

External Authentication with VMware View 5.1 Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

1 Contents

1	Contents.....	2
2	VMware View 5.1 Integration Guide.....	3
3	Pre Requisites.....	4
4	Pre-loaded Token Authentication.....	4
4.1	Configuration of VMware View 5.1.....	4
4.2	Configuration of SecurEnvoy.....	6

2 VMware View 5.1 Integration Guide

This document describes how to integrate VMware View 5.1 installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

VMware View 5.1 provides - Secure Virtual Desktop and Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as VMware View 5.1®), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of your PIN and your Phone to receive the one time passcode.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP directory server such as Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed to the SecurEnvoy Security Server via the RADIUS protocol, where it carries out a Two-Factor authentication. It provides a seamless login into the corporate network environment by the remote User entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, as does the VMware View 5.1 ®. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

VMware View 5.1

Microsoft (for installation of SecurEnvoy Security Server)

Windows 2008 server

IIS installed with SSL certificate (required for management and remote administration)

Access to Active Directory with an Administrator Account

SecurEnvoy

SecurAccess software release v6.2.500

3 Pre Requisites

It is assumed that the VMware View 5.1® is setup and operational. It is also assumed that the SecurEnvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and VMware View 5.1 ®, additional open ports will be required.

NOTE: SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from VMware View 5.1®.

4 Pre-loaded Token Authentication

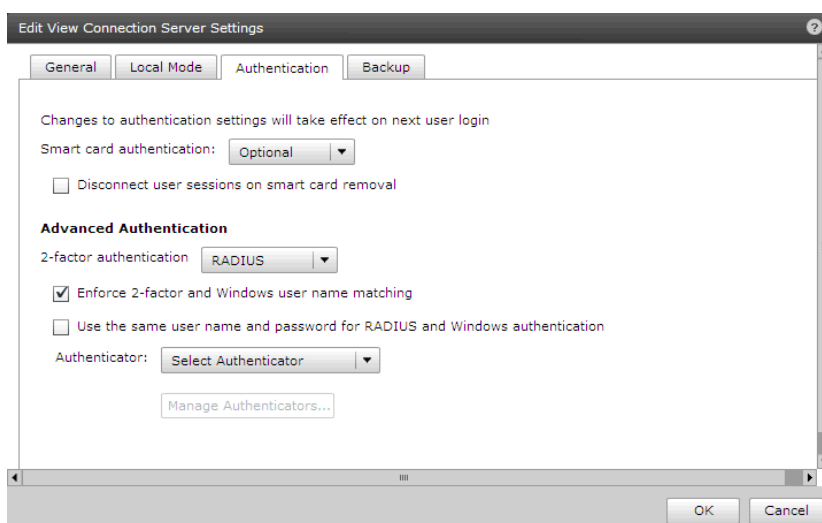
4.1 Configuration of VMware View 5.1

VMware View Administrator console

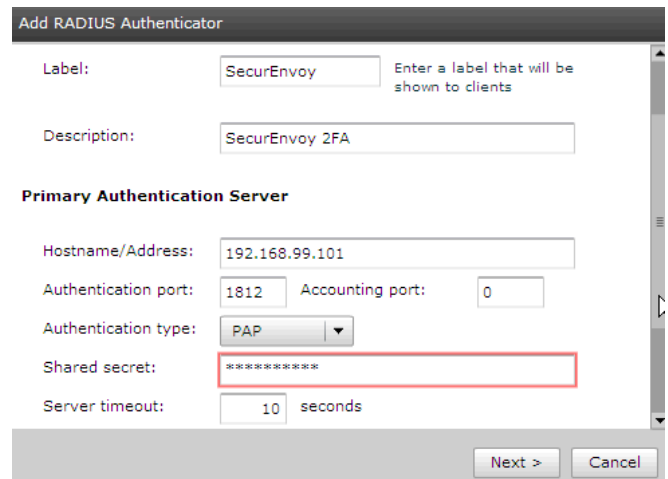
Launch the View Administrator console from the desktop shortcut or alternatively enter the following into a browser:

<https://hostname/admin> and log in.

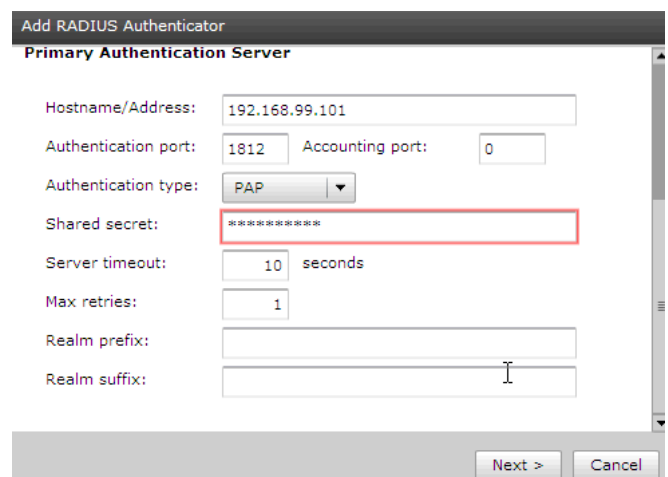
- a) Navigate to View Configuration - Servers - Connection Servers
- b) Select the Connection Server and click edit
- c) Select the Authentication Tab
- d) Under Advanced Authentication select "RADIUS"
- e) Under Authenticator select "create new authenticator" from the drop down menu



- f) Enter a Label and Description for the RADIUS settings
- g) Provide details of the SecurEnvoy server address (Hostname or IP address)
- h) Set the Authentication port (default 1812) and Accounting port to 0
- i) Make sure PAP protocol is selected

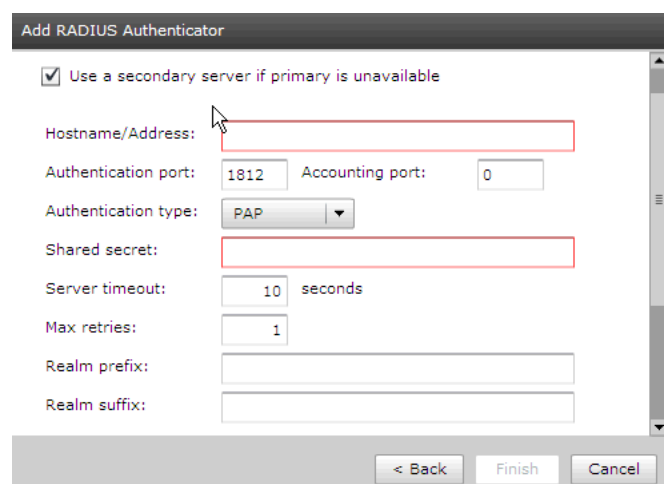


- i) Enter the shared secret (This MUST match the secret that is used upon the SecurEnvoy server)
- j) Set the Server timeout to 10 seconds
- k) Set Max retries to 1



To provide redundancy for RADIUS authentication a secondary RADIUS (SecurEnvoy server) can be declared, enable the checkbox "Use a secondary server if primary is unavailable"

- a) Populate settings as required
- b) Click "Finish" when complete

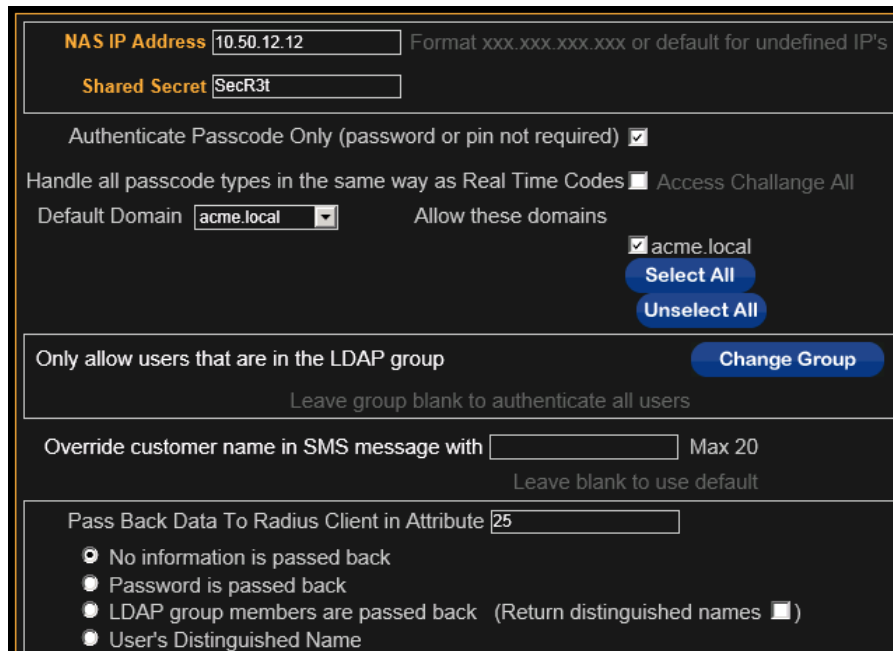


4.2 Configuration of SecurEnvoy

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** Button

Enter IP address and Shared secret for each VMware View 5.1 appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



The screenshot shows the configuration page for Radius authentication. It includes the following fields and options:

- NAS IP Address:** 10.50.12.12 (Format: xxx.xxx.xxx.xxx or default for undefined IP's)
- Shared Secret:** SecR3t
- Authenticate Passcode Only (password or pin not required):**
- Handle all passcode types in the same way as Real Time Codes:** **Access Challenge All:**
- Default Domain:** acme.local (dropdown menu)
- Allow these domains:** acme.local
 - Select All** (button)
 - Unselect All** (button)
- Only allow users that are in the LDAP group:** **Change Group** (button)
- Leave group blank to authenticate all users** (text)
- Override customer name in SMS message with:** **Max 20**
- Leave blank to use default** (text)
- Pass Back Data To Radius Client in Attribute:** 25
- Radio button options for Pass Back Data:**
 - No information is passed back
 - Password is passed back
 - LDAP group members are passed back (Return distinguished names)
 - User's Distinguished Name

Click checkbox "Authenticate Passcode Only (PIN not required)"

Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.