Cisco Secure Access - Rinnovo del certificato SAML con IDP (Microsoft Entra ID)

Sommario

Problema

Quando si utilizza l'autenticazione SSO con Microsoft Entra ID SAML come provider di identità (IdP) per Cisco Secure Access, i certificati di verifica SAML stanno per scadere.

Per evitare interruzioni dell'autenticazione e determinare se è necessario creare una nuova configurazione Single Sign-On in Secure Access durante il rinnovo dei certificati SAML Entra ID, le organizzazioni devono comprendere il processo di rinnovo dei certificati corretto.

Ambiente

- Cisco Secure Access con autenticazione SSO configurata
- Microsoft Entra ID SAML come provider di identità
- Certificati di verifica SAML con prossime date di scadenza
- Configurazione SSO esistente per SWG (Secure Web Gateway) e ZTNA (Zero Trust Network Access)

Risoluzione

Passaggio 1 - Rileva rinnovo certificato

- Il provider di identità (IdP) rinnova o ruota il proprio certificato di firma SAML.
- Ciò si verifica in genere quando il certificato sta per scadere.

Passaggio 2 - Ottenere metadati IdP aggiornati

- Esporta il nuovo XML dei metadati IdP o il nuovo certificato di firma dal provider di identità.

Passaggio 3 - Verifica della modifica del certificato

Confermare che il certificato è stato effettivamente modificato.

Verifica:

- Identificazione personale
- Data di scadenza
- Emittente

In questo modo l'SP viene aggiornato con il certificato corretto

Aggiorna configurazione provider di servizi

Accedere a Cisco Secure Access Dashboard e aggiornare la configurazione.

Passare a Connetti - Utente e gruppi.

Fare clic su Gestione configurazione

In Autenticazione SSO - Modificare il profilo di autenticazione SSO - caricare il file di metadati utilizzando un nuovo certificato oppure caricare il certificato se si esegue la configurazione manuale.

Fase 5 - Salvataggio e applicazione della configurazione

- Salvare la configurazione aggiornata

Passaggio 6 - Convalida autenticazione SSO

Eseguire un test di accesso SSO.

Causa

Il certificato di firma del provider di identità (IdP) viene utilizzato dal provider di servizi per verificare la firma dell'asserzione SAML e, quando l'IdP rinnova il certificato, l'SP deve aggiornare il proprio certificato attendibile per continuare a convalidare le richieste di autenticazione

Contenuto correlato

- Cisco Secure Access - Panoramica e configurazione di SAML Single Sign-On
- Configurazione di SAML SSO per Cisco Secure Access (esempio di Microsoft Entra ID)
- Supporto tecnico Cisco e download

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).