Konfigurieren der externen SAML SSO-Authentifizierung für die ESA- und SMA-Administration

Inhalt

- Einleitung
  - Umwelt
- Voraussetzungen
  - Checkliste zur Vorkonfiguration
- Hintergrundinformationen
  - Konfigurieren der ESA/SMA als Service Provider
  - Konfiguration des Identity Providers (IdP) für die Zusammenarbeit mit den ESA/SMA-Appliances
  - Konfigurieren der IDP-Einstellungen auf der ESA/SMA
  - Externe Authentifizierung mit SAML auf ESA/SMA aktivieren
- Fehlerbehebung
  - Der Link zur SSO-Umleitung wird auf der Anmeldeseite nicht angezeigt ("Single Sign-On verwenden").
  - Kehrt zur ESA/SMA-Anmeldeseite zurück, auf der die Option "Single Sign-On Authentication Failed! Bitte wenden Sie sich an Ihren Administrator."
  - Kehren Sie zur ESA/SMA-Anmeldeseite zurück mit "Authorization Failure! Bitte wenden Sie sich an Ihren Administrator."
- Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration der externen SAML 2.0 SSO-Authentifizierung für die ESA- und SMA-Systemadministration beschrieben.

Umwelt

- Produkte: E-Mail Security Appliance (ESA), Security Management Appliance (SMA)
- Gilt für: Systemverwaltung ESA und SMA
- Clusterverhalten: Die Profile "Service Provider" (SP) und "IdP" werden auf Computerebene konfiguriert. Die externe Authentifizierungszuordnung wird auf Cluster-Ebene konfiguriert.

Voraussetzungen

- Administratorzugriff auf die ESA/SMA-Webschnittstelle
- X.509-Zertifikat und privater Schlüssel verfügbar im Format PKCS #12 (PFX) oder PEM (selbstsigniert oder CA-signiert)
- Zugriff auf eine Identity Provider (IdP)-Anwendung eines Drittanbieters und deren SAML-Metadaten/SSO-URL

Checkliste zur Vorkonfiguration

- Überprüfen Sie den Hostnamen/FQDN der Verwaltungsschnittstelle, den Administratoren für den Zugriff auf die Appliance verwenden. Überprüfen Sie, ob die ACS-URL (Assertion Consumer Service) mit diesem Hostnamen übereinstimmt.
- Wenn sich die Appliance in einem Cluster befindet, planen Sie die Konfiguration von SAML auf Computerebene für jedes Mitglied, bevor Sie die externe SAML-Authentifizierung aktivieren.
- Bestimmen Sie, ob für die IdP eine separate Anwendung oder ein separater Bereich pro Appliance erforderlich ist.
- Stellen Sie sicher, dass die erforderlichen Zertifikate und Schlüssel verfügbar sind.
- Bestätigen Sie, dass der IdP die Gruppe oder das Rollenattribut sendet, die bzw. das für die ESA/SMA-Rollenzuordnung erforderlich ist.

Vorsicht: Dieses Dokument gilt nicht für SAML SSO in der Endbenutzerquarantäne.

Hintergrundinformationen

- Das Cisco TAC bietet keinen technischen Support für die IdP-Konfiguration von Drittanbietern. Beispielkonfigurationsreferenzen werden für häufige IDs bereitgestellt.

SSO-SAML-IDs

- Duo Access Gateway (DAG) fügt eine Zwei-Faktor-Authentifizierung hinzu, die gängige Cloud-Services mit SAML 2.0-Federation ergänzt.
- Active Directory-Verbunddienste (ADFS) - getestet mit ADFS 2, 3, 4, Azure Active Directory (Azure AD), SecureAUTH und PingFederate
- Zusätzliche Zwei-Faktor-Authentifizierung kann verwendet werden, wenn IdP sie innerhalb des SAML 2.0 Single Sign-On Frameworks unterstützt.
- Okta unterstützt die Authentifizierung mit einer IdP, die den Dienst unterstützt.

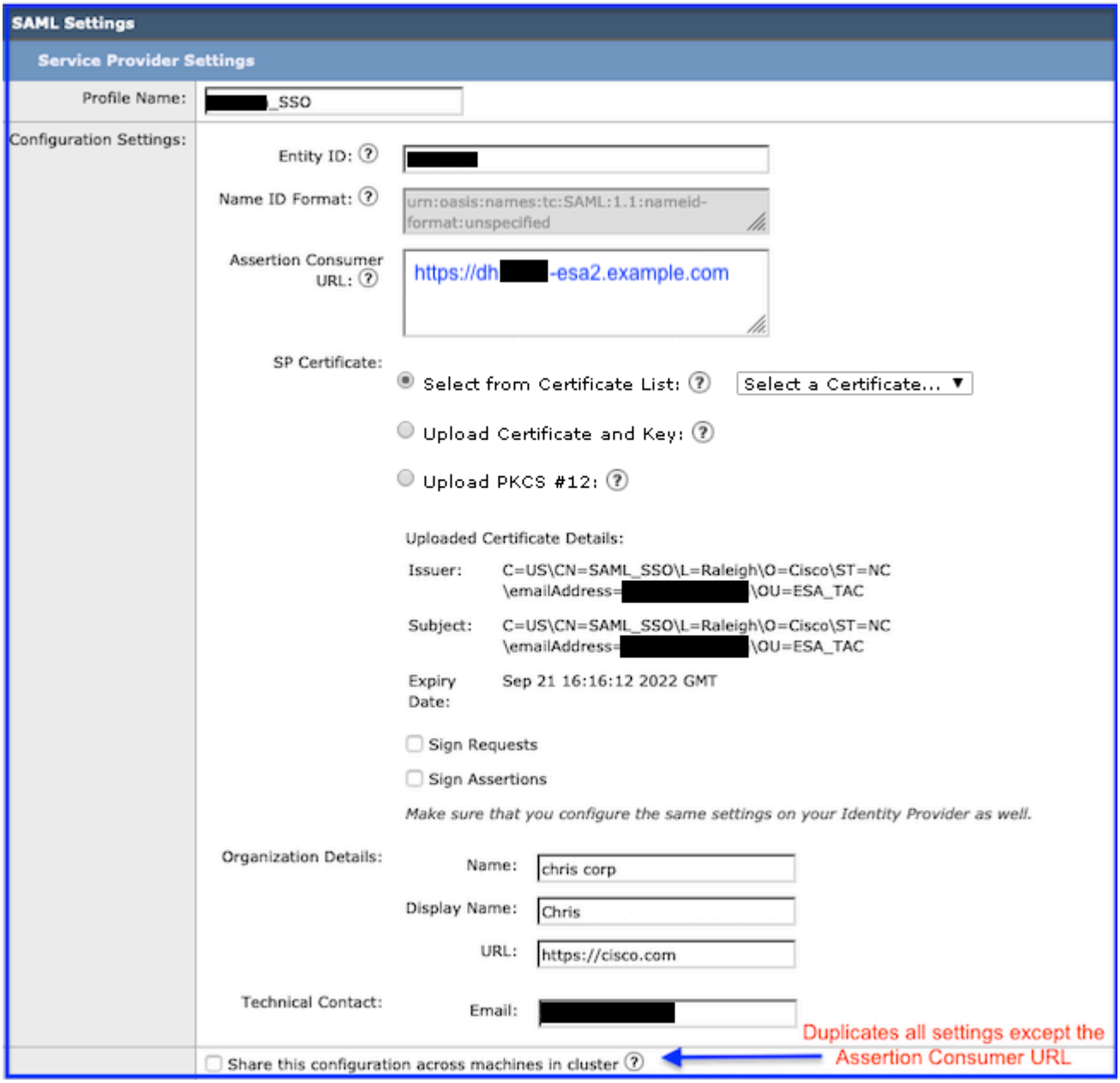
Konfigurieren der ESA/SMA als Service Provider

Navigieren Sie zu Systemverwaltung > SAML > (Computerebene) > Service Provider hinzufügen.

Anmerkung: ESAs in einem Cluster erfordern eine Konfiguration auf Computerebene für alle Mitglieder des Clusters, bevor SAML aktiviert werden kann.

- Wenn die Option unten auf der Seite "Konfiguration für Computer im Cluster freigeben" aktiviert ist, gelten die folgenden Bedingungen:
    - Alle Felder mit Ausnahme der Assertion Consumer-URL werden auf die Cluster-Mitglieder repliziert.
    - Die Assertion Consumer URL gibt den Hostnamen der Verwaltungsschnittstelle automatisch als ACS ein.
    - Umgebungen, die für den Zugriff auf den Host einen alternativen Hostnamen verwenden, erfordern eine manuelle Konfiguration für jeden Host, z. B. über CES gehostete Appliances.
    - Profilname: Name, der zur Bezeichnung der SP-Instanz in der ESA- oder SMA-Schnittstelle verwendet wird.
    - Entitäts-ID: Der Name, der für die SP-Instanz verwendet wird, wenn sie von IdP erkannt wird. Dieser Name ist die Bezeichnung, die von IdP für den SP verwendet wird. Dies kann ein beliebiger Name sein, z. B. ESA_SP oder ESA_SSO.
    - Namens-ID-Format: Nicht konfigurierbares Feld.
    - Assertion Consumer URL oder Assertion Consumer Service (ACS): Von der IdP für die Kommunikation mit diesem ESA/SMA-Host verwendete URL.
    - SP-Zertifikat:
        - Format: Öffentliche/private X.509-Zertifikate im PFX/PKCS12- oder PEM-Format.
        - Option 1: Aus Zertifikatliste auswählen: Wählen Sie Zertifikate aus, die bereits auf der ESA unter Netzwerk > Zertifikate erstellt wurden.
        - Option 2: Zertifikat und Schlüssel hochladen: Laden Sie ein Zertifikat und einen Schlüssel im PEM-Format hoch.
        - Option 3: PKCS Nr. 12 hochladen: Laden Sie eine PKCS #12-Datei hoch.
        - Optional: Erstellen Sie ein selbstsigniertes Zertifikat auf der ESA/SMA für SAML Single Sign-On.
        - Falls erforderlich, schützen Sie den privaten Schlüssel mit einem Kennwort.

Anmerkung: Wenn Zertifikate im PEM-Format verwendet werden, bewahren Sie jedes Zertifikat und jeden privaten Schlüssel in separaten Dateien auf.



Seite Service Provider Setup

Seite Service Provider Setup

- Signaturanforderungen: Option zum Signieren einer an den IdP gesendeten ESA/SMA-SAML-Kommunikation.
- Assertionen unterschreiben: Option, bei der die IdP an die ESA/SMA gesendete Assertionen signieren muss.
- Organisationsdetails: Kann mit den entsprechenden Unternehmensdaten ausgefüllt werden.
- Senden und bestätigen Sie Änderungen, um die Einstellungen beizubehalten.
- Laden Sie die SP-Metadaten von der SAML-Konfigurationsseite herunter.

Konfiguration des Identity Providers (IdP) für die Zusammenarbeit mit den ESA/SMA-Appliances

Anmerkung: Einige IdPs erfordern separate Anwendungen oder Bereiche für jede ESA. (Beispiel: DUO)

Diese Links bieten Beispielkonfigurationen für mehrere IdPs zum Zeitpunkt der Veröffentlichung. Das Cisco TAC bietet keinen technischen Support für Produkte von Drittanbietern. Diese Beispiele werden als Referenzen angegeben.

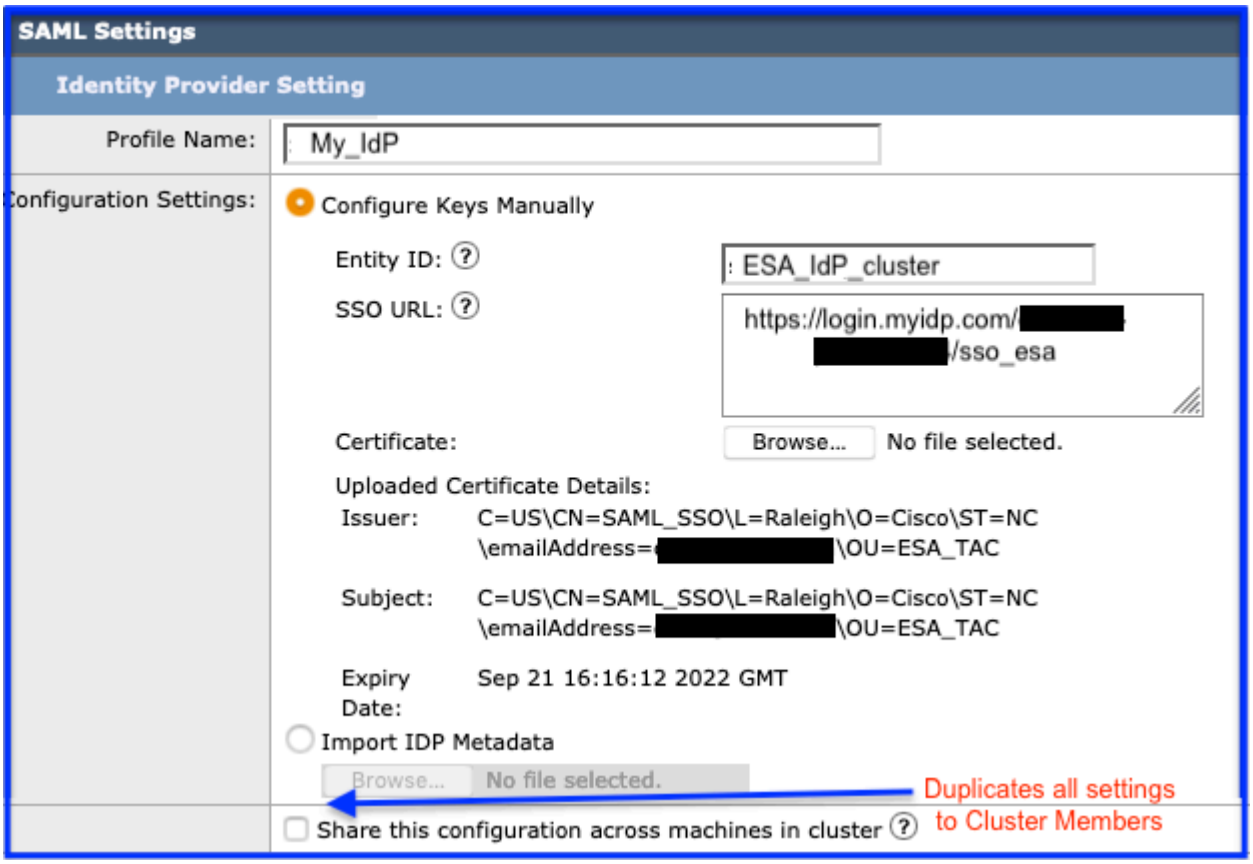
Konfigurieren der IDP-Einstellungen auf der ESA/SMA

1. Navigieren Sie zu Systemverwaltung > SAML.

2. Wählen Sie Identitätsanbieter hinzufügen aus.

- Zwei Optionen stehen zur Verfügung:
- Import-IDp-Metadaten
- Manuelles Konfigurieren von Schlüsseln:
    - Entitäts-ID: Kann jeder Wert sein, der zur Identifizierung der IdP verwendet wird.
    - SSO-URL: URL, an die der SP SAML-Authentifizierungsanforderungen sendet
    - Laden Sie den privaten Schlüssel und das öffentliche Zertifikat in separaten Dateien hoch

3. Geben Sie diese Konfiguration für alle Computer im Cluster frei, um die Konfiguration für alle ESAs im Cluster zu übernehmen:

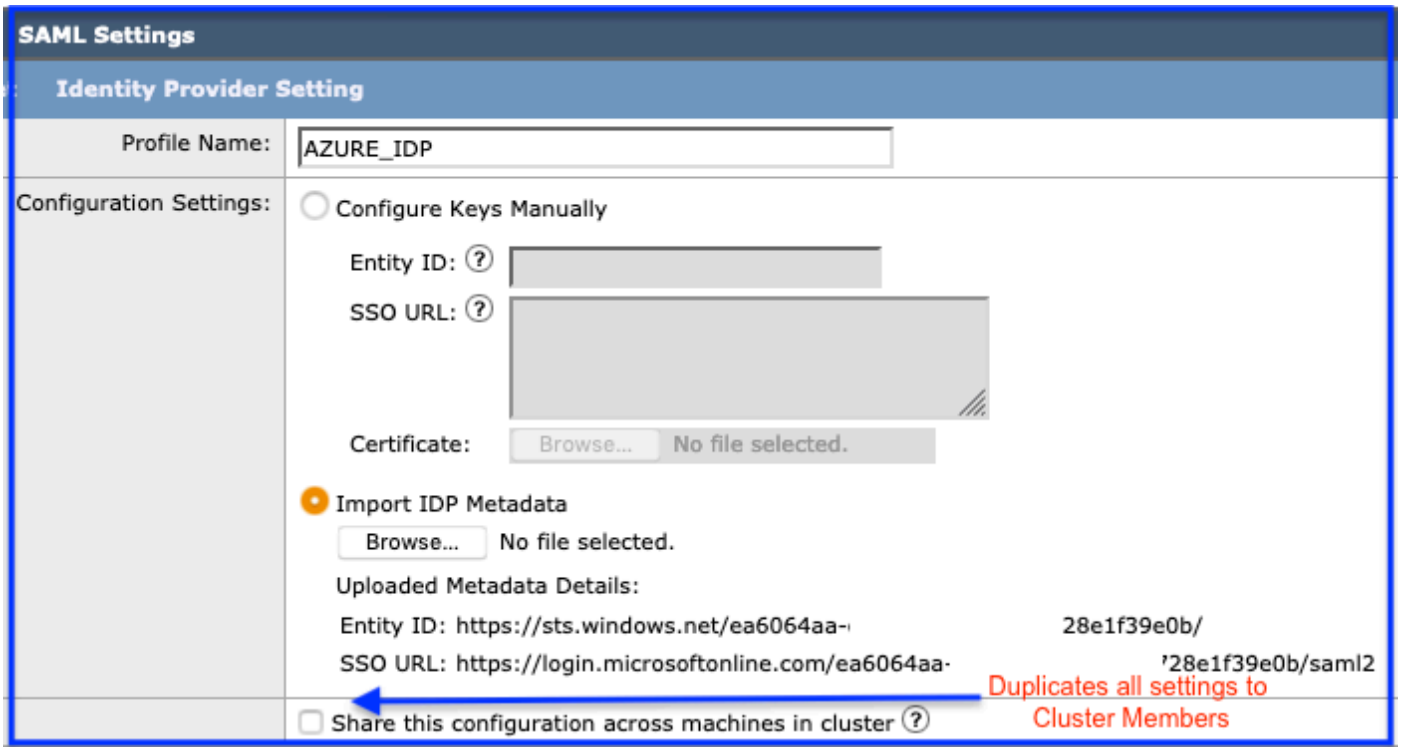


IDp-Inhalt manuell eingeben

IDp-Inhalt manuell eingeben

4. Metadaten von IdP hochladen

- Wählen Sie Import IdP Metadata aus.
- Navigieren Sie zur Metadatendatei, die von IdP gespeichert wurde, und speichern Sie die Konfiguration.
- Die Option zur gemeinsamen Nutzung dieser Konfiguration auf Computern in einem Cluster ist verfügbar, wenn sie für die Bereitstellung gilt.



Metadaten von IDP hochladen

Metadaten von IDP hochladen

Externe Authentifizierung mit SAML auf ESA/SMA aktivieren

Ähnlich wie bei der externen LDAP-Authentifizierung erfordert auch SAML Single Sign-On die Zuordnung, um Gruppen Administratorrollen zuzuweisen.

1. Navigieren Sie zu Systemverwaltung > Benutzer (Cluster-Ebene) > Externe Authentifizierung > Aktivieren.

2. Wählen Sie Authentifizierungstyp: SAML.

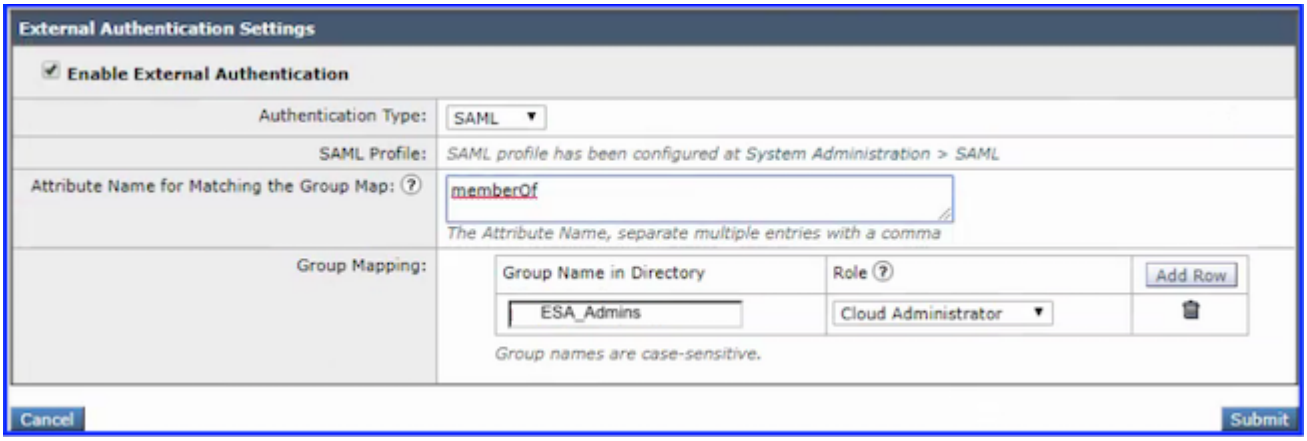
3. Attributname für die Namenszuordnung (optional): Geben Sie den Attributnamen für die Suche aus der Gruppenzuordnung ein.

Anmerkung: Der Attributname hängt von den Attributen ab, die für die Weiterleitung durch den Identity Provider in der SAML-Antwort konfiguriert wurden. Die Appliance sucht in der SAML-Antwort nach übereinstimmenden Einträgen des angegebenen Attributnamens anhand der im Feld Gruppenzuordnung konfigurierten Attribute. Wenn dieses Feld nicht konfiguriert ist, durchsucht die Appliance alle Attribute in der SAML-Antwort nach dem konfigurierten Gruppenzuordnungsfeld.

---

4. Geben Sie das Gruppennamensattribut wie im SAML-Verzeichnis definiert ein, basierend auf der vordefinierten oder benutzerdefinierten Benutzerrolle.

- Das Feld "Gruppenzuordnung" muss ein Gruppenattribut enthalten. Das Attribut Unspecified Groups kann hinzugefügt werden, um SAML-Assertionen oder -Antworten zu authentifizieren.



Einstellungen für die externe Authentifizierung

Einstellungen für die externe Authentifizierung

5. Senden und bestätigen Sie Änderungen.

Nach der erfolgreichen Konfiguration wird unten auf der Anmeldeseite ein neuer Link angezeigt. Auf der Anmeldeseite der ESA/SMA wird ein Link zur einmaligen Anmeldung verwenden angezeigt, der Administratoren an den Corporate Identity Provider (IdP) weiterleitet.

Bei Auswahl dieser Option wird der Administrator zur SAML-Anmeldeseite des Unternehmens umgeleitet.

Der Single Sign-On Link wird zur SAML weitergeleitet.

Weiterleitung über Single Sign-On Link zu SAML

Fehlerbehebung

Verwenden Sie diese Indikatoren, um festzustellen, ob das Problem mit der Appliance-Konfiguration oder der IdP-Konfiguration zusammenhängt.

Der Link zur SSO-Umleitung wird auf der Anmeldeseite nicht angezeigt ("Single Sign-On verwenden").

Vergewissern Sie sich, dass System Administration > Users > External Authentication > SAML konfiguriert ist.

Kehrt zur ESA/SMA-Anmeldeseite zurück, auf der die Option "Single Sign-On Authentication Failed! Bitte wenden Sie sich an Ihren Administrator."

Fehler: "Single Sign-On Authentication Failed! Bitte wenden Sie sich an Ihren Administrator."

- Fehler bei der Authentifizierung am IdP.
    - Dies zeigt an, dass die Konfiguration so weit fortgeschritten ist, dass die Seite für die einmalige Anmeldung und die Anmeldeinformationen übermittelt werden.
    - Dieser Fehler ist häufig auf die IdP-Konfiguration zurückzuführen und erfordert eine zusätzliche Überprüfung der IdP-Einstellungen.

Kehren Sie zur ESA/SMA-Anmeldeseite zurück mit "Authorization Failure! Bitte wenden Sie sich an Ihren Administrator."

Fehler: "Autorisierungsfehler! Bitte wenden Sie sich an Ihren Administrator."

- Die Authentifizierung wurde bestanden, aber die Autorisierung auf der ESA/SMA schlug fehl.
    - Konzentrieren Sie sich auf die Einstellungen unter Benutzer > Externe Authentifizierung > SAML.
        - Attributname, Gruppenname und Gruppenzuordnung.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Cisco Content Security Management Appliance - Bedienungsanleitungen
- Cisco Web Security - Bedienungsanleitungen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.