Configuration de l'authentification externe SAML SSO pour l'administration ESA et SMA

Table des matières

Introduction

Ce document décrit comment configurer l'authentification externe SSO SAML 2.0 pour l'administration système ESA et SMA.

Environnement

- Produits : Appliance de sécurité de la messagerie (ESA), appliance de gestion de la sécurité (SMA)
- S'applique à : Administration des systèmes ESA et SMA
- Comportement du cluster : Les profils de fournisseur de services (SP) et de fournisseur d'identité sont configurés au niveau de l'ordinateur ; le mappage d'authentification externe est configuré au niveau du cluster.

Conditions préalables

- Accès administratif à l'interface Web ESA/SMA
- Certificat X.509 et clé privée disponibles au format PKCS #12 (PFX) ou PEM (auto-signé ou CA-signé)
- Accès à une application tierce Identity Provider (IdP) et à ses métadonnées SAML/URL SSO

Liste de contrôle de préconfiguration

- Vérifiez le nom d'hôte/nom de domaine complet de l'interface de gestion que les administrateurs utilisent pour accéder à l'appliance ; vérifiez que l'URL du service client d'assertion (ACS) correspond à ce nom d'hôte.
- Si l'appliance est dans un cluster, prévoyez de configurer SAML au niveau de la machine pour chaque membre avant d'activer l'authentification externe SAML.
- Déterminez si le fournisseur d'identité nécessite une application ou un domaine distinct par appliance.
- Vérifiez que les certificats et les clés requis sont disponibles.
- Confirmez que le fournisseur d'identité envoie le groupe ou l'attribut de rôle requis pour le mappage de rôle ESA/SMA.

Mise en garde : Ce document ne s'applique pas à la mise en quarantaine de l'utilisateur final (EUQ) SAML SSO.

Informations générales

- Le centre d'assistance technique Cisco ne fournit pas d'assistance technique pour la configuration de fournisseurs d'identité tiers. Des exemples de références de configuration sont fournis pour les IDp courants.

IDp SAML SSO

- Duo Access Gateway (DAG) ajoute une authentification à deux facteurs, avec des services cloud populaires utilisant la fédération SAML 2.0.
- Services ADFS (Active Directory Federation Services) : testés avec ADFS 2,3,4, Azure Active Directory (Azure AD), SecureAUTH et PingFederate
- Une authentification à deux facteurs supplémentaire peut être utilisée si le fournisseur d'identité la prend en charge dans l'infrastructure d'authentification unique SAML 2.0.
- Okta prend en charge l'authentification avec un IdP qui prend en charge le service.

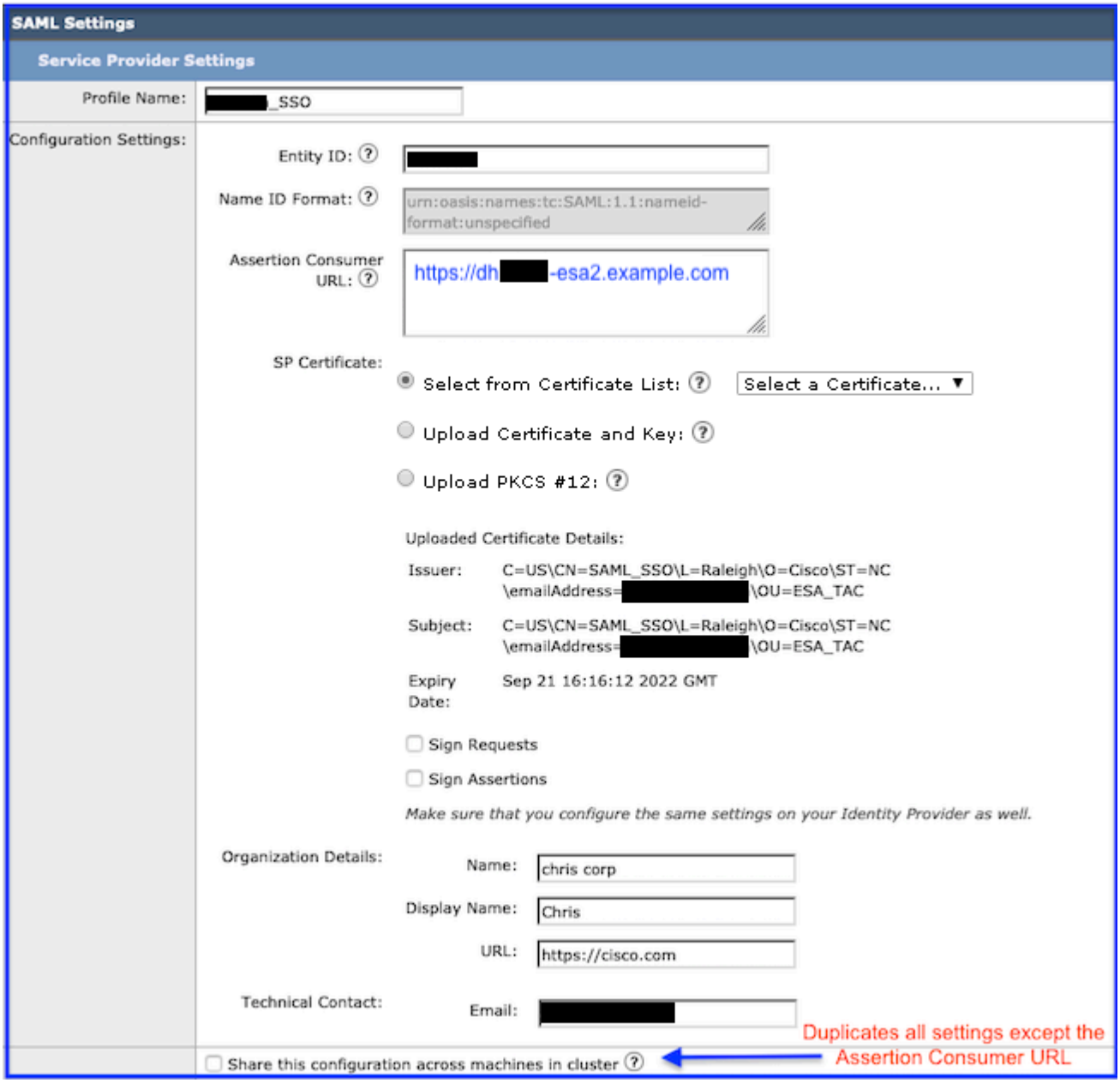
Configurer ESA/SMA en tant que fournisseur de services

Accédez à System Administration > SAML > (Machine Level) > Add Service Provider.

Remarque : Les ESA d'un cluster nécessitent une configuration au niveau de l'ordinateur pour tous les membres du cluster avant que SAML puisse être activé.

- Si l'option au bas de la page, Partager cette configuration entre les machines dans le cluster, est sélectionnée, les conditions suivantes s'appliquent :
    - Tous les champs sont répliqués vers les membres du cluster à l'exception de l'URL du consommateur d'assertions.
    - L'URL du consommateur d'assertions renseigne automatiquement le nom d'hôte de l'interface de gestion en tant qu'ACS.
    - Les environnements qui utilisent un autre nom d'hôte pour accéder à l'hôte nécessitent une configuration manuelle pour chaque hôte, par exemple, les appliances hébergées par CES.
    - Nom du profil : Nom utilisé pour étiqueter l'instance SP dans l'interface ESA ou SMA.
    - ID d'entité : Nom utilisé pour l'instance SP telle que le fournisseur d'identités la voit. Ce nom est l'étiquette utilisée par le fournisseur d'identité pour représenter le fournisseur de services. Il peut s'agir de n'importe quel nom, par exemple ESA_SP ou ESA_SSO.
    - Format d'ID de nom : Champ non configurable.
    - URL du consommateur d'assertions ou Service consommateur d'assertions (ACS) : URL utilisée par le fournisseur d'identité pour communiquer avec cet hôte ESA/SMA.
    - Certificat SP :
        - Format : Certificats publics/privés X.509 au format PFX/PKCS12 ou PEM.
        - Option 1: Sélectionner dans la liste de certificats : Sélectionnez parmi les certificats déjà créés sur l'ESA dans Réseau > Certificats.
        - Option 2: Télécharger le certificat et la clé : Téléchargez un certificat et une clé au format PEM.
        - Option 3: Télécharger PKCS n° 12 : Téléchargez un fichier PKCS #12.
        - Facultatif: Créez un certificat auto-signé sur l'ESA/SMA pour l'authentification unique SAML.
        - Si nécessaire, protégez la clé privée par mot de passe.

Remarque : Si des certificats au format PEM sont utilisés, conservez chaque certificat et chaque clé privée dans des fichiers distincts.



Page Service Provider Setup

Page Service Provider Setup

- Demandes de signature : Option permettant de signer la communication ESA/SMA SAML envoyée au fournisseur d'identité.
- Affirmations de signature : Option permettant d'exiger que le fournisseur d'identité signe les assertions envoyées à l'ESA/SMA.
- Détails de l'organisation : Peut être renseigné avec les données d'entreprise appropriées.
- Soumettre et valider les modifications pour conserver les paramètres.
- Téléchargez les métadonnées SP depuis la page Configuration SAML.

Configurez le fournisseur d'identités (IdP) pour qu'il fonctionne avec les appareils ESA/SMA

Remarque : Certains IdP nécessitent des applications ou des domaines distincts pour chaque ESA (exemple : DUO)

Ces liens fournissent des exemples de configuration pour plusieurs IdP au moment de la publication.
Le centre d'assistance technique Cisco ne fournit pas d'assistance technique pour les produits tiers. Ces exemples sont fournis à titre de référence.

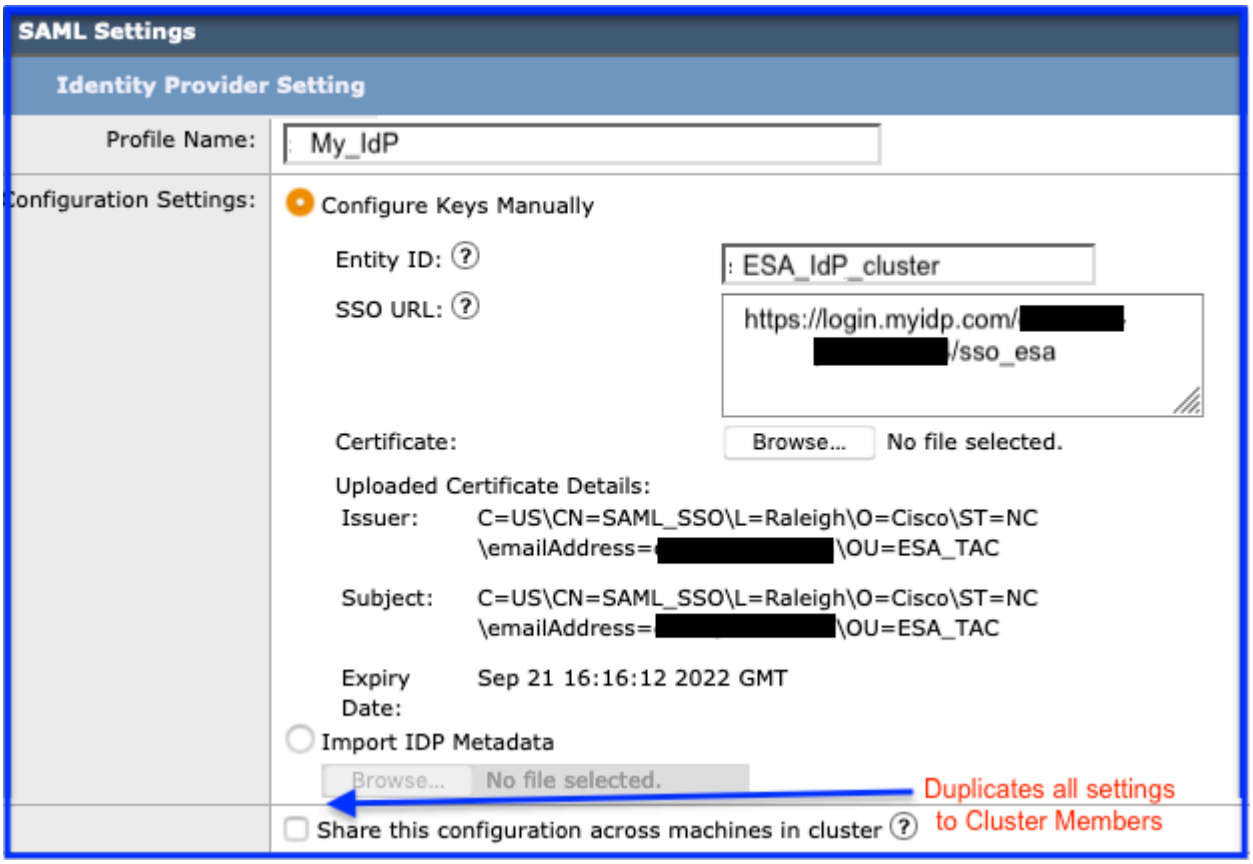
Configuration des paramètres IDP sur ESA/SMA

1. Accédez à Administration système > SAML.

2. Sélectionnez Ajouter un fournisseur d'identité.

- Deux options sont disponibles :
- Importer les métadonnées IdP
- Configuration manuelle des clés :
    - ID d'entité : Peut être n'importe quelle valeur utilisée pour identifier le fournisseur d'identité
    - URL SSO : URL à laquelle le SP envoie des demandes d'authentification SAML
    - Télécharger la clé privée et le certificat public dans des fichiers séparés

3. Partagez cette configuration entre les machines du cluster pour répliquer la configuration sur tous les ESA du cluster :

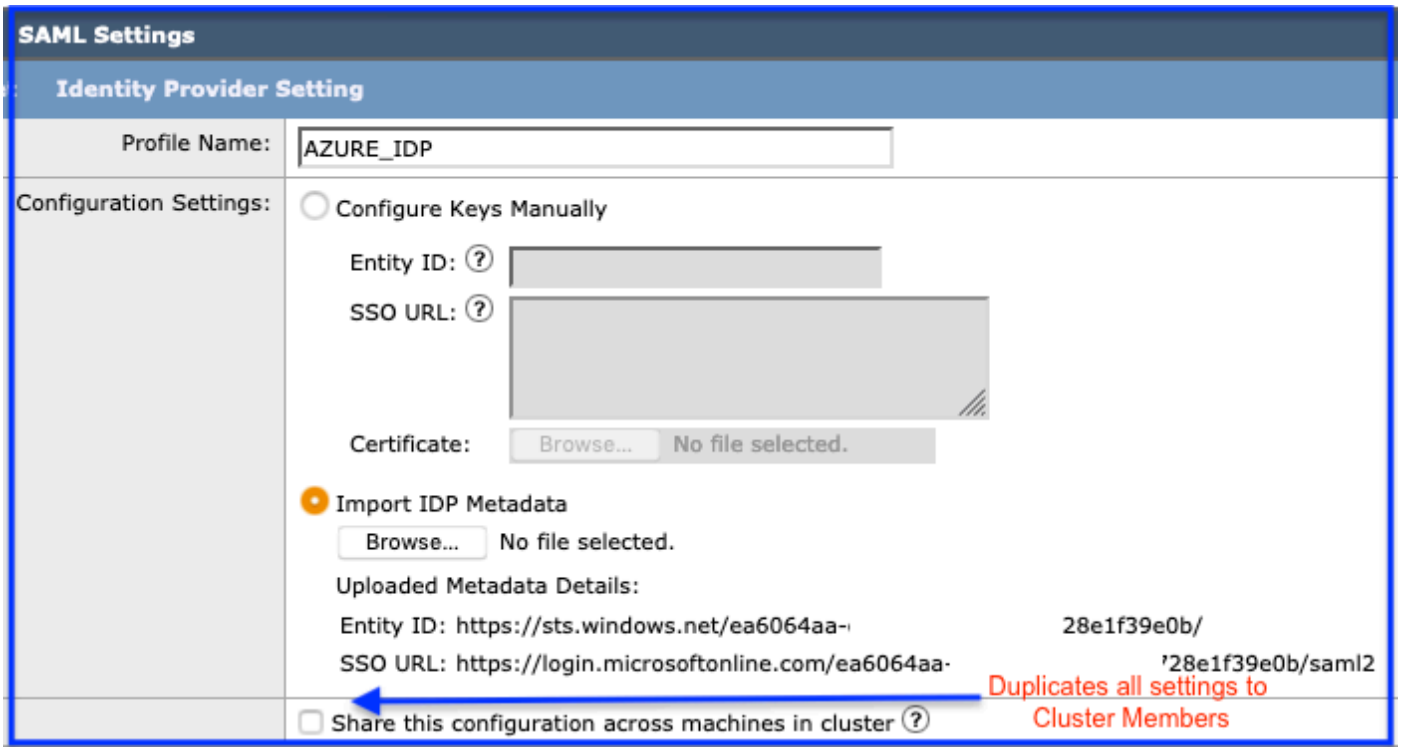


Saisir manuellement le contenu IdP

Saisir manuellement le contenu IdP

4. Télécharger des métadonnées à partir d'IdP

- Sélectionnez Importer les métadonnées IdP.
- Accédez au fichier de métadonnées enregistré à partir du fournisseur d'identité et enregistrez la configuration.
- L'option de partage de cette configuration entre les machines d'un cluster est disponible si elle s'applique au déploiement.



Télécharger des métadonnées depuis Idp

Télécharger des métadonnées depuis Idp

Activer l'authentification externe à l'aide de SAML sur ESA/SMA

Comme pour l'authentification externe LDAP, l'authentification unique SAML nécessite un mappage pour affecter des groupes à des rôles d'administration.

1. Accédez à System Administration > Users (Cluster Level) > External Authentication > Enable.

2. Sélectionnez le type d'authentification : SAML.

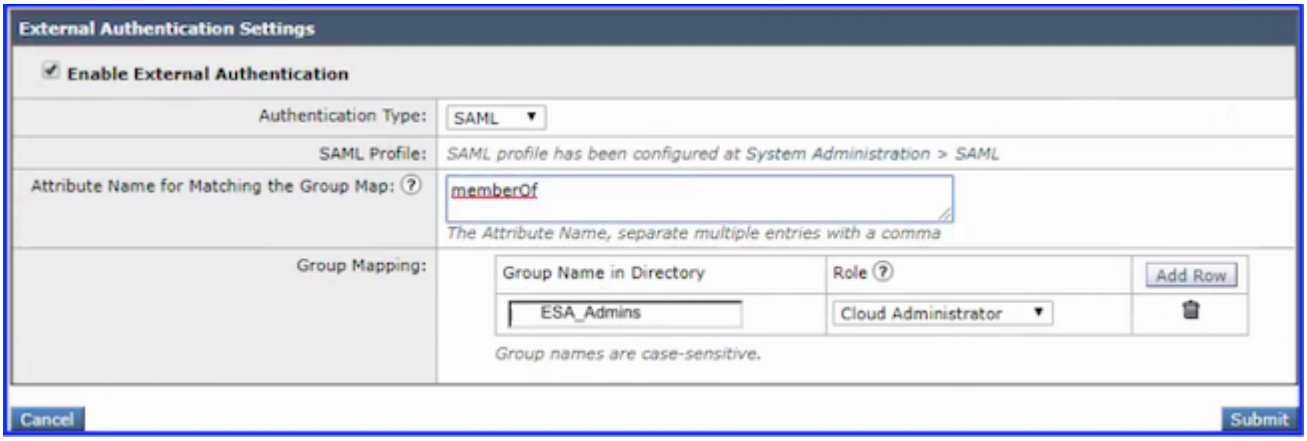
3. Nom d'attribut pour la correspondance de noms (facultatif) : Entrez le nom de l'attribut à rechercher dans le mappage de groupe.

Remarque : Le nom de l'attribut dépend des attributs configurés pour que le fournisseur d'identité relaie la réponse SAML. L'appliance recherche les entrées correspondantes du nom d'attribut spécifié dans la réponse SAML par rapport aux attributs configurés dans le champ Mappage de groupe. Si ce champ n'est pas configuré, l'appliance recherche tous les attributs présents dans la réponse SAML dans le champ Group Mapping configuré.

---

4. Entrez l'attribut de nom de groupe tel qu'il est défini dans le répertoire SAML en fonction du rôle utilisateur prédéfini ou personnalisé.

- Le champ Mappage de groupe doit contenir un attribut de groupe. L'attribut Unspecified Groups peut être ajouté pour authentifier les assertions ou les réponses SAML.



Paramètres d'authentification externe

Paramètres d'authentification externe

5. Soumettez et confirmez les modifications.

Une fois la configuration terminée, un nouveau lien s'affiche au bas de la page de connexion. La page de connexion ESA/SMA affiche un lien Utiliser l'authentification unique qui redirige les administrateurs vers le fournisseur d'identité d'entreprise.

Lorsque cette option est sélectionnée, l'administrateur est redirigé vers la page de connexion SAML de l'entreprise.

Utiliser le lien d'authentification unique redirigera vers SAML

Utiliser le lien d'authentification unique pour rediriger vers SAML

Dépannage

Utilisez ces indicateurs pour déterminer si le problème est lié à la configuration de l'appliance ou à la configuration du fournisseur d'identité.

Le lien de redirection SSO n'apparaît pas sur la page de connexion (« Utiliser l'authentification unique »)

Vérifiez que System Administration > Users > External Authentication > SAML est configuré.

La redirection retourne à la page de connexion ESA/SMA avec « Échec de l'authentification unique ! Veuillez contacter votre administrateur."

Erreur : "Échec de l'authentification SSO ! Veuillez contacter votre administrateur."

- Échec de l'authentification au niveau du fournisseur d'identité.
    - Cela indique que la configuration fonctionne au point d'atteindre la page d'authentification Single Sign-On et d'envoyer les informations d'identification.
    - Cet échec est souvent dû à la configuration IdP et nécessite une vérification supplémentaire des paramètres IdP.

Rediriger les retours vers la page de connexion ESA/SMA avec « Échec de l'autorisation ! Veuillez contacter votre administrateur."

Erreur : "Échec de l'autorisation ! Veuillez contacter votre administrateur."

- L'authentification a réussi, mais l'autorisation a échoué sur ESA/SMA.
    - Concentrez-vous sur les paramètres dans Utilisateurs > Authentification externe > SAML.
        - Nom d'attribut, Nom de groupe et Mappage de groupe.

Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides d'utilisation

- Cisco Content Security Management Appliance - Guides de l'utilisateur
- Cisco Web Security - Guides d'utilisation

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.