# Checkpoint Mobile Access Blade Integration

## Contents



# Overview

Swivel can provide strong and two factor authentication to the Check Point Mobile Access Blade. This document outlines the details required to carry this out.

# Baseline

Swivel 3.x

Check Point CR75 Mobile Access Blade and newer

# Prerequisites

Working Mobile Access Blade VPN

Swivel 3.x

Use of the TURing, will require the use of a NAT.

When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

# Downloads

Customised login page

# Demos

| TURing | SMS | Mobile App. |
|---|---|---|
| | | |
| Check Point MAB & Swivel TURing | Check Point MAB & Swivel SMS | Check Point MAB & Swivel Mobile App. |

# Swivel Configuration

## Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

## Enabling Session creation with username

To allow the TURing image, PINpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

### Setting up Swivel Dual Channel Transports

See Transport Configuration

# Mobile Access Blade Configuration

## Enabling RADIUS Authentication in Mobile Access Blade

You need to configure Swivel as an authentication server on the Mobile Access Blade

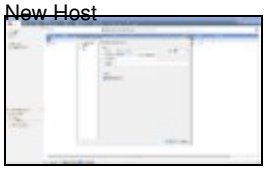
- Open Smart Dashboard and log in.
- Under Servers and OPSEC, locate the RADIUS folder and right click and select New RADIUS
- In the New RADIUS popup window click on 'New'
- Configure the Swivel server as a new host. You just need to give it a name and add the IP address.
- Select Swivel as the host, ?NEW-RADIUS? as the service, and enter the shared secret you previously set on the Swivel appliance. You can select RADIUS version 1 or 2, and PAP or MSChap as the protocol: Swivel will detect these protocols automatically. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

- 

New RADIUS

- 

New Host

- 

Configure New Host

- 

RADIUS Server Properties

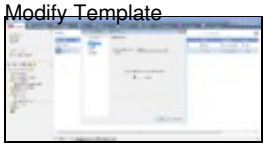
## Configuring AD Templates to use RADIUS

- Modify AD user template and select RADIUS.

Don?t forget to save and install the policy once you have made all relevant changes.

- 

Modify Template

- 

Select RADIUS

## Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

# Customising the Mobile Access Blade Login Page

## Modify custom LoginPage.php

Download the provided LoginPage.php

Modify the PHP file, and change the URL values to the site location (search for TURing)

## Connect to the Check Point Appliance

Use WinSCP to connect to the Check Point Appliance, and retrieve a copy and keep safe keeping of the login page (LoginPage.php) from:

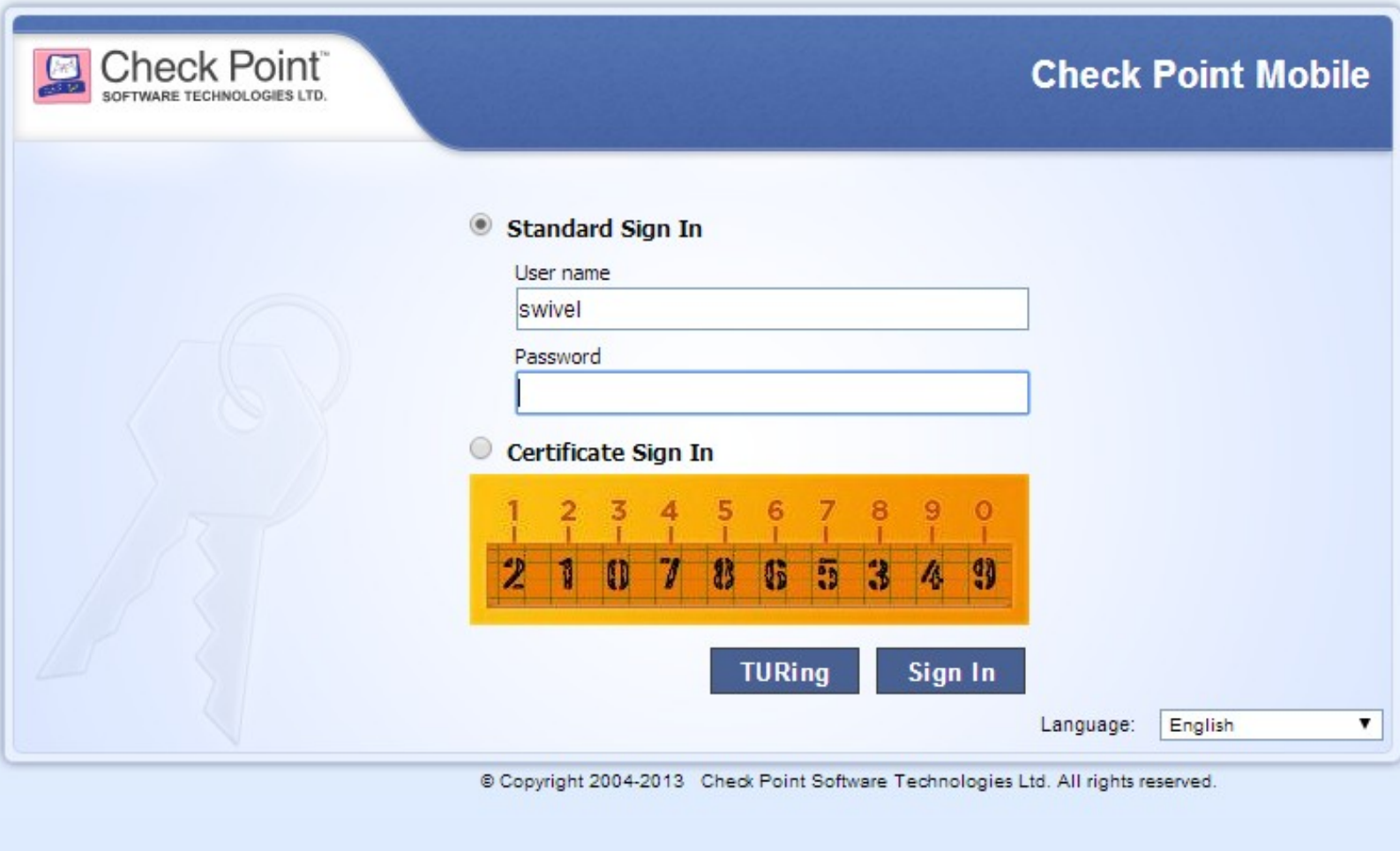
/opt/CPcvpn-R77/phpincs (note: the exact directory name CPcvpn-R** will vary depending on the Mobile Access Blade revision number).

## Upload new Login Page

Use WinSCP to upload a copy of the provided LoginPage.php to the appliance.

# Testing

With the changes in place, when a user accesses the Connectra portal the will see the modified login page.




After entering their username and either tabbing away from the username field of clicking the TURing button they will be presented with a TURing image.

The Swivel log should record a session start for that user.

The user can then use their PIN to extract their one-time code and enter this to authenticate. The Swivel log show record the RADIUS dialogue associated with this authentication.

## Troubleshooting

Check the Swivel logs for TURing images and RADIUS requests.

Image from PINsafe server absent

## Known Issues and Limitations