

Establishing two-factor authentication with Barracuda NG Firewall and HOTPin authentication server from Celestix Networks

Contact Information

www.celestix.com

info@celestix.com

Celestix Networks USA	3125 Skyway Court, Fremont, California, 94539, USA	+1 510 668 0700
Celestix Networks EMEA	30 Queens Road, Reading, RG1 4AU, United Kingdom	+44 (0)118 959 6198
Celestix Networks APAC	1 Changi North Street 1, #02-02, Singapore 498789	+65 6781 0700

Integration completed by

Kimberley Wong Kwan Lun

klun@celestix.com

This document outlines the steps required to integrate the Barracuda NG Firewall F200 with Celestix HOTPin two-factor authentication. The following steps are detailed within this guide:

- Adding users
- Enabling user self provisioning
- Configuring RADIUS integration in Barracuda
- Adding Barracuda as a RADIUS client in Celestix HOTPin
- Testing the login process

Steps to Configure Standalone Celestix HOTPin v3.5

Prerequisites

This document assumes you have followed the steps in the HOTPin Quick Start Guide, and either installed HOTPin Server v3.5, or configured your HSA Appliance ready for use. If you haven't already done so, please refer to the Quick Start Guide to complete this before proceeding.

The Quick Start Guide can be found here: <http://www.celestix.com/hotpin-tl.html>

Step 1: Launch HOTPin Administration

Launch the HOTPin Management GUI using the shortcut icon on the desktop. This will load the default web browser. HOTPin ships with a default certificate to provide HTTPS security. The browser will display a certificate security warning, this is normal, choose **“Continue to this website.”**

Microsoft Windows User Access Control will prompt for a username and password. Enter the administrator credentials.

NOTE - depending on the web browser and the default settings, the message might be slightly different.

Step 2: Adding users

To add users go to **HOTPin > Users**.

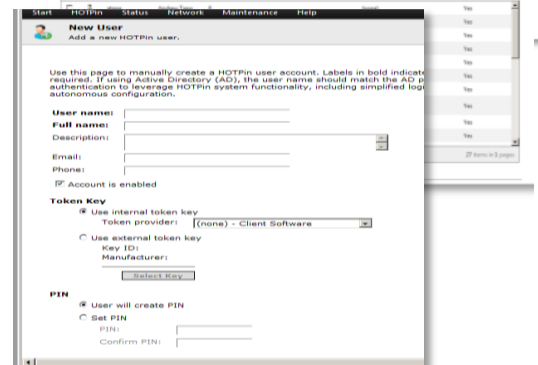
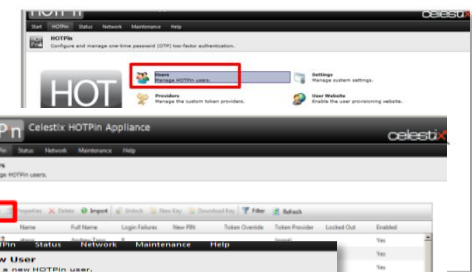
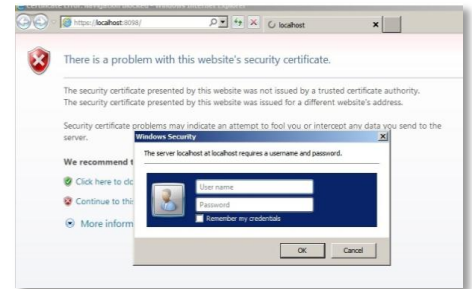
For now we'll just add one user.

Click on **'New.'** Complete the user settings for an end user.

Token Key: (none) – Client Software (default)

PIN: User will create PIN

For production and full installation we recommend you make use of the Active Directory import feature within HOTPin, and then enable Active Directory Synchronization. This can be achieved easily and simply through the main Management GUI.



Step 3: Configure the user provisioning website

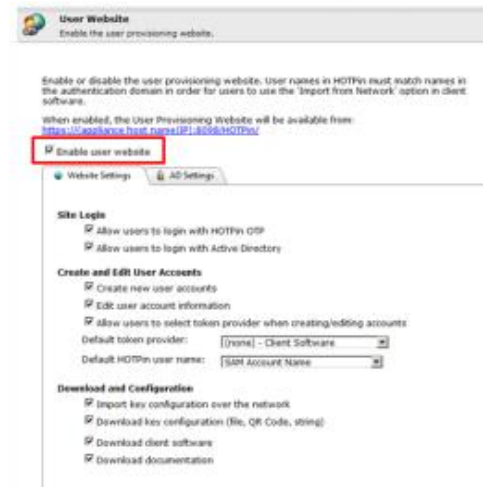
From the main Management GUI, go to **User Website** and tick the **Enable user website** box.

This will allow your users to provision a variety of tokens by accessing a user provisioning portal, but it is important to configure this in advance of giving access.

Once enabled, default access to the site is: [https://\(appliancehostname|IP\):8098/hotpin/](https://(appliancehostname|IP):8098/hotpin/)

This site is not enabled by default; it must be turned on by Administrators.

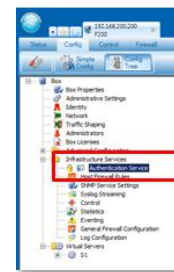
At this point, the basic configuration for Celestix HOTPin is complete, and we'll return to the User Provisioning Website later.



Configure RADIUS integration in Barracuda

Step 4: Add Authentication Server

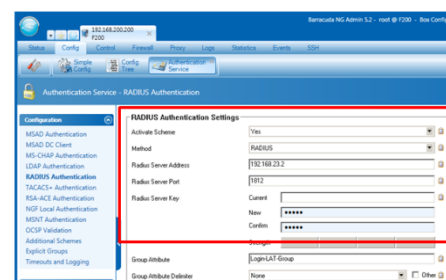
Go to **Config > Full Config > Infrastructure Services > Authentication Service > RADIUS Authentication > RADIUS Authentication Settings**.



- Select **Lock** to make changes.



- Select Yes as **Activate Scheme**.
- Select **RADIUS** as **Method**.
- Enter **Radius Server Address** of HOTPin server.
- Set **Radius Server Port** to 1812.
- Enter **Radius Server Key**.
- Enter **Group Attribute**.



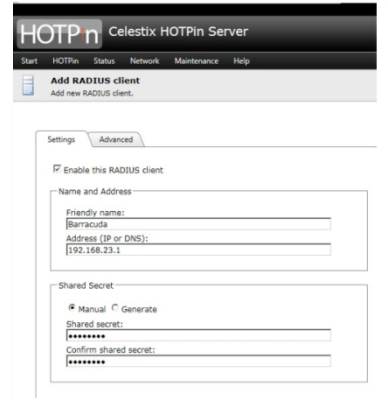
- Click on **Send Changes > Activate > Choose Yes**.



Step 5: Enabling RADIUS client on Celestix HOTPin

Go to **HOTPin > NPS Radius > RADIUS clients > New**.
 Tick **Enable this RADIUS client**.
 Enter name and IP address of the Barracuda box.
 Apply shared secret.

This completes the integration process.
 Next we'll test the login process.



Testing the login process

Celestix HOTPin supports the following platforms for generating a one-time password.

For testing purposes we recommend you use your smartphone, you can search the HOTPin app in your respective app store.

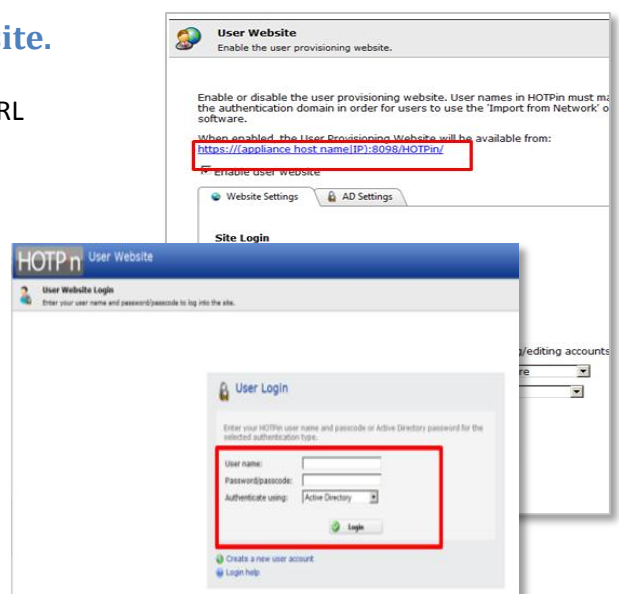
- Microsoft Windows
- MacOS
- iOS devices (iPhones and iPads)
- Android devices
- Windows phone devices
- Blackberry device



Step 6: Log on to end user provisioning website.

Go to User Website and click on the link for example this URL
[https://\(appliancehostname|IP\):8098/hotpin/](https://(appliancehostname|IP):8098/hotpin/)

After you have downloaded the HOTPin app to your Smart Device, log on to the end user provisioning site with your Active Directory credentials.



Step 7: Create Token Key

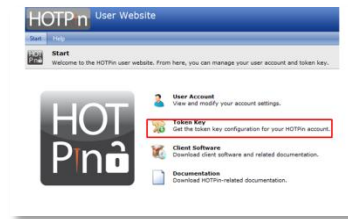
Go to **Token Key > QR Code**.

Enter QR code passphrase: Create a passphrase of at least 6 characters.

Confirm passphrase.

Code size: Select the image size.

Generate QR Code: Click to create the image.



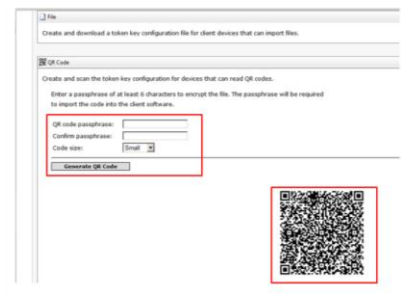
Open the app on your smart device.

Choose **Import from QR Code**.

Scan the QR Code.

Enter the **passphrase**.

Click on **Import** (iPhone) or **OK** with Android).



You are now able to generate a one time password.

This completes the device provisioning process.

Further Help

For further help, go to <http://www.celestix.com>