External Authentication with Microsoft Forefront Threat Management Gateway 2010

Authenticating Users Using SecurAccess Server by SecurEnvoy

<table>
<thead>
<tr>
<th>Contact information</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurEnvoy</td>
<td><a href="http://www.securenvoy.com">www.securenvoy.com</a></td>
<td>0845 2600010</td>
</tr>
<tr>
<td>Andy Kemshall</td>
<td><a href="mailto:akemshall@securenvoy.com">akemshall@securenvoy.com</a></td>
<td></td>
</tr>
<tr>
<td>Alex Sisson</td>
<td><a href="mailto:asisson@securenvoy.com">asisson@securenvoy.com</a></td>
<td></td>
</tr>
</tbody>
</table>
Setting up SecurEnvoy Authentication for Websites / Web applications

To set up SecurEnvoy two-factor authentication for internal websites or internal web applications (e.g. OWA) via your TMG:

- First create a rule to publish the website. You may want to test it with a one-factor LDAP listener to verify this works correctly, before adding the SecurEnvoy two-factor.

- In the rule properties, select the Listener tab, and either create a new listener, or modify an existing listener.

*When creating a new Listener with the New Listener Wizard –*

- Follow the wizard until the Authentication Settings screen is reached.
- From the drop-down box, select **HTML Form Authentication**.
- Enable the checkbox for **Collection additional delegation credentials in the form**
- Select **RADIUS OTP** from the selection of methods for validating client credentials.

![New Web Listener Definition Wizard](image)

*Figure 1: The Authentication section of the New Listener wizard*
When editing an existing Listener –

- Select the Authentication tab of the Listener properties dialog.
- In the Client Authentication Methods area, select **HTML Form Authentication**.
- Enable the checkbox for **Collection additional delegation credentials in the form**
- In the Authentication Validation Method area, select **RADIUS OTP**.

![SecuEnvoy Listener Properties](image)

**Figure 2: The Listener properties dialog, Authentication tab**
Configure Validation Servers

- Load the Listener properties dialog and select the **Configure Validation Servers** button.
- Add the details of your SecurEnvoy server, and choose a shared secret for the Radius communication.
- Change the Time-out to 10.
- Press OK.

![Add RADIUS Server](image)

*Figure 3: Adding the SecurEnvoy server details*
**Advanced settings**

- Select the **Advanced** button from the Listener properties dialog.
- Enabled the checkbox for **Require all users to authenticate**

*Figure 4: Advanced Authentication Options*
Configuring the SecurEnvoy Server

- On the SecurEnvoy server machine, launch the SecurEnvoy Local Admin desktop link
- Go to the Radius section
- Enter the IP address of your TMG server, and enter the shared secret used earlier for the TMG radius settings.

**Figure 5: Creating the Radius entry for the TMG**
Logon Forms

When browsing to the TMG external URL for the rule, the default logon form should now display:

![Default Logon Form](image)

*Figure 6: The default logon form*

Details should be entered into the form as follows:

**Remote Access Credentials:**
- **User name:** Enter your username (including Domain if needed)
- **Passcode:** Enter your LDAP password and SecurEnvoy passcode together (Or with SecurEnvoy PIN mode, enter the PIN and passcode together)
  
  Eg: Password123456

**Internal Network Credentials:**
- **Password:** Enter your LDAP password. This is not used for the TMG authentication, but for signing on to the backend webserver if it has its own authentication requirement.