# Warum kann ich bei einer Verzeichnissuche in Zugriffsrichtlinien keine AD-Gruppen für vertrauenswürdige Domänen finden?

## Inhalt

## Frage:

Warum kann ich bei einer Verzeichnissuche in Zugriffsrichtlinien keine AD-Gruppen für vertrauenswürdige Domänen finden?

**Umgebung**: Cisco Web Security Appliance (WSA), NTLM-Authentifizierung, Trusted Domains

**Symptome**:

- Der Benutzer versucht, eine "Active Directory-Gruppe" zu suchen, die als *Policy Member Definition* in einer seiner Zugriffsrichtlinien verwendet werden soll, und die Gruppe wird in der Verzeichnissuche nicht angezeigt.
- Die Gruppe gehört zu einer vertrauenswürdigen AD-Domäne und nicht zu der Domäne, der die WSA beigetreten ist.

Dieses Verhalten ist beabsichtigt. Beim Konfigurieren von Gruppen in Zugriffsrichtlinien werden die Gruppen aus vertrauenswürdigen Domänen bei der *Verzeichnissuche* nicht angezeigt.

In allen AsyncOS-Versionen kann die WSA Benutzer aus einer anderen Domäne authentifizieren und ihren jeweiligen AD-Gruppen zuordnen**, wenn** die andere Domäne über eine Zwei-Wege-Vertrauenswürdigkeit mit der Domäne verfügt, der die WSA angehört.

In einem solchen Szenario können die Gruppen aus vertrauenswürdiger Domäne in Zugriffsrichtlinien wie folgt hinzugefügt werden:

1. Navigieren Sie zu GUI —> Web Security Manager —> Zugriffsrichtlinien —> *<Policy Name>* —> Selected Groups and Users —> Groups
2. Geben Sie manuell den gesamten Gruppennamen zusammen mit dem Domänennamen in das Feld *"Verzeichnissuche"* ein.
3. Klicken Sie auf die Schaltfläche "Hinzufügen".
4. Klicken Sie auf "Fertig" und dann auf "Senden", und bestätigen Sie die Änderungen.

Beachten Sie, dass die WSA nicht mit den manuell konfigurierten Gruppen übereinstimmt, wenn die andere Domäne keine Zwei-Wege-Vertrauensbeziehung zur Domäne aufweist, der die WSA angehört.

**Hinweis:** Auf AsyncOS-Versionen 7.7 und höher unterstützt die WSA mehrere NTLM-Bereiche. In Szenarien, in denen keine Vertrauensbeziehung zwischen den beiden Domänen besteht, können wir einen neuen NTLM-Bereich für die zweite Domäne erstellen. Bei mehreren NTLM-Bereichen

kann die WSA Gruppen aus verschiedenen Domänen innerhalb der Zugriffsrichtlinien durchsuchen.