Configura autenticazione esterna SSO Microsoft Entra ID per CRES

Sommario

Introduzione

In questo documento viene descritto come configurare Microsoft Entra ID Single Sign-On per l'autenticazione al servizio Cisco Secure Email Encryption.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Servizio Secure Email Encryption (Registered Envelope)
- ID Entra Microsoft
- Certificati SSL X.509 autofirmati o con firma CA (facoltativo) in formato PEM

Componenti usati

- Accesso dell'amministratore del servizio Secure Email Encryption (Registered Envelope)
- 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.

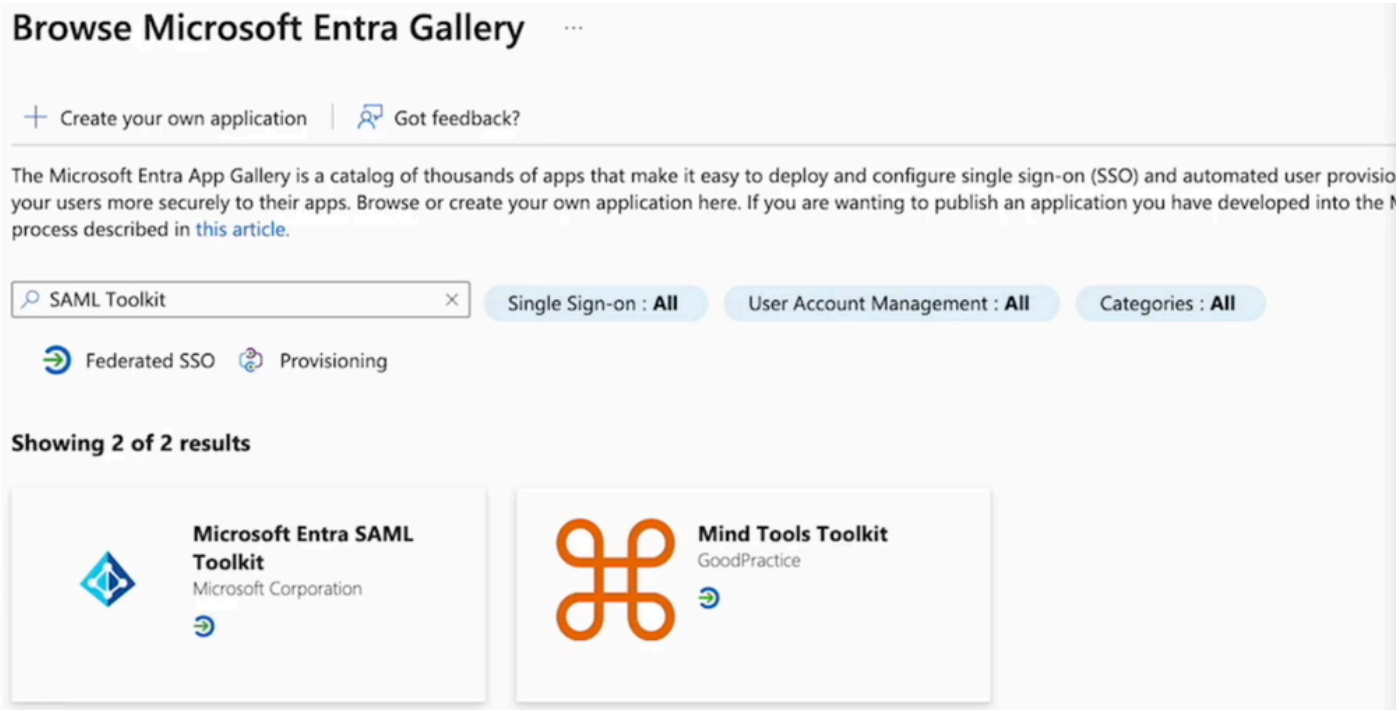
Premesse

- Registered Envelope consente l'accesso SSO per gli utenti finali che utilizzano SAML.
- 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.
- Registered Envelope può essere impostato come applicazione di identità gestita connessa a Microsoft Entra con metodi di autenticazione che includono l'autenticazione a più fattori poiché l'autenticazione solo 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

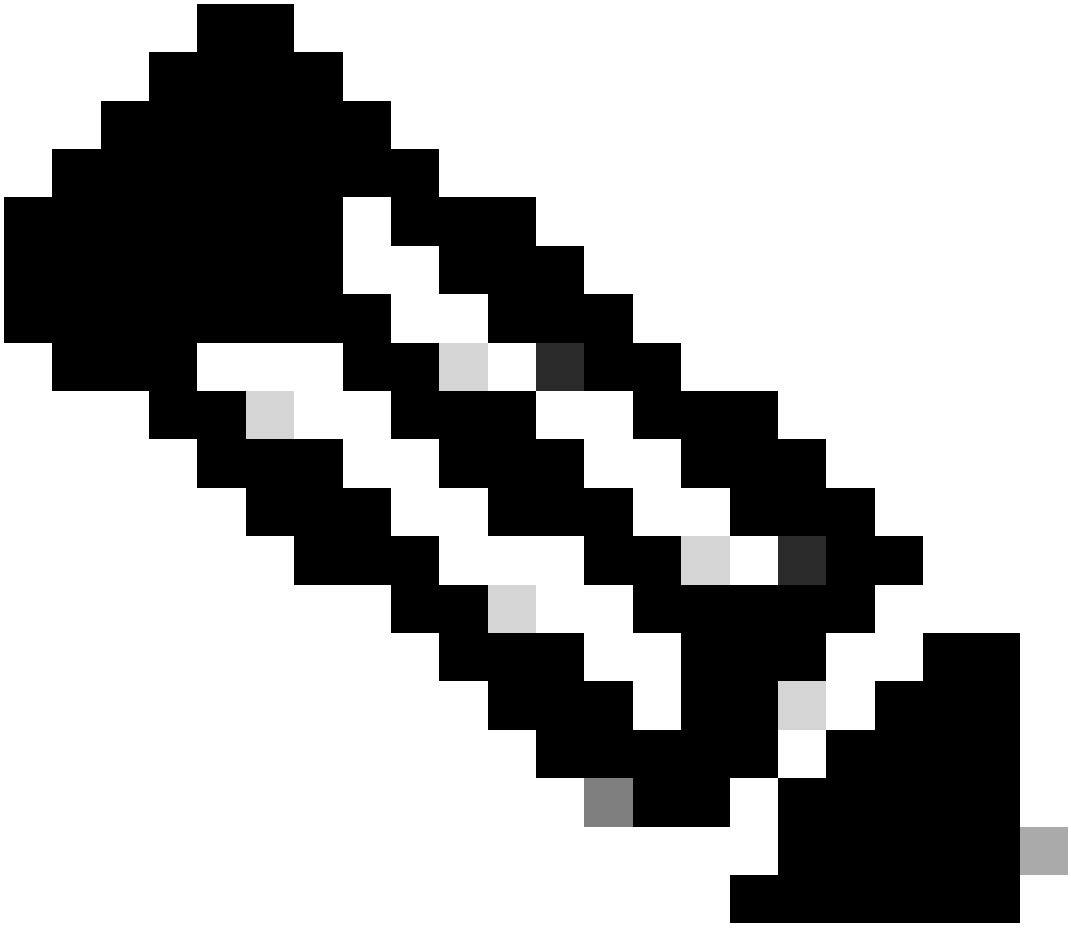
ID Entra Microsoft

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:



Esplora Raccolta Microsoft Entra

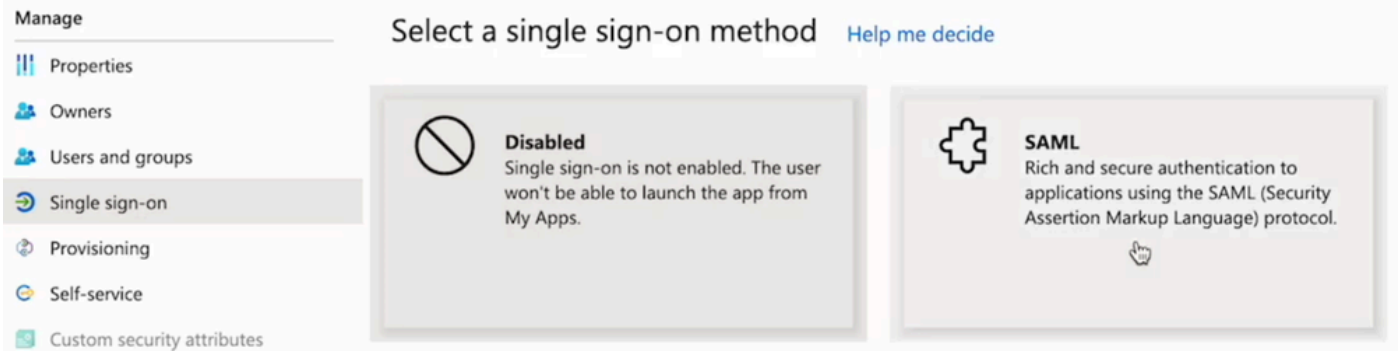
2. Assegnare al nome un valore significativo e fare clic su Crea. Ad esempio, CRES Single Sign On.



Nota: Per consentire a tutti gli utenti di accedere al portale CRES, è necessario disabilitare manualmente l'assegnazione richiesta nelle proprietà Accesso CRES (toolkit SAML) e per Assegnazione richiesta selezionare No.

---

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



4. Nel pannello Configurazione SAML di base, fare clic su Modifica, quindi immettere gli attributi

come indicato di seguito:

- Identificatore (ID entità): https://res.cisco.com/
- URL risposta (URL servizio consumer asserzione): https://res.cisco.com/websafe/ssourl
- URL di accesso: https://res.cisco.com/websafe/ssourl
- 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.

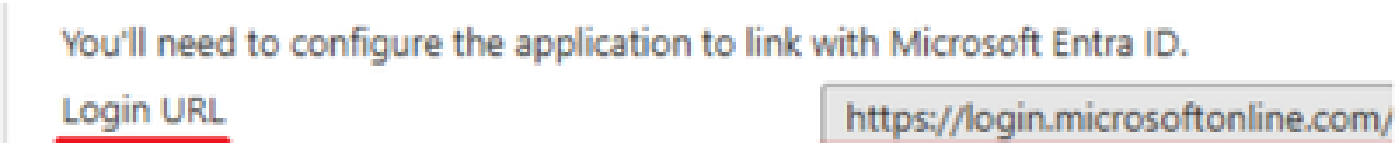
- Impostare il campo dell'attributo Source su user.userprincipalname. Si presuppone che il valore user.userprincipalname rappresenti un indirizzo di posta elettronica valido. In caso contrario, impostare Source su user.primaryauthoritativeemail.
- Nel pannello Attestazioni aggiuntive, fare clic su Modifica 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 i valori successivi nel portale CRES come richiesto:

- Salvare l'URL di accesso.



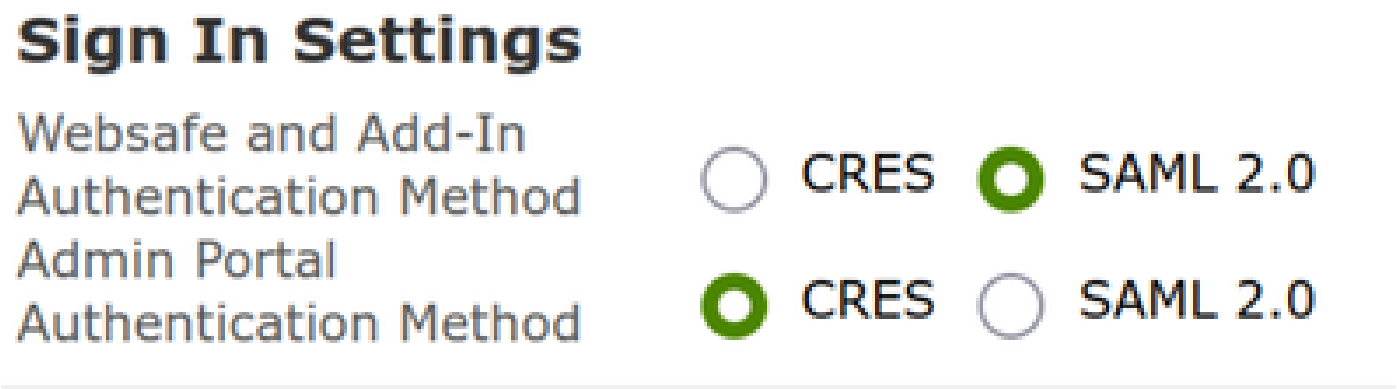
- Selezionare il collegamento Download certificato (Base64).

Servizio Cisco Email Encryption

1. Accedere al portale dell'organizzazione del servizio Secure Email Encryption come amministratore.

2. Nella scheda Conti, selezionare la scheda Gestisci conti e fare clic sul numero di conto.

3. Nella scheda Dettagli, scorrere fino a Metodo di autenticazione e selezionare SAML 2.0.



4.- Completare gli attributi come segue:

- Nome EmailAttribute alternativo SSO: indirizzo email
- ID entità provider di servizi SSO*: https://res.cisco.com/
- URL servizio clienti SSO*: Questo collegamento viene fornito da Entra ID, in
- URL di disconnessione SSO: lasciare vuoto

5.- Fare clic su Attiva SAML.

Verifica

Viene visualizzata una nuova finestra che conferma che, dopo aver eseguito correttamente l'accesso, è stata abilitata l'autenticazione SAML. Fare clic su Avanti. Viene visualizzata nuovamente la pagina di accesso del provider di identità. Accedere utilizzando le credenziali SSO. Dopo aver eseguito correttamente l'accesso, è possibile chiudere la finestra. Fare clic su Save (Salva).

Risoluzione dei problemi

Se la finestra non reindirizza l'utente alla pagina di accesso del provider di identità, viene restituita una traccia che fornisce l'errore. Esaminare Attributi e attestazioni, verificare che sia configurato con lo stesso nome della sezione Metodo di autenticazione CRES. L'indirizzo di posta elettronica dell'utente utilizzato nell'accesso SAML deve corrispondere all'indirizzo di posta elettronica del CRES. Non utilizzare alias.

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).