



Quick Config Guide

Configuring Extended Authentication with VPN Mobile Users in AOS

Overview

This guide will show how to use AAA services to provide extended authentication within a VPN configuration.

Hardware/Software Requirements

Enhanced Feature Pack AOS Version 5.1 and later is required for VPN Extended Authentication support. A working knowledge of VPN configuration is required for this guide. VPN configuration guides can be found at <http://kb.adtran.com/>. A working knowledge of AAA is also required for this guide.

Configuration Steps

Command Line Configuration

STEP 1: Enter Global Mode
Router#**conf terminal**

STEP 2: Turn AAA services on
Router(config)#**aaa on**

STEP 3: Add RADIUS server to default RADIUS server group
Router(config)# **radius-server host 10.100.13.240 key Password 1**

STEP 4: Create named list for login authentication. This list will use the default RADIUS group.
Router(config)#**aaa authentication login VPNClients group radius**

STEP 5: Enter the appropriate IKE policy
Router(config)#**crypto ike policy 100**

STEP 6: Add support for Extended Authentication for the IKE policy
Router(config-ike)**client authentication server list VPNClients**

STEP 7: Return to privilege exec mode
Router(config-ike)#**end**

STEP 8: Save running configuration to startup config (after verification)
Router#**write memory**

Note: Appropriate AAA configuration will need to be applied to all console and terminal interfaces. This guide just references VPN Extended Authentication.

Example Config

```

!
aaa on
!
!
!
radius-server host 10.100.13.240 timeout 5 retransmit 3 key Password1
!
aaa authentication login VPNClients group radius
!
!
!
!
ip crypto
!
crypto ike client configuration pool Laptop
ip-range      192.168.26.1  192.168.26.254
dns-server    192.169.32.0
!
crypto ike policy 100
no initiate
respond anymode
local-id fqdn Router
peer any
client authentication server list VPNClients
client configuration pool Laptop
attribute 1
  encryption 3des
  hash md5
  authentication pre-share
!
crypto ike remote-id fqdn Laptop preshared-key Password1 ike-policy 100 crypto m
ap VPN 10
!
crypto ipsec transform-set highlysecure esp-3des esp-md5-hmac
mode tunnel
!
crypto map VPN 10 ipsec-ike
description Laptop
match address VPN-10-vpn-selectors
set transform-set highlysecure
ike-policy 100
mobile
!

```

Note: For XAUTH with site to site VPN configurations see the following commands in the AOS command reference guide.

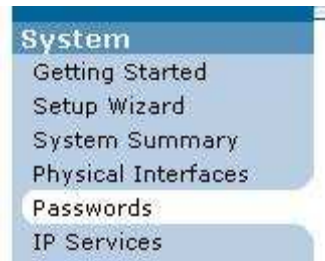
```

client authentication host
client authentication host xauth-type

```

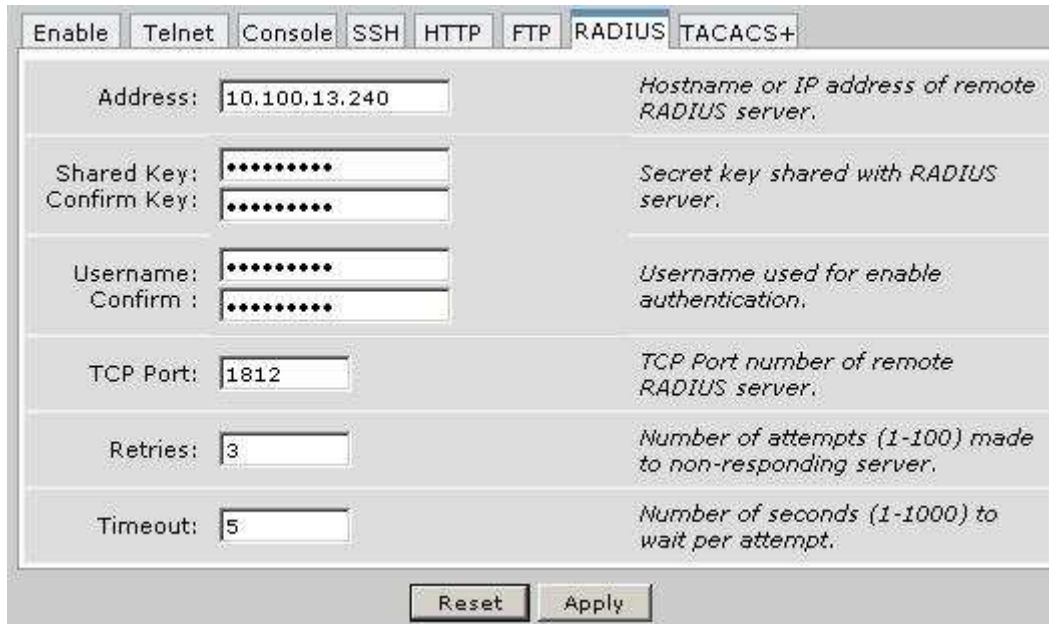
Web GUI Configuration

STEP 1: Click on the Password link.



STEP 2: Click on the RADIUS tab. Add the appropriate address, shared key, and port number for the RADIUS server. Click Apply.

Note: The username is only applicable if you want to use RADIUS to authenticate entering Privilege Exec mode.


A screenshot of the RADIUS configuration page in a web GUI. The page has several tabs: Enable, Telnet, Console, SSH, HTTP, FTP, RADIUS (selected), and TACACS+. The RADIUS tab contains the following fields and descriptions:

- Address: 10.100.13.240 (Description: Hostname or IP address of remote RADIUS server.)
- Shared Key: [Redacted] (Description: Secret key shared with RADIUS server.)
- Confirm Key: [Redacted]
- Username: [Redacted] (Description: Username used for enable authentication.)
- Confirm: [Redacted]
- TCP Port: 1812 (Description: TCP Port number of remote RADIUS server.)
- Retries: 3 (Description: Number of attempts (1-100) made to non-responding server.)
- Timeout: 5 (Description: Number of seconds (1-1000) to wait per attempt.)

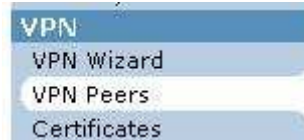
At the bottom of the form are "Reset" and "Apply" buttons.

STEP 3: Enable AAA support and click Apply.

Note: This turns AAA on for all terminal and console interfaces. This includes HTTP and FTP authentication.

A screenshot of the AAA Mode configuration page in a web GUI. It shows a checkbox labeled "AAA Mode Enabled" which is checked. To the right of the checkbox is the text: "Enables AAA authentication on every access point (TELNET, consoles, web, XAUTH, and FTP)."

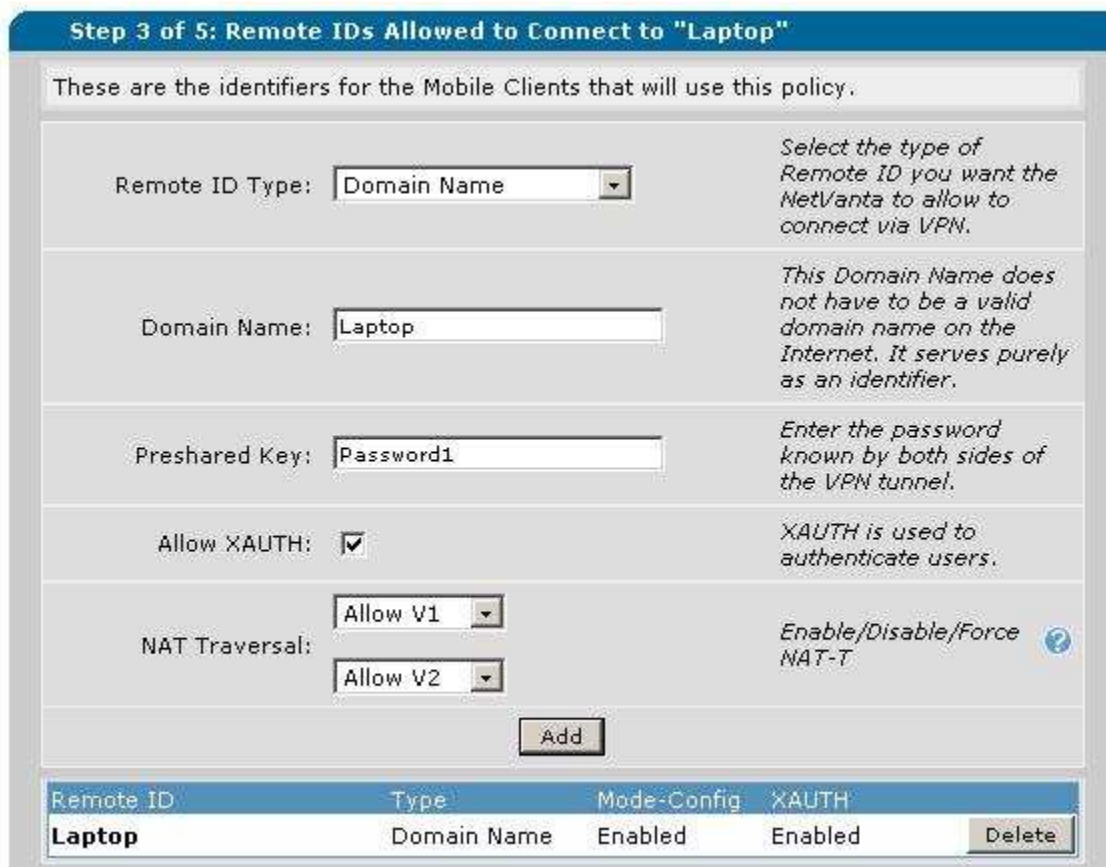
STEP 4: Click on the VPN Peers link.



STEP 5: Select the Mobile Peer which requires Extended Authentication.

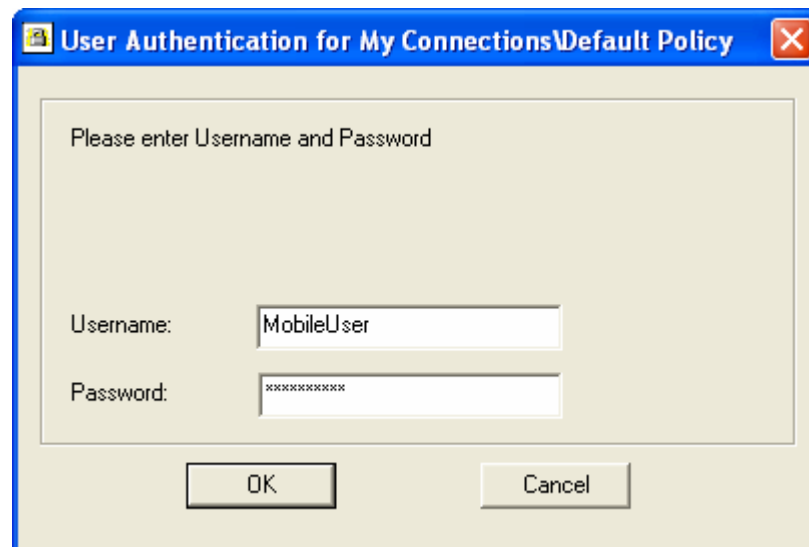
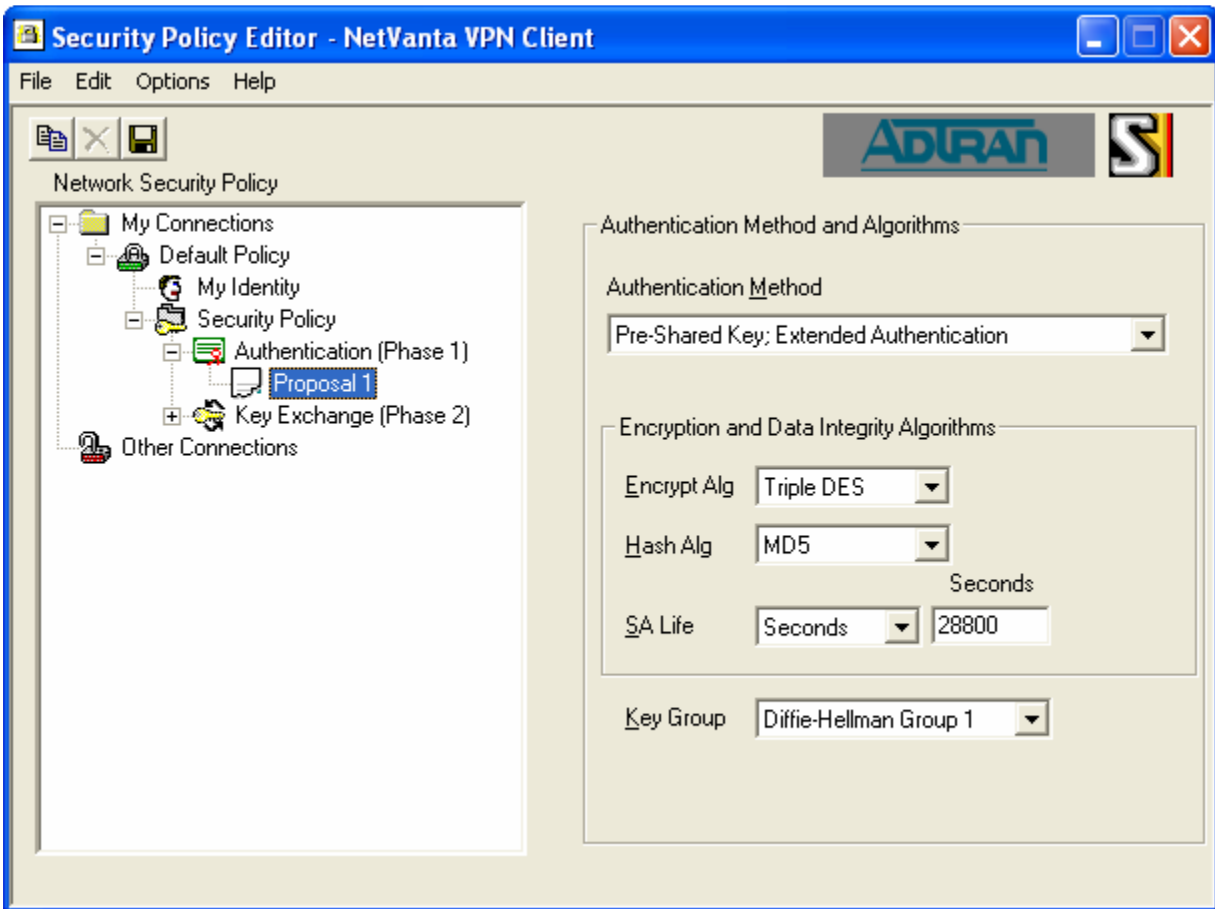


STEP 6: Select "Allow XAUTH" for the appropriate remote ID. It may require deleting the ID and creating a new one with XAUTH support.



VPN Client Config

The IKE (Phase 1) Authentication Method will have to be set to Extended Authentication. The client should be prompt for a username and password when connecting.



Example Configuration

```
!  
hostname "Router"  
no enable password  
!  
clock timezone -5-Eastern-Time  
!  
ip subnet-zero  
ip classless  
ip name-server 192.168.32.100  
ip routing  
!  
auto-config  
!  
event-history on  
no logging forwarding  
no logging email  
logging email priority-level info  
!  
no service password-encryption  
!  
username "admin" password "password"  
!  
!  
no ip firewall alg h323  
!  
aaa on  
radius-server enable-username Adtran3200  
ftp authentication LoginUseLocalUsers  
!  
radius-server host 10.100.13.240 timeout 5 retransmit 3 key Password1  
!  
aaa authentication login default group radius local  
aaa authentication login LoginUseTacacs group tacacs+  
aaa authentication login LoginUseRadius group radius  
aaa authentication login LoginUseLocalUsers local  
aaa authentication login LoginUseLinePass line  
!  
!  
!  
!  
ip crypto  
!  
crypto ike client configuration pool Laptop  
  ip-range      192.168.26.1  192.168.26.254  
  dns-server    192.169.32.0  
!  
crypto ike policy 100  
  no initiate  
  respond anymode  
  local-id fqdn Router  
  peer any  
  client authentication server list LoginUseRadius  
  client configuration pool Laptop  
  attribute 1  
    encryption 3des  
    hash md5  
    authentication pre-share  
!  
crypto ike remote-id fqdn Laptop preshared-key Password1 ike-policy 100 crypto m
```

```
ap VPN 10
!
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
  mode tunnel
!
crypto map VPN 10 ipsec-ike
  description Laptop
  match address VPN-10-vpn-selectors
  set transform-set esp-3des-esp-md5-hmac
  ike-policy 100
  mobile
!
!
!
!
interface eth 0/1
  ip address 192.168.32.1 255.255.255.0
  no shutdown
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 10.19.226.32 255.255.255.0
  crypto map VPN
  cross-connect 1 t1 1/1 1 ppp 1
!
!
!
ip access-list extended VPN-10-vpn-selectors
  permit ip 192.168.32.0 0.0.0.255 192.168.26.0 0.0.0.255
!
!
!
ip route 0.0.0.0 0.0.0.0 10.19.226.254
!
no ip tftp server
no ip tftp server overwrite
ip http authentication LoginUseLocalUsers
ip http server
no ip http secure-server
no ip snmp agent
no ip ftp server
no ip scp server
no ip sntp server
!
!
!
!
line con 0
  login authentication LoginUseLinePass
!
line telnet 0 4
  login authentication LoginUseLinePass
  no shutdown
line ssh 0 4
  login authentication LoginUseLocalUsers
  no shutdown
!
```

Troubleshooting

There are several resources available for troubleshooting. Radius Debugging can be done via the router console as well as VPN Client log. The RADIUS server itself should also provide feedback from RADIUS attempts.

Example output from “debug radius”

```
Router#debug radius
RADIUS AUTHENTICATION: Sending packet to 10.100.13.240 (1812).
RADIUS AUTHENTICATION: Waiting on response from server
RADIUS AUTHENTICATION: Receiving from RADIUS socket
RADIUS AUTHENTICATION: Response received from server (10.100.13.240)
RADIUS AUTHENTICATION: Received response from 10.100.13.240.
Router#undebug all
```

Example log file from VPN Client

```
39.889 My Connections\Default Policy - Initiating IKE Phase 1 (IP ADDR=10.19.226.32)
40.260 My Connections\Default Policy - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 6x)
40.801 My Connections\Default Policy - RECEIVED<<<< ISAKMP OAK AG (SA, KE, VID, NON, ID, HASH, VID,
NAT-D 3x, VID)
40.801 My Connections\Default Policy - Peer is NAT-T draft-02 capable
40.801 My Connections\Default Policy - Peer supports Dead Peer Detection Version 1.0
40.801 My Connections\Default Policy - Dead Peer Detection enabled
41.031 My Connections\Default Policy - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D 2x,
NOTIFY:STATUS_REPLAY_STATUS, NOTIFY:STATUS_INITIAL_CONTACT)
41.031 My Connections\Default Policy - Established IKE SA
41.031 My Connections\Default Policy - MY COOKIE 49 ce d3 3f 23 32 1e 61
41.031 My Connections\Default Policy - HIS COOKIE a3 af 39 de d8 a1 4f a
41.041 My Connections\Default Policy - RECEIVED<<<< ISAKMP OAK TRANS *(HASH, ATTR)
48.141 My Connections\Default Policy - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
49.153 My Connections\Default Policy - RECEIVED<<<< ISAKMP OAK TRANS *(HASH, ATTR)
49.153 My Connections\Default Policy - IKE Extended Authentication successful.
49.153 My Connections\Default Policy - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
49.303 My Connections\Default Policy - Initiating IKE Phase 2 with Client IDs (message id: DC10C3B8)
49.303 My Connections\Default Policy - Initiator = IP ADDR=10.19.226.6, prot = 0 port = 0
49.303 My Connections\Default Policy - Responder = IP SUBNET/MASK=192.168.32.0/255.255.255.0, prot = 0
port = 0
49.303 My Connections\Default Policy - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
49.313 My Connections\Default Policy - RECEIVED<<<< ISAKMP OAK TRANS *(HASH, ATTR)
49.313 My Connections\Default Policy - Received Private DNS Address = IP ADDR=192.169.32.0
49.313 My Connections\Default Policy - Received Private IP Address = IP ADDR=192.168.26.1
50.054 Virtual Interface constructed for local interface 192.168.26.1
50.114 Virtual Interface added: 192.168.26.1/255.255.255.255 on ISDN "SafeNet VA miniport".
50.154 FW ZA: Firewall Component is running and compliant.
50.314 My Connections\Default Policy - Abandoning IPsec SA negotiation (message id: DC10C3B8)
50.325 My Connections\Default Policy - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
51.476 My Connections\Default Policy - Initiating IKE Phase 2 with Client IDs (message id: 283D4DE8)
51.476 My Connections\Default Policy - Initiator = IP ADDR=192.168.26.1, prot = 0 port = 0
51.476 My Connections\Default Policy - Responder = IP SUBNET/MASK=192.168.32.0/255.255.255.0, prot = 0
port = 0
51.476 My Connections\Default Policy - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
51.506 My Connections\Default Policy - RECEIVED<<<< ISAKMP OAK QM *(HASH, SA,
NOTIFY:STATUS_REPLAY_STATUS, NON, ID 2x)
51.506 My Connections\Default Policy - Peer replay detection status=1.
51.506 My Connections\Default Policy - Filter entry 3 added: SECURE 192.168.026.001&255.255.255.255
192.168.032.000&255.255.255.000 010.019.226.032
```



```

51.516 Route 192.168.32.0/255.255.255.0->192.168.26.1 added.
51.516 My Connections\Default Policy - SENDING>>>> ISAKMP OAK QM *(HASH)
51.516 My Connections\Default Policy - RECEIVED<<<< ISAKMP OAK QM *(HASH,
NOTIFY:NOTIFY_CONNECTED)
51.516 My Connections\Default Policy - Loading IPsec SA (Message ID = 283D4DE8 OUTBOUND SPI =
BE69B69C INBOUND SPI = 1DC55DD0)
51.516
9-06: 11:13:35.041 My Connections\Default Policy - Deleting IPsec SA (OUTBOUND SPI = BE69B69C
INBOUND SPI = 1DC55DD0)
9-06: 11:13:35.071 My Connections\Default Policy - SENDING>>>> ISAKMP OAK INFO *(HASH, DEL)
9-06: 11:13:35.071 My Connections\Default Policy - Deleting IKE SA (IP ADDR=10.19.226.32)
9-06: 11:13:35.071 My Connections\Default Policy - MY COOKIE 49 ce d3 3f 23 32 1e 61
9-06: 11:13:35.071 My Connections\Default Policy - HIS COOKIE a3 af 39 de d8 a1 4f a
9-06: 11:13:35.071 My Connections\Default Policy - SENDING>>>> ISAKMP OAK INFO *(HASH, DEL)
9-06: 11:13:35.292 Interface lost: 192.168.26.1
9-06: 11:13:35.302 This is a GA version of NetVanta VPN Client.
9-06: 11:13:35.532 FW ZA: Firewall Component is running and compliant.
9-06: 11:13:35.532 Filter table loaded (2 entries).

```

Example output from Microsoft Windows 2003 Server Event Manager.

```

Event Type:      Information
Event Source:    IAS
Event Category:  None
Event ID:        1
Date:            9/6/2006
Time:            10:12:05 AM
User:            N/A
Computer:        LT6000R
Description:
User ceanes was granted access.
Fully-Qualified-User-Name = LT6000R\ceanes
NAS-IP-Address = 10.19.226.32
NAS-Identifier = <not present>
Client-Friendly-Name = Chris3200
Client-IP-Address = 10.19.226.32
Calling-Station-Identifier = XAUTH 100
NAS-Port-Type = <not present>
NAS-Port = 0
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = VPN Connections
Authentication-Type = PAP
EAP-Type = <undetermined>

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.
Data:
0000: 00 00 00 00      ....

```