Configura SSO Okta SAML per quarantena utente finale SMA

Sommario

Introduzione

In questo documento viene descritto come configurare Okta come provider di identità SAML 2.0 per l'accesso in quarantena agli utenti finali di Cisco Secure Email SMA.

Prerequisiti

- Prodotto: Cisco Secure Email Security Management Appliance (SMA)
- Funzionalità: SSO SAML per quarantena utente finale (EUQ)
- Provider di identità: Okta (SAML 2.0)
- Si applica a: Distribuzioni SMA che forniscono accesso EUQ su piattaforme virtuali o hardware. Sostituire i nomi host e le porte di esempio con i valori dell'ambiente.
- Contesto versione: Questa procedura è valida per le versioni SMA che supportano SAML per EUQ. Verificare i campi e le opzioni di menu disponibili nella versione installata.

Nota: Questo documento è incentrato sulla configurazione SAML EUQ SMA. Si fa riferimento all'ESA solo per la generazione di certificati quando SMA non è in grado di generare un certificato autofirmato.

Requisiti

Prima di iniziare, verificare di disporre di:

- Accesso amministrativo all'interfaccia Web SMA.
- Autorizzazioni amministrative in Okta per creare applicazioni SAML 2.0 e assegnare utenti o gruppi.
- Certificato e chiave privata per la configurazione del provider di servizi SMA. Un certificato autofirmato è accettabile per le verifiche.
- Un nome di dominio completo (FQDN) e una porta SMA raggiungibili a cui gli utenti finali possono accedere dai propri browser.
- Valori URL asserzione SAML SMA e ID entità SP (da Amministrazione sistema > SAML dopo aver creato la voce SP).
- Account utente in Okta assegnati all'applicazione Okta.
- Utenti con sincronizzazione delle directory, se la distribuzione utilizza l'integrazione delle directory.

Nota: Okta è un provider di identità di terze parti. In questo documento viene fornita una configurazione di esempio da utilizzare come riferimento per il cliente.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

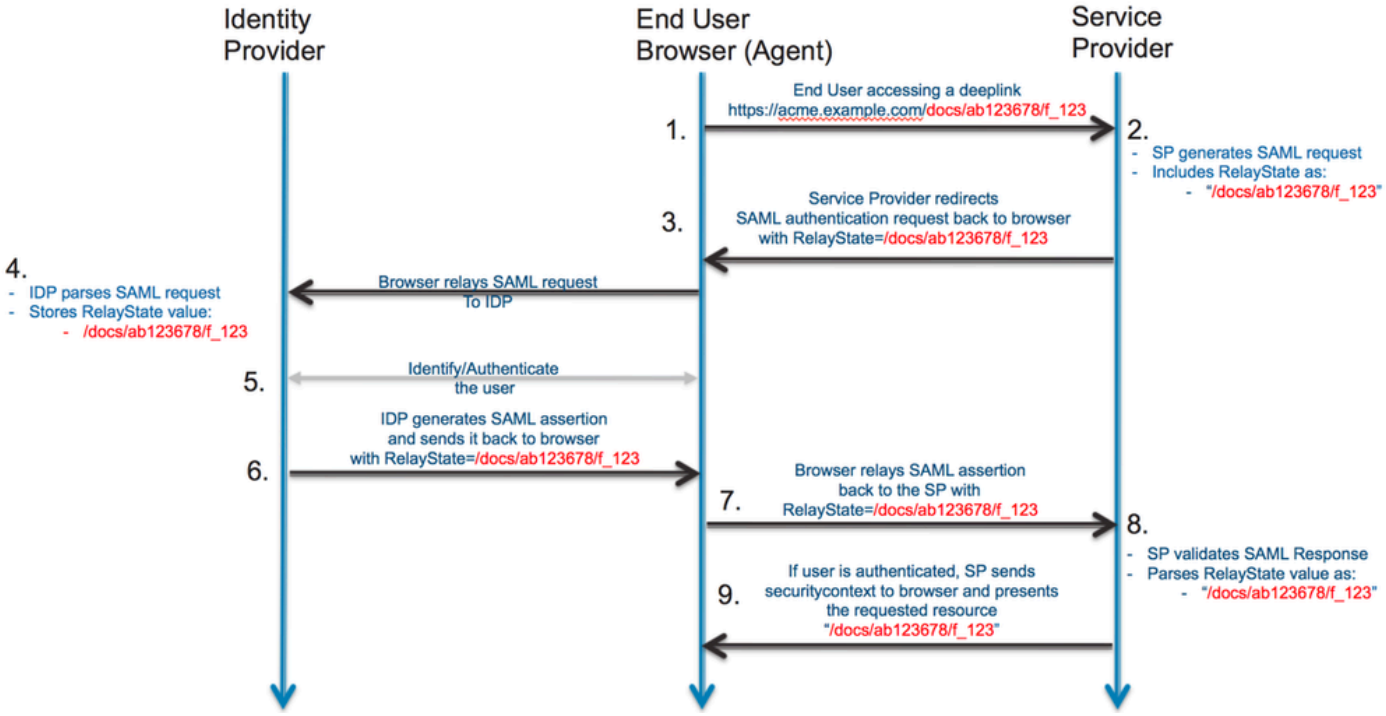
Premesse

L'obiettivo è configurare Single Sign-On (SSO) per il portale di quarantena della posta indesiderata in modo che gli utenti vengano reindirizzati a Okta per autenticare, completare l'autenticazione a più fattori (MFA) se abilitata in Okta e quindi tornare al portale EUQ SMA. Questo documento si applica solo a SMA. Il riferimento a Cisco Secure Email Gateway, in precedenza Email Security Appliance (ESA), è disponibile solo per la generazione di certificati quando SMA non è in grado di generare un certificato autofirmato.

Problema: Gli utenti devono eseguire l'autenticazione al portale di quarantena della posta indesiderata SMA con Okta utilizzando SAML SSO e MFA facoltativo.

Risoluzione: Configurare SMA come provider di servizi, configurare un'applicazione SAML in Okta, importare le impostazioni IdP di Okta in SMA, assegnare gli utenti in Okta e verificare l'accesso.

Flusso SAML:



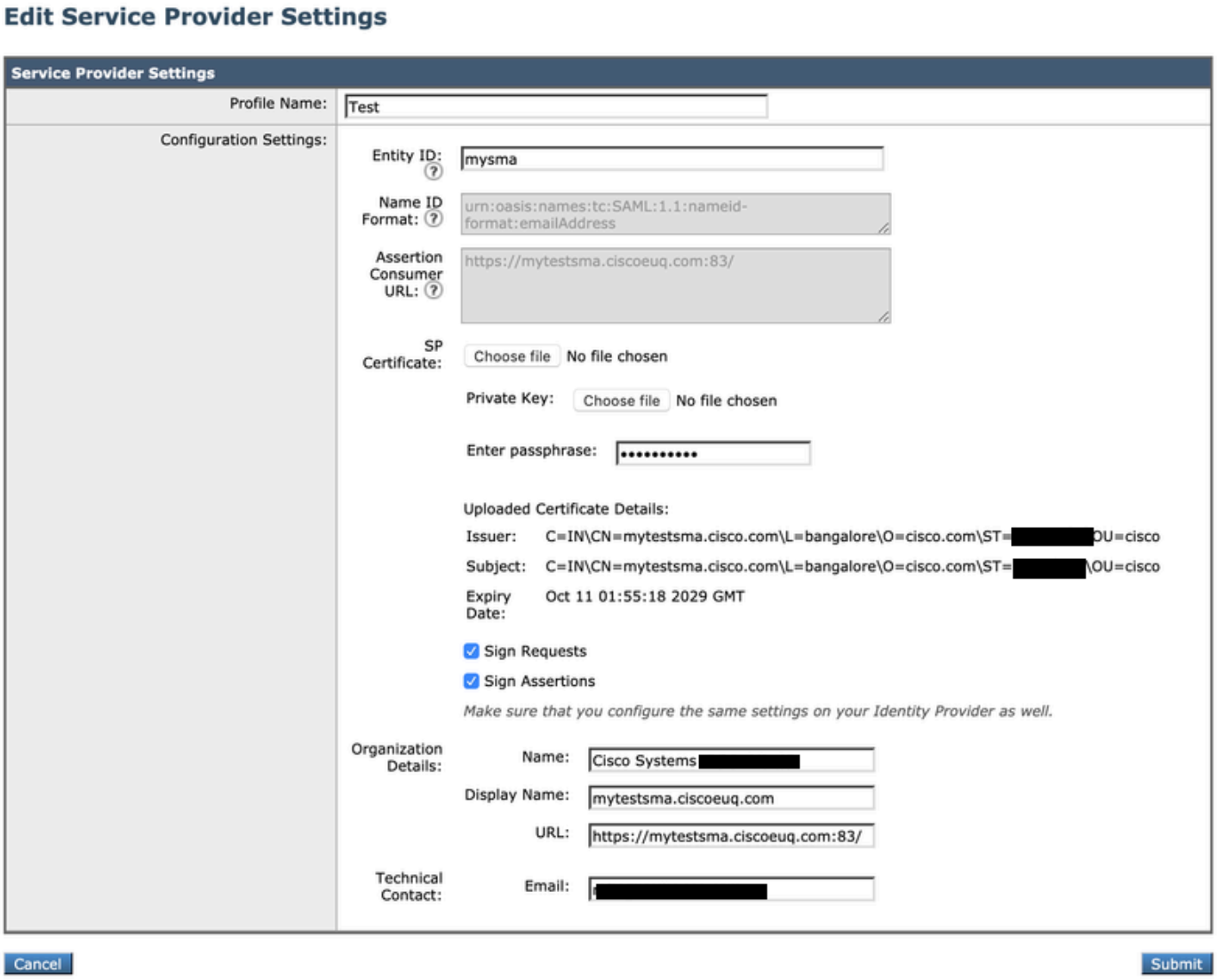
Configurazione

Configurare il provider di servizi (SP) sull'accessorio SMA

Per configurare SMA come provider di servizi SAML per l'accesso EUQ, attenersi alla seguente procedura:

1. Accedere all'interfaccia Web SMA.
2. Passare a Amministrazione sistema > SAML.
3. Selezionare Add Service Provider.
4. In ID entità provider di servizi, immettere l'ID entità che è possibile configurare anche in Okta.
5. Verificare che Formato ID nome e URL ACS (Assertion Consumer Service) siano popolati per l'interfaccia EUQ.
6. In Certificato SP, caricare un certificato per firmare le richieste SAML.

Nota: SMA non è in grado di generare un certificato autofirmato. È inoltre possibile generare un certificato su un'ESA ed esportarlo per utilizzarlo sull'SMA.



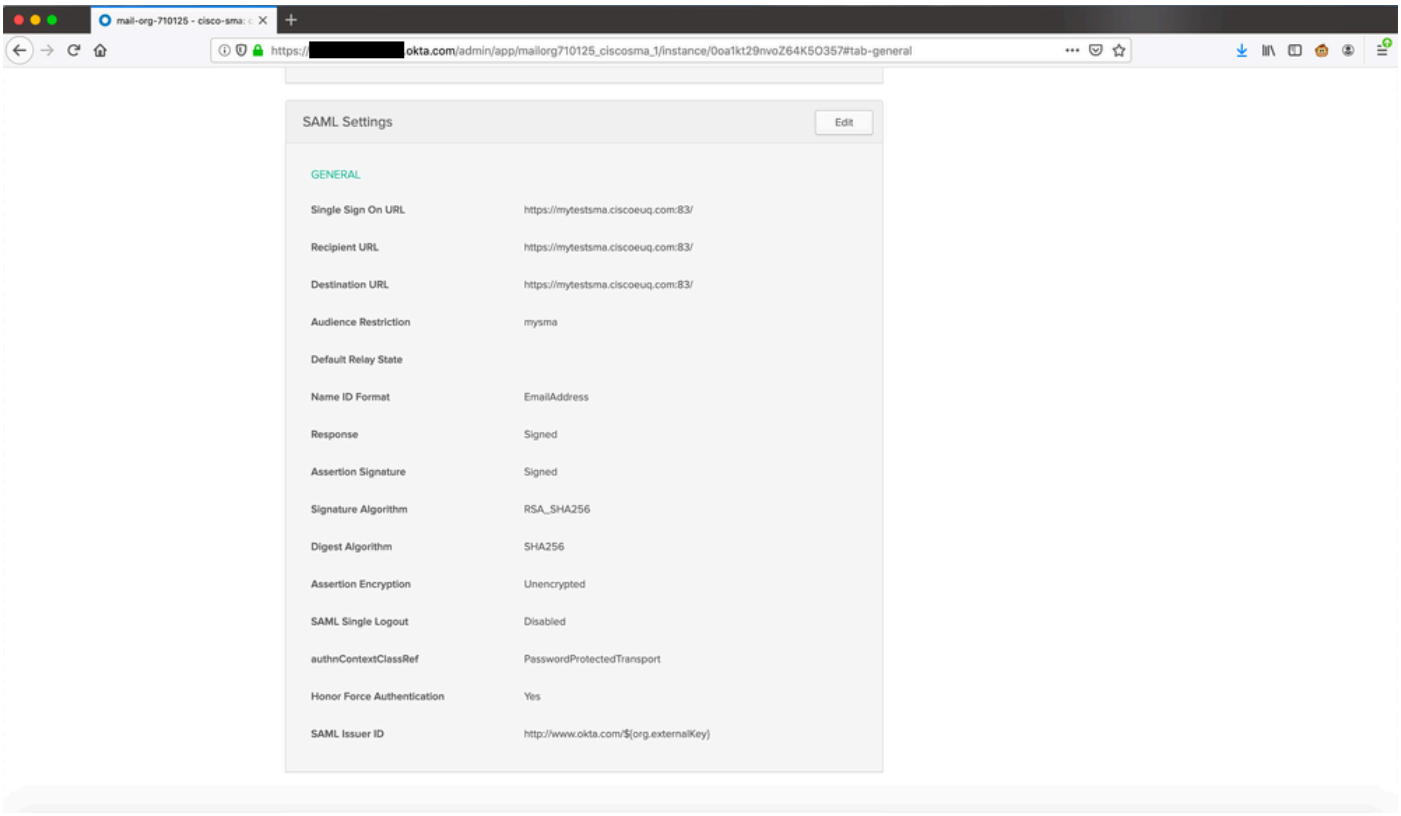
Impostazione di Service Provider nella GUI

Configurazione dell'applicazione SAML in Okta

Per creare un'applicazione SAML 2.0 in Okta per l'accesso EUQ SMA, attenersi alla seguente procedura:

1. Accedere a Okta come amministratore.
2. Passare a Applicazioni > Applicazioni, quindi selezionare Crea integrazione applicazione.
3. Selezionare SAML 2.0, quindi Avanti.
4. Immettere il nome di un'app, ad esempio EUQ SMA, quindi selezionare Avanti.
5. In URL Single Sign-On immettere l'URL ACS SMA dalle impostazioni del provider di servizi SMA.
6. In URI gruppo di destinatari (ID entità SP), immettere lo stesso ID entità configurato nell'SMA.
7. Per Formato ID nome, selezionare EmailAddress.
8. Per Nome utente applicazione, selezionare il formato del nome utente Okta appropriato per la distribuzione.
9. Completare la procedura guidata, quindi aprire la nuova applicazione e copiare il file XML

dei metadati IdP o l'URL dei metadati.

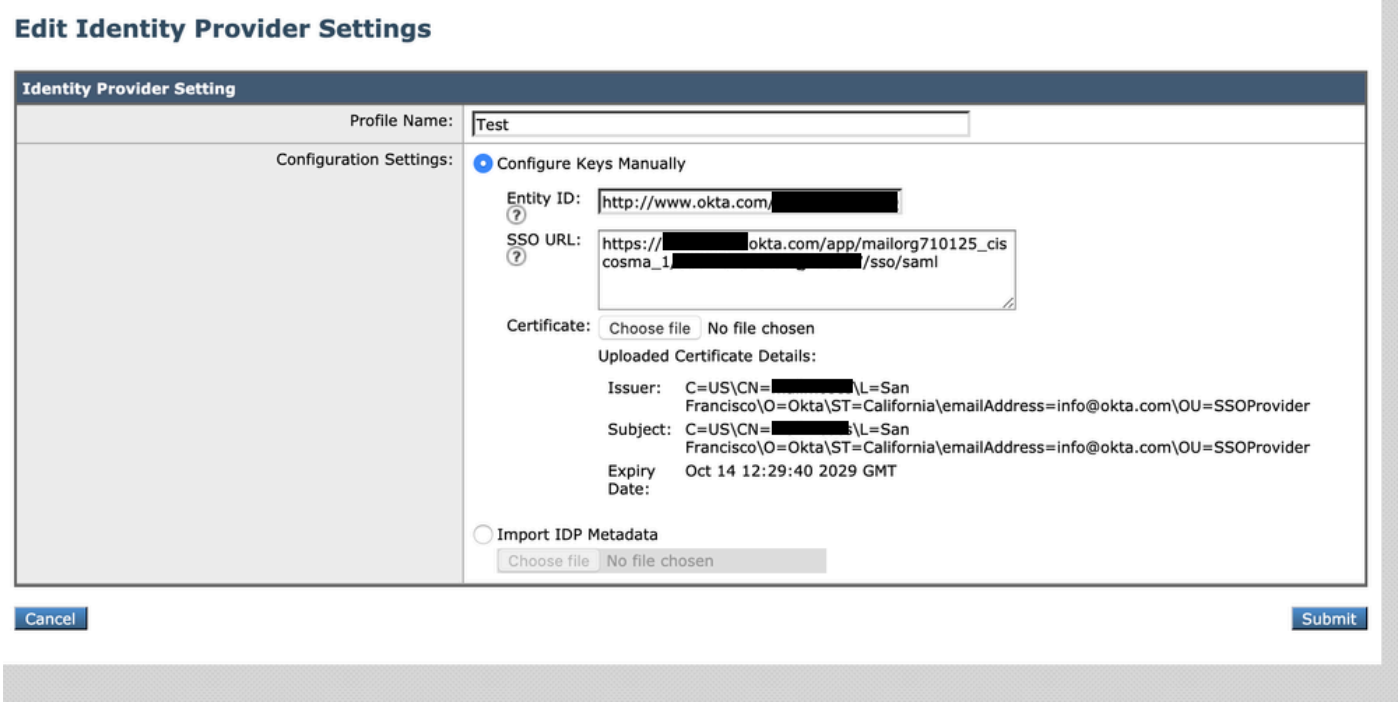


Visualizza portale Okta

Configurare il provider di identità (IdP) nell'accessorio SMA

Per configurare Okta come provider di identità (IdP) nell'SMA, attenersi alla seguente procedura:

1. Accedere all'interfaccia Web SMA.
2. Passare a Amministrazione sistema > SAML.
3. In Impostazioni provider di identità, importare i metadati IdP Okta dalla sezione precedente o immettere i valori manualmente.

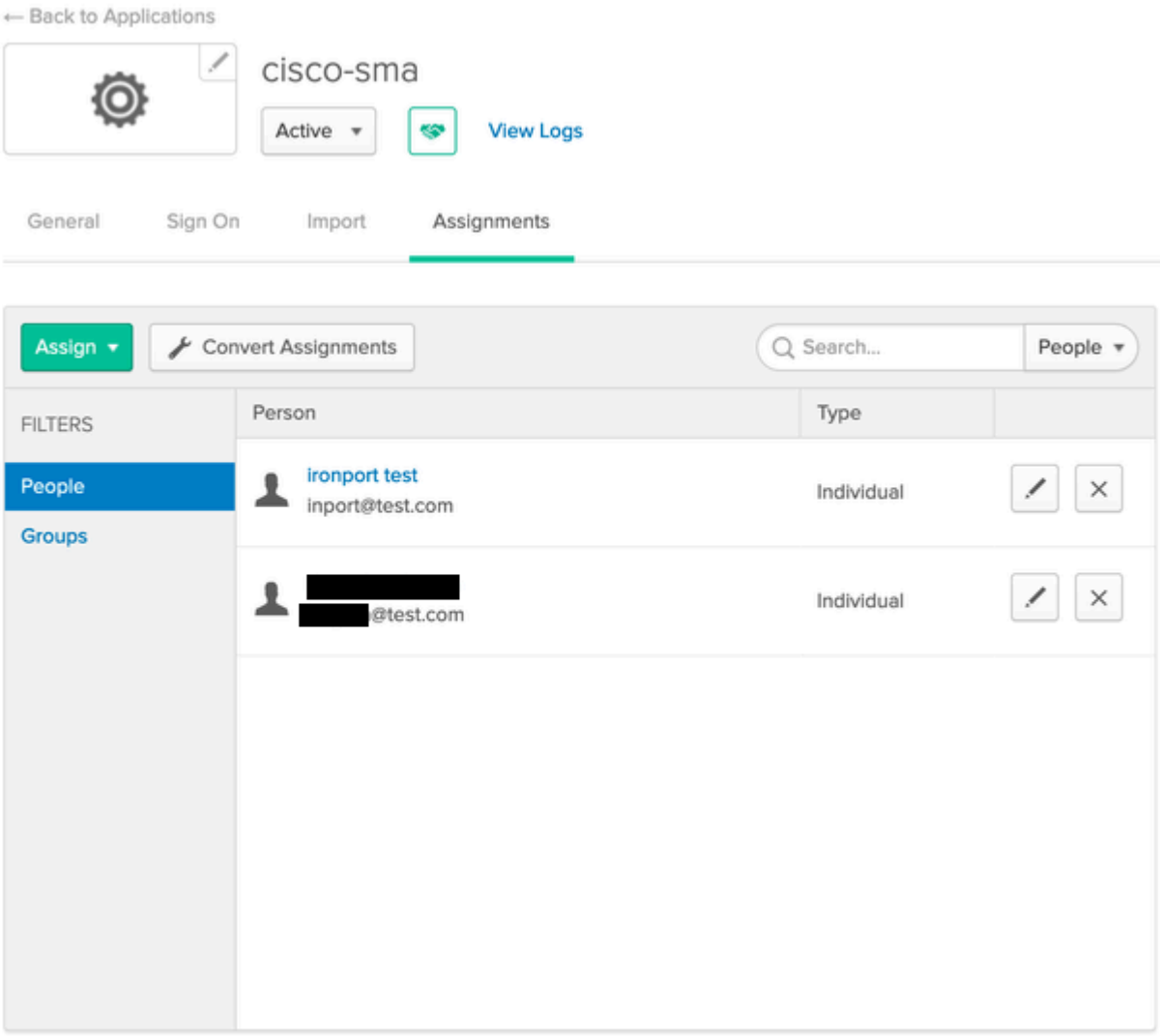


Impostazioni dei profili IdP nell'interfaccia utente di SMA

Assegnazione di utenti all'applicazione Okta

Per consentire agli utenti di eseguire l'autenticazione a EUQ SMA tramite Okta, assegnare gli utenti o i gruppi all'applicazione Okta:

1. In Okta aprire l'applicazione creata.
2. Passare a Assegnazioni > Persone, quindi selezionare Assegna.
3. Selezionare Assegna accanto a ciascun utente, quindi selezionare Fine.



Assegnazione di utenti nel portale Okta

Nota: È possibile assegnare gli utenti manualmente, sincronizzarli da Active Directory o utilizzare un'altra integrazione di directory supportata da Okta.

Configura MFA in Okta (facoltativo)

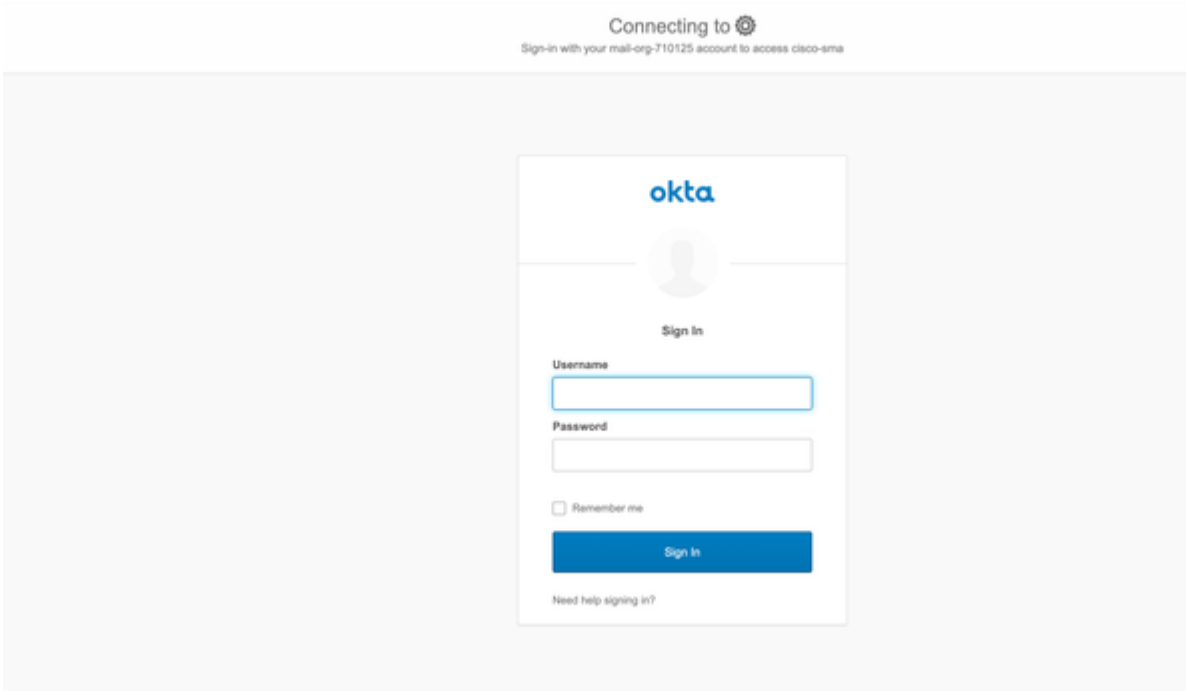
Se si desidera l'autenticazione a più fattori (MFA, Multifactor Authentication) per l'accesso alle EUQ, configurare i criteri MFA in Okta per l'applicazione:

1. In Okta Admin, selezionare Security > Authentication (Sicurezza > Autenticazione).
2. Configurare i fattori richiesti, ad esempio Okta Verify, Google Authenticator o SMS, e applicare il criterio all'applicazione EUQ SMA.

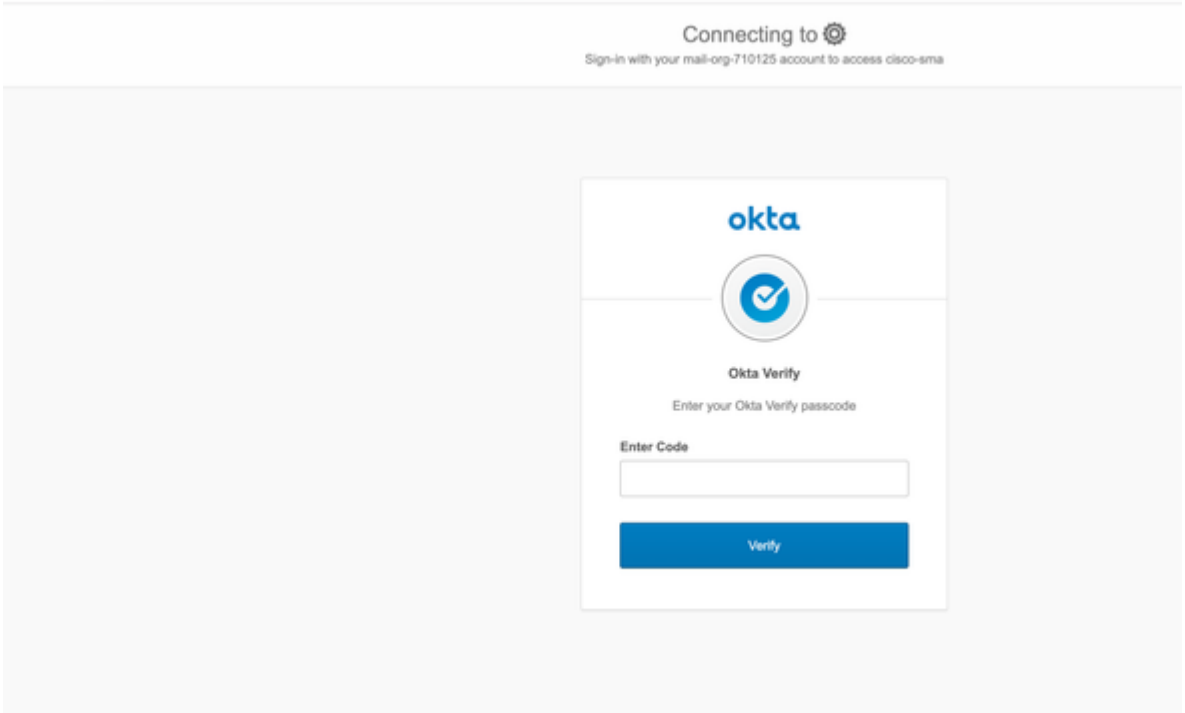
Verifica accesso SAML

Risultato previsto: Per verificare la configurazione, attenersi alla seguente procedura:

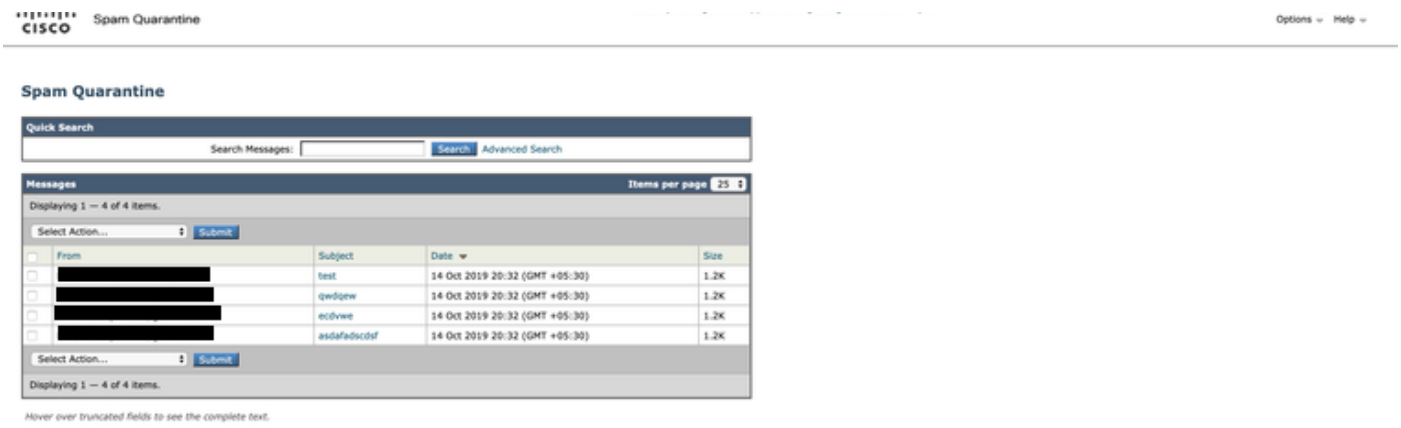
1. Individuare l'URL EUQ SMA, ad esempio https://<sma-fqdn>:<porta>/.
2. Confermare che il browser reindirizzi a Okta per l'autenticazione.
3. Se l'autenticazione a più fattori è abilitata, completare la richiesta di autenticazione a più fattori.
4. Confermare di essere reindirizzati al portale di quarantena della posta indesiderata SMA e di poter accedere alle funzioni di quarantena.



Accesso con Okta



Immetti il codice per la verifica Okta



Visualizzazione della quarantena della posta indesiderata dopo l'accesso con Okta

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).