Autenticazione SAML VPNaaS non riuscita con "Decrittografia dello stato di inoltro non riuscita" Errore durante l'utilizzo di Duo IdP

Sommario

Problema

Quando si tenta di stabilire una connessione VPNaaS utilizzando Secure Client Remote Access con autenticazione SAML e Duo come provider di identità (IdP), viene rilevato questo errore:

- Errore durante l'elaborazione della richiesta di autenticazione SSO. Contattare l'amministratore di sistema
- Decrittografia di relaystate non riuscita

L'autenticazione con la stessa configurazione IdP e Duo funziona correttamente per ZTNA (Zero Trust Network Access), ma non riesce per le connessioni VPN. In Duo sono configurate due applicazioni separate per ZTNA e VPN, entrambe con lo stesso IdP.

Ambiente

- Tecnologia: Supporto per la soluzione (SSPT - contratto obbligatorio)
- Sottotecnologia: Accesso sicuro - Accesso remoto client sicuro (VPN, postura, risorsa privata)
- Metodo di autenticazione: SAML con Duo IdP
- Due applicazioni Duo configurate: uno per ZTNA, uno per VPN
- L'autenticazione funziona per ZTNA, non riesce per VPN
- Versione del software: TUTTO
- Nessuna modifica recente alla versione di hardware/software specificata

Risoluzione

Il problema è stato risolto correggendo la configurazione dell'ID entità e dell'URL del servizio consumer di asserzione (ACS) nell'applicazione Duo per la VPN. I metadati corretti sono stati scaricati da Secure Access e caricati nell'app VPN Duo, risolvendo l'errore di decrittografia SAML Relaystate.

1. Accedere al dashboard CSA. Selezionare Connect > Enduser Connectivity -> Virtual Private Networks. Individuare il profilo a cui si è connessi.
2. Fare clic su tale profilo e su Modifica. Passare alla scheda Autenticazione.
3. Scaricare i metadati SAML per Secure Access.

4. Verificare entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml" e <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionCo
5. Verificare che entityID e AssertionConsumerService corrispondano all'applicazione Duo configurata per l'autenticazione VPN SSO.

Causa

La configurazione errata dell'ID entità e dell'URL ACS sull'applicazione VPN Duo ha causato l'errore di decrittografia SAML relaystate. La configurazione corretta non era presente in Duo per la VPN, anche se l'autenticazione ZTNA funzionava con lo stesso IdP. L'aggiornamento dell'applicazione Duo VPN con metadati accurati da Secure Access ha risolto il problema.

Contenuto correlato

- 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).