OPNET Technologies, Inc.
VNE Server

RSA SecurID Ready Implementation Guide

Last Modified: March 19, 2009

Partner Information

Product Information	
Partner Name	OPNET Technologies, Inc.
Web Site	www.opnet.com
Product Name	VNE Server
Version & Platform	VNE Server 7.0 PL1 Windows & Linux
Product Description	VNE Server collects network data from disparate sources and intelligently merges this information into a unified network representation. VNE Server provides a complete framework for continuous, unattended management of network information and enables the creation of a high-fidelity, behavioral model of your production network called the Virtual Network Environment (VNE). VNE Server's behavioral network model can be used for network diagramming, network documentation, network planning and design, configuration assurance, and situational awareness.
Product Category	Networks and Communications

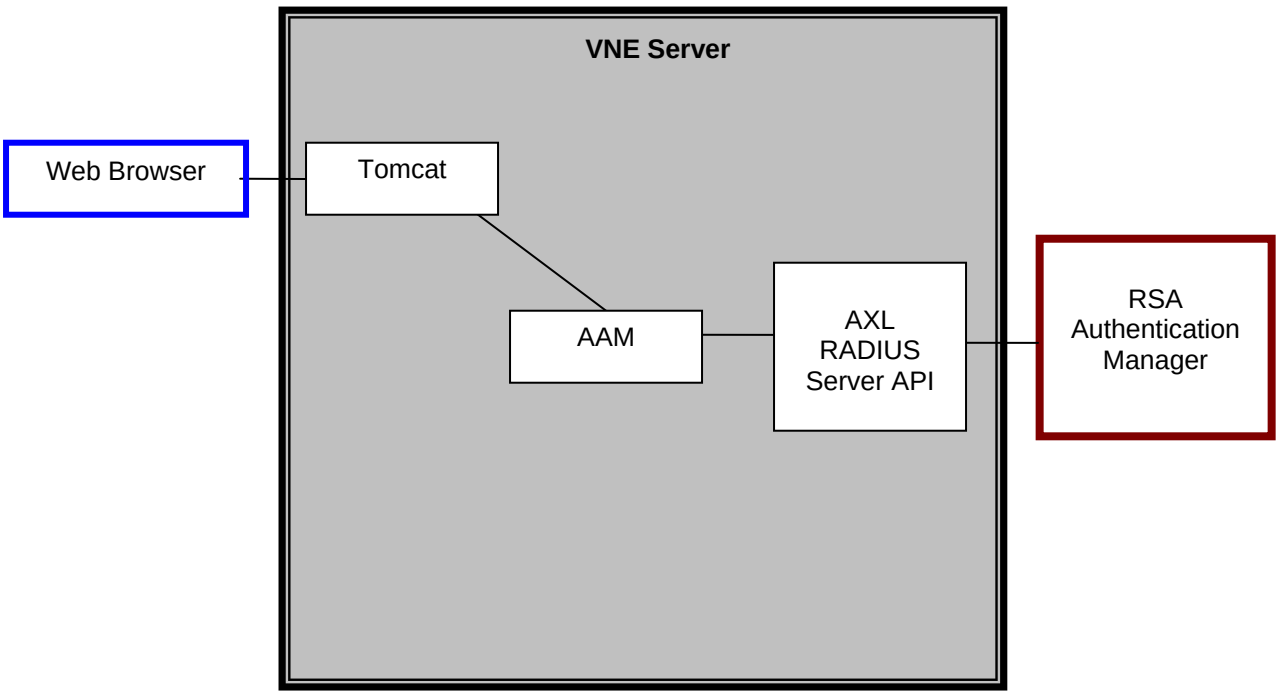
Making Networks and Applications Perform™

Solution Summary

OPNET has developed solutions based on distributed products and components that share data such as network models, configuration files, packet captures and reports. The richness and sensitivity of these data have led customers to demand that we implement improved security measures to protect these data from unauthorized access. While 1-factor authentication provides the necessary security for many organizations, there are others that require additional security measures. The purpose of this document is to configure VNE Server to use RSA SecurID 2-factor authentication.

VNE Server supports RSA SecurID authentication by communicating with RSA Authentication Manager servers via the RADIUS protocol.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
Secondary RADIUS Server Support	Yes (Platform dependent for number of servers)
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No
* = Mandatory Function when using Native SecurID Protocols	



Product Requirements

- This integration requires OPNET VNE Server 7.0 PL1 Build 8343 or higher.

Note: To view the current product requirements, please check the product web site located at:

http://www.opnet.com/solutions/system_requirements/vnes/index.html

Agent Host Configuration

To facilitate communication between the OPNET VNE Server and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the OPNET VNE Server within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the OPNET VNE Server as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the OPNET VNE Server will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**N/A**
sdconf.rec	None stored
Node Secret	None stored
sdstatus.12	N/A
sdopts.rec	Not implemented

Partner Product Configuration

Before You Begin

This section provides instructions for integrating OPNET VNE Server with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring Two-Factor Authentication on the VNE Server

Before you can use two-factor authentication, you must configure the VNE Server to communicate with your RADIUS server. The configuration is described in **Procedure IN-1** and **Procedure IN-2**.

Procedure IN-1 Create VNE Server Account with Administrative Privileges

When VNE Server is initially installed, it is configured for local authentication with a default “admin” account that has administrative privileges. Administrative privileges are required to configure and run VNE Server; therefore, before you configure VNE Server for remote authentication, you must create at least one VNE Server administrative account that matches a user account on the remote authentication server.

For example, if you log into RADIUS with the username “joe1234”, create a VNE Server account named “joe1234” and give that account administrative privileges. Administrative privileges are required to configure and run VNE Server but are not required for a user to authenticate and import data from VNE Server into OPNET analysis software.

Please follow the procedure below to create a VNE Server administrative account:

1. Login to the VNE Server using an account with administrative privileges.
2. Click on the *Users* tab.
3. In the *Modify User Accounts* area, select *Add New User* from the *Select User* drop-down menu.
4. Type a username in the User Name text field.

Important — If you will use remote authentication, make sure that the username you enter has a matching user account on the remote authentication server.

5. Type the user's name in the *First Name* and *Last Name* text fields.
6. Set the *Role* to admin.

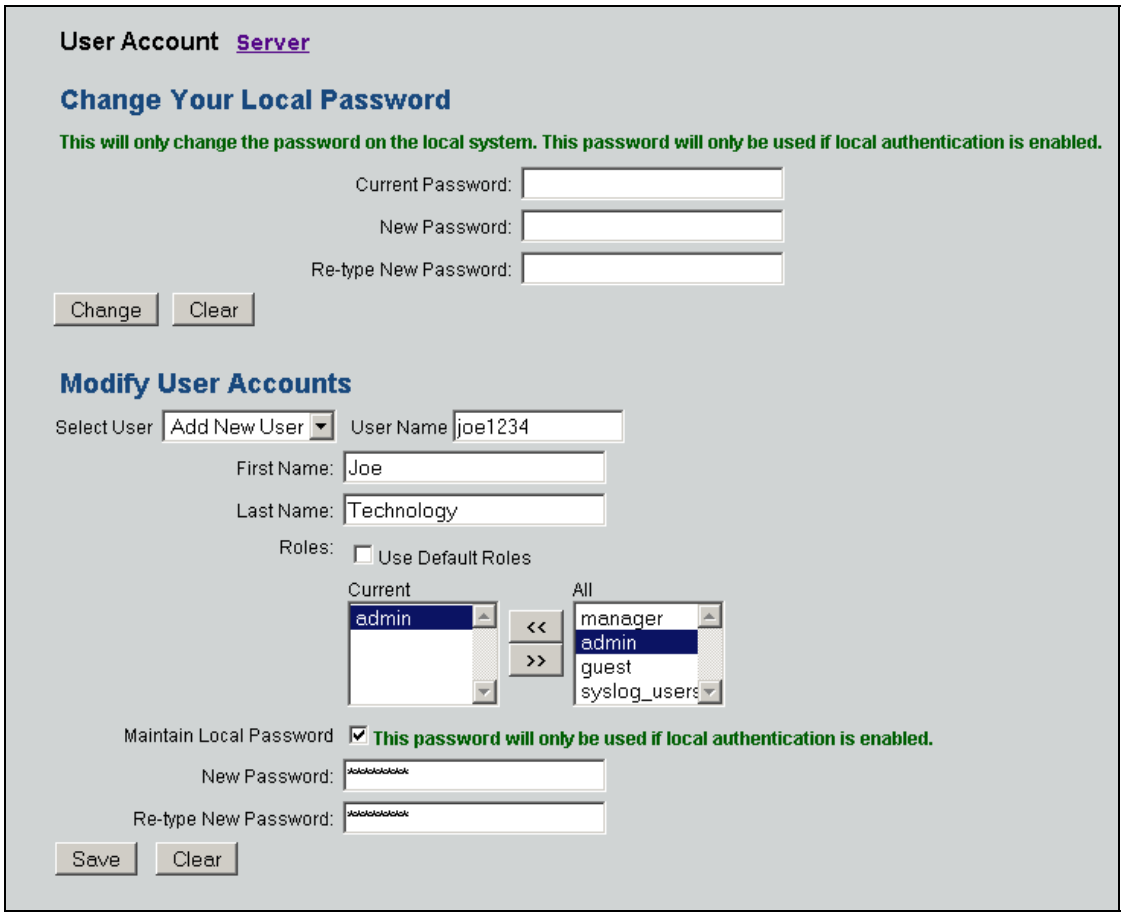


Figure IN-1 Create VNE Server Account with Admin Role

7. Define a local password for the account.

> **Note: Define a local password even if you plan to configure remote authentication. This will act as a safeguard until you verify successful login using remote authentication.**

   a. Select the *Maintain Local Password* checkbox.
   b. Enter a password in the *New Password* and *Re-type New Password* boxes. The entries must match. This password will only be used for local authentication.

8. Click *Save*.

Procedure IN-2 Configure RADIUS Two-Factor Authentication on the VNE Server

Once you have created a VNE Server administrative account as described in Procedure IN-1, you must create and configure a VNE Server *Authentication Module*.*

1. Login to the VNE Server using an account with administrative privileges.
2. Click on the *Users* tab.

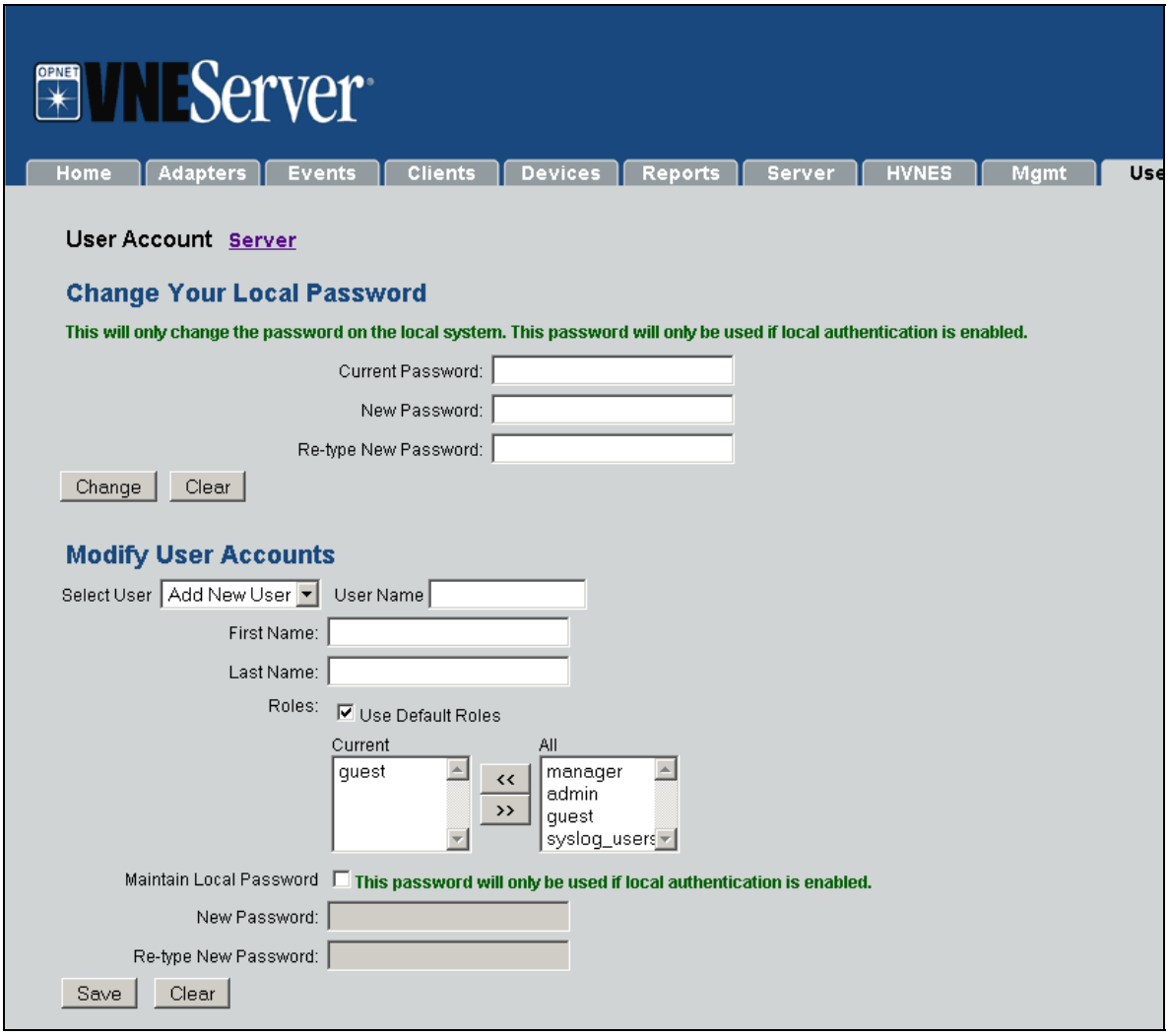


Figure IN-2- A VNE Server Users Tab

* You can add multiple *Authentication Modules* to the VNE Server *Authentication Chain*. In order to do so, please repeat the instructions in **Procedure IN-2** for each additional RADIUS server you wish to add.

3. Click on *Server*. The following screen appears.

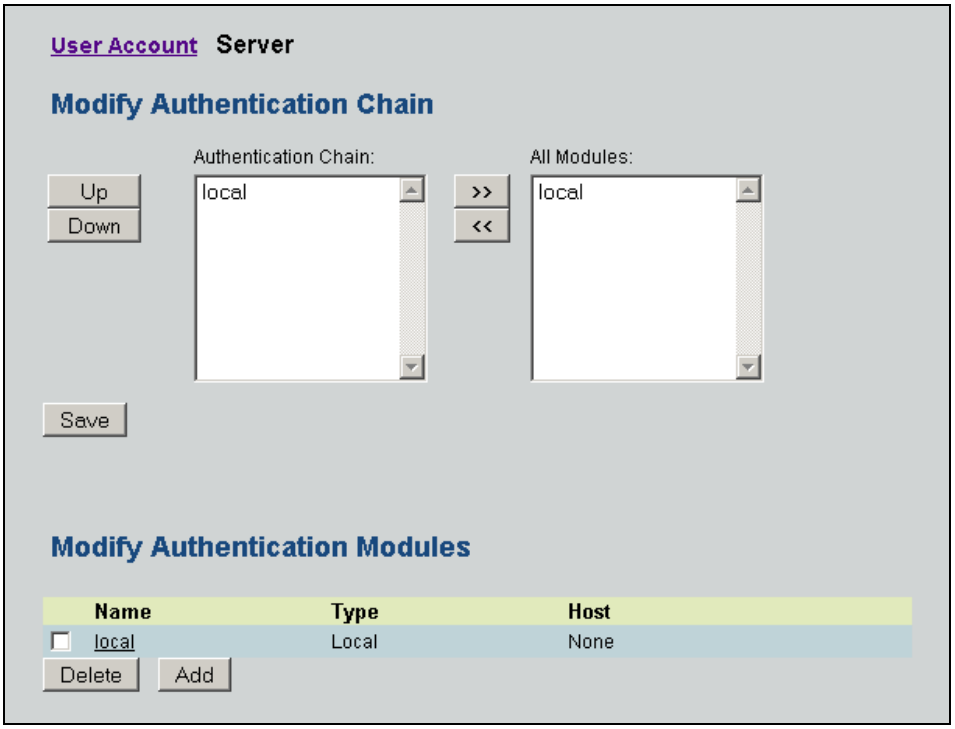


Figure IN-2 B Configure Authentication on VNE Server

4. Click the *Add* button. The following screen appears.

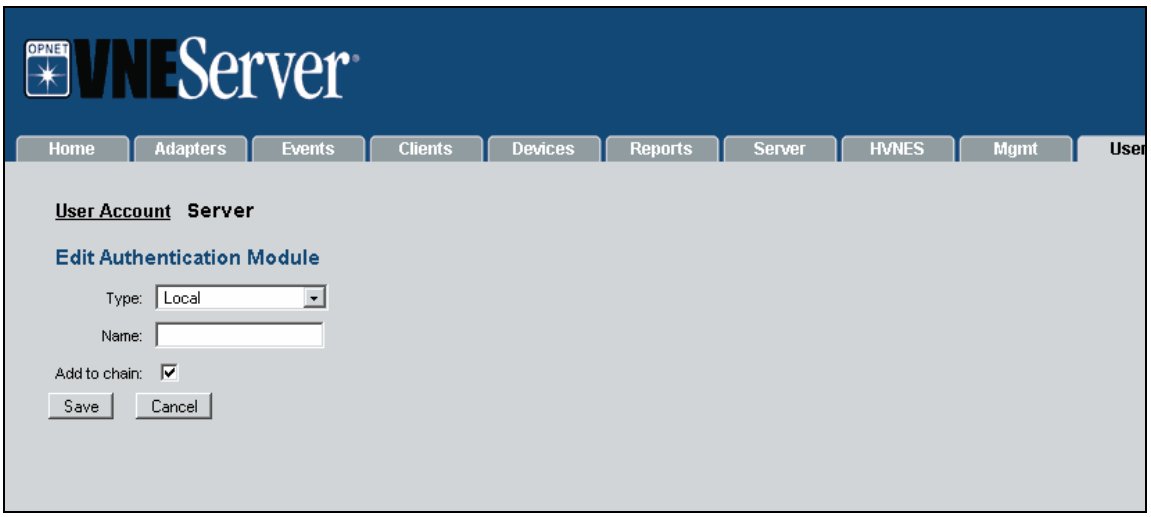


Figure IN-2 C Set Authentication Module Type

5. Select “RADIUS” from the *Type* drop-down menu.
6. Enter a name in the *Name* field. For identification purposes, we recommend that you enter the server name.
7. Select the *Add to chain* checkbox. The *Edit Authentication Module* screen appears.

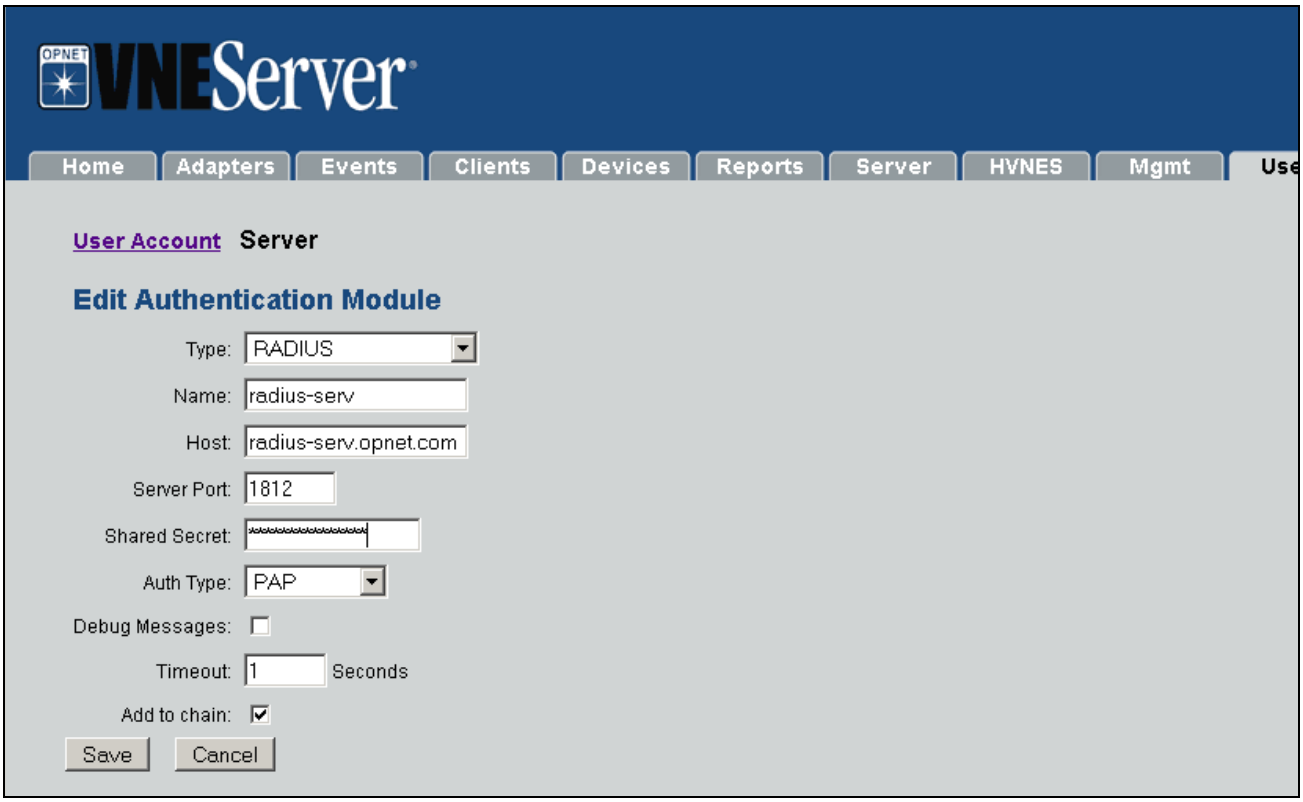
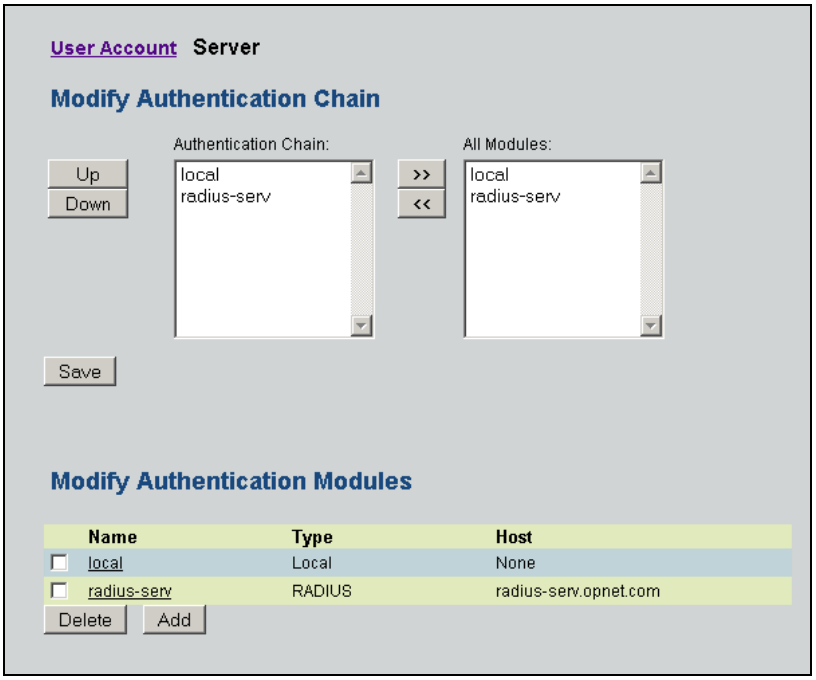


Figure IN-2 D - Edit Authentication Module for RADIUS Server

8. Enter the fully-qualified hostname for the RADIUS server in the *Host* textbox.
9. Accept or change the *Server Port* as is appropriate for your network.
10. Enter the *Shared Secret* password. (You must obtain this from the RADIUS administrator.)
11. Accept or change the *Auth Type* as is appropriate for your network.
12. Enter the number of seconds in the *Timeout* field. This timeout relates to the communication between the VNE Server and the RADIUS server[†].

[†] The default timeout value is 1 second, but you should increase it to something higher, such as 5 seconds, to allow time for the communication between the VNE Server and the RADIUS server.

13. Click *Save* to continue to the *Modify Authentication Chain* screen shown in **Figure IN-2 E**. Note that a "radius-serv" authentication module has been created and appears along with the "local" computer in both *Authentication Chain* and *All Modules*.



FigureIN-2- E Modify Authentication Chain

14. In the *Authentication Chain*, move "local" down until it is the last item[‡]. ***Keep "local" in the Authentication Chain until you verify successful login using remote authentication.***
15. Click *Save* to complete the configuration.
16. Verify that you can login to VNE Server as an administrator using remote authentication.
    a. Log out of VNE Server to end your current session.
    b. Login to VNE Server as an administrator using a RADIUS account and two-factor authentication. Enter your RSA SecurID passcode (PIN + tokencode) into the password field in the VNE Server login screen.

> **Note: If you cannot login to VNE Server using a RADIUS account and passcode, the RADIUS module may not be configured correctly for your network. Login to VNE Server using the password that you have configured for local authentication and work with your RADIUS administrator to verify the settings for the VNE Server RADIUS Authentication Module.**

    c. Verify that the *Mgmt* tab is visible. (This tab only displays for administrative users.)[§]

[‡] In an *Authentication Chain*, modules run in order from top to bottom. If remote authentication fails, local authentication can still be used to login to VNE Server.

[§] If you want to enforce login to VNE Server using only two-factor authentication, remove "local" authentication from the *Authentication Chain*. Before you do this, it is important that you verify you can login using remote authentication.

Certification Checklist For RSA Authentication Manager v6.x

Date Tested: March,12, 2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003 Server
OPNET VNE Server	7.0	Windows 2003 Server

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist For RSA Authentication Manager 7.x

Date Tested: March, 19, 2009

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003 Server
OPNET VNE Server	7.0	Windows 2003 Server

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function