Contrôle d'accès au logiciel-service (SaaS)

Cette rubrique contient les sections suivantes :

Survol du contrôle d’accès au logiciel-service (SaaS)

Secure Web Appliance utilise SAML (Security Assertion Markup Language) pour autoriser l’accès aux applications de logiciels-services. Il fonctionne avec des applications de logiciels-services qui sont strictement conformes à SAML version 2.0.

Le contrôle d’accès de logiciel-service Cisco vous permet de :

- Contrôlez quels utilisateurs peuvent accéder aux applications de logiciels-services et à partir d’où.
- Désactivez rapidement l’accès à toutes les applications d’applications-services lorsque les utilisateurs ne sont plus employés par l’entreprise.
- Réduisez le risque d’attaques d’hameçonnage qui demandent aux utilisateurs de saisir leurs informations d’identification d’utilisateur SaaS.
- Choisissez si les utilisateurs sont connectés de manière transparente (fonctionnalité de connexion unique) ou invités à saisir leur nom d’utilisateur et leur phrase secrète pour l’authentification.

Le contrôle d’accès SaaS fonctionne uniquement avec les applications SaaS qui nécessitent un mécanisme d’authentification pris en charge par Secure Web Appliance. À l’heure actuelle, le proxy Web utilise le mécanisme d’authentification « PasswordProtected Transport ».

Pour activer le contrôle d’accès au logiciel-service, vous devez configurer les paramètres sur Secure Web Appliance et l’application de logiciel-service :

Procedure

	Command or Action	Purpose
Étape 1	Configurez Secure Web Appliance comme fournisseur d'identité.	Configuration de l'appliance en tant que fournisseur d'identité, on page 2
Étape 2	Créez une politique d'authentification pour l'application de logiciel-service.	Création de politiques d'authentification d'applications de logiciel-service (SaaS), on page 4
Étape 3	Configurez l'application de logiciel-service pour la connexion unique.	Configuration de l'accès de l'utilisateur final à l'URL de connexion unique, on page 7
Étape 4	(Facultatif) Configurez plusieurs Secure Web Appliance.	Utilisation du contrôle d'accès au logiciel-service (SaaS) et de plusieurs appliances, on page 4

Configuration de l'appliance en tant que fournisseur d'identité

Lorsque vous configurez Secure Web Appliance comme fournisseur d'identité, les paramètres que vous définissez s'appliquent à toutes les applications de logiciels-services avec lesquelles il communique. Secure Web Appliance utilise un certificat et une clé pour signer chaque affirmation SAML qu'il crée.

Before you begin

- (Facultatif) Localisez un certificat (format PEM) et une clé pour la signature des Assertions SAML.
- Chargez le certificat dans chaque application de logiciel-service.

Étape 1 Choisissez **Network > Identity Provider for SaaS** ((Réseau > Fournisseur d'identité pour logiciel-service).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez la case **Enable SaaS Single Sign-on Service** (Activer le service de connexion unique SaaS).

Étape 4 Entrez un nom de domaine virtuel dans le champ **Identity Provider Domain Name** (Nom de domaine du fournisseur d'identité).

Étape 5 Saisissez un identifiant textuel unique dans le champ **Identity Provider Entity ID** (ID d'entité du fournisseur d'identité) (une chaîne au format URI est recommandée).

Étape 6 Chargez ou générez un certificat et une clé :

Méthode	Étapes supplémentaires
Charger un certificat et une clé	**a.** Sélectionnez **Use Uploaded Certificate and Key** (Utiliser le certificat et la clé téléchargés). **b.** Dans le champ **Certificate** (Certificat), cliquez sur Browse (Parcourir); localisez le fichier à télécharger. **Note** Le proxy Web utilise le premier certificat ou la première clé du fichier. Le fichier de certificat doit être au format PEM. Format DER non pris en charge. **c.** Dans le champ **Key** (Clé), cliquez sur Browse (Parcourir); localisez le fichier à télécharger. Si la clé est chiffrée, sélectionnez **Key is Encrypted** (La clé est chiffrée). **Note** La longueur de la clé doit être de 512, 1024 ou 2048 bits. Le fichier de clé privée doit être au format PEM. Format DER non pris en charge. **d.** Cliquez sur **Upload Files** (Charger des fichiers). **e.** Cliquez sur **Download Certificate** (Télécharger le certificat) pour télécharger une copie du certificat et la transférer vers les applications de logiciel-service avec lesquelles Secure Web Appliance communique.
Générer un certificat et une clé	**a.** Sélectionnez **Use Generate Certificate and Key** (Utiliser le certificat et la clé générés). **b.** Cliquez sur **Generate New Certificate and Key** (Générer un nouveau certificat et une nouvelle clé). **1.** Dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé), saisissez les informations à afficher dans le certificat de signature. **Note** Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ Common Name (Nom commun). **2.** Cliquez sur **Generate** (Générer). **c.** Cliquez sur **Download Certificate** (Télécharger le certificat) pour transférer le certificat vers les applications de logiciel-service avec lesquelles Secure Web Appliance communiquera. **d.** (Facultatif) Pour utiliser un certificat signé, cliquez sur le lien **Download Certificate Signing Request** (DCSR) (Télécharger la demande de signature de certificat) pour envoyer une demande à une autorité de certification (CA). Après avoir reçu un certificat signé de l'autorité de certification, cliquez sur **Browse** (Parcourir) et accédez à l'emplacement du certificat signé. Cliquez sur **Upload Files** (Charger des fichiers). (bogue 37984)

Note Si l'appliance a à la fois un certificat et une paire de clés téléchargés et un certificat et une paire de clés générés, elle utilise uniquement le certificat et la paire de clés actuellement sélectionnés dans la section du certificat de signature.

Étape 7 Prenez note des paramètres lorsque vous configurez l'appliance en tant que fournisseur d'identité. Certains de ces paramètres doivent être utilisés lors de la configuration de l'application de logiciel-service pour la connexion unique.

Étape 8 Envoyez et validez les modifications.

What to do next

Après avoir spécifié le certificat et la clé à utiliser pour la signature des déclarations SAML, chargez le certificat dans chaque application de logiciel-service.

Thèmes connexes

- Configuration de l'accès de l'utilisateur final à l'URL de connexion unique, on page 7

Utilisation du contrôle d'accès au logiciel-service (SaaS) et de plusieurs appliances

Before you begin

Configuration de l'appliance en tant que fournisseur d'identité, on page 2

Étape 1 Configurez le même nom de domaine de fournisseur d'identité pour chaque Secure Web Appliance.

Étape 2 Configurez le même ID d'entité de fournisseur d'identité pour chaque Secure Web Appliance.

Étape 3 Chargez le même certificat et la même clé privée sur chaque appliance dans la page **Network > Identity Provider for SaaS** (Réseau > Fournisseur d'identité pour SaaS).

Étape 4 Chargez ce certificat dans chaque application de logiciel-service que vous configurez.

Création de politiques d'authentification d'applications de logiciel-service (SaaS)

Before you begin

- Créez les identités associées.
- Configurez le fournisseur d'identité, voir Configuration de l'appliance en tant que fournisseur d'identité, on page 2.
- Fournissez un certificat de signature de fournisseur d'identité et une clé : Network > Identity Provider for SaaS > Enable and Edit Settings (Réseau > Fournisseur d'identité pour logiciel-service > Activer et modifier les paramètres).
- Créez un domaine d'authentification, Domaines d'authentification.

Étape 1 Choisissez **Web Security Manager > SaaS Policies** (Web Security Manager > Politiques SaaS)

Étape 2 Cliquez sur **Add Application** (Ajouter une application).

Étape 3 Configurez les paramètres.

Propriété	Description
Nom de l'application	Saisissez un nom pour identifier l'application de logiciel-service pour cette politique; chaque nom d'application doit être unique. Secure Web Appliance utilise le nom de l'application pour générer une URL de connexion unique.
Description	(Facultatif) Saisissez la description de cette politique SaaS.
Métadonnées pour le fournisseur de services	Configurez les métadonnées qui décrivent le fournisseur de services référencé dans cette politique. Vous pouvez soit décrire les propriétés du fournisseur de services manuellement, soit charger un fichier de métadonnées fourni par l'application de logiciel-service. Secure Web Appliance utilise les métadonnées pour déterminer comment communiquer avec l'application de logiciel-service (fournisseur de services) à l'aide de SAML. Contactez l'application de logiciel-service pour connaître les paramètres corrects de configuration des métadonnées. **Configure Keys Manually** (Configurer les clés manuellement) : si vous sélectionnez cette option, fournissez les éléments suivants : • **ID d'entité du fournisseur de services**. Saisissez le texte (généralement au format URI) que l'application de logiciel-service utilise pour s'identifier en tant que fournisseur de services. • **Name ID Format** (Format de l'ID du nom). Choisissez dans la liste déroulante le format que l'appliance doit utiliser pour identifier les utilisateurs dans l'assertion SAML envoyée aux fournisseurs de services. La valeur que vous entrez ici doit correspondre au paramètre correspondant configuré sur l'application de logiciel-service. • **Assertion Consumer Service URL** (URL de l'ACS (Assertion Consumer Service)). Entrez l'URL à laquelle Secure Web Appliance doit envoyer l'assertion SAML qu'elle crée. Lisez la documentation de l'application de logiciel-service pour déterminer la bonne URL à utiliser (également appelée URL de connexion). **Import File from Hard Disk** (Importer un fichier du disque dur) : si vous sélectionnez cette option, cliquez sur Parcourir, localisez le fichier, puis cliquez sur **Import** (Importer). **Note** Ce fichier de métadonnées est un document XML, selon la norme SAML, qui décrit une instance de fournisseur de services. Toutes les applications de logiciel-service n'utilisent pas de fichiers de métadonnées, mais pour celles qui le font, contactez le fournisseur d'applications de logiciel-service pour le fichier.

Propriété	Description
User Identification / Authentication for SaaS SSO (Identification/authentification de l'utilisateur pour SSO SaaS)	Préciser comment les utilisateurs sont identifiés ou authentifiés pour la connexion unique de logiciel-service : • Invitez toujours les utilisateurs à fournir leurs informations d'authentification locales. • Invitez les utilisateurs à fournir leurs identifiants d'authentification locale si le proxy Web a obtenu leurs noms d'utilisateur de manière transparente. • Enregistrez automatiquement les utilisateurs de logiciels-services à l'aide de leurs informations d'authentification locales. Choisissez le domaine ou la séquence d'authentification que le proxy Web doit utiliser pour authentifier les utilisateurs accédant à cette application de logiciel-service. Les utilisateurs doivent être membres du domaine d'authentification ou de la séquence d'authentification pour accéder avec succès à l'application de logiciel-service. Si un moteur de services d'identité est utilisé pour l'authentification et que LDAP a été sélectionné, le domaine sera utilisé pour les noms d'utilisateur SAML et le mappage d'attributs.
SAML User Name Mapping (Mappage des noms d'utilisateur SAML)	Précisez comment le proxy Web doit présenter les noms d'utilisateur pour le fournisseur de services dans l'assertion SAML. Vous pouvez transmettre les noms d'utilisateur tels qu'ils sont utilisés à l'intérieur de votre réseau (**pas de mappage**) ou vous pouvez modifier les noms d'utilisateurs internes dans un format différent à l'aide de l'une des méthodes suivantes : • **Requête LDAP**. Les noms d'utilisateur envoyés au fournisseur de services sont basés sur un ou plusieurs attributs de requête LDAP. Saisissez une expression contenant des champs d'attribut LDAP et du texte personnalisé facultatif. Vous devez mettre les noms d'attributs entre crochets. Vous pouvez inclure n'importe quel nombre d'attributs. Par exemple, pour les attributs LDAP « utilisateur » et « domaine », vous pourriez entrer <user>@<domain>.com. • **Mappage fixe des règles**. Les noms d'utilisateur envoyés au fournisseur de services sont basés sur le nom d'utilisateur interne et une chaîne fixe est ajoutée avant ou après le nom d'utilisateur interne. Entrez la chaîne fixe dans le champ **Expression Name** (Nom de l'expression), avec %s avant ou après la chaîne pour indiquer sa position dans le nom d'utilisateur interne.
SAML Attribute Mapping (Mappage des attributs SAML)	(Facultatif) Vous pouvez fournir à l'application de logiciel-service des informations supplémentaires sur les utilisateurs internes à partir du serveur d'authentification LDAP si l'application de logiciel-service l'exige. Mappez chaque attribut de serveur LDAP sur un attribut SAML.
Authentication Context (Contexte d'authentification)	Choisissez le mécanisme d'authentification que le proxy Web utilise pour authentifier ses utilisateurs internes. **Note** Le contexte d'authentification informe le fournisseur de services du mécanisme d'authentification utilisé par le fournisseur d'identité pour authentifier les utilisateurs internes. Certains fournisseurs de services exigent un mécanisme d'authentification particulier pour permettre aux utilisateurs d'accéder à l'application de logiciel-service. Si un fournisseur de services exige un contexte d'authentification qui n'est pas pris en charge par un fournisseur d'identité, les utilisateurs ne peuvent pas accéder au fournisseur de services en utilisant la connexion unique du fournisseur d'identité.

Étape 4 Envoyez et validez les modifications.

What to do next

Définissez les paramètres de connexion unique du côté de l'application de logiciel-service en utilisant les mêmes paramètres pour configurer l'application.

Configuration de l'accès de l'utilisateur final à l'URL de connexion unique

Après avoir configuré Secure Web Appliance comme fournisseur d'identité et créé une politique d'authentification d'application de logiciel-service pour l'application de logiciel-service (SaaS), l'appliance crée une URL de connexion unique (URL SSO). Secure Web Appliance utilise le nom de l'application configuré dans la politique d'authentification de l'application de logiciel-service pour générer l'URL de connexion unique; le format de l'URL de connexion unique est :

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

Étape 1 Obtenez l'URL de connexion unique sur la page **Web Security Manager > SaaS Policies** (Web Security Manager > Politiques SaaS).

Étape 2 Rendre l'URL disponible pour les utilisateurs finaux en fonction du type de flux.

Étape 3 Si vous choisissez Identity provider initiated flow (Flux lancé par le fournisseur d'identité), l'appliance redirige les utilisateurs vers l'application de logiciel-service.

Étape 4 Si vous choisissez les flux initiés par le fournisseur de services, vous devez configurer cette URL dans l'application de logiciel-service.

- Toujours demander aux utilisateurs de logiciels-services de s'authentifier par proxy. Après avoir saisi des informations d'authentification valides, les utilisateurs sont connectés à l'application de logiciel-service.
- Enregistrez de manière transparente les utilisateurs de logiciels-services (SaaS). Les utilisateurs sont automatiquement connectés à l'application de logiciel-service.

  Note Pour obtenir un comportement de connexion unique utilisant des demandes de transfert explicites pour tous les utilisateurs authentifiés lorsque l'appliance est déployée en mode transparent, sélectionnez « **Apply same surrogate settings to explicit forward requests** » (Appliquer les mêmes paramètres de substitution pour les demandes de transfert explicites) lorsque vous configurez le groupe d'identités.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.