**Configuring 802.1x Network Device Authentication**

**Prerequisites**

An 802.1x authentication system requires the following components:

* PCoIP zero client with firmware 4.0.3 or newer
* PCoIP Management Console 1.8.1 or newer
* Windows Server 2008 R2 with AD DS (Active Directory Domain Services)
* Windows Server 2008 R2 with AD CS (Active Directory Certificate Services)
* Windows Server 2008 R2 with NPS (Network Policy and Access Services)
* VMware View Connection Server
* A switch with 802.1x support configured

**Procedure**

**Overview**

Configuring 802.1x device authentication entails the following steps:

1. In the Windows 2008 server, [create a client user](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Create).
2. In the Certificate Authority (CA) server, [export the root CA certificate](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Export).
3. In the CA server, [create a certificate template for client authentication](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Create2).
4. From the CA Web Enrollment interface interface for the certificate server, [issue the client certificate](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Issue).
5. From the machine on which you issued the certificate, [export the client certificate](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Export2).
6. Using OpenSSL, [convert the certificate format from .pfx to .pem](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Convert).
7. In the Windows 2008 server, [import the client certificate into the client user account](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Import).
8. From the MC or device's AWI, [import the certificates](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Import2).

Note: The instructions in the following sections are based on Windows Server 2008 R2. If you are using a newer version of Windows Server, the steps may vary slightly.

**Create a Client User**

1. Log in to the Windows 2008 server.
2. Click **Start > Administrative Tools > Server Manager**.
3. Navigate to **Roles > Active Directory Domain Services > Active Directory Users and Computers > *<domain.local>* > Users**.
4. Right-click **Users**, select **New > User**, and then follow the wizard.

**Export the Root CA Certificate**

1. Log in to the Certificate Authority (CA) server.
2. Open a Microsoft Management Console window (e.g.,enter **mmc.exe** in the **Start** menu search field).
3. From the console window, select **File > Add/Remove Snap-in.**
4. Add the **Certificates** snap-in, selecting **Computer account** and then **Local computer**.
5. Click **Finish**, and then **OK** to close the **Add or Remove Snap-ins** dialog.
6. From the console, select **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
7. In the right panel, right-click the certificate, and then select **All Tasks** > **Export**.
8. Follow the wizard to export the certificate:
   1. Select **Base-64 encoded X.509 (.CER)**.
   2. Click **Browse**, specify a name and location for the certificate, and then click **Save**.
   3. Click **Finish**, and then **OK.**

**Create a Certificate Template for Client Authentication**

1. From the CA server, click **Start > Administrative Tools > Certification Authority**.
2. Expand the tree for your CA.
3. Right-click **Certificate Templates**, and then click **Manage**.
4. Right-click the **Computer** template, and then click **Duplicate Template**.
5. Configure the template as follows:
   1. From the **Compatibility** tab, select **Windows Server 2003**.
   2. From the **General** tab, enter a name for the template (e.g., "zero client 802.1x") and change the validity period to match the organization's security policy.
   3. From the **Request Handling** tab, select **Allow private key to be exported**.
   4. From the **Subject Name** tab, select **Supply in the request**.
   5. From the **Security** tab, select the user who will be requesting the certificate, and then give **Enroll** permission to this user.
   6. Click **OK** and close the **Certificate Templates Console** window.
6. From the **Certification Authority** window, .right-click **Certificate Templates**, select **New**, and then click **Certificate Template to Issue**
7. Select the certificate you just created (i.e., "zero client 802.1x), and then click **OK**. The template will now appear in the **Certificate Templates** list.
8. Close the window.

**Issue the Client Certificate**

Note: Do not use any other browser except Internet Explorer to log into the certificate server.

1. Using Internet Explorer on your local machine, go to your Certificate Authority URL using the format**https://<*server*>/certsrv/** (e.g., "https://ca.domain.local/certsrv/").
2. Click **Request a certificate** and then **advanced certificate request**.
3. Click **Create and submit a request to this CA**.
4. At the pop-up window, click **Yes**.
5. Fill out the **Advanced Certificate Request** form as follows:
   1. In the **Certificate Template** section, select the certificate for clients (e.g., "Zero Client 802.1x").
   2. In the **Identifying Information for Offline Template** section, enter the account name in the **Name** field. The other fields are not required.  
      *Important! The name you enter in the Name field must be the fully qualified domain name of the client user you created in*[*Create a Client User*](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Create)*(e.g., "ZeroClient@mydomain.local")*.
   3. In the **Additional Options** section, set the Request Format to **PKCS10**.
   4. If desired, enter a name in the **Friendly Name** field.
   5. Click **Submit**, and then **Yes** at the pop-up window.
   6. At the **Certificate Issued** window, click **Install this certificate**.

**Export the Client Certificate**

1. From the machine on which you issued the certificate, open a Microsoft Management Console window (e.g., enter **mmc.exe** in the **Start** menu search field).
2. From the console window, select **File > Add/Remove Snap-in**.
3. Add the **Certificates** snap-in, selecting **My user account**.
4. Click **Finish**, and then **OK** to close the **Add or Remove Snap-ins** dialog.
5. Select **Certificates - Current User > Personal > Certificates**.
6. In the right panel, right-click the certificate, and then select **All Tasks** > **Export**.
7. Follow the wizard to export the certificate:
   1. Click **Yes, export the private key**.
   2. Select **Personal Information Exchange - PKCS #12 (.PFX)**.
   3. Enter a password for the certificate.
   4. Click **Browse**, specify a name and location for the certificate, and then click **Save**.
   5. Click **Finish**, and then **OK**.
8. Repeat steps 5 to 7 again to export the zero client certificate, but this time *without* the private key (**No, do not export the private key**), selecting the **DER encoded binary X.509 (.CER)**format instead of the PKCS format.
9. Save this .cer file to a location where it can be accessed by the Windows 2008 server and imported into Active Directory.

**Convert the Certificate Format from .pfx to .pem**

1. Download and install Windows OpenSSL from **http://www.slproweb.com/products/Win32OpenSSL.html**. (The light version is sufficient.)
2. Copy the .pfx client certificate file you saved above to the **C:\OpenSSL-Win32\bin** directory.
3. Open a command prompt window, and then enter the following command to convert the certificate format from .pfx to .pem:  
   **C:\OpenSSL-Win32\bin\openssl.exe pkcs12 ‑in *<client\_cert>*.pfx ‑out <*client\_cert*>.pem ‑nodes**  
   where *<client\_cert>* is the name of the .pfx certificate file you saved to your local machine.
4. When prompted, enter the password for the certificate file.
5. At the command prompt, enter the following command to create an RSA private key file:  
   **C:\OpenSSL-Win32\bin\openssl.exe rsa –in <*client\_cert*>.pem –out < *client\_cert*>\_rsa.pem**  
   where <*client\_cert*> is the name of the .pem certificate file you created in the previous step.
6. In Notepad:
   1. Open both the original .pem file and the RSA .pem file you just created. The RSA .pem file contains only an RSA private key. Because the zero client certificate requires its private key in RSA format, you need to replace its private key with this RSA private key.
   2. Copy the entire contents of the RSA .pem file (everything from -----**BEGIN RSA PRIVATE KEY** ----- to -----**END RSA PRIVATE KEY-----**), and paste it into the original .pem file, replacing its private key with this RSA private key.  
        
      In other words, make sure that all the text from **-----BEGIN PRIVATE KEY-----** to **-----END PRIVATE KEY** (including the dashes) in the original .pem file is replaced with the contents of -----**BEGIN RSA PRIVATE KEY** ----- to -----**END RSA PRIVATE KEY-----** (including the dashes) from the RSA .pem file
   3. Save the original .pem file and close it. The certificate is now ready to be uploaded to the zero client.

**Import the Client Certificate into the Client User Account**

1. Log in to the Windows 2008 server.
2. Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. From the **View** menu, select **Advanced Features**.
4. Navigate to the user you created for the zero client.
5. Right-click the user, and then select **Name Mappings**.
6. In the **X.509 Certificates** section, click **Add**.
7. Locate and select the zero client certificate you exported that does not contain the private key (This file was saved to a network location in Step 9 of [Export the Client Certificate](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/07_HowTo/802.1x.htm#Export2).)
8. Leave both identity boxes checked, click **OK**, and then click **OK** again.

**Import the Certificates to Client Device**

To import the certificates into a profile using the Management Console (MC):

1. From a browser, enter the IP address of the MC web page, and then log in to the MC.
2. From the **Profiles** tab, click **Add New**, and then enter a name for the new profile.
3. Click**Save** to save the profile.
4. Click **Set Properties** to edit the new profile's configuration.
5. In the [**Certificate Store**](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/06_GUI_Reference/27_Config_Certificate/MC_Certificate.htm) category, click + to expand it, and then click **Add New**.
6. In the **Add Certificate to Store** dialog, click **Browse**, and then upload both the root CA certificate and the certificate with the private key.
7. For the zero client certificate, select **802.1X** from the drop-down list.
8. Expand the [**Security Configuration**](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/06_GUI_Reference/15_Config_Security/MC_Security_Settings.htm) category, and then click **Edit Properties**.
9. Select **Enable 802.1x Security**, and then set the value to **True**.
10. Select **802.1x Authentication Identity**, enter the user name you have defined for the zero client, and then click **Save**.
11. Apply this profile to the desired group.

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the zero client or remote workstation card.
2. From the AWI menu, select **Upload >**[**Certificate**](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/06_GUI_Reference/27_Config_Certificate/AWI_Certificate.htm).
3. Upload both the Root CA certificate and the certificate with the private key, using the **Browse** button to locate each certificate and the **Upload** button to upload them.
4. From the AWI menu, select**Configuration >**[**Network**](http://www.teradici.com/web-help/PCoIP_ZC_Host_Admin_HTML5/06_GUI_Reference/02_Config_Network/AWI_Network_Settings.htm).
5. Select **Enable 802.1x Security**.
6. Click the **Choose** button beside the **Client Certificate** field.
7. Select the certificate with the private key, and then click **Select**.
8. Enter the identity name of the certificate. Typically, this is the fully qualified domain name that appears after **Subject:** (e.g., "zeroclient@mydomain.local").

Note: For the identity, your Windows server may be configured to use the certificate's **Subject**, the **Subject Alternative Name**, or another field. Please check with your administrator.

1. Click **Apply**, and then **Reset**.

For more information about 802.1x, please see the following Knowledge Base topics on the [Teradici support site](http://techsupport.teradici.com/):

* Support for 802.1x on zero clients: 15134-590
* Setting up Windows Server 2008 R2 as an 802.1x authentication server: 15134-1245
* General 802.1x troubleshooting steps: 15134-928