# Locking Users into a VPN 3000 Concentrator Group Using a RADIUS Server

**Document ID: 13831**

## Contents

## Introduction

The Cisco VPN 3000 Concentrator has the ability to lock users into a Concentrator group which overrides the group the user has configured in the Cisco VPN 3000 Client. In this way, access restrictions can be applied to various groups configured on the VPN Concentrator with the assurance that the users are locked into that group with the RADIUS server.

This document details how to set up this feature on Cisco Secure ACS for Windows and Cisco Secure for UNIX (CSUnix).

The configuration on the VPN Concentrator is similar to a standard configuration. The ability to lock users into a group defined on the VPN Concentrator is enabled by defining a return attribute in the RADIUS user profile. This attribute contains the VPN Concentrator group name which the administrator wants the user to be locked into. This attribute is the Class attribute (IETF RADIUS attribute number 25), and has to be returned to the VPN Concentrator in this format:

```
OU=groupname;
```

where *groupname* is the name of the group on the VPN Concentrator that the user locks into. *OU* has to be in capital letters, and there must be a semicolon at the end.

In this example, VPN Client software is distributed to all users with an existing connection profile using a *group name* of "Everyone" and password "Anything". Each user has a discrete username/password (in this example, the username/password is TEST/TEST). When the user's name is sent to the RADIUS server, the RADIUS server sends down information on the *real group* that the user is to be in. In the example, it is "filtergroup."

By doing this, you can completely control the group assignment on the RADIUS server transparent to the users. If the RADIUS server does not assign a group to the user, the user remains in the "Everyone" group. Since the "Everyone" group has very restrictive filters, the user cannot pass any traffic. If the RADIUS server does assign a group to the user, the user inherits the attributes, including the less–restrictive filter, particular to the group. In this example, you apply a filter to the group "filtergroup" on the VPN Concentrator to permit all

traffic.

# Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on these software and hardware versions:

**Note:** This was also successfully tested with ACS 3.3, VPN Concentrator 4.1.7, and VPN Client 4.0.5.

- Cisco VPN 3000 Concentrator Series version 4.0(1)Rel
- Cisco VPN Client version 4.0(1)Rel
- Cisco Secure ACS for Windows versions 2.4 through 3.2
- Cisco Secure for UNIX versions 2.3, 2.5, and 2.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

# Configure the Cisco VPN 3000 Concentrator

**Note:** This configuration assumes that the VPN Concentrator is already set up with IP addresses, default gateway, address pools, and so on. The user must be able to authenticate locally before continuing. If that does not work, then these changes will not work.

1. Under **Configuration** > **System** > **Servers** > **Authentication**, add the IP address of the RADIUS server.
2. Once you have added the server, use the **Test** button to verify that you can authenticate the user successfully.

   If this does not work, the group lock does not work.
3. Define a filter that drops access to everything in the internal network.

   This is applied to group "Everyone" so that even if the users can authenticate into this group and stay in it, they are still not able to access anything.
4. Under **Configuration** > **Policy Management** > **Traffic Management** > **Rules**, add a rule called **Drop All** and leave everything at the defaults.
5. Under **Configuration** > **Policy Management** > **Traffic Management** > **Filters**, create a filter called **Drop All**, leave everything at the defaults, and add the Drop All rule to it.
6. Under **Configuration** > **User Management** > **Groups** add a group called **Everyone**.

   This is the group that all users have pre−configured in the VPN Client. They authenticate into this group initially, and then are locked into a different group after user authentication. Define the group normally. Make sure you add the Drop All filter (that you just created) under the General tab. In order

to use RADIUS authentication for users in this group, set the group's Type (under the Identity tab) to be **Internal** and Authentication (under the IPSec tab) to **RADIUS**. Make sure the Group Lock feature is not checked for this group.

**Note:** Even if you do not define a Drop All filter, make sure there is at least one filter defined here.

7. Define the user's ultimate destination group (the example is "filtergroup"), applying a filter.

**Note:** You must define a filter here. If you do not want to block any traffic for these users, create an "Allow All" filter and apply the "Any In" and "Any Out" rules to it. You must define a filter of some kind in order to pass traffic. In order to use RADIUS authentication for users in this group, set the group's Type (under the Identity tab) to be **Internal** and Authentication (under the IPSec tab) to **RADIUS**. Make sure the Group Lock feature is not checked for this group.

# Configure the RADIUS Server

## Cisco Secure ACS for Windows

These steps set up your Cisco Secure ACS for Windows RADIUS server to lock a user into a particular group configured on the VPN Concentrator. Keep in mind that groups defined on the RADIUS server have nothing to do with groups defined on the VPN Concentrator. You can use groups on the RADIUS server to make administration of your users easier. The names do not have to match what is configured on the VPN Concentrator.

1. Add the VPN Concentrator as a Network Access Server (NAS) on the RADIUS server under the Network Configuration section.

   a. Add the IP address of the VPN Concentrator in the NAS IP Address box.
   b. Add the same key you defined earlier on the VPN Concentrator in the Key box.
   c. From the Authenticate Using drop−down menu, select **RADIUS (IETF)**.
   d. Click **Submit + Restart**.

2. Under Interface Configuration, select **RADIUS (IETF)** and make sure attribute **25 (Class)** is checked.

   This allows you to change it in the Group/User configuration.
3. Add the user.

   In this example, the user is called "TEST." This user can be in any Cisco Secure ACS for Windows group. Other than passing down attribute 25 to tell the VPN Concentrator what group to use for the user, there is no correlation between Cisco Secure ACS for Windows groups and VPN Concentrator groups. This user is placed in "Group_1."
4. Under Group Setup, edit settings on the group (in our example, this is "Group_1").
5. Click the green **IETF RADIUS** button to take you to the appropriate attributes.
6. Scroll down and modify attribute 25.
7. Add the attribute as shown here. Substitute the group name that you want to lock the users into for filtergroup.

   Make sure OU is in capital letters and that there is a semicolon after the group name.
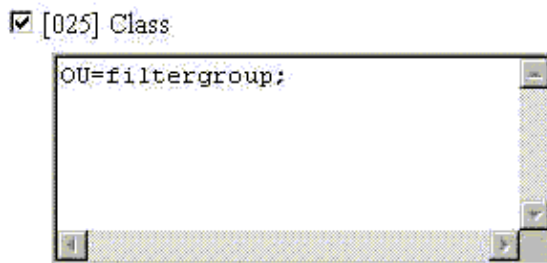


8. Click **Submit + Restart**.

## Cisco Secure for UNIX

These steps set up your Cisco Secure UNIX RADIUS server to lock a user into a particular group configured on the VPN Concentrator. Keep in mind that groups defined on the RADIUS server have nothing to do with groups defined on the VPN Concentrator. You can use groups on the RADIUS server to make administration of your users easier. The names do not have to match what is configured on the VPN Concentrator.

1. Add the VPN Concentrator in as a NAS on the RADIUS server under the Advanced section.

   Choose a dictionary that allows attribute 25 to be sent as a reply−attribute. For example, IETF or Ascend.
2. Add the user.

   In this example, the user is "TEST." This user can be in any Cisco Secure UNIX group or no group. Other than passing down attribute 25 to tell the VPN Concentrator what group to use for the user, there is no correlation between Cisco Secure UNIX groups and VPN Concentrator groups.
3. Under the user/group profile, define a RADIUS (IETF) return attribute.
4. Add the Class attribute, attribute number **25**, and make its value **OU=filtergroup;**. Substitute the group defined on the VPN Concentrator for filtergroup.

   **Note:** In Cisco Secure UNIX, define the attribute surrounded by quotation marks. They are stripped off when the attribute is sent to the VPN Concentrator. The user/group profile should look similar to this.
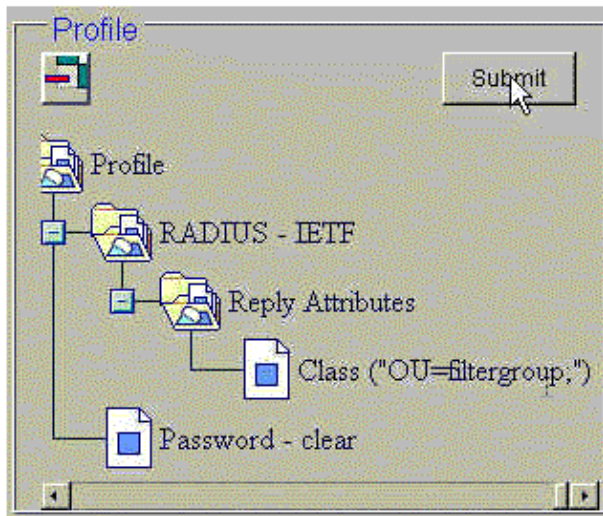
5. Click **Submit** to save each entry.

The finished Cisco Secure UNIX entries appear similar to this output:

```
# ./ViewProfile -p 9900 -u NAS.172.18.124.132
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
Dictionary="DICTIONARY.IETF"

}

# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"

!--- The semi-colon does NOT appear
!--- after the group name, even though it has to be included
!--- when it defines the attribute via the GUI.

}
}

}

# ./ViewProfile -p 9900 -u filtergroup
User Profile Information
user = filtergroup{
profile_id = 80
profile_cycle = 1
radius=IETF {
check_items= {
```

```
                2="filtergroup"
                }
                }

                }

                # ./ViewProfile -p 9900 -u Everyone
                User Profile Information
                user = Everyone{
                profile_id = 67
                profile_cycle = 1
                radius=IETF {
                check_items= {
                2="Anything"
                }
                }

                }
```

# Verify

There is currently no verification procedure available for this configuration.

# Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

# Related Information

- **Cisco VPN 3000 Client User and Group Attribute Processing on the VPN 3000 Concentrator**
- **Cisco IOS Software Configuration**
- **RADIUS (Remote Authentication Dial–In User Service) Technology Support Page**
- **Cisco VPN 3000 Series Concentrators Support Pages**
- **Cisco VPN 3000 Client Support Pages**
- **IP Security Protocol (IPSec) Product Support Pages**
- **Requests for Comments (RFCs)**
- **Documentation for Cisco Secure ACS for Windows**
- **Cisco Secure ACS for Windows Product Support Page**
- **Documentation for Cisco Secure ACS for UNIX**
- **Security Products Field Notices**
- **Cisco Secure ACS for UNIX Product Support Page**
- **Technical Support – Cisco Systems**

Updated: Feb 26, 2008                                                    Document ID: 13831