DLPポリシーの包含および除外の設定

内容

はじめに

このドキュメントでは、DLPポリシーの包含および除外オプションを使用して、データ損失防止ルールを特定のIDに合わせて調整する方法について説明します。

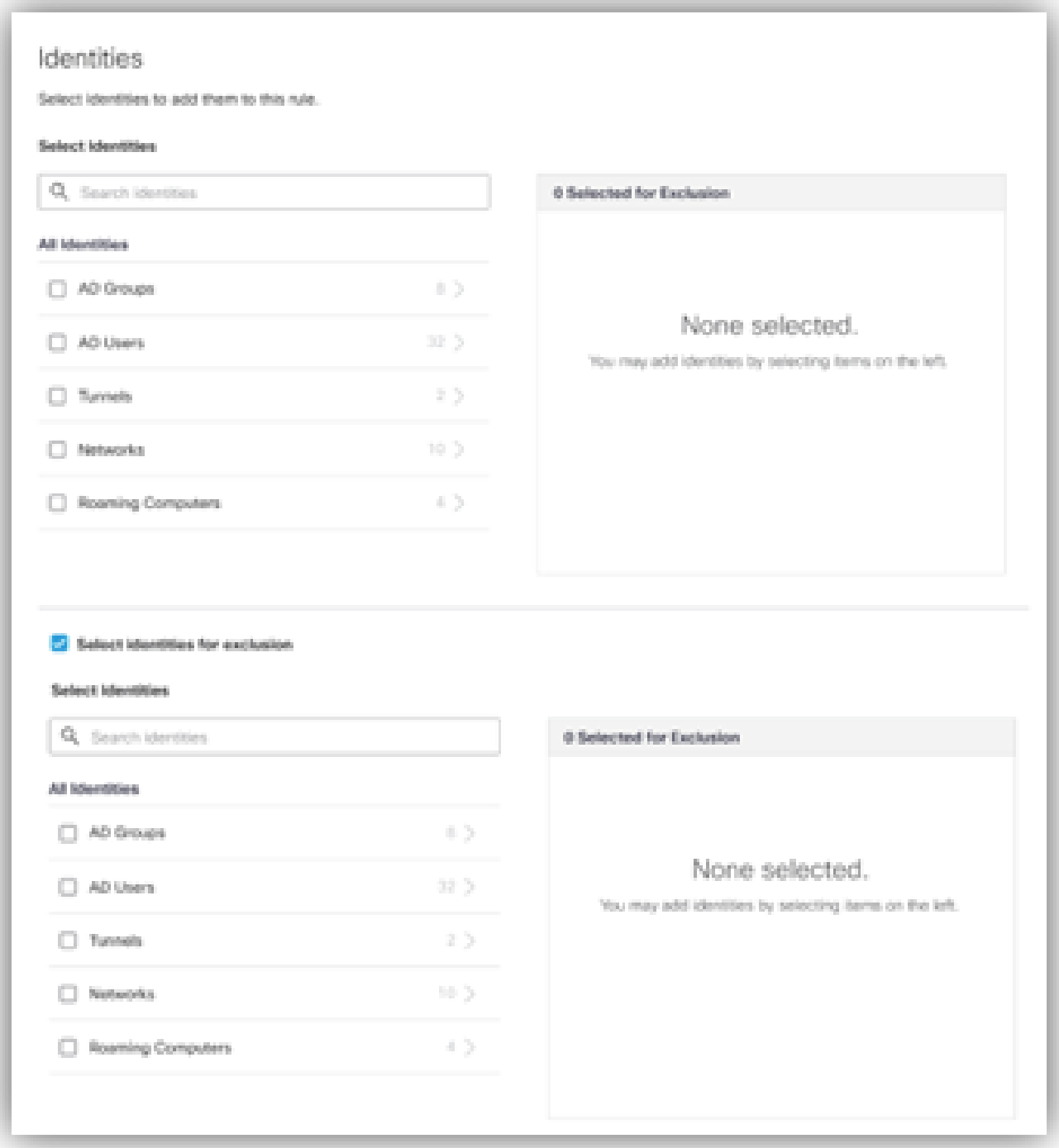
概要

DLPポリシーに含めるオプションと除外オプションを使用すると、データ損失防止ルールの対象となるIDを正確に定義できます。特定のユーザまたはグループを含めたり除外したりすることで、ポリシーの適用をより詳細に制御できます。

DLPポリシーの包含および除外オプションの利用

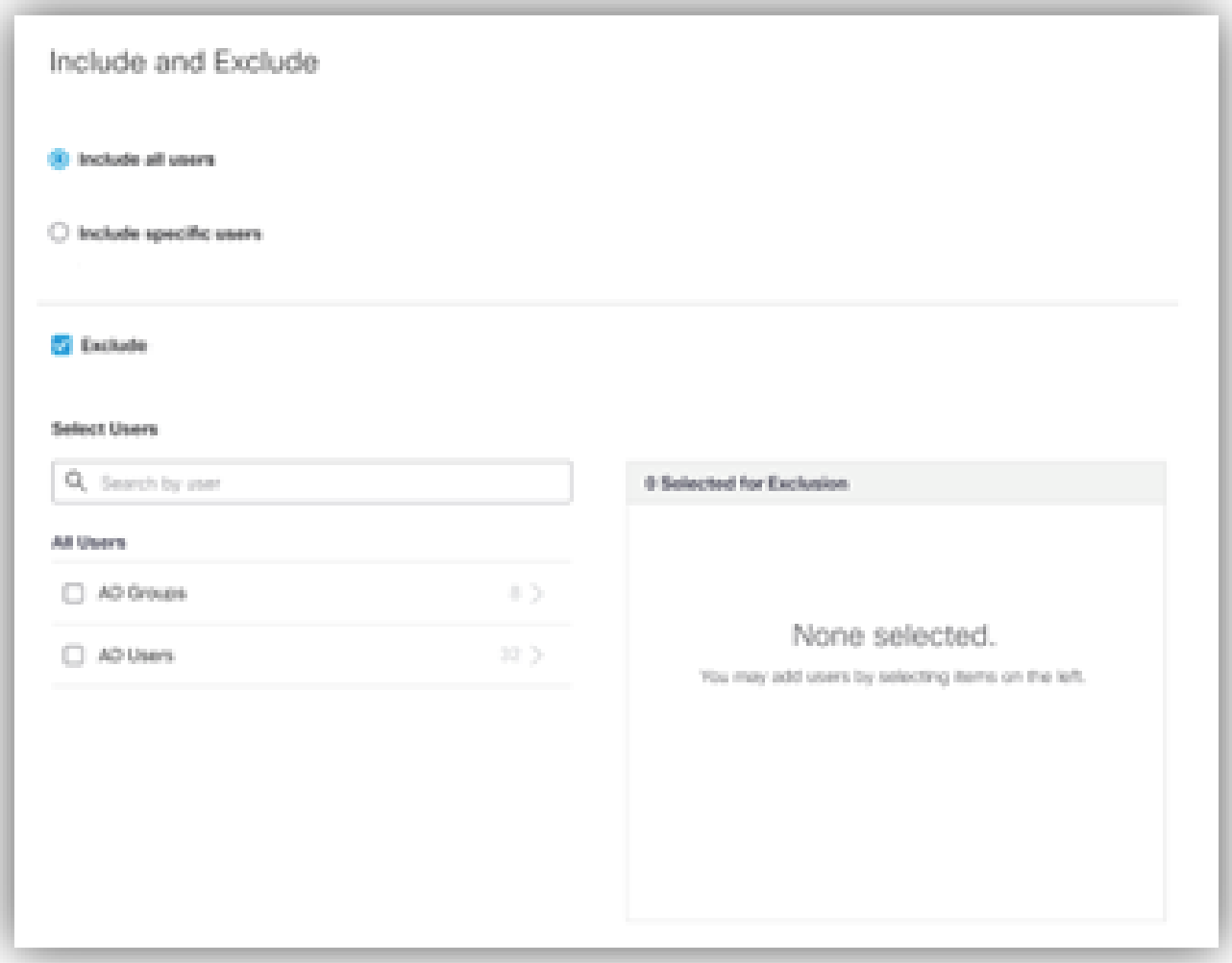
リアルタイムDLPルール

- UmbrellaまたはSecure Accessダッシュボードで、リアルタイムDLPルールを作成または編集します。
- Destinationsectionに移動します。
  - 同じリストにID（ユーザーまたはグループ）を含めたり、除外したりできるようになりました。
- これにより、指定したIDだけにDLPアクションを適用したり、必要に応じて特定のIDを除外したりできます。



SaaS API DLPルール

- SaaS API DLPルール設定で、「Include and Excludesection」に移動します。
  - ここで、同時に追加または除外するActive Directory(AD)ユーザおよびADグループを指定できます。
- これにより、選択したIDにDLPポリシーを適用したり、特定のユーザーまたはグループにポリシーが適用されないようにしたりすることができます。



詳細情報の検索

詳細な手順については、『Umbrella and Secure Access』のドキュメントを参照してください。

傘：

- データ損失防止ポリシーへのリアルタイムルールの追加
- データ損失防止ポリシーへのSaaS APIルールの追加

セキュアアクセス：

- データ損失防止ポリシーへのリアルタイムルールの追加
- データ損失防止ポリシーへのSaaS APIルールの追加

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。