External Authentication with Checkpoint® R77.20

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	

Checkpoint R77.20 Integration Guide

This document describes how to integrate a Checkpoint® R75.40 with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Checkpoint® R75.40 provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Checkpoint® R75.40) 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, whereas the Checkpoint® R77.20 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:

Checkpoint®
Checkpoint R77.30

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 v7.3.501

Index

External Authentication with Checkpoint® R77.20 1
Authenticating Users Using SecurAccess Server by SecurEnvoy 1
1.0 Pre Requisites 3
1.1 Configuration of Checkpoint R77.20® 4
2.0 Configuration of SecurEnvoy 7
3.0 Test Logon 9

1.0 Pre Requisites

It is assumed that the Checkpoint R77.20® Checkpoint R77.20® has been installed and basic configuration carried out. A user can connect by authenticating with their Microsoft AD Domain username and password. (This could be configured for any username and password authentication server)

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Checkpoint R77.20®, additional open ports will be required.

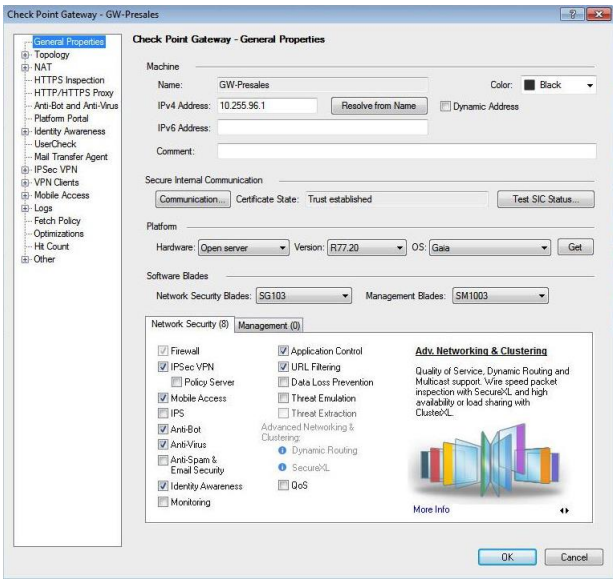
***NOTE:** Add radius profiles for each Checkpoint R77.20® that requires Two-Factor Authentication.*

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✗

1.1 Configuration of Checkpoint R77.20®

Launch the Checkpoint® R77.20 admin interface through the Smart dashboard GUI.

Verify that the Check Point firewall is currently VPN "Enabled"
Go to "Network Objects" "Checkpoint" and selecting the Checkpoint firewall you wish to configure. "Properties"



The next step is to add the SecurEnvoy RADIUS Server as a host object, define it as a valid machine on the network.

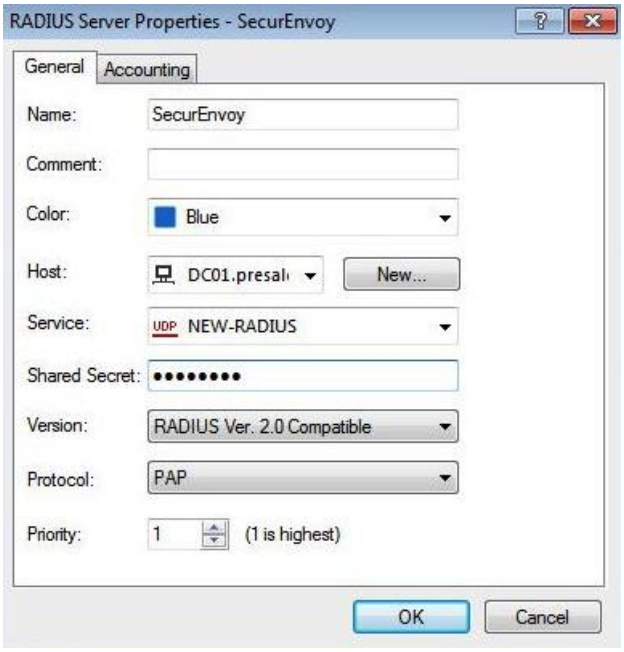
Go to "Network Objects" "Right-Click" Node _ New node to add.
Populate the required information.

Click OK to Save.

Under the "Servers and OPSEC Applications" tab

Select "Radius" _ New RADIUS… and then add in the new RADIUS server details.
Select the "SecurEnvoy-Radius" host you created earlier, set the Service type to use "udp NEW-RADIUS", and specify the common "Shared Secret" key to be used.

(The "Share Secret" key is configured on both the Check Point firewall and SecurEnvoy RADIUS Server). Make sure the Protocol type is set to "PAP".



The SecurEnvoy RADIUS Server is configured by default to communicate on Port 1812, using Protocol UDP.

Under the "Service" tab, select "UDP" as the Protocol type, and browse to "New-RADIUS". Make sure that it is set to "Port 1812".

For Version select RADIUS Ver 2.0
On the properties of "New-RADIUS",

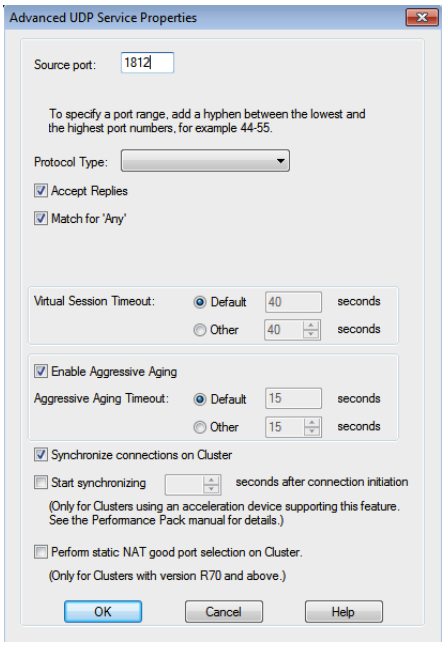
Click Ok to save.

Select the "Advanced…" tab and make sure that the Source port is set to "1812".

Also make sure that the "Accept Replies" check-box has been enabled.

See diagram.

Click OK to Save.



NOTE

There are many ways of setting up VPN users in Checkpoint. Configuration can be set to authenticate users by various methods, Users can be setup and authenticated directly upon Checkpoint, they can be setup as LDAP users and authenticate against Microsoft Active Directory, or can be authenticated against RADIUS.

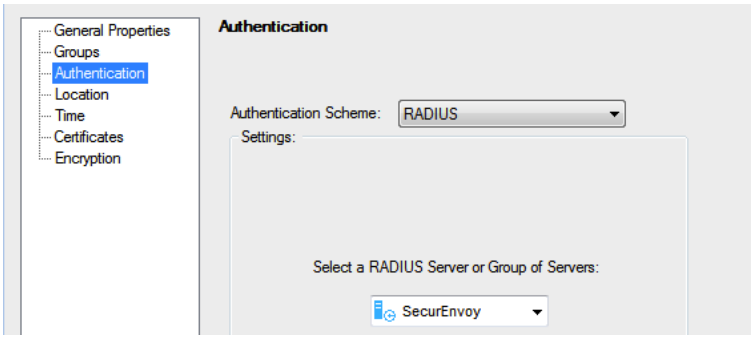
In this example, we are going to configure Checkpoint to authenticate all external users to the SecurEnvoy RADIUS Server.

An External User Profile will be created that mandates RADIUS Authentication for all users that do not have a Check Point user account.
The Match all users profile with the profile name generic* is limited to only one property set. Checkpoint applies the restrictions specified for an ordinary user in the User Properties tabs (for example Groups).
For authentication purposes Check Point uses the name typed in by the user instead of generic*.

The following steps describe the process to configure an External Profile of "Match All Users".

Go to **Manage > Users and Administrators > New > External User Profile > Match All Users**

The user generic* is created and a new window opens.
Select Authentication from the left tool bar.
Select RADIUS from the drop down box, as the user's Authentication Scheme.

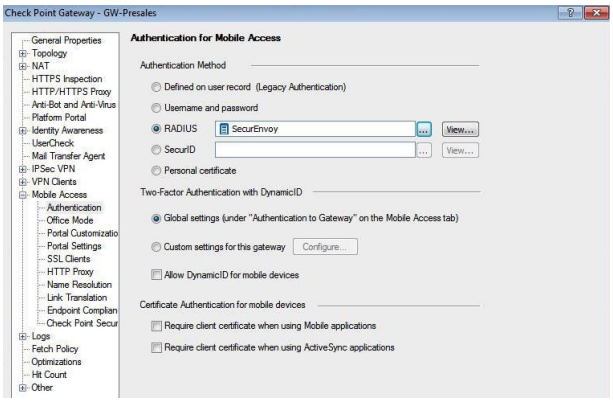


Click OK to save changes.

Go to **Mobile Access > Authentication > Allowed Authentication schemes on Gateways**

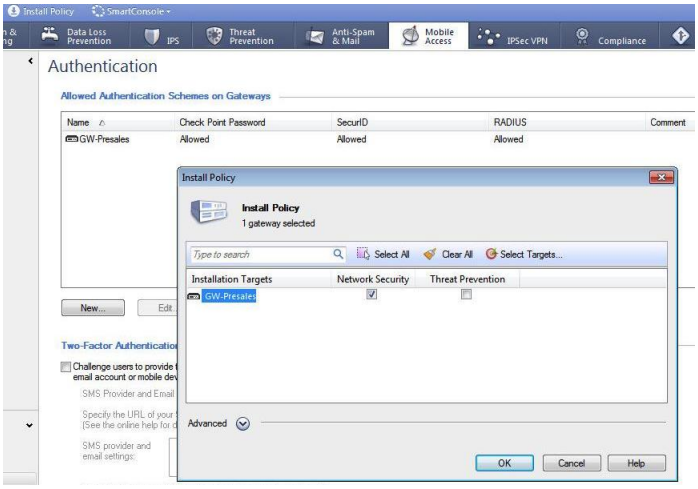
Select an existing scheme to modify or create a new one. In this example an existing scheme was utilised.

Select RADIUS and then set to use SecurEnvoy (Network Object).



Click OK to save changes.

Once complete then select "Install Policy" from the Top toolbar.



2.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent or generated upon the user's mobile phone.

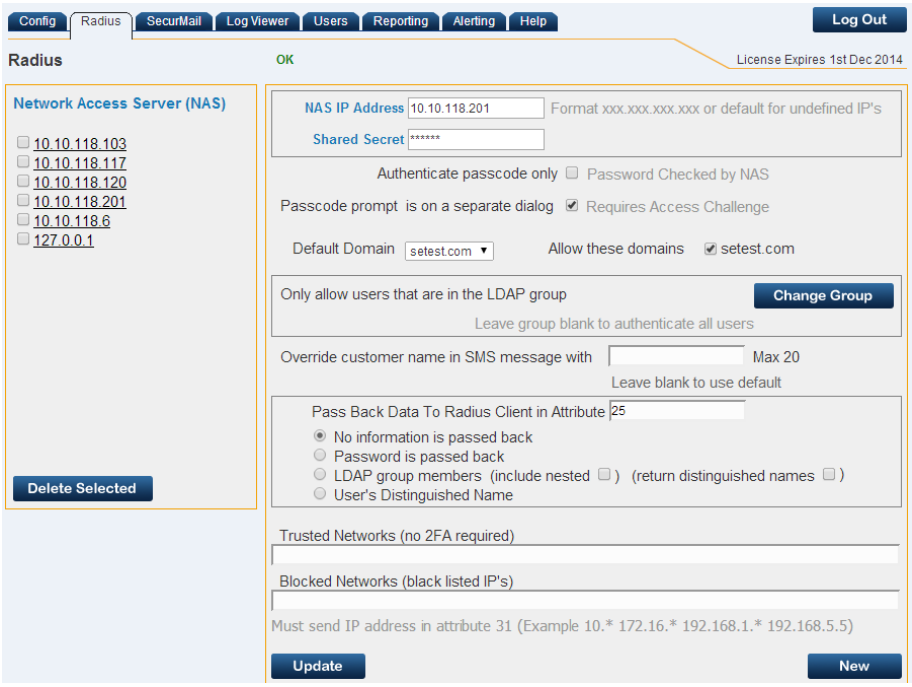
Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** tab

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

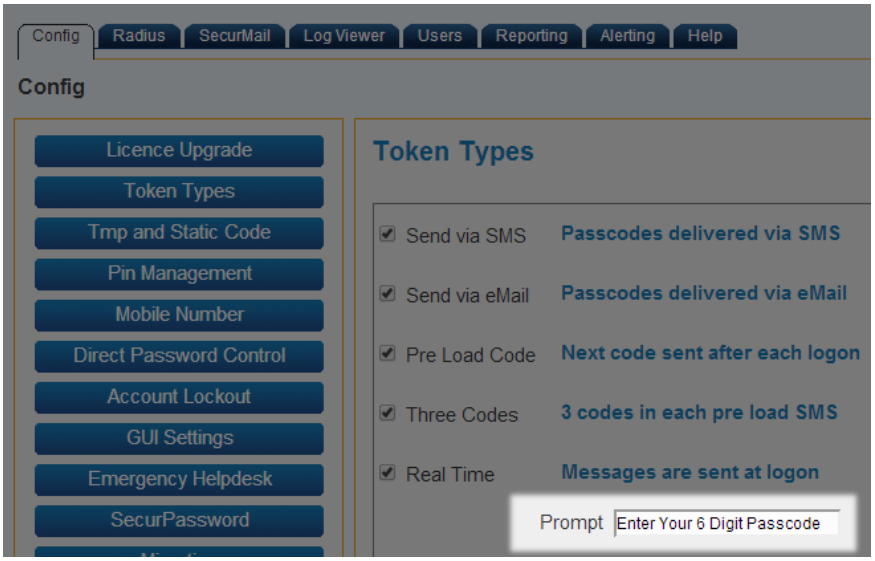
Click checkbox "Passcode prompt is on a separate dialog".

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



Navigate to SecurEnvoy GUI Config setting "Token Types" Prompt:

Set the prompt for the challenge –response message to the user. By default this is: "Enter your 6 digit Passcode"



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

3.0 Test Logon

Browse to the web URL address of the Checkpoint R77.30® SSL

Two input dialogue boxes will be displayed.

User will enter: UserID in the Username box
Microsoft AD Domain password in password box



Enter SMS /Email Passcode in the SecurEnvoy Passcode box (received via SMS /Email upon your mobile phone)
Or enter the passcode displayed upon the SecurEnvoy Soft Token application.

