External Authentication with Ultra Protect v7.2® SSL VPN 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

© 2012 SecurEnvoy Ltd. All rights reserved

2 Ultra Protect v7.2® SSLVPN Integration Guide

This document describes how to integrate a Ultra Protect v7.2® SSL VPN installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Ultra Protect v7.2® SSL VPN provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Ultra Protect v7.2 ®), 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 seemless login into the corporate network environment by the remote User entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas the Ultra Protect v7.2® Server environment uses a GUI application. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Ultra Protect v7.2® SSL VPN
Ultra Protect v7.2

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

© 2012 SecurEnvoy Ltd. All rights reserved

3 Pre Requisites

It is assumed that the Ultra Protect v7.2® 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 the Ultra Protect v7.2® SSL VPN, 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 the Ultra Protect v7.2® SSL VPN.

There are two configurations that can be used when deploying SecurEnvoy as an authentication mechanism with Ultra Protect. If the real time pass code authentication option is to be configured within SecurEnvoy please refer to section 5, if pre-loaded token authentication is to be configured then please refer to section 4 on how the systems should be configured.

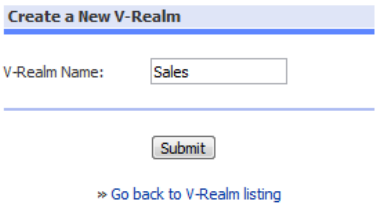
4 Pre-loaded Token Authentication

4.1 Configuration of Ultra Protect v7.2

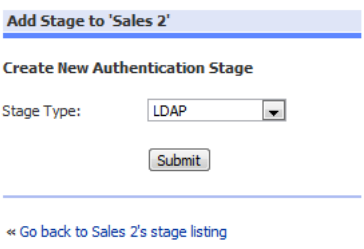
Launch the Ultra Protect v7.2 admin interface through a web browser.

This sections covers the creation of a new V-Realm, if one is already created then continue to the creation of the stage section.

a) Navigate to Authentication Settings and click on V-Realm Management
b) Select Add V-Realm
c) Enter a V-Realm Name *e.g. Sales*

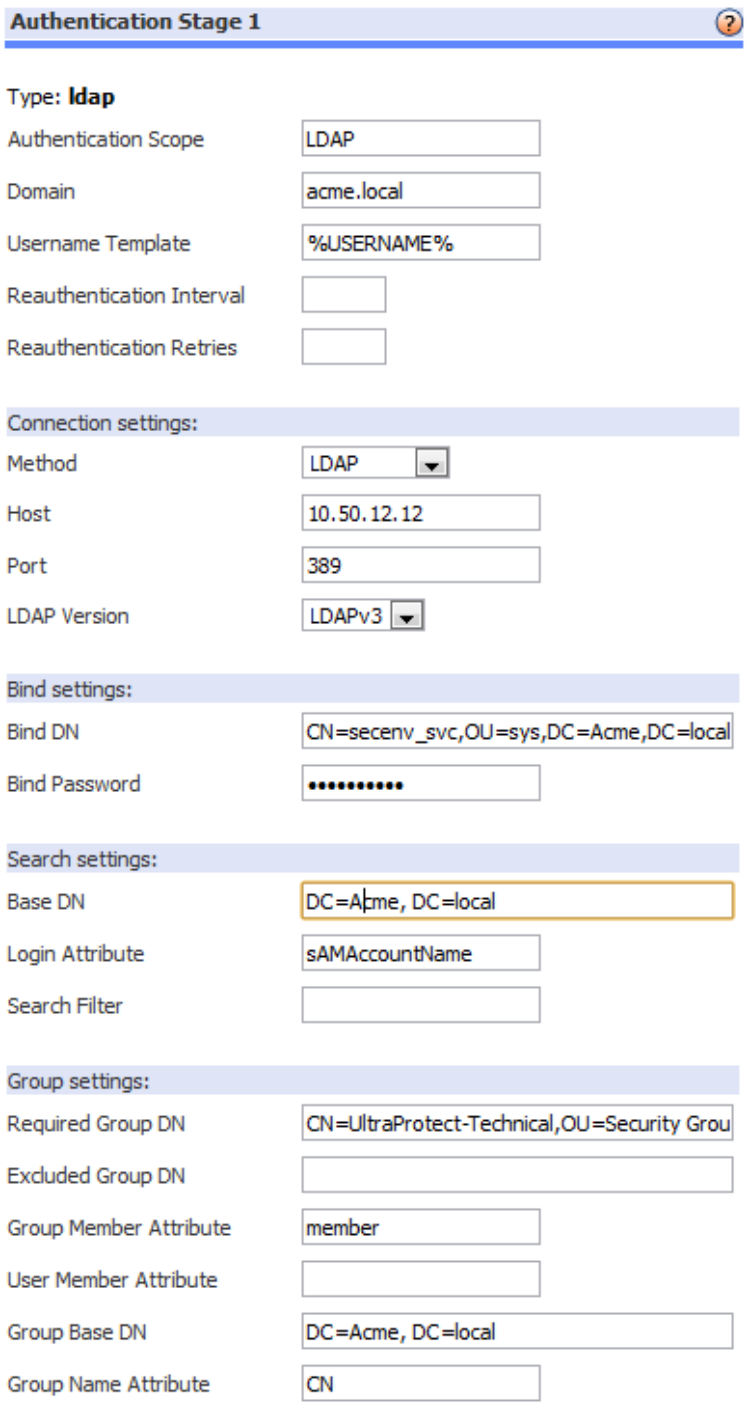


d) Click "Submit"
e) On the Create New Authentication Stage select LDAP



© 2012 SecurEnvoy Ltd. All rights reserved

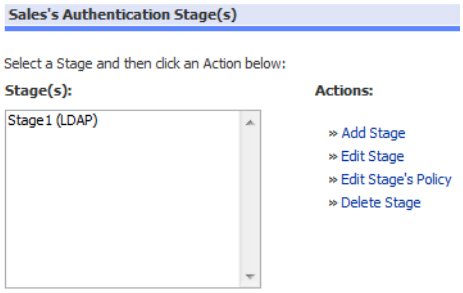
f) Complete the information required to 'connect' the authentication stage to Active Directory:



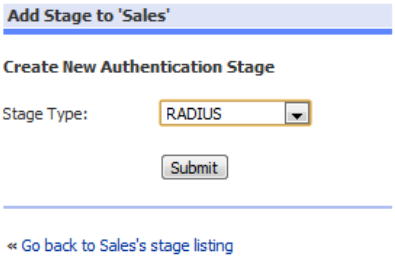
g) Click on '**Submit**'
h) Click '**Go back to V-Realm listing**'

© 2012 SecurEnvoy Ltd. All rights reserved

i) Create a new stage



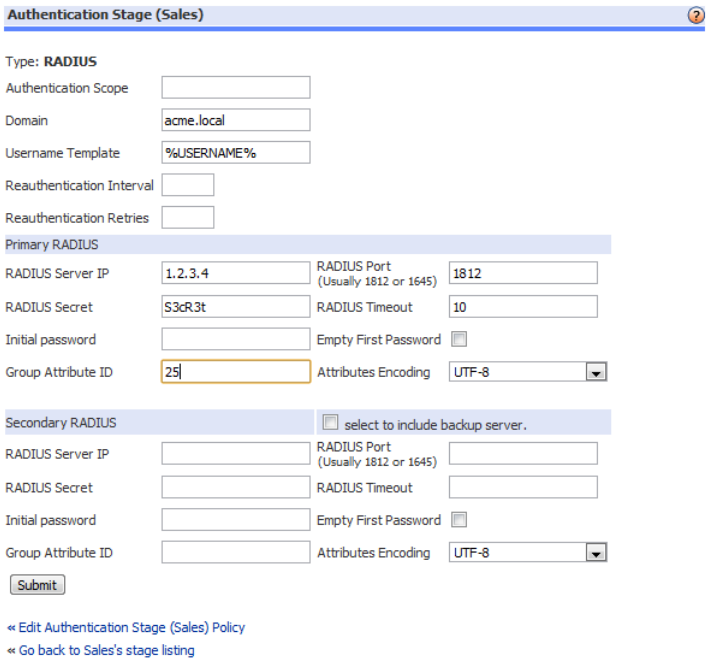
j) Select '**Add Stage**'



k) Complete the information required to 'connect' the authentication stage to SecurEnvoy:

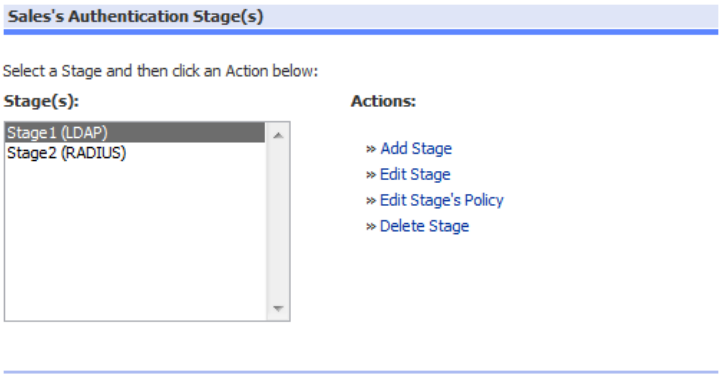
Domain
Radius Connection details and Shared Secret

Group Attribute ID (by default SecurEnvoy will pass group membership information back to the Ultra PROTECT box as ID 25)



© 2012 SecurEnvoy Ltd. All rights reserved Confidential

l) Click 'submit'
m) Click '**Go back to V-Realm listing'**

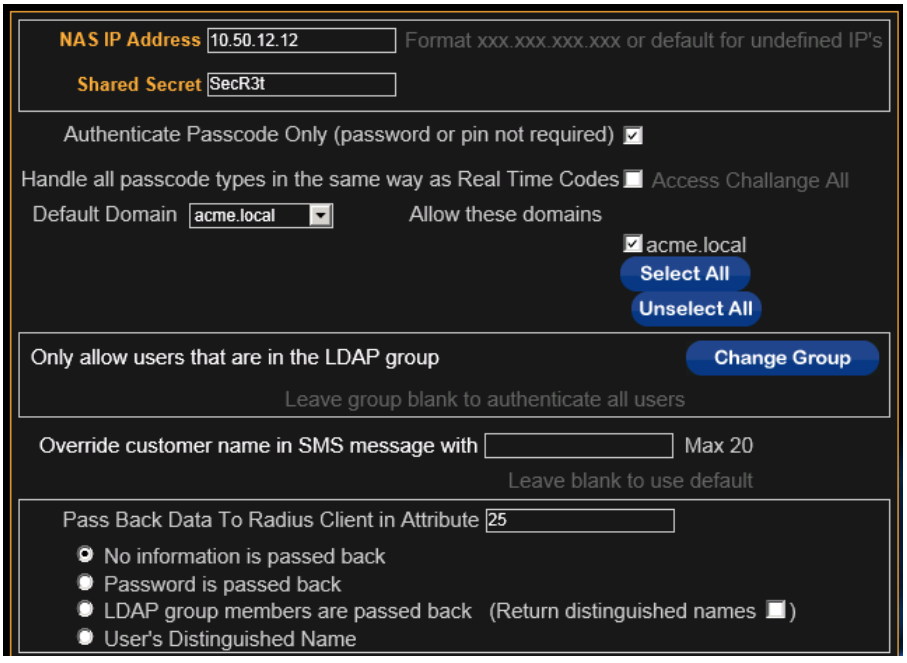


4.2 Configuration of SecurEnvoy

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 Ultra Protect v7.2® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



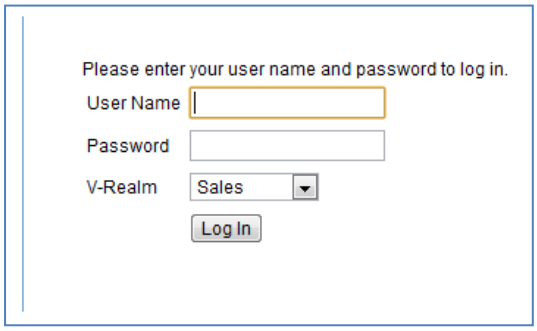
Click checkbox "Authenticate Passcode Only (PIN not required)

Click **"Update"** to confirm settings.
Click **"Logout"** when finished. This will log out of the Administrative session.

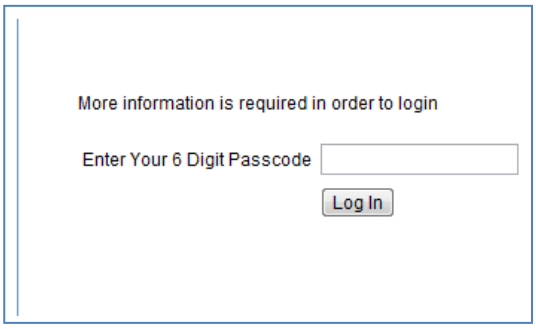
© 2012 SecurEnvoy Ltd. All rights reserved

4.1 Test Logon

Open a browser and navigate to the logon page



Enter Domain UserID and Pasword



Once validated user is then enters Passcode from SMS/Email/Soft Token

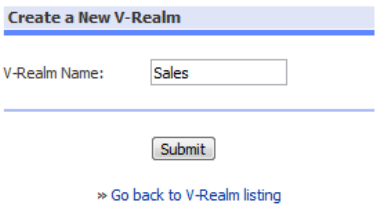
5 Real Time Token Authentication

5.1 Configuration of Ultra Protect v7.2

Launch the Ultra Protect v7.2 admin interface through a web browser.

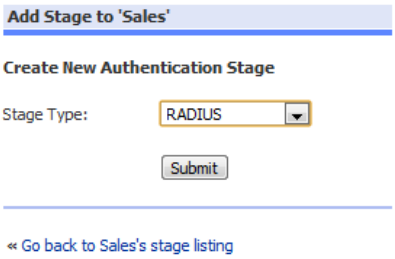
This sections covers the creation of a new V-Realm, if one is already created then continue to the creation of the stage section

a) Navigate to Authentication Settings and click on V-Realm Management
b) Select Add V-Realm
c) Enter a V-Realm Name *e.g. Sales*



d) Click "Submit"
e) Click '**Go back to V-Realm listing'**
f) On the Create New Authentication Stage Select RADIUS

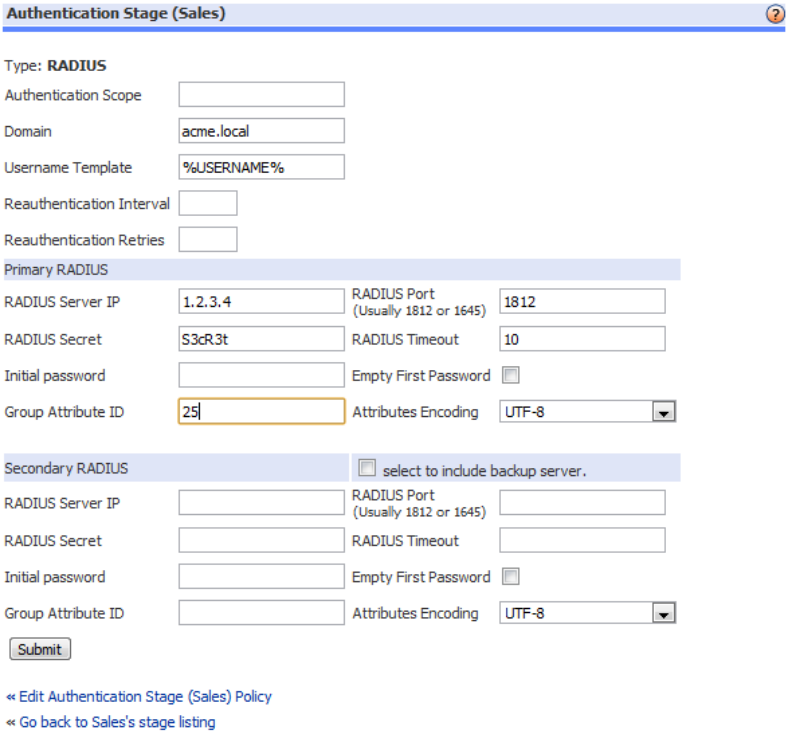
© 2012 SecurEnvoy Ltd. All rights reserved



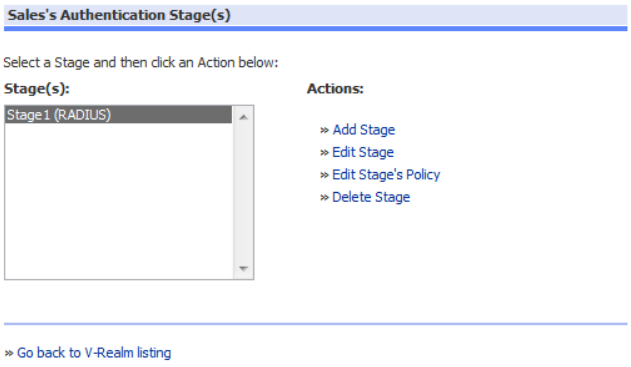
g) Complete the information required to 'connect' the authentication stage to SecurEnvoy:

Domain
Radius Connection details and Shared Secret

Group Attribute ID (by default SecurEnvoy will pass group membership information back to the Ultra PROTECT box as ID 25)



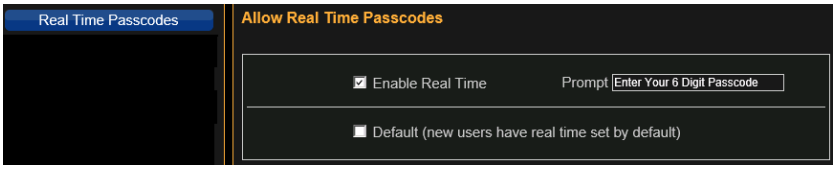
h) Click 'submit' – **PLEASE NOTE THERE SHOULD ONLY BE ONE STAGE**



© 2012 SecurEnvoy Ltd. All rights reserved

5.2 Configuration of SecurEnvoy

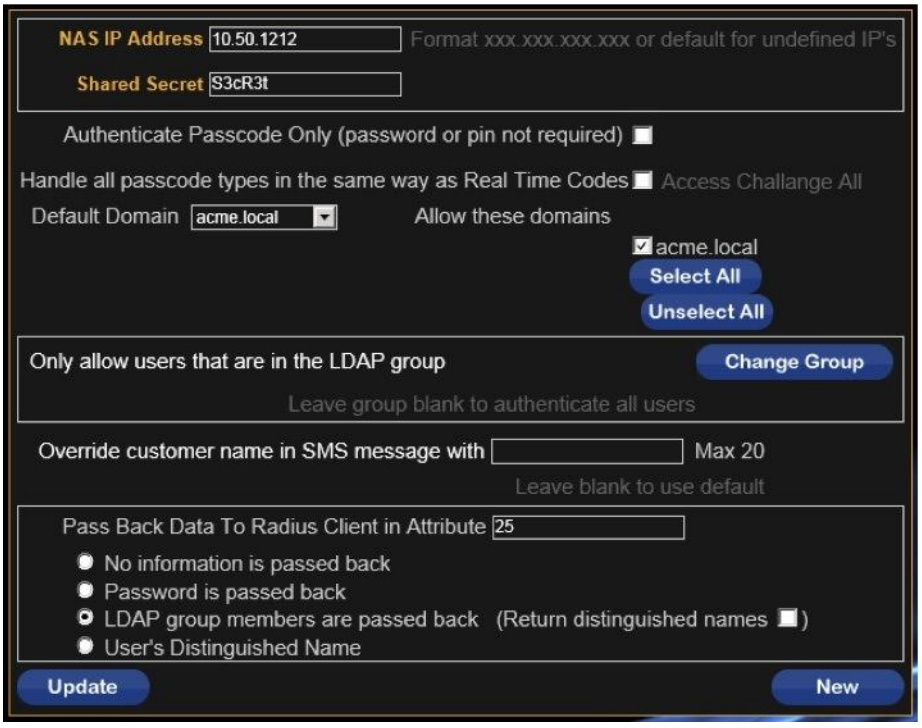
This configuration relates specifically where the real-time passcode option has been set up on the SecurEnvoy server (within the Config section).



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 Ultra Protect v7.2® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



If group membership information needs to be passed back to the Ultra Protect system then select 'LDAP group members are passed back'.

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

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

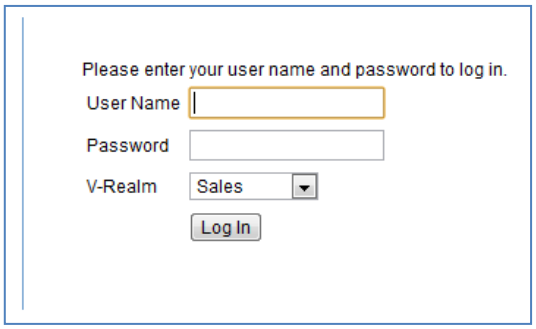
Confirm that the user's records have the '**Use Real time Not Preload'** option enabled in their user record.

© 2012 SecurEnvoy Ltd. All rights reserved

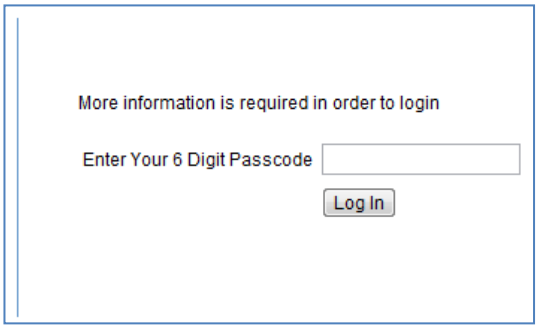
5.3 Test Logon

Open a browser and navigate to the logon page

A real time pass code will sent to your device; enter when prompted for the passcode.



User enters Domain UserID and Password



Once validated a user is then sent their Passcode via SMS.

User enters Passcode from SMS to complete the logon process.

© 2012 SecurEnvoy Ltd. All rights reserved