Configurer Okta SAML SSO pour la quarantaine de l'utilisateur final SMA

Table des matières

Introduction

Ce document décrit comment configurer Okta en tant que fournisseur d'identité SAML 2.0 pour l'accès de l'utilisateur final à la quarantaine Cisco Secure Email SMA.

Conditions préalables

- Produit : Appliance de gestion de la sécurité de la messagerie électronique (SMA) Cisco
- Fonctionnalité : SSO SAML pour la quarantaine de l'utilisateur final (EUQ)
- Fournisseur d'identité : Okta (SAML 2.0)
- S'applique à : Déploiements SMA qui fournissent un accès EUQ sur des plates-formes virtuelles ou matérielles. Remplacez les exemples de noms d'hôte et de ports par les valeurs de votre environnement.
- Contexte de version : Cette procédure s'applique aux versions SMA qui prennent en charge SAML pour EUQ. Vérifiez les champs et options de menu disponibles dans votre version installée.

Remarque : Ce document se concentre sur la configuration SAML SMA EUQ. ESA est référencé uniquement pour la génération de certificat lorsque SMA ne peut pas générer de certificat auto-signé.

Exigences

Avant de commencer, vérifiez que vous disposez des éléments suivants :

- Accès administratif à l'interface Web de SMA.
- Autorisations administratives dans Okta pour créer des applications SAML 2.0 et affecter des utilisateurs ou des groupes.
- Un certificat et une clé privée pour la configuration du fournisseur de services SMA. Un certificat auto-signé est acceptable pour les tests.
- Un nom de domaine complet (FQDN) et un port SMA EUQ accessibles auxquels les utilisateurs finaux peuvent accéder depuis leur navigateur.
- Les valeurs de l'URL d'assertion SAML SMA et de l'ID d'entité SP (de Administration système > SAML après avoir créé l'entrée SP).
- Comptes utilisateur dans Okta qui sont affectés à l'application Okta.
- Utilisateurs synchronisés avec les annuaires, si votre déploiement utilise l'intégration d'annuaires.

Remarque : Okta est un fournisseur d'identité tiers. Ce document fournit un exemple de configuration pour référence client.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

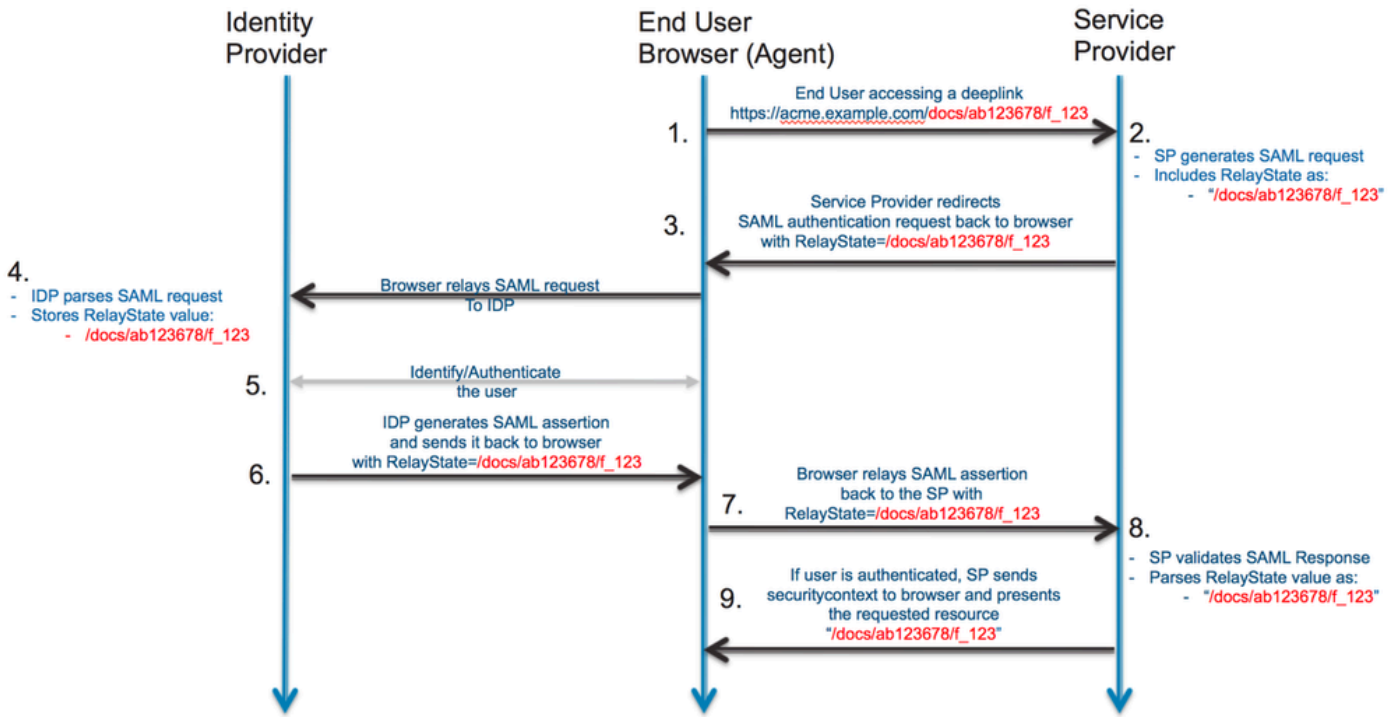
Informations générales

L'objectif est de configurer l'authentification unique (SSO) pour le portail de quarantaine du spam afin que les utilisateurs soient redirigés vers Okta pour s'authentifier, effectuer l'authentification multifacteur (MFA) si elle est activée dans Okta, puis revenir au portail EUQ SMA. Ce document s'applique uniquement à SMA. Cisco Secure Email Gateway, anciennement Email Security Appliance (ESA), est référencé uniquement pour la génération de certificats lorsque SMA ne peut pas générer de certificat auto-signé.

Problème : Les utilisateurs doivent s'authentifier sur le portail de quarantaine du spam SMA avec Okta en utilisant SAML SSO et MFA en option.

Résolution : Configurez SMA en tant que fournisseur de services, configurez une application SAML dans Okta, importez les paramètres du fournisseur d'ID Okta dans SMA, attribuez des utilisateurs dans Okta et vérifiez l'accès.

Flux SAML :



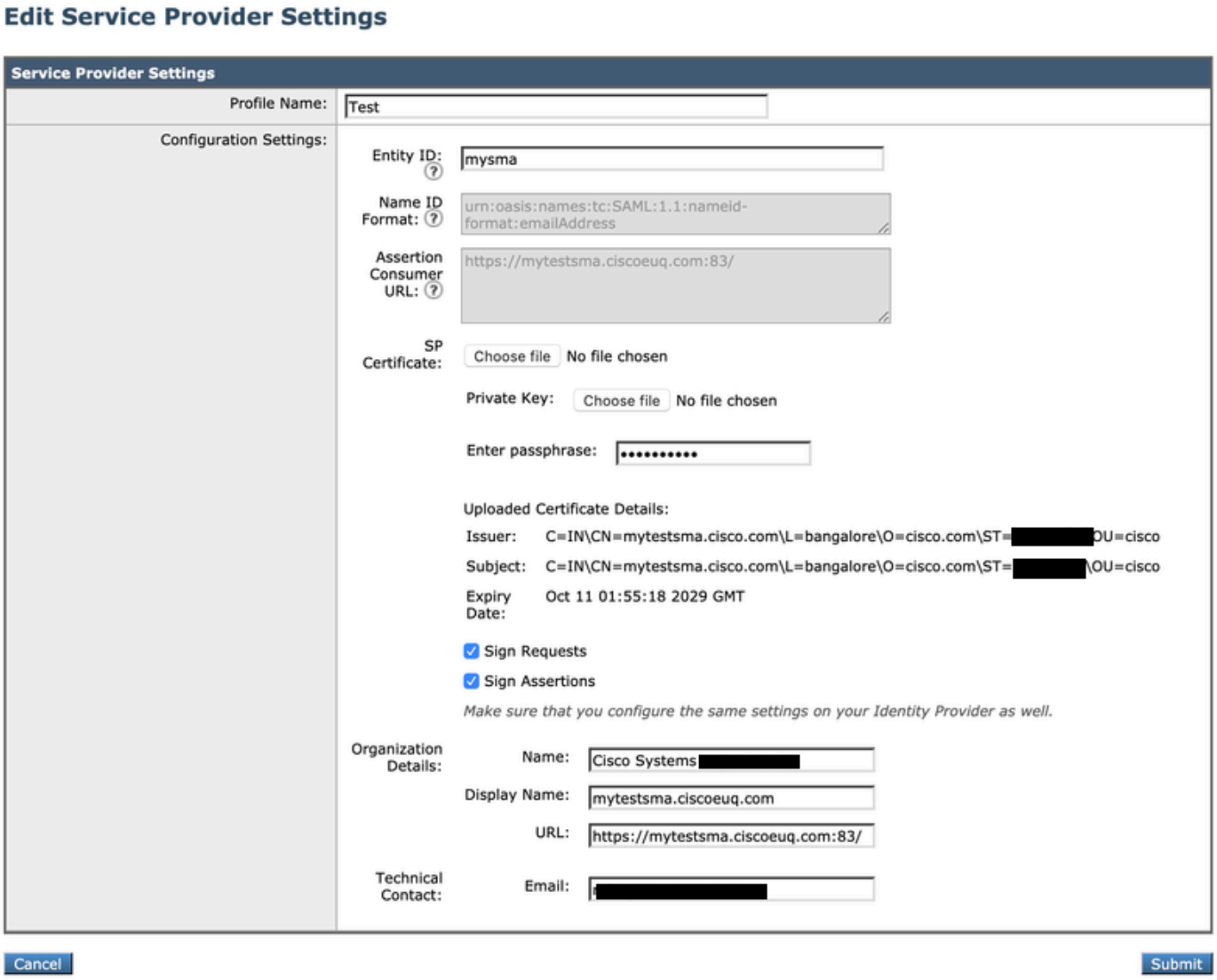
Configuration

Configurer le fournisseur de services (SP) sur l'appliance SMA

Pour configurer le SMA en tant que fournisseur de services SAML pour l'accès EUQ, procédez comme suit :

1. Connectez-vous à l'interface Web SMA.
2. Accédez à Administration système > SAML.
3. Sélectionnez Ajouter un fournisseur de services.
4. Dans ID d'entité du fournisseur de services, entrez l'ID d'entité que vous pouvez également configurer dans Okta.
5. Vérifiez que le format d'ID de nom et l'URL ACS (Assertion Consumer Service) sont renseignés pour l'interface EUQ.
6. Dans SP Certificate, téléchargez un certificat pour signer des requêtes SAML.

Remarque : SMA ne peut pas générer de certificat auto-signé. Vous pouvez également générer un certificat sur un ESA et l'exporter pour l'utiliser sur le SMA.

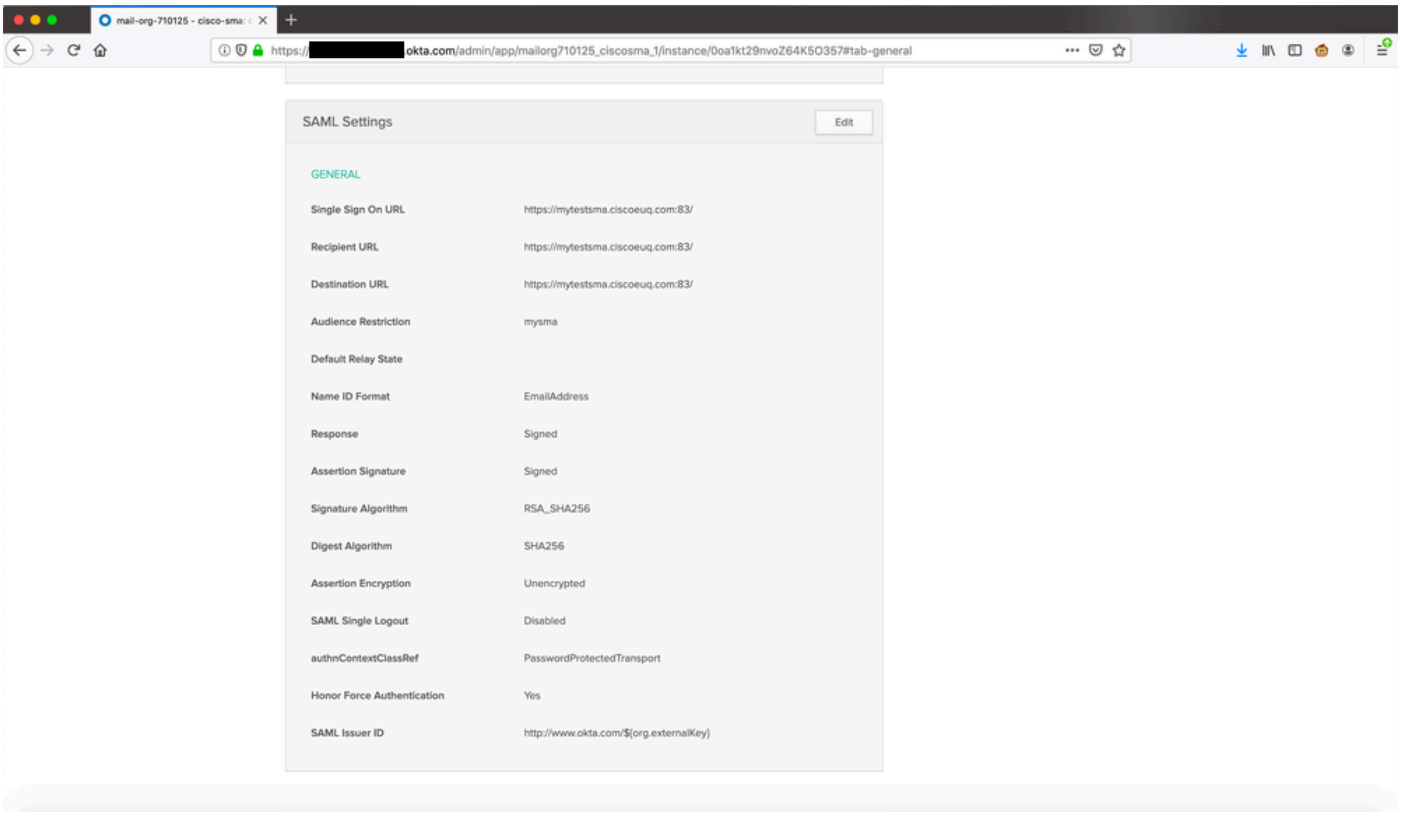


Paramètres du fournisseur de services dans l'interface utilisateur graphique

Configurer l'application SAML dans Okta

Pour créer une application SAML 2.0 dans Okta pour l'accès SMA EUQ, procédez comme suit :

1. Connectez-vous à Okta en tant qu'administrateur.
2. Accédez à Applications > Applications, puis sélectionnez Create App Integration.
3. Sélectionnez SAML 2.0, puis Next.
4. Entrez un nom d'application, par exemple, SMA EUQ, puis sélectionnez Next.
5. Dans Single sign-on URL, saisissez l'URL ACS SMA à partir des paramètres du fournisseur de services SMA.
6. Dans URI d'auditoire (ID d'entité SP), entrez le même ID d'entité configuré sur le SMA.
7. Pour le format d'ID de nom, sélectionnez AdresseE-mail.
8. Dans Application username, sélectionnez le format de nom d'utilisateur Okta approprié pour votre déploiement.
9. Terminez l'Assistant, puis ouvrez la nouvelle application et copiez le fichier XML de métadonnées IdP ou l'URL de métadonnées.

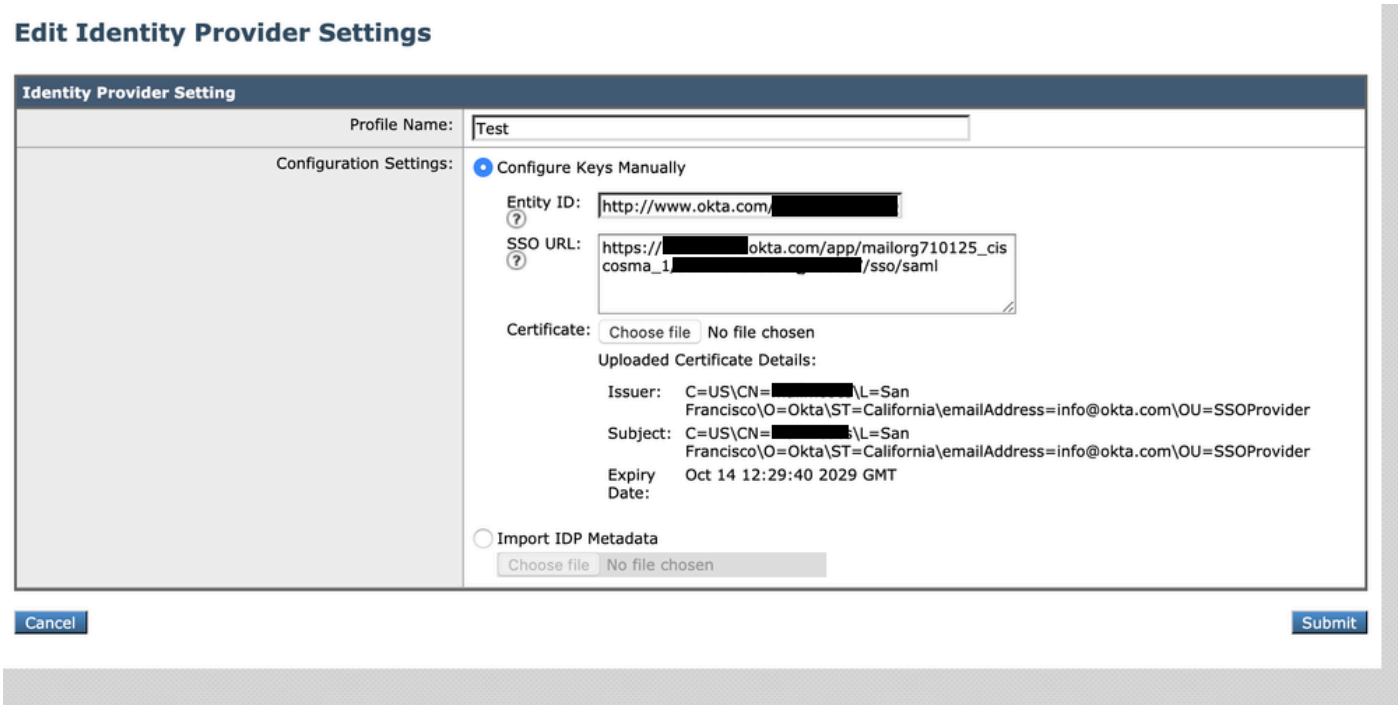


Afficher le portail Okta

Configurer le fournisseur d'identité (IdP) sur l'appareil SMA

Pour configurer Okta en tant que fournisseur d'identité (IdP) sur le SMA, procédez comme suit :

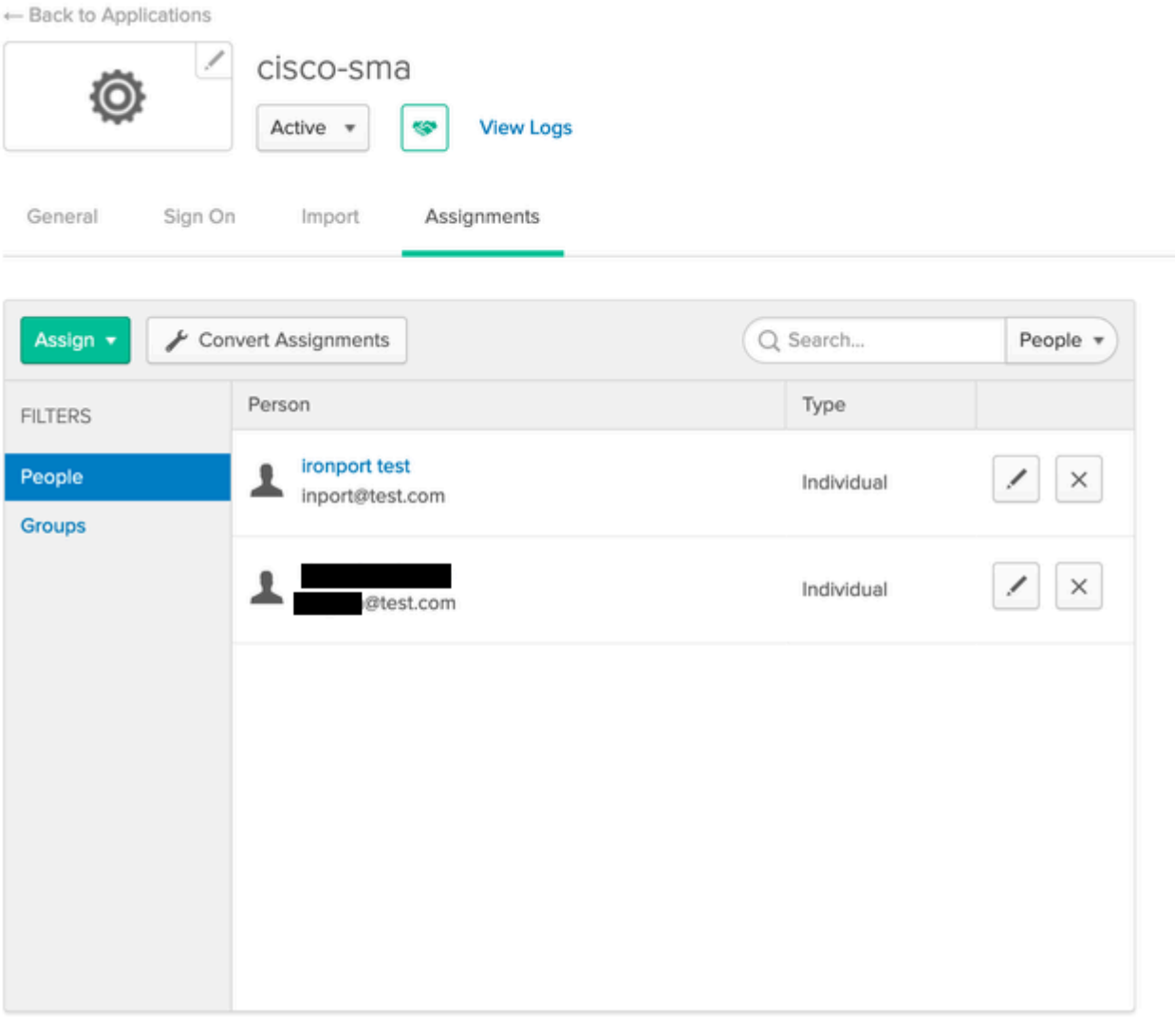
1. Connectez-vous à l'interface Web SMA.
2. Accédez à Administration système > SAML.
3. Sous Identity Provider Settings, importez les métadonnées Okta IdP de la section précédente ou entrez les valeurs manuellement.



Affecter des utilisateurs à l'application Okta

Pour permettre aux utilisateurs de s'authentifier auprès de SMA EUQ via Okta, affectez des utilisateurs ou des groupes à l'application Okta :

1. Dans Okta, ouvrez l'application que vous avez créée.
2. Accédez à Affectations > Personnes, puis sélectionnez Affecter.
3. Sélectionnez Assign en regard de chaque utilisateur, puis sélectionnez Done.



Affectation d'utilisateurs dans Okta Portal

Remarque : Vous pouvez affecter des utilisateurs manuellement, synchroniser des utilisateurs à partir d'Active Directory ou utiliser une autre intégration d'annuaire prise en charge par Okta.

Configurer MFA dans Okta (facultatif)

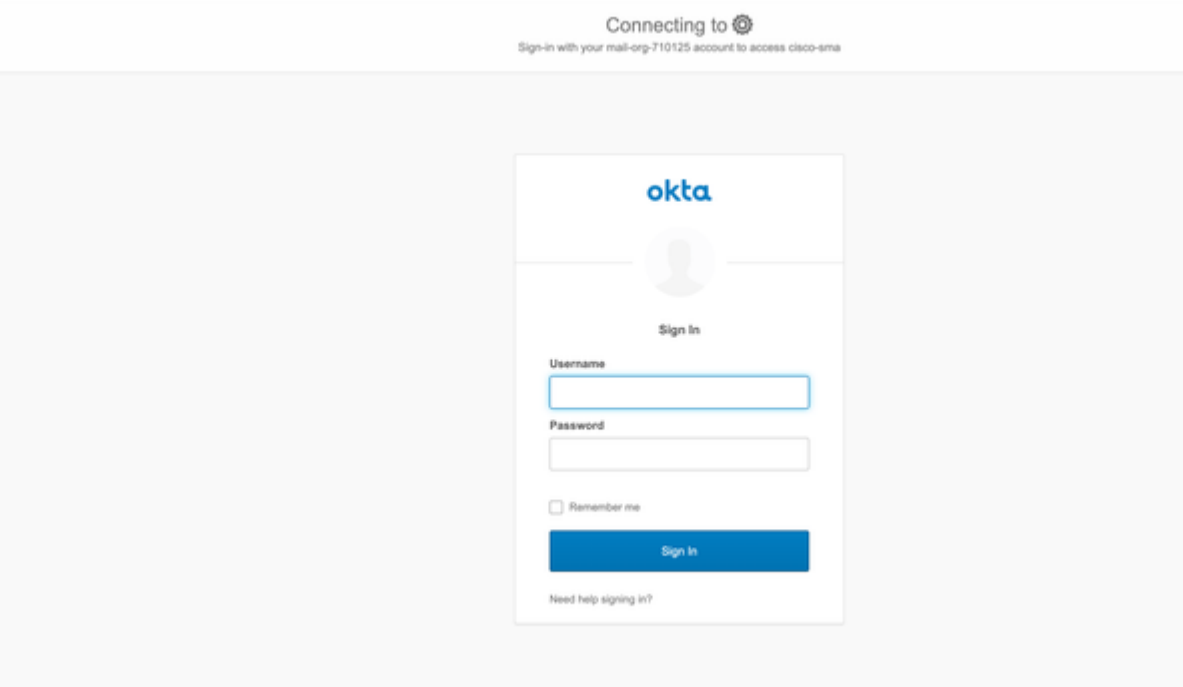
Si vous voulez l'authentification multifacteur (MFA) pour l'accès EUQ, configurez les politiques MFA dans Okta pour l'application :

1. Dans Okta Admin, accédez à Security > Authentication.
2. Configurez les facteurs requis, par exemple, Okta Verify, Google Authenticator ou SMS, et appliquez la stratégie à l'application SMA EUQ.

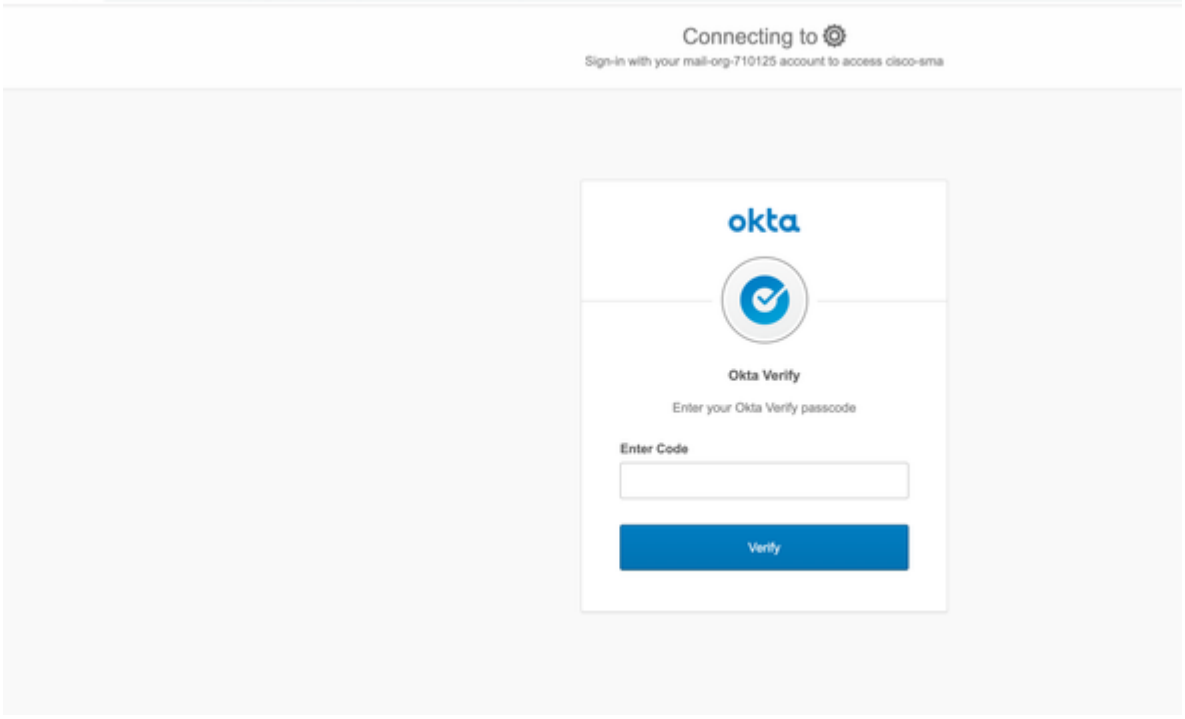
Vérification de la connexion SAML

Résultat prévu : Pour vérifier la configuration, procédez comme suit :

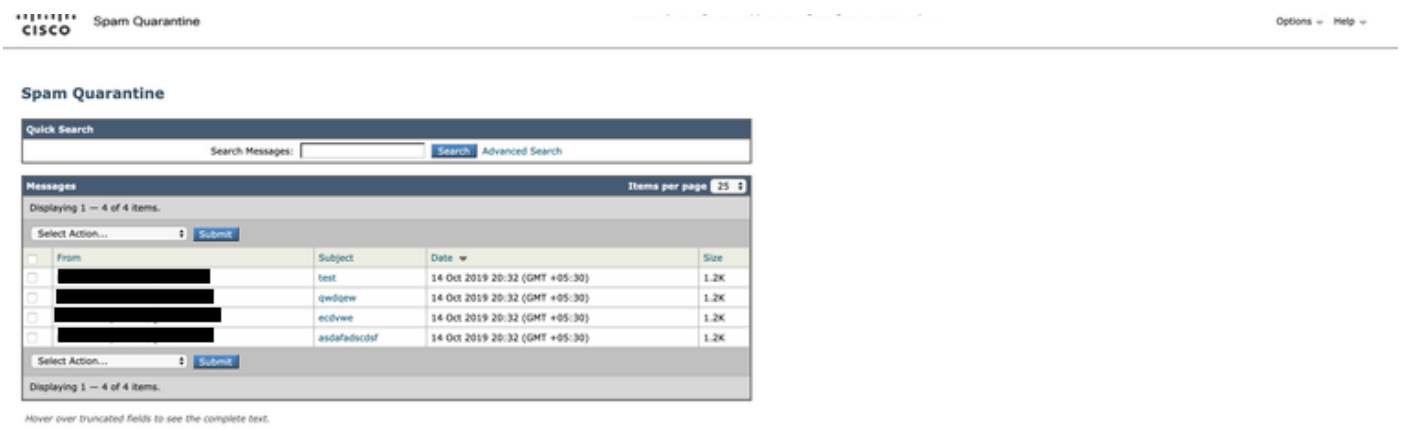
1. Accédez à l'URL de votre EUQ SMA, par exemple, https://<sma-fqdn>:<port>/.
2. Vérifiez que le navigateur redirige vers Okta pour l'authentification.
3. Si l'AMF est activée, terminez la demande d'AMF.
4. Vérifiez que vous êtes redirigé vers le portail de quarantaine du spam SMA et que vous pouvez accéder aux fonctions de quarantaine.



Connexion en utilisant Okta



Entrez le code de vérification Okta



Affichage de la quarantaine du spam après la connexion à Okta

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.