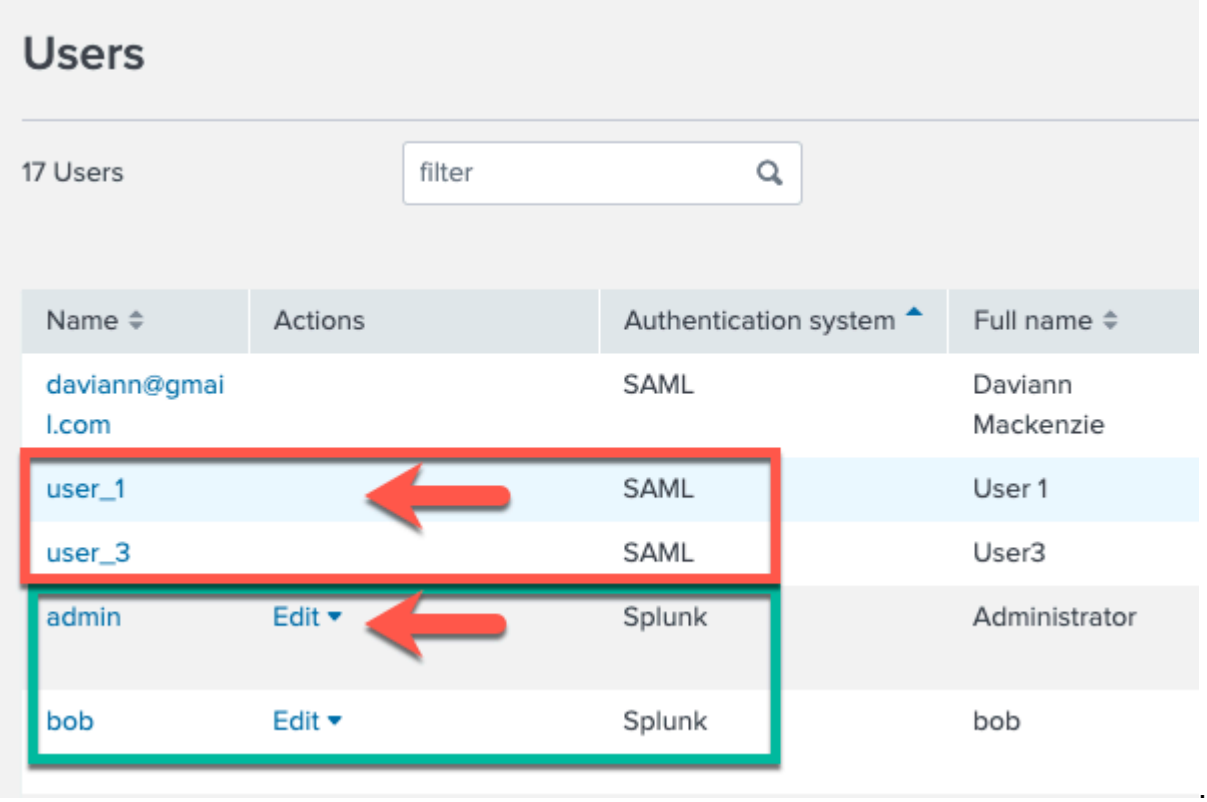
Impossibile gestire gli utenti SAML tramite interfaccia utente Splunk.

Applicabilità

Splunk Cloud Splunk Enterprise

Descrizione

Gli amministratori non sono in grado di gestire gli utenti SAML come possono fare con gli account creati localmente tramite l'interfaccia utente degli utenti

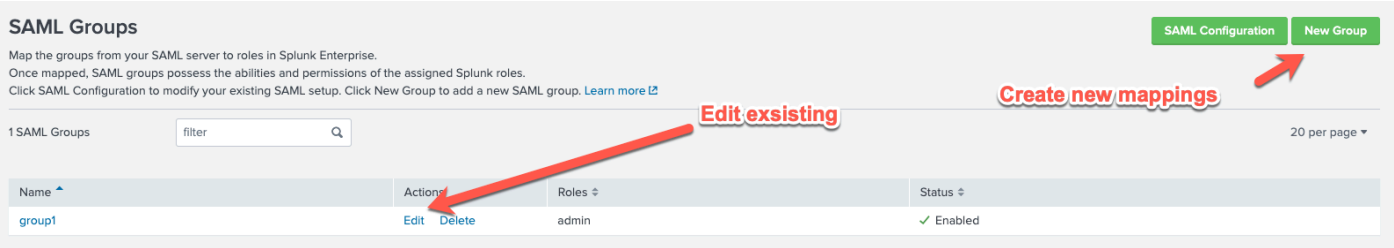


Risoluzione

Gli utenti a cui è stato assegnato il provisioning tramite l'integrazione SAML possono essere gestiti solo utilizzando due meccanismi:

1. IdP (provider di identità): L'IdP invierà all'istanza di Splunk durante l'accesso i "Ruoli" associati all'utente che accede. Se è necessario aggiungere o rimuovere ruoli per un utente, questa operazione verrà eseguita tramite IdP o tramite LDAP se l'IdP sta recuperando utenti da tale posizione.

2. Gruppi SAML (mapping): https://<Splunk instance>/en-GB/manager/launcher/saml
Da questa interfaccia è possibile mappare il ruolo utente proveniente dall'IdP ai ruoli Splunk



Nella documentazione Modifica o rimozione dei mapping dei ruoli sono illustrate queste opzioni

Se si desidera rimuovere utenti SAML, è necessario eseguire questa operazione prima a un livello IdP/LDAP rimuovendo i ruoli associati (utilizzati nel mapping Gruppi in Splunk). Al termine, gli utenti possono essere rimossi nell'istanza Splunk.

Se si utilizza Splunk Cloud, vedere questo articolo Come rimuovere i vecchi utenti SAML in Splunk

Se si utilizza un'istanza Splunk locale, rivedere questa soluzione della community Rimozione dei vecchi utenti SAML

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).