

**External authentication with
Fortinet Fortigate® UTM appliances
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	
	Special thanks to Simon Orchard of Trygg Data for Fortinet configuration	

Fortinet Fortigate UTM appliance Integration Guide

This document describes how to integrate a Fortinet Fortigate® UTM appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

The Fortinet Fortigate® UTM appliance provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Fortinet's Fortigate series), 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 onetime passcode.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The 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 via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration, as does the Fortinet Fortigate® UTM appliance. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Fortinet

Fortigate 60B, Ver. 3.00 MR 7 patch 2

SecurEnvoy

Windows 2003 server SP1

IIS installed with SSL certificate (required for remote administration)

Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.1.501

Index

1.0	Pre Requisites	3
2.0	Configuration of Fortigate® for SSL VPN users	3
4.0	Configuration of Fortigate® for IPSec dialup VPN users	5
5.0	Configuring the Forticlient IPSec client	6
6.0	Configuration of SecurEnvoy	7
7.0	Test Logon	8
7.1	SSL VPN	8
7.2	Forticlient IPSec	9
8.0	Single Sign On	9

1.0 Pre Requisites

It is assumed that the Fortinet® UTM appliance is setup and operational. An existing Domain user can authenticate using a Domain password and access applications.

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 Fortinet® FIREWALL 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 Fortinet® UTM appliance.

NOTE: Add radius profiles for each Fortigate® UTM appliance that requires Two-Factor Authentication.

2.0 Configuration of Fortigate® UTM appliance for SSL VPN users

To enable a SecurEnvoy Two-Factor authentication logon to the Fortigate® UTM appliance, login to the administration interface.

See diagrams below



- In the web GUI of the Fortigate unit, go to User -> Remote.
- Click on the Radius tab and Create New.
- Enter a name for the new connection, the IP address of the server where the Securenvoy Radius server is installed along with the Radius password as defined in the Securenvoy Radius server configuration.
- Make sure the Authentication scheme is set to use PAP.
- Under called station ID enter the relevant internal interface IP of the Fortigate unit and click OK.



Next configure SSL VPN users to authenticate via Radius.

- Go to User Group and click on Create New. Give the group a name and under Type select SSL VPN. Under Available Users/Groups, highlight the Radius server previously defined and add it to the Members window by clicking the -> arrow. Click OK.

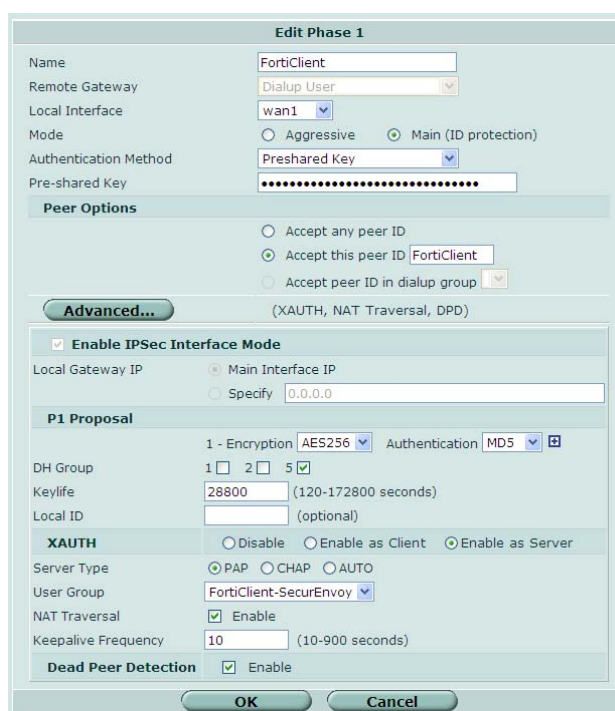


4.0 Configuration of Fortigate® UTM appliance for IPSec dialup VPN users

- When creating a Radius integrated IPSec user group, choose Firewall as Type, the rest is the same as for SSL VPN.

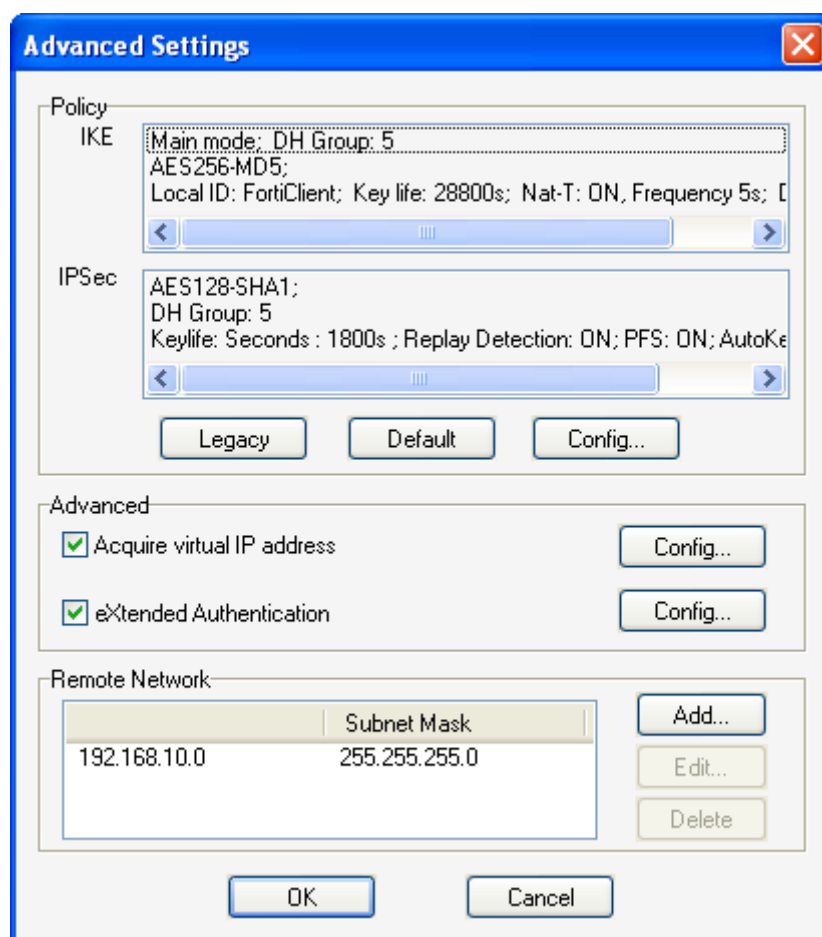


- Next, edit Phase 1 of a previously defined IPSec dialup connection. Click Advanced and choose Enable as server under Xauth. Disable Dead Peer Detection. Under User Group choose the previously defined Radius user group and click OK.



5.0 Configuring the Forticlient IPsec client.

- In the Forticlient console, go to VPN, choose the VPN connection to integrate, click advanced, edit and advanced.
- Click, eXtended Authentication. Under Config, ensure 'Prompt to login' is enabled.



Advanced Settings

Policy

IKE: Main mode: DH Group: 5
AES256-MD5;
Local ID: FortiClient; Key life: 28800s; Nat-T: ON, Frequency 5s; [

IPSec: AES128-SHA1;
DH Group: 5
Keylife: Seconds : 1800s ; Replay Detection: ON; PFS: ON; AutoKe

Legacy Default Config...

Advanced

Acquire virtual IP address Config...

eXtended Authentication Config...

Remote Network

Remote Network	Subnet Mask
192.168.10.0	255.255.255.0

Add... Edit... Delete

OK Cancel

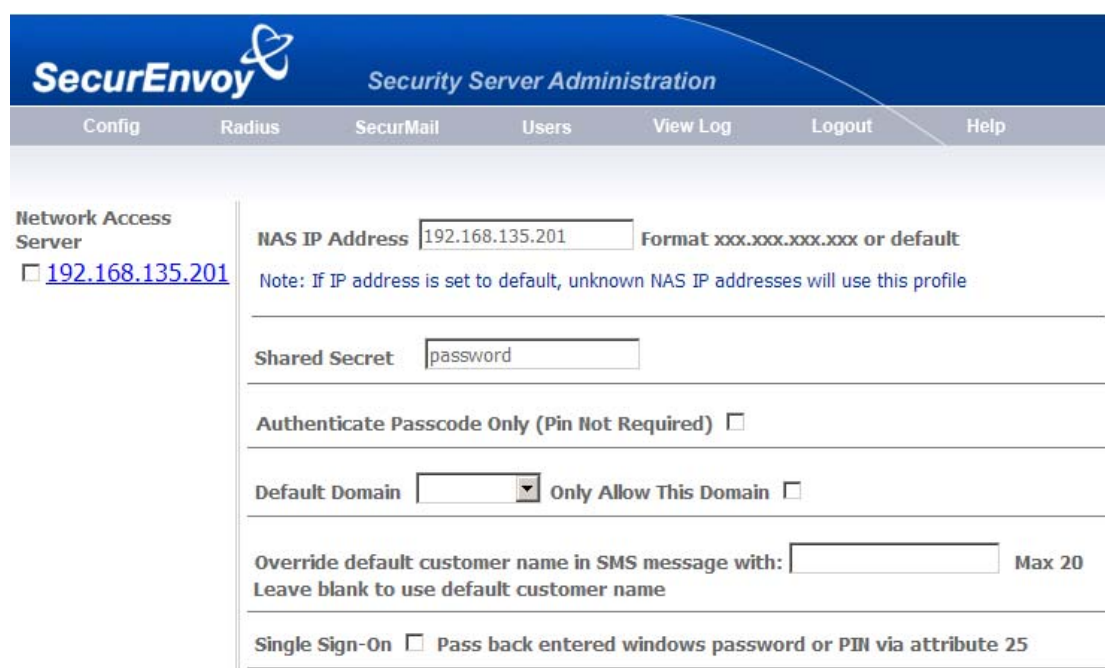
6.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing Microsoft password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

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 Fortinet® UTM appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



The screenshot shows the SecurEnvoy Security Server Administration interface. The top navigation bar includes links for Config, Radius, SecurMail, Users, View Log, Logout, and Help. The main content area is titled "Network Access Server" and features a list of servers with a checkbox next to the IP address "192.168.135.201". The configuration form for this server includes the following fields and options:

- NAS IP Address:** A text input field containing "192.168.135.201" with a note: "Format xxx.xxx.xxx.xxx or default". Below this is a note: "Note: If IP address is set to default, unknown NAS IP addresses will use this profile".
- Shared Secret:** A text input field containing "password".
- Authenticate Passcode Only (Pin Not Required):** A checkbox that is currently unchecked.
- Default Domain:** A dropdown menu with a downward arrow, followed by the text "Only Allow This Domain" and an unchecked checkbox.
- Override default customer name in SMS message with:** A text input field with "Max 20" characters. Below it is the instruction "Leave blank to use default customer name".
- Single Sign-On:** A checkbox that is currently unchecked, followed by the text "Pass back entered windows password or PIN via attribute 25".

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

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

7.0 Test Logon

7.1 SSL VPN

Browse to the SSL VPN web location of the Fortigate appliance

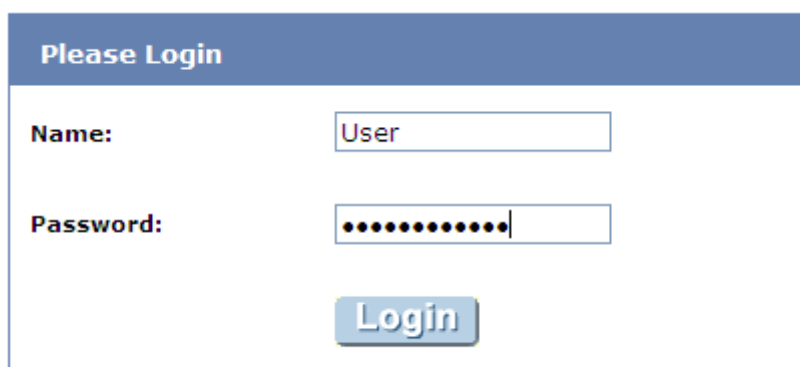
Two input dialogue boxes will be displayed.

User will enter: UserID in the Name box

Domain password in Password box appended with the Passcode (via SMS)

Click logon to complete the process.

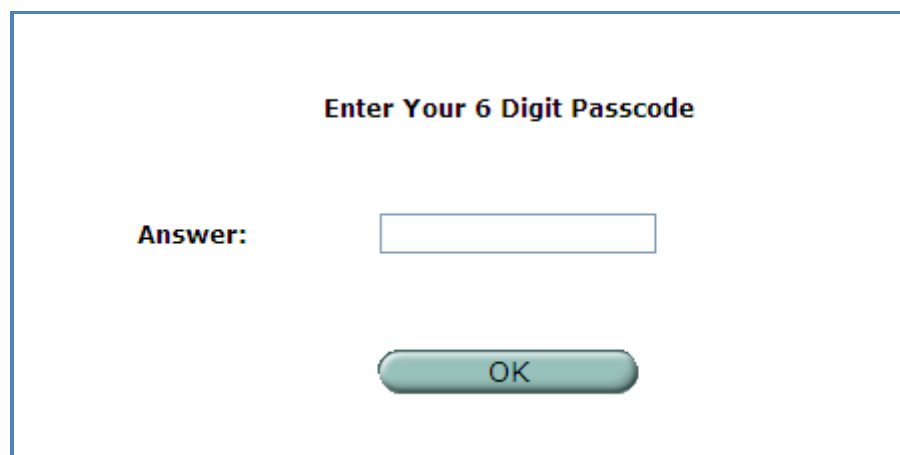
Once authenticated a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication.



The image shows a login dialog box titled "Please Login". It contains two input fields: "Name:" with the text "User" and "Password:" with a masked password of ten dots. Below the fields is a blue "Login" button.

When using SecurEnvoy "real-time codes", enter you username and password and click Login. A new page will be displayed where your 6 digit code is entered. The passcode is then sent to the user's mobile phone in real time.

To setup Real time passcode delivery upon SecurEnvoy, open the SecurEnvoy admin GUI, select "Config" click enable "real time" under SMS delivery click update. Select the "user" and find the user who requires "Real time delivery" select their profile, then tickbox "send real-time not pre load", click update user.



The image shows a dialog box titled "Enter Your 6 Digit Passcode". It contains one input field labeled "Answer:" and a green "OK" button.

7.2 Forticlient IPsec

Connect the IPsec tunnel as normal from Forticlient. When prompted for login details append the SecurAccess 6 digit code to the password.



8.0 Single Sign On

To enable a single sign on SecurEnvoy Radius can be set up to send the users Microsoft password back to the Fortigate appliance via Radius Attribute 25

Open the SecurEnvoy admin GUI, select "Radius", and select the Radius profile for Fortigate appliance.

Enable the checkbox "Single sign on", click update.

