Configura autenticazione esterna SSO ID Microsoft per DMP

Sommario

Introduzione

In questo documento viene descritto come configurare il servizio Single Sign-on Microsoft Entra ID per l'autenticazione al portale Cisco Domain Protection.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Domain Protection
- ID Entra Microsoft
- Certificati SSL X.509 autofirmati o con firma CA (facoltativo) in formato PEM

Componenti usati

- Accesso amministratore di Cisco Domain Protection
- Accesso amministratore di Microsoft Entra ID

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.

Premesse

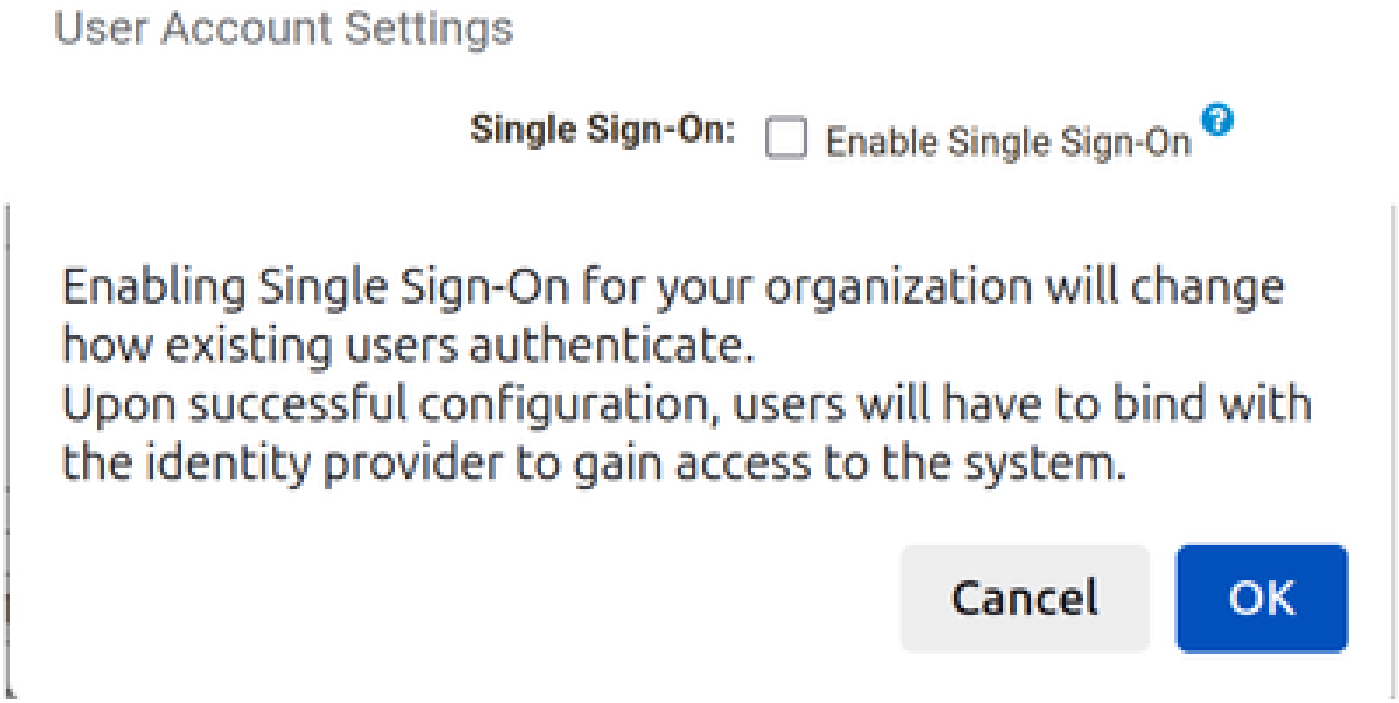
- Cisco Domain Protection consente l'accesso SSO per gli utenti finali tramite il protocollo SAML 2.0.
- Microsoft Entra SSO consente e controlla l'accesso al software come app di servizio (SaaS), alle app cloud o alle app locali da qualsiasi luogo con Single Sign-On.
- È possibile impostare Cisco Domain Protection come applicazione di identità gestita connessa a Microsoft Entra con metodi di autenticazione che includono l'autenticazione a più fattori, in quanto l'autenticazione basata solo su password non è sicura né consigliata.
- 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, fare riferimento a: Che cos'è SAML?

Configurazione

Protezione del dominio Cisco (parte 1)

1. Accedere al portale di amministrazione di Cisco Domain Protection e selezionare Amministrazione > Organizzazione. Fare clic sul pulsante Modifica dettagli organizzazione, come mostrato nell'immagine:

2. Passare alla sezione Impostazioni account utente e fare clic sulla casella di controllo Abilita Single Sign-On. Viene visualizzato un messaggio come mostrato nell'immagine:

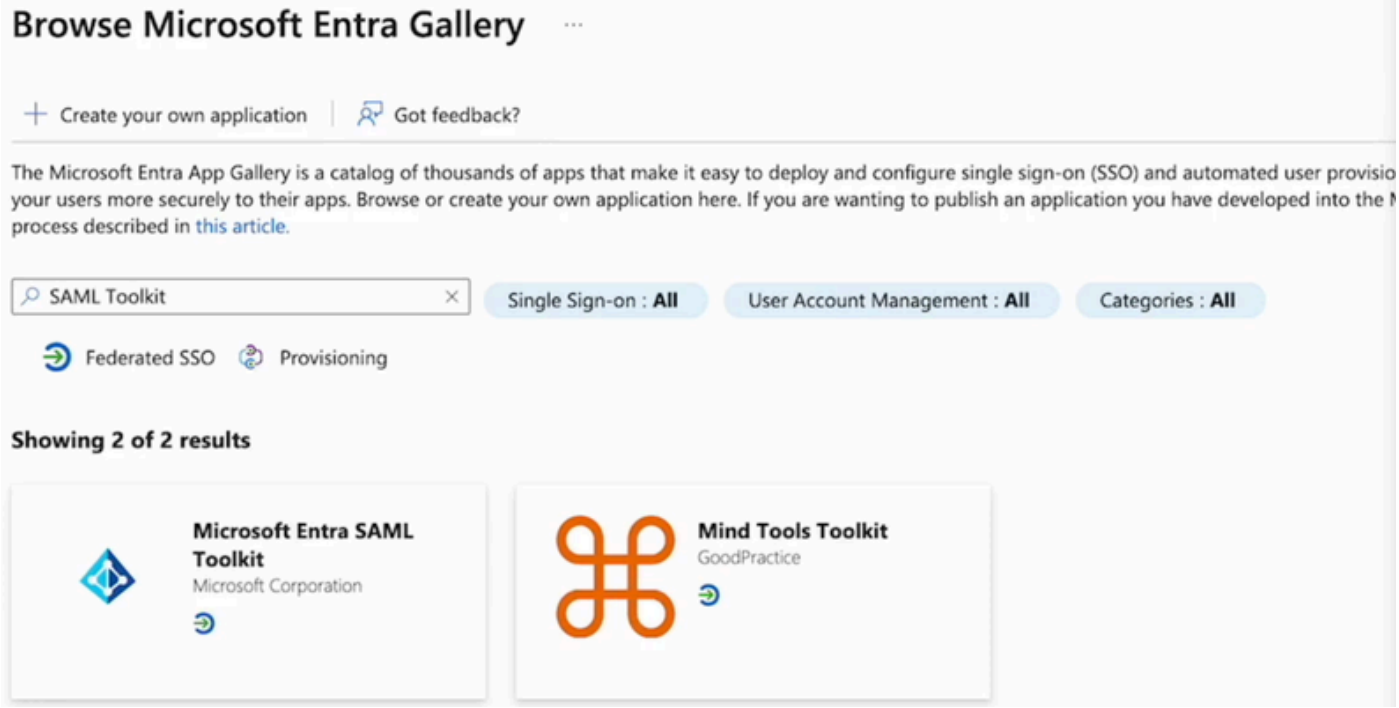


3. Fare clic sul pulsante OK e copiare i parametri ID entità e URL servizio consumer di asserzione (ACS). Questi parametri devono essere utilizzati nell'autenticazione SAML di base di Microsoft Entra ID. Tornare in seguito per impostare i parametri Formato identificatore nome, Endpoint SAML 2.0 e Certificato pubblico.

- ID entità: dmp.cisco.com
- URL servizio consumer asserzione:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

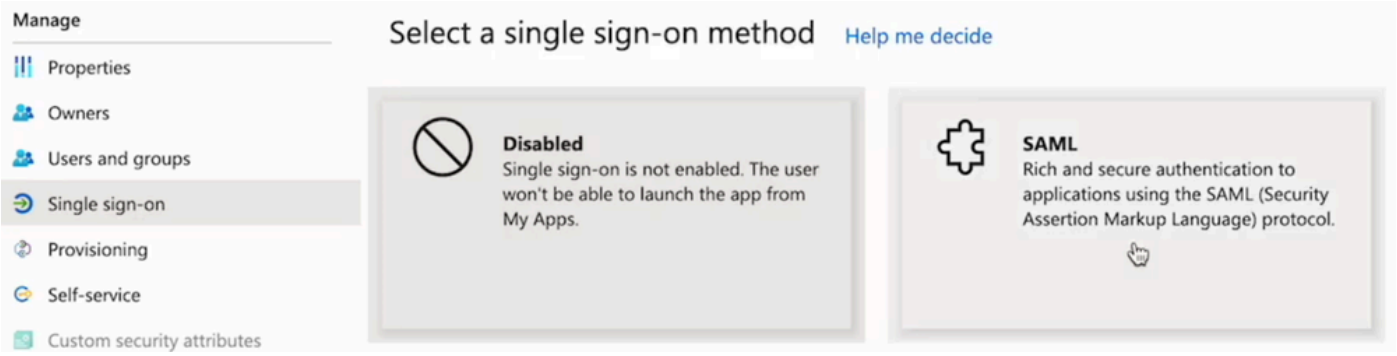
ID Entra Microsoft

1. Passare all'interfaccia di amministrazione Microsoft Entra ID e fare clic sul pulsante Aggiungi. Selezionare Enterprise Application e cercare Microsoft Entra SAML Toolkit, come mostrato nell'immagine:



2. Assegnare al nome un valore significativo e fare clic su Crea. Ad esempio, Domain Protection Sign On.

3. Passare al pannello laterale sinistro, sotto la sezione Gestisci. Fare clic su Single Sign-on e selezionare SAML.



4. Nel pannello Configurazione SAML di base, fare clic su Modifica, quindi specificare i parametri:

- Identificatore (ID entità): dmp.cisco.com
- URL risposta (URL servizio consumer asserzione): https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- URL di accesso: https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Fare clic su Save (Salva).

5. Nel pannello Attributi e attestazioni, fare clic su Modifica.

In Attestazione obbligatoria fare clic sull'attestazione ID utente univoco (ID nome) per modificarla.

- Impostare il campo dell'attributo Source su user.userprincipalname. Si presuppone che il

valore user.userprincipalname rappresenti un indirizzo di posta elettronica valido. In caso contrario, impostare Source su user.primaryauthoritativeemail.

- Nel pannello Attestazioni aggiuntive, fare clic su Modifica e creare i mapping tra le proprietà utente di Microsoft Entra ID e gli attributi SAML.

Nome	Spazio dei nomi	Attributo di origine
indirizzo email	Nessun valore	user.nomeprincipaleutente
Nome	Nessun valore	user.nomedato
cognome	Nessun valore	user.cognome

Assicurarsi di cancellare il campo Spazio dei nomi per ogni attestazione, come illustrato di seguito:

6. Dopo aver compilato le sezioni Attributi e Attestazioni, viene compilata l'ultima sezione del certificato di firma SAML.

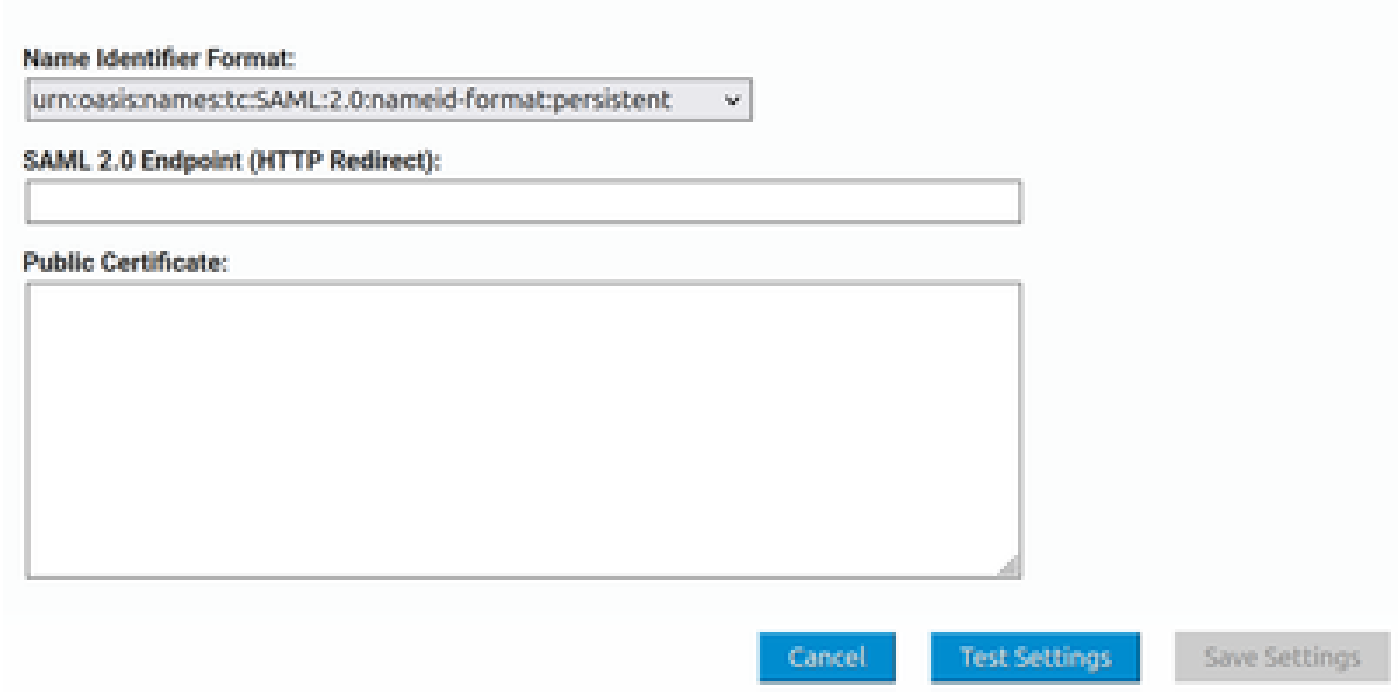
- Salvare l'URL di accesso.

- Salvare il certificato (Base64).

Protezione del dominio Cisco (parte 2)

Tornare alla sezione Protezione dominio Cisco > Abilita Single Sign-On.

- Formato identificatore nome: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- Endpoint SAML 2.0 (reindirizzamento HTTP): URL di accesso fornito da Microsoft Entra ID
- Certificato pubblico: Certificato (Base64) fornito da Microsoft Entra ID



Verifica

Fare clic su Impostazioni test. Verrà reindirizzato alla pagina di accesso del provider di identità. Eseguire l'accesso utilizzando le credenziali SSO.

Dopo aver eseguito correttamente l'accesso, è possibile chiudere la finestra. Fare clic su Salva impostazioni.

Risoluzione dei problemi

```
Error - Error parsing X509 certificate
```

- Verificare che il certificato sia in Base64.

```
Error - Please enter a valid URL
```

- Verificare che l'URL di accesso fornito da Microsoft Entra ID sia corretto.

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).