダとして設定する場合は、設定を書き留めておきます。これらの設定の一部は、SaaS アプリケーションをシングル サイン オン用に設定する際に使用する必要があります。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

SAML アサーションの署名に使用する証明書とキーを指定したら、各 SaaS アプリケーションに証明書をアップロードします。

関連項目

- シングル サイン オン URL へのエンドユーザー アクセスの設定 （8 ページ）

SaaS アクセス コントロールと複数のアプライアンスの使用

始める前に

ID プロバイダとしてのアプライアンスの設定 （2 ページ）

ステップ 1 各 Secure Web Applianceに対して同じ ID プロバイダーのドメイン名を設定します。

ステップ 2 各 Secure Web Applianceに対して同じ ID プロバイダーのエンティティ ID を設定します。

ステップ 3 [ネットワーク（Network）] > [SaaS の ID プロバイダ（Identity Provider for SaaS）] ページで、各アプライアンスに同じ証明書と秘密キーをアップロードします。

ステップ 4 設定する各 SaaS アプリケーションにこの証明書をアップロードします。

SaaS アプリケーション認証ポリシーの作成

始める前に

- 関連付けられた ID を作成します。
- ID プロバイダを設定します（ID プロバイダとしてのアプライアンスの設定 （2 ページ）を参照）。

- ID プロバイダの署名証明書とキーを入力します（[ネットワーク（Network）] > [SaaS の ID プロバイダ（Identity Provider for SaaS）] > [設定の有効化と編集（Enable and Edit Settings）]）。
- 認証レルムを作成します。認証レルム

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [SaaS ポリシー（SaaS Policies）] を選択します。

ステップ 2 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 3 以下の設定項目を設定します。

プロパティ	説明
アプリケーション	このポリシーの SaaS アプリケーションを識別する名前を入力します。各アプリケーション名は一意である必要があります。 Secure Web Applianceは、アプリケーション名を使用して、シングル サインオン URL を生成できます。
説明	（任意）この SaaS ポリシーの説明を入力します。

プロパティ	説明
サービスプロバイダのメタデータ（Metadata for Service Provider）	このポリシーで参照されるサービスプロバイダを示すメタデータを設定します。サービスプロバイダのプロパティを手動で記述するか、またはSaaSアプリケーションによって提供されるメタデータ ファイルをアップロードできます。 Secure Web Applianceは、SAML を使用して SaaS アプリケーション（サービスプロバイダー）と通信する方法を決定するために、メタデータを使用します。メタデータの適切な設定については、SaaS アプリケーションを参照してください。 キーの手動設定（Configure Keys Manually）：このオプションを選択した場合は、以下を入力します。 • [サービスプロバイダのエンティティID（Service Provider Entity ID）]。SaaS アプリケーションが自身をサービス プロバイダとして識別するために使用するテキスト（通常は URI 形式）を入力します。 • [名前IDの形式（Name ID Format）]。サービス プロバイダに送信する SAML アサーションでアプライアンスがユーザーを識別するために使用する形式を、ドロップダウン リストから選択します。ここで入力する値は、SaaS アプリケーションの対応する設定と一致している必要があります。 • [Assertion Consumer ServiceのURL（Assertion Consumer Service URL）]。 Secure Web Applianceが作成したSAMLアサーションの送信先URLを入力します。SaaS アプリケーションのマニュアルを参照して、使用する適切な URL （ログイン URL）を決定してください。 [ハードディスクからファイルをインポート（Import File from Hard Disk）]：このオプションを選択した場合は、[参照（Browse）] をクリックしてファイルを検索し、[インポート（Import）] をクリックします。 （注） このメタデータ ファイルは、サービス プロバイダのインスタンスを説明する SAML 標準に準拠した XML ドキュメントです。すべての SaaS アプリケーションがメタデータ ファイルを使用するわけではありませんが、使用する場合は、ファイルについてSaaSアプリケーションのプロバイダにお問い合わせください。

プロパティ	説明
ユーザー識別/SaaS SSO の認証（User Identification / Authentication for SaaS SSO）	SaaS シングル サインオンに対してユーザーを識別または認証する方法を指定します。 • ユーザーに対して、常にローカル認証クレデンシャルの入力を求める。 • Web プロキシが透過的にユーザー名を取得した場合に、ユーザーに対してローカル認証クレデンシャルの入力を求める。 • SaaS ユーザーのローカル認証クレデンシャルを使用して、ユーザーを自動的にサインインさせる。 この SaaS アプリケーションにアクセスするユーザーを認証するために、Web プロキシが使用する認証レルムまたはシーケンスを選択します。SaaS アプリケーションに正常にアクセスするには、ユーザーは認証レルムまたは認証シーケンスのメンバーである必要があります。Identity Services Engine を認証に使用しており、LDAP を選択した場合は、SAML ユーザー名と属性のマッピングにレルムが使用されます。
SAML ユーザー名のマッピング（SAML User Name Mapping）	Web プロキシが SAML アサーションでサービス プロバイダにユーザー名を示す方法を指定します。ネットワーク内で使用されているユーザー名を渡すか（[マッピングなし（No mapping）]）、または以下のいずれかの方法で内部ユーザー名を別の形式に変更できます。 • [LDAP クエリー（LDAP query）]。サービス プロバイダに送信されるユーザー名は、1 つ以上の LDAP クエリー属性に基づきます。LDAP 属性フィールドと任意のカスタム テキストを含む式を入力します。属性名は山カッコで囲む必要があります。任意の数の属性を含めることができます。たとえば、LDAP 属性が「user」と「domain」の場合は、<user>@<domain>.com と入力できます。 • [固定ルール マッピング（Fixed Rule Mapping）]。サービス プロバイダに送信されるユーザー名は、前または後ろに固定文字列を追加した内部ユーザー名に基づきます。[式名（Expression Name）] フィールドに固定文字列を入力し、その前または後ろに %s を付けて内部ユーザー名における位置を示します。
SAML 属性マッピング（SAML Attribute Mapping）	（任意）SaaS アプリケーションから要求された場合は、LDAP 認証サーバーから内部ユーザーに関する追加情報を SaaS アプリケーションに提供できます。各 LDAP サーバー属性を SAML 属性にマッピングします。
認証コンテキスト（Authentication Context）	Web プロキシが内部ユーザーを認証するために使用する認証メカニズムを選択します。 （注） 認証コンテキストは、ID プロバイダが内部ユーザーの認証に使用した認証メカニズムをサービス プロバイダに通知します。一部のサービス プロバイダでは、ユーザーに SaaS アプリケーションへのアクセスを許可するために特定の認証メカニズムが必要です。サービス プロバイダが ID プロバイダでサポートされていない認証コンテキストを必要とする場合、ユーザーはシングル サイン オンを使用して ID プロバイダからサービス プロバイダにアクセスできません。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

アプリケーションを設定したのと同じパラメータを使用して、SaaSアプリケーション側にシングル サインオンを設定します。

シングル サイン オン URL へのエンドユーザー アクセスの設定

Secure Web Applianceを ID プロバイダーとして設定し、SaaS アプリケーション用に SaaS アプリケーション認証ポリシーを作成すると、アプライアンスによってシングルサインオン URL（SSO URL）が作成されます。 Secure Web ApplianceはSaaS アプリケーション認証ポリシーで設定されたアプリケーション名を使用して、シングルサインオンURLを生成します。SSOURLの形式は以下のとおりです。

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [SaaS ポリシー（SaaS Policies）] ページで、シングルサインオン URL を取得します。

ステップ 2 フロー タイプに応じてエンドユーザーが URL を使用できるようにします。

ステップ 3 IDプロバイダによって開始されるフローを選択すると、アプライアンスはユーザーをSaaSアプリケーションにリダイレクトします。

ステップ 4 サービス プロバイダによって開始されるフローを選択する場合は、この URL を SaaS アプリケーションで設定する必要があります。

- 常にSaaSユーザーにプロキシ認証を要求する。ユーザーは有効なクレデンシャルを入力した後、SaaS アプリケーションにログインします。
- SaaS ユーザーを透過的にサインインさせる。ユーザーは SaaS アプリケーションに自動的にログインします。

（注） アプライアンスが透過モードで展開されている場合に、明示的な転送要求を使用して、すべての認証済みユーザーに対するシングル サイン オン動作を実現するには、ID グループを設定する際に、[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）] 設定を選択します。

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。