Configurazione di Duo IdP SAML SSO per ESA e SMA

Sommario

Introduzione

In questo documento viene descritto come configurare Duo Access Gateway per SAML SSO per Cisco ESA e SMA.

Ambiente

- Cisco ESA/SMA: Versione più recente di AsyncOS
- Duo Access Gateway: installate e raggiungibili dall'interfaccia di gestione ESA/SMA
- Origine autenticazione: Active Directory, OpenLDAP, Azure AD o un altro provider di identità SAML (per il mapping degli attributi)

Problema

Questo documento descrive solo la configurazione lato Duo. Non copre la configurazione di Cisco ESA/SMA Service Provider (SP).

Prerequisiti

Terminologia

- Provider di identità (IdP)
- Single Sign-On (SSO)

- Email Security Appliance (ESA)
- Security Management Appliance (SMA)
- Assertion Consumer Service (ACS)
- Provider di servizi (SP)

Requisiti

Prima di iniziare:

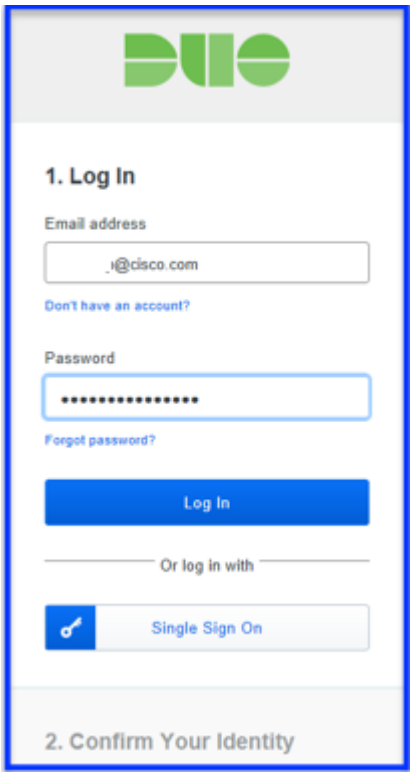
- Assicurarsi che Duo Access Gateway sia distribuito e che disponga di un'origine di autenticazione configurata.
- Distribuire Duo Access Gateway con un'origine di autenticazione configurata.
- Duo può richiedere un'applicazione separata per ciascuna ESA se non sono supportati più URL Assertion Consumer Service (ACS).

La configurazione è costituita da due fasi:

1. Configurare l'applicazione cloud Duo.
2. Aggiungere la nuova applicazione cloud a Duo Access Gateway.

Crea l'applicazione cloud

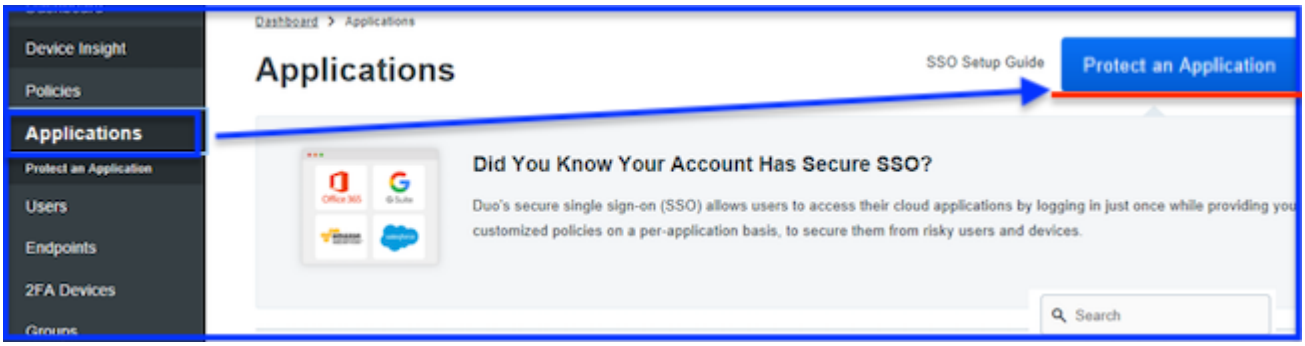
1. Accedere a https://admin.duosecurity.com/.



duo.com

duo.com

2. Passare a Applicazioni > Proteggi applicazione.

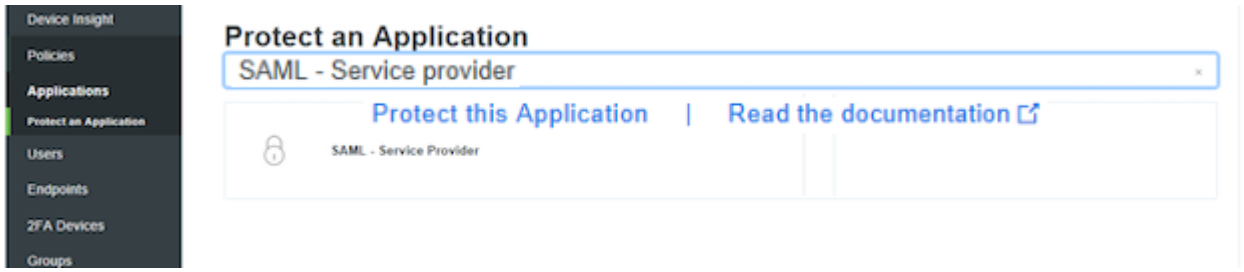


Proteggere un'applicazione

Proteggere un'applicazione

3. Cercare SAML - Service Provider.

4. Quando viene visualizzata l'icona SAML, selezionare Proteggi applicazione.



Proteggi applicazione

Proteggi applicazione

5. Completare il profilo del provider di servizi:

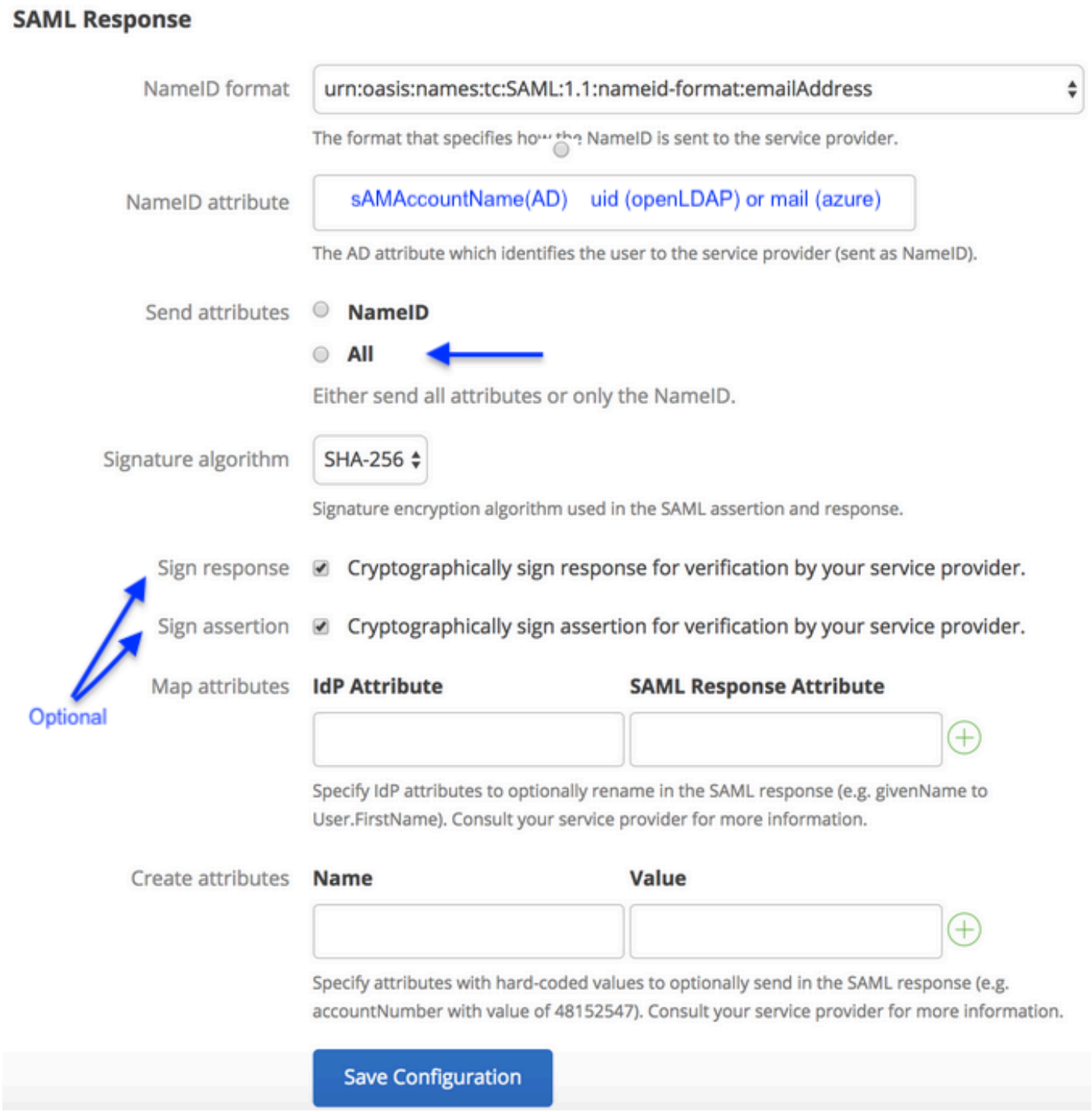
- Nome provider di servizi: Immettere un nome a scelta.
- ID entità: Inserire un nome comune per identificare l'ESA/SMA.
- Servizio consumer di asserzione: Immettere l'URL ESA/SMA raggiungibile.

6. Utilizzare i seguenti valori di attributo NameID in base all'origine dell'autenticazione:

Attributo	Active Directory	OpenLDAP	Provider di identità SAML (IdP)	Azure AD
Attributo Mail	posta	posta	posta	posta
attributo Username	NomeAccountAMA	uid	posta	posta
Attributo Nome	nomespecificato	gn	nomespecificato	nomespecificato
Attributo Cognome	SN	SN	SN	cognome

- Gli attributi di invio sono facoltativi. Selezionare NameID o ALL.
- La risposta del segno e l'asserzione del segno sono facoltative. Queste impostazioni devono corrispondere su IdP e SP.

7. Selezionare Salva configurazione.



Risposta SAML

Risposta SAML

8. Infine, scaricare il file di configurazione.

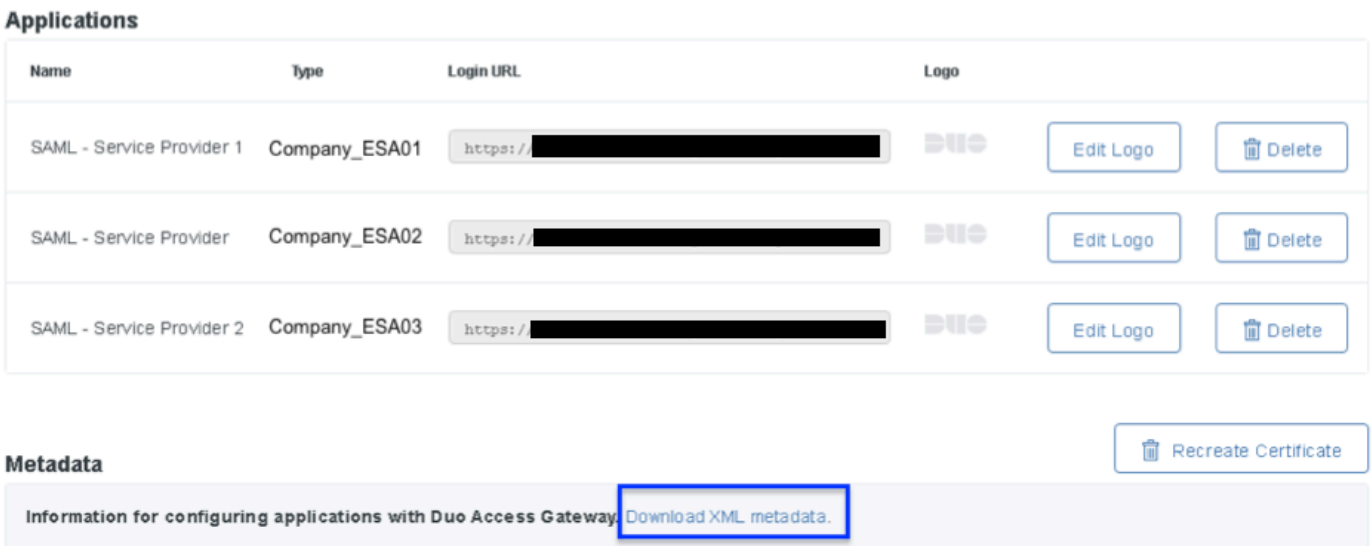
Aggiunta di una nuova applicazione cloud a Duo Access Gateway

1. Accedere a Duo Access Gateway.

2. Passare a Applicazione > Aggiungi applicazione > File di configurazione > Scegli file.

3. Selezionare la configurazione dell'applicazione creata al passo 1, quindi selezionare UPLOAD.

4. Scaricare i metadati XML da utilizzare sugli host SP come configurazione IdP.



Visualizzazione delle applicazioni e download dei metadati XML

Visualizzazione delle applicazioni e download dei metadati XML

5. Tornare all'ESA/SMA per completare la configurazione dell'SSO SAML.

- Risultato previsto: Viene creata l'applicazione Duo Access Gateway e i metadati XML IdP sono pronti per l'importazione in ESA/SMA.

6. Utilizzare i metadati scaricati nella successiva procedura ESA/SMA.

Fasi successive (configurazione ESA/SMA)

Questo articolo riguarda solo la configurazione lato Duo. Per completare l'impostazione dell'ESA/SMA, seguire le istruzioni.

Verifica

- Confermare che l'applicazione venga visualizzata in Duo Access Gateway in Applicazioni.
- Confermare che i metadati XML IdP siano stati scaricati correttamente e siano pronti per l'importazione in ESA/SMA.

Informazioni correlate

- Documentazione Duo per SAML SSO

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).