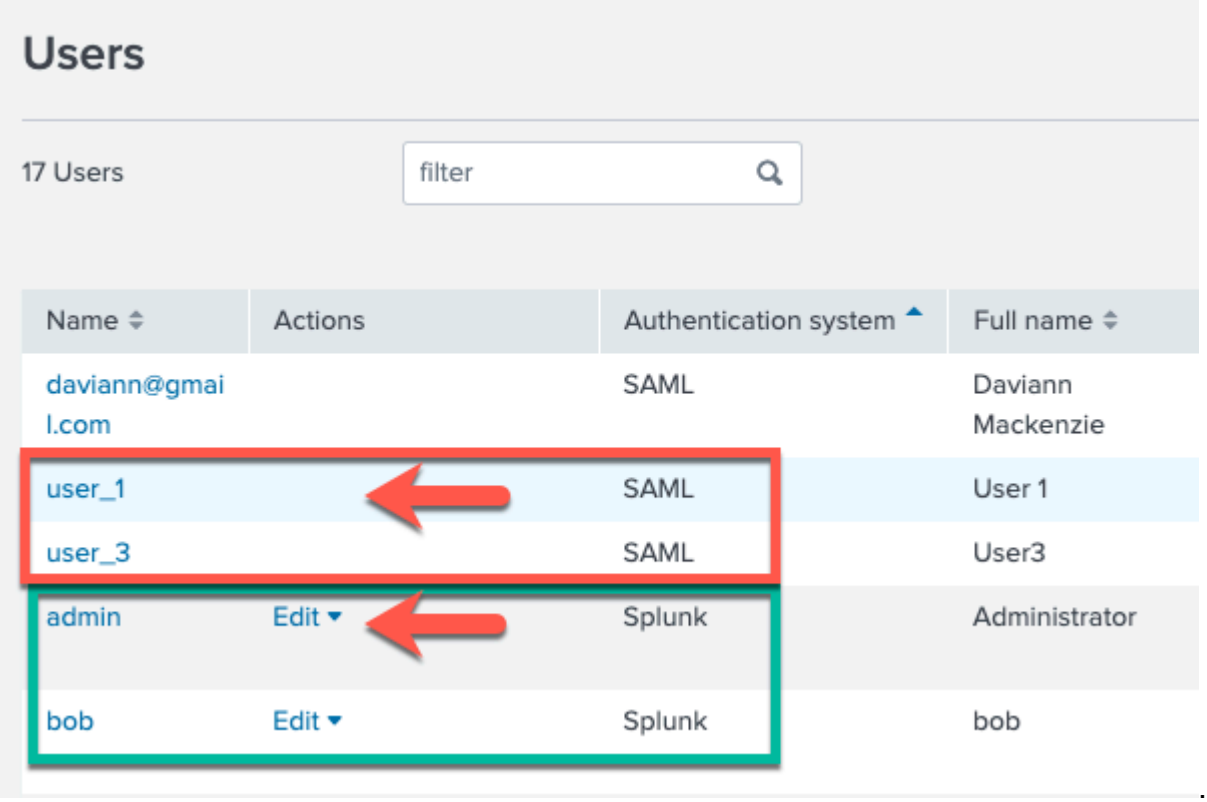
Não é possível gerenciar usuários SAML via interface do usuário de tronco.

Aplicabilidade

Splunk Cloud Splunk Enterprise

Descrição

Os administradores não podem gerenciar usuários SAML da mesma forma que fazem com contas criadas localmente por meio da IU Usuários

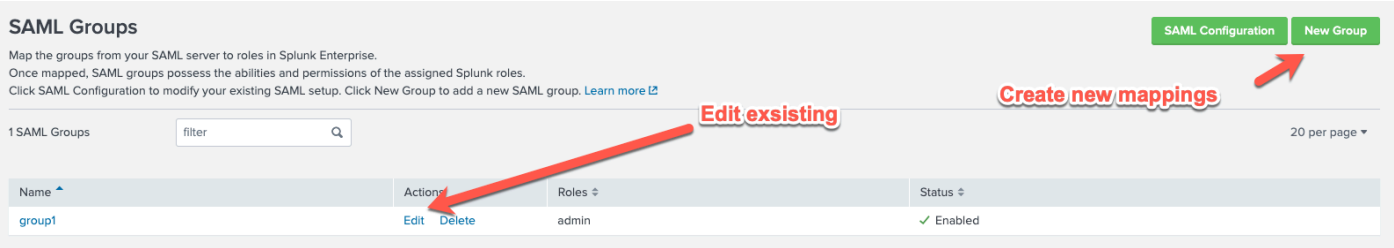


Resolução

Os usuários que são provisionados através da integração SAML só podem ser gerenciados usando dois mecanismos:

1. IdP (Identity Provider, Provedor de Identidade): O IdP enviará para a instância Splunk durante o login as "Funções" associadas ao usuário que faz login. Se for necessário adicionar ou remover funções para um usuário, isso será feito por meio de IdP ou LDAP, se o IdP estiver recuperando usuários de lá.

2. Grupos SAML (mapeamento): https://<instância de Splunk>/en-GB/manager/launcher/saml
Nessa interface, a função de usuário proveniente do IdP pode ser mapeada para funções Splunk



A documentação Modificar ou remover mapeamentos de função aborda essas opções

Se você estiver procurando remover usuários SAML, isso precisará ser feito primeiro em um nível IdP/LDAP removendo as funções associadas (usadas no mapeamento de grupos no Splunk). Depois que isso for feito, os usuários poderão ser removidos na instância do Splunk.

Se você estiver usando o Splunk Cloud, consulte este artigo Como remover usuários SAML antigos no Splunk

Se você estiver usando uma instância do Splunk no local, revise esta solução de comunidade Remover Usuários SAML Antigos

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.