Creating a Policy in NPS to support EAP-TLS authentication

When using WPA2-Enterprise with 802.1X authentication EAP-TLS can be specified as an authentication method. When EAP-TLS is the chosen authentication method both the wireless client and the RADIUS server use certificates to verify their identities to each other and perform mutual authentication. Below are the steps for configuring a policy in Windows Network Policy Server to support EAP-TLS.

Creating a Connection Request Policy to support IEEE 802.11 wireless connections.

1. Open the **Network Policy Server** console.
2. Navigate to **NPS(Local)>Policies>Connection Request Policies**.
3. Right-click **Connection Request Policies** and select **New**.
4. On **Specify Connection Policy Name and Connection Type** enter a **Policy name**: and click **Next**.
5. On **Specify Conditions** click **Add**.
6. Select **NAS Port Type** as a condition.
7. For **NAS Port Type** check **Wireless - IEEE 802.11** and **Wireless - Other** click **OK**.
8. Click **Next**.
9. On **Specify Connection Request Forwarding** leave the defaults and click **Next**.
10. On **Specify Authentication Methods** leave the defaults and click **Next**.
11. On **Configure Settings** click **Next**.
12. Review the settings on **Completing Connection Request Policy Wizard** and click **Finish**.
13. Right-click the Connection Policy created and select **Move up** so its processing order is before any other policies.
Creating a Network Policy to support EAP-TLS as the authentication method for IEEE 802.11 wireless connections.

1. Right-click **Network Policies** and select New.
2. On **Specify Network Policy Name** and **Connection Type** enter a **Policy name**: and click **Next**.
3. On **Specify Conditions** click **Add**.
4. Select **NAS Port Type** as a condition.
5. For **NAS Port Type** check **Wireless - IEEE 802.11** and **Wireless - Other** click **OK**.
6. Click **Next**.
7. On **Specify Access Permissions** make sure **Access granted** is selected and click **Next**.
8. On **Configure Authentication Methods** click **Add** and choose **Microsoft: Smart Card or other certificate** for **Add EAP** and click **OK**.
9. Uncheck any boxes under **Less secure authentication methods**.
10. Select **Microsoft: Smart Card or other certificate** for **EAP types** and click **Edit**.
11. Verify the **Certificate issued to**: drop down shows the correct certificate and issuer which is the Active Directory CA server. Then click **OK**.
12. Click **Next**.
13. On **Configure Constraints** click **Next**.
14. On **Configure Settings** choose **NAP Enforcement**.
15. Under **Auto-Remediation**, uncheck the box **Auto-remediation of client computers** and click **Next**.
16. Review the settings on **Completing New Network Policy** and Click **Finish**.
17. Right-click the Network Policy created and select **Move up** so its processing order is before any other policies.
**Conditions - If the following conditions are met:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS Port Type</td>
<td>Wireless - IEEE 802.11 OR Wireless - Other</td>
</tr>
</tbody>
</table>

**Settings - Then the following settings are applied:**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>EAP</td>
</tr>
<tr>
<td>Access Permission</td>
<td>Grant Access</td>
</tr>
<tr>
<td>Update Noncompliant Clients</td>
<td>False</td>
</tr>
<tr>
<td>NAP Enforcement</td>
<td>Allow full network access</td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>PPP</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Framed</td>
</tr>
<tr>
<td>Extensible Authentication Protocol Method</td>
<td>Microsoft: Smart Card or other certificate</td>
</tr>
<tr>
<td>Extensible Authentication Protocol Configuration</td>
<td>Configured</td>
</tr>
</tbody>
</table>
