

# Configuring the Celestix MSA Series Security Appliance Web Publishing with HOTPin

## Contact Information

[www.celestix.com](http://www.celestix.com)

[info@celestix.com](mailto:info@celestix.com)

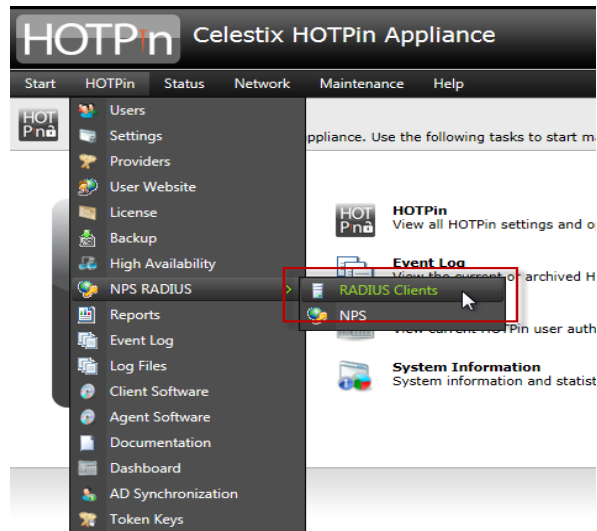
Celestix Networks USA	3125 Skyway Court, Fremont, California, 94539, USA	+1 510 668 0700
Celestix Networks EMEA	54 London Street, Reading, RG1 4QS, United Kingdom	+44 (0)118 959 6198
Celestix Networks APAC	1 Changi North Street 1, #02-02, Singapore 498789	+65 6781 0700

## Integration completed by

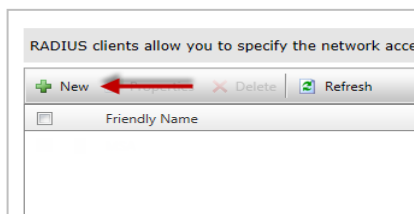
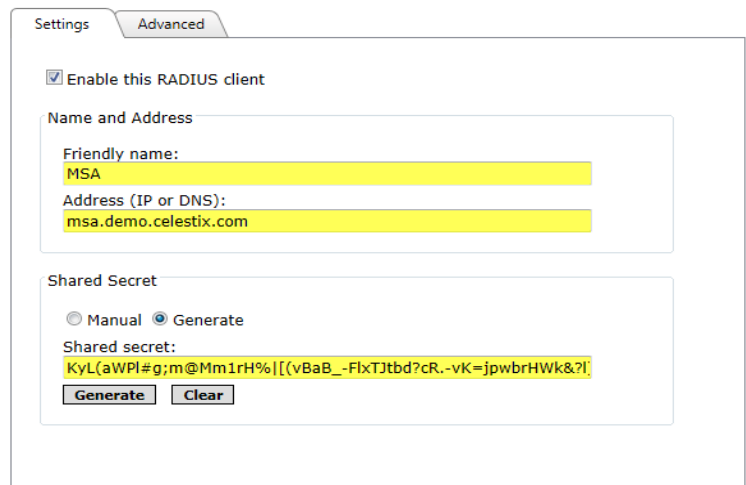
Richard Hicks

[rhicks@celestix.com](mailto:rhicks@celestix.com)

1. In the HOTPin web interface, click **HOTPin**, choose **NPS RADIUS**, then select **RADIUS Clients**



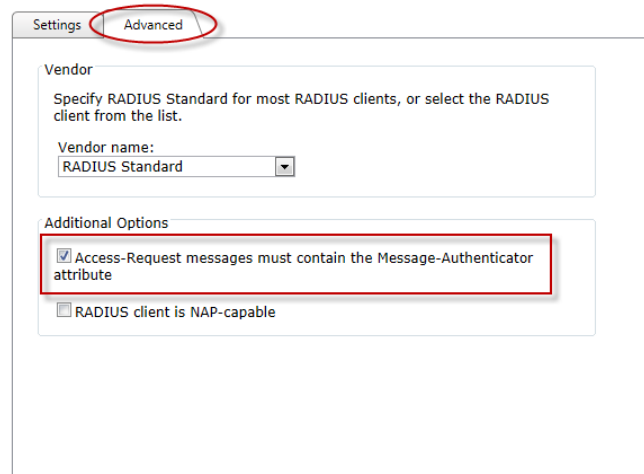
2. Click **New**, then enter a **Friendly name** and **Address** for the Celestix MSA. Specify a **Shared Secret** or choose the option to generate one automatically. Copy this string for use later on the MSA.

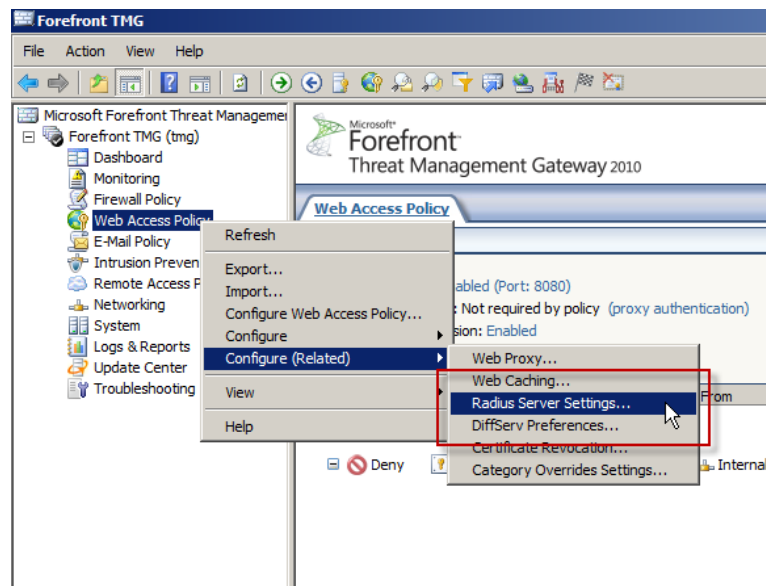
The screenshot shows the 'Advanced' settings page for a RADIUS client. The page is titled 'Settings' and 'Advanced'. It contains the following fields and options:

- Enable this RADIUS client
- Name and Address**
  - Friendly name:
  - Address (IP or DNS):
- Shared Secret**
  - Manual  Generate
  - Shared secret:
  -

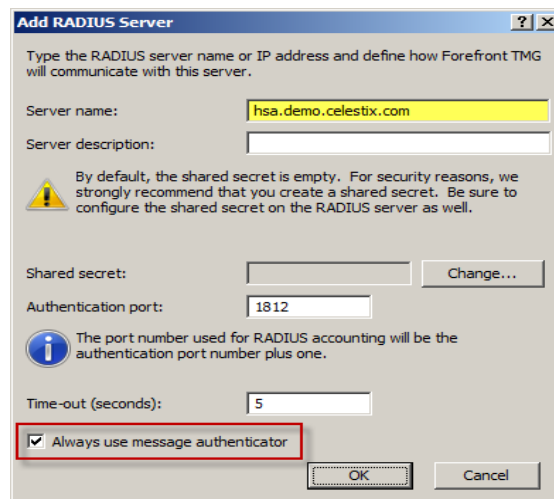
3. Click the **Advanced** tab and select the option **Access-Request messages must contain the Message-Authenticator attribute**.



4. In the Forefront TMG 2010 management console, right-click **Web Access Policy** in the navigation tree, choose **Configure (Related)**, then select **Radius Server Settings**.



- Click **Add**, then enter the hostname or IP address of the HOTPin server and optionally provide a description for this server. Click the **Change** button and enter the share secret specified on the HOTPin server. Leave the **Authentication port** set to its default port (1812) and the **Time-out (seconds)** set to its default (5). Select the option to **Always use message authenticator** and then click **Ok** twice.



**Add RADIUS Server**

Type the RADIUS server name or IP address and define how Forefront TMG will communicate with this server.

Server name:

Server description:

By default, the shared secret is empty. For security reasons, we strongly recommend that you create a shared secret. Be sure to configure the shared secret on the RADIUS server as well.

Shared secret:

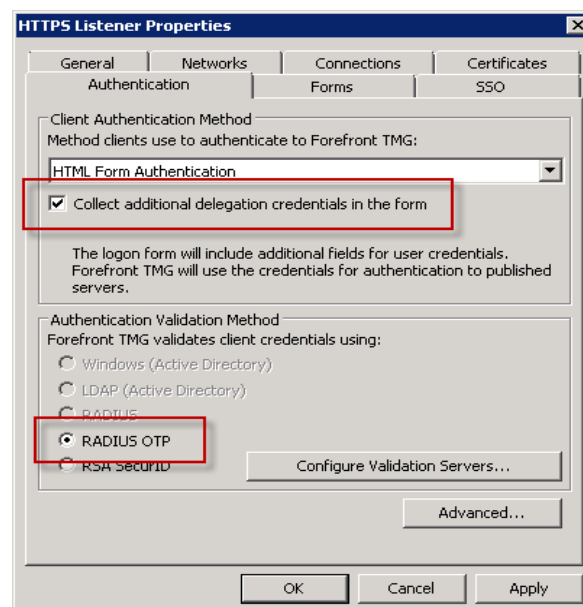
Authentication port:

The port number used for RADIUS accounting will be the authentication port number plus one.

Time-out (seconds):

Always use message authenticator

- Highlight the **Firewall Policy** node in the navigation tree, then select the **Toolbox** tab, expand **Web Listeners**, then double-click the appropriate HTTPS web listener. Select the option to **Collect additional delegation credentials in the form**, and then choose **RADIUS OTP** for the **Authentication Validation Method**.



**HTTPS Listener Properties**

General | Networks | Connections | Certificates

Authentication | Forms | SSO

Client Authentication Method  
Method clients use to authenticate to Forefront TMG:

Collect additional delegation credentials in the form

The logon form will include additional fields for user credentials. Forefront TMG will use the credentials for authentication to published servers.

Authentication Validation Method  
Forefront TMG validates client credentials using:  
 Windows (Active Directory)  
 LDAP (Active Directory)  
 RADIUS  
 RADIUS OTP  
 RSA SecurID