



SaaS アクセス コントロール

この章は、次の項で構成されています。

- SaaS アクセス コントロールの概要 (1 ページ)
- ID プロバイダーとしてのアプライアンスの設定 (2 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 (4 ページ)
- SaaS アプリケーション認証ポリシーの作成 (4 ページ)
- シングルサインオン URL へのエンドユーザ アクセスの設定 (7 ページ)

SaaS アクセス コントロールの概要

Web セキュリティ アプライアンスは、Security Assertion Markup Language (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および場所を制御する。
- ユーザ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。
- ユーザに SaaS ユーザ 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)、ユーザに認証ユーザ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、Web セキュリティ アプライアンス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、Web セキュリティ アプライアンスと 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。

ID プロバイダーとしてのアプライアンスの設定

手順

	コマンドまたはアクション	目的
ステップ1	Web セキュリティ アプライアンスを ID プロバイダーとして設定します。	ID プロバイダー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 へのエンドユーザアクセスの設定（7 ページ）
ステップ4	（任意）複数の Web セキュリティ アプライアンスを設定します。	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 プロバイダーとしてのアプライアンスの設定

Web セキュリティ アプライアンスを 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。Web セキュリティ アプライアンスは、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 プロバイダー（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ーのドメイン名（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ーのエンティティ 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	<ol style="list-style-type: none"> [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。 [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。 [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。 [ファイルのアップロード (Upload File)] をクリックします。 [証明書をダウンロード (Download Certificate)] をクリックして、Web セキュリティアプライアンスが通信する 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	<ol style="list-style-type: none"> [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。 [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。 <ol style="list-style-type: none"> [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。 [生成 (Generate)] をクリックします。 [証明書をダウンロード (Download Certificate)] をクリックして、Web セキュリティアプライアンスが通信する SaaS アプリケーションに証明書を転送します。 (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)

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

(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プロバイダー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 \(7 ページ\)](#)

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 プロバイダーとしてのアプライアンスの設定 \(2 ページ\)](#)

ステップ1 各 Web セキュリティ アプライアンスに対して同じ 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 Web セキュリティ アプライアンスに対して同じ 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 プロバイダー (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 プロバイダーを設定します ([ID プロバイダーとしてのアプライアンスの設定 \(2 ページ\)](#) を参照)。
- ・ID プロバイダー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 プロバイダー (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。Web セキュリティアプライアンスは、アプリケーション名を使用してシングルサインオン URL を生成します。
説明	(任意) この SaaS ポリシーの説明を入力します。
サービスプロバイダーのメタデータ (Metadata for Service Provider)	<p>このポリシーで参照されるサービスプロバイダーを示すメタデータを設定します。サービスプロバイダー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。</p> <p>Web セキュリティアプライアンスはメタデータを使用して、SAML により 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。</p> <p>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。</p> <ul style="list-style-type: none"> [サービスプロバイダーのエンティティ 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ー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ーに送信する SAML アサーションでアプライアンスがユーザ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)]。Web セキュリティアプライアンスが作成した 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。 <p>[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。</p> <p>(注) このメタデータファイルは、サービスプロバイダー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ーにお問い合わせください。</p>

SaaS アプリケーション認証ポリシーの作成

プロパティ	説明
ユーザ識別/SaaS SSO の認証 (User Identification / Authentication for SaaS SSO)	<p>SaaS シングルサインオンに対してユーザを識別または認証する方法を指定します。</p> <ul style="list-style-type: none"> ユーザに対して、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名を取得した場合に、ユーザ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 ユーザのローカル認証クレデンシャルを使用して、ユーザを自動的にサインインさせる。 <p>この SaaS アプリケーションにアクセスするユーザを認証するために、Web プロキシが使用する認証レルムまたはシークエンスを選択します。SaaS アプリケーションに正常にアクセスするには、ユーザは認証レルムまたは認証シークエ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 ユーザ名と属性のマッピングにレルムが使用されます。</p>
SAML ユーザ名のマッピング (SAML User Name Mapping)	<p>Web プロキシが SAML アサーションでサービスプロバイダーにユーザ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名を別の形式に変更できます。</p> <ul style="list-style-type: none"> [LDAP クエリー (LDAP query)]。サービスプロバイダーに送信されるユーザ名は、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ーに送信されるユーザ名は、前または後ろに固定文字列を追加した内部ユーザ名に基づきます。[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 認証サーバから内部ユーザ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)	<p>Web プロキシが内部ユーザ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。</p> <p>(注) 認証コンテキストは、ID プロバイダーが内部ユーザ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ーに通知します。一部のサービスプロバイダーでは、ユーザに SaaS アプリケーションへのアクセスを許可するため特定の認証メカニズムが必要です。サービスプロバイダーが ID プロバイダー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、ユーザはシングルサインオンを使用して ID プロバイダーからサービスプロバイダーにアクセスできません。</p>

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 アクセスの設定

Web セキュリティアプライアンスを ID プロバイダーとして設定し、SaaS アプリケーションの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。Web セキュリティアプライアンスは 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。SSO URL 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 プロバイダー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ー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 ユーザにプロキシ認証を要求する。ユーザ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 ユーザを透過的にサインインさせる。ユーザは 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。

■ シングルサインオン URLへのエンドユーザ アクセスの設定