配置DLP策略包含和排除

目錄

簡介

本文檔介紹如何在DLP策略中使用包含和排除選項來根據特定身份定製資料丟失防護規則。

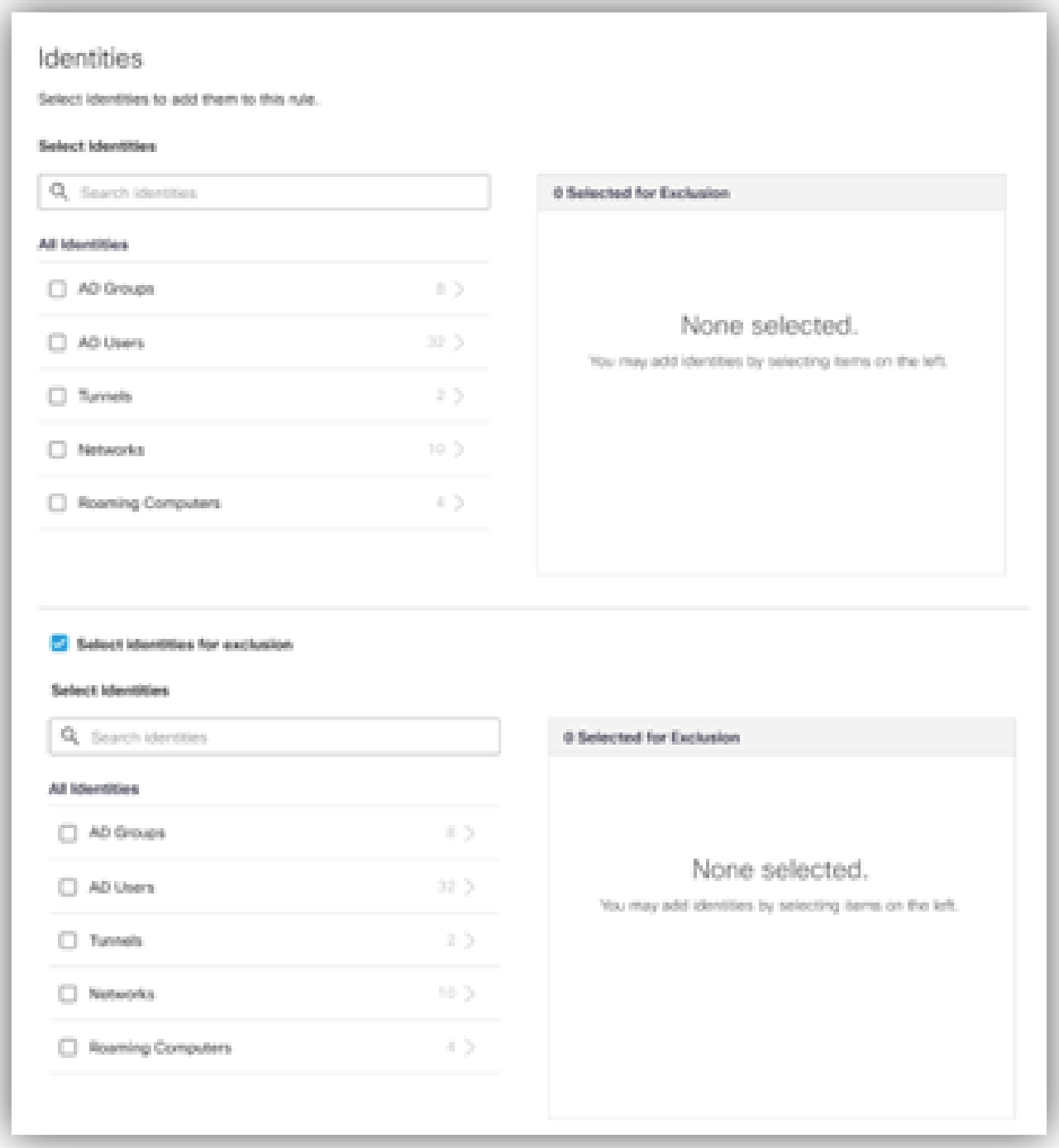
概觀

通過DLP策略中的包含和排除選項，您可以精確定義資料丟失預防規則所涵蓋的身份。您可以包括或排除特定使用者或組，從而對策略實施提供更精細的控制。

利用DLP策略包含和排除選項

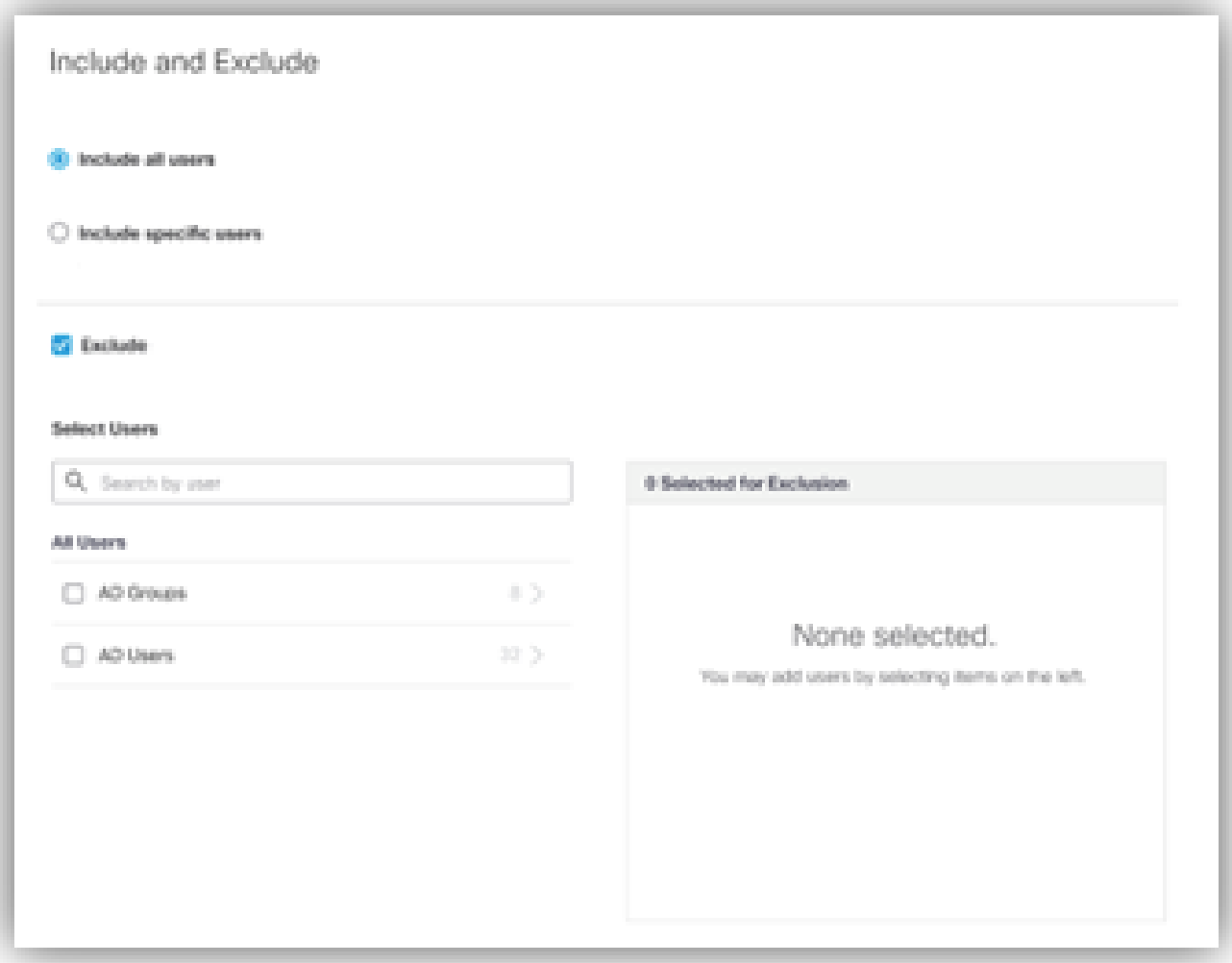
即時DLP規則

- 在Umbrella或Secure Access控制面板中，建立或編輯即時DLP規則。
- 轉到Destinationsection。
  - 現在，您可以從同一清單中包括和排除身份（使用者或組）。
- 這允許您僅將DLP操作應用於指定的身份或根據需要豁免某些身份。



SaaS API DLP規則

- 在SaaS API DLP規則配置中，轉至Include and Excludesection。
  - 在這裡，您可以指定同時包括或排除哪些Active Directory(AD)使用者和AD組。
- 這樣，您就可以在選定身份上實施DLP策略，或阻止策略應用於某些使用者或組。



尋找詳細資訊

請參閱Umbrella和Secure Access文檔以獲得逐步指導：

Umbrella:

- 向資料丟失保護策略新增即時規則
- 將SaaS API規則新增到資料丟失防護策略

安全訪問：

- 向資料丟失保護策略新增即時規則
- 將SaaS API規則新增到資料丟失防護策略

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。