Configure DLP Policy Inclusion and Exclusion

Contents

Introduction

This document describes how to use inclusion and exclusion options in DLP policies to tailor data loss prevention rules to specific identities.

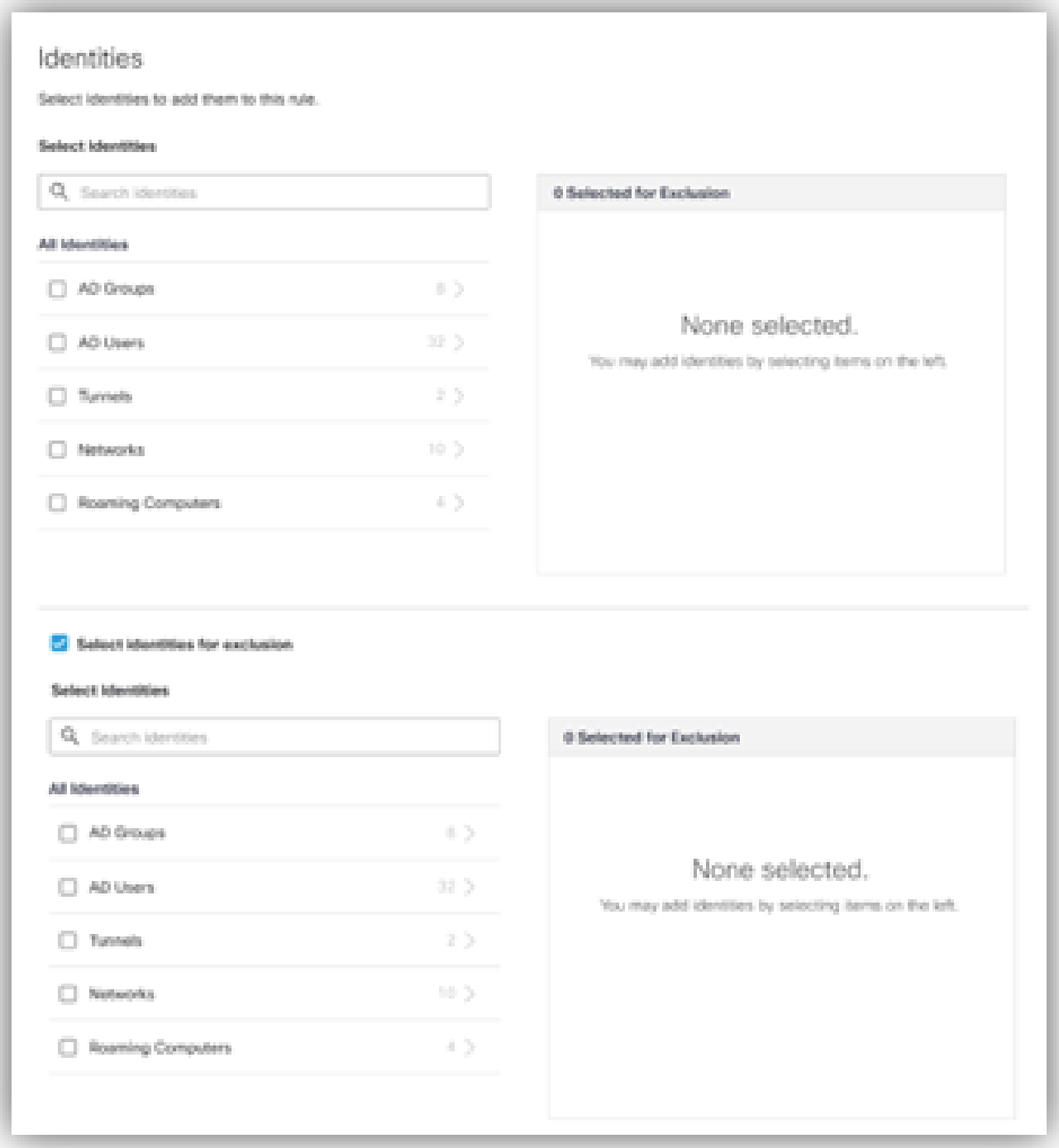
Overview

Inclusion and exclusion options in DLP policies let you precisely define which identities are covered by your data loss prevention rules. You can include or exclude specific users or groups, providing more granular control over policy enforcement.

Utilize DLP Policy Inclusion and Exclusion Options

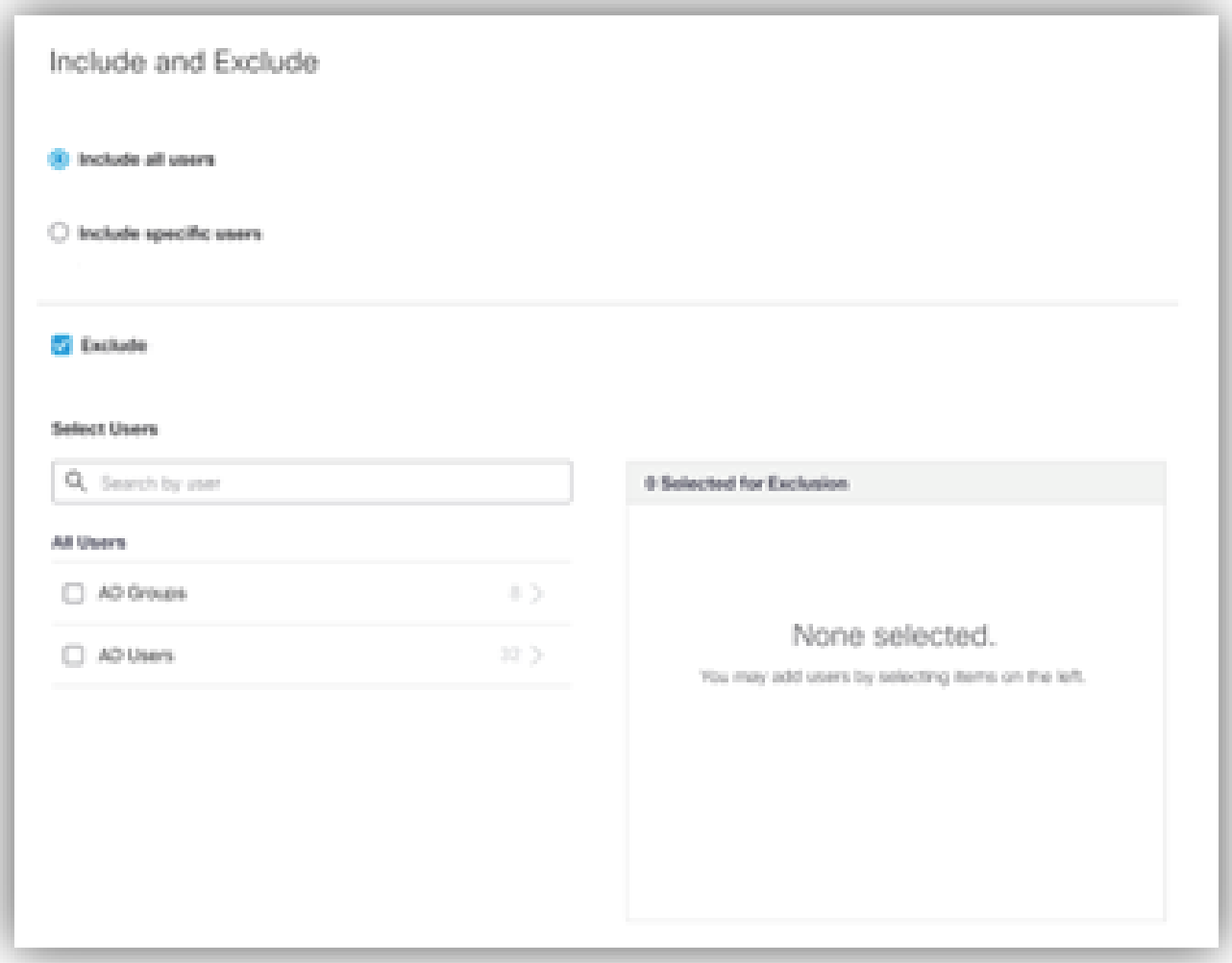
Real-Time DLP Rules

- In the Umbrella or Secure Access dashboard, create or edit a Real-Time DLP rule.
- Go to the**Destination**section.
  - You can now both include and exclude identities (users or groups) from the same list.
- This allows you to apply DLP actions to only the specified identities or to exempt certain identities as needed.



SaaS API DLP Rules

- In the SaaS API DLP rule configuration, go to the**Include and Exclude**section.
  - Here, you can specify which Active Directory (AD) users and AD groups to include or exclude at the same time.
- This enables you to enforce DLP policies on select identities or prevent policies from applying to certain users or groups.



Find More Information

Refer to Umbrella and Secure Access documentation for step-by-step guidance:

Umbrella:

- Add a Real Time Rule to the Data Loss Prevention Policy
- Add a SaaS API Rule to the Data Loss Prevention Policy

Secure Access:

- Add a Real Time Rule to the Data Loss Prevention Policy
- Add a SaaS API Rule to the Data Loss Prevention Policy