

External Authentication with Checkpoint UTM-1 Edge 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	

1 Contents

1	Contents	2
2	Checkpoint UTM-1 Edge Integration Guide	3
3	Pre Requisites.....	4
4	Tokenless Authentication (All Types).....	4
4.1	Configuration of Checkpoint® UTM-1 Edge	4
4.2	Configuration of SecurEnvoy	5
4.3	Test Logon (SSL VPN).....	6
4.4	Test Logon.....	6

2 Checkpoint UTM-1 Edge Integration Guide

This document describes how to integrate a Checkpoint® UTM-1 Edge with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Checkpoint® UTM-1 Edge provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Checkpoint® UTM-1 Edge) 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® UTM-1 Edge 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 UTM-1 Edge

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 Checkpoint® UTM-1 Edge 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 Checkpoint® UTM-1 Edge, 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 Checkpoint® .

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 Checkpoint® UTM-1 Edge supports RADIUS (Challenge Response). Configuration in this guide refers to this type of approach.

4 Tokenless Authentication (All Types)

4.1 Configuration of Checkpoint® UTM-1 Edge

Launch the Checkpoint® UTM-1 Edge admin interface through the management GUI.

The Checkpoint® UTM-1 Edge device will check the RADIUS server for any user accounts that are not declared on the device.

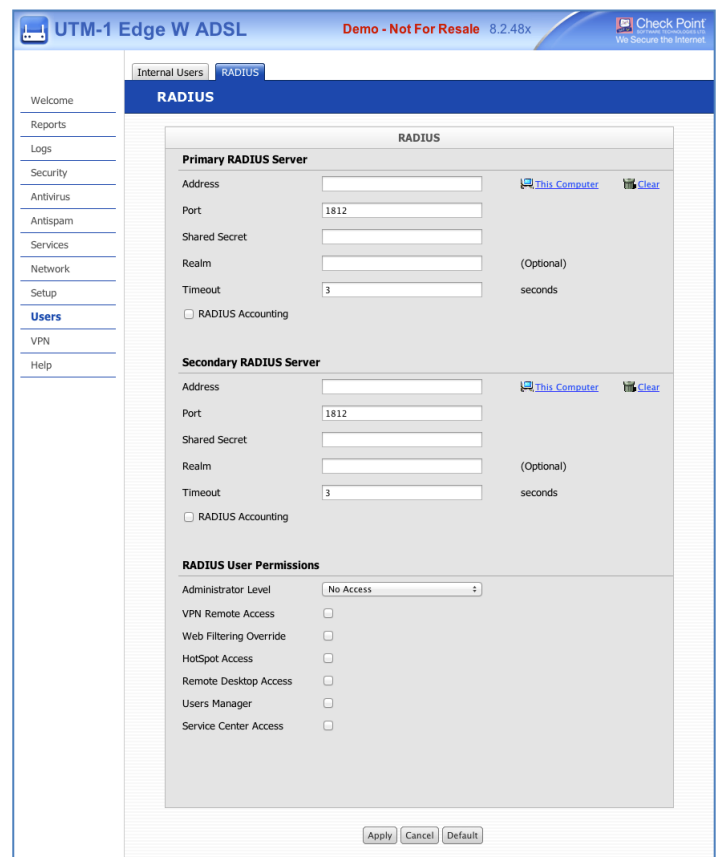
For further information on CheckPoint RADIUS setup, please see CheckPoint online help.

Navigate to Users, and then select the RADIUS Tab

Enter the SecurEnvoy server address, port and shared secret information.

(A Backup SecurEnvoy server can also be configured)

Click "Apply" when complete.



The screenshot shows the 'RADIUS' configuration page in the Checkpoint UTM-1 Edge admin interface. The page is titled 'RADIUS' and contains the following sections:

- Primary RADIUS Server:**
 - Address: [Text Field] [This Computer] [Clear]
 - Port: 1812
 - Shared Secret: [Text Field]
 - Realm: [Text Field] (Optional)
 - Timeout: 3 seconds
 - RADIUS Accounting
- Secondary RADIUS Server:**
 - Address: [Text Field] [This Computer] [Clear]
 - Port: 1812
 - Shared Secret: [Text Field]
 - Realm: [Text Field] (Optional)
 - Timeout: 3 seconds
 - RADIUS Accounting
- RADIUS User Permissions:**
 - Administrator Level: [No Access]
 - VPN Remote Access:
 - Web Filtering Override:
 - HotSpot Access:
 - Remote Desktop Access:
 - Users Manager:
 - Service Center Access:

At the bottom of the page, there are buttons for 'Apply', 'Cancel', and 'Default'.

4.2 Configuration of SecurEnvoy

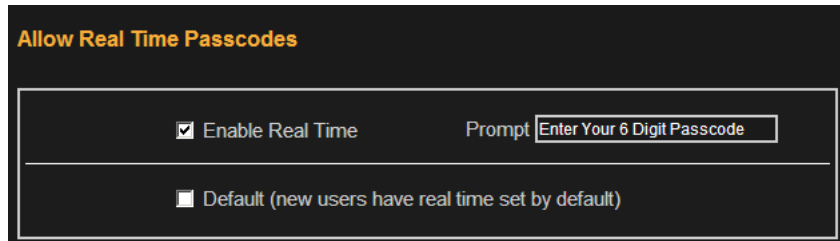
Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

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

Go to Config-Real Time Passcodes

Enable the checkbox

Click Update to complete



Allow Real Time Passcodes

Enable Real Time Prompt

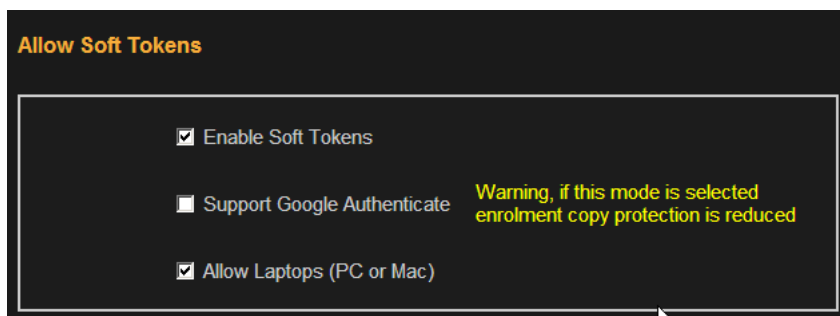
Default (new users have real time set by default)

Go to Config-Soft Tokens

Enable Soft Tokens

Enable PC Soft Tokens (If Required)

Click Update to complete



Allow Soft Tokens

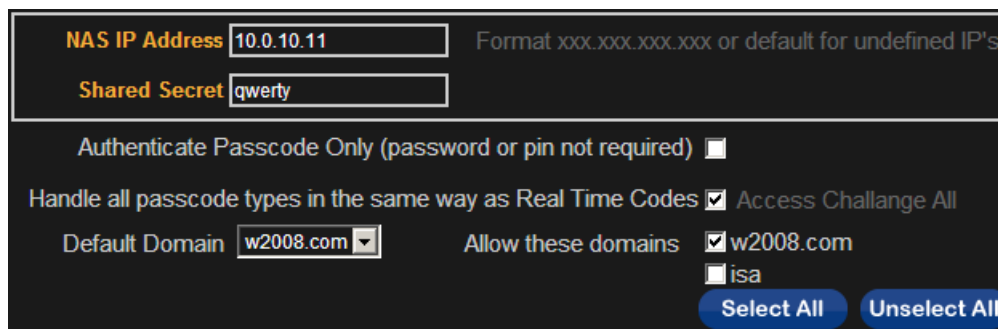
Enable Soft Tokens

Support Google Authenticate **Warning, if this mode is selected enrolment copy protection is reduced**

Allow Laptops (PC or Mac)

Click the **"Radius"** Button

Enter IP address and Shared secret for each Checkpoint®R75.40 that wishes to use **SecurEnvoy** Two-Factor authentication.



NAS IP Address Format xxx.xxx.xxx.xxx or default for undefined IP's

Shared Secret

Authenticate Passcode Only (password or pin not required)

Handle all passcode types in the same way as Real Time Codes Access Challenge All

Default Domain Allow these domains w2008.com isa

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

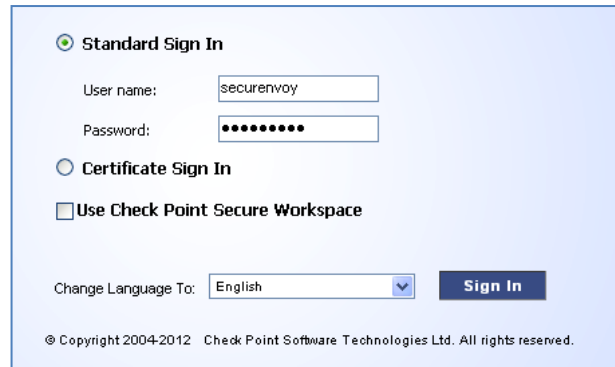
Click **"Update"** to confirm settings.

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](https://remote.office.com)

User enters their Domain UserID and password, click "Sign In"



Standard Sign In

User name:

Password:

Certificate Sign In

Use Check Point Secure Workspace

Change Language To:

© Copyright 2004-2012 Check Point Software Technologies Ltd. All rights reserved.

User is then prompted for their 6 digit Passcode.

Click "Submit" to complete the logon.



Enter Your 6 Digit Passcode

© Copyright 2004-2012 Check Point Software Technologies Ltd. All rights reserved.

4.4 Test Logon

User launches the Endpoint VPN Client.

User enters their Domain UserID and password then clicks "Connect"



Check Point Endpoint Security

ENDPOINT SECURITY

Check Point SOFTWARE TECHNOLOGIES LTD.

Site:

Authentication

Username:

Password:

User is then prompted for their 6 digit Passcode.

Click "Connect" to complete the logon



Check Point Endpoint Security

ENDPOINT SECURITY

Check Point SOFTWARE TECHNOLOGIES LTD.

Site:

Authentication

Username:

Prompt: Enter Your 6 Digit Passcode

Response: