Summary
This article describes how to configure Radius Authentication/Authorization on Windows 2008 for use with the Citrix Access Gateway Standard Edition appliance.

Requirements
Citrix Access Gateway 4.5.x or 4.6.x Standard Edition
Windows 2008 Server with Network Policy and Access Services role installed

Note: These tasks were performed on a Windows 2008 Server with the Network Policy and Access Services - formerly known as Internet Authentication Service (IAS) role installed.

Procedure
To configure radius Authentication/Authorization on Windows 2008, complete the following procedures:
• Configuration on the Windows 2008 Server
• Configuration on the Citrix Access Gateway Standard Edition appliance

Configuration on the Windows 2008 Server:
On the Windows 2008 server, complete the following procedure:
1. Open the Server Manager and select Roles > Install new Role Service.
2. From the Add Roles wizard, select Network Policy and Access Services and click Next.
3. Select **Network Policy Server** from the Select Role Services window, as shown in the following screenshot:
4. Follow the on-screen instructions and click **Install**.

5. After installation, create a Radius Client and configure a Network Policy to allow Radius authentication through the Citrix Access Gateway. To launch the Network Policy Server navigate to **Start > All Programs > Administrative Tools > Network Policy Server**.

6. In the **Radius Clients and Servers**, right click the **Radius clients** option and select **New Radius Client**, as shown in the following screen shot:
7. Specify the details, as shown in the following screen shot.
For Vendor Name, leave the option default which is RADIUS Standard and click OK.
8. Configure the Connection Request Policy.

**Note:** By default, Windows has already a request policy created and enabled known as **Use Windows authentication for all users** to allow all domain users authenticate through RADIUS. If this Connection Request Policy has been disabled or removed, make sure to create a policy that is complaint to your security needs.
9. Right-click **Network Policies** and select the **New** option to create Network Policies.

10. Enter a Policy Name and ensure to set the **Type of network access server** as **Unspecified** and then select **Next**.
11. In the **Specify Conditions window**, click **Add** and select **User Groups**.
12. In the User **Groups** window, select **Add Groups** and enter the Domain Users Group that should be allowed to authenticate using Radius.

13. Select **Access granted** and click **Next**.
14. In the Configure Authentication Methods, ensure to select only Encrypted authentication (CHAP) and Unencrypted authentication (PAP, SPAP) only. Any other authentication methods specified should be cleared.
15. Click **Next**.
16. The **Configure Constraints** window is optional for this implementation. Click **Next**.
17. In the Configure Settings window, navigate to **Radius Attributes > Standard**. Ensure to remove Framed-Protocol and Service-Type attributes.
18. In the **Configure Settings** window, select **Vendor Specific**.
19. Click **Add**.
20. Select **Custom** from the drop-down menu and click **Add**.
21. Click **Add** in the Attribute Information window.

**Attribute Information**

- Attribute name: Vendor-Specific
- Attribute number: 26
- Attribute format: OctetString

**Attribute values:**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Value</th>
</tr>
</thead>
</table>

[Add button]
22. Select **Yes. It conforms**.
   By default **No. It does not conform** is selected.
   Select **Configure Attribute**.

23. Retain the value of **Vendor-assigned attribute number = 0**.
    Select **String** in the **Attribute format** field. Set the Attribute value to
    **CTXSUserGroups=GroupName** where **GroupName** equals the Group you will define on the Citrix Access Gateway.
    **Note:** Ensure to enter the Group Name correctly. It is case sensitive. If you need to add more than one Group Name, separate each name with a semicolon (;).

24. Verify that the information entered for Vendor Specific is correct and click **Next**.
25. Confirm that the Network Policy settings are correct and click **Finish**.
26. Ensure that in the **Processing Order** field, the Network Policy has the appropriate priority.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Status</th>
<th>Processing Order</th>
<th>Access Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAG</td>
<td>Enabled</td>
<td>1</td>
<td>Grant Access</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Connections to Microsoft RAS</td>
<td>Enabled</td>
<td>2</td>
<td>Deny Access</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Connections to other access</td>
<td>Enabled</td>
<td>3</td>
<td>Deny Access</td>
<td>Unspecified</td>
</tr>
</tbody>
</table>

**Configuration on the Citrix Access Gateway Standard Edition Appliance**

On the Citrix Access Gateway, complete the following procedure:
1. Launch the Citrix Access Gateway Administration Tool.
2. Select the **Authentication** tab.
3. Either delete the default realm and recreate it as Radius authentication or create a new realm.
4. Verify the following details:
   - The **server IP address** will be the Windows Server you configured to act as a Radius Server
   - The default **RADIUS port is 1812**
   - The **shared secret** is the secret value you created when you added the
Access Gateway server as a Radius client in the Network Policy Server configuration in the preceding procedure.

5. Select the **Authorization** tab and specify the following settings:
   - Retain the Authorization type as **RADIUS authorization**
   - The Vendor Code as **0**
   - The Vendor-assigned attribute number as **0**
   - The Attribute Value Prefix as **CTXSUserGroups=**
6. In the **Access Policy Manager** create a **User Group** name that matches with the name that you assigned on the Radius server on Windows 2008. This example, creates a new User Group called **CAG**, the same name that is assigned for **GroupName** in step 23.