Securing Virtual Desktops with PCoIP® Zero Clients

TER1212005

Issue 1

PCoIP CONNECTED

TERADICI™

Teradici Corporation
#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada
p +1 604 451 5800 f +1 604 451 5818
www.teradici.com

Revision History

Version	Date	Description
1	January 25, 2013	Initial release.

Contents

Revision History ... 3

1 PCoIP® Zero Client Security Features ... 6

1.1 Introduction ... 6

1.2 Security Benefits for Enterprises and Users ... 6

1.2.1 Data Control ... 6

1.2.2 User Authentication ... 6

1.2.3 Encryption ... 7

1.2.4 802.1x Network Authentication ... 7

2 802.1x Network Device Authentication for PCoIP Zero Clients ... 8

2.1 Configuration Overview ... 8

2.1.1 Prerequisites ... 8

2.1.2 Procedure ... 8

2.2 Configuration Steps ... 9

2.2.1 Create a Zero Client User ... 9

2.2.2 Export the Root CA certificate ... 9

2.2.3 Create Certificate Template for Zero Client Authentication ... 9

2.2.4 Issue the Zero Client Certicate ... 9

2.2.5 Convert the Certificate Format from .pfx to .pem ... 10

2.2.6 Import the Zero Client Certificate into the Zero Client User Account ... 11

2.2.7 Import the Certificates to the Zero Client ... 11

3 Secure Network and Session Configuration for PCoIP zero clients ... 17

3.1 Configuration Overview ... 17

3.1.1 Prerequisites ... 17

3.1.2 PCoIP Zero Client Security Settings Checklist ... 17

3.2 Configuration Steps ... 19

3.2.1 Network Configuration: Disable SNMP ... 19

3.2.2 Discovery Configuration: Disable SLP Discovery ... 20

3.2.3 Session Configuration: Set the Session Connection Type ... 20

3.2.4 Session Configuration: Enable SSL support ... 21

3.2.5 Session Configuration: Set the Certificate Check mode ... 21

3.2.6 Session Configuration: Set the Certificate check lockout mode ... 22

3.2.7 Session Configuration: Set the Trusted Connection Server Cache ... 22

3.2.8 Session Configuration: Set the Connection Server Cache Mode ... 23

3.2.9 Session Configuration: Set the Connection Server Cache Entry ... 23

3.2.10 Session Configuration: Disabling the Username Caching ... 24

3.2.11 Session Configuration: Setting Smart Card Support ... 24

3.2.12 Encryption Configuration: Setting Encryption Types ... 25

3.2.13 OSD configuration: Hide Menu Entries ... 25

3.2.14 Time Configuration: Set the NTP Server ... 26

3.2.15 Security Configuration 26
3.2.16 Profile Zero Client USB Authorization /Unauthorization 27
3.2.17 Certificate Store: Upload a Certificate 28
3.3 Other Configuration 28

1 PCoIP® Zero Client Security Features

This document outlines the security benefits of PCoIP zero clients. It also describes how to configure 802.1x network authentication for PCoIP zero clients, and presents examples of security configuration settings commonly used in security-critical deployments.

1.1 Introduction

PCoIP zero clients are ultra-secure, easy to manage devices that offer the richest user experience in a VMware View® environment. PCoIP zero clients are based on the TERA chipset by Teradici and are available in a variety of form factors from a number of trusted OEMs. Form factors include standalone desktop devices, integrated monitors, touchscreen displays, and IP phones. With embedded hardware support for PCoIP and no local storage, PCoIP zero clients are the most trusted VDI client wherever security and performance are critical.

1.2 Security Benefits for Enterprises and Users

1.2.1 Data Control

When control and lockdown of sensitive data is a primary objective, PCoIP zero clients with VMware View enable an environment where no application data ever leaves the data center. The VM sends only encrypted PCoIP data to the client. PCoIP zero clients have no local storage, and no sensitive application data is ever processed or stored on the client.

1.2.2 User Authentication

PCoIP zero clients support a number of third-party, hardware-based, user authentication methods including:

- SIPR hardware tokens
- Common Access Card (CAC) and Personal Identity Verfication (PIV) smart cards
- SafeNet eToken models
- RSA SecurID
- Proximity cards
- Many others

For a complete list of supported user-authentication methods, see the KB article 15134-299 in the Teradici Knowledge Base.

1.2.3 Encryption

PCoIP zero clients support a variety of encryption types:

- **Session negotiation security**:
  - TLS 1.0 with AES-128-CBC-SHA
  - TLS 1.0 with AES-256-CBC-SHA
  - Suite B ciphers
- **Session security**:
  - AES-128-GCM
  - AES-256-GCM (with Tera2 processor)
  - Salsa20-256-Round12 (with Tera1 processor)

Zero clients employ encryption to ensure that data is protected:

- **Media stream**: All media data is encrypted as it moves from the server to the client. This includes display data, USB data, and audio network traffic.
- **Management channel**: All management data is encrypted.

1.2.4 802.1x Network Authentication

PCoIP zero clients support 802.1x network device authentication using EAP-TLS certificates. Under this method, all network end devices must be authenticated before they are granted access to the network.

This is a typical method of device authentication for high security environments, providing an additional layer of security beyond username and password credentials. The configuration of 802.1x is described in the next section.

2 802.1x Network Device Authentication for PCoIP Zero Clients

This section describes how to configure PCoIP zero clients for 802.1x network device authentication.

2.1 Configuration Overview

2.1.1 Prerequisites

An 802.1x authentication system with PCoIP zero clients 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

2.1.2 Procedure

Configuring 802.1x device authentication entails the following steps:

- In Active Directory:
  - Create a zero client user.
- In the Certificate Authority (CA) server:
  - Export the root CA certificate
  - Create a certificate template for zero client authentication
- From the SSL browser interface for the certificate server:
  - Issue the zero client certificate
- In Windows OpenSSL
  - Convert the certificate format from .pfx to .pem
- In Active Directory
  - Import the zero client certificate into the zero client user account
- From the zero client Management Console or the Administrator Web Interface:
  - Import the certificates

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.

2.2 Configuration Steps

2.2.1 Create a Zero Client User

1. Log in to **Active Directory**.
2. Click **Start**, **Administrative Tools**, and then **Server Manager**.
3. Expand **Roles**, **Active Directory Domain Services**, **Active Directory Users and Computers**, **e.g.“labbit.local”**, **Users**.
4. Right-click **Users**, select **New**, then **User**, and then follow the wizard.

2.2.2 Export the Root CA certificate

1. Log in to the CA server.
2. Click **Start**. In the Start Search field, type `mmc.exe`, and then press **Enter**.
3. Add the **Snap-in Certificates** for a Computer account.
4. Under **Certificates (Local Computer)**, click **Personal**, then click **Certificates**.
5. On the right panel, right-click the certificate (e.g. labbit Root CA), click **All Tasks**, then click **Export**.
6. Follow the wizard to export the certificate.

2.2.3 Create Certificate Template for Zero Client Authentication

1. Log in to the CA server.
2. Click **Start**, **Administrative Tools**, and then **Certification Authority**.
3. Expand the tree for your CA.
4. Right-click **Certificate Templates**, and then click **Manage**.
5. Right-click **Computer template**, and then click **Duplicate Template**.
6. Select **Windows Server 2003 Enterprise**, and click **OK**.
7. Click the **General** tab. Enter a name for the template (e.g. zero client 802.1x) and change the **Validity period** to match the organizations’ security policy.
8. Click the R**equest Handling** tab and select **Allow private key to be exported**.
9. Click the **Subject Name** tab, select **Supply in the request**, and then click **OK**.
10. Close the **Certificate Templates Console**.
11. Open the **Certificate Authority** again, right-click **Certificate Template**, select **New**, and then click **Certificate Template to Issue**.
12. Select the certificate (i.e. zero client 802.1x) you just created and then click **OK**.

2.2.4 Issue the Zero Client Certicate

NOTE: Use Internet Explorer to log into the SSL interface for the certificate server.

1. Start Internet Explorer and go to the CA URL: https://server/certsrv (e.g. https://ca.labbit.local/certsrv/).
2. Click **Request a Certificate**.

3. Click **Advanced Certificate Request**.
4. Click **Create** and submit a request to this CA.
5. Click **Yes** to popup window.
6. Under **Certificate Template**, select the certificate for zero clients (e.g. Zero Client 802.1x).
7. Fill in the fields in the **Identifying Information For Offline Template** section.
8. Under **Additional Options**, set the **Request Format** to **PKCS10**.
9. Enter a name in the **Friendly Name** field if you wish.
10. Click **Submit**, and click **Yes** to the warning popup.
11. Click **Install the Certificate**. When you see the success message, close the window.
12. Go to the CA server and open a Microsoft Management Console (MMC) console.
13. Click **File**, and then select **Add/Remove Snap-in**.
14. Add the Certificates snap-in, selecting Computer account for the local computer.
15. Expand **Certificates (Local User)**, **Personal**, **Certificates**.
16. Right click the certificate you created/installed. Select **All Tasks**, and click **Export**.
17. Click **Next**.
18. Select **Yes**, export the private key, and click **Next**.
19. Select **Personal Information Exchange** – PKCS #12 (PFX), leave the default settings, and click **Next**.
20. Enter a password, and then click **Next**.
21. Click the **Browse** button to enter a **Location** and a **File Name**.
22. Click **Next**, and then click **Finish**.

Repeat the same process without the private key selecting DER encoded binary X.509 (.CER).

2.2.5 Convert the Certificate Format from .pfx to .pem

For more information, see KB #927 in the Teradici Knowledge Base.

1. Download and install Windows OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.html (the light version is sufficient).
2. At a command prompt, enter the following:

   ```
   C:\OpenSSL-Win32\bin\openssl.exe pkcs12 -in <client_
   cert.pfx> -out <client_cert.pem> -nodes
   ```

   Note: The private key is protected with a passphrase.

3. Remove a passphrase from a private key. At a command prompt, enter the following:

   ```
   C:\OpenSSL-Win32\bin\openssl.exe rsa -in <client_cert.pem>
   -out < client_cert_rsa_key.pem>
   ```

Note: For <client_cert_rsa_key.pem> only include the RSA private key (without the passphrase).

4. Manually cut and paste the RSA private key into your original certificate (<client_cert.pem>) replacing the old private key.

   Make sure the "-----BEGIN PRIVATE KEY-----" and "-----END PRIVATE KEY-----" are replaced with "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" as well.

2.2.6 Import the Zero Client Certificate into the Zero Client User Account

1. Log in to Active Directory.
2. Click **Start**, **Administrative Tools**, and then **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 select **Name Mappings**.
6. On **X.509 certificates**, click **Add**.
7. Find and select the certificate you exported that does not contain the private key.
8. Leave both identity boxes checked and click **OK**, then click **OK** again.

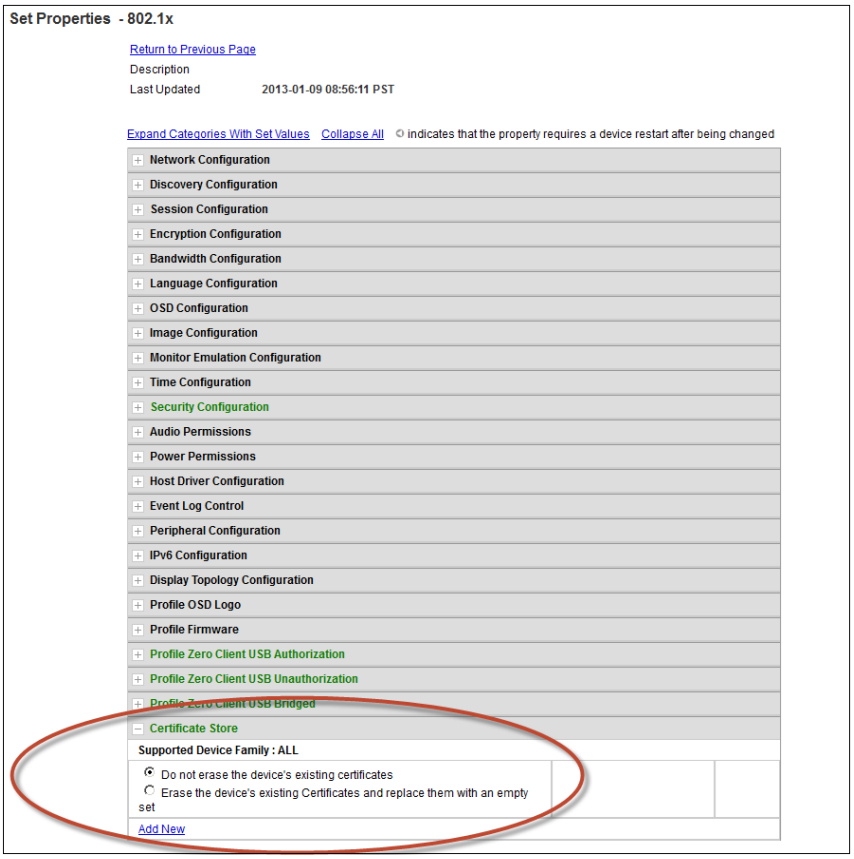
2.2.7 Import the Certificates to the Zero Client

You can import the certificates to the zero client using either the PCoIP Management Console (MC) or the Aministrator Web Interface (AWI):

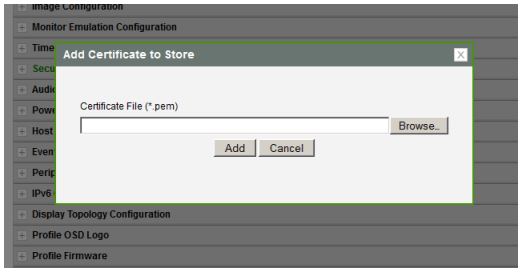
To import certificates using the MC:

1. From an Internet browser, enter the IP address of the MC web page, and then log in to the MC.
2. Click the **Profiles** tab.
3. Click **Add New**, and enter with a name for the new profile, then click **Save**.
4. Click **Set Properties** to change the new profiles configuration.

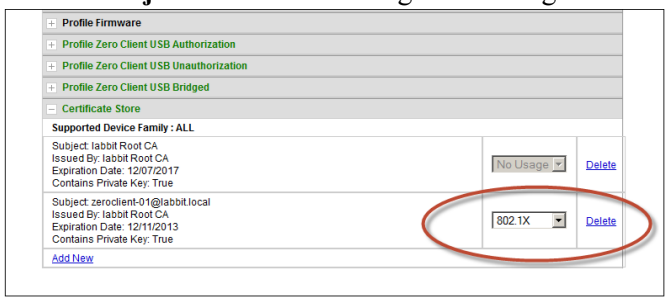
5. Click + to expand the **Certificate Store** category, then click **Add New**.



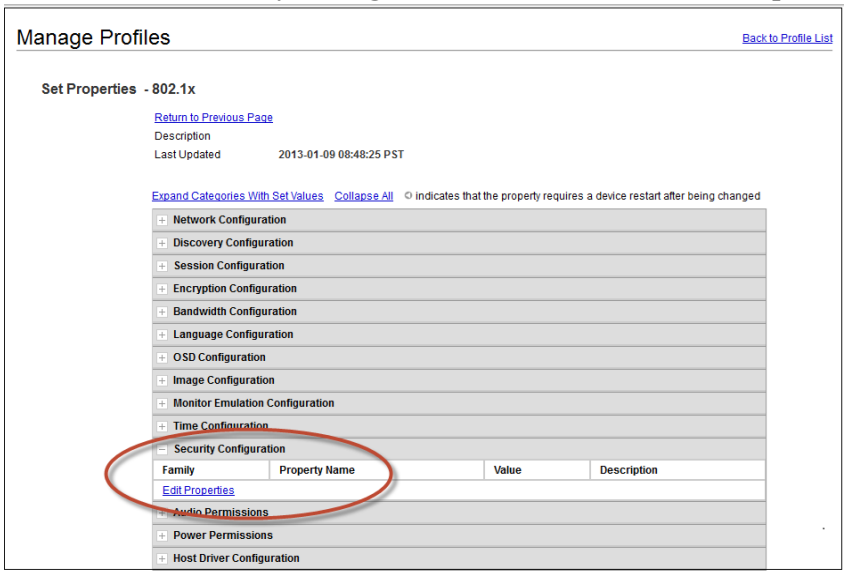
6. On the **Add Certificate to Store** dialog box, click **Browse** to upload both the Root CA certificate and the certificate with the private key.



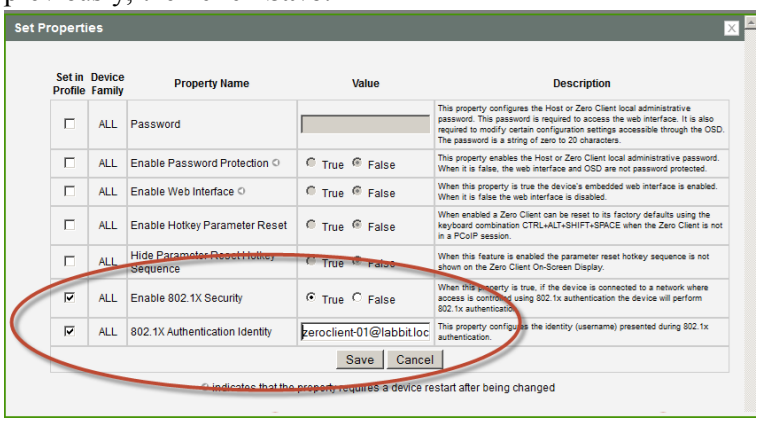
7. For the **Subject zero client** change the setting from **No Usage** to **802.1X**.



8. Click + beside **Security Configuration**, and then click **Edit Properties**.



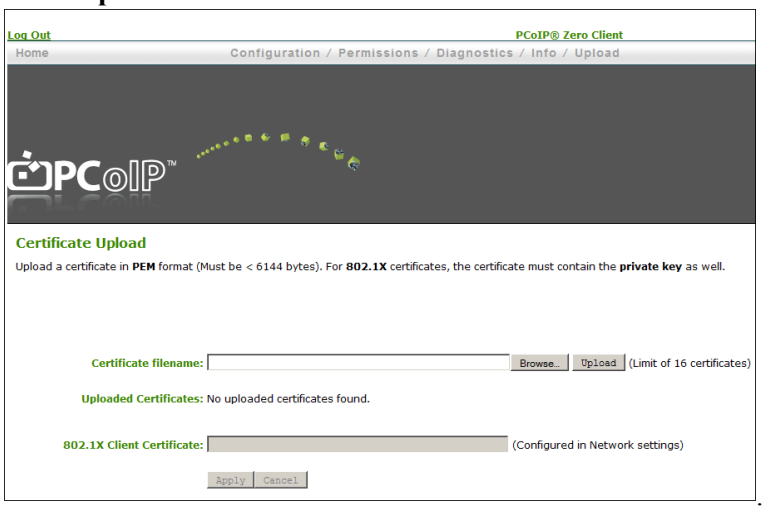
9. Select **Enable 802.1x Security** and set the value to **True**.
10. Select **802.1x Authentication Identity**. Enter the user name you have defined previously, then click **Save**.



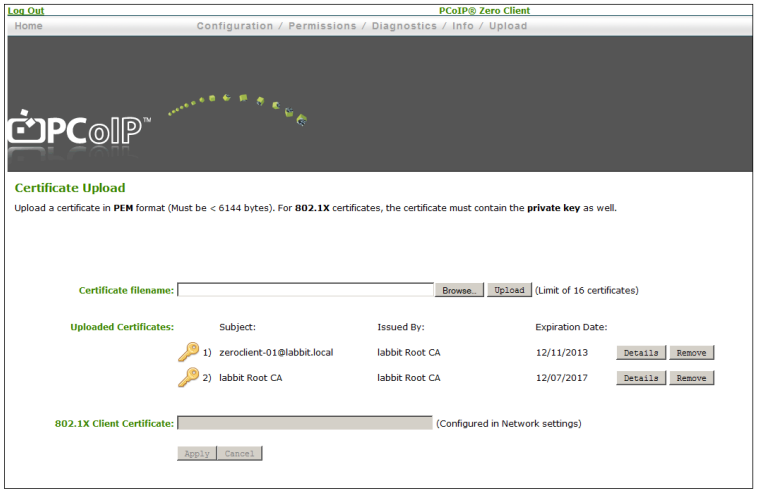
11. Apply the profile to a desired group.

To import certificates using the AWI:

1. From an Internet browser, enter the IP address of the client, and then log in to the AWI.
2. Click **Upload** and then select **Certificate**

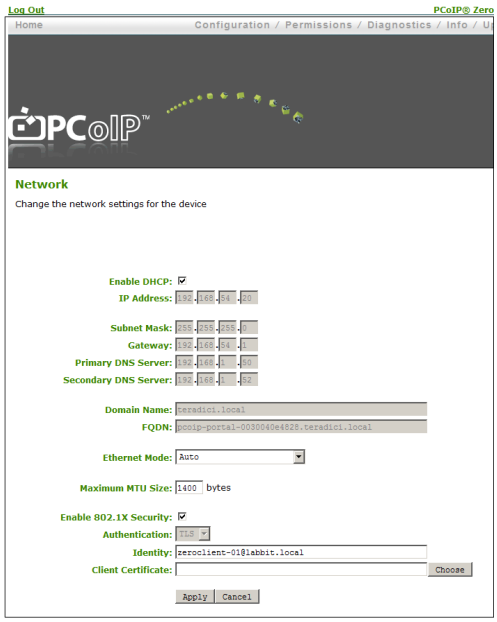


3. Upload both the Root CA certificate and the certificate with the private key.

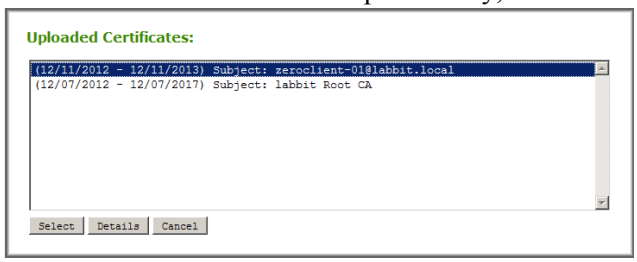


4. Click **Configuration** and then click **Network**.
5. Select **Enable 802.1x Security**.
6. Click the **Choose** button beside the **Client Certificate** field.

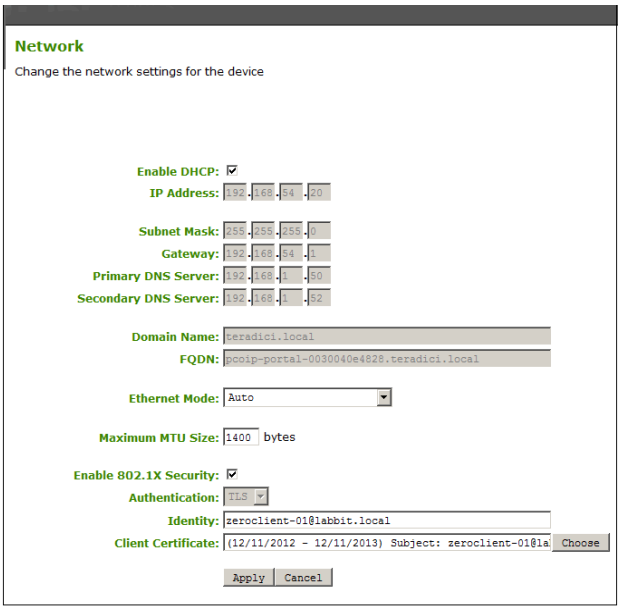
7. Fill out the identity to match the certificate subject.



8. Select the certificate with the private key, and then click **Select**.



9. Click **Apply**, and then click **Reset**.


Network
Change the network settings for the device
Enable DHCP:
IP Address: 192 . 168 . 54 . 20
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 54 . 1
Primary DNS Server: 192 . 168 . 1 . 50
Secondary DNS Server: 192 . 168 . 1 . 52
Domain Name: teradici.local
FQDN: pcoip-portal-0030040e4828.teradici.local
Ethernet Mode: Auto
Maximum MTU Size: 1400 bytes
Enable 802.1X Security:
Authentication: TLS
Identity: zeroclient-01@labbit.local
Client Certificate: (12/11/2012 - 12/11/2013) Subject: zeroclient-01@la
Choose
Apply
Cancel

3 Secure Network and Session Configuration for PCoIP zero clients

This section presents a list of PCoIP zero client security settings that are frequently used in high security deployments. Your network administrator or your security advisor must determine whether these settings are appropriate for your own network environment.

The instructions in this section describe how to configure your security settings using the PCoIP Management Console (MC). Many–but not all–of these settings can also be configured through the On Screen Display (OSD) or the Administrative Web Interface (AWI).

3.1 Configuration Overview

3.1.1 Prerequisites

- PCoIP zero client with firmware 4.0.3 or newer
- PCoIP Management Console 1.8.1 or newer

3.1.2 PCoIP Zero Client Security Settings Checklist

The table below lists a set of example security settings that are frequently used in high security environments. For more information about any of these settings, see the TER1206003 PCoIP Zero Client and Host Adminstrator's Guide.

Configuration Category	Setting Name	Setting
Network Configuration	Enable SNMP	False
Discovery Configuration	Enable SLP Discovery	False
Session Configuration	Session Connection Type	View Connection Server
	Certificate Check Mode	Reject the unverifiable connection (Secure)
	Certificate Check Lockout Mode	Locked
	Clear Trusted Connection Server Cache	Clear Cache
	Connection Server Cache Mode	Last servers used

Configuration Category	Setting Name	Setting
	Connection Server Cache Entry (1-25)	Enter the allowed VCS address(es)
	Enable Login Username Caching	False
	Prefer GSC-IS Over PIV Endpoint	True
Encryption Configuration	Session Negotiation Security Level	Maximum Compatibility - in software or mixed host environments Suite B - in hardware-only host card environments
	T2 Enable AES-128-GCM	True
	T2 Enable AES-256-GCM	True
	T1 Enable AES-128-GCM	True
	T1 Enable Salsa20-256-Round12	True - in software or mixed host environments False - in hardware-only host card environments
OSD Configuration	Hidden Menu Entries	Hide menus (as desired)
Time Configuration	NTP Server Hostname	<NTP server address>
Security Configuration	Password	Create a password in accordance with the local security policy
	Enable Password Protection	True. This enables password protection for the AWI and the OSD.
	Enable Web Interface	False (disable the web UI if desired)
	Enable Hotkey Parameter Reset	False
	Enable 802.1x Security	True

Configuration Category	Setting Name	Setting
Profile Zero Client USB Authorization /Unauthorization	Example: To allow USB access to HID devices only.	**Authorized**: **Device Class**: Human Interface Device **Sub Class**: Any **Protocol**: Any **Unauthorized**: - No unauthorization rules. Delete any existing rules. When there are no rules, the MC displays two radio buttons. Select **Erase the device's existing USB unauthorizations and replace them with an empty set**.
	Example: To allow USB access to all devices except mass storage, use these settings.	**Authorized**: **Device Class**: Any , **Sub Class**: Any , **Protocol**: Any **Unauthorized**: **Device Class** Mass Storage **Sub Class**: Any **Protocol**: Any
Certificate Store		VCS certificate issuer (root or intermediate) or VCS certificate. Note that SSL certificates are required in VMware View 5.1 and newer versions. If SSL is turned off in firmware version FW4.0 and older, passwords are sent unencrypted over the network.

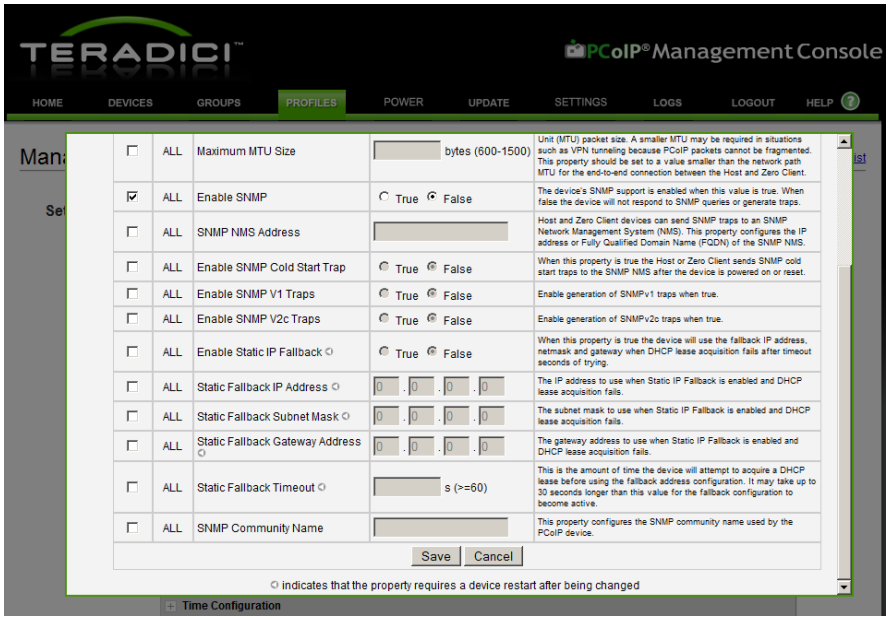
3.2 Configuration Steps

This section provides step-by-step instructions for configuring the security settings that are frequently used in high security deployments.

To use the Management Console (MC), open an Internet browser, enter the IP address of the MC web page, and then log in to the MC.

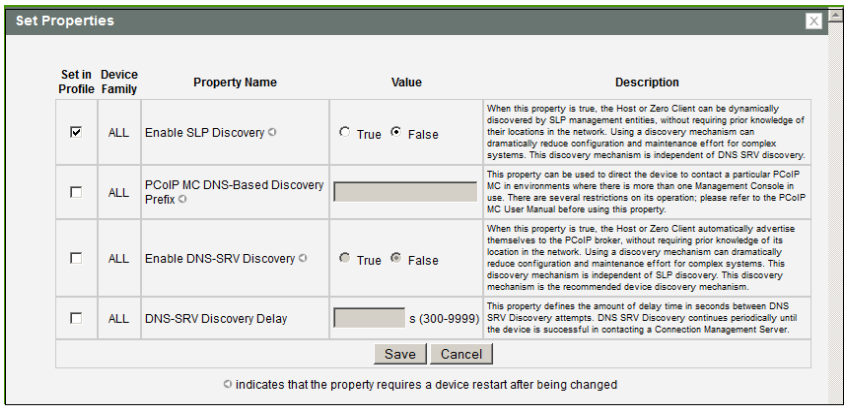
3.2.1 Network Configuration: Disable SNMP

1. Expand the **Network Configuration** category.
2. Click **Edit Properties**.
3. Select **Enable SNMP** and set the value to **False**.
4. Click the **Save** button.



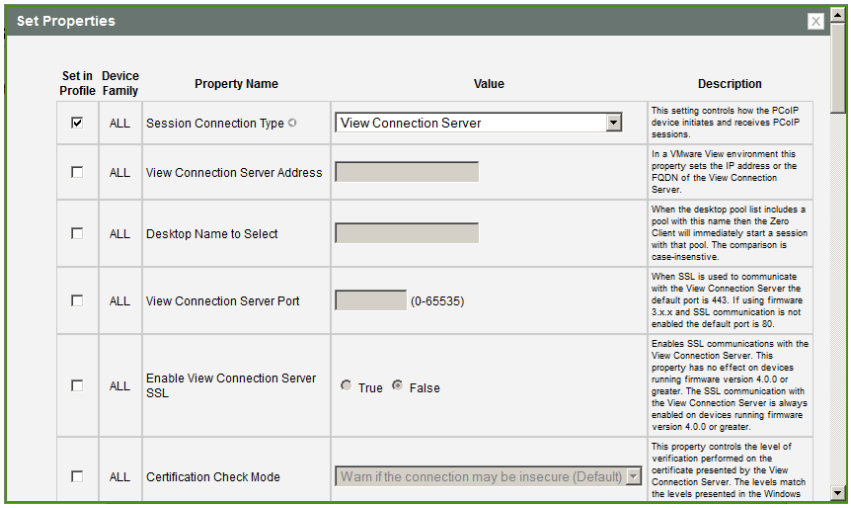
3.2.2 **Discovery Configuration:** Disable SLP Discovery

1. Expand the **Discovery Configuration** category.
2. Click **Edit Properties**.
3. Select **Enable SLP Discovery** and set the value to **False**.
4. Click the **Save** button.



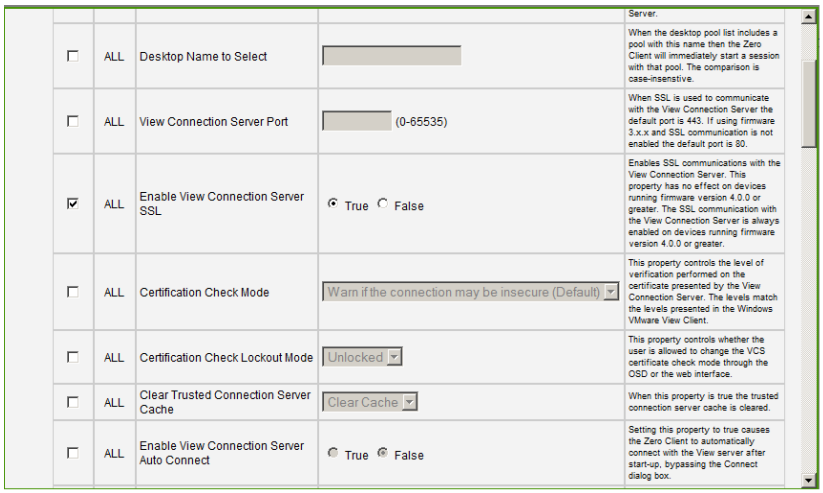
3.2.3 **Session Configuration:** Set the Session Connection Type

1. Expand the **Session Configuration** category.
2. Click **Edit Properties**.
3. Select **Session Connection Type** and the select **View Connection Server** from the drop-down list.
4. Click the **Save** button.



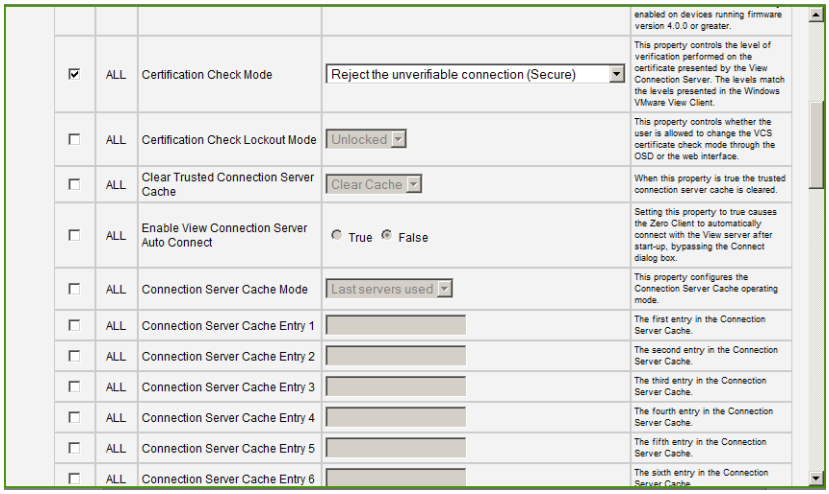
3.2.4 Session Configuration: Enable SSL support

1. Expand the **Session Configuration category**.
2. Click **Edit Properties**.
3. Select **Enable View Connection Server SSL** and set the value to **True**.
4. Click the **Save button**.



3.2.5 Session Configuration: Set the Certificate Check mode

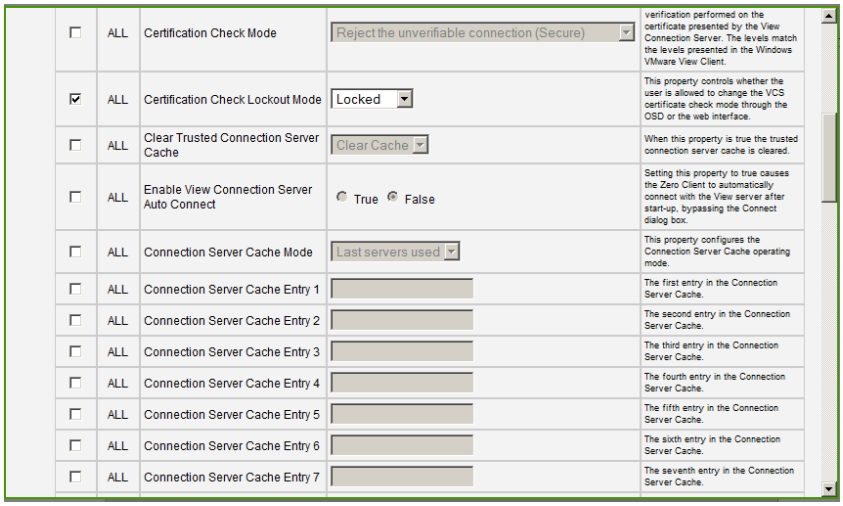
1. Expand the **Session Configuration** category.
2. Click **Edit Properties**.
3. Select **Certification Check Mode** and set the value to **Reject the unverifiable connection (Secure)**.
4. Click the **Save** button.



				enabled on devices running firmware version 4.0.0 or greater.
☑	ALL	Certification Check Mode	Reject the unverifiable connection (Secure)	This property controls the level of verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client.
☐	ALL	Certification Check Lockout Mode	Unlocked	This property controls whether the user is allowed to change the VCS certificate check mode through the OSD or the web interface.
☐	ALL	Clear Trusted Connection Server Cache	Clear Cache	When this property is true the trusted connection server cache is cleared.
☐	ALL	Enable View Connection Server Auto Connect	○ True ◉ False	Setting this property to true causes the Zero Client to automatically connect with the View server after start-up, bypassing the Connect dialog box.
☐	ALL	Connection Server Cache Mode	Last servers used	This property configures the Connection Server Cache operating mode.
☐	ALL	Connection Server Cache Entry 1		The first entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 2		The second entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 3		The third entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 4		The fourth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 5		The fifth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 6		The sixth entry in the Connection Server Cache.

3.2.6 **Session Configuration:** Set the Certificate check lockout mode

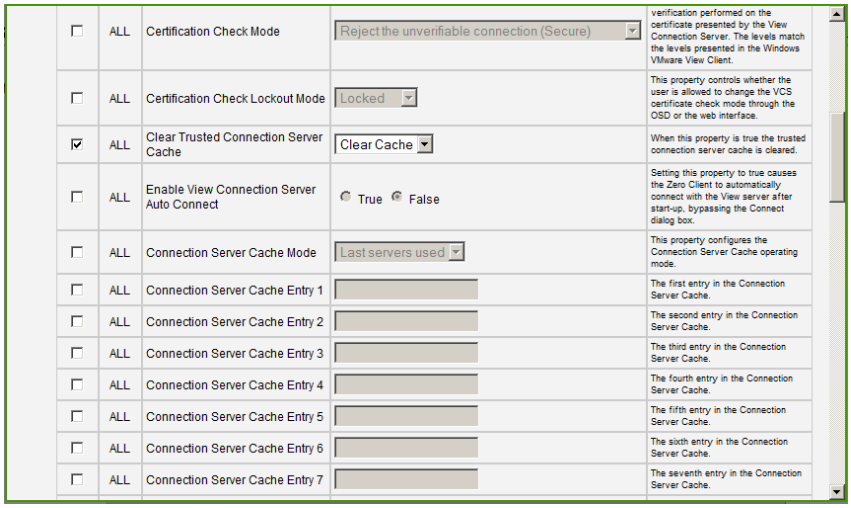
1. Expand the **Session Configuration** category.
2. Click **Edit Properties**.
3. Select **Certification Check Lockout Mode** and set the value to **Locked**.
4. Click the **Save** button.



☐	ALL	Certification Check Mode	Reject the unverifiable connection (Secure)	verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client.
☑	ALL	Certification Check Lockout Mode	Locked	This property controls whether the user is allowed to change the VCS certificate check mode through the OSD or the web interface.
☐	ALL	Clear Trusted Connection Server Cache	Clear Cache	When this property is true the trusted connection server cache is cleared.
☐	ALL	Enable View Connection Server Auto Connect	○ True ◉ False	Setting this property to true causes the Zero Client to automatically connect with the View server after start-up, bypassing the Connect dialog box.
☐	ALL	Connection Server Cache Mode	Last servers used	This property configures the Connection Server Cache operating mode.
☐	ALL	Connection Server Cache Entry 1		The first entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 2		The second entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 3		The third entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 4		The fourth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 5		The fifth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 6		The sixth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 7		The seventh entry in the Connection Server Cache.

3.2.7 **Session Configuration:** Set the Trusted Connection Server Cache

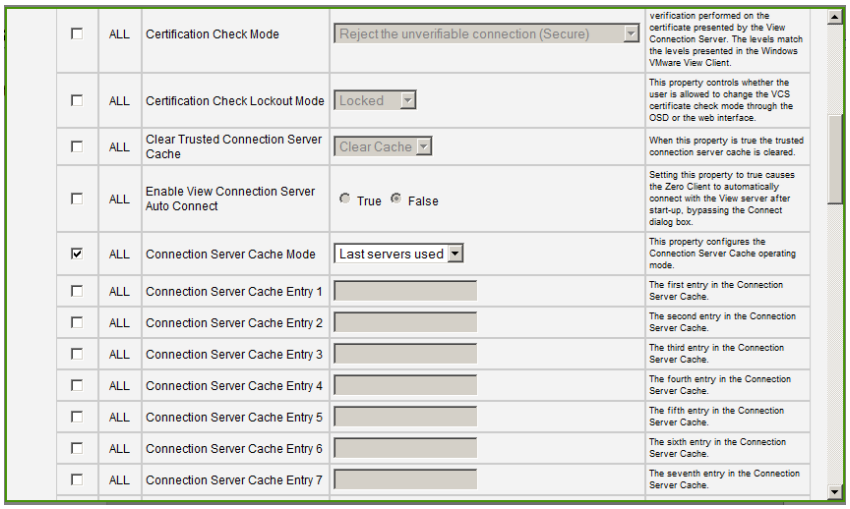
1. Expand the **Session Configuration** category.
2. Click **Edit Properties**.
3. Select **Certification Trusted Connection Sever Cache** and set the value to **Clear Cache**.
4. Click the **Save** button.



☐	ALL	Certification Check Mode	Reject the unverifiable connection (Secure)	verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client.
☐	ALL	Certification Check Lockout Mode	Locked	This property controls whether the user is allowed to change the VCS certificate check mode through the OSD or the web interface.
☑	ALL	Clear Trusted Connection Server Cache	Clear Cache	When this property is true the trusted connection server cache is cleared.
☐	ALL	Enable View Connection Server Auto Connect	○ True ◉ False	Setting this property to true causes the Zero Client to automatically connect with the View server after start-up, bypassing the Connect dialog box.
☐	ALL	Connection Server Cache Mode	Last servers used	This property configures the Connection Server Cache operating mode.
☐	ALL	Connection Server Cache Entry 1		The first entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 2		The second entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 3		The third entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 4		The fourth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 5		The fifth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 6		The sixth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 7		The seventh entry in the Connection Server Cache.

3.2.8 **Session Configuration:** Set the Connection Server Cache Mode

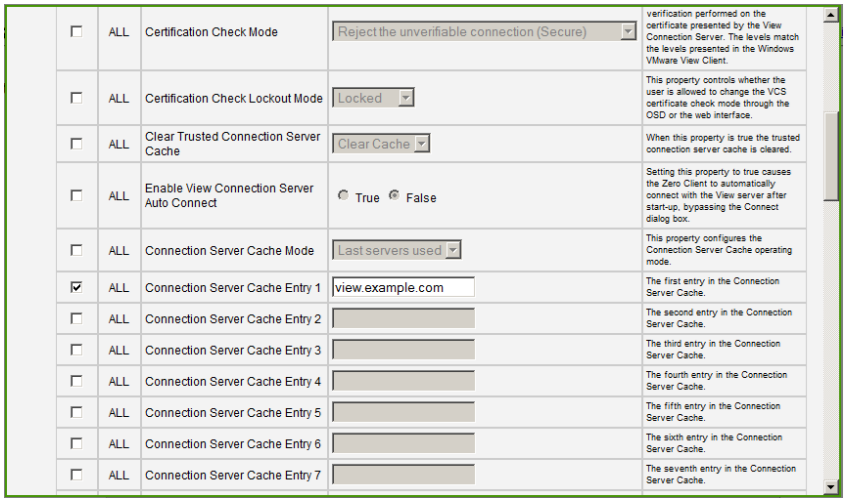
1. Expand the **Session Configuration** category.
2. Click **Edit Properties**.
3. Select **Connection Server Cache Mode** and set the value to **Last servers used**.
4. Click the **Save** button.



☐	ALL	Certification Check Mode	Reject the unverifiable connection (Secure)	verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client.
☐	ALL	Certification Check Lockout Mode	Locked	This property controls whether the user is allowed to change the VCS certificate check mode through the OSD or the web interface.
☐	ALL	Clear Trusted Connection Server Cache	Clear Cache	When this property is true the trusted connection server cache is cleared.
☐	ALL	Enable View Connection Server Auto Connect	○ True ◉ False	Setting this property to true causes the Zero Client to automatically connect with the View server after start-up, bypassing the Connect dialog box.
☑	ALL	Connection Server Cache Mode	Last servers used	This property configures the Connection Server Cache operating mode.
☐	ALL	Connection Server Cache Entry 1		The first entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 2		The second entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 3		The third entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 4		The fourth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 5		The fifth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 6		The sixth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 7		The seventh entry in the Connection Server Cache.

3.2.9 **Session Configuration:** Set the Connection Server Cache Entry

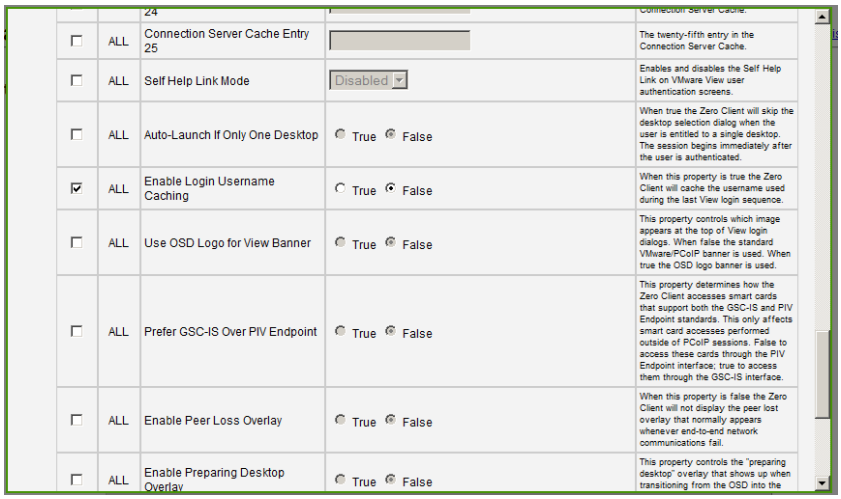
1. Expand the **Session Configuration** category.
2. Click **Edit Properties**.
3. Select **Connection Server Cache Entry(s)** and enter with the value or values of the View connection server address(es).
4. Click the **Save** button.



☐	ALL	Certification Check Mode	Reject the unverifiable connection (Secure)	verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client.
☐	ALL	Certification Check Lockout Mode	Locked	This property controls whether the user is allowed to change the VCS certificate check mode through the OSD or the web interface.
☐	ALL	Clear Trusted Connection Server Cache	Clear Cache	When this property is true the trusted connection server cache is cleared.
☐	ALL	Enable View Connection Server Auto Connect	○ True ◉ False	Setting this property to true causes the Zero Client to automatically connect with the View server after start-up, bypassing the Connect dialog box.
☐	ALL	Connection Server Cache Mode	Last servers used	This property configures the Connection Server Cache operating mode.
☑	ALL	Connection Server Cache Entry 1	view.example.com	The first entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 2		The second entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 3		The third entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 4		The fourth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 5		The fifth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 6		The sixth entry in the Connection Server Cache.
☐	ALL	Connection Server Cache Entry 7		The seventh entry in the Connection Server Cache.

3.2.10 Session Configuration: Disabling the Username Caching

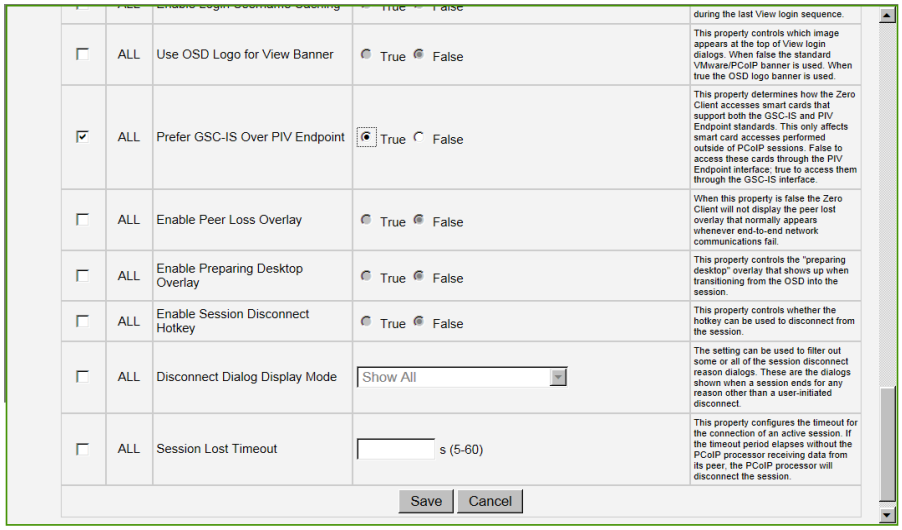
1. Expand the Session Configuration category.
2. Click **Edit Properties**.
3. Select **Enable Login Username Caching** and set the value to **False**.
4. Click the **Save** button.



☐	ALL	Connection Server Cache Entry 25		The twenty-fifth entry in the Connection Server Cache.
☐	ALL	Self Help Link Mode	Disabled	Enables and disables the Self Help Link on VMware View user authentication screens.
☐	ALL	Auto-Launch If Only One Desktop	○ True ◉ False	When true the Zero Client will skip the desktop selection dialog when the user is entitled to a single desktop. The session begins immediately after the user is authenticated.
☑	ALL	Enable Login Username Caching	○ True ◉ False	When this property is true the Zero Client will cache the username used during the last View login sequence.
☐	ALL	Use OSD Logo for View Banner	○ True ◉ False	This property controls which image appears at the top of View login dialogs. When false the standard VMware/PCoIP banner is used. When true the OSD logo banner is used.
☐	ALL	Prefer GSC-IS Over PIV Endpoint	○ True ◉ False	This property determines how the Zero Client accesses smart cards that support both the GSC-IS and PIV Endpoint standards. This only affects smart card accesses performed outside of PCoIP sessions. False to access these cards through the PIV Endpoint interface; true to access them through the GSC-IS interface.
☐	ALL	Enable Peer Loss Overlay	○ True ◉ False	When this property is false the Zero Client will not display the peer lost overlay that normally appears whenever end-to-end network communications fail.
☐	ALL	Enable Preparing Desktop Overlay	○ True ◉ False	This property controls the "preparing desktop" overlay that shows up when transitioning from the OSD into the

3.2.11 Session Configuration: Setting Smart Card Support

1. Expand the Session Configuration category.
2. Click **Edit Properties**.
3. Select **Prefer GSC-IS Over PIV Endpoint** and set the value to **True**.
4. Click the **Save** button.

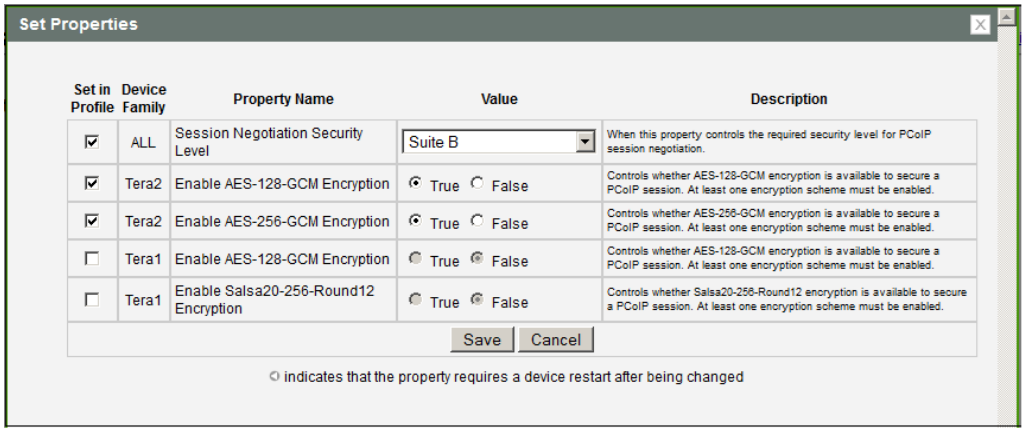


				during the last View login sequence.
☐	ALL	Use OSD Logo for View Banner	○ True ◉ False	This property controls which image appears at the top of View login dialogs. When false the standard VMware/PCoIP banner is used. When true the OSD logo banner is used.
☑	ALL	Prefer GSC-IS Over PIV Endpoint	◉ True ○ False	This property determines how the Zero Client accesses smart cards that support both the GSC-IS and PIV Endpoint standards. This only affects smart card accesses performed outside of PCoIP sessions. False to access these cards through the PIV Endpoint interface; true to access them through the GSC-IS interface.
☐	ALL	Enable Peer Loss Overlay	○ True ◉ False	When this property is false the Zero Client will not display the peer lost overlay that normally appears whenever end-to-end network communications fail.
☐	ALL	Enable Preparing Desktop Overlay	○ True ◉ False	This property controls the "preparing desktop" overlay that shows up when transitioning from the OSD into the session.
☐	ALL	Enable Session Disconnect Hotkey	○ True ◉ False	This property controls whether the hotkey can be used to disconnect from the session.
☐	ALL	Disconnect Dialog Display Mode	Show All	The setting can be used to filter out some or all of the session disconnect reason dialogs. These are the dialogs shown when a session ends for any reason other than a user-initiated disconnect.
☐	ALL	Session Lost Timeout	s (5-60)	This property configures the timeout for the connection of an active session. If the timeout period elapses without the PCoIP processor receiving data from its peer, the PCoIP processor will disconnect the session.

Save Cancel

3.2.12 Encryption Configuration: Setting Encryption Types

1. Expand the **Encryption Configuration** category.
2. Click **Edit Properties**.
3. Select **Session Negotiation Security Level** and set the value to **Suite B**.
4. Select **Enable AES-128-GCM Encryption** and set the value to **True**.
5. Select **Enable AES-256-GCM Encryption** and set the value to **True**.
6. Click the **Save** button.



Set Properties

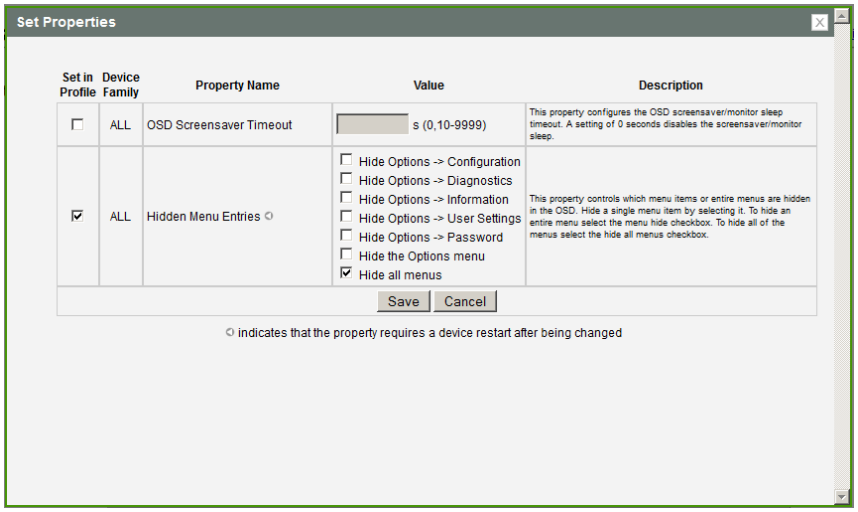
Set in Profile	Device Family	Property Name	Value	Description
☑	ALL	Session Negotiation Security Level	Suite B	When this property controls the required security level for PCoIP session negotiation.
☑	Tera2	Enable AES-128-GCM Encryption	◉ True ○ False	Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
☑	Tera2	Enable AES-256-GCM Encryption	◉ True ○ False	Controls whether AES-256-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
☐	Tera1	Enable AES-128-GCM Encryption	○ True ◉ False	Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
☐	Tera1	Enable Salsa20-256-Round12 Encryption	○ True ◉ False	Controls whether Salsa20-256-Round12 encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.

Save Cancel

○ indicates that the property requires a device restart after being changed

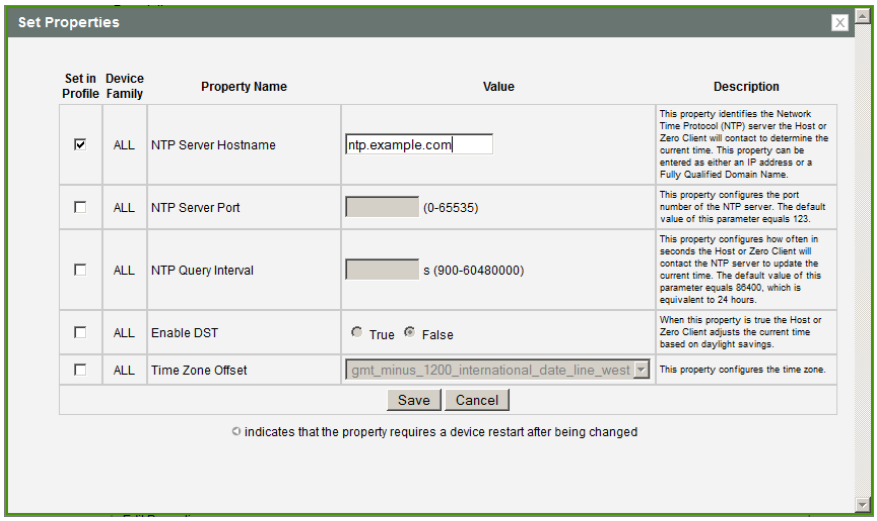
3.2.13 OSD configuration: Hide Menu Entries

1. Expand the **OSD Configuration** category.
2. Click **Edit Properties**.
3. Select **Hidden Menu Entries**, and select the menu items you want to hide.
4. Click the **Save** button.



3.2.14 Time Configuration: Set the NTP Server

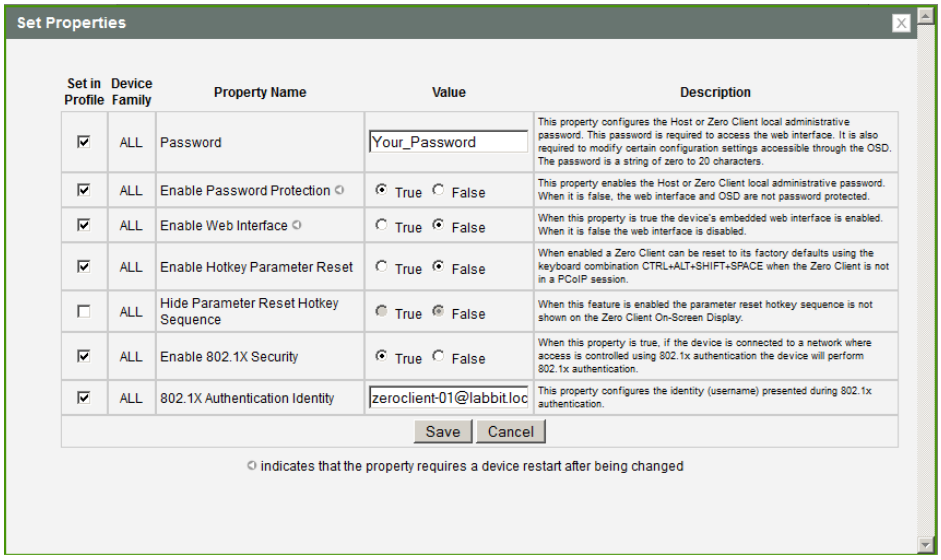
1. Expand the **Time Configuration** category.
2. Click **Edit Properties**.
3. Select **NTP Server Hostname** and enter the **Value** with your NTP server hostname or IP address.
4. Click the **Save** button.



3.2.15 Security Configuration

1. Expand the **Security Configuration** category.
2. Click **Edit Properties**.
3. Select **Password** and enter with a desired password for the **Value**.
4. Select **Enable Password Protection** and set the value to **True**.
5. Select **Enable Web Interface** and set the value to **False**.
6. Select **Enable Hotkey Parameter Reset** and set the value to **False**.

7. Select **Enable 802.1X Security** and set the value to **True**.
8. Select **802.1X Authentication Identity** and enter with a username configured for the 802.1X authentication.
9. Click the **Save** button.

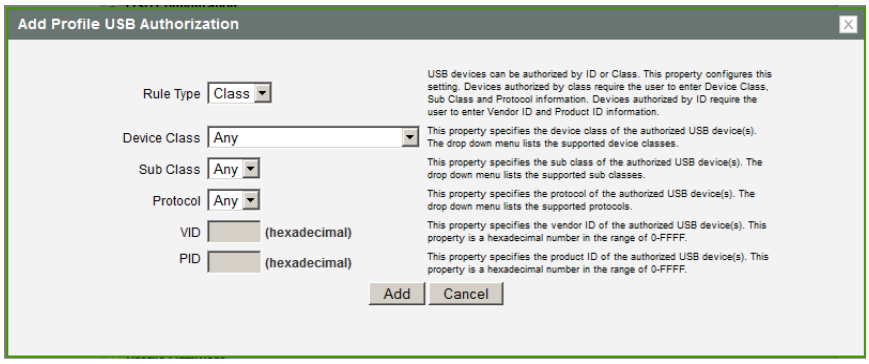


3.2.16 Profile Zero Client USB Authorization /Unauthorization

1. To allow USB access to all devices except mass storage:
2. Expand the **Profile Zero Client USB Authorization** category.
3. Click **Edit Properties**.
4. Configure as below:

   Rule Type Class
   Device Class Any
   Sub Class Any
   Protocol Any

5. Click the Add button.

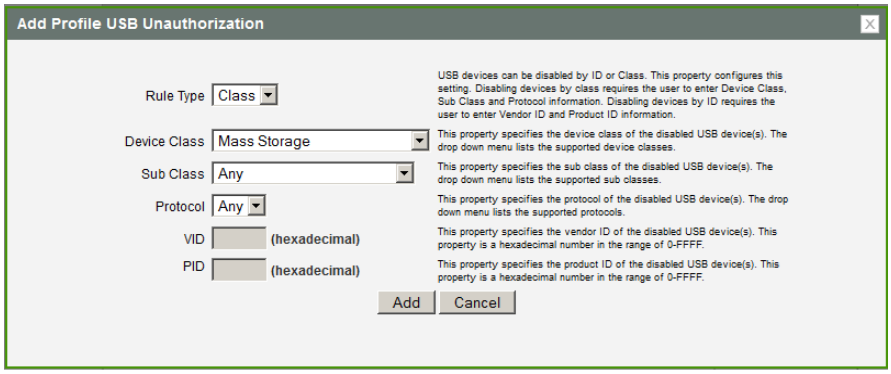


6. Expand the **Profile zero client USB Unauthorization category**.

7. Click **Edit Properties**.
8. Configure as below:

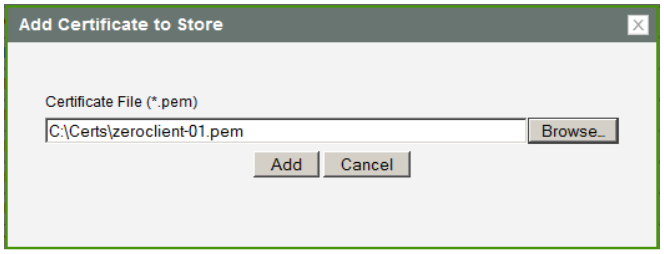
   Rule Type Class
   Device Class Mass Storage
   Sub Class Any
   Protocol Any

9. Click the **Add** button.



3.2.17 **Certificate Store:** Upload a Certificate

1. Expand the **Certificate Store** category.
2. Click **Add New**.
3. Click the **Browse** button and select or enter a location for the certificate file (.pem).
4. Click the **Add** button.



3.3 Other Configuration

For SIPR Hardware Token User Authentication with PCoIP zero clients there is no configuration on the zero client side.