Configurazione di OKTA SSO per la quarantena della posta indesiderata per l'utente finale

Sommario

Introduzione

In questo documento viene descritto come configurare OKTA SSO per accedere alla quarantena della posta indesiderata per l'utente finale di Security Management Appliance.

Prerequisiti

- Accesso come amministratore a Cisco Security Management Appliance.
- 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 Security Management Appliance consente l'accesso SSO per gli utenti finali che utilizzano la quarantena della posta indesiderata per l'utente finale e si integra con OKTA, un gestore di identità che fornisce servizi di autenticazione e autorizzazione alle applicazioni. Cisco End User Spam Quarantine può essere impostata come un'applicazione connessa a OKTA per l'autenticazione e l'autorizzazione e che utilizza SAML, un formato di dati standard aperto basato su XML che consente agli amministratori di accedere senza problemi a un set definito di applicazioni dopo aver effettuato l'accesso a una di esse.

Per ulteriori informazioni su SAML, vedere: [Informazioni generali su SAML](#)

Componenti

- Account amministratore cloud Cisco Security Management Appliance.
- Account amministratore OKTA.

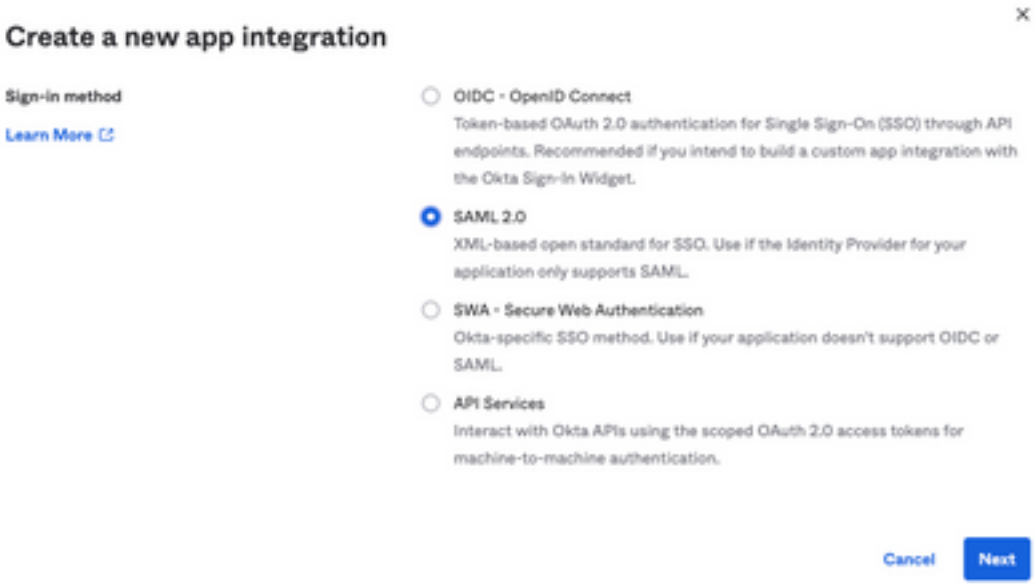
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

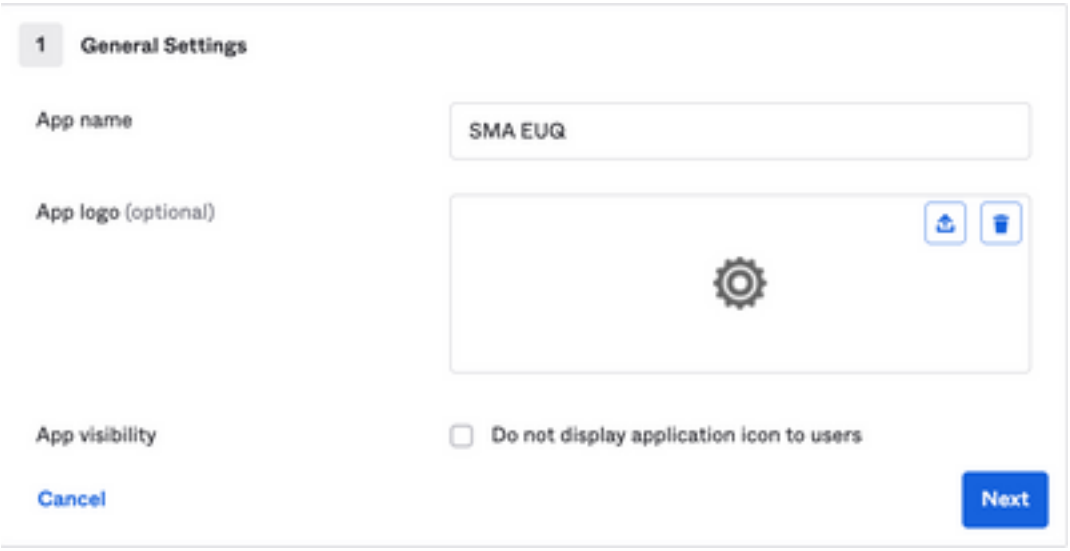
Sotto Okta.

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

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



3. Inserire il nome dell'app SMA EUQ e scegliere Next, come mostrato nell'immagine:



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

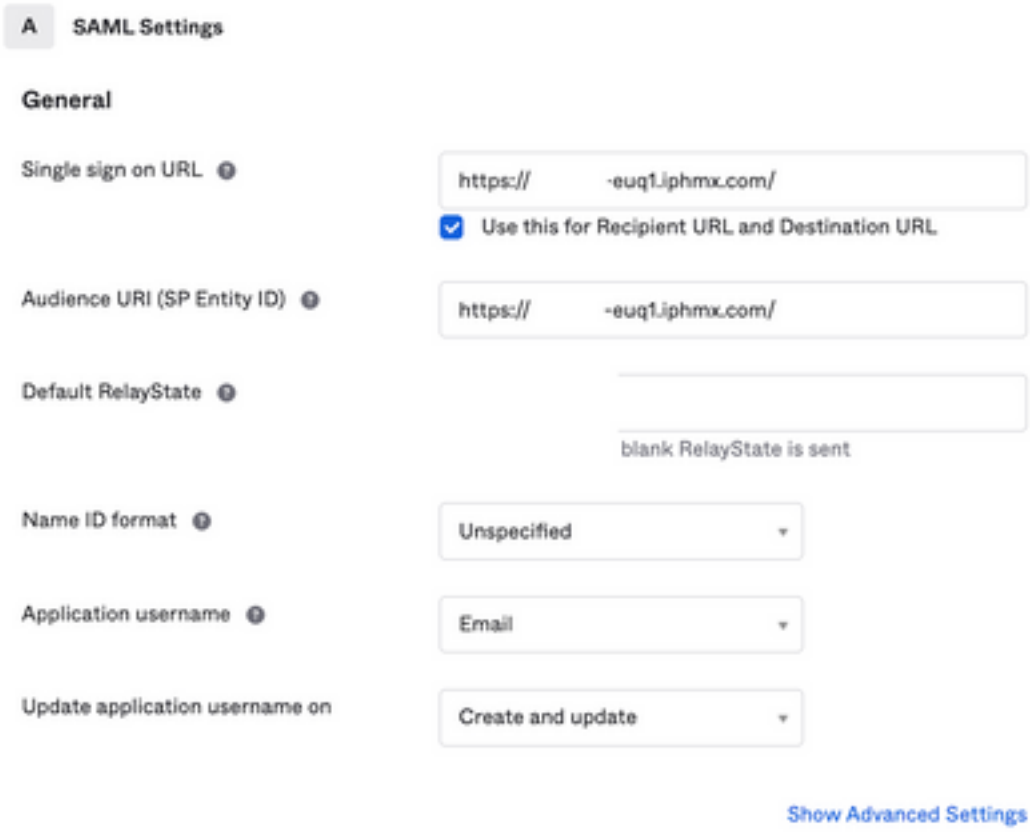
- URL Single Sign-On: servizio consumer di asserzione ottenuto dall'interfaccia EUQ SMA.

- URI gruppo di destinatari (ID entità SP): ID entità ottenuto dall'ID entità EUQ SMA.

- Formato ID nome: mantienilo come Non specificato.

- Nome utente applicazione: indirizzo di posta elettronica che richiede all'utente di immettere il proprio indirizzo di posta elettronica nel processo di autenticazione.

- Aggiorna nome utente applicazione in: Crea e aggiorna.



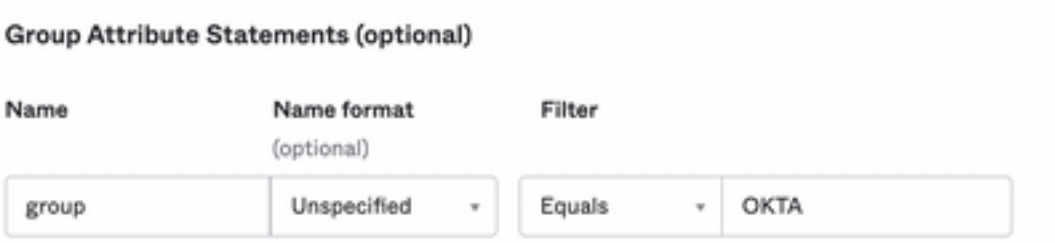
Scorri fino a Group Attibute Statements (optional) , come mostrato nell'immagine:

Immettere l'istruzione dell'attributo successiva:

-Nome: group

- Formato nome: Unspecified

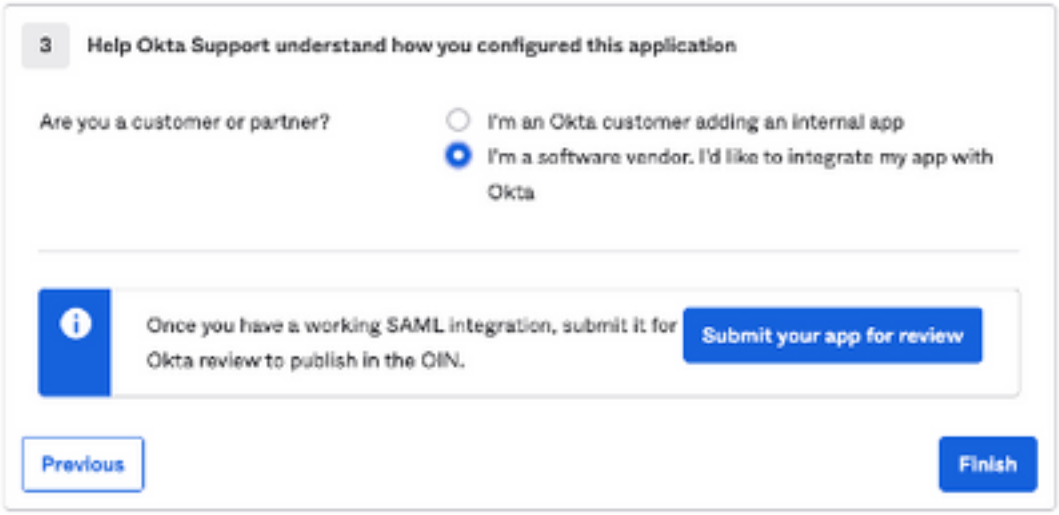
- Filtro: Equals e OKTA



Seleziona Next .

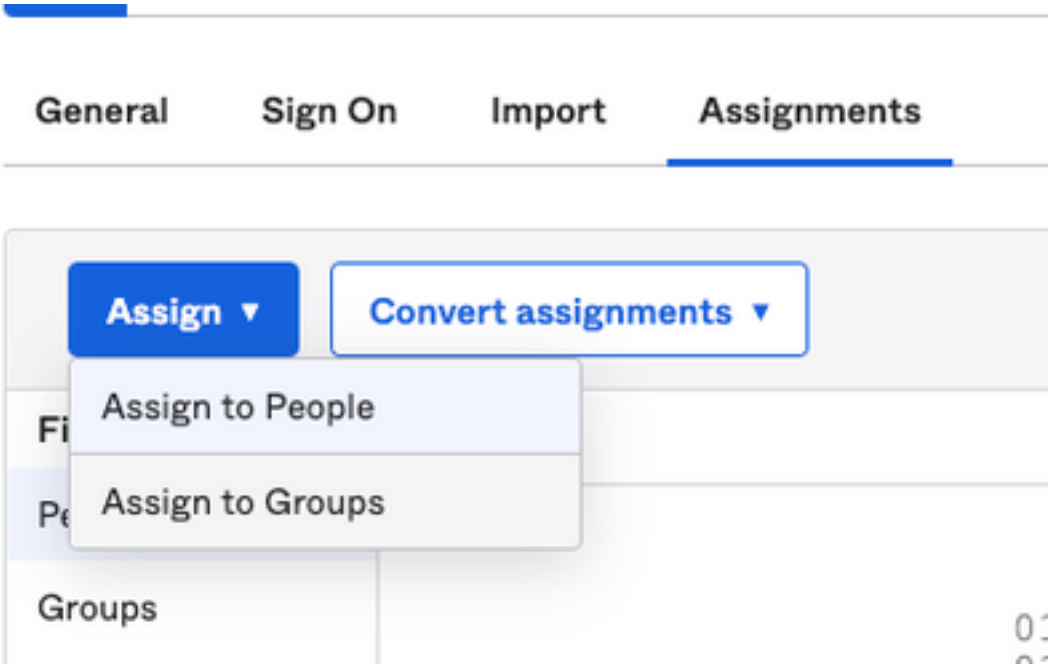
5. Quando gli viene chiesto di Help Okta to understand how you configured this application, immettere il motivo

applicabile all'ambiente corrente, come mostrato nell'immagine:



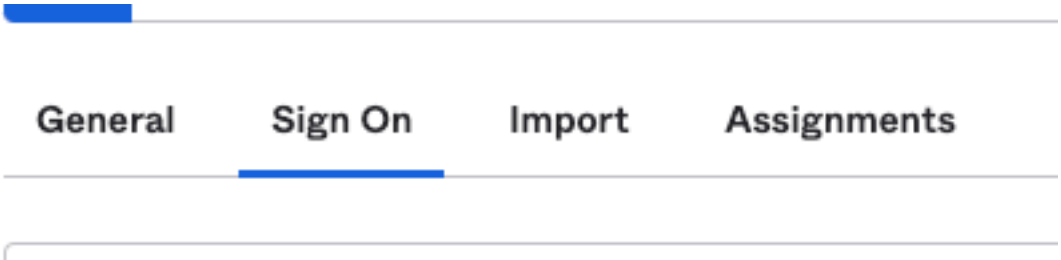
Scegli Finish per procedere al passaggio successivo.

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

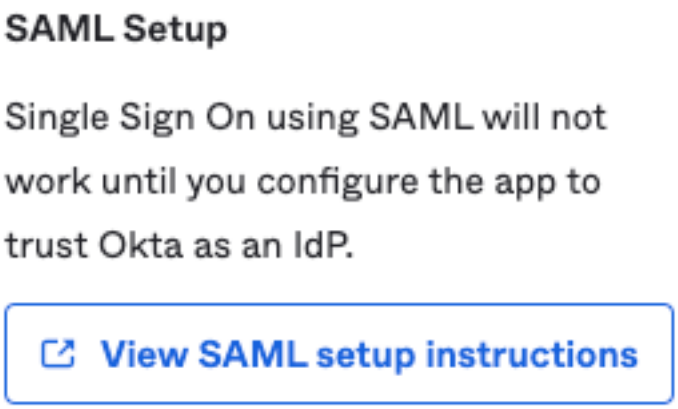


7. Scegliere il gruppo OKTA, ovvero il gruppo con gli utenti autorizzati ad accedere all'ambiente

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



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

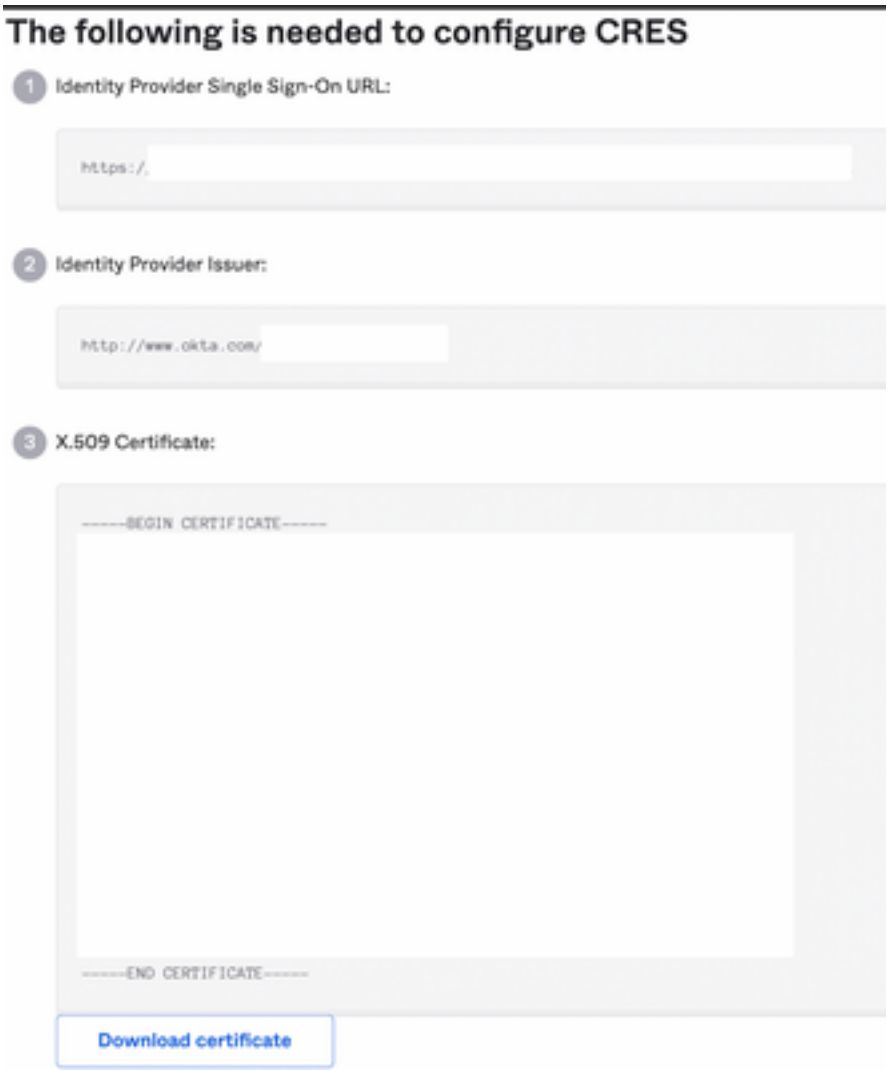


10. Salvare queste informazioni in un blocco note, è necessario inserire nel Cisco Security Management Appliance Configurazione SAML, come mostrato nell'immagine:

- URL Single Sign-On del provider di identità

- Emittente provider di identità

- Certificato X.509

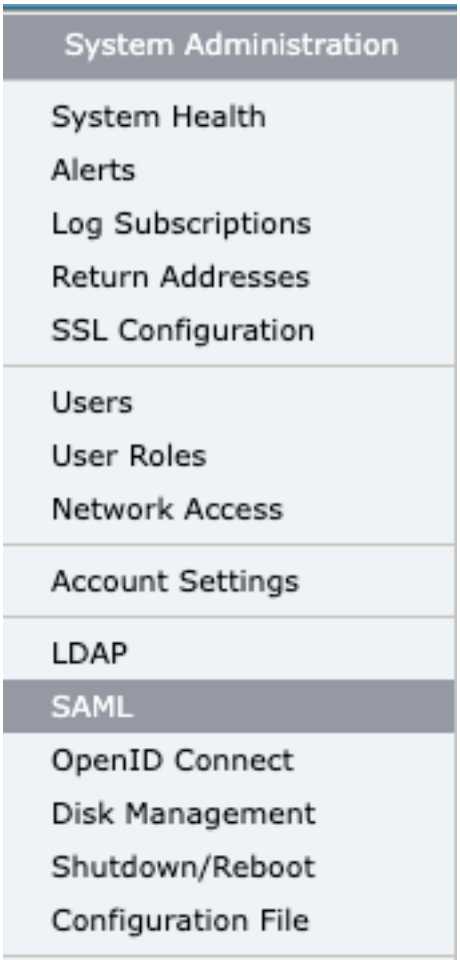


11. Dopo aver completato la configurazione dell'OKTA, è possibile tornare a Cisco Security Management Appliance.

In Cisco Security Management Appliance:

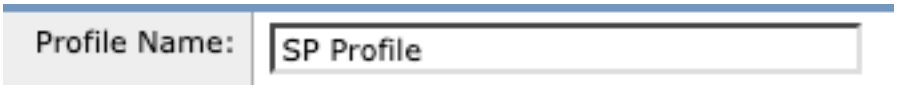
1. Accedere a Cisco Security Management Appliance come amministratore del cloud, come mostrato nell'immagine:

2. Il System Administration, scegliere la scheda SAML come mostrato nell'immagine:



3. Viene visualizzata una nuova finestra per configurare SAML. Inferiore SAML for End-User Quarantine, fare clic Add Service Provider , come mostrato nell'immagine:

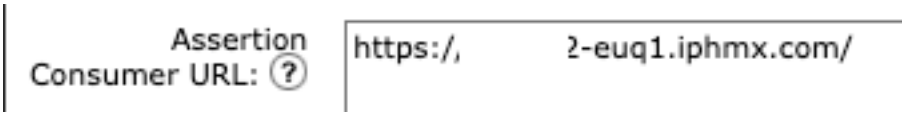
4. Nell'ambito Profile Name , immettere un Nome profilo per il profilo del provider di servizi, come mostrato nell'immagine:



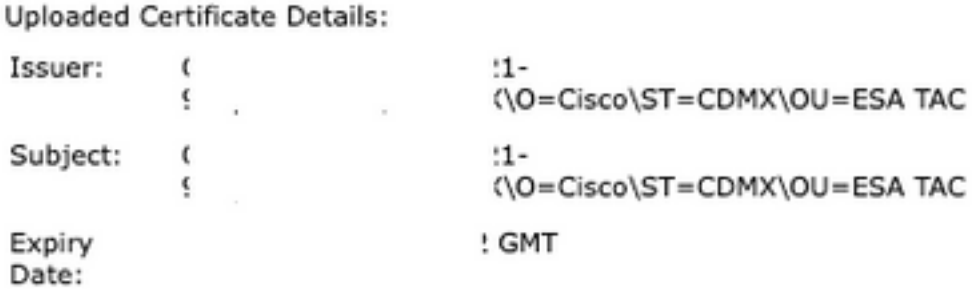
5. Per Entity ID , immettere un nome univoco globale per il provider di servizi (in questo caso, l'accessorio). Il formato dell'ID entità del provider di servizi è in genere un URI, come illustrato nell'immagine:

6. Per **Name ID Format** , questo campo non è configurabile. Questo valore è necessario durante la configurazione del provider di identità, come mostrato nell'immagine:

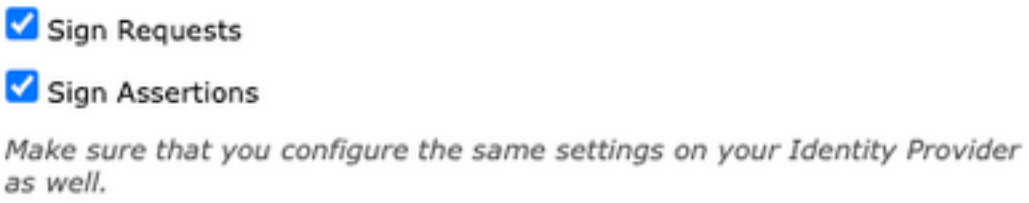
7. Per **Assertion Consumer URL**, immettere l'URL a cui il provider di identità invia l'asserzione SAML dopo il completamento dell'autenticazione. In questo caso, si tratta dell'URL della quarantena.



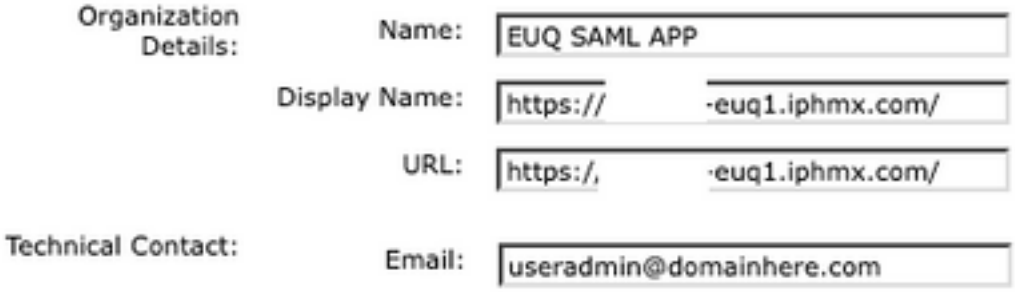
8. Per SP Certificate , caricare il certificato e la chiave oppure caricare il file PKCS #12. Una volta caricato, il Uploaded Certificate Details come mostrato nell'immagine:



9. Per Sign Requests and Sign Assertions , selezionare entrambe le caselle di controllo se si desidera firmare le richieste SAML e le asserzioni. Se si selezionano queste opzioni, assicurarsi di configurare le stesse impostazioni su OKTA, come mostrato nell'immagine:

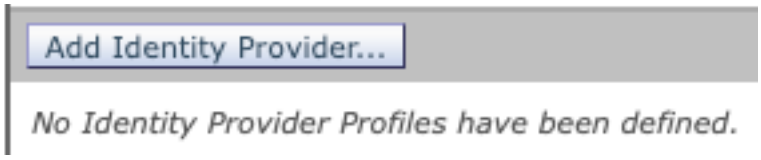


10. Per Organization Details, immettere i dettagli dell'organizzazione, come mostrato nell'immagine:



11. Submit e Commit modifiche prima di procedere alla configurazione Identity Provider Settings .

12. Nell'ambito SAML , fare clic su Add Identity Provider, come mostrato nell'immagine:



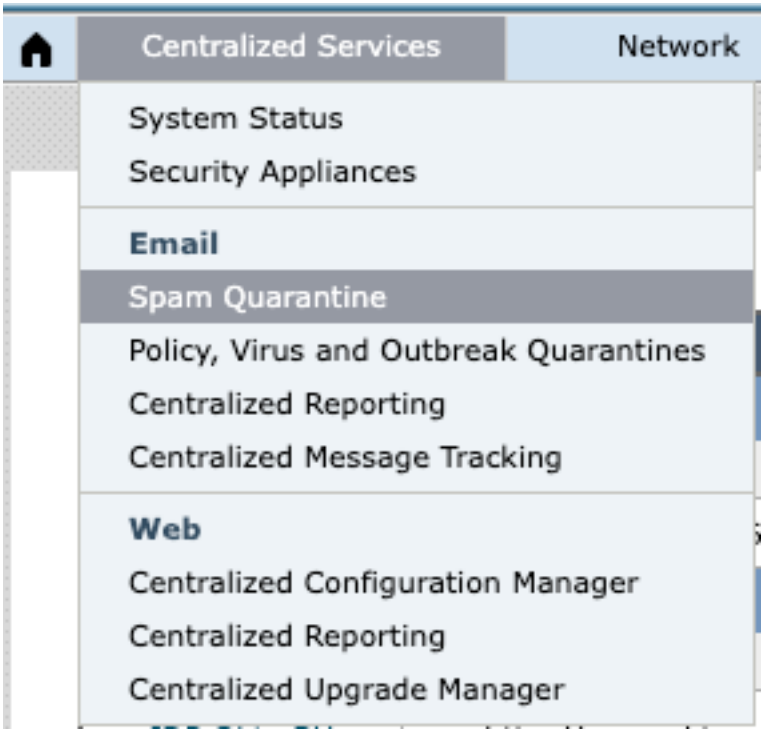
13. Nell'ambito Profile Name: immettere un nome per il profilo del provider di identità, come mostrato nell'immagine:

14. Selezionare Configure Keys Manually e Immettere queste informazioni, come mostrato nell'immagine:

- ID entità: l'ID entità del provider di identità viene utilizzato per identificare in modo univoco il provider di identità. Si ottiene dalle impostazioni OKTA nei passaggi precedenti.
- URL SSO: l'URL al quale l'SP deve inviare le richieste di autenticazione SAML. Si ottiene dalle impostazioni OKTA nei passaggi precedenti.
- Certificato: il certificato fornito da OKTA.

15. Submit e Commit le modifiche per procedere all'attivazione dell'accesso SAML.

16. Nell'ambito Centralized Services > Email , fare clic su Spam Quarantine, come mostrato nell'immagine:



17. Nell'ambito Spam Quarantine -> Spam Quarantine Settings , fare clic su Edit Settings , as shown in the image:

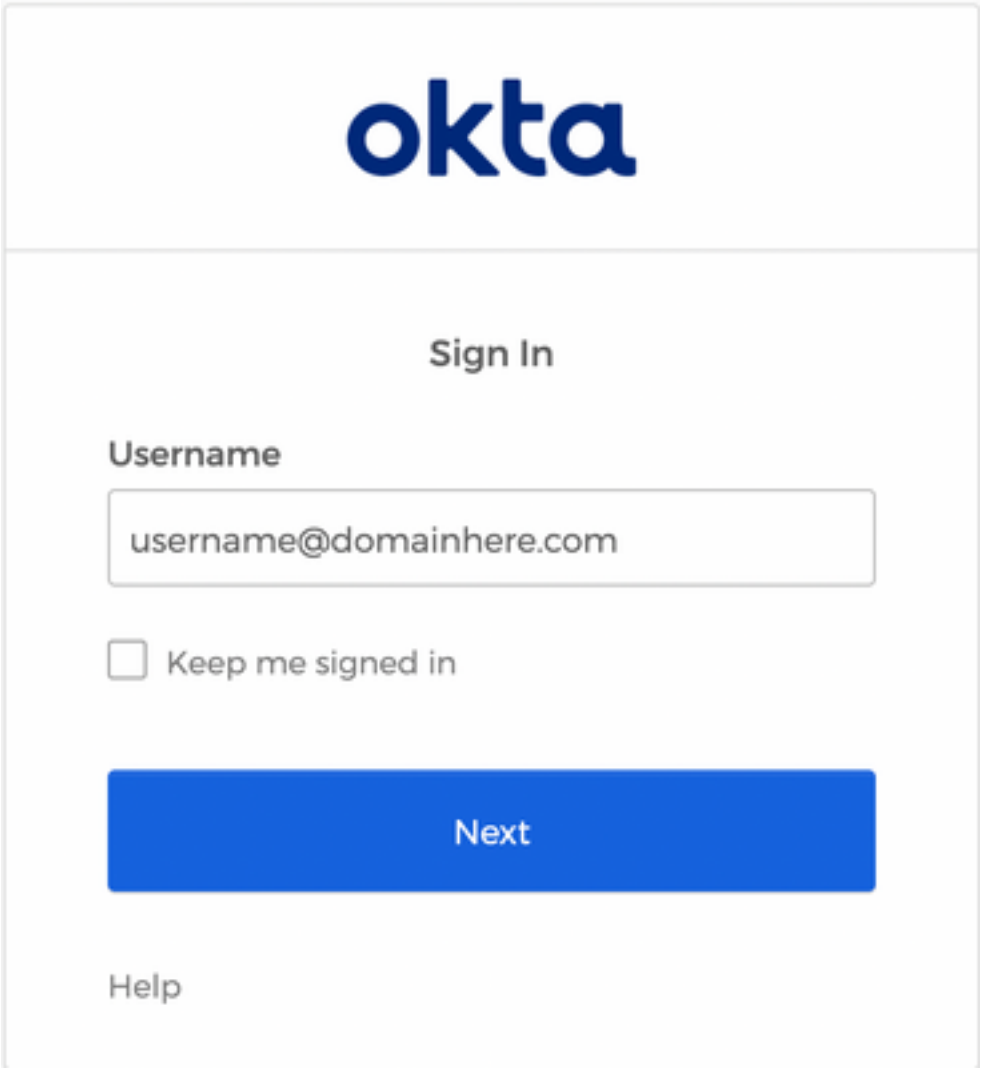
18. Scorri fino a End-User Quarantine Access > End-User Authentication , selezionare SAML 2.0 , come mostrato nell'immagine:

19. Submit e Commit modifiche per abilitare l'autenticazione SAML per **End User Spam Quarantine** .

Verifica

1. In un browser Web, immettere l'URL della quarantena della posta indesiderata per l'utente finale della società, come mostrato nell'immagine:

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, la End User Spam Quarantine apre il contenuto della quarantena per l'utente che accede, come mostrato nell'immagine:

Ora l'utente finale può accedere alla quarantena della posta indesiderata con le credenziali OKTA.

.

Informazioni correlate

Guide per l'utente finale di Cisco Secure Email e Web Manager

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).