Configurazione dell'autenticazione esterna SAML SSO per l'amministrazione di ESA e SMA

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione esterna SSO SAML 2.0 per l'amministrazione del sistema ESA e SMA.

Ambiente

- Prodotti: Email Security Appliance (ESA), Security Management Appliance (SMA)
- Si applica a: Amministrazione dei sistemi ESA e SMA
- Comportamento cluster: I profili Service Provider (SP) e IdP sono configurati a livello di computer; il mapping dell'autenticazione esterna è configurato a livello di cluster.

Prerequisiti

- Accesso amministrativo all’interfaccia web ESA/SMA

- Certificato X.509 e chiave privata disponibili in formato PKCS #12 (PFX) o PEM (autofirmato o con firma CA)
- Accesso a un'applicazione Identity Provider (IdP) di terze parti e al relativo URL SAML di metadati/SSO

Elenco di controllo preconfigurazione

- Verificare il nome host/nome di dominio completo (FQDN) dell'interfaccia di gestione utilizzata dagli amministratori per accedere all'accessorio. verificare che l'URL del servizio consumer di asserzione (ACS) corrisponda a tale nome host.
- Se l'accessorio si trova in un cluster, pianificare la configurazione di SAML a livello di computer per ciascun membro prima di abilitare l'autenticazione esterna SAML.
- Determinare se l'IdP richiede un'applicazione o un'area di autenticazione separata per accessorio.
- Verificare che i certificati e le chiavi richiesti siano disponibili.
- Confermare che l'IdP invia l'attributo di gruppo o di ruolo richiesto per il mapping dei ruoli ESA/SMA.

Attenzione: Questo documento non si applica a SAML SSO di Quarantena utente finale (EUQ).

Premesse

- Cisco TAC non fornisce supporto tecnico per la configurazione dei provider di identità. Per gli IdP comuni vengono forniti riferimenti di configurazione di esempio.

IdP SAML SSO

- Duo Access Gateway (DAG) aggiunge l'autenticazione a due fattori, completa dei servizi cloud più diffusi tramite la federazione SAML 2.0.
- ADFS (Active Directory Federation Services) - testato con ADFS 2,3,4, Azure Active Directory (Azure AD), SecureAUTH e PingFederate
- È possibile utilizzare un'ulteriore autenticazione a due fattori se l'IdP la supporta nel framework SAML 2.0 Single Sign-On.
- Okta supporta l'autenticazione con un IdP che supporta il servizio.

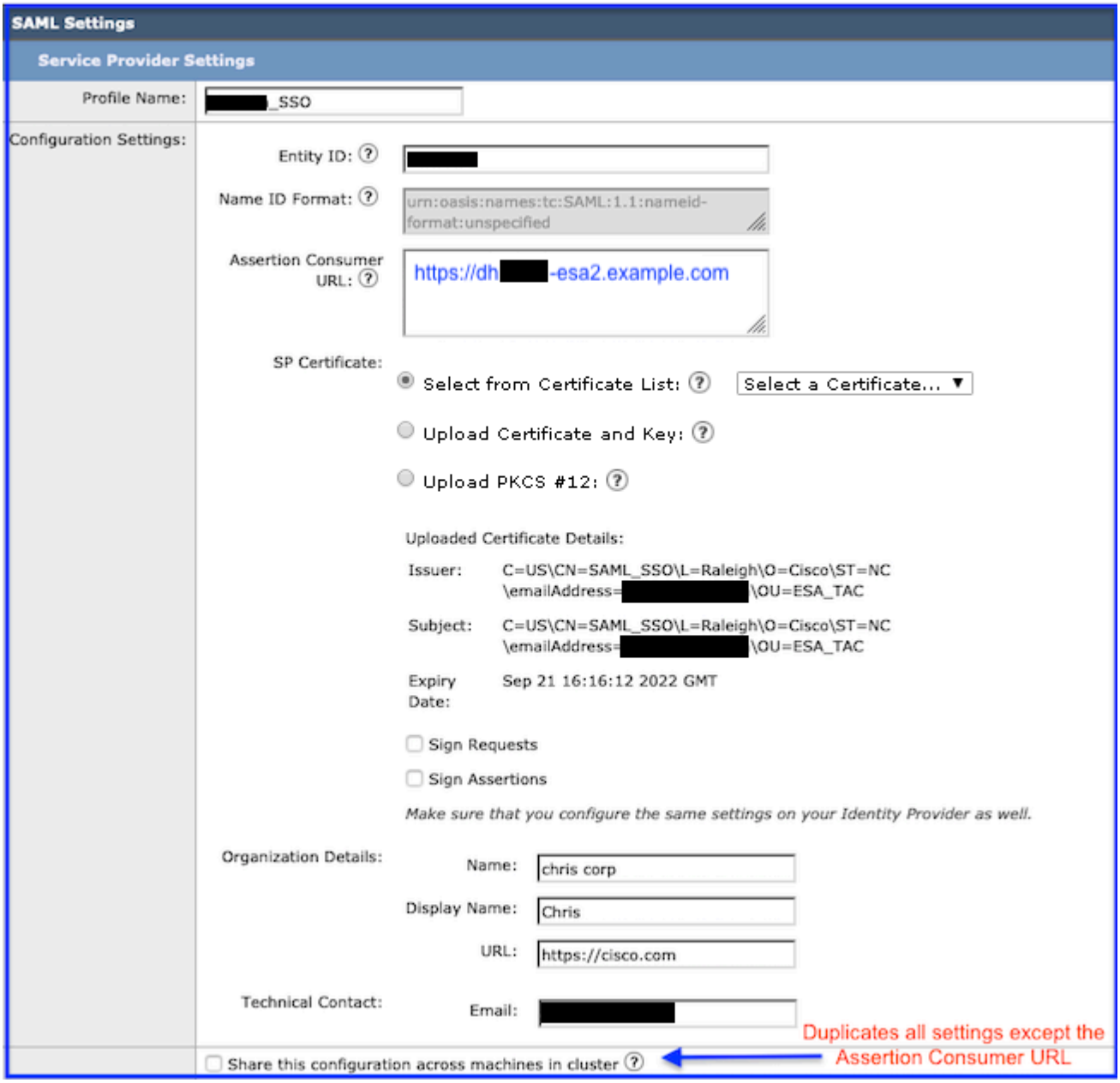
Configurazione di ESA/SMA come provider di servizi

Passare a Amministrazione sistema > SAML > (Livello computer) > Aggiungi provider di servizi.

Nota: Affinché sia possibile abilitare SAML, le ESA in un cluster richiedono una configurazione a livello di computer per tutti i membri del cluster.

- Se l'opzione nella parte inferiore della pagina, Condividi questa configurazione tra computer nel cluster, è selezionata, si applicano le condizioni seguenti:
  - Tutti i campi vengono replicati nei membri del cluster, ad eccezione dell'URL consumer di asserzione.
  - L'URL consumer di asserzione inserisce automaticamente il nome host dell'interfaccia di gestione come ACS.
  - Gli ambienti che utilizzano un nome host alternativo per accedere all'host richiedono la configurazione manuale per ogni host, ad esempio gli accessori ospitati nel servizio Web di registrazione certificati.
  - Nome profilo: Nome utilizzato per etichettare l'istanza SP nell'interfaccia ESA o SMA.
  - ID entità: Nome utilizzato per l'istanza SP così come viene rilevato dall'IdP. Questo nome è l'etichetta utilizzata dall'IdP per rappresentare l'SP. Può essere un nome qualsiasi, ad esempio ESA_SP o ESA_SSO.
  - Formato ID nome: Campo non configurabile.
  - URL consumer asserzione o servizio consumer asserzione (ACS): URL utilizzato dall'IdP per comunicare con questo host ESA/SMA.
  - Certificato SP:
    - Formato: Certificati X.509 pubblici/privati in formato PFX/PKCS12 o PEM.
    - Opzione 1: Selezionare dall'elenco certificati: Selezionare tra i certificati già creati sull'ESA in Rete > Certificati.
    - Opzione 2: Carica certificato e chiave: Caricare un certificato e una chiave in formato PEM.
    - Opzione 3: Upload PKCS #12: Caricare un file PKCS #12.
    - Facoltativo: Creare un certificato autofirmato su ESA/SMA per SAML Single Sign-On.
    - Se necessario, proteggere la chiave privata con una password.

Nota: Se vengono utilizzati certificati in formato PEM, conservare ogni certificato e ogni chiave privata in file separati.



Pagina Impostazione di Service Provider

Pagina Impostazione di Service Provider

- Richieste di firma: Opzione per firmare la comunicazione SAML ESA/SMA inviata all'IdP.
- Asserzioni segno: Opzione per richiedere all'IdP di firmare le asserzioni inviate all'ESA/SMA.
- Dettagli organizzazione: Può essere compilato con i dati aziendali appropriati.
- Invia e conferma modifiche per mantenere le impostazioni.
- Scaricare i metadati SP dalla pagina Configurazione SAML.

Configurare il provider di identità (IdP) per l'utilizzo con le appliance ESA/SMA

Nota: Alcuni IdP richiedono applicazioni o realm separati per ciascuna ESA (ad esempio: DUO)

Questi collegamenti forniscono configurazioni di esempio per più IdP al momento della pubblicazione.
Cisco TAC non fornisce supporto tecnico per prodotti di terze parti. Questi esempi vengono forniti come riferimenti.

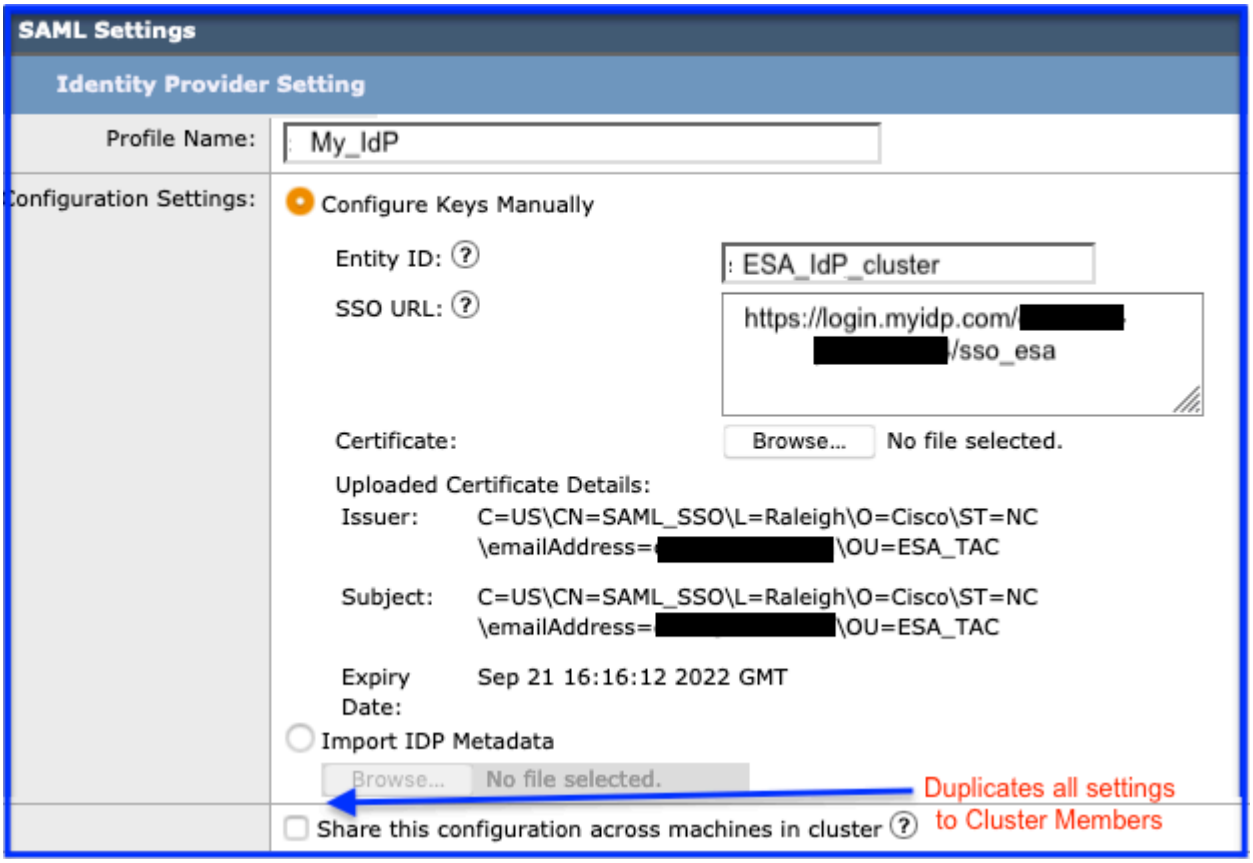
Configurazione delle impostazioni IDP su ESA/SMA

1. Passare a Amministrazione sistema > SAML.

2. Selezionare Aggiungi provider di identità.

- Sono disponibili due opzioni:
- Importa metadati IdP
- Configura chiavi manualmente:
  - ID entità: Può essere qualsiasi valore utilizzato per identificare l'oggetto IdP
  - URL SSO: URL a cui l'SP invia le richieste di autenticazione SAML
  - Carica la chiave privata e il certificato pubblico in file separati

3. Condividere questa configurazione tra i computer del cluster per replicarla in tutte le ESA del cluster:

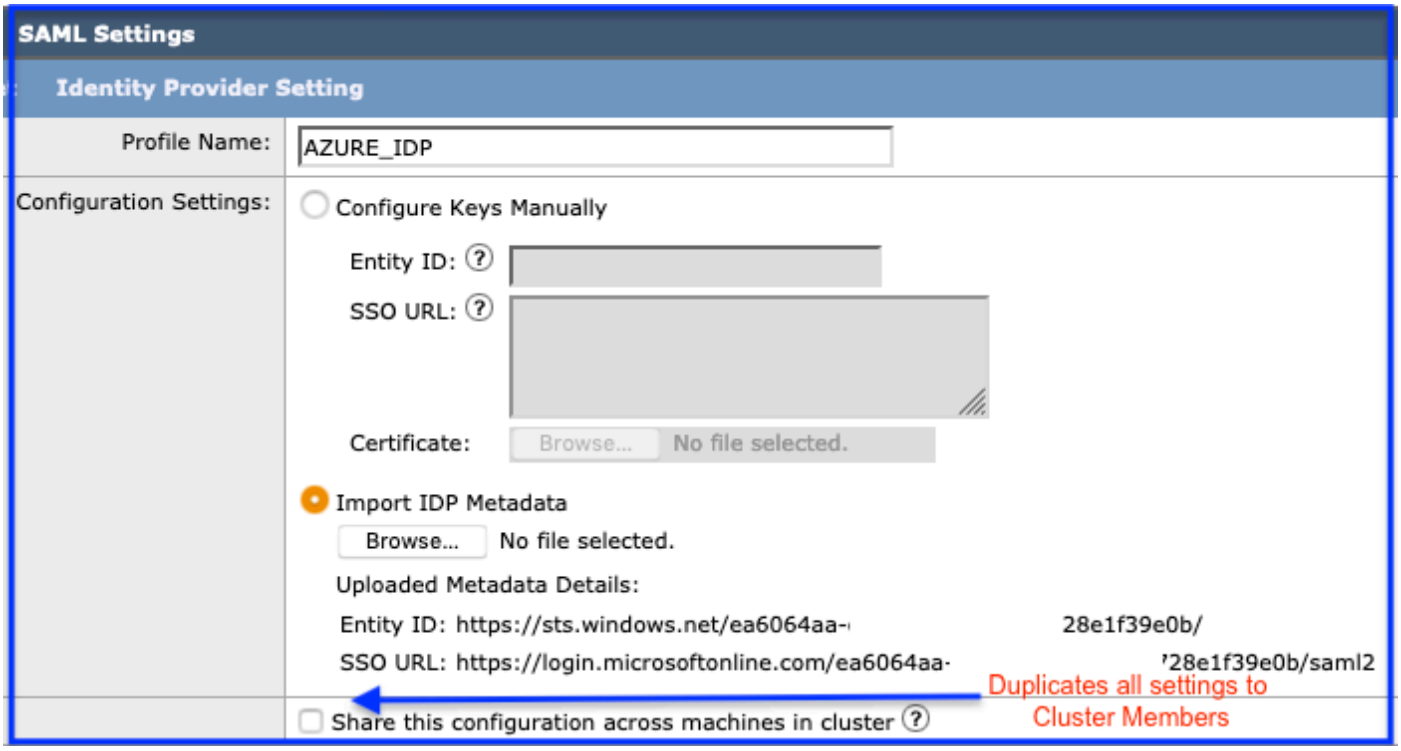


Immetti manualmente il contenuto del provider di identità

Immetti manualmente il contenuto del provider di identità

4. Carica metadati da IdP

- Selezionare Importa metadati IdP.
- Individuare il file di metadati salvato dall'IdP e salvare la configurazione.
- L'opzione per condividere la configurazione tra computer in un cluster è disponibile se applicabile alla distribuzione.



Carica metadati da Idp

Carica metadati da Idp

Abilitare l'autenticazione esterna utilizzando SAML su ESA/SMA

Analogamente all'autenticazione esterna LDAP, SAML Single Sign-On richiede la mappatura per assegnare i gruppi ai ruoli amministrativi.

1. Passare a Amministrazione sistema > Utenti (livello cluster) > Autenticazione esterna > Abilita.

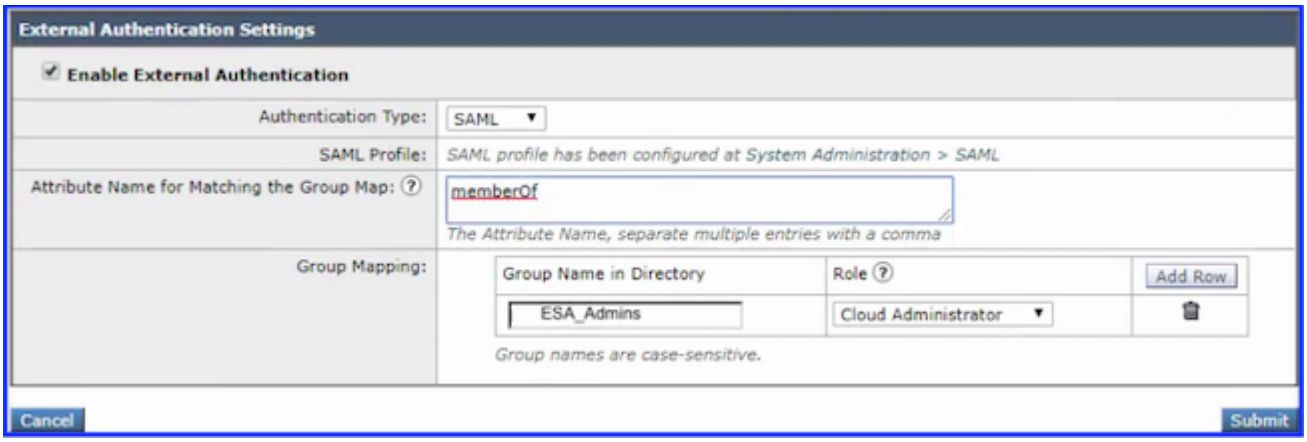
2. Selezionare il tipo di autenticazione: SAML.

3. Nome dell'attributo per la corrispondenza con la mappa dei nomi (facoltativo): Immettere il nome dell'attributo da cercare dal mapping di gruppo.

Nota: Il nome dell'attributo dipende dagli attributi configurati per l'inoltro del provider di identità nella risposta SAML. L'accessorio cerca le voci corrispondenti al nome dell'attributo specificato nella risposta SAML in base agli attributi configurati nel campo Mapping gruppo. Se questo campo non è configurato, l'accessorio cerca tutti gli attributi presenti nella risposta SAML nel campo Mapping gruppi configurato.

4. Inserire l'attributo del nome del gruppo definito nella directory SAML in base al ruolo utente predefinito o personalizzato.

- Il campo Mapping gruppi deve contenere un attributo gruppo. È possibile aggiungere l'attributo Unspecified Groups per autenticare le asserzioni o le risposte SAML.



Impostazioni autenticazione esterna

Impostazioni autenticazione esterna

5. Sottomettere e confermare le modifiche.

Una volta completata la configurazione, nella parte inferiore della pagina di accesso viene visualizzato un nuovo collegamento. La pagina di accesso ESA/SMA visualizza il collegamento Use Single Sign-On che reindirizza gli amministratori al provider di identità aziendale (IdP).

Se l'opzione è selezionata, l'amministratore viene reindirizzato alla pagina di accesso SAML aziendale.

Utilizza collegamento Single Sign-On per il reindirizzamento a SAML

Usa reindirizzamento collegamento Single Sign-On a SAML

Risoluzione dei problemi

Utilizzare questi indicatori per determinare se il problema è correlato alla configurazione dell'accessorio o alla configurazione del provider di identità.

Il collegamento di reindirizzamento SSO non viene visualizzato nella pagina di accesso ("Usa Single Sign-On")

Verificare che Amministrazione sistema > Utenti > Autenticazione esterna > SAML sia configurato.

Reindirizzare i ritorni alla pagina di accesso ESA/SMA con "Single Sign-On Authentication Failed! Contattare l'amministratore."

Errore: "Autenticazione Single Sign-On Non Riuscita. Contattare l'amministratore."

- Autenticazione non riuscita in IdP.
  - Ciò indica che la configurazione è in grado di raggiungere la pagina di autenticazione Single Sign-On e di inviare le credenziali.
  - Questo errore è spesso dovuto alla configurazione del provider di identità e richiede un'ulteriore verifica delle impostazioni del provider di identità.

Reindirizzare i ritorni alla pagina di login ESA/SMA con "Authorization Failure! Contattare l'amministratore."

Errore: "Errore di autorizzazione! Contattare l'amministratore."

- Autenticazione passata, ma autorizzazione non riuscita in ESA/SMA.
    - Attivare le impostazioni in Utenti > Autenticazione esterna > SAML.
        - Nome attributo, Nome gruppo e Mapping gruppo.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Cisco Content Security Management Appliance - Guide per l'utente
- Cisco Web Security - Guide per l'utente

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).