# Cisco VPN Client Benutzer- und Gruppen-Attributverarbeitung auf dem VPN 3000 Concentrator

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie Cisco VPN-Clients im VPN Concentrator authentifiziert werden und wie der Cisco VPN 3000 Concentrator Benutzer- und Gruppenattribute verwendet.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco VPN 3000 Concentrator.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

## VPN-Client verbindet sich mit einem VPN 300-Konzentrator

Wenn ein VPN-Client eine Verbindung mit einem VPN 3000-Konzentrator herstellt, können bis zu vier Authentifizierungen erfolgen.

1. Die Gruppe wird authentifiziert. (Dies wird häufig als "Tunnelgruppe" bezeichnet.)
2. Der Benutzer wird authentifiziert.
3. (Optional) Wenn der Benutzer Teil einer anderen Gruppe ist, wird diese Gruppe als Nächstes authentifiziert. Wenn der Benutzer keiner anderen Gruppe oder Tunnel-Gruppe angehört, wird der Benutzer standardmäßig zur Basisgruppe hinzugefügt, und dieser Schritt tritt NICHT auf.
4. Die "Tunnelgruppe" aus Schritt 1 wird erneut authentifiziert. (Dies ist der Fall, wenn die Funktion "Gruppensperrung" verwendet wird. Diese Funktion ist ab Version 2.1 verfügbar.)

Dies ist ein Beispiel für Ereignisse, die im Ereignisprotokoll für einen über die interne Datenbank authentifizierten VPN-Client angezeigt werden ( "testuser" ist Teil der Gruppe "Engineering").

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

**Hinweis:** Um diese Ereignisse anzuzeigen, müssen Sie die Auth Event Class mit dem Schweregrad 1-6 in **Configuration > System > Events > Classes** konfigurieren.

**Gruppensperrfunktion** - Wenn die Gruppensperrfunktion in der Gruppe - Tunnel_Group aktiviert ist, muss der Benutzer Teil der Gruppe Tunnel_Group sein, um eine Verbindung herzustellen. Im vorherigen Beispiel werden alle Ereignisse angezeigt, aber "testuser" stellt keine Verbindung her, da sie Teil der Gruppe - Engineering und nicht der Gruppe - Tunnel_Group sind. Diese Veranstaltung wird auch angezeigt:

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

Weitere Informationen über die Gruppensperrfunktion und eine Beispielkonfiguration finden Sie unter Locken von Benutzern in eine VPN 3000-Concentrator-Gruppe mithilfe eines RADIUS-Servers.

## Externe Authentifizierung von Gruppen und Benutzern über RADIUS

Der VPN 3000 Concentrator kann auch so konfiguriert werden, dass Benutzer und Gruppen extern über einen RADIUS-Server authentifiziert werden. Dies erfordert jedoch, dass die Namen der Gruppen im VPN-Konzentrator konfiguriert werden. Der Gruppentyp ist jedoch als "Extern" konfiguriert.

- Externe Gruppen können Cisco/Altiga-Attribute zurückgeben, wenn der RADIUS-Server VSAs

(Vendor Specific Attributes) unterstützt.
- Alle Cisco/Altiga-Attribute, die NICHT standardmäßig über RADIUS an die Werte in der Basisgruppe zurückgegeben werden.
- Wenn der RADIUS-Server KEINE VSAs unterstützt, gelten für ALLE Attribute die Standardattribute für die Basisgruppenattribute.

**Hinweis:** Ein RADIUS-Server behandelt Gruppennamen nicht anders als Benutzernamen. Eine Gruppe auf einem RADIUS-Server wird wie ein Standardbenutzer konfiguriert.

In diesen Schritten wird beschrieben, was geschieht, wenn ein IPSec-Client eine Verbindung zum VPN 3000-Konzentrator herstellt, wenn sowohl Benutzer als auch Gruppen extern authentifiziert werden. Ähnlich wie im internen Fall können bis zu vier Authentifizierungen erfolgen.

1. Die Gruppe wird über RADIUS authentifiziert. Der RADIUS-Server kann viele oder gar keine Attribute für die Gruppe zurückgeben. Der RADIUS-Server muss mindestens das Cisco/Altiga-Attribut "IPSec Authentication = RADIUS" zurückgeben, um dem VPN Concentrator die Authentifizierung des Benutzers mitzuteilen. Andernfalls muss die IPSec-Authentifizierungsmethode der Basisgruppe auf "RADIUS" festgelegt werden.
2. Der Benutzer wird über RADIUS authentifiziert. Der RADIUS-Server kann viele oder gar keine Attribute für den Benutzer zurückgeben. Wenn der RADIUS-Server das Attribut CLASS (das RADIUS-Standardattribut #25) zurückgibt, verwendet der VPN 3000 Concentrator dieses Attribut als Gruppennamen und wechselt zu Schritt 3, oder er fährt mit Schritt 4 fort.
3. Die Benutzergruppe wird anschließend über RADIUS authentifiziert. Der RADIUS-Server kann viele oder gar keine Attribute für die Gruppe zurückgeben.
4. Die "Tunnelgruppe" aus Schritt 1 wird erneut über RADIUS authentifiziert. Das Authentifizierungs-Subsystem muss die Tunnelgruppe erneut authentifizieren, da es die Attribute (falls vorhanden) aus der Authentifizierung in Schritt 1 nicht gespeichert hat. Dies ist der Fall, wenn die Funktion "Gruppensperrung" verwendet wird.

## Verwendung von Benutzer- und Gruppenattributen durch den VPN 3000-Concentrator

Nachdem der VPN 3000-Concentrator den Benutzer und die Gruppen authentifiziert hat, muss er die erhaltenen Attribute organisieren. Der VPN Concentrator verwendet die Attribute in dieser Reihenfolge der Voreinstellungen. Es spielt keine Rolle, ob die Authentifizierung intern oder extern erfolgt ist:

1. **Benutzerattribute** - Diese haben Vorrang vor allen anderen.
2. **Gruppenattribute** - Alle Attribute, die in den Benutzerattributen fehlen, werden durch die Gruppenattribute ausgefüllt. Alle gleichen Elemente werden durch die Benutzerattribute überschrieben.
3. **Tunnelgruppenattribute** - Alle Attribute, die in den Benutzer- oder Gruppenattributen fehlen, werden durch die Tunnelgruppenattribute ausgefüllt. Alle gleichen Elemente werden durch die Benutzerattribute überschrieben.
4. **Basigruppenattribute** - Alle Attribute, die in den Attributen "Benutzer", "Gruppe" oder "Tunnel Group" fehlen, werden durch die Attribute "Base Group" ausgefüllt.

## Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- Support-Seite für Cisco VPN-Clients
- IPSec-Support-Seite
- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Technischer Support - Cisco Systems