Softether VPN Remote Access with Duo Multi-Factor Authentication (MFA)

This guide assumes you have a working Softether VPN server configured for remote access along with Active Directory for remote user authentication and a Duo account with your users and their mobile devices pre-enrolled and the Duo app pre-installed and configured for your Duo account.

> Please note this MFA implementation **ONLY** works by utilizing the Duo Mobile app **Push Notifications.**

If you don't have a Duo account, you can sign up for a free trial on the Duo website. Additionally, you also need to deploy a Duo Authentication Proxy server on your network using Linux or Windows.

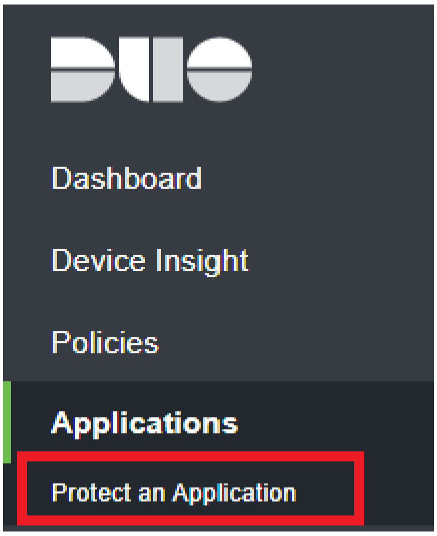
This guide specifically focuses on a Duo Authentication Proxy on Linux but it can be easily adapted to a Windows based installation.

If you need to deploy a Softether VPN server you can take a look at our docker compose example to deploy using Docker, Traefik as the reverse proxy and Lets Encrypt support.

Configure Softether Application in Duo Admin Panel

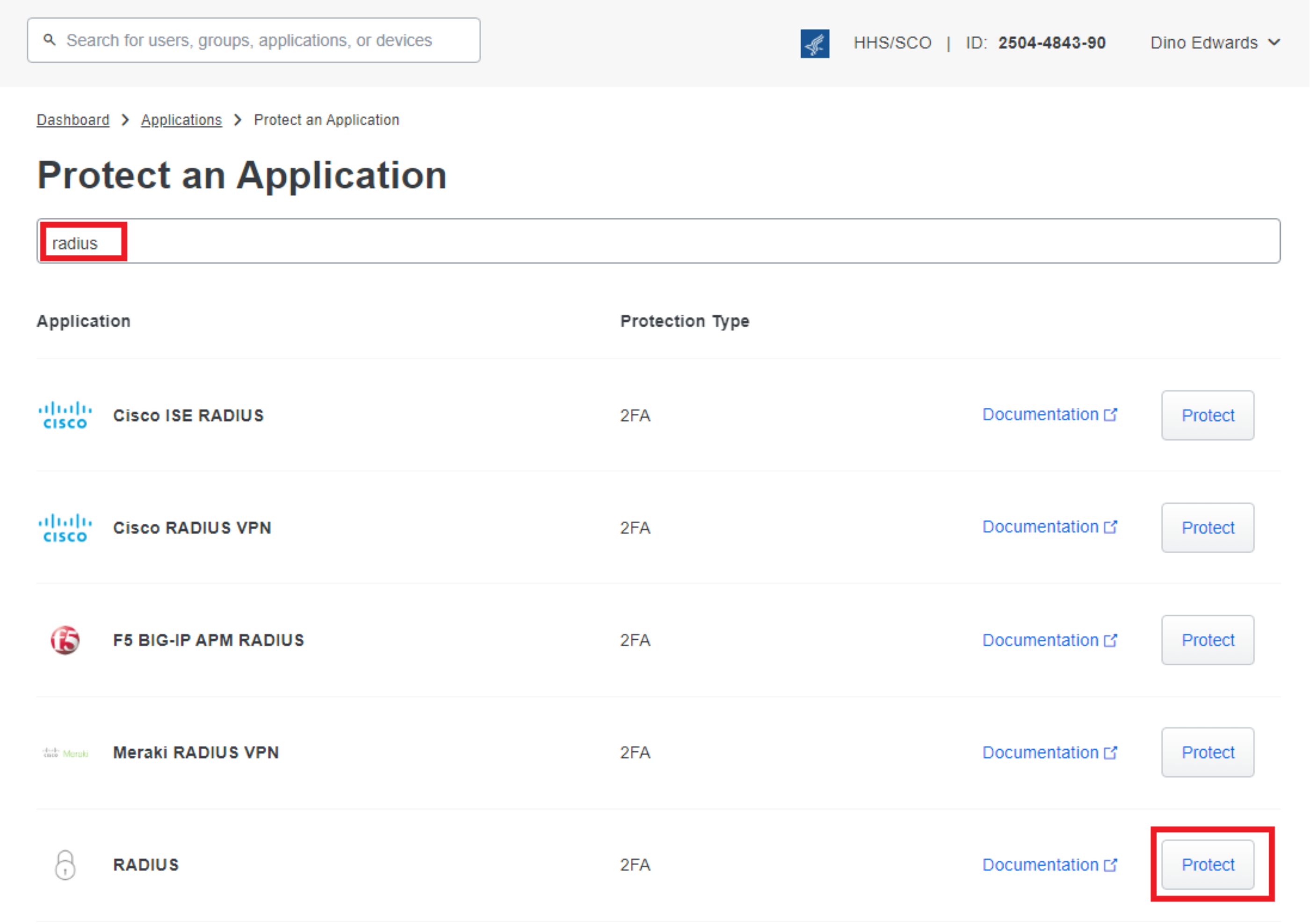
- Login to your Duo Admin Panel and navigate to **Applications --> Protect and Application** (**Figure 1**).

Figure 1



- In the **Protect an Application** page, enter **radius** in the **Filter by keywords** field and click the **Protect** button to the right of the **RADIUS** application from the resultant list (**Figure 2**).

Figure 2


Search for users, groups, applications, or devices
HHS/SCO | ID: 2504-4843-90
Dino Edwards
Dashboard > Applications > Protect an Application

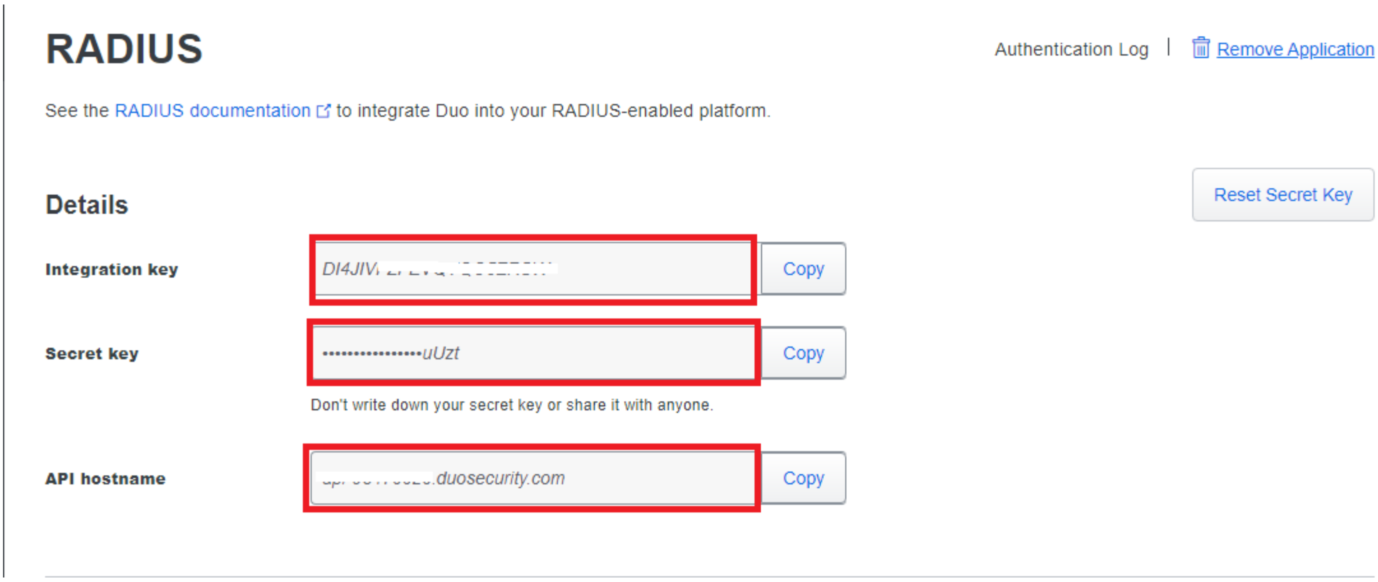
Protect an Application

radius

Application	Protection Type		
Cisco ISE RADIUS	2FA	Documentation	Protect
Cisco RADIUS VPN	2FA	Documentation	Protect
F5 BIG-IP APM RADIUS	2FA	Documentation	Protect
Meraki RADIUS VPN	2FA	Documentation	Protect
RADIUS	2FA	Documentation	Protect

- In the **RADIUS** application page, copy the **Integration key, Secret Key and the API hostname** to be used later in the configuration of the Duo Authentication Proxy (**Figure 3**).

Figure 3



RADIUS

Authentication Log | Remove Application

See the RADIUS documentation to integrate Duo into your RADIUS-enabled platform.

Details

Reset Secret Key

Integration key DI4JIV[redacted] Copy

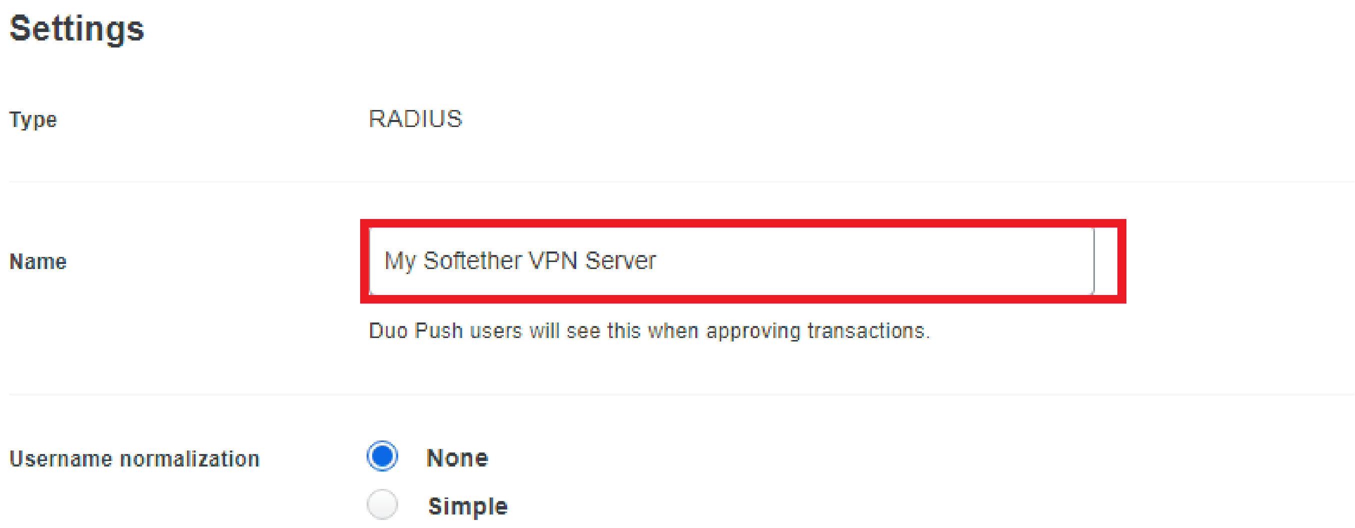
Secret key ••••••••••••••••uUzt Copy

Don't write down your secret key or share it with anyone.

API hostname [redacted].duosecurity.com Copy

- Optionally, you can scroll down to the **Settings** section of the RADIUS application and set the **Name** to a name specific to your environment (**Figure 4**).

Figure 4



Settings

Type RADIUS

Name My Softether VPN Server

Duo Push users will see this when approving transactions.

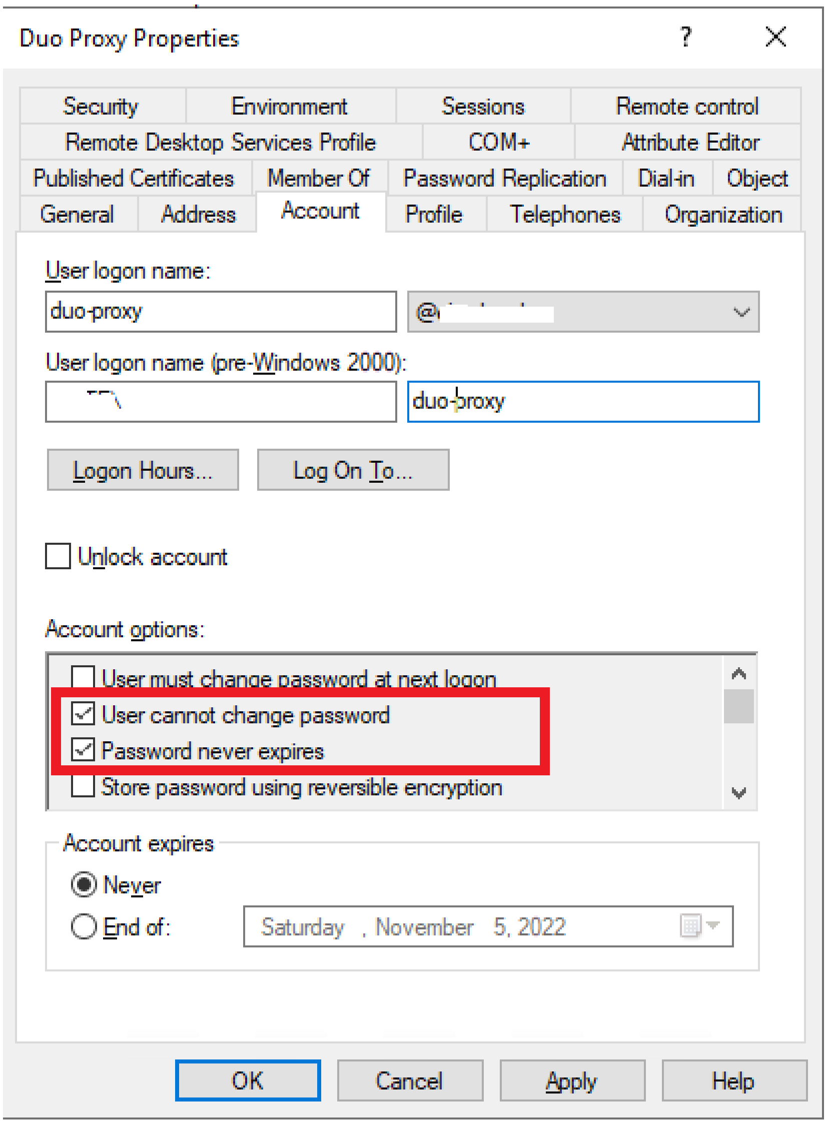
Username normalization ● None ○ Simple

- Ensure you click the **Save** button on the very bottom of the RADIUS application page.

Create an AD service account to enumerate users in Active Directory

- The service account should NOT have any special permissions. membership only in the **Domain Users** group should be sufficient unless you have special security considerations in your AD environment. The account should have **User cannot change password** and **Password never expires** checked in the **Account** tab of the user properties (**Figure 5**).

Figure 5



User logon name: duo-proxy @[redacted]

User logon name (pre-Windows 2000): [redacted] duo-proxy

□ Unlock account

Account options:

□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Saturday , November 5, 2022

Configure Duo Authentication Proxy

The Duo Authentication Proxy integrates with the Duo cloud to perform Duo push notifications, integrates with Active Directory to perform user authentication and it also serves as a RADIUS server which Softether utilizes to authenticate users. You could use a separate RADIUS server to integrate with Active Directory and configure Duo Authentication Proxy with it but that's outside the scope of this guide.

If you followed the **Duo Authentication Proxy - Reference** New Proxy Install for Linux, the proxy gets installed in the **/opt/duoauthproxy** directory by default. If you did a custom installation, adjust the paths below as necessary.

- Edit the /opt/duoauthproxy/conf/authproxy.cfg file:

```
vi /opt/duoauthproxy/conf/authproxy.cfg
```

- Delete any existing entries and insert the following entries instead, substituting all the entries enclosed within the Less-Than/Greater-Than **<>** symbols with the actual data from your environment. The **<RADIUS_SHARED_SECRET>** is simply a random string of upper/lower case letters and numbers that will be used as a secret string between your Softether VPN server and the Duo Authentication Proxy. We recommend at least a 20 character string. Refer to the Duo Authentication Proxy - Reference for details on the client configuration options below, in particular how to configure the **failmode** option for your needs and adding additional Active Domain Controllers.

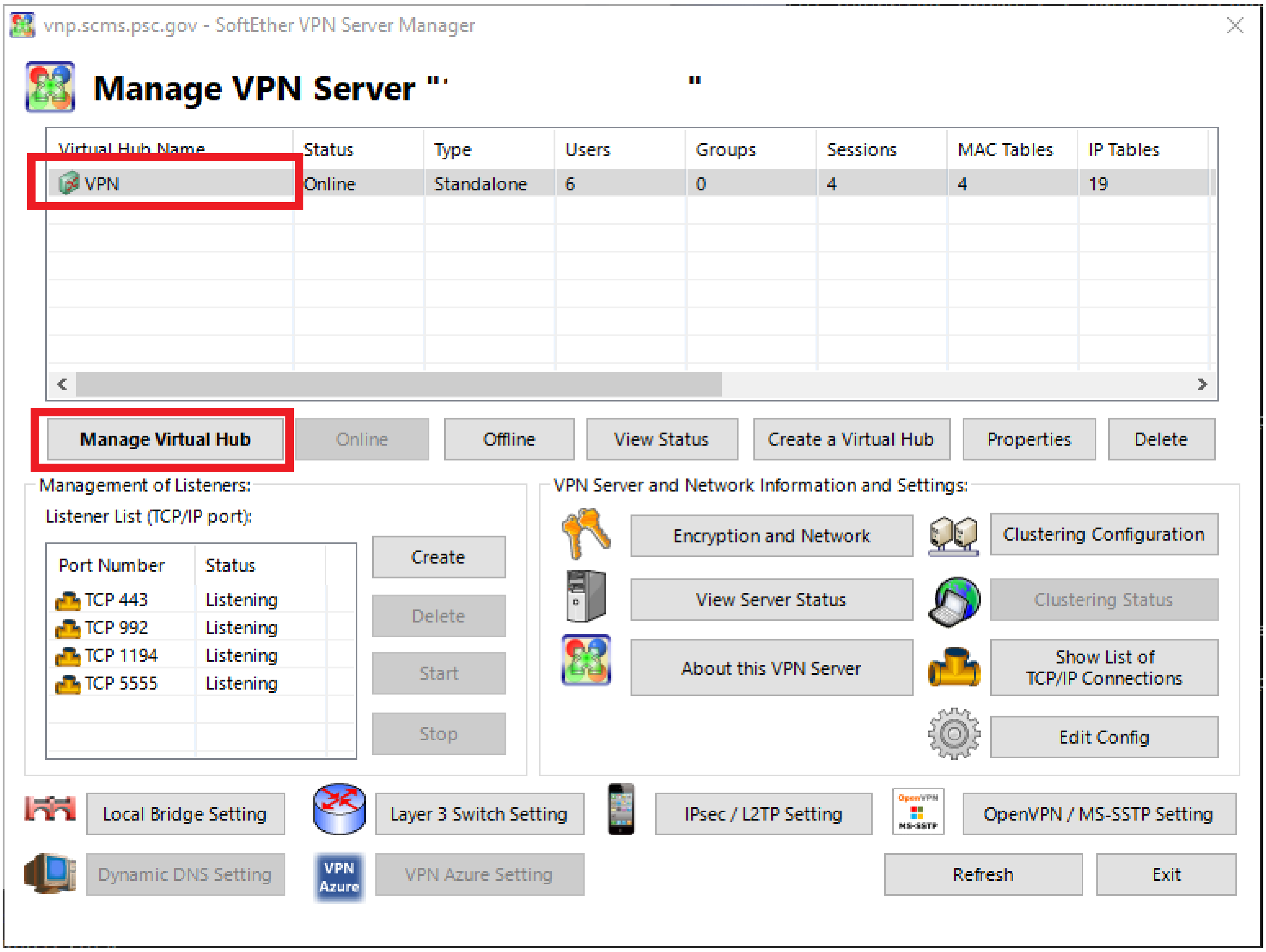
```
[ad_client]
host=<AD_DOMAIN_CONTROLLER>
service_account_username=<AD_DUO_SERVICE_ACCOUNT_USERNAME>
service_account_password=<AD_DUO_SERVICE_ACCOUNT_PASSWORD>
search_dn=DC=DOMAIN,DC=TLD

[radius_server_auto]
ikey=<DUO_INTEGRATION_KEY>
skey=<DUO_SECRET_KEY>
api_host=<DUO_API_HOSTNAME>
radius_ip_1=<SOFTETHER_VPN_SERVER_IP>
radius_secret_1=<RADIUS_SHARED_SECRET>
failmode=safe
client=ad_client
port=1812
```

Configure Softether VPN Server

- Connect to your Softether VPN Server, select the appropriate hub and click the **Manage Virtual Hub** button (**Figure 6**).

Figure 6



vnp.scms.psc.gov - SoftEther VPN Server Manager

Manage VPN Server "'   "

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
VPN	Online	Standalone	6	0	4	4	19

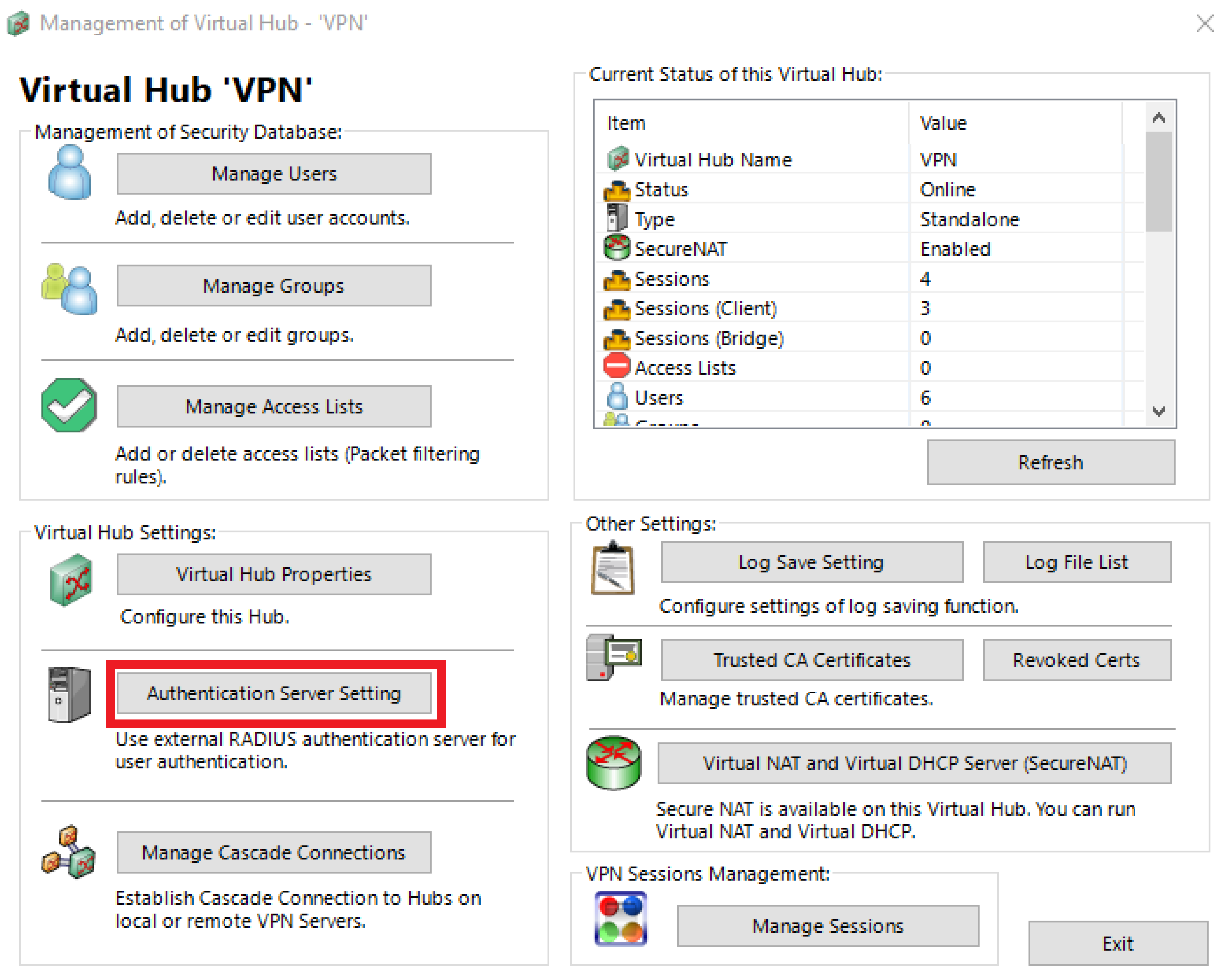
Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

- In the Management of Virtual Hub window, click the **Authentication Server Setting** button (**Figure 7**).

Figure 7



Add, delete or edit user accounts.

Add, delete or edit groups.

Add or delete access lists (Packet filtering rules).

Configure this Hub.

Use external RADIUS authentication server for user authentication.

Establish Cascade Connection to Hubs on local or remote VPN Servers.

Item	Value
Virtual Hub Name	VPN
Status	Online
Type	Standalone
SecureNAT	Enabled
Sessions	4
Sessions (Client)	3
Sessions (Bridge)	0
Access Lists	0
Users	6
Groups	0

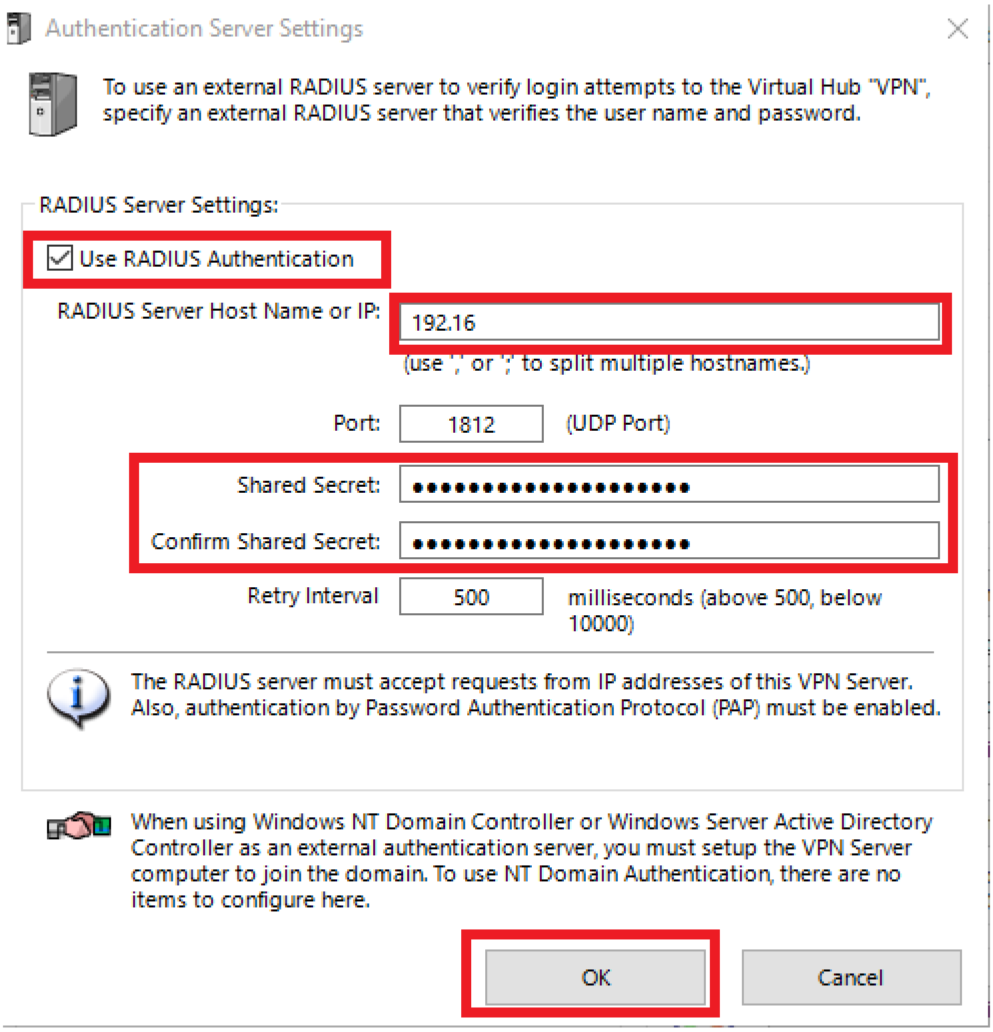
Configure settings of log saving function.

Manage trusted CA certificates.

Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

- In the **Authentication Server Settings** window, check the **Use RADIUS Authentication**, enter the IP address or host name of your **Duo Authentication Proxy** server in the **RADIUS Server Hostname or IP** field, enter and confirm the **<RADIUS_SHARED_SECRET>** you generated from above in the **Shared Secret** and **Confirm Shared Secret** fields and click the **OK** button (**Figure 8**).

Figure 8



Authentication Server Settings

To use an external RADIUS server to verify login attempts to the Virtual Hub "VPN", specify an external RADIUS server that verifies the user name and password.

RADIUS Server Settings:

☑ Use RADIUS Authentication

RADIUS Server Host Name or IP: 192.16

(use ',' or ';' to split multiple hostnames.)

Port: 1812 (UDP Port)

Shared Secret: ••••••••••••••••••••

Confirm Shared Secret: ••••••••••••••••••••

Retry Interval 500 milliseconds (above 500, below 10000)

The RADIUS server must accept requests from IP addresses of this VPN Server. Also, authentication by Password Authentication Protocol (PAP) must be enabled.

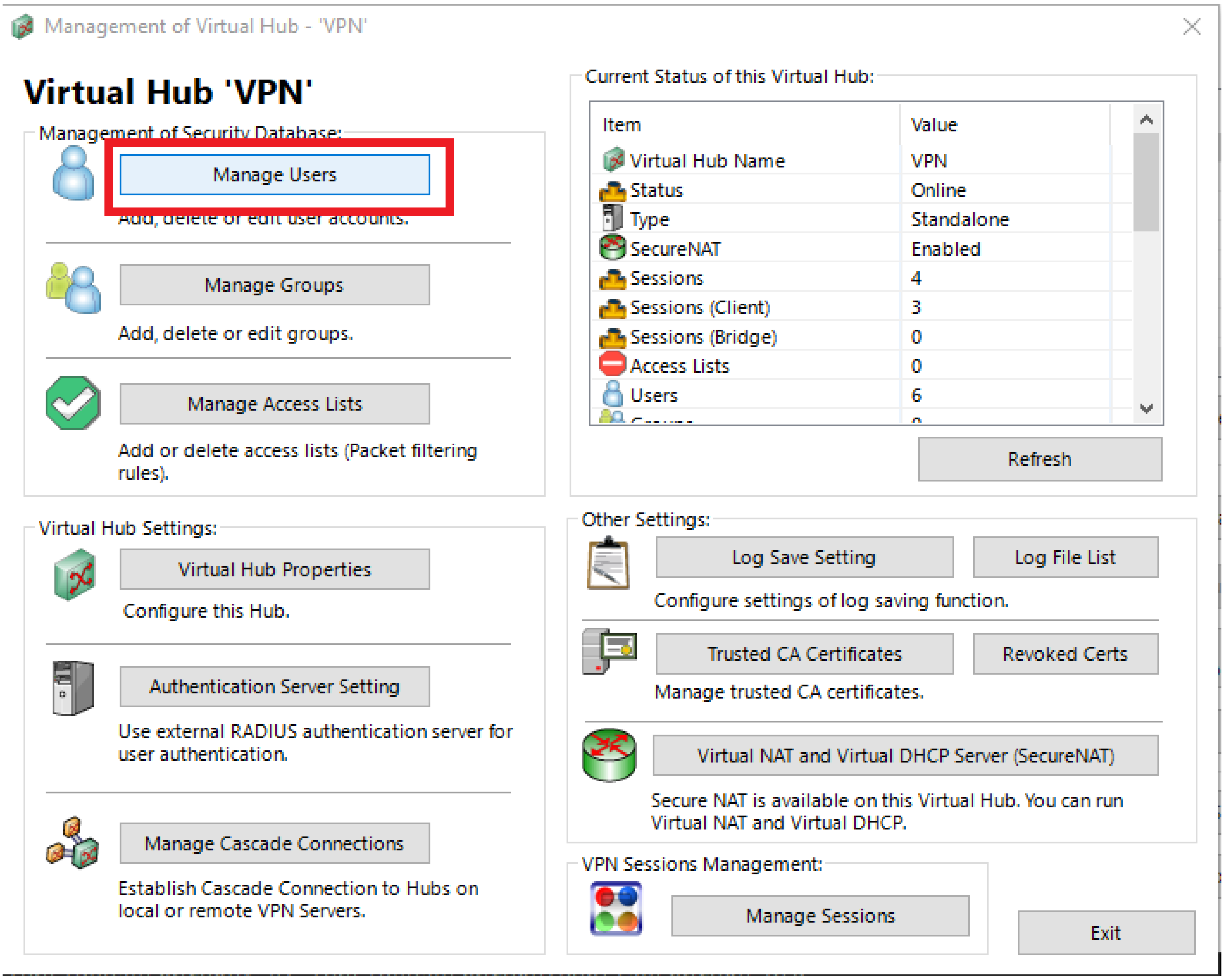
When using Windows NT Domain Controller or Windows Server Active Directory Controller as an external authentication server, you must setup the VPN Server computer to join the domain. To use NT Domain Authentication, there are no items to configure here.

Configure Softether VPN Server Users

When adding users in Softether VPN server to authenticate using Duo MFA, the username that you are adding in Softether VPN **MUST** match an existing username in the Duo Admin panel.

- Back in the **Management of Virtual Hub** window, click on the **Manage Users** button (**Figure 9**).

Figure 9



Management of Virtual Hub - 'VPN'

Virtual Hub 'VPN'

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	VPN
Status	Online
Type	Standalone
SecureNAT	Enabled
Sessions	4
Sessions (Client)	3
Sessions (Bridge)	0
Access Lists	0
Users	6
Groups	0

Add, delete or edit user accounts.

Add, delete or edit groups.

Add or delete access lists (Packet filtering rules).

Configure this Hub.

Use external RADIUS authentication server for user authentication.

Establish Cascade Connection to Hubs on local or remote VPN Servers.

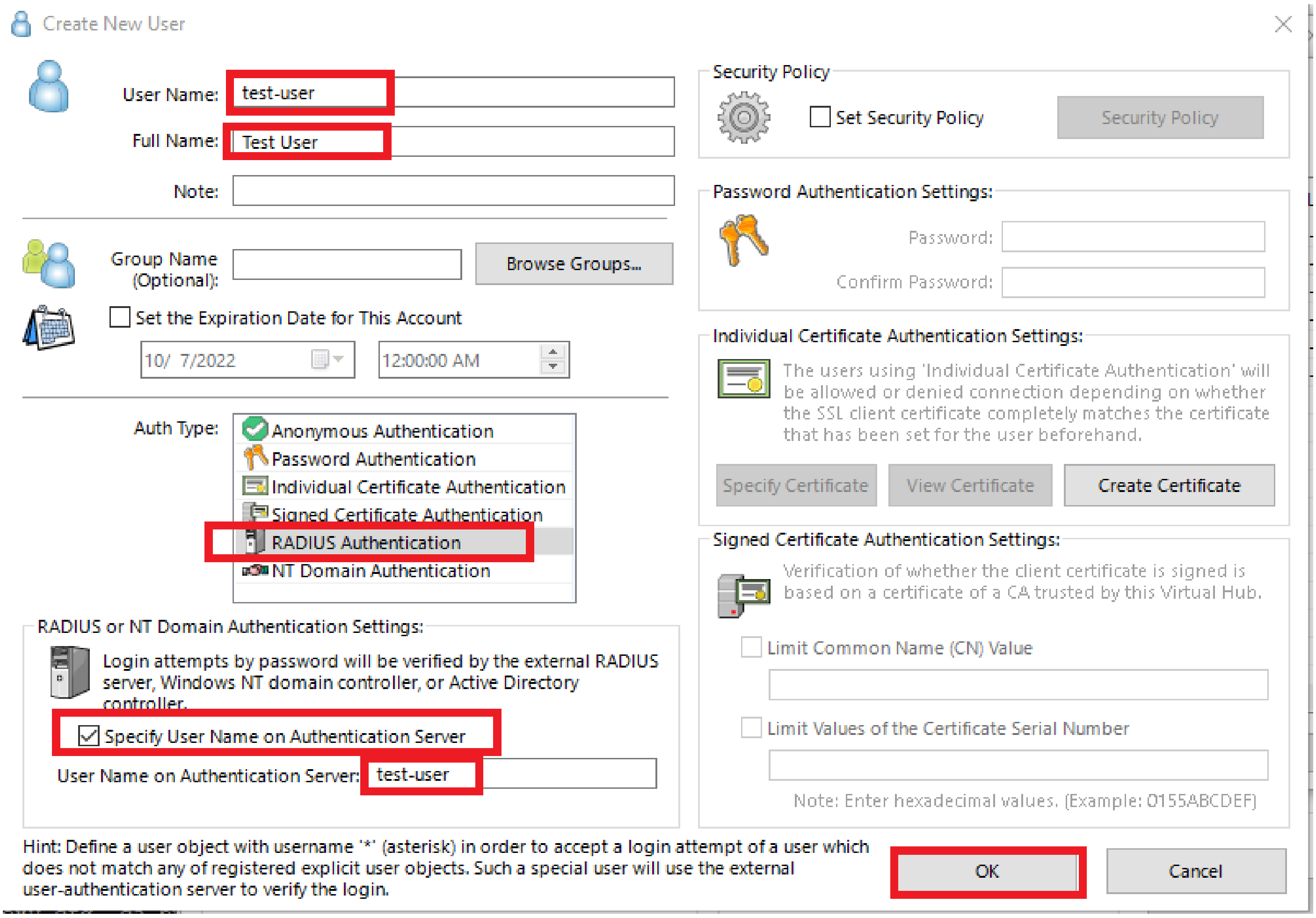
Configure settings of log saving function.

Manage trusted CA certificates.

Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

- In the **Manage Users** window, click **New** and in the **Create New User** window, fill in the **User Name** field, the **Full Nam**e field, ensure you set the **Auth Type** field to **RADIUS Authentication**, check the **Specify User Name on Authentication Server** field and enter the username of the user as it appears in Active Directory in the **User Name on Authentication Server** field and click the **OK** button (**Figure 10**).

Figure 10



Create New User

User Name: test-user

Full Name: Test User

Note:

Group Name (Optional): Browse Groups...

□ Set the Expiration Date for This Account

10/ 7/2022 12:00:00 AM

Auth Type:

- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication
- NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.

☑ Specify User Name on Authentication Server

User Name on Authentication Server: test-user

Security Policy

□ Set Security Policy

Password Authentication Settings:

Password:

Confirm Password:

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Signed Certificate Authentication Settings:

Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

□ Limit Common Name (CN) Value

□ Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEF)

Hint: Define a user object with username '*' (asterisk) in order to accept a login attempt of a user which does not match any of registered explicit user objects. Such a special user will use the external user-authentication server to verify the login.

If everything is setup correctly, when this user connects to your Softether VPN they should be prompted by the Duo app on their mobile device to approve the login. There is a hard coded limit of **10 seconds** for Softether to wait for authentication to complete. The user must approve the Duo MFA prompt within those 10 seconds or authentication will fail.

Revision #16
Created 6 October 2022 17:11:21 by Dino Edwards
Updated 7 October 2022 13:50:31 by Dino Edwards