

Configuring the Celestix MSA Series Security Appliance Remote Access VPN with HOTPin

Contact Information

www.celestix.com

info@celestix.com

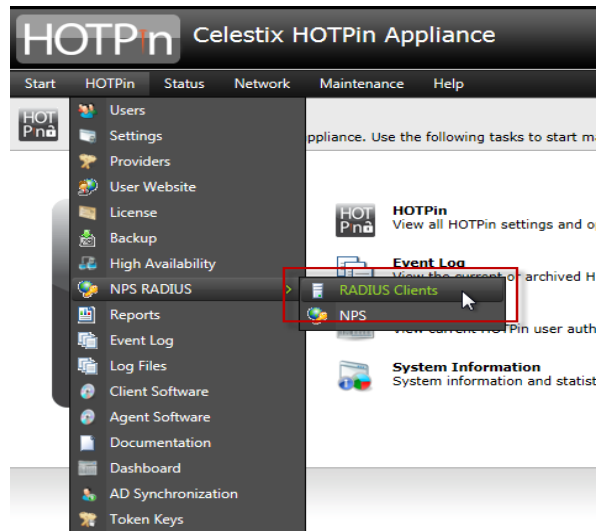
Celestix Networks USA	3125 Skyway Court, Fremont, California, 94539, USA	+1 510 668 0700
Celestix Networks EMEA	54 London Street, Reading, RG1 4QS, United Kingdom	+44 (0)118 959 6198
Celestix Networks APAC	1 Changi North Street 1, #02-02, Singapore 498789	+65 6781 0700

Integration completed by

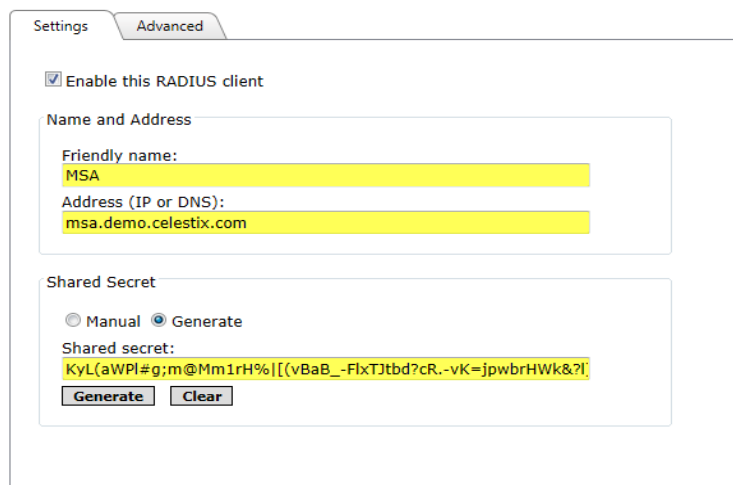
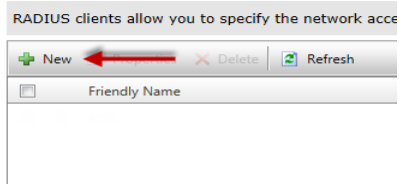
Richard Hicks

rhicks@celestix.com

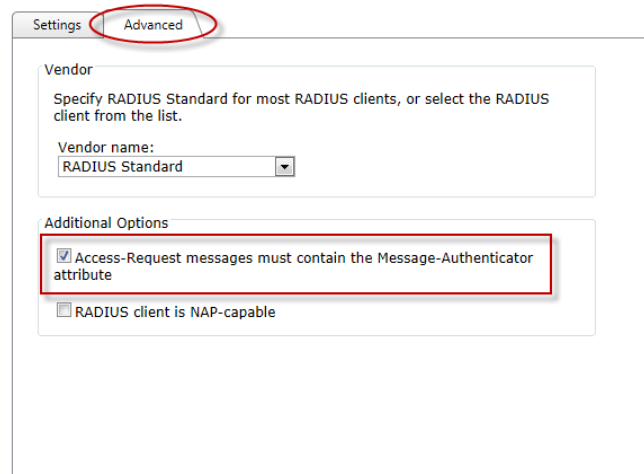
1. In the HOTPin web interface, click **HOTPin**, choose **NPS RADIUS**, then select **RADIUS Clients**



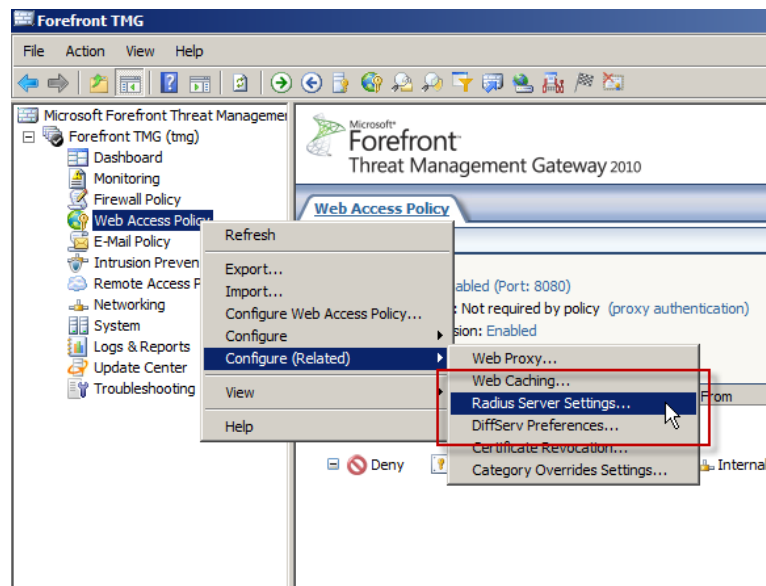
2. Click **New**, then enter a **Friendly name** and **Address** for the Celestix MSA. Specify a **Shared Secret** or choose the option to generate one automatically. Copy this string for use later on the MSA.



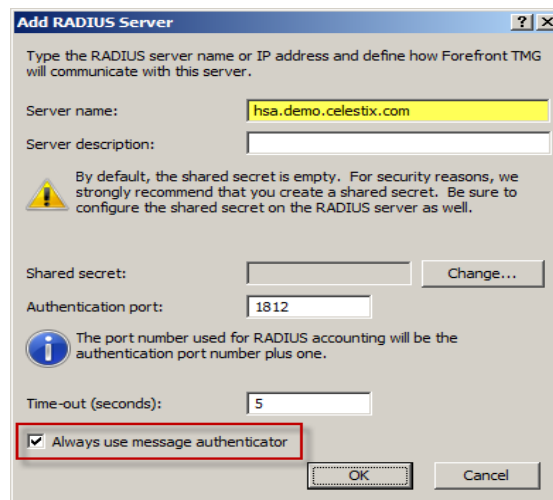
- Click the **Advanced** tab and select the option **Access-Request messages must contain the Message-Authenticator attribute**.



- 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:

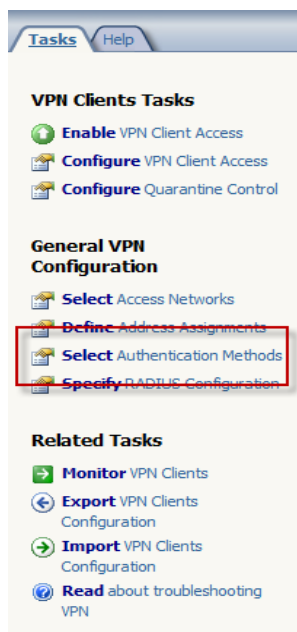
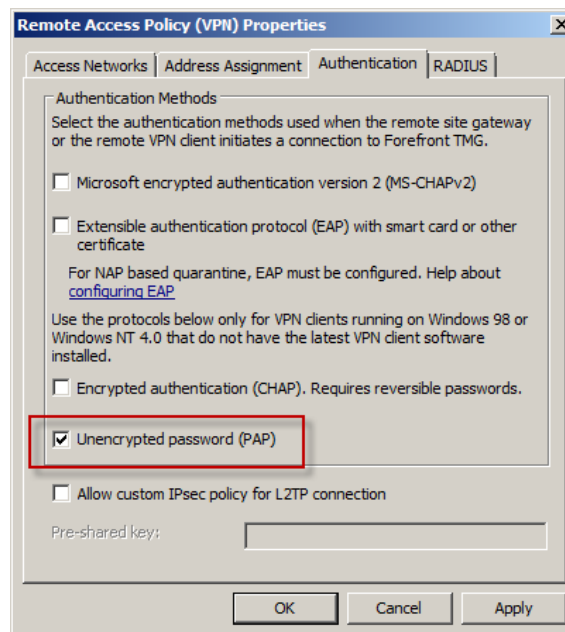
Authentication port:

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

Time-out (seconds):

Always use message authenticator

- Highlight the **Remote Access Policy (VPN)** in the navigation tree, and then click **Select Authentication Methods** in the **Tasks** pane. Select **ONLY** the option to use **Unencrypted password (PAP)**.

Remote Access Policy (VPN) Properties

Access Networks | Address Assignment | Authentication | **RADIUS**

Authentication Methods

Select the authentication methods used when the remote site gateway or the remote VPN client initiates a connection to Forefront TMG.

Microsoft encrypted authentication version 2 (MS-CHAPv2)

Extensible authentication protocol (EAP) with smart card or other certificate

For NAP based quarantine, EAP must be configured. Help about [configuring EAP](#).

Use the protocols below only for VPN clients running on Windows 98 or Windows NT 4.0 that do not have the latest VPN client software installed.

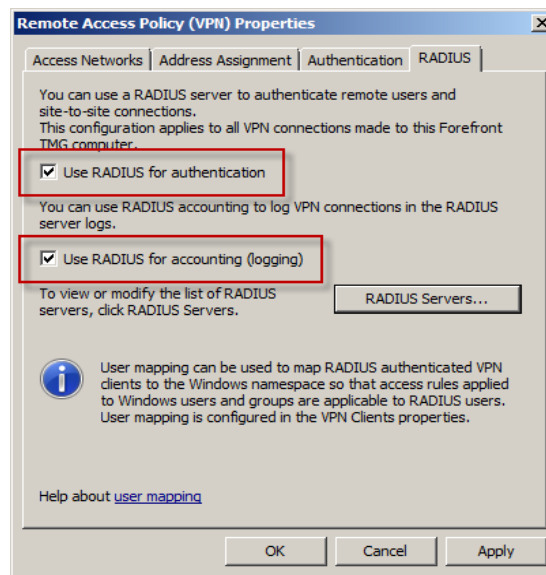
Encrypted authentication (CHAP). Requires reversible passwords.

Unencrypted password (PAP)

Allow custom IPsec policy for L2TP connection

Pre-shared key:

7. Select the **RADIUS** tab, and then choose the option to **Use RADIUS for authentication**. Optionally you can also select the option to **Use RADIUS for accounting (logging)**.



8. On the VPN client, open the properties for the connection and choose the **Security** tab. In the **Data encryption** drop down box, choose the option **Optional encryption (connect even if no encryption)**. For **Authentication** select **Allow these protocols** and choose **ONLY Unencrypted password (PAP)**.

