Configuring 802.1x Network Device Authentication

https://teradici.com/web-help/pcoip_zero_client/tera2/20.10/config_8021x_network_device_authentication/

Configuring 802.1x Network Device Authentication¶

Setting	Default	AWI	OSD	Management Console
Enable 802.1x security				
Identity				
Authentication	TLS (this is the only available setting)			
Client Certificate				
Enable 802.1X Support for Legacy Switches				

This section describes the components you need to configure 802.1x authentication, and the detailed steps you need to follow to configure the authentication. The instructions provided in this topic were done on a Microsoft 2019 Datacenter. If you are performing these instructions from a different version of Microsoft Server you may have to consult your server documentation for any changes in procedures.

Preparing for 802.1x Configuration

¶

The supported 802.1x configuration has the PCoIP Zero Client pre-populated with a proper certificate. It then connects and presents the certificate to the 802.1x switch and is authenticated. PCoIP Zero Clients will also connect under a different configuration of the switch which has the MAC address of authorized endpoints stored in it's configuration.

Using certificates to sign other certificates

If a certificate is used to sign another certificate, it must have the digitalSignature key usage field enabled.

Before you begin the configuration process, make sure you have these components:

- Tera2 PCoIP Zero Client with firmware 5.x or newer
- PCoIP Management Console 2 or newer
- Windows Server 2019 with AD DS (Active Directory Domain Services)
- Windows Server 2019 with AD CS (Active Directory Certificate Services)
- Windows Server 2019 with NPS (Network Policy and Access Services)
- A switch with 802.1x support configured

Configuring Devices for 802.1x Authentication¶

To configure 802.1x device authentication, complete the following steps:

1. Create a 802.1x Client User.
2. Export the Root CA Certificate.
3. Create a Certificate Template for 802.1x Client Authentication.
4. Issue the 802.1x Client Certificate.
5. Export the 802.1x Client Certificate.
6. Convert the Certificate Format from .pfx to .pem.
7. Import the 802.1x Client Certificate into the Client User Account.

8. Import the Certificates to the 802.1x Client Device.

The following sections assume you are using Windows Server 2019 Datacenter

The instructions in the following sections are based on Windows Server 2019 Datacenter. If you are using a newer version of Windows Server, the steps may vary slightly.

Create a 802.1x Client User¶

In the Windows server, create a 802.1x client user.

Create a 802.1x Client User

1. Log in to the Windows server.
2. Click **Start > Windows Administrative Tools > Active Directory Users and Computers**.
3. Navigate to **Roles > Active Directory Domain Services > Active Directory Users and Computers > <your_domain.local> > Users**.
4. Right-click Users, select **New > User**, and follow the wizard.
   (Example: Create a user called pcoip_endpoint which would have a UPN name of pcoip_endpoint@<mydomain.local>)

Export the Root CA Certificate¶

In the Certificate Authority (CA) server, export the root CA certificate.

To export the root CA certificate:

1. Log in to the Certificate Authority (CA) server.
2. Open a Microsoft Management Console window (for example,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 **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 select **All Tasks > Export**.
8. Follow the wizard to export the certificate:
   1. Select **Base-64 encoded X.509 (.CER)** and click **Next**.

2. Click **Browse**, specify a name and location for the certificate, and then click **Save**.
3. Click **Finish**, and then click **OK**.

Create a Certificate Template for 802.1x Client Authentication¶

In the CA Server, create a certificate template for client authentication.

To 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 *Extensions* tab, ensure the **Digital signature** is included in the certificate **Key Usage**
   3. From the *General* tab, enter a name for the template (for example, **PCoIP Endpoint 802.1x**) and change the validity period to match the organization's security policy.
   4. From the *Request Handling* tab, select **Allow private key to be exported**.
   5. From the *Subject Name* tab, select **Supply in the request** and then click **OK**.
   6. From the *Security* tab, select the user who will be requesting the certificate, and give **Enroll** permission to this user.
   7. 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 (that is, **PCoIP Endpoint 802.1x**), and then click **OK**. The template will now appear in the *Certificate Templates* list.
8. Close the window.

Issue the 802.1x Client Certificate¶

From the CA Web Enrollment interface for the certificate server, issue the client certificate.

To issue the 802.1x client certificate:

Use Internet Explorer to log in to certificate server

Do not use any other browser except Internet Explorer to log into the certificate server or some options may not appear.

1. Using Internet Explorer on your local machine, go to your Certificate Authority URL using the format **https://<server&tgt/certsrv/** (for example, **https://ca.domain.local/certsrv/**).
2. Click **Request a certificate** and then click **advanced certificate request**.
3. Click **Create and submit a request to this CA**.
4. From 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 (for example, **PCoIP Endpoint 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.
    The other fields are not required.
    Enter the same name as the universal principal name of the client user
    The name you enter in the *Name* field must be the universal principal name (UPN) of the client user you created in Create a 802.1x Client User(for example, **pcoip_endpoint@mydomainlocal**)
    3. In the *Key Options* section, check **Mark keys as exportable**.
    4. In the *Additional Options* section, set the Request Format to **PKCS10**.
    5. If desired, enter a name in the *Friendly Name* field.
    6. Click **Submit**.
    7. From the *Certificate Issued* window, click the **Install this certificate** link.
    (This will save the certificate in the **Current User > Personal** store.)

Export the 802.1x Client Certificate

¶

From the machine on which you issued the certificate, export the client certificate.

To export the client certificate:

1. From the machine on which you issued the certificate, open a Microsoft Management Console window (for example, 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 click **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 select **All Tasks > Export**.

7. Follow the Certificate Export wizard to export the certificate by clicking **Next**:
    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 **Next**, **Finish**, and then click **OK**.
8. Repeat Steps 5 to 7 again to export the PCoIP endpoint 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 Domain Controller and imported into Active Directory.

Convert the Certificate Format from .pfx to .pem¶

Using OpenSSL, convert the certificate format from .pfx to .pem.

To convert the certificate format from .pfx to .pem:

1. Download and install Windows OpenSSL from **https://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 (C:\OpenSSL-Win32\bin), and enter the following command to convert the certificate format from **.pfx** to **.pem** where *<client_cert>* is the name of the **.pfx** certificate file you saved to your local machine.
   `openssl.exe pkcs12 -in <client_cert>.pfx -out <client_cert>.pem -nodes`
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 where is the name of the .pem certificate file you created in the previous step.
   `openssl.exe rsa –in <client_cert>.pem –out < client_cert>_rsa.pem`
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 PCoIP Endpoint 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.

RSA .pem file
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 PCoIP Endpoint.

Import the 802.1x Client Certificate into the Client User Account¶

In the Windows Domain Controller, import the client certificate into the client user account.

To import the 802.1x client certificate into the client user account:

1. Log in to the Windows Domain Controller.
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 PCoIP Endpoint.
5. Right-click the user, and select **Name Mappings**.
6. In the *X.509 Certificates* section, click **Add**.
7. Locate and select the PCoIP Endpoint certificate you exported that does not contain the private key (This file was saved to a network location in step 9 of Export the 802.1x Client Certificate.)
8. Make sure both identity boxes are selected and click **OK**, and then click **OK** again.

Import the Certificates to the 802.1x Client Device¶

From the PCoIP endpoint’s AWI, import the certificates.

To import the certificates into a profile using the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the PCoIP Endpoint.
2. From the AWI, select **Upload > Certificate**.
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 OSD or AWI, select **Configuration > Network**.
5. Select **Enable 802.1x Security**.
6. Click **Choose** 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 universal principal name (UPN) that appears after Subject: (for example, **pcoip_endpoint@mydomain.local**).
   Windows server may be configured to use the certificate's Subject, the Subject Alternative Name, or another field
   For the identity name, your Windows server may be configured to use the certificate's *Subject*, the *Subject Alternative Name*, or another field. Check with your administrator.
9. To enable greater 802.1x compatibility for older switches on the network, select **Enable 802.1X Support for Legacy Switches**. This setting is only available from the PCoIP endpoints AWI *Network* page.
10. Click **Apply**, and then click **Reset**.

Revision #1
Created 5 January 2024 04:56:01 by ColtM
Updated 7 August 2024 23:24:39 by ColtM