

www.securenvoy.com

Checkpoint R80.10 Integration Guide

SecurAccess Integration Guide

Version 1.0 - 18/09/18



Checkpoint Integration Guide

Contents

1.1	SOLUTION SUMMARY	3
1.2	GUIDE USAGE	3
1.3	PREREQUISITES	3
1.4	AUTHENTICATION	4
1.41 1.42 1.42 1.42 1.45 1.46	SETUP RADIUS - SECURACCESS SETUP RADIUS - CHECKPOINT (WEB PORTAL) SETUP RADIUS - CHECKPOINT (SMART CONSOLE) SETUP LDAP - CHECKPOINT (SMART CONSOLE) VPN CLIENT - AUTHENTICATION POLICY MOBILE ACCESS - AUTHENTICATION POLICY CHECKPOINT ENDPOINT CLIENT.	4 7 9 11 13
1.5.	1 SECUREMOTE	14



1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Checkpoint's R80.10 Firewall through the use of RADIUS for group membership and access control.

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.
- It is expected that the Checkpoint device has been setup and is already working with LDAP authentication for VPN connectivity.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
 - Windows Server 2003 or higher.

Note: Please see SecurEnvoy's SecurAccess deployment guide on how to setup MFA server solution.

- A Checkpoint firewall appliance or virtual version GAIA R80.10 and above.
- Checkpoint Endpoint Protection client software E80.65 and above installed on all clients that
 connect remotely to the network unless the Clientless solution will be used.
- Familiarity with the following technologies:
 - RADIUS configuration
 - Checkpoint Smart Console



1.4 Authentication

The following section describes the steps required to configure the Checkpoint FW to authenticate users via RADIUS.

1.41 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the Checkpoint FW as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the IP address of the Checkpoint device and click "Add"

A Deschoor pic Company									
	Radius	Enable Radius Service Enter Network Port							
Domains		1.07a							
<mark>부핚</mark> Config									
Gateways	Add New Client								
Radius	192.168.200.59 Format: x000000000 Enter <i>default</i> for all addresses Add								
Se Users									

- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update

Checkpoint		
Shared Secret		

Authenticate passcode only	Password Checked by NAS	
Two Step (passcode on a separ	ate dialog) Required for One Swipe Push. Client must support Access Challenge	
Default Domain		



1.42 Setup RADIUS – Checkpoint (Web Portal)

Open a web browser and navigate to the IP or DNS address of your Checkpoint Firewall. On connection with web-based interface, login using your admin account.

	1 This system is for authorized use only.
Gaia Portal R80.10	Username: admin Password:

On access to the web portal, make sure View Mode is set to Advanced and navigate to Authentication Servers

44	User Management		
View mode: Advanced	oser Monagement - Authentication servers		
Toverview 🕜	RADIUS Servers		
ਭ 💑 Network Management	Add Edit Delete		
ਭ 🍄 System Management	Priority Host Address	UDP Port Timeout	
🗄 🚭 Advanced Routing	1 192.168.200.54	1812 3	
🖃 🤽 User Management			
🧟 Change My Password			
💁 Users 🏖 Roles	Network Access Server (NAS): eth0 : 192.168.200.60	~	
Password Policy	If no NAS IP Address was chosen, the IPv4 address that ma	tches the host name will be used by defa	
 System Groups GUI Clients High Availability Maintenance Upgrades (CPUSE) 	RADIUS Servers Advanced Configuration RADIUS Users Default Shell: /etc/dl.sh Super User UID: 96 96 • Image: Remote users with RADIUS attribute "Super User" will login Apply TACACS+ configuration Enable TACACS+ authentication Apply TACACS+ Servers Add Edit Delete Priority IP Address	with this UID.	



- From within the authentication servers section, click Add under RADIUS Servers to add the SecurEnvoy server.
- Add in the IP address of the SecurEnvoy server, add in the Shared Secret password configured previously and increase the Timeout in to 22 seconds.

Please Note: Select Network Access Server (NAS) interface that will be used to communicate to the SecurEnvoy Server

	RADIUS Serv	ers		
Q	Add	Edit Delete		
	Priority	Host Address	UDP Port	Timeout
	1	192.168.200.54	1812	22
	Edit RADIUS S	erver		×
	Priority:			1
	UDP Port:	1812		
	Shared Sec	et:		-1
	Set thi 50	s timeout, so that the sum of all RADIUS server timeo	uts is less thar	n l
	Timeout in	22		
			OK Ca	ncel



1.43 Setup RADIUS – Checkpoint (Smart Console)

From your Checkpoint SmartConsole Server or Client, login to the Checkpoint Firewall.



We will need to define a couple of Objects that are specific to the RADIUS and LDAP servers that we will use to check and authenticate the users.

From the Object Category list, select Servers and create a new RADIUS Server

Q Search ← ★ New ▼		Objects
Object Categories	38	Validatior
+ Services	518	SI
Applications/Categories	7509	
🗱 VPN Communities	2	
🔺 Data Types	62	
💵 Users	4	
Servers	3	
O Time Objects	3	
🞗 UserCheck Interactions	13	
 Limit 	4	





On presentation of the new RADIUS Server Object, complete the following details

Name: Give the Object a new name Host: Create a Host object that includes the IP address of the SecurAccess Server Service: Select NEW-RADIUS Shared Secret: Enter your shared secret as entered in the previous section Version: Select RADIUS Ver 2.0 Protocol: PAP

	RADIUS			Q 🖗 🛛	×
		ecurAccess nter Object Comment			
	General	General			
	Accounting	Host:	SLSA01.securlab.co	*	
		Service:	🚔 NEW-RADIUS	*	
1		Shared secret:	•••••		
		Version:	RADIUS Ver. 2.0	*	
		Protocol:	РАР	*	
		Priority:	1 *		
			ОК	ancel	



1.44 Setup LDAP – Checkpoint (Smart Console)

So that we do not require individual user accounts to be created on the Checkpoint appliance to match RADIUS authentications, we will create a connection to an LDAP server for the purpose of user matching.

From the Objects list, select LDAP Accounts Unit



On presentation of the LDAP dialogue box, configure and select the following items on the General tab.

Name: Provide to Server Object with a name Profile: Select Microsoft_AD Domain: Active Directory Domain Account Unit Usage: Make sure User Management and Active Directory Query are selected

 LDAP Account Unit Properties - Securlab-AD ? X	
General Servers Objects Management Authentication	
Name: Securlab-AD	
Color: Black V	
Profile: (Microsoft_AD v Domain: securlab.co	
Account Unit usage	
Active Directory Query	
Additional conliguration Enable Unicode support Active Directory SSO configuration	
OK Cancel	



Select the Servers Tab from the dialogue box and select Add to define the LDAP Server properties.

LDAP Account Unit Properties -	Securlab-AD	LDAP Server Properties ? X
General Servers Objects Manag	gement Authentication	General Encryption
LDAP Servers	ıls	Host Rew
Host	P Default pri Logi 636 1 CN=	L Username: administrator
		Login DN: CN=administrator,CN=Users,DC=securlab,I
		Password:
		Confirm password:
		Default priority: 1 🗘 (1 is highest)
		Check Point Gateways are allowed to:
		Read data from this server
Add Edit.	Remove	Write data to this server
		OK Cancel
	ОК	Cancel

Configure the following details to allow the Checkpoint appliance to query the LDAP server.

Host: Select or create a New Host (This is Domain Controller you with to query) Username: An administrator or system account that has rights to query AD Login DN: Enter the full Distinguished name Password: Enter Administrator or System account password

LDAP Server Properties	?	x
General Encryption		
Use Encryption (SSL) Encryption port 636 Verify that server has the follo	wing Fingerprints:	
F0:A5:D5:FA:B2:89:E6:28:65:D	DF:CF:2E:7A:F9:D1:84 Fetch	
Min/Max Encryption Strength:		
Min O Authentication	Max Authentication	
Export	CExport	
⊖ Strong	Strong	

If using SSL, select Use Encryption (SSL) from the Encryption tab and select OK to finish.



1.45 VPN Client – Authentication Policy

From the Checkpoint Smart Console, right click on the managed gateway and select Edit from the drop-down list.

Se -	😭 Objects 🔹	😍 In	stall Policy						
	Columns:	🖻 Gene	eral	*					
GATEWAYS	Status	Name		IP	Version	Active Blades	Hardware	CPU Usa	Recom
& SERVERS	0	6	SLCHFW	192.168.200.60	R80.10	III 🕸 🗢 🔡	Open server	5%	3 update
===		s	Scripts	· · ·					
SECURITY		đ	Actions	•					
POLICIES		0	Monitor						
~		0	View						
LOGS & MONITOR			Edit	>					
. بىلىر.		ſ,	Clone						
÷.		×	Delete						
SETTINGS		<u> </u>	Where U	lsed					
			Сору То	Clipboard					
			Copy As	Image					

In order to complete the RADIUS configuration, an authentication server needs to be assigned to the VPN client and Mobile Access policy.

From the VPN Clients\Authentication section, select Add to define a RADIUS server profile

General Properties	Compatibility with Older clients				
 Network Management 	8 For a list of clients supporting single authentication option only, please see sk111583				
- HTTPS Inspection	Allow older clients to connect to this gateway				
Platform Portal	Authentication Method: Defined On User Record (Legacy)	Settings			
IPSec VPN					
- Link Selection	Multiple Authentication Clients Settings				
VPN Advanced	For a list of newer clients that support Multiple Login Options, see sk111583				
- VPN Clients	· · · · · · · · · · · · · · · · · · ·				
Office Mode	+ Add) Edit X Remove 👚 Up 🐥 Down				
Remote Access	Display O Display Name Authentication Factors				
Mobile Access	1 Radius-MFA RADIUS				
Authentication					
Office Mode					
- Portal Customizatio					
- SSL Clients					
- HTTP Proxy					
- Name Resolution					
- Link Translation					
- Endpoint Complian					
Check Point Secure					
Capsule Workspace					
- Logs					
Hit Count					
Other	DynamicID Settings				
	✓ Use Global Settings (Under "Authentication to Gateway" on the Mobile Access tab)				
	Edit				



Create a name for the new RADIUS Server and select Add to define the configuration details of the server.

Multiple Login Options	7 X
Login Option	Login Option
	General Properties
	Name: Radius-MFA Color: Olive
	Comment:
	Display Name: Radius-MFA
	Authentication Methods Personal Certificate" can only be used as a first suthentication method. Tynamic D" can not be used as a first suthentication method. + Add
	1 RADIUS
	Authentication Factor 7 X
	Authentication Factors Personal Certificate Personal Certificat
	OK Cancel

Configure the authentication factor as RADIUS and select the Server created previously under the Checkpoint objects section

On selecting the User Directories tab, make sure the following areas of configured as per the above config.



1.46 Mobile Access – Authentication Policy

In order to complete the RADIUS configuration for the Mobile Access Policy, an authentication server needs to be assigned.

From the Mobile Access \Authentication section, select Add to define a RADIUS server profile and select the previously configured RADIUS profile.

	Compatibility with Older clients				
Network Management	: B For a list of clients suppor	ting single authentication option only please see sk111583			
HTTPS Inspection					
HTTP/HTTPS Proxy	Allow older clients to conr	nect to this gateway			
- Platform Portal	Authentication Method:	Username and Password			
IPSec VPN	Mobilo dovisos do pot rov	quiro a Porconal Cortificato	Settings		
VPIN Clients	Mobile devices do not rec	quire a Personal Certificate.			
Authentication	Multiple Authentication Clients Se	ettings			
Office Mode					
Portal Customizatic	For a list of newer clients	that support Multiple Login Options, see sk111583			
Portal Settings					
HTTP Provy	+ Add S Edit X Rei	move 👕 Up 🧇 Down			
Name Resolution	Display O Display Name	Authentication Factors			
Link Translation	1 Radius-MFA	RADIUS			
- Endpoint Complian					
Capsule Workspace	é				
Optimizations					
- Hit Count					
	DynamicID Settings ————				
	DynamicID Settings	Jer "Authentication to Gateway" on the Mobile Access tab)			
	DynamicID Settings	Jer "Authentication to Gateway" on the Mobile Access tab)			
	DynamicID Settings ✓ Use Global Settings (Und Edit	Jer "Authentication to Gateway" on the Mobile Access tab)			
	DynamicID Settings ✓ Use Global Settings (Und Edit	der "Authentication to Gateway" on the Mobile Access tab)			
	DynamicID Settings	der "Authentication to Gateway" on the Mobile Access tab)			
< 111 >	DynamicID Settings	Jer "Authentication to Gateway" on the Mobile Access tab)			



1.5 Checkpoint Endpoint Client

The following section describes steps required to configure the Checkpoint Endpoint client to authenticate with SecurEnvoy's MFA solution.

1.5.1 SecuRemote

- Run the Checkpoint Endpoint Client and change the Login Option Settings.
- Make sure you select the RADIUS profile you configured in the previous section.

😚 Properties of checkpoint.securlab.co 🛛 🗙	🔒 TrGUI	- 🗆 X
Details Settings Authentication	SecuRemote [.]	
Please select your preferred login option from the following list	Site: checkpoint.securlab.co	*
Radius-MFA (Default)	Authentication	
	Please provide user name and password to authenticat User name dclare-enrol Password •••••••	
Import Renew Enroll OK Cancel Help	Connect Cancel Help Selected Login Option: Radius-MFA	Change Login Option Settings

Click Connect to establish a connection to the Checkpoint firewall. Dependent on the SecurEnvoy Token type selected by the user, the login screen will present different views

PUSH Notifications

Please Reach Out to Your Local <u>SecurEnvoy T</u>eam...



UK & IRELAND

The Square, Basing View Basingstoke, Hampshire RG21 4EB, UK

Sales

- E sales@SecurEnvoy.com
- T 44 (0) 845 2600011

Technical Support

- E support@SecurEnvoy.com
- T 44 (0) 845 2600012



EUROPE

Freibadstraße 30, 81543 München, Germany

General Information

E info@SecurEnvoy.com T +49 89 70074522



ASIA-PAC

Level 40 100 Miller Street North Sydney NSW 2060

Sales

- E info@SecurEnvoy.com
- T +612 9911 7778



USA - West Coast

Mission Valley Business Center 8880 Rio San Diego Drive 8th Floor San Diego CA 92108

General Information

- E info@SecurEnvoy.com
- T (866)777-6211



USA - Mid West

3333 Warrenville Rd Suite #200 Lisle, IL 60532

General Information

E info@SecurEnvoy.com T (866)777-6211



USA – East Coast

373 Park Ave South New York, NY 10016

General Information

E info@SecurEnvoy.com T (866)777-6211



www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010 Company No. 04866711 VAT Number GB 862076128