

# Wie konfiguriere ich meine WSA für die LDAP-Authentifizierungsgruppenrichtlinie?

## Inhalt

[Frage:](#)

## Frage:

**Umgebung:** Cisco Web Security Appliance (WSA), alle Versionen von AsyncOS

Dieser Knowledge Base-Artikel bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Wenden Sie sich für weitere Unterstützung an den Softwareanbieter.

Damit "Authentication Group" (Authentifizierungsgruppe) funktioniert, müssen wir zunächst einen Authentifizierungsbereich unter "GUI > Network > Authentication" (GUI > Netzwerk > Authentifizierung) konfigurieren.

1. Legen Sie zunächst "Authentication Protocol" als "LDAP" fest und navigieren Sie zu "Group Authorization" (Gruppenautorisierung) (wobei der andere Abschnitt korrekt konfiguriert ist).
2. Geben Sie Ihr "Group Name Attribute" an. Dieses Attribut enthält den Wert, der unter "Web Security Manager" > "Web Access Policies" > "Click Add Group" > "Select Group Type to Authentication Group" > "Directory Lookup" (Verzeichnissuche) angezeigt wird. Dieses Attribut muss eindeutig sein, und der durch dieses Attribut dargestellte Leaf-Knoten muss eine Liste von Benutzern in seiner Gruppe enthalten.
3. Geben Sie als Nächstes die "Gruppenfilterabfrage" an. Dies ist der Suchfilter, den die WSA verwendet, um alle GROUP im LDAP-Verzeichnis zu finden.
4. Geben Sie jetzt "Group Membership Attribute" (Gruppenmitgliedschaftsattribut) an. Dies ist das Attribut im Leaf-Knoten, das die Member mit einem eindeutigen Wert enthält. Da dieses Attribut das Mitglied dieser GRUPPE enthält, werden mehrere Einträge angezeigt. Stellen Sie sicher, dass der in diesem Attribut enthaltene Wert dem Wert entspricht, der in "User Name Attribute" auf derselben Seite enthalten ist.

Im Folgenden sehen Sie ein Beispiel dafür, wie die WSA die LDAP-Bereichskonfiguration verwendet, um einen Benutzernamen mit einer LDAP-Gruppe abzugleichen:

1. Angenommen, wir setzen "Gruppenfilter-Abfrage" auf "objectClass=group"
2. Die WSA würde diesen Filter zuerst verwenden, um das LDAP-Verzeichnis zu durchsuchen und das Ergebnis zu finden.
3. Anschließend sucht die WSA mithilfe des Ergebnisses nach dem unter "Gruppenmitgliedschaft-Attribut" angegebenen Attribut. Nehmen wir an, dies ist ein Attribut

namens "Mitglied".

4. Wenn sich ein Benutzer nun über den WSA-Proxy als 'USERNAME\_A' anmeldet, sucht die WSA im LDAP-Server nach dem Benutzerkonto. Falls eine Übereinstimmung vorliegt, verwendet die WSA das unter "User Name Attribute" angegebene Attribut (Beispiel: uid) und überprüft, ob "uid" mit den Benutzern übereinstimmt, die im oben erfassten Attribut "member" aufgeführt sind.
5. Wenn eine Übereinstimmung vorliegt, würde der Benutzer die konfigurierte Richtlinie verwenden. Andernfalls würde die WSA die nächste Richtlinie in der Zeile auswerten.

Weitere Informationen zu den Attributen, die mit Ihrem LDAP-Server konfiguriert werden müssen, finden Sie unter "Softerra LDAP Browser" <http://www.ldapbrowser.com>