

# External Authentication with F5® APM Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House	
	Brunel Road	
	Theale	
	Reading	
	RG7 4AB	
Phil Underwood	Punderwood@securenvoy.com	
Special thanks to	5 The Sterling Centre,	
Pranav Kumar of	Eastern Road,	
TSAvnet for F5	Bracknell, Berkshire,	
Integration	RG12 2PW	



# **1** Contents

1	Cor	ntents	.2
2	F5(	APM Integration Guide	. 3
3	Pre	Requisites	.4
4	Tok	enless Authentication (All Types)	.4
	4.1	Configuration of F5® APM	.4
	4.2	Configuration of SecurEnvoy	. 8
	4.3	Test Logon (SSL VPN)	.9
		,	



## 2 F5® APM Integration Guide

This document describes how to integrate a F5® APM with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

F5® APM provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as F5® APM) 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, either by receiving a passcode via SMS, email or by using the Soft Token.

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 F5® APM 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:

### F5® APM

**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 F5® APM 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 F5® APM, 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 F5® APM.

Only a single configuration is required, this will then support users with SMS sent via Pre-Load and Real Time as well as Soft Tokens, as F5® APM supports RADIUS (Challenge Response). Configuration in this guide refers to this type of approach.

# 4 Tokenless Authentication (All Types)

## 4.1 Configuration of F5® APM

- 1. Using a web browser log into the F5 APM
- In Navigation pane, go to Access Policy – AAA servers – and select RADIUS
- 3. Enter details for the SecurEnvoy server (RADIUS)
  - a. Name
  - b. Set mode to authentication
  - c. Server connection set as Direct
  - d. Add SecurEnvoy server IP address
  - e. Set authentication port to 1812
  - f. Enter the shared secret (requires defining on SecurEnvoy server)
  - g. Set timeout to 10
  - h. Set retries to 1
  - i. Click Finish to complete





- 4. Now add the AAA server to an existing access-policy or in this example create a new profile.
  - a. Select new profile
  - b. Assign a name
  - c. Set Cookie options to Secure
  - d. Assign Language to English
  - e. Click finished to complete

General Properties		
Name	86-1	
Parent Profile	access	
Settings		Custom
Inactivity Timeout	900 seconds	1
Access Policy Timeout	300 seconds	1
Maximum Session Timeout	0 seconds	1
Max Concurrent Users	0	1
Max Sessions Per User	0	
Max In Progress Sessions Per	0	1
Restrict to Single Client IP		
Configurations		
Logout URI Include		
Logout URI Timeout	5 seconds	
CCO Access Authentication Dom	1	
Domain Cookie		
Cookie Options	Secure     Persitent     HTTP Only	
SSO Configuration	None x	
Language Settings		
Additional Languages	Mar (aa)	
Languages	Accepted Languages Explicit, (el) Accepted Languages  (applicit, (el) Accepted Languages ((el) Accepted Langua	

5. Navigate to the Access Profiles list, click the name of the profile you wish to add RADIUS authentication. In this example select the access policy named earlier (SE-1).

Access Policy	» Access Profiles : Access Profiles List						
🚓 🚽 Access	Profile List Windows Group Policy List						
*	Search					C	reate Import
🔽 💌 Status	▲ Name	Application	Access Policy	Export	Сору	Virtual Servers	Partition / Path
E 🕨	SE-1		Edit	Export	Сору		Common
<b>•</b>	Wiki_Access		Edit	Export	Сору	wiki_VS wiki_VS_443	Common
0 🕨	access		(none)	(none)	(none)		Common
Delete Apr	Access Policy						

- 6. Click the edit access policy for SE-1
  - a. Then select Add New Macro, the following screen is shown.

← → C ▲ ▲ bttps://192.168.250	.105/sam/admin/vpe2/	public/php/vpe.php?r[accessPolicyName]	=/Common/SE-1		
8 Google 🗋 Bracknell SA 🗋 Warrington SA	Facebook C2 The Ch	ampion Com 🐠 eBay - one of the UK 🚺 Ba	sttlelog / Battlefiel 🌾 N	lewzbin - Usene	
6					
Access Policy: /Common/SE-1		When you click Add Item, the selected ite	em is immediately added to you	r access policy.	
fallback	Predefined Actions     General Purpose				
Start - Deny	Logon Page	Web form-based logon page for collecting end user credentials	O HTTP 401 Response	HTTP 401 authentica	
Add New Macro	External Logon Page	Redirect user to externally hosted web form-based logon page	Full Resource Assign	Advanced Resources	
An access policy consists of a start point, actions, and purpose-built set of predefined access policy items, to	Resource Assign	Simple assignment of Connectivity Resources	O ACL Assign	Simple ass Lists (ACL:	



b. Continue through the Macro, the following screen is shown for the Logon Page

ess Policy: /Common/SE-1 [Edit Endings] (Endings: Allo	Properties Branch R	les		
	Name: Logon Page			
t	Logon Page Agent			
	Split domain from full U	ername No 💌		
w Macro	Туре	Post Variable Name	Session Variable Name	Read Only
policy consists of a start point, actions, and one or more endings. To in	s 1 text 💌	username	username	No 👻
set or predenned access poicy items, to simplify access poicy creat started with Device Wizards. On the main pavination pane, expand 3	2 password -	password	password	No 💌
ager for more on creating and editing an access policy.	3 none 💌	field3	field3	No 💌
nline Help for more Visual Policy Editor basics.	4 none 💌	field4	field4	No 👻
	5 none 💌	field5	field 5	No 💌
	Customization			
	Language	en 💌	Re	set all defaults
	Form Header Text	Secure Logon for F5 Networks		
	Logon Page Input Field #1	Username		
	Logon Page Input Field #2	Password		
	Logon Page Input Field #3	Field 3		
	Logon Page Input Field #4	Field 4		
	Logon Page Input Field #5	Field 5		
	Lanas Dutter	Logon		

b Continue through the Macro, the following screen is for setting authentication, select RADIUS auth

← → C ▲ ▲ ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓	.105/sam/admin/vpe2/p	ublic/php/vpe.php?r[accessPolicyName]=	=/Common/SE-1		
8 Google 🗋 Bracknell SA 🗋 Warrington SA	Facebook C2 The Cha	mpion Com 🐠 eBay - one of the UK 🚺 Bat	ttlelog / Battlefiel 🧌 Ne	wzbin - Usenet Se 🙍 Nagios XI - Logi	n   🀉 High Elf P
Apply Access Policy					
Access Policy: /Common/SE-1 📑	O Dynamic ACL	Assignment of Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP	Rule Event	Raises an iRule ACCESS_POLICY_AGENT_ for use with custom iRules scripts	EVENT event
Start	Empty	Creates an Empty Action for constructing custom Branch Rules			
	Authentication				
Add New Macro	AD Auth	Active Directory authentication of end user credentials	O AD Query	Active Directory query to pull user attribu with resource assignment or other functio Mapping	tes for use ins / Group
An access policy consists of a start point, actions, and purpose-built set of predefined access policy items, to	Olient Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile	CRLDP Auth	Certificate Revocation List Distribution Po client certificate authentication	int (CRLDP)
You can get started with <u>Device Wizards</u> . On the main <i>Policy Manager</i> for more on creating and editing an place are the Optime Units for each final Data. Edited	O HTTP Auth	HTTP authentication of end user credentials	DAP Auth	LDAP authentication of end user credenti	als
Please see the <u>Unline resp</u> for more visual Policy Edito	C LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions / Group Mapping	e 💿 OCSP Auth	Online Certificate Status Protocol (OCSP) certificate authentication	client
	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate	RADIUS Auth	RADIUS authentication of end user crede	ntials

c. Continue through the Macro, the following screen is for selecting the RADIUS server

Properties* Branch Rules	
Name: RADIUS Auth	
RADIUS	
AAA Server	/Common/Secure_Envoy_AAA
Show Extended Error	Disabled 💌
Max Logon Attempts Allowed	1 💌

d. Continue through the Macro, the following screen is to set the logic for authentication



← → C ☆ (2010) (192.168.250.105/sam/admin/vpe2/public/php/vpe.php	p?r[accessPolicyName]=/Common/SE-1
8 Google 🗋 Bracknell SA 🗋 Warrington SA 📑 Facebook 😋 The Champion Com 🐠 eBa	ay - one of the UK 🔢 Battlelog / Battlefiel 🌾 Newzbin
fs Apply Access Policy	
Access Policy: /Common/SE-1 Edit Endings (Endings: Allow, Deny [default])	
fallback ,Xfallback ,XSuccessful ,	
Start + Logon Page + Deny	
fallback + Deny	Select Ending:
	Allow
Add New Menne	Deny
Add New Macro	

e. Once complete, the logic should look like the screenshot below



- f. Navigate to Virtual servers (Create virtual server as per F5 guides)
- g. Select the correct Virtual server



h. Apply access policy to virtual server

Connection Limit	0
Address Translation	C Enabled
Port Translation	C Enabled
Source Port	Preserve
Clone Pool (Client)	None
Clone Pool (Server)	None
Auto Last Hop	Default
Last Hop Pool	None
Analytics Profile	None  Note: Changes you make might take up to 10 minutes to be reflected in the charts.
NAT64	Enabled
Request Logging Profile	None
Access Policy	
Access Profile	Wiki_Access 💌
Connectivity Profile	None 💌
Rewrite Profile	None
Citrix & Java Support	Enabled
OAM Support	Enabled



## 4.2 Configuration of SecurEnvoy

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

To Support Pre-Load and Real-Time SMS as well as Soft Tokens the following configuration is required.



### Click the "Radius" Button

Enter IP address and Shared secret for each F5® APM that wishes to use **SecurEnvoy** Two-Factor authentication.

NAS IP Address 10.0.10.11	Format xxx.xxx.xxx or default for undefined IP's
Shared Secret qwerty	
Authenticate Passcode Only (passw	rord or pin not required)
Handle all passcode types in the same w	ay as Real Time Codes 🗹 Access Challange All
Default Domain w2008.com 🗸	Allow these domains 🗹 w2008.com
	□ isa
	Select All Unselect All

Click checkbox "Handle all passcodes in the same way as Real Time"

Click "Update" to confirm settings.

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



## 4.3 Test Logon (SSL VPN)

Navigate to the relevant URL for the SSL VPN e.g. Https://remote.office.com

User enters their Domain UserID and password, Click  $\cent{``Logon''}$ 

6
Secure Logon for F5 Networks
Username
Password
Logon
<b>(5</b> )
Enter Your 6 Digit Passcode
Logon

User is then prompted for their 6 digit Passcode.

Click "Logon" to complete the logon.