

Using Cisco Secure ACS for Windows with the VPN 3000 Concentrator – IPsec

Document ID: 13874

Contents

Introduction

Prerequisites

Requirements

Components Used

Conventions

Use Groups on the VPN 3000 Concentrator

How the VPN 3000 Concentrator Uses Group and User Attributes

Configure the RADIUS Server and the VPN 3000 Concentrator

Add Accounting

Specify Individual IP Pools for Each Group

Debugging

Related Information

Introduction

This document recommends the easiest configuration for Cisco Secure Access Control Server (ACS) for Windows to authenticate users that connect to a VPN 3000 Concentrator. A group on a VPN 3000 Concentrator is a collection of users treated as a single entity. The configuration of groups, as opposed to individual users, can simplify system management and streamline configuration tasks. In previous releases, only identity, security, access, performance, DNS, WINS, and tunneling protocols were configured for groups.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure ACS for Windows RADIUS is installed and operates properly with other devices.
- Cisco VPN 3000 Concentrator is configured and can be managed with the HTML interface.

Components Used

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

- Cisco Secure ACS for Windows RADIUS version 4.0 or later.
- Cisco VPN 3000 Concentrator version 4.7 or later.

With Microsoft Windows release 3.0 and later, you can configure and perform these functions on a per-group basis.

- Authentication (RADIUS, NT Domain, SDI, or Internal Server.)*
- Accounting (RADIUS user accounting collects data on user connect time and packets transmitted.)
- Address pools (Allows you to assign IP addresses from an internally configured pool.)

Note: * Group-based authentication does not support multiple SDI servers as of Cisco bug ID CSCdu57258 (registered customers only)

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Use Groups on the VPN 3000 Concentrator

Groups can be defined for both Cisco Secure ACS for Windows and the VPN 3000 Concentrator, but they use groups somewhat differently. Perform these tasks in order to simplify things:

- **Configure a single group on the VPN 3000 Concentrator** for establishing the initial tunnel. This is often called the Tunnel Group and it is used to establish an encrypted Internet Key Exchange (IKE) session to the VPN 3000 Concentrator using a pre-shared key (the group password). This is the same group name and password that should be configured on all VPN 3000 Clients that want to connect to the VPN Concentrator.
- **Configure groups on the Cisco Secure ACS for Windows Server** that use standard RADIUS Attributes and Vendor Specific Attributes (VSAs) for policy management. The VSAs that should be used with the VPN 3000 Concentrator are the RADIUS (VPN 3000) attributes.
- **Configure users on the Cisco Secure ACS for Windows RADIUS server and assign them to one of the groups** configured on the same server. The users inherit attributes defined for their group and Cisco Secure ACS for Windows sends those attributes to VPN Concentrator when the user is authenticated.

How the VPN 3000 Concentrator Uses Group and User Attributes

After the VPN 3000 Concentrator authenticates the Tunnel Group with the VPN Concentrator and the user with RADIUS, it must organize the attributes it has received. The concentrator uses the attributes in this order of preference, whether the authentication is done in the VPN Concentrator or with RADIUS:

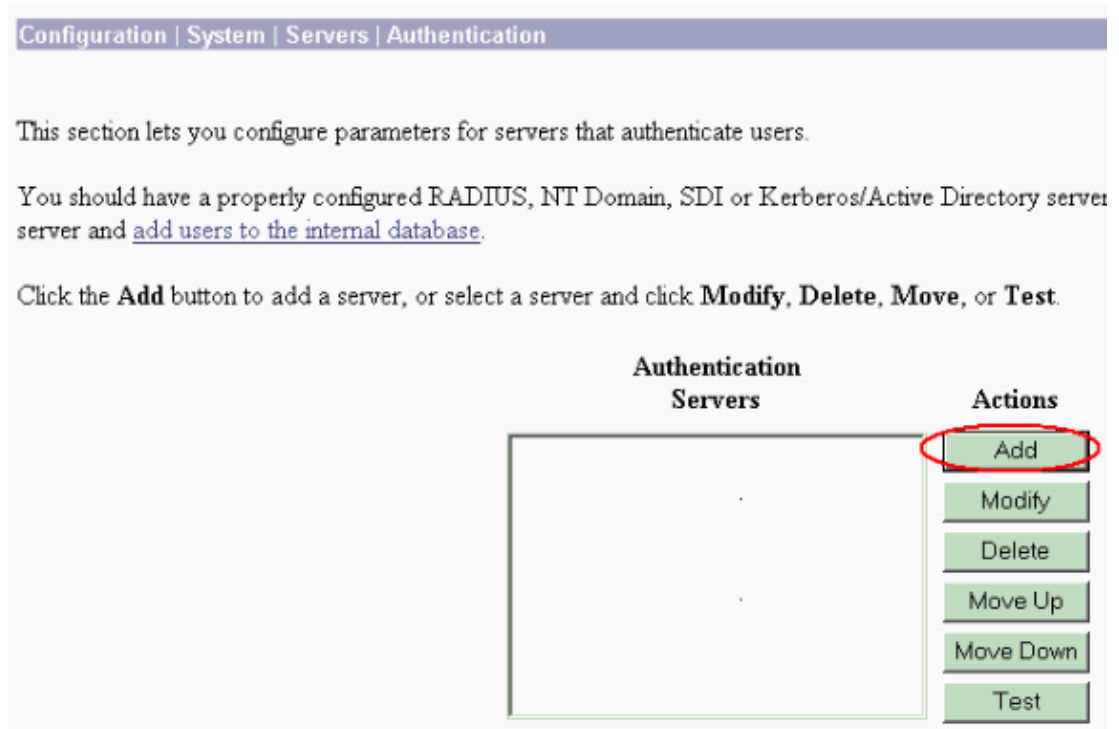
1. **User attributes** These attributes always take precedence over any others.
2. **Tunnel Group attributes** Any attributes not returned when the user was authenticated are filled in by the Tunnel Group attributes.
3. **Base Group attributes** Any attributes missing from the user or Tunnel Group attributes are filled in by the VPN Concentrator Base Group attributes.

Configure the RADIUS Server and the VPN 3000 Concentrator

Complete these steps to configure the RADIUS server and the VPN 3000 Concentrator.

1. **Add the Cisco Secure ACS for Windows RADIUS server to the VPN 3000 Concentrator configuration.**
 - a. Use a web browser to connect to the VPN 3000 Concentrator by typing the IP address of the private interface in the Location or Address bar of your browser.
 - b. Log on to the VPN Concentrator (Default: Login = **admin**, password = **admin**).

- c. Select **Configuration > System > Servers > Authentication**, and click **Add** (from the left menu).



- d. Select the server type **RADIUS** and add these parameters for your Cisco Secure ACS for Windows RADIUS server. Leave all other parameters in their default state.

- ◇ **Authentication Server** Enter the IP address of your Cisco Secure ACS for Windows RADIUS server.
- ◇ **Server Secret** Enter the RADIUS server secret. This must be the same secret you use when you configure the VPN 3000 Concentrator in the Cisco Secure ACS for Windows configuration.
- ◇ **Verify** Re-enter the password for verification.

This adds the authentication server in the global configuration of the VPN 3000 Concentrator. This server is used by all groups except for when an authentication server has been specifically defined. If an authentication server is not configured for a group, it reverts to the global authentication server.

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type: Selecting *Internal Server* will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.

Authentication Server: Enter IP address or hostname.

Used For: Select the operation(s) for which this RADIUS server will be used.

Server Port: Enter 0 for default port (1645).

Timeout: Enter the timeout for this server (seconds).

Retries: Enter the number of retries for this server.

Server Secret: Enter the RADIUS server secret.

Verify: Re-enter the secret.

2. Configure the Tunnel Group on the VPN 3000 Concentrator.

- a. Select **Configuration > User Management > Groups** (from the left menu) and click **Add**.
- b. Change or add these parameters in the Configuration tabs. Do not click **Apply** until you change all of these parameters:

Note: These parameters are the minimum needed for remote access VPN connections. These parameters also assume the default settings in the Base Group on the VPN 3000 Concentrator have not been changed.

Identity

- ◇ **Group Name** Type a group name. For example, IPsecUsers.
- ◇ **Password** Enter a password for the group. This is the pre-shared key for the IKE session.
- ◇ **Verify** Re-enter the password for verification.
- ◇ **Type** Leave this as the default: Internal.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box to enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters		
Attribute	Value	Description
Group Name	IPsecUsers	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

IPsec

- ◇ **Tunnel Type** Select **Remote-Access**.
- ◇ **Authentication** RADIUS. This tells the VPN Concentrator what method to use to authenticate users.
- ◇ **Mode Config** Select the **Mode Config** checkbox.

IPSec	
Attribute	Value
IPSec SA	ESP-3DES-MD5
IKE Peer Identity Validation	If supported by certificate
IKE Keepalives	<input checked="" type="checkbox"/>
Confidence Interval	300
Tunnel Type	Remote Access
Remote Access	
Group Lock	<input type="checkbox"/>
Authentication	RADIUS
Authorization Type	None
Authorization Required	<input type="checkbox"/>
DN Field	CN otherwise OU
IPComp	None
Reauthentication on Rekey	<input type="checkbox"/>
Client Type & Version Limiting	
Mode Configuration	<input checked="" type="checkbox"/>

Apply Cancel

c. Click **Apply**.

3. Configure multiple authentication servers on the VPN 3000 Concentrator.

- a. Once the group is defined, highlight that group, and click **Modify Auth. Servers**. Individual authentication servers can be defined for each group even if these servers do not exist in the global servers.
- b. Select the server type **RADIUS**, and add these parameters for your Cisco Secure ACS for Windows RADIUS server. Leave all other parameters in their default state.
 - ◇ **Authentication Server** Enter the IP address of your Cisco Secure ACS for Windows RADIUS server.
 - ◇ **Server Secret** Enter the RADIUS server secret. This must be the same secret you use when you configure the VPN 3000 Concentrator in the Cisco Secure ACS for Windows configuration.
 - ◇ **Verify** Re-enter the password for verification.

Configuration | User Management | Groups | Authentication Servers | Add

Configure and add a user authentication server.

Server Type	<input type="text" value="RADIUS"/>	Select the type of authentication server. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.
Authentication Server	<input type="text" value="10.2.2.2"/>	Enter IP address or hostname.
Used For	<input type="text" value="User Authentication"/>	Select the operation(s) for which this RADIUS server will be used.
Server Port	<input type="text" value="0"/>	Enter 0 for default port (1645).
Timeout	<input type="text" value="4"/>	Enter the timeout for this server (seconds).
Retries	<input type="text" value="2"/>	Enter the number of retries for this server.
Server Secret	<input type="password" value=""/>	Enter the RADIUS server secret.
Verify	<input type="password" value=""/>	Re-enter the secret.

4. Add the VPN 3000 Concentrator to the Cisco Secure ACS for Windows server configuration.

- a. Double-click the **ACS Admin** icon to start the admin session on the PC that runs the Cisco Secure ACS for Windows RADIUS server. Log in with the proper username and password, if required.
- b. Select **Network Configuration**, and click **Add Entry** under the Network Device group.
 - a. Create the new group name.
 - b. Click **Submit**. The new group name appears in the Network Device Groups list.

Instead of creating a new group, you can click the **Not Assigned** group and add the VPN Concentrator as the AAA client. But Cisco does not recommend that you create a new group.

- c. Click the **New** group and click **Add Entry** under the AAA clients.

Note: In the context of Cisco Secure ACS, an AAA client is any network device that provides AAA client functionality and supports an AAA security protocol that is also supported by Cisco Secure ACS. This includes Cisco access servers, Cisco PIX firewalls, Cisco VPN 3000 Series Concentrators, Cisco VPN 5000 Series Concentrators, Cisco IOS® routers, Cisco Aironet Access Point 340 and 350 devices, and some Cisco Catalyst switches.

- d. Add these parameters for your VPN 3000 Concentrator:
 - ◇ **AAA Client Hostname** Enter the hostname of your VPN 3000 Concentrator (for DNS resolution).
 - ◇ **AAA Client IP Address** Enter the IP address of your VPN 3000 Concentrator.
 - ◇ **Key** Enter the RADIUS server secret. This must be the same secret you configured when you added the Authentication Server on the VPN Concentrator in step 1.
 - ◇ **Network Device Group** From the list, select the network device group in which the VPN Concentrator belongs.
 - ◇ **Authenticate Using** Select **RADIUS (Cisco VPN 3000/ASA/PIX 7.x and later)**. This allows the VPN 3000 VSAs to display in the Group configuration window.



Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="10.1.1.2"/>
Key	<input type="text" value="csacs123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

- c. Click **Submit**.
- d. Select **Interface Configuration**, click **RADIUS Cisco VPN 3000/ASA/PIX 7.x and later**, and check **Group [26] Vendor-Specific**.

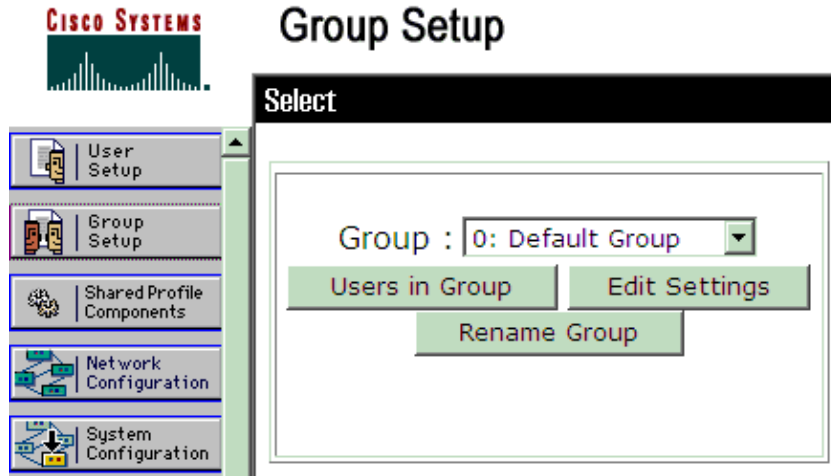
Note: 'RADIUS attribute 26' refers to all vendor specific attributes. For example, select **Interface Configuration > RADIUS (Cisco VPN 3000/ASA/PIX 7.x and later)** and see that all of the available attributes start with 026. This shows that all of these vendor specific attributes fall under the IETF RADIUS 26 standard. These attributes do not show up in User or Group setup by default. In order to show up in the Group setup, create an AAA client (in this case VPN 3000 Concentrator) that authenticates with RADIUS in the network configuration. Then check the attributes that need to appear in User Setup, Group Setup, or both from the Interface configuration.

The document describes the available attributes and its usage RADIUS Attributes.

- e. Click **Submit**.

5. Add groups to the Cisco Secure ACS for Windows configuration.

- a. Select **Group Setup**, then select one of the template groups (for example, Group 0), and click **Rename Group**.



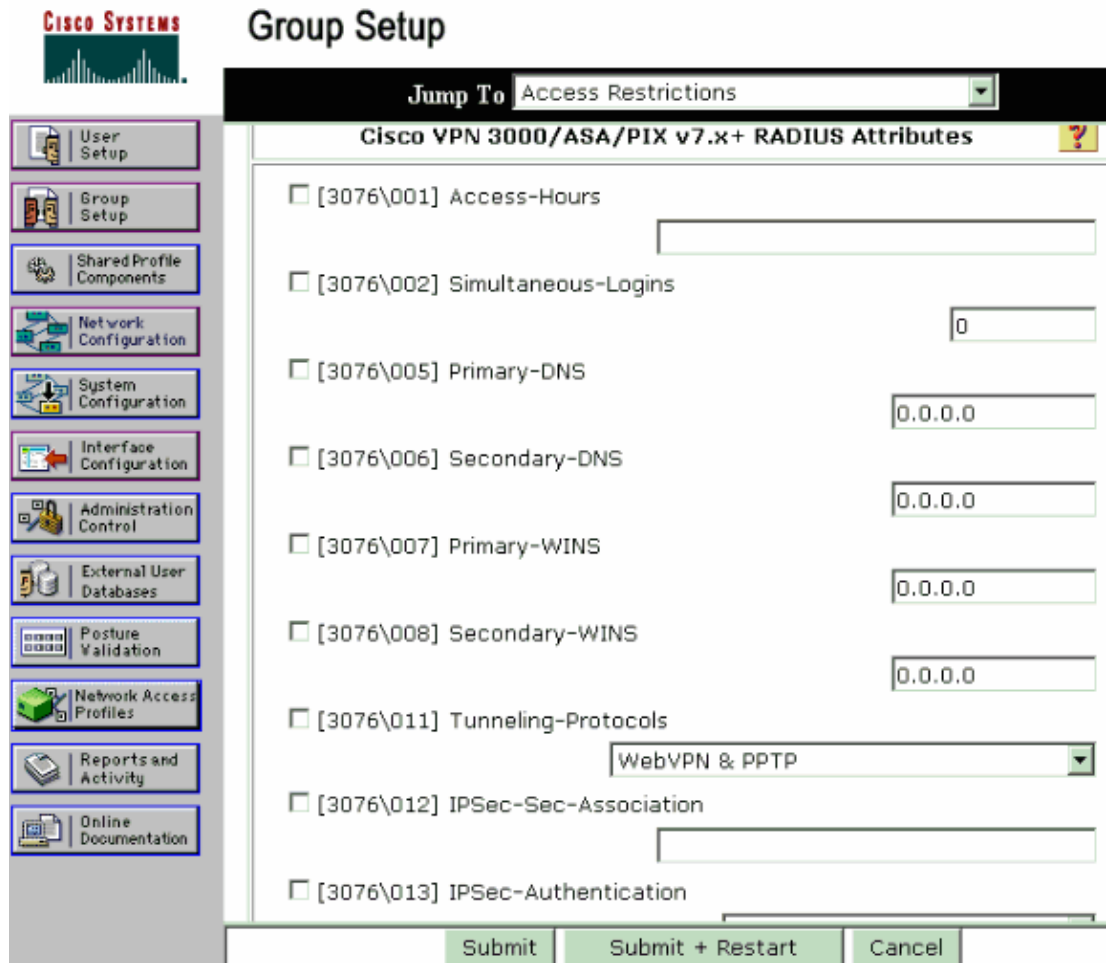
Change the name to something appropriate for your organization. For example, Engineering, Sales, or Marketing. Since users are added to these groups, make the group name reflect the actual purpose of that group. If all users are put into the same group, you can call it VPN Users Group.

- b. Click **Edit Settings** to edit the parameters in your newly renamed group.
- c. Click **Cisco VPN 3000 RADIUS/ASA/PIX 7.x and later** and configure these recommended attributes. This allows users assigned to this group to inherit the Cisco VPN 3000 RADIUS attributes, which allows you to centralize policies for all users in Cisco Secure ACS for Windows.

Note: Technically, Cisco VPN 3000/ASA/PIX 7.x and later RADIUS attributes are not required to be configured as long as the Tunnel Group is set up as step 2 recommends and the Base Group in the VPN Concentrator does not change from the original default settings.

Recommended VPN 3000 Attributes:

- ◇ **Primary–DNS** Enter the IP address of your Primary DNS server.
- ◇ **Secondary–DNS** Enter the IP address of your Secondary DNS server.
- ◇ **Primary–WINS** Enter the IP address of your Primary WINS server.
- ◇ **Secondary–WINS** Enter the IP address of your Secondary WINS server.
- ◇ **Tunneling–Protocols** Select **IPsec**. This allows *only* IPsec Client connections. PPTP or L2TP are not allowed.
- ◇ **IPsec–Sec–Association** Enter **ESP–3DES–MD5**. This ensures all your IPsec clients connect with the highest encryption available.
- ◇ **IPsec–Allow–Password–Store** Select **Disallow** so users are *not* allowed to save their password in the VPN Client.
- ◇ **IPsec–Banner** Enter a welcome message banner to be presented to the user upon connection. For example, "Welcome to MyCompany employee VPN access!"
- ◇ **IPSec–Default Domain** Enter the domain name of your company. For example, "mycompany.com".



This set of attributes is not necessary. But if you are unsure if the Base Group attributes of the VPN 3000 Concentrator have changed, then Cisco recommends that you configure these attributes:

- ◇ **Simultaneous-Logins** Enter the number of times you allow a user to simultaneously log in with the same username. The recommendation is 1 or 2.
- ◇ **SEP-Card-Assignment** Select **Any-SEP**.
- ◇ **IPsec-Mode-Config** Select **ON**.
- ◇ **IPsec-Through-NAT** Select **OFF**, unless you want users in this group to connect using IPsec over the UDP protocol. If you select ON, the VPN Client still has the ability to locally disable IPsec through NAT and connect normally.
- ◇ **IPsec-Through-NAT-Port** Select a UDP port number in the range of 4001 through 49151. This is used only if IPsec-through-NAT is ON.

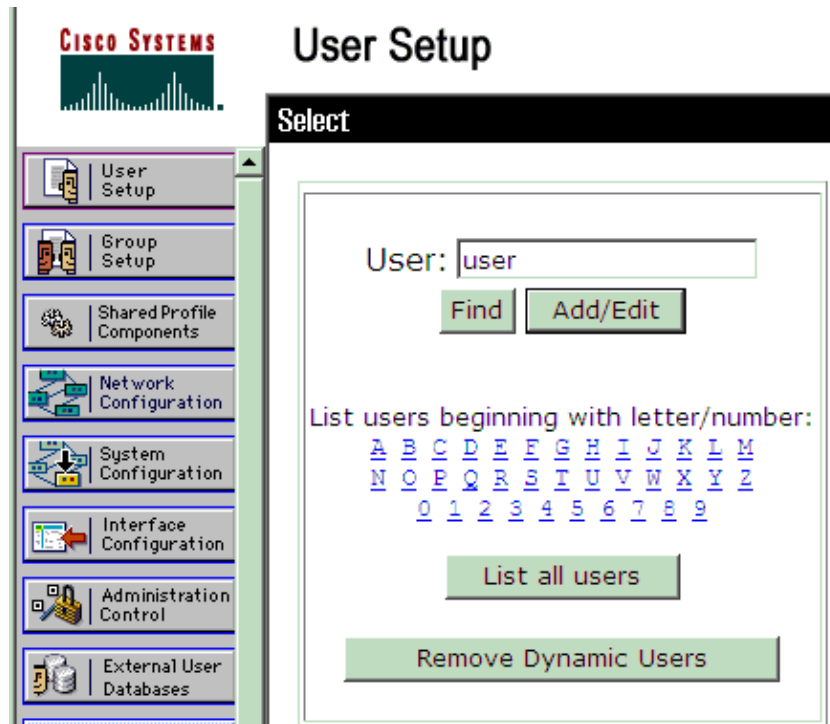
The next set of attributes requires that you set something up on the VPN Concentrator first before you can use them. This is only recommended for advanced users.

- ◇ **Access-Hours** This requires you to set up a range of Access Hours on the VPN 3000 Concentrator under **Configuration > Policy Management**. Instead, use Access Hours available in Cisco Secure ACS for Windows to manage this attribute.
- ◇ **IPsec-Split-Tunnel-List** This requires you to set up a Network List on the VPN Concentrator under **Configuration > Policy Management > Traffic Management**. This is a list of networks sent down to the client that tell the client to encrypt data to only those networks in the list.

- d. Select **Submit > Restart** to save the configuration and activate the new group.
- e. Repeat these steps to add more groups.

6. Configure Users on Cisco Secure ACS for Windows.

a. Select **User Setup**, enter a username, and click **Add/Edit**.



b. Configure these parameters under the user setup section:

- ◇ **Password Authentication** Select **Cisco Secure Database**.
- ◇ **Cisco Secure PAP – Password** Enter a password for the user.
- ◇ **Cisco Secure PAP – Confirm Password** Re–enter the password for the new user.
- ◇ **Group to which the user is assigned** Select the name of the group you created in the previous step.

User Setup

User Setup

Password Authentication:

CiscoSecure Database ▼

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

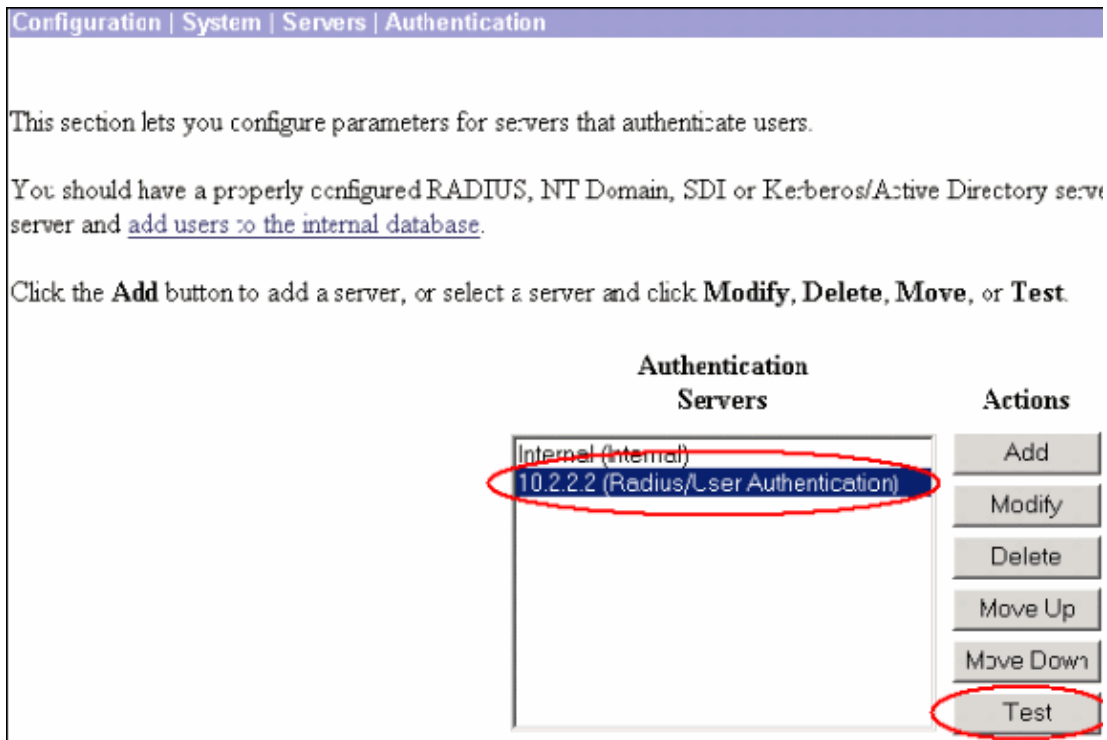
Group to which the user is assigned:

vpn3000 ▼

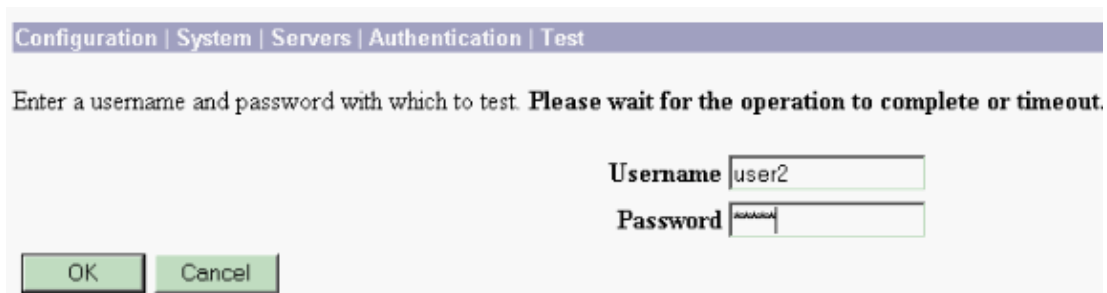
- c. Click **Submit** to save and activate the user settings.
- d. Repeat these steps to add additional users.

7. Test Authentication.

Select **Configuration > System > Servers > Authentication > Test** on the VPN 3000 Concentrator.



Test authentication from the VPN Concentrator to the Cisco Secure ACS for Windows server by entering the username and password you configured in the Cisco Secure ACS for Windows.



On a good authentication, the VPN Concentrator shows an "**Authentication Successful**" message.



If there are failures in Cisco Secure ACS for Windows, the Cisco Secure ACS for Windows **Reports and Activity > Failed Attempts** menu shows the failures. In a default installation, these failure reports are on disk in c:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts.

Note: The Cisco VPN 3000 Concentrator only uses Password Authentication Protocol (PAP) when TEST authentication is used.

8. Connect to the VPN 3000 Concentrator.

Now you can connect to the VPN 3000 Concentrator using the client. Be sure the VPN Client is configured to use the same group name and password configured in step 2.

Add Accounting

After authentication works, you can add accounting.

On the VPN 3000, select **Configuration > System > Servers > Accounting**.

Configuration | System | Servers | Accounting

This section lets you configure parameters for RADIUS user accounting servers.

Be sure that any servers you reference are properly configured.

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, or **Move**.

Accounting Servers	Actions
--- Empty ---	<input type="button" value="Add"/>
	<input type="button" value="Modify"/>
	<input type="button" value="Delete"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>

Click **Add** in order to add the Cisco Secure ACS for Windows server.

Configuration | System | Servers | Accounting | Add

Configure and add a RADIUS user accounting server.

Accounting Server	<input type="text" value="10.2.2.2"/>	Enter IP address or hostname.
Server Port	<input type="text" value="1646"/>	Enter the server UDP port number. Default is 1646.
Timeout	<input type="text" value="1"/>	Enter the timeout for this server (seconds).
Retries	<input type="text" value="3"/>	Enter the number of retries for this server.
Server Secret	<input type="password" value="•••••"/>	Enter the RADIUS server secret.
Verify	<input type="password" value="•••••"/>	Re-enter the server secret.

You can add individual accounting servers to each group when you select **Configuration > User Management > Groups**. Highlight a group and click **Modify Acct. Servers**.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, click the appropriate button.

Actions	Current Groups	Modify
<input type="button" value="Add Group"/>	IPsecUsers (Internally Configured) turaro (Internally Configured)	<input type="button" value="Authentication Servers"/>
<input type="button" value="Modify Group"/>		<input type="button" value="Authorization Servers"/>
<input type="button" value="Delete Group"/>		<input type="button" value="Accounting Servers"/>
		<input type="button" value="Address Pools"/>
		<input type="button" value="Client Update"/>
		<input type="button" value="Bandwidth Assignment"/>
		<input type="button" value="WebVPN Servers and URLs"/>
		<input type="button" value="WebVPN Port Forwarding"/>

Enter the IP address of the Accounting Server with the Server Secret.

Change a configured RADIUS user accounting server.

Accounting Server	<input type="text" value="10.2.2.2"/>	Enter IP address or hostname.
Server Port	<input type="text" value="1646"/>	Enter the server UDP port number. Default is 1646.
Timeout	<input type="text" value="1"/>	Enter the timeout for this server (seconds).
Retries	<input type="text" value="3"/>	Enter the number of retries for this server.
Server Secret	<input type="password" value="....."/>	Enter the RADIUS server secret.
Verify	<input type="password" value="....."/>	Re-enter the server secret.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

In Cisco Secure ACS for Windows, the accounting records appear as this output shows:

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,
Acct-Session-Id, Acct-Session-Time,Service-Type,Framed-Protocol,
Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets,
Acct-Output-Packets,Framed-IP-Address,NAS-Port,
NAS-IP-Address03/23/2000,14:04:10, csntuser,3000,,Start,7ED00001,,Framed,
PPP,,,,,10.99.99.1,1009,172.18.124.133 03/23/2000,14:07:01,csntuser,3000,,
Stop,7ED00001,171,Framed,PPP,5256,0,34,0,10.99.99.1, 1009,172.18.124.133
```

Specify Individual IP Pools for Each Group

You can specify individual IP pools to each group. The user is assigned an IP address from the pool configured for the group. If a pool is not defined for a particular group, the user is assigned an IP address from the global pool. Select **Configuration > User Management > Groups** to configure individual pools for each group.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, click the appropriate button.

Actions	Current Groups	Modify
<input type="button" value="Add Group"/>	IPsecUsers (Internally Configured) turaro (Internally Configured)	<input type="button" value="Authentication Servers"/>
<input type="button" value="Modify Group"/>		<input type="button" value="Authorization Servers"/>
<input type="button" value="Delete Group"/>		<input type="button" value="Accounting Servers"/>
		<input type="button" value="Address Pools"/>
		<input type="button" value="Client Update"/>
		<input type="button" value="Bandwidth Assignment"/>
		<input type="button" value="WebVPN Servers and URLs"/>
		<input type="button" value="WebVPN Port Forwarding"/>

Highlight a group and click **Modify Address Pool**. Click **Add** to add the IP pool. The pool of IP addresses defined here can be a subset of the global pool.

Add an address pool.

Range Start Enter the start of the IP pool address range.

Range End Enter the end of the IP pool address range.

Subnet Mask Enter the subnet mask of the IP pool address range.
Enter 0.0.0.0 to use default behavior.

Debugging

If connections do not work, you can add AUTH, IKE, and IPsec event classes to the VPN Concentrator when you select **Configuration > System > Events > Classes > Modify (Severity to Log=1–9, Severity to Console=1–3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG, and IPSECDECODE are also available, but may provide too much information. If detailed information is needed on the attributes that are passed down from the RADIUS server, AUTHDECODE, IKEDECODE, and IPSECDECODE provide this at the Severity to Log=1–13 level.

This screen lets you modify an event class configured for special handling.

Class Name

Enable Check to enable special handling of this class.

If one of the following values has been set to *Use Event List*, the Event List can be seen by viewing **Configuration | System | Events | General**.
 Changing a value set to *Use Event List* will override the sections of the Event List referring to this event class.

Events to Log Select the events to enter in the log.
 Events to Console Select the events to display on the console.
 Events to Syslog Select the events to send to a Syslog Server.
 Events to E-mail Select the events to send to an E-mail Recipient.
 Events to Trap Select the events to send to an SNMP Trap Destination.

Retrieve the event log from **Monitoring > Filterable Event Log**.

Monitoring | Filterable Event Log

Select Filter Options

Event Class Severities
 AUTH
 AUTHDBG
 AUTHDECODE
 1
 2
 3

Client IP Address Events/Page

Group Direction

```

12111 01/08/2007 18:29:12.950 SEV=4 AUTH/15 RPT=6038
Server name = 10.2.2.2, type = RADIUS,
group = none (global server), status = Not-in-service

12113 01/08/2007 18:30:12.950 SEV=4 AUTH/15 RPT=6039
Server name = 10.2.2.2, type = RADIUS,
group = none (global server), status = Not-in-service

12115 01/08/2007 18:31:12.950 SEV=4 AUTH/15 RPT=6040
Server name = 10.2.2.2, type = RADIUS,
group = none (global server), status = Not-in-service

12117 01/08/2007 18:32:12.950 SEV=4 AUTH/15 RPT=6041
Server name = 10.2.2.2, type = RADIUS,
group = none (global server), status = Not-in-service

12119 01/08/2007 18:33:12.950 SEV=4 AUTH/15 RPT=6042
    
```

Cisco Secure ACS for Windows failures are found in **Reports and Activity > Failed attempts > active.csv**.

Related Information

- [Configuring Dynamic Filters on a RADIUS Server](#)
 - [Cisco VPN 3000 Series Concentrator Support Page](#)
 - [Cisco VPN 3000 Series Client Support Page](#)
 - [IPsec Support Page](#)
 - [Cisco Secure ACS for Windows Support Page](#)
 - [Documentation for Cisco Secure ACS for Windows](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 18, 2007

Document ID: 13874
