Cox Managed CPE Services

RADIUS Authentication for AnyConnect VPN
Version 1.3 [Draft]

September, 2015
Contents
RADIUS AUTHENTICATION FOR ANYCONNECT VPN......................................................... 1
INSTALL THE NPS AND RADIUS ROLES ON WINDOWS SERVER 2008 ...................... 3
  STEP 1: INSTALL NETWORK POLICY AND ACCESS SERVICES........................................ 3
  STEP 2: ADD CISCO ROUTER AS CLIENT ON NPS SERVER........................................... 9
  STEP 3: DEFINE POLICY ON NPS SERVER...................................................................... 12
INSTALL THE NPS AND RADIUS ROLES ON WINDOWS SERVER 2012 ...................... 25
  STEP 1: INSTALL NETWORK POLICY AND ACCESS SERVICES........................................ 25
  STEP 2: ADD CISCO ROUTER AS A CLIENT ON THE NPS SERVER.................................. 31
  STEP 3: DEFINE POLICY ON NPS SERVER...................................................................... 33
ANYCONNECT VPN WITH CERTIFICATE AUTHORITY..................................................... 39
  PRIVATE CA.................................................................................................................. 39
    Generating CA Certificate for managed device............................................................ 39
    Generating Identity Certificate for managed device...................................................... 42
    Installing Certificate on Managed Device (To be performed by support team)............. 46
  GLOBAL CA.................................................................................................................. 49
SAMPLE CONFIGURATION ON CLIENT......................................................................... 50
  CONFIGURATION EXAMPLE ON ISR ROUTER WITH RADIUS AUTHENTICATION FOR CISCO ANYCONNECT VPN
   ........................................................................................................................................ 50
RADIUS Authentication for AnyConnect VPN

Introduction

This document details the configuration tasks needed in order to have a managed services device use a Microsoft Windows Server 2008 or Microsoft Windows 2012 R2 server with the RADIUS protocol to authenticate AnyConnect VPN users against Active Directory.

Network Policy Service (NPS) is one of the server roles offered by Windows Server 2008 and Windows Server 2012 R2. It is similar to the Internet Authentication Service (IAS) found in Windows 2003 Server, which itself is an implementation of a RADIUS server to provide remote dial-in user authentication.

In this configuration, the Cox managed router is a RADIUS client to an NPS RADIUS server. The router sends RADIUS authentication requests on behalf of VPN users and NPS authenticates them against Active Directory.

Assumption

This document only covers the installation of a RADIUS and Network Policy Server role on a server already configured for Active Directory on Windows Server 2008 and Windows Server 2012 R2.

Installation and configuration of Active Directory and DNS are beyond the scope of this document. Reference guides for installing the Active Directory role on Windows Server 2008 and Windows Server 2012 are located at the following URLs, respectively:

http://www.rackspace.com/knowledge_center/article/installing-active-directory-domain-services-on-windows-server-2008-r2-enterprise-64-bit

http://www.rackspace.com/knowledge_center/article/installing-active-directory-on-windows-server-2012

Note: The DNS role is automatically installed when Active Directory is installed.

Requirements for Setting Up Router in Active Directory

- **LAN IP Address of Cisco ISR Router**: This IP Address is the default gateway address of Cox managed router device.
- **RADIUS shared secret**: This is configured on a Cisco router - < TBD >.
- **VPN Users Group**: This group was defined in the Active Directory server and will be referenced while setting up the RADIUS role.
Install the NPS and RADIUS Roles on Windows Server 2008

Prerequisites
Before you begin, ensure the following tasks are completed:

- Active Directory and DNS server are installed and working (required)
- Organization Unit and User accounts in Active Directory are created (optional)

Step 1: Install Network Policy and Access Services

How to Install the Network Policy and Access Services

Use the following steps to install the network policy and access services.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the Add Roles Wizard, select the <strong>Server Roles</strong> option. <strong>Result:</strong> The list of Roles appears.</td>
</tr>
<tr>
<td>2.</td>
<td>Check the <strong>Network Policy and Access Services</strong> box and click the <strong>Next</strong> button.</td>
</tr>
</tbody>
</table>

Figure 1. Select Server Roles screen
How to Install the Network Policy and Access Services, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 3.   | Check the **Network Policy Server** option and click the **Next** button.  
A. Select the **Role Services** menu option on the left navigation bar.  

**Figure 2. Select Role Services screen**

4. Click the **Next** button and continue to click through the confirmation screen.

*Continued on next page*
How to Install the Network Policy and Access Services, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Click the <strong>Install</strong> button.</td>
</tr>
</tbody>
</table>

**Figure 3. Confirm Installation Selections screen**

![Confirm Installation Selections screen](image1)

**Figure 4. Installation Progress screen**

![Installation Progress screen](image2)
6. When the role is installed, set up the server using the Network Policy Server (NPS) management tool. You can find the tool under Administrative Tools.

7. When you launch the NPS tool, right-click the entry NPS (Local) and click the Register Server in Active Directory.

8. Follow the prompts and keep the default values.
Installing the NPS and RADIUS Roles on Windows Server 2008

Figures 7 and 8. Network Policy Server and Network Proxy Server

RADIUS Authentication for AnyConnect VPN

Company Confidential. A printed copy of this document is considered uncontrolled.
Step 2: Add Cisco Router as Client on NPS Server

Overview

The second phase of the Installation process is to add the Cisco Router as a client on the NPS server.

How to Add a Cisco Router as a Client on the NPS Server

Use the following steps to add the Cisco router. The first step of this second phase requires you to add the ISR as a RADIUS client in the NPS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Go to Administrative Tools and select Network Policy Server. Right-click RADIUS Clients and select the New menu option.</td>
</tr>
</tbody>
</table>

Figure 9. RADIUS Clients
2. When you expand the RADIUS Clients and Servers folder, the RADIUS Clients option appears.

   1. Click the **RADIUS Clients** option.
      
      **Result:** The **New RADIUS Client** dialog box appears.

   2. Check the **Settings** tab and enter a **Friendly name**, **Address (IP or DNS)**, and select the **Shared Secret** template configured on the Cisco Router from the drop-down menu.

**Figure 10.** **New RADIUS Client – Settings tab**

*Continued on next page*
How to Add a Cisco Router as a Client on the NPS Server, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Click the <strong>Advanced</strong> tab.</td>
</tr>
<tr>
<td>4.</td>
<td>From the Vendor name drop-down list, choose <strong>RADIUS Standard</strong>.</td>
</tr>
</tbody>
</table>

**Figure 11. New RADIUS Client – Advanced tab**

5. Click the **OK** button.
Step 3: Define Policy on NPS Server

Overview

In this phase, you will create a new Connection Request Policy for VPN users. The purpose of the Connection Request Policy is to specify whether the requests from RADIUS clients are to be processed locally or forwarded to remote RADIUS servers.

How to Create a New Connection Request Policy for VPN Users

Use the following steps to create a new Connection Request Policy for VPN users.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Expand the **Network Policy and Access Services** menu in the left navigation bar.  
**Figure 12. Server Manager left navigation bar** |
| 2.   | Expand the **NPS (Local)** option in the left navigation bar. |

*Continued on next page*
How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Expand the <strong>Policies</strong> folder in the left navigation bar.</td>
</tr>
</tbody>
</table>
| 4.   | Right-click **Connection Request Policies**.  
**Result:** The *New Connection Request Policy* dialog box appears. |
| 5.   | Enter a description for the policy in the **Policy name** field. |
| 6.   | Select the **Type of network access server** radio button and click the arrow on the drop-down menu. |
| 7.   | Select the **Unspecified** option. |

*Figure 12.  New Connect Request Policy dialog box*

*Continued on next page*
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 8.   | Click the **Next** button.  
**Result**: The *Specify Conditions* dialog appears.  
**Figure 13. Specify Conditions dialog box** |
| 9.   | From the **Select Condition** section, click the **Client Friendly Name** option and then click the **Add** button.  
**Result**: The **Client Friendly Name** dialog box appears. |

*Continued on next page*
How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Enter the friendly name that you used when creating the RADIUS Client. See Error! Not a valid result for table.. Figure 14. Client Friendly Name dialog box</td>
</tr>
</tbody>
</table>

![Client Friendly Name dialog box](image)

| 11.  | Click the OK button and the Next button. Result: The Specify Connect Request Forwarding dialog box appears. Figure 15. Specify Connection Request Forwarding dialog box |

![Specify Connection Request Forwarding dialog box](image)

| 12.  | Check that the Authenticate requests on this server radio button is selected. |

Continued on next page
How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 13. | Click the **Next** button.  
**Result:** The **Specify Authentication Methods** dialog box appears.  
**Figure 16. Authentication Methods dialog box** |
| 14. | Check the **Override network policy authentication settings** box. |
| 15. | From the **Less secure authentication methods** section, check the **Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)** box and the **User can change password after it has expired** box. |

*Continued on next page*
How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 16.  | Click the Next button.  
**Result**: The **Configure Settings** dialog box appears.  
**Figure 17. Configure Settings dialog box** |

![Configure Settings dialog box](image)

| 17.  | From the left navigation bar, select the **Attribute** option and then select the **User Name** from the drop down menu. |
| 18.  | Click the Next button.  
**Result**: The **Completing Connection Request Policy Wizard** dialog box appears.  
**Figure 18. Completing Connection Request Policy Wizard dialog box** |

![Completing Connection Request Policy Wizard dialog box](image)
19. Click the **Finish** button.

**Overview**  
Once you have created a **New Request Connect Policy for VPN users**, you need to create a **Network Policy**. Here, you can specify which users are allowed to authenticate. For example, you can add Active Directory user groups as a condition.

*Note:* Only those users who belong to a specified Windows group are authenticated under this policy.

**How to Create a Network Policy**  
Use the following steps to create a network policy.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the left navigation bar, expand the <strong>Network Policy and Access Services</strong> option.</td>
</tr>
<tr>
<td>2.</td>
<td>Expand the <strong>NPS (Local)</strong> option.</td>
</tr>
<tr>
<td>3.</td>
<td>Right-click <strong>Network Policies</strong> under the <strong>Policies</strong> option to create a new policy. <strong>Result:</strong> The <strong>Specify Network Policy Name and Connection Type</strong> dialog box appears.</td>
</tr>
</tbody>
</table>

**Figure 19.** **Specify Network Policy Name and Connect Type** dialog box
4. Check that the **Grant access** radio button is selected.

5. From the **Type of network access server** drop-down menu, select the **Unspecified** option.

6. Click the **Next** button.
   **Result:** The **Specify Conditions** dialog box appears.
   **Figure 20. Specify Conditions dialog box**

7. Highlight **User Groups** and click the **Add** button.
   **Result:** The **Select Group** dialog box appears.
   **Figure 21. Select Group dialog box**

8. Click the **Object Types** button and make your selection.

9. Click the **Locations** button and make your select.

10. Click the **Check Names** button to add a users’ group condition to a specific AD user group. (**Note:** You can use a generic group like **Domain Users** or create a group specifically to restrict access.)

Continued on next page
How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 11.  | Click the **OK** button.  
**Result:** The **Specify Conditions** dialog box appears.  
**Figure 22. Specify Conditions dialog box** |
| 12.  | Click the **Next** button.  
**Result:** The **Specify Access Permissions** dialog box appears.  
**Figure 23. Specify Access Permissions dialog box** |
13. Click the **Next** button and keep the **Access granted** radio button selected.

14. Click the **Next** button.  
**Result:** The **Configure Authentication Methods** dialog box appears.  
**Figure 24. Configure Authentication Methods dialog box**

15. Leave the default selections under the **Less secure authentication methods** section.

16. Check the **Unencrypted authentication (PAP, SPAP)** box.

17. Click the **Next** button.  
**Result:** The **Configure Constraints** dialog box appears.
18. Keep the default Constraints settings.

**Figure 25. Configure Constraints dialog box**

*Continued on next page*
### How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 19.  | Click the **Next** button.  
**Result:** The **Configure Settings** dialog box appears.  
**Figure 26.** **Configure Settings dialog box** |
| 20.  | Accept the default Radius Settings.  
*Continued on next page* |
### How to Create a New Connection Request Policy for VPN Users, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 21.  | Click the **Next** button.  
**Result:** The **Completing New Network Policy** dialog box appears.  
**Figure 27.** [Completing New Network Policy dialog box](image) |
| 22.  | Review the settings in the screen above and click the **Finish** button.  
**Figure 28.** [Network Policies review screen](image) |
Install the NPS and RADIUS Roles on Windows Server 2012

Overview
Just as with the steps you performed to install the NPS and RADIUS Roles on Windows Server 2008, you will need to replicate the process to complete the installation for Windows Server 2012.

Step 1: Install Network Policy and Access Services

How to Add Roles and Features
Use the following steps to install roles, role services, and features based on the computing needs of your company, such as sharing documents or hosting a website.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Server Manager Dashboard and click the Add roles and features option.</td>
</tr>
</tbody>
</table>

Figure 29. Add Roles and Features Wizard

Continued on next page
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Click the <strong>Next</strong> button.</td>
<td><strong>Result</strong>: The <strong>Select installation type</strong> dialog box appears.</td>
</tr>
<tr>
<td><img src="image" alt="Select installation type dialog box" /></td>
<td></td>
</tr>
<tr>
<td>3. Make sure the <strong>Role-based or feature-based installation</strong> radio button is selected.</td>
<td></td>
</tr>
</tbody>
</table>

*Continued on next page*
## How to Add Roles and Features, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 4.   | Click the **Next** button.  
**Result:** The Select destination server dialog box appears.  
**Figure 31.** Select destination server dialog box. |
| 5.   | Click the **Next** button.  
**Result:** The Select server roles dialog box appears.  
**Figure 32.** Select server roles dialog box |
6. Check the **Network Policy and Access Services** box.

7. Click the **Next** button.
   **Result:** The **Add features that are required for Network Policy and Access Services** dialog box appears.

**Figure 33. Add features that are required for Network Policy and Access Services dialog box**

![Add features that are required for Network Policy and Access Services dialog box](image)

8. Check the **Include management tools (if applicable)** box.

9. Click the **Add features** button.

*Continued on next page*
How to Add Roles and Features, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td>Click the <strong>Next</strong> button until you get to the <strong>Confirm installation selections</strong> dialog box. <strong>Figure 34. Confirm installation selections dialog box</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>Click the <strong>Install</strong> button. <strong>Figure 35. Installation progress dialog box</strong></td>
</tr>
<tr>
<td>12.</td>
<td>When the installation completes, click the <strong>Close</strong> button.</td>
</tr>
</tbody>
</table>

RADIUS Authentication for AnyConnect VPN

Company Confidential. A printed copy of this document is considered uncontrolled.
How to Register the Server in Active Directory

Use the following steps to register the server in active directory.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | Open the **Network Policy Server (NPS)** console from the **Start** menu or from **Server Manager**.  
**Figure 36. Network Policy Server (NPS) Console dialog box** |
| 2.   | Right-click the **NPS** option in the left navigation bar and select the **Register server in Active Directory**.  
**Figure 37. Menu options** |
| 3.   | Click the **OK** button on the “**To enable NPS to authenticate users...**” and the “**This computer is now authorized...**” dialog boxes. |
Step 2: Add Cisco Router as a Client on the NPS Server

Overview
The second step is to add the Cisco router as a client on the NPS server.

How to Add a Cisco Router as a Client on the NPS Server
Use the following steps to add the router as a client on the server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | From the left navigation bar, expand the RADIUS Clients and Servers folder and right-click the **RADIUS Clients** option.  
**Result**: A sub menu appears.  
**Figure 38.** RADIUS Clients – New |

*Continued on next page*
How to Add a Cisco Router as a Client on the NPS Server, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 2.   | Click New.  
**Result:** The VPNHUB Properties dialog box appears.  
**Figure 39.** VPNHUB Properties dialog box |
| 3.   | Click the **Settings** tab. |
| 4.   | Enter a description for the Cisco ISR in the **Friendly name** field. |
| 5.   | Enter the IP address in the **Address (IP or DNS)** field. |
| 6.   | Select an existing Share Secrets template from the **Shared Secret** drop-down menu. |
| 7.   | Click the **OK** button. |
Step 3: Define Policy on NPS Server

Overview
The third step is to define the policy on the NPS server.

How to Define a Policy on the NPS Server
Use the following steps to define a policy on the NPS Server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the left navigation bar, expand the NPS (Local) menu and then expand the <em>Policies</em> option.</td>
</tr>
</tbody>
</table>
| 2.   | Right-click the *Network Policies* folder and select *New*.  
**Result:** The *Specify Network Policy Name and Connection Type* dialog box appears. |
| 3.   | Enter a *Policy name* for the connection policy and click the *Next* button.  
**Result:** The *Select Condition* dialog box appears. |

![Specify Network Policy Name and Connection Type dialog box](image)

Continued on next page
How to Define a Policy on the NPS Server, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Figure 41. Select Condition dialog box</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image1" alt="Select Condition dialog box" /></td>
</tr>
<tr>
<td>5.</td>
<td>Click the Add button. <strong>Result:</strong> The User Groups dialog box appears.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Figure 42. User Groups dialog box</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image2" alt="User Groups dialog box" /></td>
</tr>
<tr>
<td>7.</td>
<td>Click the Add Groups button.</td>
</tr>
<tr>
<td>8.</td>
<td>Enter the VPN Users group that was created earlier on Active Directory. (See page 16.)</td>
</tr>
</tbody>
</table>

*Continued on next page*
How to Define a Policy on the NPS Server, continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 9.   | Click the **OK** button.  
**Result:** The **Specify Access Permission** dialog box appears.  
**Figure 43.** **Select Group dialog box** |
| 10.  | **Figure 44.** **Specify Access Permission** dialog box |
| 11.  | Check that the **Access granted** radio button is selected. |
12. Click the Next button.
   Result: The Configure Authentication Methods dialog box appears.

   Figure 45. Configure Authentication Methods dialog box

13. Check the MS-CHAPv2 and MS-CHAP boxes.

14. Click the Next button.
   Result: The Configure Settings dialog box appears.

15. Click the Next button.
   Result: The Completing New Network Policy dialog box appears.

16. Figure 46. Completing New Network Policy dialog box
| 17. | Review the final options and click the **Finish** button. |
AnyConnect mobility VPN client supports certificate authority, which issues digital certificate to certify the ownership of a public key. This allows managed device to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted party – trusted both by the subject (owner) of the certificate and by the managed device relying upon the certificate.

Managed device requires two types of certificate to be issued by CA –
1. CA Certificate
2. Identity Certificate

There are two types of CA covered in this document
1. Private CA server setup by Enterprise
2. Globally Known public CA server.

Private CA

Private CA is a solution to improve the security and management of private intranet certificates while adhering to corporate and industry compliance standards.

Following steps involves the process in which required certificate should be generated from CA and should be applied on the managed device.

Note: Some of the steps will be performed by support team and are clearly mentioned.

Generating CA Certificate for managed device

Step1 - CA server should be accessed using a web browser. If logged on locally to CA server use https://localhost/certsrv or if remotely logging on then use https://x.x.x.x/certsrv where ‘x.x.x.x ‘ is the IP address of the CA server. User will see following screen
Step 2 – Next step is to download the first of two certificates “CA Certificate”. Click on “download a ca certificate, certification chain or CRL” as highlighted below.

Step 3 – In this step, Click “NO” on Digital Certificate Operation window as shown below
Step 4: Once user clicks NO, following window will appear. On this window under Enrollment Method – Select “Base 64” and then click on Download ca certificate.

Step 5: Once you click on Download ca certificate it will prompt you to save that certificate. Click on Save and save it on your desired location.
Generating Identity Certificate for managed device

Step 1 - CA server should be accessed using a web browser. If logged on locally to CA server use https://localhost/certsrv or if remotely logging on then use https://x.x.x.x/certsrv where ‘x.x.x.x’ is the IP address of the CA server. User will see following screen.
Step 2: (Step performed by Support Team) For generating identity certificate, CA server will require a CSR (Certificate Signing Request) file which will be generated from managed device using following command. Highlight portion of this CSR file will be pasted on the CA server to generate identity certificate.

```
Router(config)#crypto pki enroll cisco
% Start certificate enrollment..

% The subject name in the certificate will include: 10.64.117.16
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
% Display Certificate Request to terminal? [yes/no]: no
% Certificate Request follows:

MIIBFTCB5IBADAdMRswGQYJKoZIhvcNAQkCFgwxXMCRZNCxMTcwdlYw9g28wDQYJKoZIhvcNAQEBBDQgY0AMIGfA8BAIiI2Vzd3dwH2s6GdAnMo2Zao1dQ4FLQm0SL+CIgGwTm83JCqaKQ1NaJy=5dGVWh073ET7AgFz1HWR1whCnJ/G010FSc0UuFmVwY8s4AnjYFa=Q13xPvXZm2K131zceLZbdMRHdSvQtx5Rcv1wAZD94Nv+Bya+7yzqghFqMBAaAQeITAFBgkqhk1G9wO8CQx4EJAQMA4AHAuDmWEB/xGEw1P0oDANBkgkqhk1G9wO8A0QFAAhBqGJZ1yPQqCokSyT7n6uTf2BEgpin3rZyn7GeQVctEH

---End - This line not part of the certificate request--
```

Step 3: On CA Server, click on “Request a certificate”

Step 4: Next screen – Click on Advanced Certificate request.
Step 5: Next screen – Click on “Submit a certificate by using a base 64” option as highlighted in below

Step 6: On Next screen, User needs to select “Administrator” as Certificate Template and also paste CSR (Certificate Signing Request – generated in step2) file in Saved request Box as shown in following screenshots.
Installing the NPS and RADIUS Roles on Windows Server 2012

Step 7: Click “Submit” and Digital Certificate Operation warning will pop-up – Select “NO”

Step 8- After selecting no, user will land on following page. On this page select “Base 64 encoded “ option as by default DER encoded will be selected then click on download certificate and save the certificate.
Note: Both Certificate files (CA & Identity), which are generated and saved, should be provided to support team for installing them on managed device

**Installing Certificate on Managed Device (To be performed by support team)**

Step1: Install CA Certificate as shown below.
Step 2: Install Identity Certificate.
Configuration Example

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself.

BEGIN CERTIFICATE-----
MIIFjxCCBqgAwIBAgIIT9qAAABn3p1x7K1/7QAAAAAGTANBgkghiG9w0BAQUF
ADBEmRuwEwYKZCMiZPyLG8GRYFbG9jYWxsaEBg0DWh9I/aKf/aKf/aKf/aKf/aKf/aKf
MTAzNDQwMB8RUwEwYKZCMiZPyLG8GRYFbG9jYWxsaEBg0DWh9I/aKf/aKf/aKf/aKf/aKf/aKf
Bz8RUwEwYKZCMiZPyLG8GRYFbG9jYWxsaEBg0DWh9I/aKf/aKf/aKf/aKf/aKf/aKf
-----END CERTIFICATE-----

Step 3: Verify whether both certificates are installed properly.
Global CA

Global CA or Root CA servers are well known public CA servers and they offer digital certificates. An enterprise should subscribe to digital certificate from digital certificate provider. In this process, User will be able to log on to digital certificate provider’s website with required credentials and upload a CSR (Certificate Signing Request) file to generate digital certificate. These digital certificate will be sent to user’s email or will be available on provider’s website, this process depends on different providers. Managed Device support team will be able to provider CSR file, which needs to be generated from managed device. After submitting/uploading CSR file, user will receive certificate files which should be sent to Managed device’s support team for installation on managed device.
Sample Configuration on Client

Configuration Example on ISR router with RADIUS Authentication for Cisco AnyConnect VPN

AAA Commands

aaa new-model
aaa group server radius TESTAD
server TESTAD
aaa authentication login WEBVPN-LIST group radius local

RADIUS Commands

radius server TESTAD
address ipv4 10.106.223.6 <<< AD Server IP Address
key cisco@123
exit

AnyConnect VPN Commands

crypto vpn anyconnect flash0:/webvpn/anyconnect-win-4.0.00061-k9.pkg sequence 1
crypto vpn anyconnect flash0:/webvpn/anyconnect-macosx-i386-4.0.00061-k9.pkg sequence 2
webvpn gateway WEBVPN-GW
ip address 10.64.117.16 port 8888
http-redirect port 80
ssl trustpoint test
in service
!
webvpn context WEBVPN-CONTEXT
virtual-template 10
aaa authentication list WEB
gateway WEBVPN-GW
!
ssl authenticate verify all
install service

policy group WEBVPN-GROUP
  functions svc-enabled
  functions svc-required
  svc address-pool "WEBVPN-POOL" netmask 255.255.255.0
  svc keep-client-installed
  svc split include 192.168.1.0 255.255.255.0
default-group-policy WEBVPN-GROUP

End of Document