配置DLP策略包含和排除

目录

简介

本文档介绍如何在DLP策略中使用包含和排除选项来根据特定身份定制数据丢失保护规则。

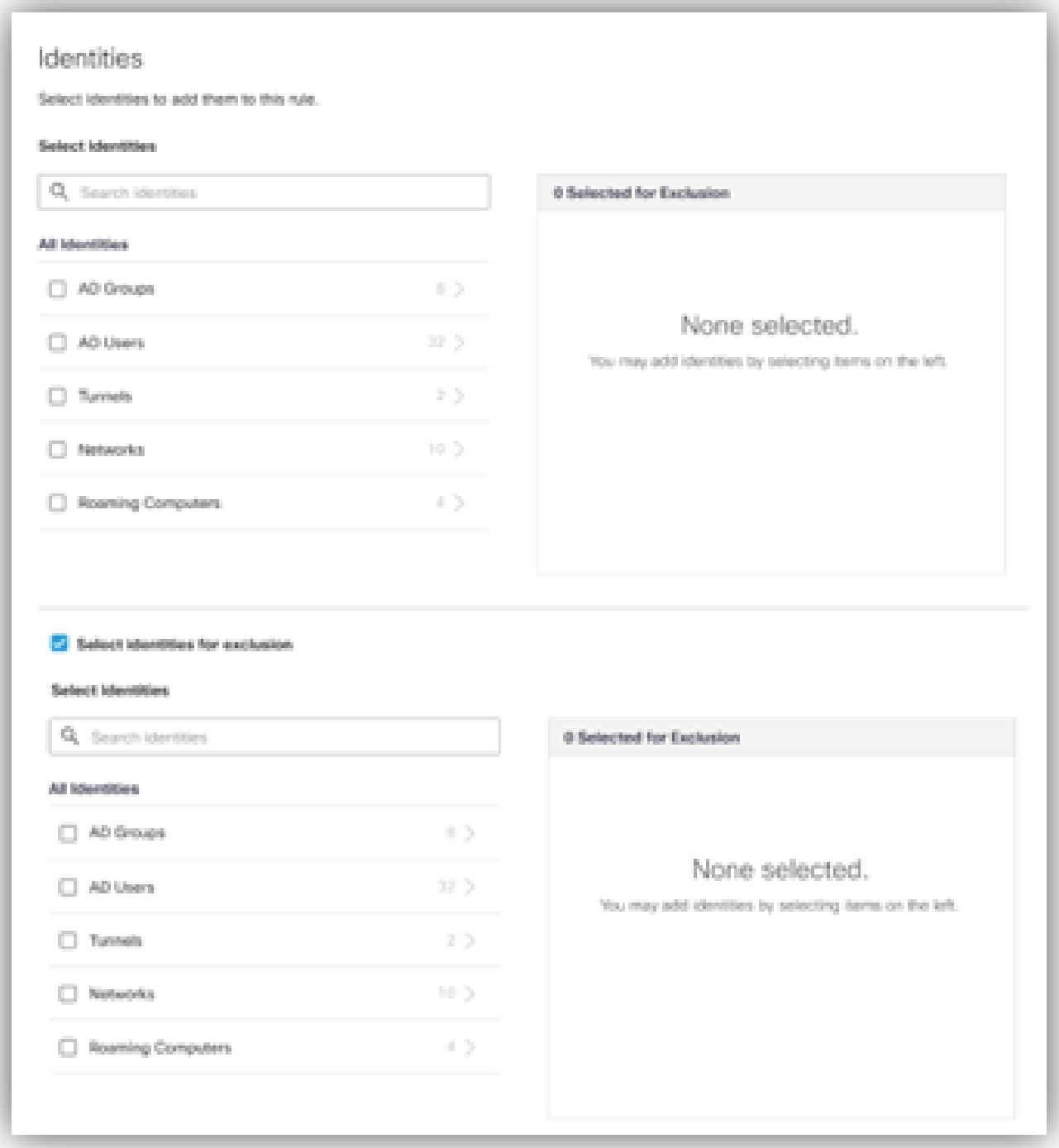
概述

通过DLP策略中的包含和排除选项，您可以精确定义数据丢失预防规则所涵盖的身份。您可以包括或排除特定用户或组，从而更精细地控制策略实施。

利用DLP策略包含和排除选项

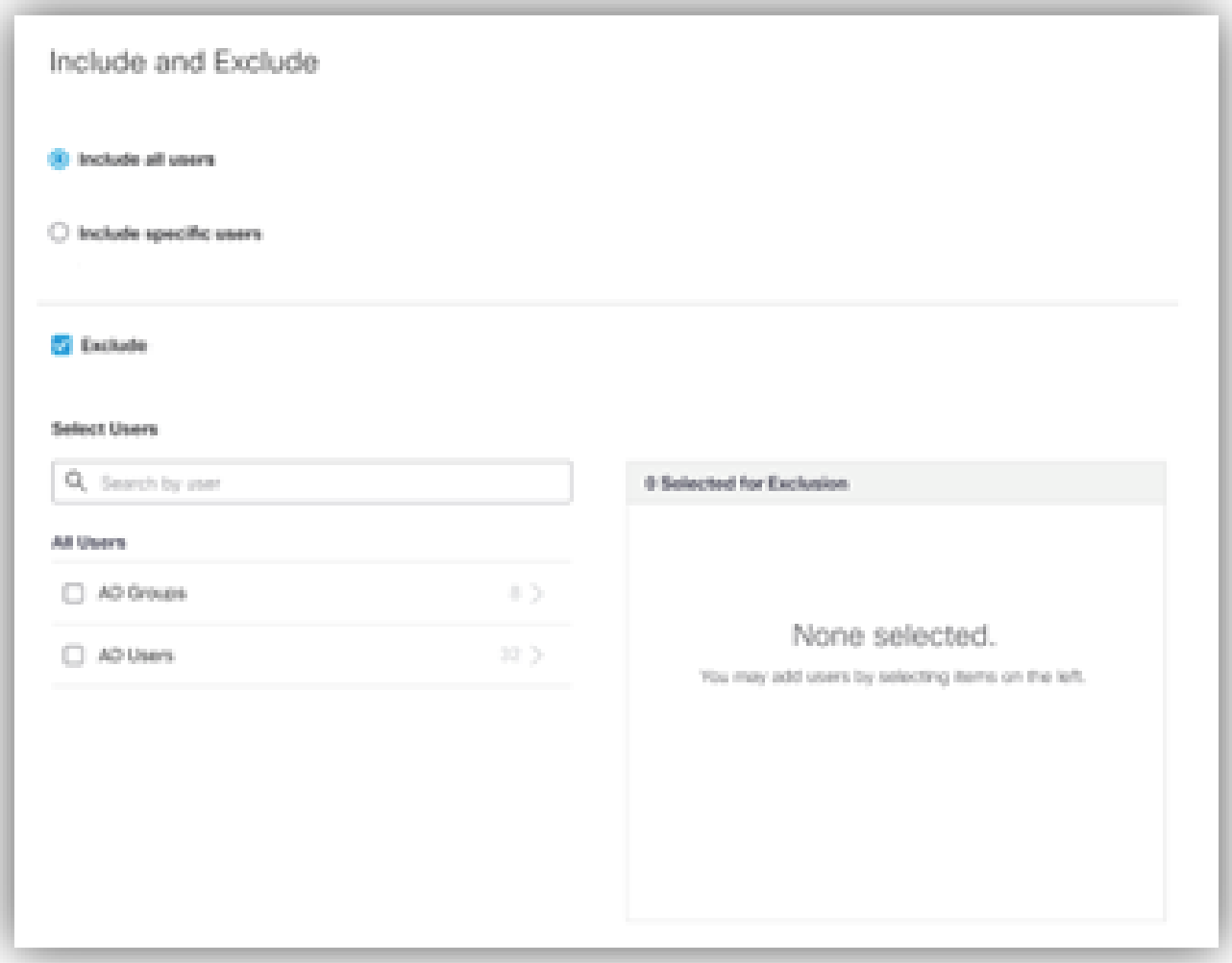
实时DLP规则

- 在Umbrella或安全访问控制面板中，创建或编辑实时DLP规则。
- 转到Destinationsection。
  - 现在，您可以在同一列表中包括和排除身份（用户或组）。
- 这允许您将DLP操作仅应用于指定的身份或根据需要免除某些身份。



SaaS API DLP规则

- 在SaaS API DLP规则配置中，转至Include and Excludesection。
  - 此处，您可以指定同时包括或排除哪些Active Directory(AD)用户和AD组。
- 这样，您就可以在选定的身份上实施DLP策略，或阻止策略应用于某些用户或组。



查找更多信息

有关分步指导，请参阅Umbrella and Secure Access文档：

雨伞：

- 向数据丢失保护策略添加实时规则
- 将SaaS API规则添加到防数据丢失策略

安全访问：

- 向数据丢失保护策略添加实时规则
- 将SaaS API规则添加到防数据丢失策略

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。