# Kennenlernen der Umbrella Policy-Auswahl unter Beteiligung mehrerer Organisationen

## Inhalt



## Einleitung

In diesem Dokument werden die Richtlinien mehrerer Umbrella-Organisationen beschrieben, die in bestimmten Szenarien berücksichtigt werden.

## Überblick

In bestimmten Szenarien können die Richtlinien mehrerer Umbrella-Organisationen berücksichtigt werden. Ein Beispiel hierfür wäre ein Roaming-Client oder ein Mobilgerät für eine Organisation, die sich mit dem Netzwerk einer anderen Organisation verbindet. In diesem Artikel wird erläutert, wie die Richtlinie derzeit in diesem Fall gewählt wird und welche Änderungen Umbrella plant, um dieses Verhalten zu verbessern.

## Richtlinienauswahl über ein einziges Unternehmen

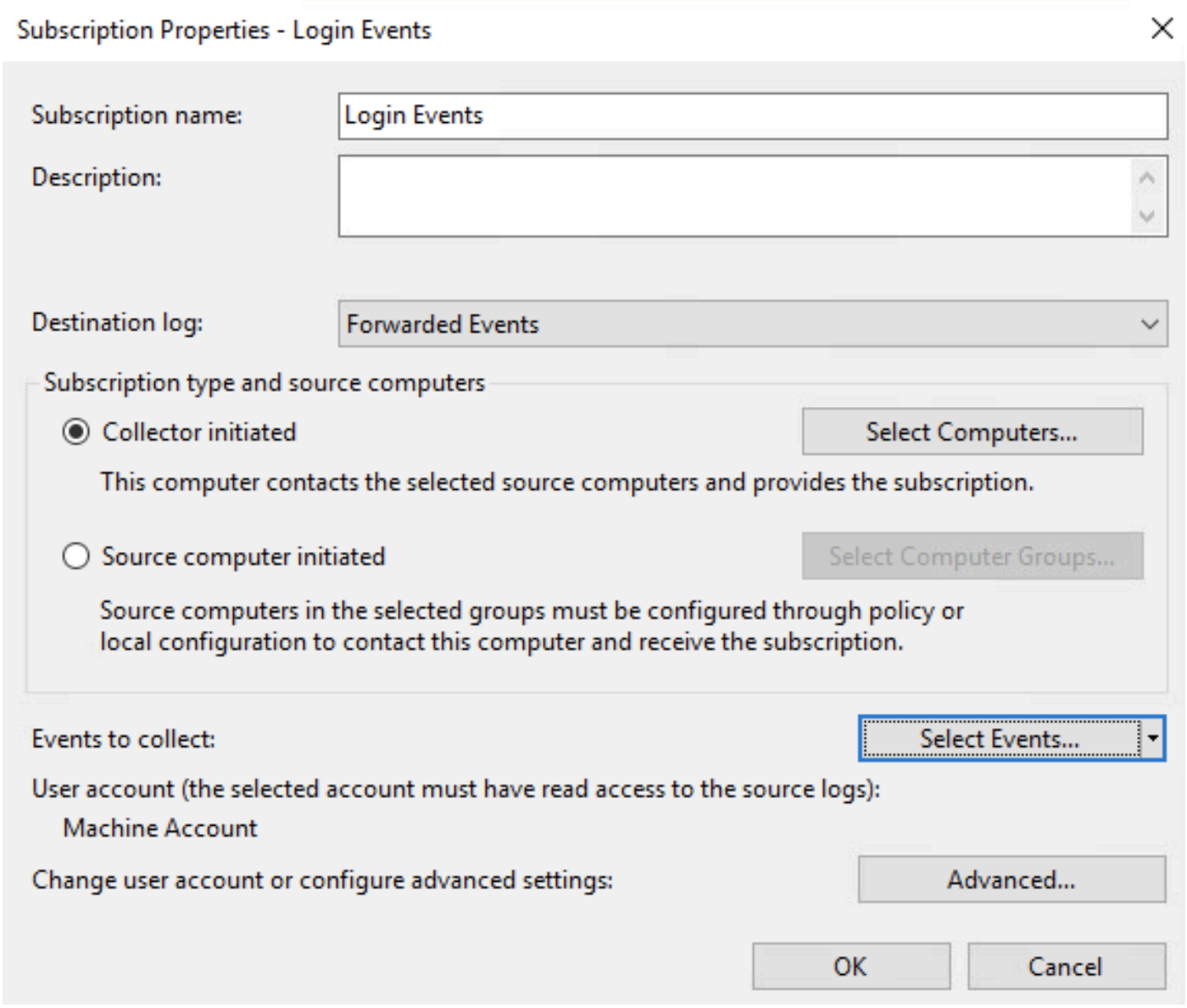
Wenn eine DNS-Abfrage an Umbrella gesendet wird, können der Abfrage mehrere Identitäten zugeordnet werden. Beispielsweise würde eine Abfrage von einem Roaming-Client (RC) hinter einem geschützten Netzwerk sowohl die Geräte-ID des RC als auch die IP-Adresse des Netzwerks enthalten. Ebenso umfasst eine Abfrage von einer virtuellen Appliance die Standort-ID, das interne Netzwerk, den AD-Benutzer und die AD-Gruppe.

Normalerweise sind die in der Abfrage enthaltenen Identitäten alle einer einzelnen Organisation zugeordnet. In diesem Fall verwendet die durchgesetzte Richtlinie die in unserer Dokumentation beschriebenen Richtlinien-Prioritätsregeln:

https://docs.umbrella.com/deployment-umbrella/docs/policy-precedence

Kurz gesagt, Umbrella weist jeder Richtlinie eine Priorität zu, basierend auf ihrer Reihenfolge im Dashboard , wobei die oberste Richtlinie die höchste Priorität hat. Die Umbrella-Resolver wählen die Richtlinie mit der höchsten Priorität aus, die für mindestens eine der in der Abfrage vorhandenen Identitäten gilt.

In Organisation A können z. B. folgende Richtlinien definiert sein:



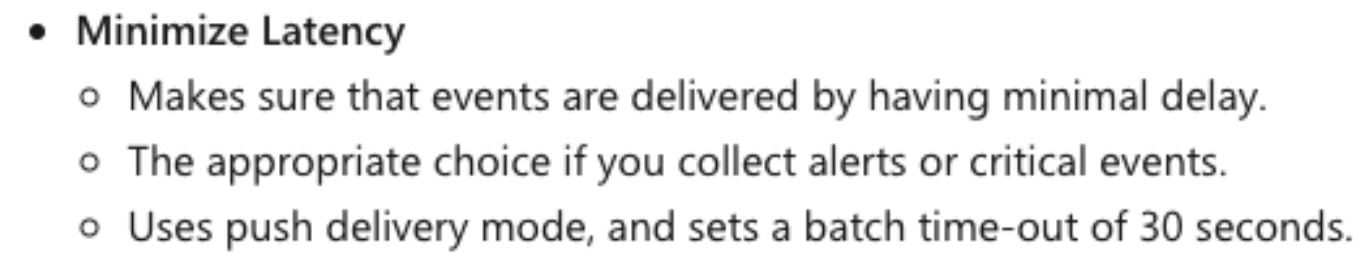

mceclip0.png

Die Richtlinie des Roaming-Computers hat die Priorität 2, während die Richtlinie des Netzwerks die Priorität 1 hat. Wenn also eine Abfrage von einem Roaming-Computer eingeht, der zu einem externen Netzwerk gehört, wird die Richtlinie 2 angewendet. Wenn der Roaming-Computer jedoch einem der Netzwerke von Organisation A hinzugefügt wurde, würde Richtlinie 1 gelten, da die Richtlinie des Netzwerks eine höhere Priorität hat.

## Richtlinienauswahl bei mehreren Organisationen

Dieselbe Logik wird angewendet, wenn Identitäten aus mehreren Organisationen in der Abfrage enthalten sind. Da jedoch mehrere Organisationen beteiligt sind, wird die relative Priorität jeder Richtlinie in Bezug auf die Richtlinienliste der einzelnen Organisationen berücksichtigt.

Ein Beispiel erklärt dies am besten. Für Organisation A und Organisation B sind in den jeweiligen Umbrella Dashboards folgende Richtlinien definiert:




mceclip2.png

Ein Roaming-Computer aus Organisation A wird dann einem Netzwerk hinzugefügt, das zu Organisation B gehört. Die an Umbrella gesendete DNS-Abfrage enthält somit die Geräte-ID von Organisation A und die IP-Adresse des Netzwerks von Organisation B.

Mithilfe der Logik einer einzelnen Organisation erhalten wir die Prioritäten für die Richtlinien jeder Identität. Der RC von Organisation A erhält die Richtlinie A2, die eine Priorität von 2 hat, während das Netzwerk von Organisation B die Richtlinie B1 erhält, die eine Priorität von 1 hat. Daher wird die Richtlinie für das Netzwerk von Organisation B, die Richtlinie B1, angewendet.

## Reporting mit mehreren Organisationen

Wenn eine Abfrage Identitäten aus mehreren Organisationen enthält, wird die Abfrage nur in den Berichten für die Organisation angezeigt, deren Richtlinie ausgewählt wurde. Die Berichte für diese Organisation enthalten AUSSCHLIESSLICH die Identitäten, die zu dieser Organisation gehören. Eine Organisation hat NIE Einblick in die anderen Identitäten in der Abfrage, die zu anderen Organisationen gehören.

## Auswirkungen auf das aktuelle Verhalten bei der Richtlinienauswahl

Aufgrund des beschriebenen Verhaltens bei der Richtlinienauswahl ist es möglich, dass die Richtlinie einer Identität einer Organisation durch die Richtlinie einer anderen Organisation außer Kraft gesetzt wird. Dies umfasst alle Richtlinienfunktionen, einschließlich Sicherheits- und Inhaltsblockierung, Ziellisten, Design von Blockseiten und Protokollierungseinstellungen (unter Berücksichtigung der Einschränkungen bei der Berichterstellung), mit Ausnahme von Blockseitenumleitungen.

### Dedizierte Blockseiten für Szenarien mit mehreren Organisationen

Ab dem 16. Juli 2021, wenn die Umbrella-Resolver erkennen, dass eine Abfrage Identitäten von mehreren Organisationen enthält, werden blockierte Abfragen auf eine dedizierte Blockseite umgeleitet. Diese Blockseite informiert den Benutzer darüber, dass mehr als eine Organisation erkannt wurde und die Abfrage daher möglicherweise aufgrund der Richtlinie einer anderen Organisation blockiert wurde.

# Geplante Änderungen für die Richtlinienauswahl unter Einbeziehung mehrerer Organisationen

Umbrella plant, das Verhalten der Richtlinienauswahl zu ändern, wenn mehr als eine Organisation beteiligt ist. Künftige Änderungen:

## Verhalten bei Richtlinienauswahl

Umbrella ändert das Richtlinienauswahlverhalten, sodass die Richtlinie mit der höchsten Priorität für jede Organisation ausgewählt und durchgesetzt wird. Wenn dann eine dieser Richtlinien die Abfrage blockiert, wird die Abfrage blockiert. Auf diese Weise können alle beteiligten Organisationen sicherstellen, dass ihre Richtlinien nicht umgangen werden. Dieses Verhalten lässt sich am besten anhand einer Analogie erklären:

Alice Eltern sagen, dass ihre individuellen Regeln wichtiger sind als Hausregeln. Alice darf nicht zu jeder Zeit und an jedem Ort Eis essen.

Bobs Eltern sagen, dass Hausregeln wichtiger sind als individuelle Regeln. Sie lassen niemals Pizza zu Hause.

Aktuelles Modell:

Alice geht zu Bob. Es gelten die Hausregeln von Bob und nicht die von Alice. Alice kann Eis essen, aber keine Pizza. Bobs Eltern erhalten einen Bericht, dass jemand Eis in ihrem Haus gegessen hat, aber es heißt nicht, dass es Alice mit Namen war.

Vorgeschlagenes Modell:

Alice geht zu Bob. Es gelten die Hausregeln von Bob, und es gelten die individuellen Regeln von Alice. Alice hat weder Eis noch Pizza. Bobs Eltern erhalten einen Bericht, der besagt, dass jemandem Pizza und Eis verweigert wurde, aber er sagt nicht, dass es Alice mit Namen war.

## Berichte für alle beteiligten Organisationen

Wenn das Richtlinienauswahl-Verhalten festgelegt wurde, stellt Umbrella außerdem sicher, dass alle Abfragen, die Identitäten mehrerer Organisationen betreffen, in die Berichte aller beteiligten Organisationen aufgenommen werden. Die Berichte enthalten NUR Identitäten, die zu dieser Organisation gehören - eine bestimmte Organisation sieht NIE die Identitäten einer anderen Organisation.

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.