Konfigurieren der Einbindung und Ausgrenzung von SvD-Policys

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Einschluss- und Ausschlussoptionen in SvD-Policys verwenden, um die Regeln zum Schutz vor Datenverlust an bestimmte Identitäten anzupassen.

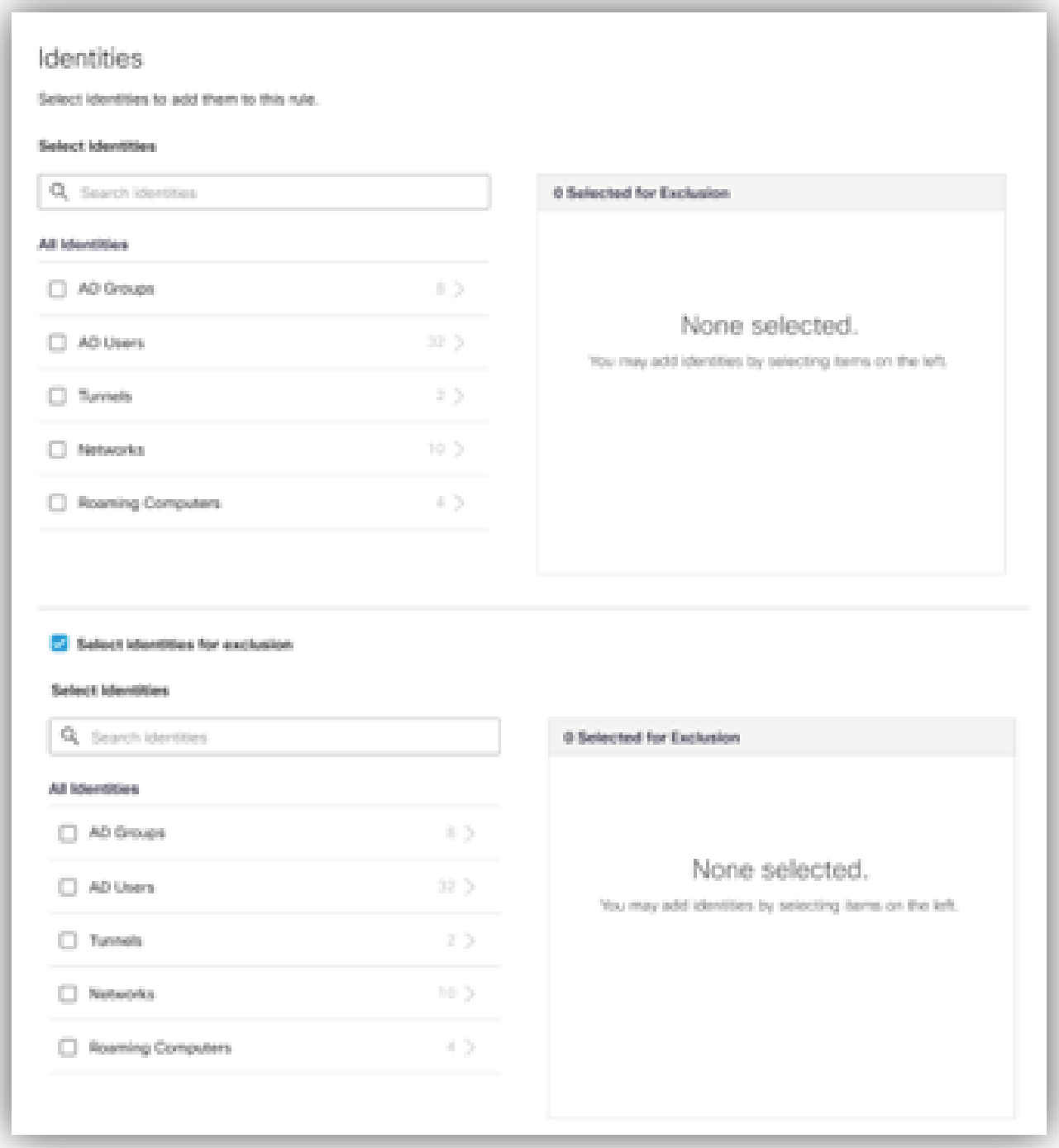
Überblick

Mit den Einschluss- und Ausschlussoptionen in SvD-Policys können Sie genau definieren, welche Identitäten von Ihren Regeln zum Schutz vor Datenverlust abgedeckt werden. Bestimmte Benutzer oder Gruppen können ein- oder ausgeschlossen werden, wodurch die Durchsetzung von Richtlinien präziser kontrolliert werden kann.

Nutzen Sie DLP-Richtlinienoptionen für Ein- und Ausschluss

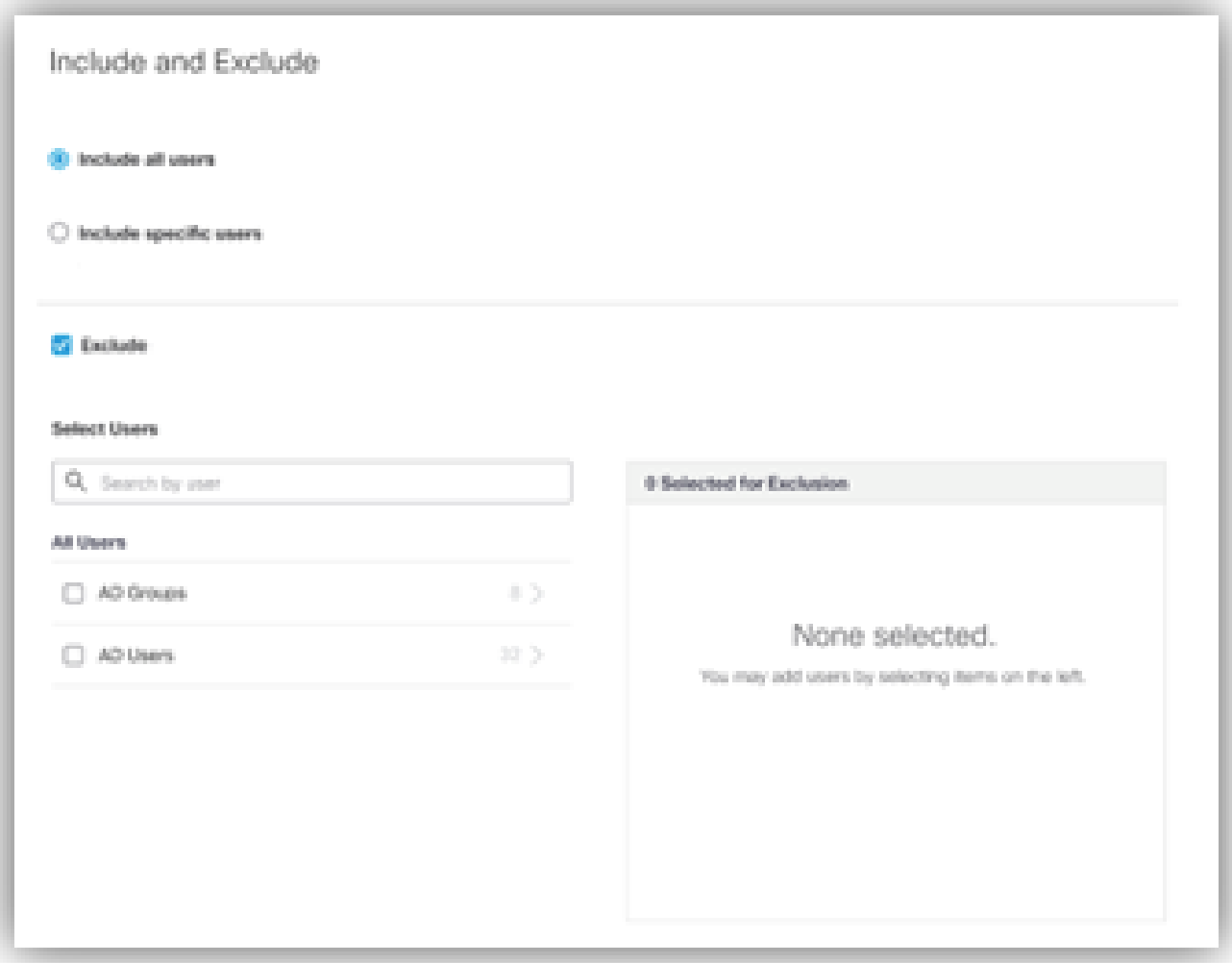
DLP-Regeln in Echtzeit

- Erstellen oder bearbeiten Sie im Dashboard Umbrella (Umbrella) oder Secure Access (Sicherer Zugriff) eine Regel für Echtzeit-SvD.
- Fahren Sie mit dem AbschnittZiel fort.
    - Sie können nun Identitäten (Benutzer oder Gruppen) in derselben Liste ein- und ausschließen.
- Dadurch können Sie SvD-Aktionen nur auf die angegebenen Identitäten anwenden oder bestimmte Identitäten bei Bedarf ausschließen.



SaaS-API-SvD-Regeln

- Navigieren Sie in der Konfiguration der SaaS-API-SvD-Regel zu den Abschnitten "Include" und "Excluding".
    - Hier können Sie angeben, welche Active Directory-Benutzer (AD) und AD-Gruppen gleichzeitig ein- oder ausgeschlossen werden sollen.
- Auf diese Weise können Sie SvD-Richtlinien für ausgewählte Identitäten durchsetzen oder verhindern, dass Richtlinien auf bestimmte Benutzer oder Gruppen angewendet werden.



Weitere Informationen

Eine schrittweise Anleitung finden Sie in der Umbrella and Secure Access-Dokumentation:

Regenschirm:

- Hinzufügen einer Echtzeitregel zur Richtlinie zum Schutz vor Datenverlust
- Hinzufügen einer SaaS-API-Regel zur Richtlinie zum Schutz vor Datenverlust

Sicherer Zugriff:

- Hinzufügen einer Echtzeitregel zur Richtlinie zum Schutz vor Datenverlust
- Hinzufügen einer SaaS-API-Regel zur Richtlinie zum Schutz vor Datenverlust

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.