

Configura autenticazione esterna OKTA SSO per CRES

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Premesse](#)

[Requisiti](#)

[Configurazione](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione esterna OKTA SSO per l'accesso al servizio Cisco Secure Email Encryption (Registered Envelope).

Prerequisiti

Accesso come amministratore al servizio Cisco Secure Email Encryption (Registered Envelope).

Accesso come amministratore a OKTA.

Certificati SSL X.509 autofirmati o firmati dalla CA (facoltativi) in formato PKCS #12 o PEM (forniti da OKTA).

Premesse

- Cisco Secure Email Encryption Service (Registered Envelope) consente di eseguire l'accesso SSO per gli utenti finali che utilizzano SAML.
- OKTA è un programma di gestione delle identità che fornisce servizi di autenticazione e autorizzazione alle applicazioni.
- È possibile impostare Cisco Secure Email Encryption Service (Registered Envelope) come applicazione connessa a OKTA per l'autenticazione e l'autorizzazione.
- SAML è un formato di dati standard aperto basato su XML che consente agli amministratori di accedere senza problemi a un set definito di applicazioni dopo l'accesso a una di tali applicazioni.
- Per ulteriori informazioni su SAML, vedere: [Informazioni generali su SAML](#)

Requisiti

- Account amministratore del servizio Cisco Secure Email Encryption (Registered Envelope).
- Account amministratore OKTA.

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.

Configurazione

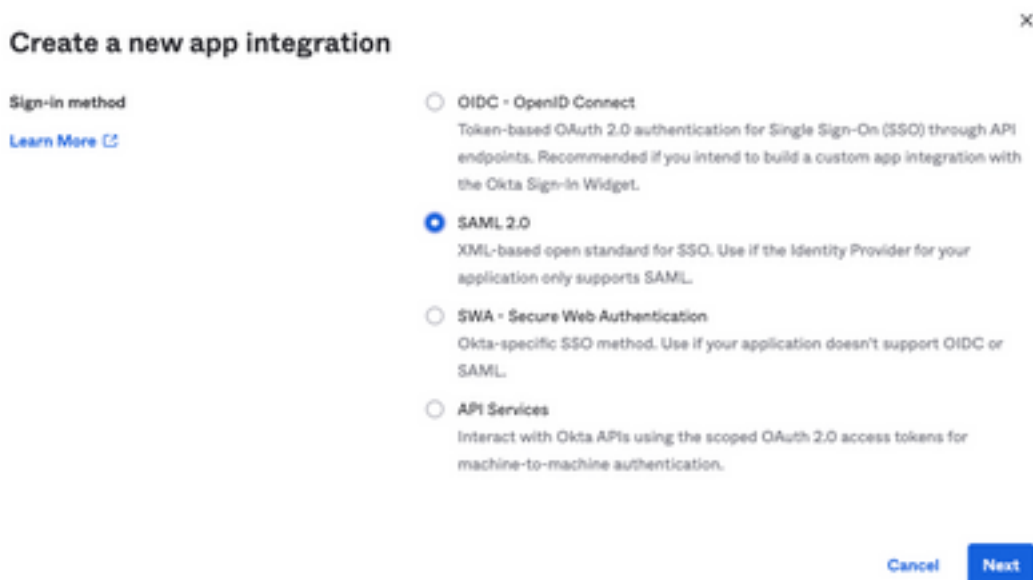
Sotto Okta.

1. Passare al portale delle applicazioni e selezionare **Create App Integration**, come mostrato nell'immagine:

Applications




2. Selezionare **SAML 2.0** come tipo di applicazione, come illustrato nell'immagine:



3. Inserire il nome dell'app **CRES** e selezionare **Next**, come mostrato nell'immagine:

1 General Settings

App name

App logo (optional) 

App visibility Do not display application icon to users


[Cancel](#) [Next](#)


4. Nell'ambito del SAML settings, riempire gli spazi vuoti, come mostrato nell'immagine:


- URL Single Sign-On: questo è il servizio consumer di asserzione ottenuto dal servizio Cisco Secure Email Encryption.
- URI gruppo di destinatari (ID entità SP): ID entità ottenuto dal servizio Cisco Secure Email Encryption.
- Formato ID nome: mantienilo come Non specificato.
- Nome utente applicazione: email, che richiede all'utente di inserire il proprio indirizzo email nel processo di autenticazione.
- Aggiorna nome utente applicazione in: Crea e aggiorna.


A SAML Settings


General

Single sign on URL 
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) 

Default RelayState 
If no value is set, a blank RelayState is sent

Name ID format 

Application username 

Update application username on

[Show Advanced Settings](#)

Scorri fino a Group Attribute Statements (optional), come mostrato nell'immagine:

Immettere l'istruzione dell'attributo successiva:

- Nome: group
- Formato nome: Unspecified
- Filtro: Equals e OKTA

Group Attribute Statements (optional)

| Name | Name format (optional) | Filter |
|-------|---------------------------|---------------|
| group | Unspecified ▾ | Equals ▾ OKTA |

Seleziona Next .


5. Quando gli viene chiesto di Help Okta to understand how you configured this application, immettere il motivo applicabile all'ambiente corrente, come mostrato nell'immagine:

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

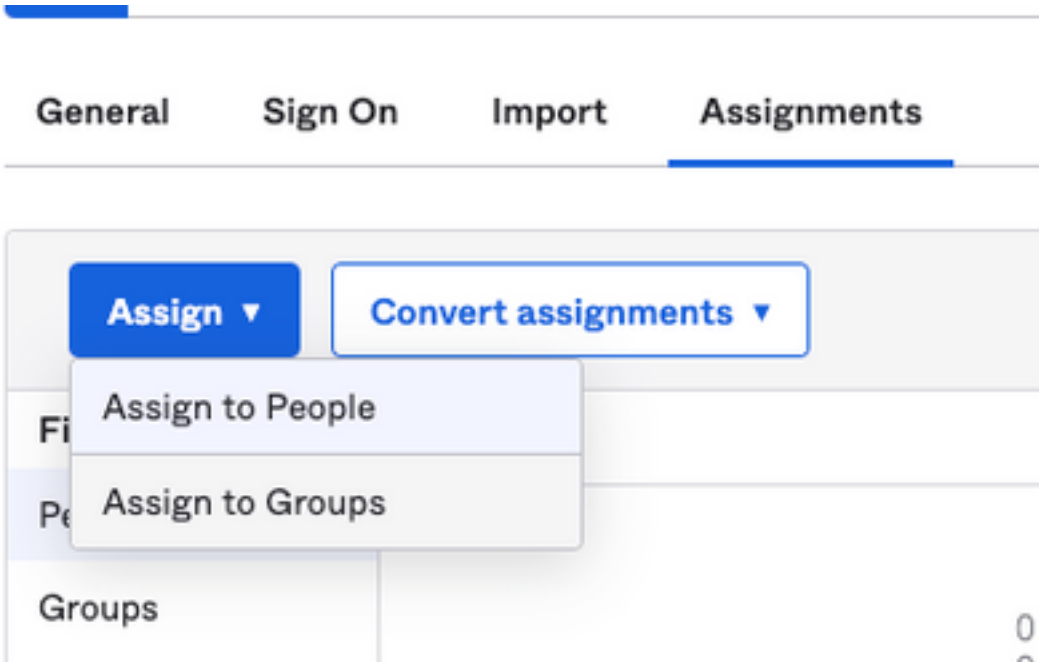
I'm a software vendor. I'd like to integrate my app with Okta

 Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

[Previous](#) [Finish](#)

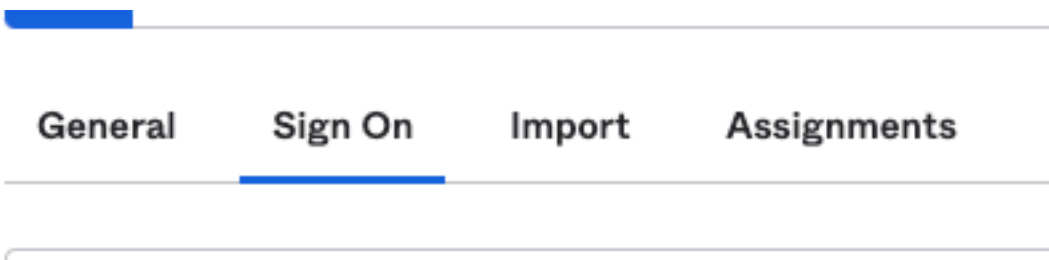
Seleziona Finish per procedere al passaggio successivo.

6. Selezionare Assignments , quindi selezionare Assign > Assign to Groups, come mostrato nell'immagine:



7. Selezionare il gruppo OKTA, ovvero il gruppo con gli utenti autorizzati ad accedere all'ambiente.

8. Selezionare Sign On, come mostrato nell'immagine:



9. Scorrere verso il basso e verso l'angolo destro, selezionare il View SAML setup instructions come mostrato nell'immagine:

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

10. Salvare in un blocco note le informazioni successive necessarie per inserire Cisco Secure Email Encryption Service come mostrato nell'immagine:

- URL Single Sign-On del provider di identità

- Emittente provider di identità

- Certificato X.509

The following is needed to configure CRES

1 Identity Provider Single Sign-On URL:

https://

2 Identity Provider Issuer:

http://www.okta.com/

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----

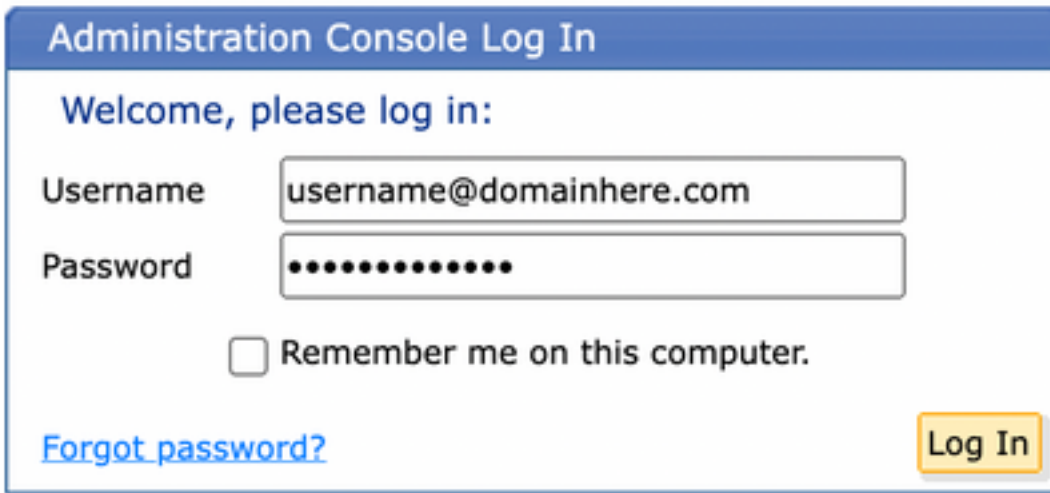
-----END CERTIFICATE-----

[Download certificate](#)

11. Dopo aver completato la configurazione dell'OKTA, è possibile tornare al servizio Cisco Secure Email Encryption.

In Cisco Secure Email Encryption Service (Registered Envelope):

1. Accedere al portale dell'organizzazione come amministratore. Il collegamento è: [Cres Administration Portal](#), come mostrato nell'immagine:



Administration Console Log In

Welcome, please log in:

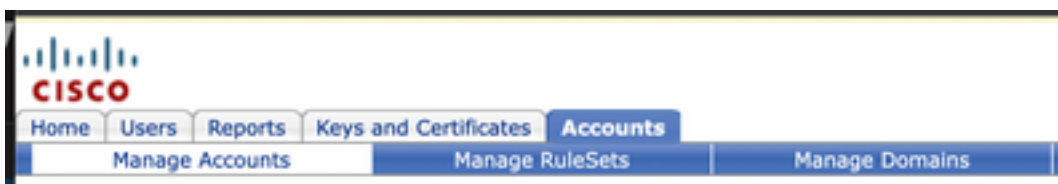
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. Il Accounts , selezionare la scheda Manage Accounts come mostrato nell'immagine:



3. Fare clic su un numero di conto e selezionare il Details come mostrato nell'immagine:



4. Scorri fino a Authentication Method e selezionare SAML 2.0, come mostrato nell'immagine:

Authentication Method

5. Per il SSO Alternate Email Attribute, lasciarla vuota, come mostrato nell'immagine:

SSO Alternate Email Attribute Name

6. Per il SSO Service Provider Entity ID*, inserire <https://res.cisco.com/> , come mostrato nell'immagine:

SSO Service Provider Entity ID*

7. Per il SSO Customer Service URL*, immettere il Identity Provider Single Sign-On URL forniti da Okta, come mostrato nell'immagine:

SSO Customer Service
URL*

https:// .okta.com/app/

8. Ai fini della SSO Logout URL, lasciarla vuota, come mostrato nell'immagine:

SSO Logout URL

9. Per il SSO Identity Provider Verification Certificate, caricare il certificato X.509 fornito da OKTA.

10. Selezionare **save** per salvare le impostazioni, come mostrato nell'immagine:

Save

Back to Accounts List

11. Selezionare **Activate SAML** per avviare il processo di autenticazione SAML e applicare l'autenticazione SSO, come mostrato nell'immagine:

Activate
SAML

Save

Back to
Accounts List

12. Viene visualizzata una nuova finestra che informa che l'autenticazione SAML diventa attiva dopo la riuscita dell'autenticazione con il provider di identità SAML. Seleziona **Continue**, come mostrato nell'immagine:

SAML authentication will be active after a successful authentication with the SAML Identity Provider.
Please click continue to authenticate.

Continue

13. Viene visualizzata una nuova finestra per l'autenticazione con le credenziali OKTA. Immettere il **Username** e selezionare **Next**, come mostrato nell'immagine:



Sign In

Username

Keep me signed in

Next

Help

14. Se il processo di autenticazione ha esito positivo, la SAML Authentication Successful viene visualizzato. Seleziona Continue per chiudere questa finestra, come mostrato nell'immagine:

SAML Authentication Successful.

Please click continue to close.

Continue

15. Confermare la SSO Enable Date viene impostata sulla data e sull'ora in cui l'autenticazione SAML è stata eseguita correttamente, come mostrato nell'immagine:

| | |
|---|---|
| Authentication Method | SAML 2.0 ▾ |
| SSO Enable Date | 10/18/2022 15:21:07 CDT |
| SSO Email Name ID Format | transient |
| SSO Alternate Email Attribute Name | <input type="text"/> |
| SSO Service Provider Entity ID* | <input type="text" value="https://res.cisco.com/"/> |
| SSO Customer Service URL* | <input type="text" value="https:// i.okta.com/app/"/> |
| SSO Logout URL | <input type="text"/> |
| SSO Service Provider Verification Certificate | Download |
| SSO Binding | HTTP-Redirect, HTTP-POST |
| SSO Assertion Consumer URL | https://res.cisco.com/websafe/ssourl |
| Current Certificate | |

Configurazione SAML completata. A partire da questo momento, gli utenti che appartengono all'organizzazione CRES vengono reindirizzati per utilizzare le loro credenziali OKTA quando immettono il loro indirizzo e-mail.

Verifica

1. Passare al [portale del servizio Crittografia e-mail sicura](#). Immettere l'indirizzo e-mail registrato per il CRES, come mostrato nell'immagine:

Secure Email Encryption Service

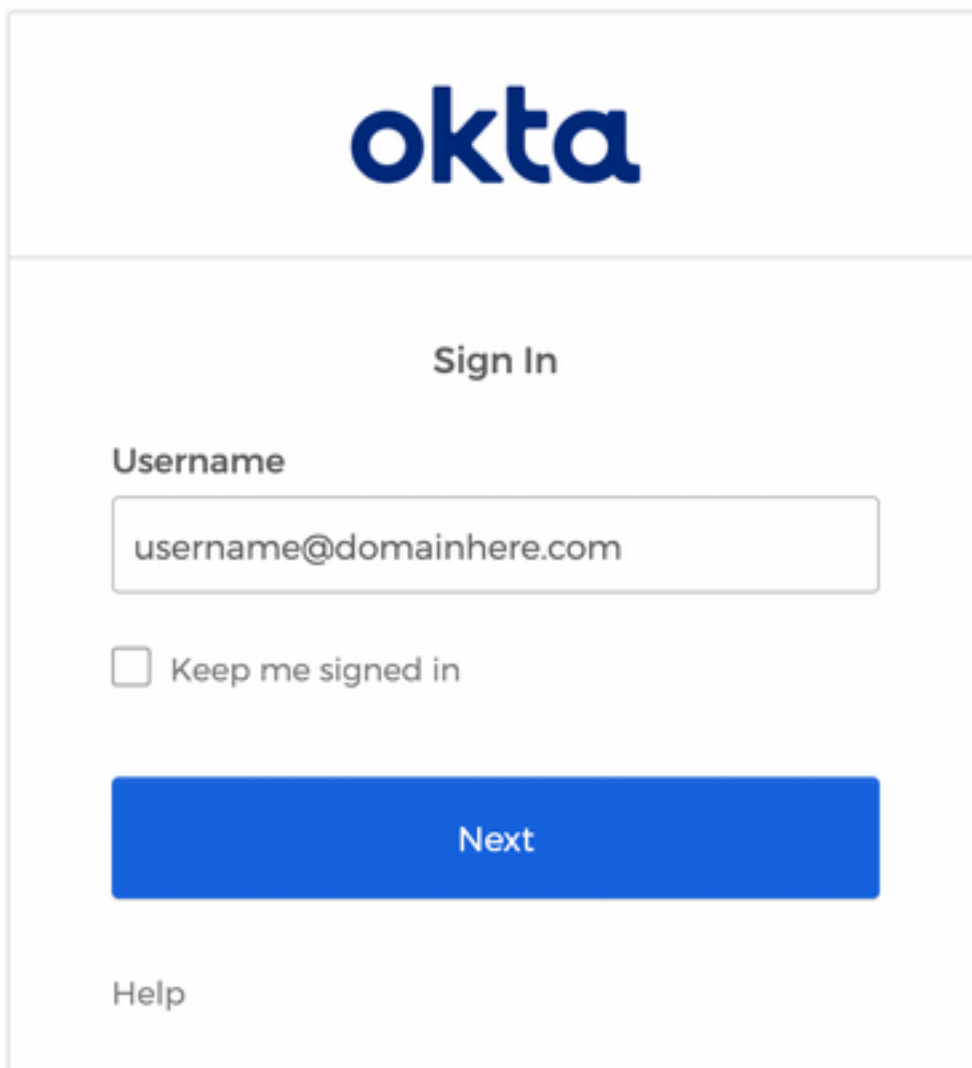
Username*

Log In

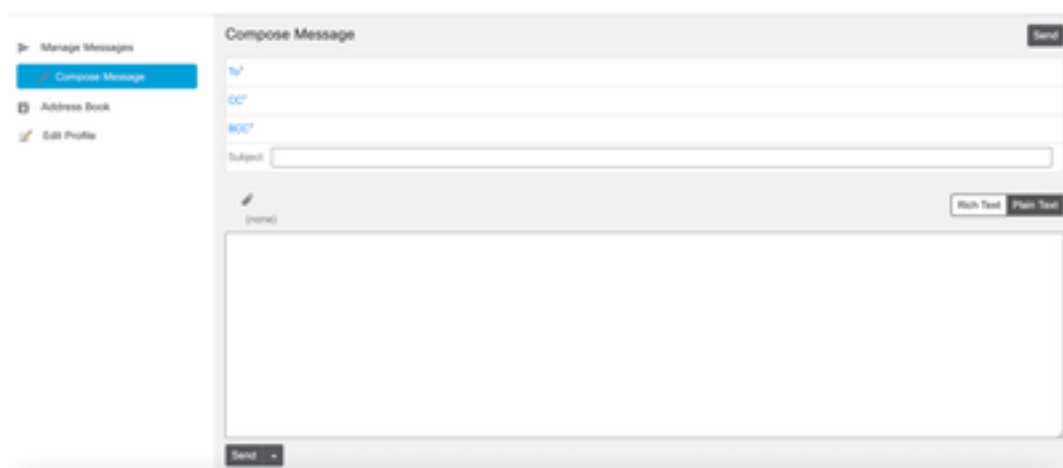
OR

 Sign in with Google

2. Viene visualizzata una nuova finestra per procedere con l'autenticazione OKTA Accedere con le **credenziali OKTA**, come mostrato nell'immagine:



3. Se l'autenticazione ha esito positivo, il servizio Secure Email Encryption apre il Compose Message come mostrato nell'immagine:



Ora l'utente finale può accedere al portale del servizio Secure Email Encryption per comporre messaggi di posta elettronica sicuri o aprire nuove buste con le credenziali OKTA.

Informazioni correlate

[Guida per l'amministratore dell'account di Cisco Secure Email Encryption Service 6.2](#)

[Guide per l'utente finale di Cisco Secure Gateway](#)

[Supporto 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).