Dell Wyse ThinOS Lite Release 2.6

Administrator's Guide

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2018 - 11

Rev. A00

Contents

1

Introduction

The Dell Wyse ThinOS Lite family of products are zero clients built for Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) and Citrix Virtual Apps (formerly XenApp) environments. These products represent an entirely new approach in delivering virtual desktops. ThinOS Lite zero clients deliver a Citrix HDX experience with zero delays, zero management, zero security risks, and almost zero energy use. Users will benefit from an instant-on, plug-n-play, high performance zero client while administrators can have following privileges such as virus resistant, hands-off, self-updating zero client deployed.

About this Guide

This guide is intended for administrators of thin clients running ThinOS Lite. It provides information and detailed system configurations to help you design and manage a ThinOS Lite environment.

Supported Products

This guide is intended for the following Dell Wyse ThinOS Lite products:

- Wyse 5010 zero client for Citrix (D00DX) (ThinOS Lite Pro 2)
- Wyse 3010 zero client for Citrix (T00X) (ThinOS Lite 2)
- Wyse 3020 zero client for Citrix (T00DX) (ThinOS Lite 3)
- R00LX (ThinOS Lite Pro)
- C00X (ThinOS Lite)

Finding the Information You Need in this Guide

You can use either the Search window or Find toolbar to locate a word, series of words, or partial word in an active PDF document. For detailed information on using these features, refer to the Help in your PDF reader.

Technical Support

To access technical resources self-service portal, knowledge base, software downloads, registration, warranty extensions/ RMAs, reference manuals, and so on, visit www.dell.com/wyse/support . For Customer Support, visit www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus , and phone numbers for Basic and Pro Support are available at www.dell.com/supportcontacts.

NOTE: Before proceeding, verify if your product has a Dell service tag. For Dell service tagged products, go to www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse.

What is new in this release

The following are the updates or new features in this release:

- **Citrix updates**:
  - Updated the Citrix RTME package to version 2.5. See, Citrix HDX RealTime Multimedia Engine—RTME.
  - Added support for Okta using Citrix NetScaler Gateway. See, Okta Integration through Citrix NetScaler.
- **Enhancements**:

- UI enhancement to configure the IPv4 settings for a wireless connection. See, Configure the WLAN settings.
- UI enhancement to allow user to connect to a remote host or device using the Telnet client. See, Using the troubleshooting options.
- UI enhancement to verify the version of the installed packages and generate logs. See, Accessing system information.
- UI enhancement on the Wyse Device Manager console to display the device details of peripheral devices connected to the ThinOS client. For more information, see the *Dell Wyse Device Manager Administrator's Guide* at www.dell.com/support.
- Added support for Caradigm Way2Care. See, Caradigm Way2Care enhancement.
- Added support for Vertical Synchronization to eliminate screen tearing. See, Vertical Synchronization.

- **INI parameter updates**:

  Added new INI parameters. See, Parameters for a xen.ini file.

2

Before working on ThinOS Lite

This section contains information about firmware upgrade and system configuration that you need to know before using ThinOS Lite version 2.6.

Firmware upgrade

Firmware upgrade is the process of updating your existing ThinOS Lite firmware version to the latest version. To upgrade the ThinOS Lite firmware, use any of the following:

- File Transfer Protocol (FTP) Windows server
- HTTP/HTTPS Windows server
- Wyse Management Suite version

NOTE: Ensure that you are enrolled in our Software Maintenance Program and are eligible to receive new versions of ThinOS Lite software and subsequent releases of corresponding documentation uploaded on Dell Digital Locker.

IMPORTANT: To avoid uncertain issues, ensure that when you upgrade your firmware, you do not skip versions.

Table 1. Firmware images

Platform	ThinOS Lite
Wyse 5010 zero client for Citrix	ZD00_xen
Wyse 3020 zero client for Citrix	T00D_xen
Wyse 3010 zero client for Citrix	T00_xen.bin

Table 2. BIOS Binary

Platform	BIOS file
Wyse 5010 zero client for Citrix	D10G_bios.bin
Wyse 3020 zero client for Citrix	Not available
Wyse 3010 zero client for Citrix	Not available

Table 3. Package information

Package name	Details
Base.i386.pkg	Automatically updated upon firmware upgrade.
RTME.i386.pkg	Upload the new package to central configuration, and system can update without the need of INI configuration.
FR.i386.pkg	Upload the new package to central configuration, and configure the INI parameter for update this package.

Firmware upgrade using FTP server

Ensure that you have set up a Windows PC or Server with Microsoft Internet Information Services (IIS) and FTP services installed. If you do not have the FTP server installed, then refer to the article about how to setup an FTP server at support.microsoft.com.

Installing the Windows IIS creates the directory **C:\inetpub\ftproot**, which is known as the FTP root. In the **ftproot** directory, create a folder **wyse** and a sub folder **xen**. The directory structure must read as **C:\inetpub\ftproot\WYSE\xen**.

To upgrade the ThinOS Lite firmware using FTP server:

1. Go to www.dell.com/support.
2. Download the latest ThinOS Lite firmware and latest ThinOS Lite packages that corresponds to your thin client model. If the firmware and packages are in the form of a compressed self-extracting (.EXE) or zipped file (.ZIP), then extract the files.
3. Place the extracted firmware files in the **C:\inetpub\ftproot\WYSE\xen** folder, and the packages to **C:\inetpub\ftproot\WYSE\xen \pkg** on your FTP server.
4. Create a xen.ini text file (using a text editor) in the **C:\inetpub\ftproot\WYSE\xen** folder with the following INI parameters:

   `Autoload=2 loadpkg=1 Addpkg=FR`

   The option `Autoload=2`, ensures that the thin client uses the firmware installed on the server to upgrade, only if the firmware on the thin client is older than the version on the server. The option `LoadPkg` specifies how to update the external packages. If `LoadPkg` is not in the statement, it will inherit the value of `AutoLoad`.

   Base package is integrated into the ThinOS Lite firmware image. Installing the latest ThinOS Lite firmware image automatically installs the latest version of these packages on the ThinOS Lite client. If you set `AutoLoad=1 LoadPkg=0`, the firmware is checked, but the packages are not checked. The packages check is performed after firmware check. From ThinOS Lite 2.3, the external packages update mechanism is changed. Some packages are default, and loaded according to value of `LoadPkg`. For example RTME. Some packages need additional parameter `AddPkg` to add. For example, FR. The option `AddPkg` is for adding packages. It depends on the value of `LoadPkg`. For more information about the INI parameter usage, see the INI parameter chapter in the Dell Wyse ThinOS Lite admin guide.
5. Save the xen.ini file.
6. On the ThinOS Lite client desktop, navigate to **System Setup** > **Central Configuration** > **General**.
7. In the **General** tab, enter the IP address of the FTP server or directory. For example: **150.00.0.260/wyse**. The **Username** field must have the value `Anonymous` and the **Password** field is already pre-configured.

   NOTE:

   - If there is no default password or if the password is changed, then you must set your password. For example, abe@abc.com.

     You can also reset the thin client to factory default settings. When you reset the thin client to factory default settings, the anonymous user is configured with the default password. However, you need to reconfigure the thin client.
   - You can also use DHCP option tags 161 and 162 to configure the ThinOS Lite client, file server and path information. You must create these options on your DHCP server, configure them with the correct server information, and enable the DHCP server scope in your environment.
8. Click **OK**.
9. Restart the thin client and wait until the auto-installation of packages is complete.

To verify that the thin client is upgraded, on the ThinOS Lite desktop, navigate to **System Information** > **General**, and check the System Version.

Firmware upgrade using HTTP or HTTPS

Ensure that you have set up a Windows PC or Server with Microsoft Internet Information Services (IIS) and HTTP or HTTPS services installed. If you do not have the HTTP or HTTPS server installed, then refer to the article about how to setup an HTTP or HTTPS server at support.microsoft.com.

Ensure that the web server can identify the file types used by ThinOS Lite. Create two MIME types under IIS. The MIME's option needs to be configured on a per site basis. On a default IIS, install:

1 Launch the IIS admin console.
2 Browse to the default website, right-click and select **Properties**.
3 Click the **HTTP Headers** tab, and in the **MIME Map** section, select **File types** > **New Type**.
4 Add the two MIME types. Use **.INI** and **.** for the associated extension fields.
5 Apply the settings and close the IIS admin console.

Installing IIS creates the default directory **C:\inetpub\WWWroot**, which is known as the WWW root. In the **WWWroot** directory, create a folder **WYSE** and a sub folder **xen**. The directory structure must read as **C:\inetpub\wwwroot\WYSE\xen**.

To upgrade the ThinOS Lite firmware using HTTP or HTTPS server:

1 Go to www.dell.com/support.
2 Download the latest ThinOS Lite firmware and latest ThinOS Lite packages that corresponds to your thin client model. If the firmware and packages are in the form of a compressed self-extracting (.EXE) or zipped file (.ZIP), then extract the files.
3 Place the extracted firmware files in the **C:\inetpub\wwwroot\WYSE\xen** folder, and the packages to **C:\inetpub\wwwroot\WYSE\xen\pkg** on your HTTP or HTTPS server.
4 Create a xen.ini text file (using a text editor) in the **C:\inetpub\wwwroot\WYSE\xen** folder with the following INI parameters:

   ```
   Autoload=2 loadpkg=1 Addpkg=FR
   ```

   The option `Autoload=2`, ensures that the thin client uses the firmware installed on the server to upgrade, only if the firmware on the thin client is older than the version on the server. The option `LoadPkg` specifies how to update the external packages. If `LoadPkg` is not in the statement, it will inherit the value of `AutoLoad`.

   Base package is integrated into the ThinOS Lite firmware image. Installing the latest ThinOS Lite firmware image automatically installs the latest version of these packages on the ThinOS Lite client. If you set `AutoLoad=1 LoadPkg=0`, the firmware is checked, but the packages are not checked. The packages check is performed after firmware check. From ThinOS Lite 2.3, the external packages update mechanism is changed. Some packages are default, and loaded according to value of `LoadPkg`. For example RTME. Some packages need additional parameter `AddPkg` to add. For example, FR, Horizon, and TCX. The option `AddPkg` is for adding packages. It depends on the value of `LoadPkg`. For more information about the INI parameter usage, see INI parameter chapter in Dell Wyse ThinOS Lite Admin Guide.
5 Save the xen.ini file.
6 On the ThinOS Lite client desktop, navigate to **System Setup** > **Central Configuration** > **General**.
7 In the **General** tab, enter the IP address of the file server or directory. For example: **https://IPaddress/wyse**.

   NOTE: You can also use DHCP option tags 161 and 162 to configure the ThinOS Lite client, file server and path information. You must create these options on your DHCP server, configure them with the correct server information, and enable the DHCP server scope in your environment.
8 Click **OK**.
9 Restart the thin client and wait until the auto-installation of packages is complete.

Firmware upgrade using Wyse Management Suite version 1.1

Ensure that you have created a custom group and assigned the ThinOS Lite devices to that group in Wyse Management Suite—see Wyse Management Suite v1.1 Administrator's Guide.

Ensure that your ThinOS Lite clients are registered to Wyse Management Suite. See, Configuring the WDA settings.

To upgrade the ThinOS Lite firmware using Wyse Management Suite:

1 Go to www.dell.com/support.
2 Download the latest ThinOS Lite firmware and ThinOS Lite packages that corresponds to your thin client model.
3 Log in to Wyse Management Suite using valid credentials.
4 On the **Apps & Data** page, in the **OS Image Repository** section, click **ThinOS**.

5 Click **Add Firmware File**.

The **Add File** dialog box is displayed.

6 Browse and select the downloaded firmware file. Enter an appropriate description.

7 Click **Upload**.

The ThinOS Lite firmware file is uploaded, and the firmware file is listed on the **Apps & Data - ThinOS Lite OS Image Repository** page.

8 Select the check box that corresponds to your ThinOS Lite firmware file.

9 On the **Groups & Configs** page, select a custom group, and click **Edit Policies** > **ThinOS**.

The **Select ThinOS Lite Configuration Mode** screen is displayed.

10 Click **Advanced Configuration**.

11 In the **Device Configuration** pane, click **Firmware Upgrade**, and then click **Configure this item**.

12 From the **Platform type** drop-down list, select your thin client model.

13 From the **Firmware to auto deploy** drop-down list, select the firmware file that corresponds to your thin client model.

14 Click **Save & Publish**.

The thin client restarts, and the firmware version is upgraded.

System configuration and deployment

- ThinOS BIOS policy can be configured using Wyse Management Suite Console, Wyse Management Suite group INI, Wyse Management Suite advanced settings and FTP INI. Dell recommends that you use any one of the methods to configure the BIOS policy. Setting the BIOS policy simultaneously using different methods may cause a policy mismatch, and the device reboots repeatedly. This reboot loop issue is observed when you select the **reboot immediately** option in the **BIOS policy** settings section on the Wyse Management Suite console.
- All the installed packages are deleted when you update the ThinOS Lite version between major releases—2.5 to 2.6—using FTP, WDM, or Wyse Management Suite.

  Solution for updating firmware using FTP and WDM—Ensure that you have set the PKG install parameters in the WNOS.ini, and the pkg files are uploaded in the directory. After the device reboot, the packages are re-installed automatically.

  Solution for updating firmware using Wyse Management Suite—Wyse Management Suite App policy works only once after the policy is created. The deleted package cannot be reinstalled using the same policy. Dell recommends that you create a new App policy to install the package after the firmware update is complete.
- WDM vulnerability is fixed in this release. You must configure either the DHCP or the DNS option/record of the WDM server fingerprint to automatically fetch and validate the fingerprint before checking in to the WDM server. However, there is no impact to the ThinOS Lite device functionality if you do not to configure the fingerprint validation environment. For more information about how to set up fingerprint using WDM, see the *Dell Wyse ThinOS Lite Version 2.6 Administrator's Guide* at www.dell.com/support.

How to set up fingerprint using Wyse Device Manager

To set up your fingerprint using WDM, do the following:

1 Export the WDM server certificate from the WDM server that you want to access.

2 Extract the fingerprint value from the WDM certificate in the required format.

You must use a system with OpenSSL installed. OpenSSL can be used to extract the fingerprint in required format from the WDM certificate itself.

The fingerprint is generated from the following command:

```
openssl x509 -in <your certificate name>.crt -pubkey -noout | openssl pkey -pubin -outform
der | openssl dgst -sha256 -binary | openssl enc -base64
```

NOTE: If cert.crt is in DER format instead of the PEM format, you must add `-inform` to the first command. The certificate supports SHA256 in base64 encoded format.

3 Configure either the DHCP option or the DNS TXT record.

- If you want to use the DHCP option, configure the following option tags defined in the DHCP server:

- Option ID—200
- Name—WDM_Fingerprint
- Type—String

- If you want to use the DNS TXT record, enter the name as **WDM_Fingerprint**, and provide the fingerprint string value.

NOTE: If the DNS TXT record for fingerprint cannot be retrieved, the device fetches the values from the DHCP scope option. If the fingerprint certificate is already available, the device checks in to the WDM server. If the connection fails, the failure logs are registered on the zero client.

Central Configuration—Automating Updates and Configurations

This appendix describes how to set up your environment to provide your zero clients running ThinOS Lite with automatic updates and configurations in the following procedures.

NOTE: Dell Wyse zero clients do not require device management software. They are configured to obtain their IP address, as well as the location of firmware and configuration instructions, from a DHCP server. However, you can use Wyse Device Manager (WDM) or Wyse Management Suite for a more hands-on management of your zero clients. For information about configuring your zero clients to communicate with a WDM server or Wyse Management Suite, see the related INI parameters in Dell Wyse ThinOS INI Guide.

3

Getting started

Use the following information to quickly learn the basics and get started using your zero client:

- Connecting to a Remote Server
- Using Your Desktop
- Configuring Zero Client Settings and Connection Settings
- Connecting to a Monitor
- Connecting to a Printer
- Locking the Zero Client
- Signing Off and Shutting Down
- Additional Getting Started Details

ThinOS Lite supports the headless mode that enables you to boot the operating system without a monitor.

ThinOS Lite is centrally managed and configured using INI files to automatically push updates and any desired default configuration to all supported zero clients in your environment. For more information, see Central Configuration: Automating Updates and Configurations.

If no INI files are detected, you can use local dialog boxes on each zero client to make available configurations. ThinOS Lite saves many of these locally configured settings such as resolution, mouse, and keyboard to persist after reboot. However, once INI files are detected, rebooting causes ThinOS Lite to become stateless while ignoring locally configured settings after a reboot and then the settings contained in the INI file will be used.

Configuring ThinOS Lite using First Boot Wizard

First Boot Wizard runs the first time you start a new thin client. The thin client launches the out-of-box experience application before you enter the ThinOS Lite desktop, and allows you to perform a set of tasks, such as, configuring system preferences, setting up the internet connectivity, loading USB configurations, configuring management software, and configuring broker connections. The thin client configures settings that are applied during the first-boot experience, and processes before your log into ThinOS Lite. If you are an existing thin client user, and you have upgraded to ThinOS Lite v2.5 or later, then you can reset your thin client to factory default settings to enter First Boot Wizard.

The following flowcharts represent the First Boot Wizard workflow:

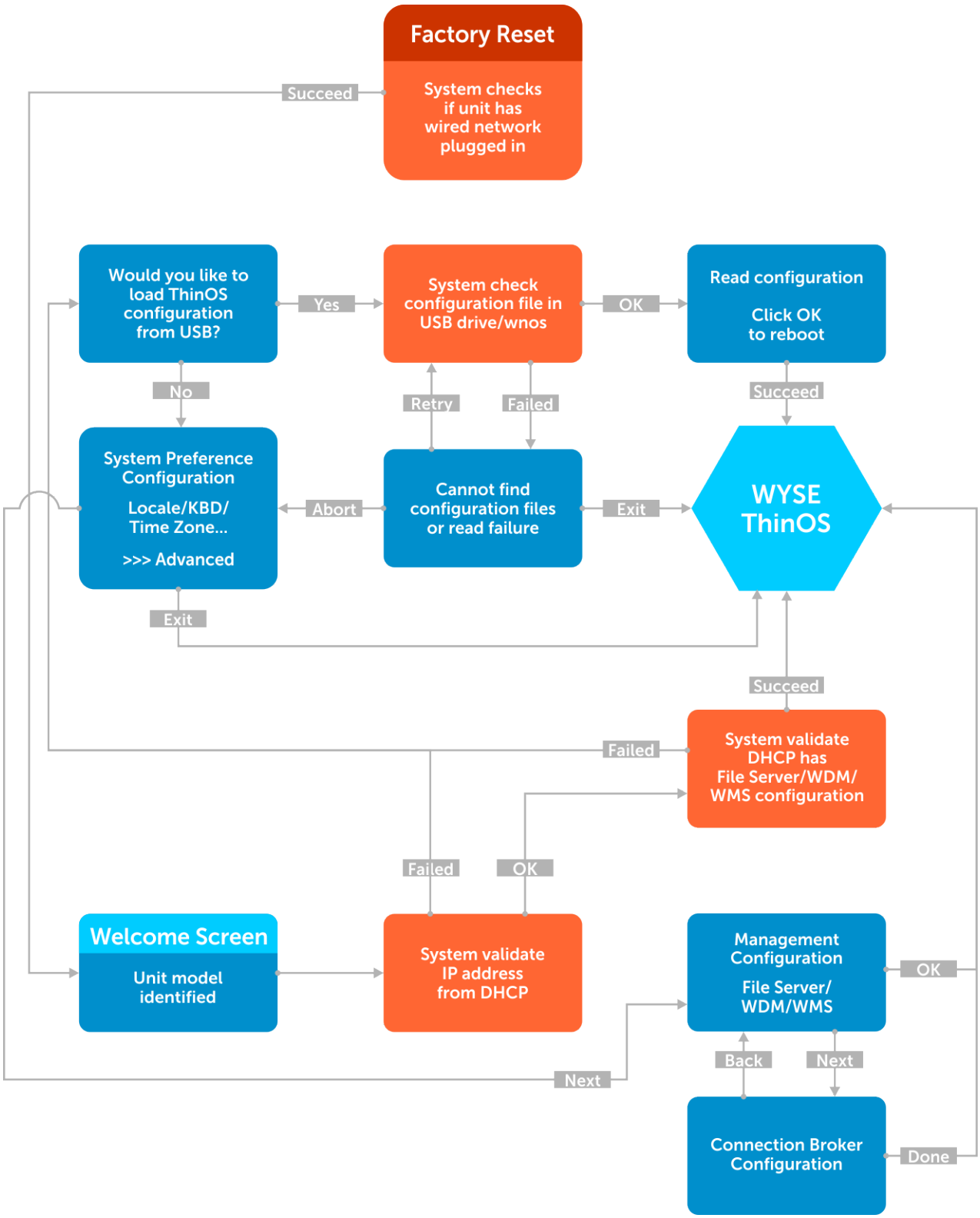


Figure 1. First Boot Wizard_Success

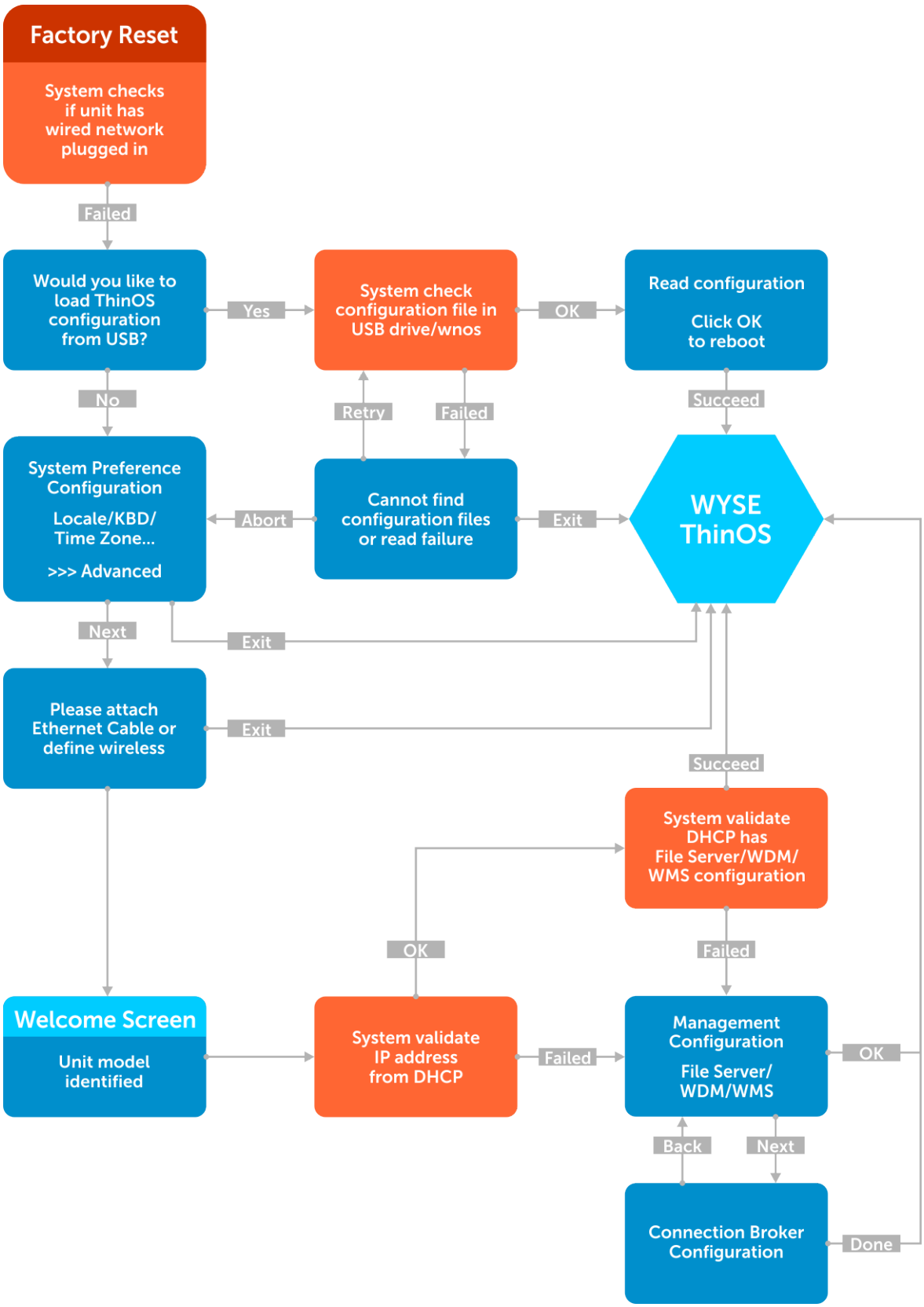


Figure 2. First Boot Wizard _Failure

1 Connect a new zero client or existing zero client to the Ethernet using a wired connection. The existing zero client must be reset to factory default settings to enter First Boot Wizard.

2 Turn on your zero client.

The zero client checks for a wired network connection. If the network connection is successful, a welcome screen with the model name of your zero client is displayed.

The zero client validates the IP address from DHCP. If the DHCP contains the file server or Wyse Device Manager or Wyse Management Suite configurations, then the ThinOS Lite system desktop is loaded without entering First Boot Wizard. If the DHCP validation fails or if you have not connected to Ethernet, then follow the next step.

NOTE: To exit First Boot Wizard during the network connection status check on the welcome screen, press the Ctrl + Esc key.

3 On the **Would you like to load a ThinOS Lite configuration file from USB?** screen, do either of the following:

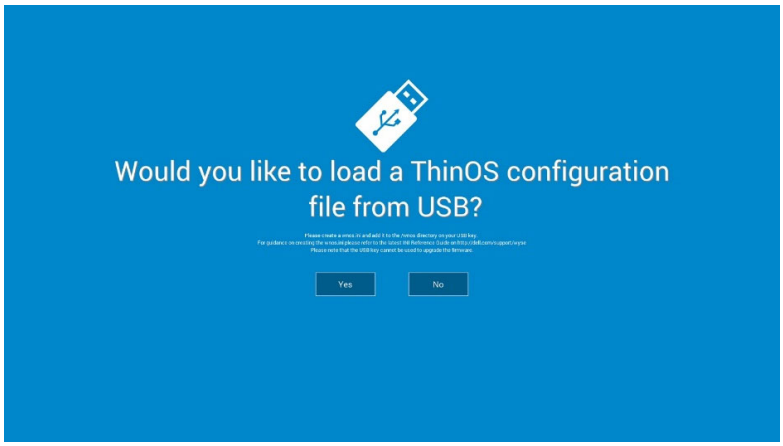


Figure 3. USB configuration

- To load a ThinOS Lite configuration file from the USB drive, ensure that you create a xen.ini file and add the file to the **/xen directory** on the USB drive. Plug the USB drive to zero client, and click **Yes**.

  NOTE:
  Only FAT, FAT32, and ExFAT file systems on the USB disk are supported. NTFS file system is not supported.

  The zero client validates the configuration file in the USB drive.

  – If the ThinOS Lite configuration file in the USB drive is correct, the **Read configuration success** message is displayed. Click **OK** to exit First Boot Wizard, and log in to ThinOS Lite system desktop.
  – If the ThinOS Lite configuration file in the USB drive is corrupted or the required file is not available, then the **Can not find configuration files, or read configuration failure message** is displayed. Upload the correct file on the USB drive, plug the USB drive again, and then click **Retry**. If the file is correct, the **Read configuration success** message is displayed. Click **OK** to exit First Boot Wizard, and log in to ThinOS Lite system desktop.

    If you do not want to use the **Retry** option to load the ThinOS Lite configuration file, then click **Abort** to enter the **System Preferences configuration** setup.

    NOTE: To exit the Can not find configuration files, or read configuration failure message screen, and load the ThinOS Lite system desktop, click Exit.

- To enter the **System Preferences configuration** setup, click **No**.

4 On the **System Preferences Configuration** screen, configure the following options:

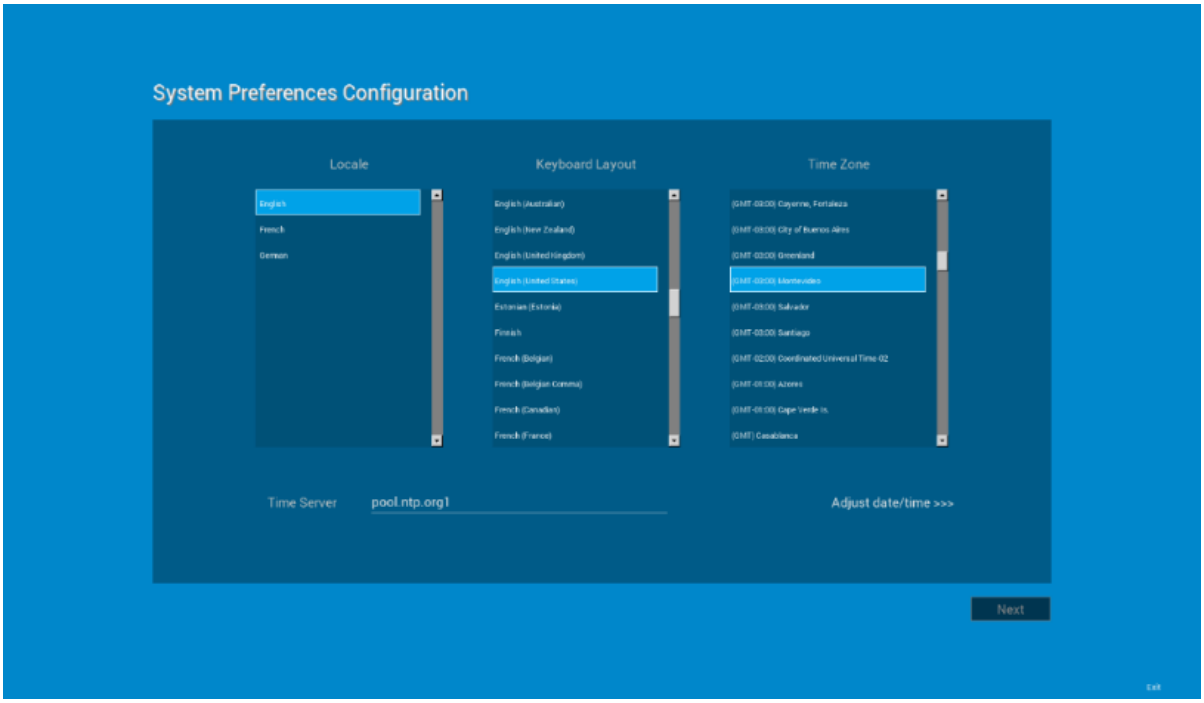


Figure 4. System preferences configuration

- **Locale**—Select a language to start ThinOS Lite in the regional specific language.
- **Keyboard Layout**—Select a keyboard layout to set the keyboard layout in the regional specific language.
  Time Zone—Select a time zone to set the time zone for your zero client.
- **Time Server**—Displays the IP addresses or host names with optional port number of time servers.
- **Advanced**—Click **Advanced** to configure settings, such as daylight saving, time format, date format, and time servers.

> **NOTE: To exit the System Preferences Configuration screen, and load the ThinOS Lite system desktop, click Exit.**

If you are not connected to Ethernet, you cannot continue with the setup, and the **Attach the Ethernet cable** screen is displayed. Do either of the following:

- Connect the Ethernet cable to the zero client.
- Click **Define a wireless connection**. From the list, select a wireless network, and click **Connect**.

NOTE:

- The option to define a wireless connection is not available on zero clients without a WLAN module.
- To exit the **Attach the Ethernet cable** screen, and load the ThinOS Lite system desktop, click **Exit**.

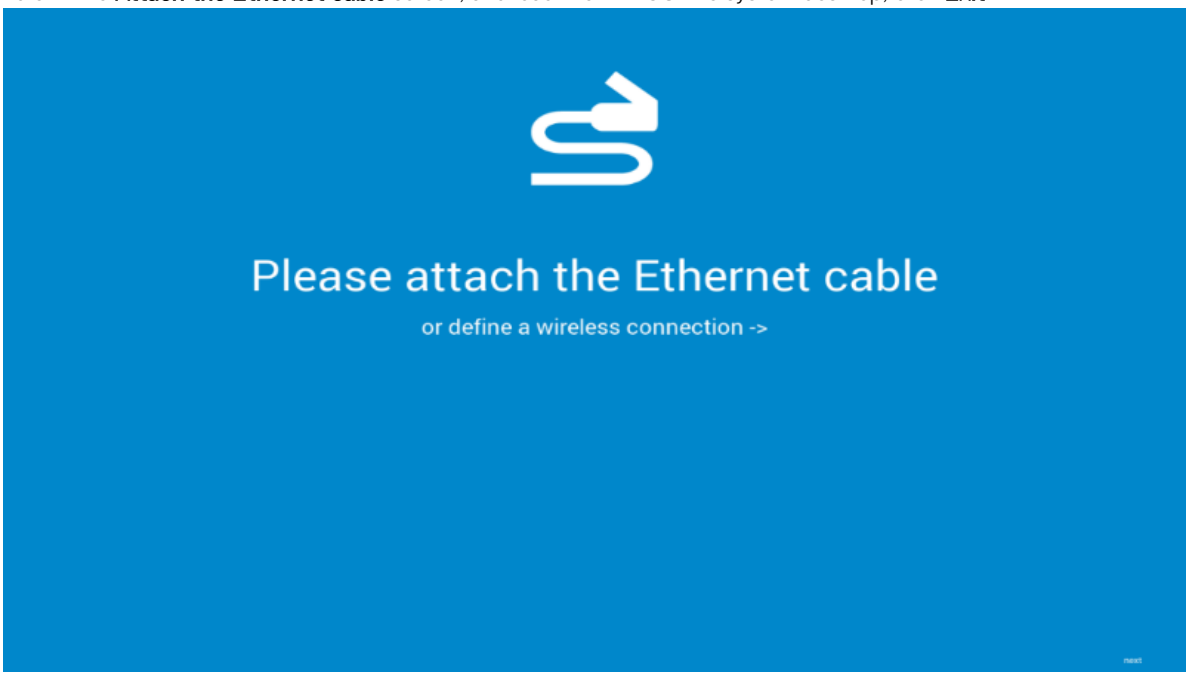


Figure 5. Ethernet cable

After the connection is established, the zero client validates the IP address from DHCP. If the DHCP contains the file server or Wyse Device Manager or Wyse Management Suite configurations, then the ThinOS Lite system desktop is loaded. If the DHCP validation fails, or the network connection fails, then the **Management Configuration** screen is displayed. Follow the steps 6-9.

5 Click **Next** to enter the **Management Configuration** setup.

6 On the **Management Configuration** screen, configure the following:

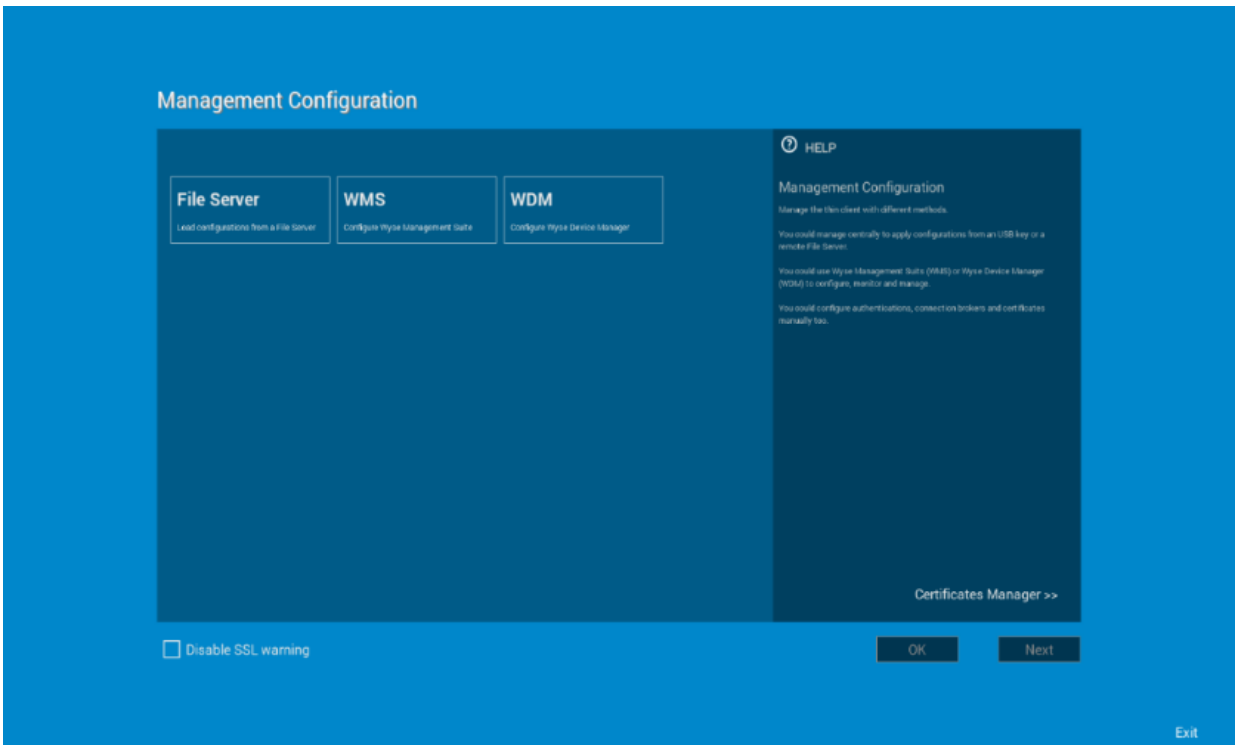


Figure 6. Management configuration

- **File Server**—Enter the file server details to apply configurations including INI files from a file server.
- **WMS**—Enter the group registration key and the Wyse Management Suite server URL to register the zero client to the Wyse Management Suite.
- **WDM**—Enter the IP addresses or host names.
- **Disable SSL warning**—Select this check box to disable the SSL (Secure Sockets Layer) connection warnings.
- **Certificates Manager**—Click **Certificates Manager** to import or request a certificate.

> **NOTE: To exit the Management Configuration screen, and load the ThinOS Lite system desktop, click Exit.**

7 Click **Done** to exit First Boot Wizard or click **Next** to enter the **Connection Broker Configuration** setup.

8 On the **Connection Broker Configuration** screen, configure the Citrix broker connection. The broker allows you to connect to full desktops using Citrix Virtual Apps and Desktops (formerly XenDesktop) or individual applications using Citrix Virtual Apps (formerly XenApp) from a centralized host through Citrix Receiver Client.

- **Server Address**—Enter the host name or IP address of the broker connection.
- **Enable theme: ThinOS Lite**—Select this check box to boot the zero client in ThinOS Lite mode.
- **StoreFront style**—Select this check box to enable the Citrix StoreFront based layout of published applications and desktops on the zero client.
- **Certificates Manager**—Click **Certificates Manager** to import or request a certificate.
- **Disable SSL warning**—Select this check box to disable the warnings for your SSL (Secure Sockets Layer) connection.

9 Click **Done**.

> **NOTE: To configure the Management Configuration setup again, click Back, and follow the steps 6 and 7.**

The device exists from First Boot Wizard mode, and the ThinOS Lite desktop is displayed.

Connecting to a remote server

On your initial connection to central configuration, we recommended that you connect using a **wired connection** plug in the network-connected Ethernet cable to your zero client before starting the zero client to obtain the configurations desired by the administrator. This **wired connection** will also provide any wireless configurations provided by the administrator through INI files.

If you must initially connect to central configuration through wireless, use the Wireless tab in the **Network Setup** dialog box to enter the SSID and encryption configurations required or set up by the network administrator.

Central Configuration — If you are configured for automatic detection using INI files — see the Parameters for a xen.ini File in this guide, your zero client will automatically detect and connect to the configured remote services during the boot-up process. Press the power button to turn on your zero client to see the **Login** dialog box. Enter your User name, Password, and Domain, and then click **Login**. After authentication is successful, your available connections are presented.

Manual Connection — If you are not yet set up for central configuration, you will see the Zero Toolbar, where you can configure the initial server connection you want using the **Remote Connections** dialog box before you can log in. For more information, see Connecting to a Remote Server manually.

You only need to complete this manual configuration once or after reboot to factory defaults. After the zero client knows the location of your server, it automatically connects to the server for login when you start the zero client in the future. After you confirm that your environment is ready for deployment, you can create INI files for central configuration.

Connecting a remote server manually

To connect a Remote Server manually, complete the following tasks:

1 From the floating bar menu, click the **System Setup** , and then click **Remote Connections**. The **Remote Connections** dialog box is displayed.

2 Click the **Broker Setup** tab of the **Remote Connections** dialog box to configure one of the following connections:

- A specific Citrix broker server connection — Enter the IP Address of the server in the **Broker Server** box.

> **NOTE: For more details, see Configuring the Remote Connections.**

3 Click **OK**, and then restart the zero client.

Click the **Shutdown** icon on the Zero Toolbar to open, and use the **Shutdown** dialog box to restart the zero client.

> **NOTE:**
>
> If a Specific Broker Server Connection is configured— After zero client restart, the **Login** dialog box appears for your server. Enter the User name, Password, and Domain and click **Login**. After authentication is successful, your Zero Toolbar is presented with your assigned connections defined by the broker server.

Using your desktop

What you view after logging on to the server depends on the administrator configurations.

- **Users with a zero desktop** - will see the zero desktop with the zero toolbar showing the assigned list of connections from which to select. This option is recommended for VDI and any full-screen only connections. For more information on using the zero desktop, see Zero Desktop Features.

Configuring zero client settings and connection settings

While the use of INI files is recommended to configure zero client settings and connection settings available to users. You can use the dialog box on a zero client to:

- Set up your zero client hardware, look and feel, and system settings.
- Configure connection settings.

Connecting to a printer

To connect a local printer to your zero client, be sure you obtain and use the correct adapter cables which are not included. Before use, you may need to install the driver for the printer by following the printer driver installation instructions.

Connecting to a monitor

Depending on your zero client model, connections to monitors can be made using either a VGA (analog) monitor port, a DVI (digital) monitor port, or a DisplayPort (digital) and the proper Dell monitor cables/splitters/adapters.

NOTE:
For dual-monitor supported zero clients— when using a DVI to DVI/VGA splitter, ensure that the DVI monitor will be the primary monitor; when using a DisplayPort, ensure that the DisplayPort monitor will be the primary monitor.

Locking the zero client

To help ensure that no one else can access your private information without permission, ThinOS Lite allows you to lock your zero client so that credentials are required to unlock and use the zero client after you do one of the following:

- **Unplug a signed-on smart card** — If an administrator has set SCRemovalBehavior=1 for the Signing parameter in the INI files and you unplug the smart card that you used to sign on to the zero client, then the zero client will lock. To unlock the zero client for use, you must use the same smart card and your correct PIN. Note that removing a signed-on smart card can also cause the zero client to log-off, if an administrator has set the INI files to do so in this case you must sign-on as usual to use the zero client.
- **Use LockTerminal from the Shortcut Menu and Shutdown dialog box** — On the Zero Desktop, use the **Shutdown** dialog box, for more information, see Signing Off and Shutting Down. To open the zero client for use, you must use your correct credentials.
- **Use the screen saver** — If an administrator has set LockTerminal=2 for the ScreenSaver parameter, and when the screen saver is activated, then the thin client is locked. To unlock the thin client, enter the login password in the unlock dialog box. However, you cannot see the wallpaper while using the unlock dialog box.

Signing off and shutting down

Use the **Shutdown** dialog box to select the available option you want:

- **Zero Desktop** — Click the **Shutdown** icon on the Zero Toolbar.

NOTE: You can also configure automatic behavior after all desktop sessions are closed by using the Remote Connections dialog box, see Central Configuration: Automating Updates and Configurations.

Additional getting started details

This section includes additional details, such as Zero desktop features, Login dialog box features, System setting menu, and System information.

Zero desktop features

This section includes information on:

- Zero Interactive Desktop Guidelines
- Zero Toolbar
- List of Connections

Zero interactive desktop guidelines

The Zero Desktop has a default background with the Zero Toolbar at the left of the screen.

The following table lists the available Zero Desktop shortcuts:

Table 4. Zero Desktop shortcuts

Action	Press
Display the Zero Toolbar	**Ctrl+Alt+UpArrow**
Open a selection box for toggling between the desktop and currently-active connections	**Ctrl+Alt+DownArrow**
Lock the zero client	**Ctrl+Alt+LeftArrow** or **Ctrl+Alt+RightArrow**
Keyboard shortcuts to menu commands	**Left-Alt+UnderlinedLetter** or **Right-Alt+UnderlinedLetter**
Capture the full desktop to the clipboard	**Print Screen**
Capture the active window to the clipboard	**Alt+PrintScreen**

NOTE:

- You can copy and paste between application sessions and between sessions and the desktop, however, this function depends on session server configurations.
- In addition to the standard two-button mouse, the zero client supports a Microsoft Wheel Mouse used for scrolling. Other similar types of a wheel mouse may or may not work.

To switch the left and right buttons, use the **Peripherals** dialog box, see Configuring the Peripherals Settings.

Zero toolbar

The Zero Toolbar usually appears at the left corner of the Zero Desktop. However, depending on administrator configurations, the toolbar can be removed or hidden. It is shown only when a user moves the mouse pointer over the left edge of the desktop screen.

Table 5. Toolbar icons

Icon	What It Does
Home	Opens the list of available connections.
System Information	Displays zero client system information.
System Settings	Opens the System Settings menu to configure zero client system settings and perform diagnostics.
Shutdown Terminal	Click the **Shutdown Terminal** icon to use the Shutdown options available on the zero client. Note that the **Shutdown Terminal** icon does not display on the toolbar when using the **Admin Mode** button to configure system settings.

NOTE:
If configured to display by an administrator, the current date and time are shown on the Zero Toolbar. The zero client is capable of synchronizing its clock to time provided by a Simple Network Time Protocol (SNTP) server.

List of connections

On the Zero Toolbar, you can click the **Home** icon to open your list of assigned connections. In some cases, the list may contain only default connections.

Use the following guidelines depending on user privilege level, some options may not be available for use:

Table 6. Connection Options

Option	What It Does
Name of the connection	Opens the connection you want to use. **NOTE: All open connections display a blue icon to the left of the connection name in the list.**
Reset icon	Resets the connection. **NOTE: It is useful when a connection is not functioning properly or you need to reboot the connection.**
Close icon	Closes the connection.

Option	What It Does
	NOTE: The Close icon is grayed out for connections that are not open.
Edit icon	Opens the **Connection Settings** dialog box, see Advanced Details on Configuring ICA Connections to change the connection options. **NOTE: Depending on user privilege level, editing options may not be available for use.**
Configuring Global Connection Settings	If you do not use INI files to provide global connection settings, you can click **Global Connection Settings** to open and use the **Global Connection Settings** dialog box to configure settings that affect all of the connection in the list.

Login dialog box features

While the **Login** dialog box allows you to log on to the server, it also allows you to:

- Obtain system information.
- Access Admin Mode to configure zero client settings.
- Change or reset your own password and unlock your account.
- Open the **Shutdown** dialog box by using CTRL+ALT+DELETE.

In the **Login** dialog Box, use the following guidelines:

- **System Information** — Click the **Sys Info** button to open the **System Information** dialog box. You can view the zero client system information such as System Version, IP Address, information on devices connected to your zero client, event logs and so on.
- **Admin Mode** — Click the **Admin Mode** button to configure various settings locally on the zero client other than broker desktop configurations. For example, you can choose to manually configure the Citrix Xen Broker Server URL or override the URL that is centrally defined by file servers by using the **Remote Connections** dialog box as described in Remote Connections
  - **Zero Desktop** — Use the Leave Administrator Mode option in the Shutdown dialog box, or use the **Leave Administrator Mode** icon (X) in the upper-right pane of the System Settings menu.

    NOTE:
    - By default the Admin Mode button is not displayed on the **log on** dialog box. You can display it by selecting the **Show local admin button** check box in the Shutdown dialog box, see Signing Off and Shutting Down.
    - By default there is no password needed for **Admin Mode** button use. You can password protect the **Admin Mode** button (to require login credentials) by using the AdminMode parameter in a wnos.ini file, see the *INI section* in this Guide.
- **Shutdown** — Press **CTRL+ALT+DELETE** to open and use the **Shutdown** dialog box to sign off, shut down, restart, reset the system setting to factory defaults, and so on. For information, see Signing Off and Shutting Down.
- **Account Self-Service** — Click the **Account Self-Service** icon shown when configured using the AccountSelfService option of the PasswordServer INI parameter to open and use the **Account Self-Service** dialog box to change or reset your own password and unlock your account. For information on INI parameter, see the *INI section* in this Guide.

This process assumes that the security questions and answers have been pre-registered by the user inside of their Windows environment. Users must use HTTPS (not HTTP) for an account self-service server address such as https://IPAddress, in the Broker Setup tab.After answering the security questions, your new password will be set or your account will be unlocked.

Using the system setup menu

To access the system setup menu:

1 Click **System Setup** from Zero Toolbar.

The System Setup Menu is displayed.

2 On the system setup menu, you are able to view and use the following options:

a **Network Setup** — Allows selection of DHCP or manual entry of network settings, as well as entry of locations of servers essential to zero client operation. This menu selection is disabled for Low-privileged users.

b **Remote Connections** — Allows you to configure zero client network connections for Citrix Xen.

c **Central Configuration** — Allows you to configure zero client central connection settings such as file server and optional WDM server settings.

d **VPN Manager** — Allows you to configure zero client VPN manager.

e **System Preference** — Allows user selection of zero client parameters that are matter of personal preference.

f **Display** — Allows you to configure the monitor resolution and refresh rate.

g **Peripherals** — Allows you to select the peripherals settings such as keyboard, mouse, volume and touch screen settings.

h **Printer** — Allows configuration of network printers and local printers that are connected to the zero client.

i **System Tools** — Opens a submenu from which the xen.ini and user.ini windows can be opened to view the contents of the files.

j **Trouble shooting Options** — Displays Performance Monitor graphs that display client CPU, Memory and Networking information and trace route response messages.

Accessing system information

Use the **System Information** dialog box to view system information:

- **Zero Desktop** — Click the **System Information** icon on the Zero toolbar.

The **System Information** dialog box includes:

- **General tab** — Displays general information such as System Version, Serial Number, Memory Size (Total and Free), CPU Speed, ROM Size, Monitor, Parallel ports, Terminal Name, Boot from, Memory speed, SSD size, Resolution and Serial ports.
- **Copyright/Patents tab** — Displays the software copyright and patent notices.
- Acknowledgements button is added under Copyrights tab in System Information. This button is related to third party software and is available only in following clients:
  - Wyse 5010 Zero Client for Citrix — D00DX (ThinOS Lite Pro 2)
- **Event Log tab** — Displays the zero client start-up steps normally beginning from System Version to Checking Firmware or error Messages that are helpful for debugging problems. The details about the monitors connected to the zero client are also displayed.

  When you install the packages or restart the client, the zero client verifies the version of the installed packages. If you have not installed the latest package version, the details about the current package version and the recommended package version are displayed.
- **Status tab** — Displays status information about TCP performance related parameters, UDP performance related parameters, CPU Busy, System Up Time, CCM status, Free Memory, Active sessions, and WDM status.
- **IPv6 tab** — Displays IPv6 information such as Link-local Address, IPv6 Address and IPv6 Default Gateway.
- **ENET tab** — Displays information about wired network information.
- **WLAN tab** — Displays information about wireless network information.

- **About tab**—Displays information about ThinOS Lite operating system. The following attributes are listed:
  - Platform name
  - Operating system type
  - Build name
  - Build version
  - BIOS name
  - BIOS version
  - Citrix Broker or Receiver version—This represents ICA revisions between the ThinOS Lite versions.
  - Dell vWorkspace version
  - Imprivata version
  - Caradigm version
  - SECUREMATRIX version
  - HealthCast version

NOTE: This tab is displayed when IPv6 is enabled in the General tab of the Network Setup dialog box, see Configuring the Network Settings.

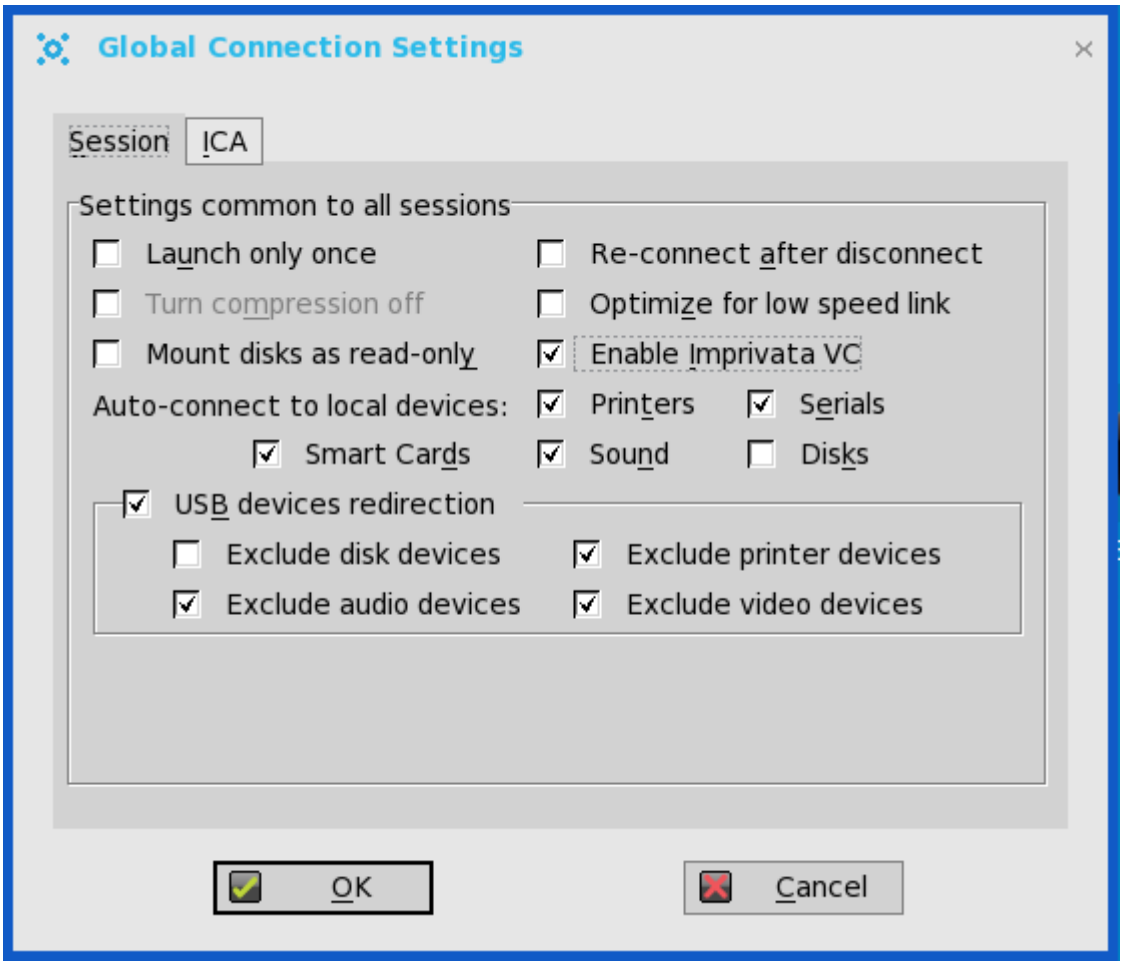
- Kernel mode—The components are implemented in Kernel according to the specification. The version is displayed as [max].[min], which is the base version of protocol or server or client of the component. For example, the Imprivata version is 5.2, and so on.
- User mode—The components are from the source, or binaries from third party that are compiled or integrated into ThinOS Lite. The version is displayed as [max].[min].[svn_revision]. The [max] and [min] is the base version of the third component, and the [svn_revision] is the source control revision of ThinOS Lite. Using the ThinOS Lite specified version, you can identify the changes between different revisions. For example, the Citrix Receiver version is 14.0.44705. The components are matched to the installed packages. If the packages are removed, the field remains empty in the **About** tab.

4

Global connection settings

If you do not use INI files to provide central configuration (global connection settings) to users, you can use the Global Connection Settings dialog box to configure settings that affect all of the connections in your list of connections:
To Configure the Global Connection Settings:

1 From the floating bar menu, click the **Home** icon, and then click **Global Connection Settings**.
The **Global Connection Settings** dialog box is displayed.



2 Click the **Session** tab to select the check boxes you want for the options that are available to all sessions.

- The Smart Card check box specifies the default setting for connecting to a smart card reader at startup.
- When using the **Disks** check box for automatic connection to connected USB sticks, use the following guidelines:
  - More than one disk can be used at the same time, however, the maximum number of USB sticks including different subareas is 12.
  - Be sure to save all data and sign off from the session mapping the USB stick before removing the USB stick.

IMPORTANT: The figure shown is an example for Zero Desktop.

NOTE:

ICA sessions always have automatic connection to attached smart card readers.

NOTE: USB devices redirection— By default, audio, video and printer devices will not use HDX USB for redirection. You can make selections for USB device redirection on the Session tab of the Global Connection Settings dialog box.

3 Click **ICA** tab to select the check boxes you want for the options that are available to all ICA sessions. Select the audio quality optimized for your connection.

NOTE:

- **Map to** — When a drive is entered, maps a disk under the drive.

5

Configuring the connectivity

This chapter helps you to understand various configuration settings for a secure connection. Connectivity menu includes:

- Configuring the Network Settings.
- Configuring the Remote Connections.
- Configuring the Central Configurations.
- Configuring the Caradigm Vault Server.
- Configuring objects on Imprivata Server.
- Configuring the VPN Manager.

Configuring the network settings

To configure the network settings use the following options:

- Configuring the General Settings
- Configuring the DHCP Options Settings
- Configuring the ENET Settings
- Configuring the WLAN Settings

Configuring the general settings

To configure the general network settings:

1 From the floating bar menu, click the **System Setup** , and then click **Network setup**.
The **Network Setup** dialog box is displayed.

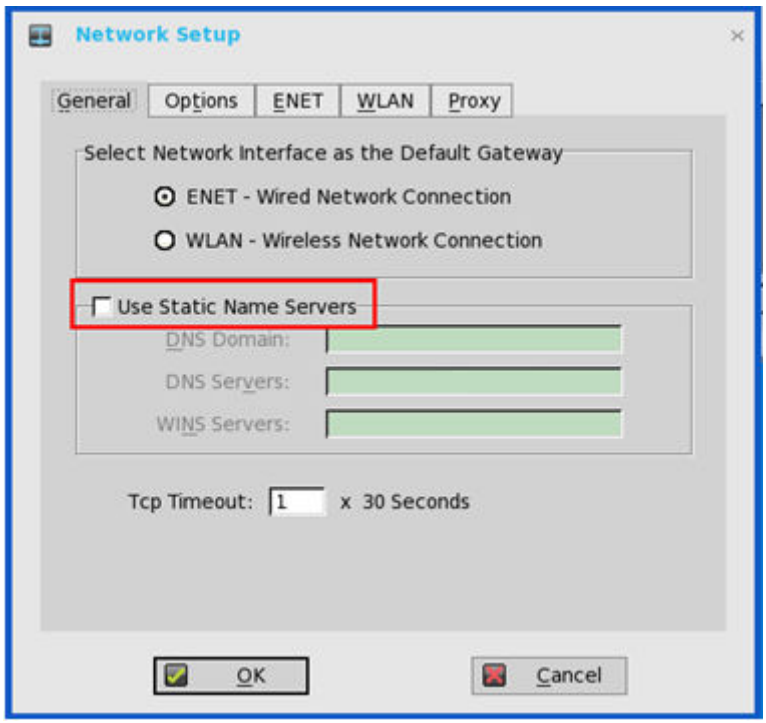


Figure 7. Network setup

2 Click the **General** tab and use the following guidelines:

a To set the default gateway, select the type of network interface from the available options.

1 **Single Network support**— Either wireless or wired network is connected.

- **ENET** — Click this option, if you want set up the Ethernet Wired Network Connection.
- **WLAN** — Click this option, if you want set up the Wireless Network Connection.
- If the user use wireless network after selecting ENET connection or wired network after selecting WLAN connection, then the system log "WLAN: set default gateway xx.xx.xx.xx" for first case and "ENET: set default gateway xx.xx.xx.xx" for second case are printed to ensure that the UI setting reflects the actual usage.
- **Use Static Name Servers**— By default, this check box is not selected, and thin client fetches the server IP address from DHCP. Select this check box to manually assign static IP addresses. If name servers are changed using GUI, INI or link down/ up, then the details are displayed in **Event Logs**. In dynamic mode, the DNS/WINS can be merged from Ethernet and Wireless, if network is not working.

2 **Dual Network support** — Both wireless and wired networks are connected. The default gateway is determined by the UI settings.

NOTE: The UI will not be changed automatically.

b Enter the URL address of the DNS Domain in the **DNS Domain** box.

c Enter the IP address of the DNS Server in the **DNS Server** box.

Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. Enter the DNS Domain and the network address of an available DNS Server. The function of the DNS Domain entry is to provide a default suffix to be used in name resolution. The values for these two boxes may be supplied by a DHCP server. If the DHCP server supplies these values, they replace any locally configured values. If the DHCP server does not supply these values, the locally configured values will be used.

NOTE: You can enter upto 16 DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server and the rest are secondary DNS servers or backup DNS servers.

d Enter the IP address of the WINS Server in the **WINS Server** box.

Use of WINS is optional. Enter the network address of an available WINS name server. WINS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it

is used to make the connection. These entries can be supplied through DHCP, if DHCP is used. DNS and WINS provide essentially the same function, name resolution. If both DNS and WINS are available, the zero client attempts to resolve the name using DNS first and then WINS.

You can enter two WINS Server addresses (primary and secondary), separated by a semicolon, comma, or space.

e Enter the digit multiplier of 30 seconds in the **TCP Timeout** box to set the timeout value of a TCP connection. The value must be **1** or **2** which means the connection timeout value is from 1x30= 30 seconds to 2x30= 60 seconds. If the data for connecting to the server is not acknowledged and the connection is time out, setting the timeout period retransmits the sent data and again tries to connect to the server till the connection is established.

3 Click **OK** to save the settings.

Configuring the DHCP options settings

To configure the Option settings :

1 From the floating bar menu, click the **System Setup** , and then click **Network Setup**.
The **Network Setup** dialog box is displayed.

2 Click the **Options** tab, and use the following guidelines:

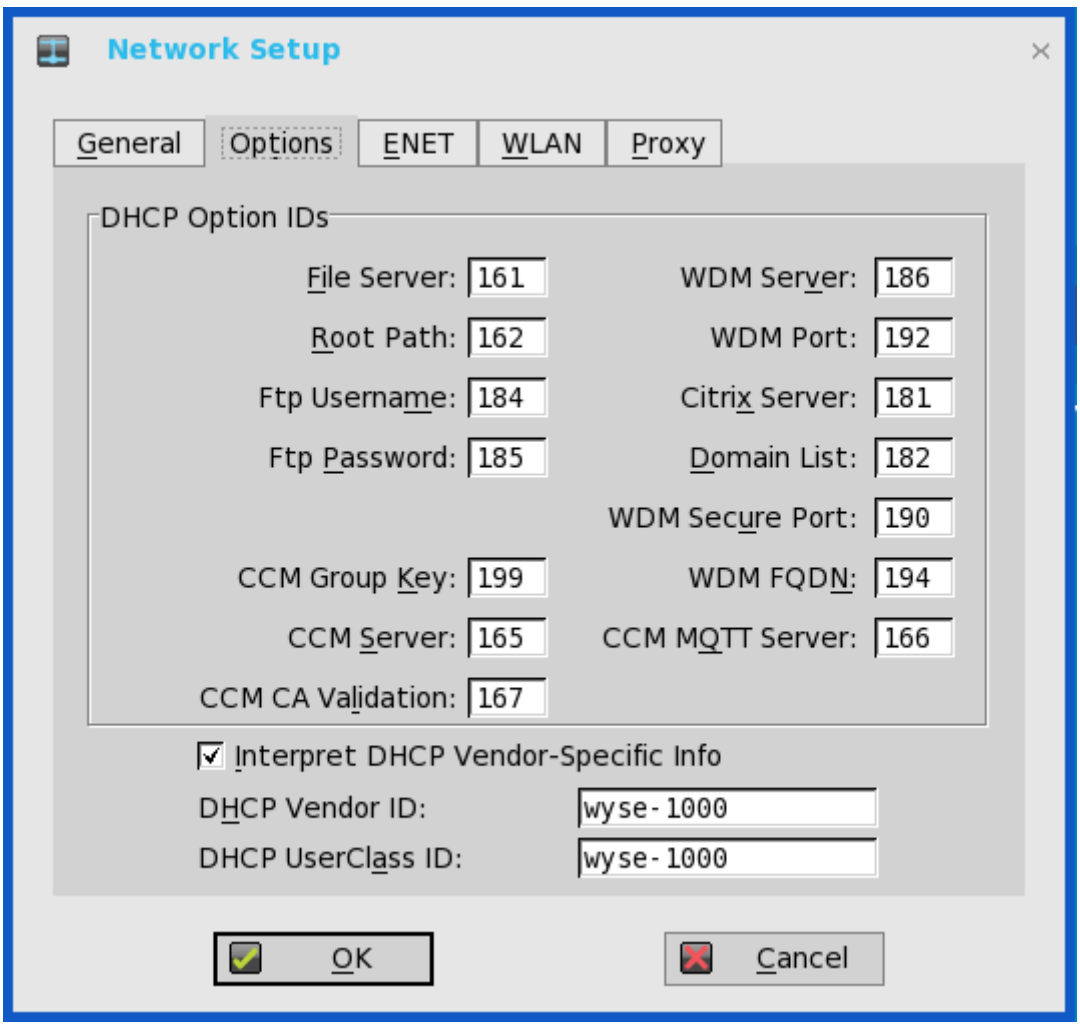


Figure 8. Network Setup

a **DHCP Option IDs** — Enter the supported DHCP options; each value can only be used once and must be between 128 and 254). For information on DHCP options, see Using DHCP options

b **Interpret DHCP Vendor-Specific Info** — Select this check box for automatic interpretation of the vendor information.
c **DHCP Vendor ID** — Shows the DHCP Vendor ID when the dynamically allocated over DHCP/ BOOTP option is selected.
d **DHCP UserClass ID** — Shows the DHCP UserClass ID when the dynamically allocated over DHCP/BOOTP option is selected.

3 Click **OK** to save the settings.

Configuring the ENET settings

To configure the ENET settings:

1 From the floating bar menu, click **System Setup**, and then click **Network Setup**.
The **Network Setup** dialog box is displayed.

2 Click the **ENET** tab, and use the following guidelines:

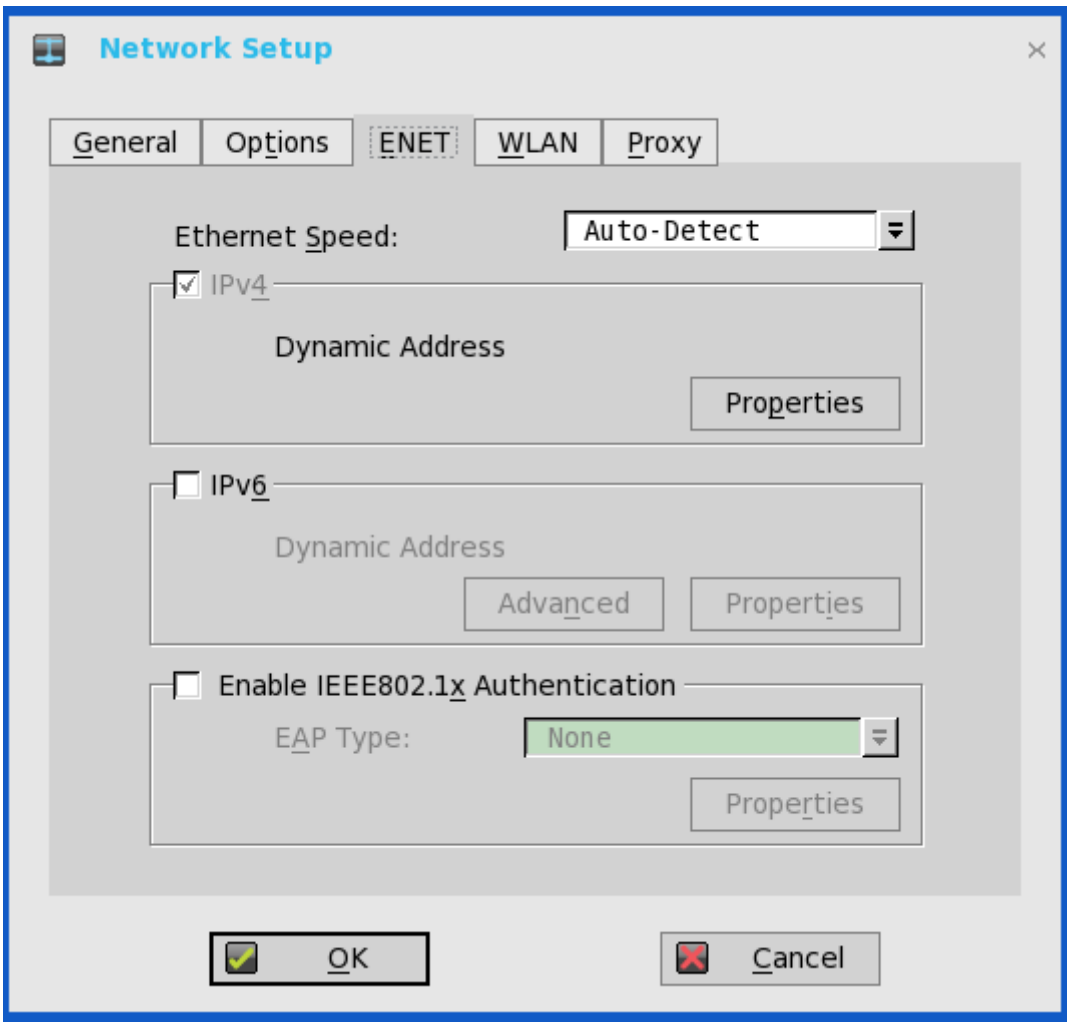


Figure 9. ENET settings

a **Ethernet Speed** — Normally the default (**Auto-Detect**) should be selected, but another selection can be made if automatic negotiation is not supported by your network equipment. Selections include **Auto-Detect**, **10 MB Half-Duplex**, **10 MB Full-Duplex**, **100 MB Half-Duplex**, **100 MB Full-Duplex**, and **1 GB Full-Duplex**.
The **10 MB Full-Duplex** option can be selected locally at the device, however, this mode may need to be negotiated through **AutoDetect**.

b The **IPV4** check box is selected by default. Click **Properties** to set various options supported by IPV4.

- **Dynamically allocated over DHCP/BOOTP** — Selecting this option enables your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server using DHCP options to provide information. Any value provided by the DHCP server replaces any value entered locally on the Options tab, however, locally entered values are used if the DHCP server fails to provide replacement values.
- **Statically specified IP Address** — Select this option to manual enter the IP Address, Subnet Mask and Default Gateway:
  - **IP Address** — Must be a valid network address in the server environment. The network administrator must provide this information.
  - **Subnet Mask** — Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices: same subnet or other subnet. If the location is other subnet, messages sent to that address must be sent through the Default Gateway, whether specified through local configuration or through DHCP. The network administrator must provide this value.
  - **Default Gateway** — Use of gateways is optional. Gateways are used to interconnect multiple networks (routing or delivering IP packets between them). The default gateway is used for accessing the internet or an intranet with multiple subnets. If no gateway is specified, the thin client can only address other systems on the same subnet. Enter the address of the router that connects the thin client to the internet. The address must exist on the same subnet as the thin client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.

c Select the **IPV6** check box, and then click **Advanced** to select various IPV6 supported setting options from the available check boxes.

The following check boxes are displayed in the **IPv6 Advanced Settings** dialog box:

- Allow IPv4 to be disabled when IPv6 is enabled
- Prefer IPv4 over IPv6 when both are available
- Disable Stateless Address Auto configuration (SLAAC)
- Disable Duplicate Address Detection (DAD)
- Disable ICMPv6 Echo Reply
- Disable ICMPv6 Redirect Support
- Use Standard DHCPv6 Timers

Click **properties** and use the following guidelines:

- **Wait DHCP** — Selecting this option enables your thin client to wait for IPV6 DHCP before the sign-in, if not selected the system will only wait for IPV4 DHCP if enabled.
- **Dynamically allocated over DHCP/BOOTP** — Selecting this option enables your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server (using DHCP options) to provide information. Any value provided by the DHCP server replaces any value entered locally on the **Options tab**, however, locally entered values are used if the DHCP server fails to provide replacement values.
- **Statically specified IP Address** — Select this option to manually enter the IP Address, Subnet Mask and Default Gateway.
  - **IP Address** — Must be a valid network address in the server environment. The network administrator must provide this information.
  - **Subnet Mask** — Enter the value of the subnet mask. For more information, see various options supported by IPV4 in this section.
  - **Default Gateway** — Use of gateways is optional. For more information, see various options supported by IPV4 in this section.
- **DNS Servers** — Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS is used to make the connection. Enter the network address of an available DNS Server. The value for this box may be supplied by a DHCP server. If the DHCP server supplies this value, it replaces any locally configured value. If the DHCP server does not supply this value, the locally configured value is used.

d Select the check box to enable IEEE802.1x authentication.

EAP Type — If you have enabled the **Enable IEEEE 802.1x authentication** check box, select the EAP Type option you want (**TLS**, **LEAP**, **PEAP** or **FAST**).

- **TLS** — If you select the **TLS** option, click **Properties** to open and configure the **Authentication Properties** dialog box.
  - Select the **Validate Server Certificate** check box because it is mandatory to validate your server certificate.

    NOTE:
    The CA certificate must be installed on the thin client. Also note that the server certificate text field supports a maximum of approximately 255 characters, and supports multiple server names.
  - If you select the **Connect to these servers** check box, the box is enabled where you can enter the IP address of server.
  - Click **Browse** to find and select the Client Certificate file and Private Key file you want.

    NOTE: Make sure you select PFX file only.
  - From the **Authenticate** drop-down list, select either User Authentication or Machine Authentication based on your choice.

    The following kinds of server names are supported — all examples are based on Cert Common name **company.wyse.com**
    - *.wyse.com
    - *wyse.com
    - *.com

      NOTE:
      Using only the FQDN, that is company.wyse.com does not work. You must use one of the options (note that *.wyse.com is the most common option as multiple authentication servers may exist): servername.wyse.com
- **LEAP** — If you select the **LEAP** option, click **Properties** to open and configure the **Authentication Properties** dialog box. Be sure to use the correct username and password for authentication. The maximum length for the username or the password is 31 characters.
- **PEAP** — If you select the **PEAP** option, click **Properties** to open and configure the **Authentication Properties** dialog box. Be sure to select either **EAP_GTC** or **EAP_MSCHAPv2**, and then use the correct username, password and domain. Validate Server Certificate is optional.
- **FAST**—If you select the **FAST** option, click **Properties** to open and configure the **Authentication Properties** dialog box. Be sure to select either **EAP_GTC** or **EAP_MSCHAPv2**, and then use the correct username, password and domain. Validate Server Certificate is optional.

  From ThinOS Lite 2.3, EAP-FAST authentication is supported. During the initial connection, when there is a request for a Tunnel PAC from the authenticator, the PAC is used to complete the authentication. Therefore, the first time connection always fails and the following connections succeed. Only automatic PAC provisioning is supported. The user/machine PAC provisioning generated with Cisco EAP-FAST utility is not supported.

Configuring EAP-GTC and EAP-MSCHAPV2

- To configure EAP-GTC, enter the username only. The password or PIN is required when authenticating.
- To configure EAP-MSCHAPv2, enter the username, password and domain.

  IMPORTANT: The domain\username in the username box is supported, but you must leave the domain box blank.

  The CA certificate must be installed on the thin client and the server certificate is forced to be validated. When EAP-MSCCHAPV2 is selected as EAP type in the **Authentication Properties** dialog box for PEAP or FAST authentication, an option to hide the domain is available for selection. Username and Password boxes are available for use, but the **Domain** text box is disabled.

When EAP-MSCHAPV2 is selected as EAP type in the **Authentication Properties** dialog box for PEAP or FAST authentication, a check box to enable Single Sign-On feature is available for selection.

3 Click **OK** to save the settings.

Configuring the WLAN settings

1 From the floating bar menu, click **System Setup**, and then click **Network Setup**.
The **Network Setup** dialog box is displayed.

2 Click the **WLAN** tab, and use the following guidelines:

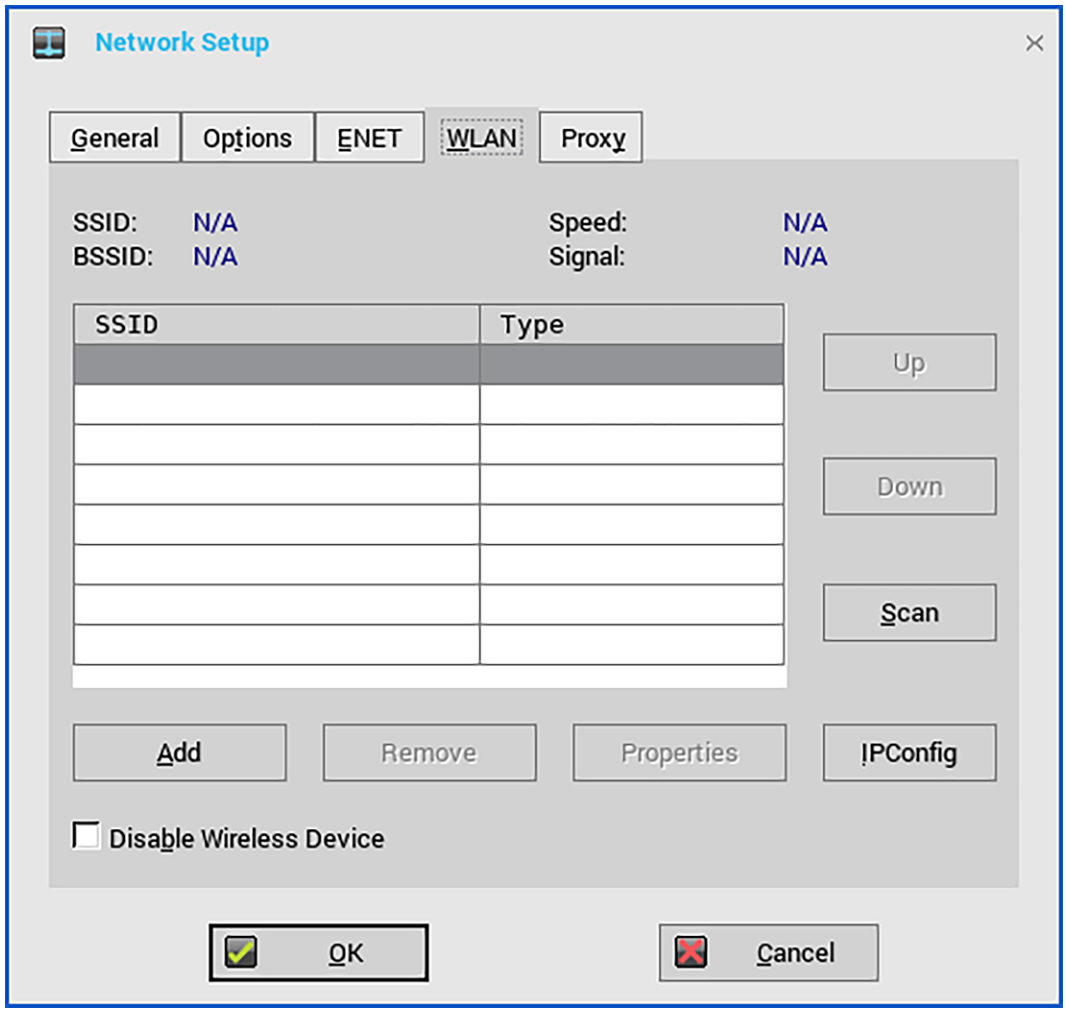


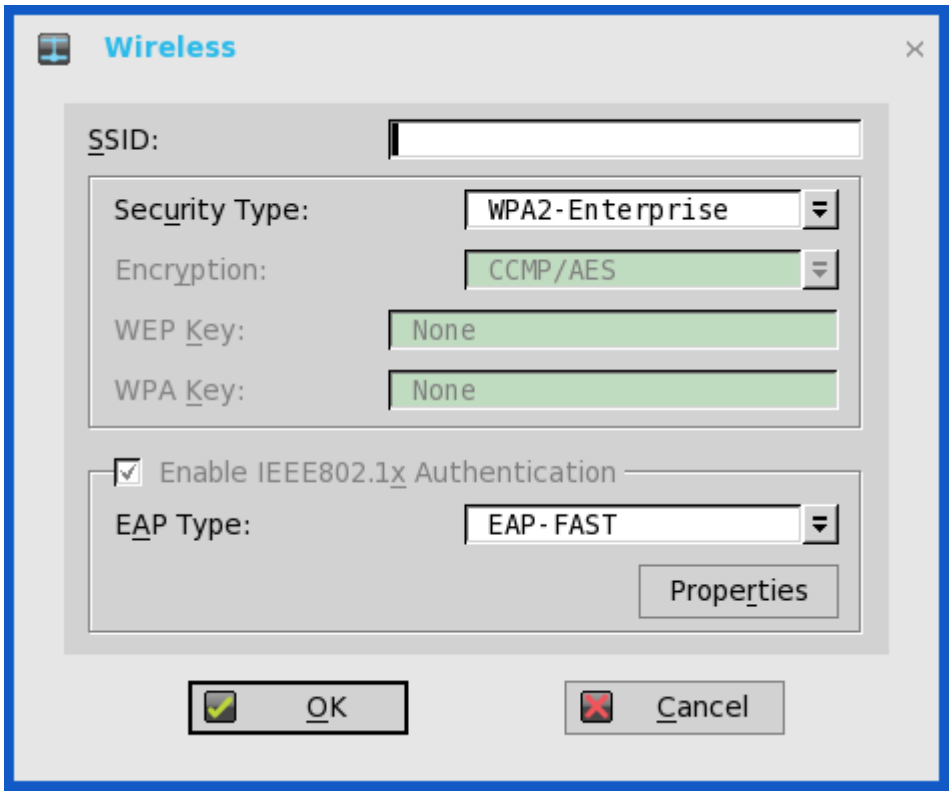
Figure 10. WLAN settings

a **Add**— Use this option to add and configure a new SSID connection.
You can configure the SSID connection from the available security type options.

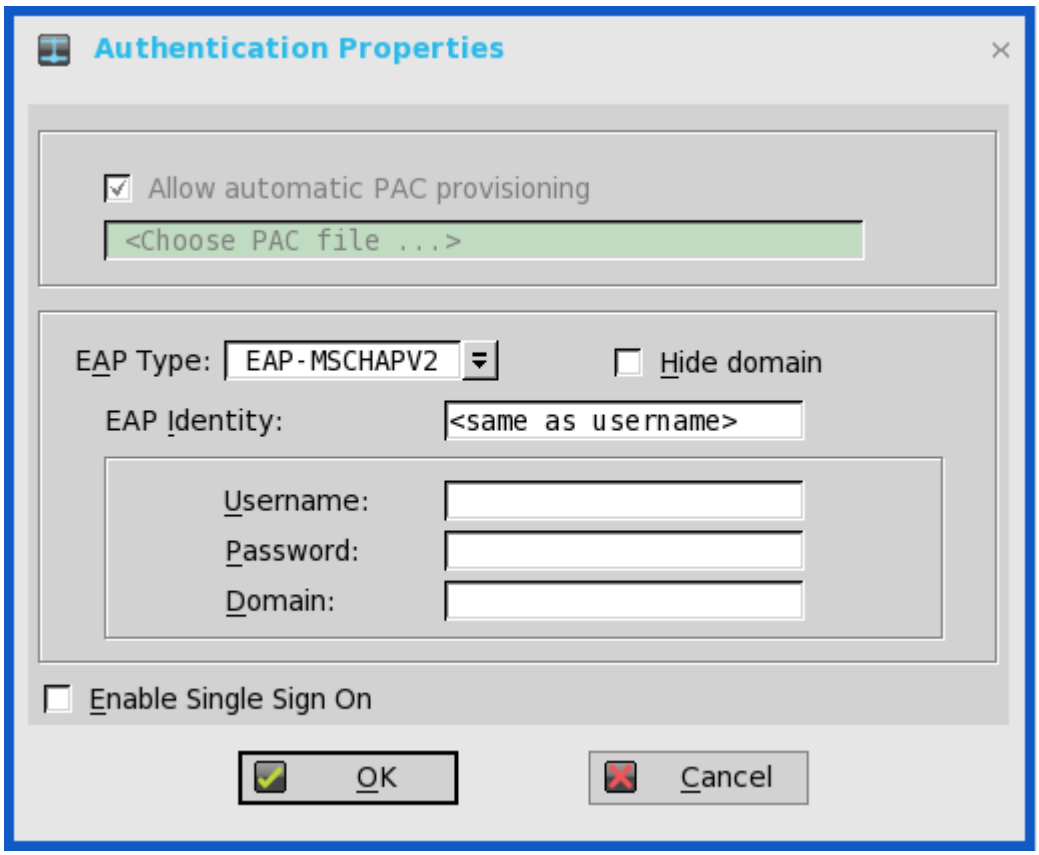
b After you configure the SSID connection, the added SSID connection is listed on the page of the **WLAN** tab.

- **Remove** — Use this option, if you want to remove a SSID connection by selecting the SSID connection from the list.
- **Properties** — Use this option to view and configure the authentication properties of a SSID connection that is displayed in the list. From the ThinOS Lite 2.3 release, a new EAP type named **EAP-Fast** is added in the **EAP** type drop-down list. During the initial connection, when there is a request for a Tunnel PAC from the authenticator, the PAC is used to complete the authentication. Therefore, the first time connection always fails and the following connections succeed.

Only automatic PAC provisioning is supported from 2.3 release. The user/machine PAC provisioning generated with Cisco EAP-FAST utility is not supported.



If you select EAP type as **EAP-Fast**, then **EAP-MSCHAPV2** and **EAP-GTC** options are listed in the **EAP** type drop-down list in the **Authentication Properties** dialog box (2nd authentication method supports MSCHAPv2/GTC only for EAP-FAST).



c Select the **Disable Wireless Device** check box, if you want to disable a wireless device.

- **Always**: Click this radio button if you want to disable the wireless device at all times.
- **EnetUp**: Click this radio button if you want to disable the wireless device whenever the wired network is connected.

d Click **IPConfig** to configure the IPv4 settings for the wireless connection. To set the IPv4 connection to use DHCP or the specified static IP address, do the following:

1 Click **Properties**.

2 If you want to allow your zero client to automatically receive information from the DHCP server, click **Dynamically allocated over DHCP/BOOTP**.

3 If you want to manually configure the IP address, click **Statically specified IP Address**, and provide the IPv4 details.

3 Click **OK** to save the settings.

IMPORTANT: From ThinOS Lite version 2.5, device reboot is not required to change the network settings. All the changes take effect immediately. For example, ThinOS Lite connects to the new wireless SSID immediately without reboot. However for ARM platforms—Wyse 3010 zero client, and Wyse 3020 zero client—the disable/enable wireless requires reboot.

Configuring the proxy settings

The network **Proxy** tab is added to support Wyse Management Suite, HDX Flash Redirection and Real Time Multimedia Engine (RTME).

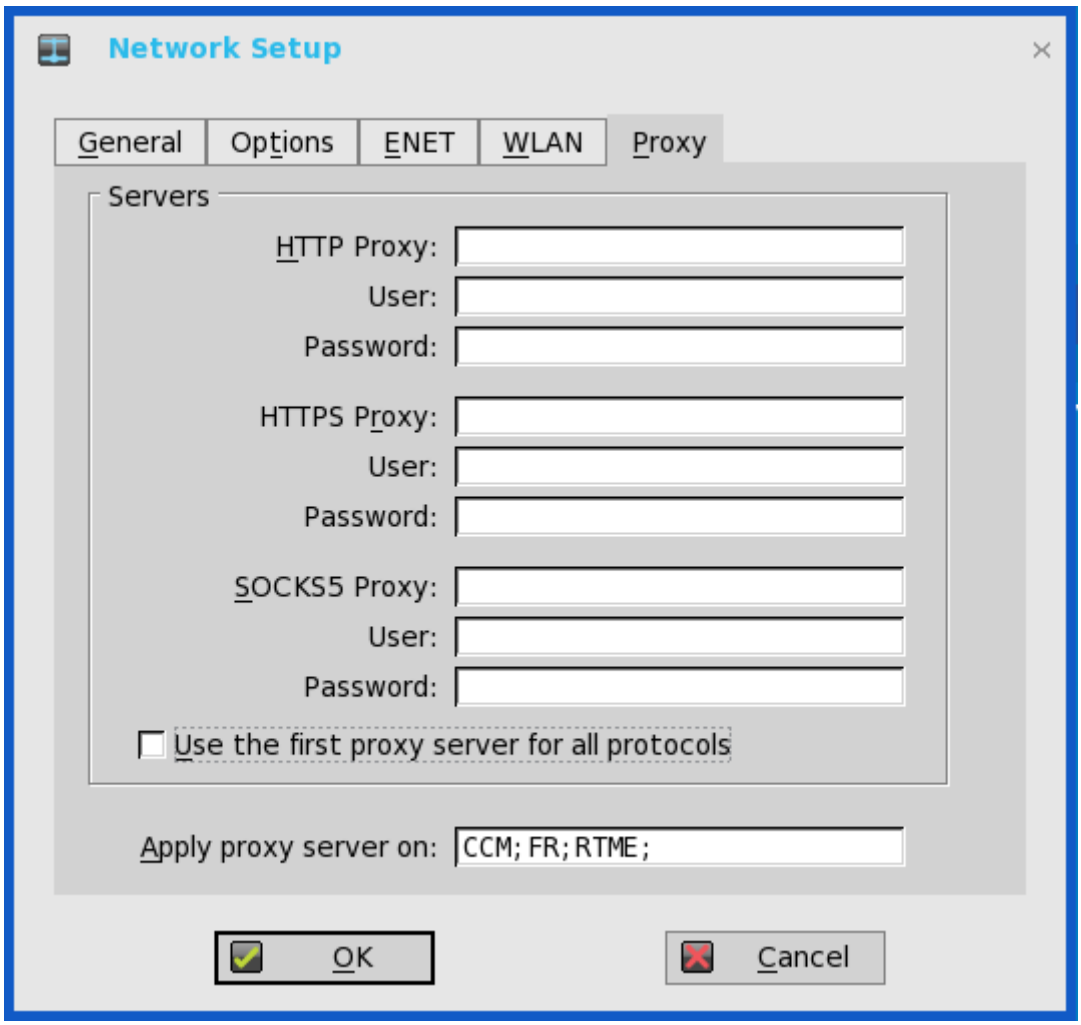


Figure 11. Network Setup

Supported Protocols

- For **HDX FR**, HTTP and HTTPS protocols are supported.
  - If both are configured, the HDX FR works with HTTPS proxy.
  - User credential pass through is possible with $UN/$PW.
- For **WMS**, HTTP, HTTPS and Socks5 (recommended) protocols are supported.
- For RTME, HTTP and HTTPS protocols are supported.

1 From the desktop menu, click **System Setup**, and then click **Network Setup**.
The **Network Setup** dialog box is displayed.

2 Click the **Proxy** tab, and use the following guidelines:

a Enter the HTTP proxy port number or HTTPS proxy port number, Username and Password in the respective fields. However, Credential pass through ($UN/$PW) is not recommended because it starts before user sign on.

Wyse Management Suite uses both HTTP/HTTPS and MQTT protocols to communicate with CCM/MQTT server. However, the HTTP proxy cannot redirect TCP packages to MQTT server which requires a Socks5 proxy server. If there is only HTTP server available, then the real-time command that requires MQTT will not work.

HTTP/HTTPS proxy default port is 808, and SOCK5 proxy default port is 1080.

b Select the **Use the first proxy server for all protocols** check box to allow all the protocols to use the same server in HTTP Proxy fields. Both HTTP and HTTPS proxy use the same host and port, and Socks5 proxy agent uses HTTP host with default Socks 5 port (1080).

c If SOCKS5 proxy is configured, then Wyse Management Suite proxy uses the SOCKS5 only. If SOCKS5 is not configured, then Wyse Management Suite proxy searches for alternative protocols, for example, HTTP in the configuration.

d Specify the supported applications as Wyse Management Suite, FR, and RTME in the **Apply proxy server on** field.

3 Click **OK** to save the settings.

User Scenarios

1 Configure correct proxy server host and port.

2 Configure the user credentials according to the proxy server settings.

3 On system restart, the client checks in to the Wyse Management Suite server through Socks5 proxy server.

4 MQTT connection is established through Socks5 proxy server.

5 Real-time commands work fine through Socks5 proxy server.

6 Connect to the Citrix desktop, configure proxy in internet options of the browser, and then playback HDX FR through the HTTP/ HTTPS proxy authentication.

Configuring the remote connections

Use the **Remote Connections** dialog box to configure zero client remote connections for Citrix broker setup, visual options, and general connection settings.

Use the following options to configure the remote configurations:

- Configuring the Broker Setup
- Configuring the Visual Settings
- Configuring the General Options
- Configuring the Authentication Settings

Configuring the Citrix broker setup

To configure the broker setup, do the following:

1 From the floating bar menu, click the **System Setup** , and then click **Remote Connections**.
The **Remote Connections** dialog box is displayed.

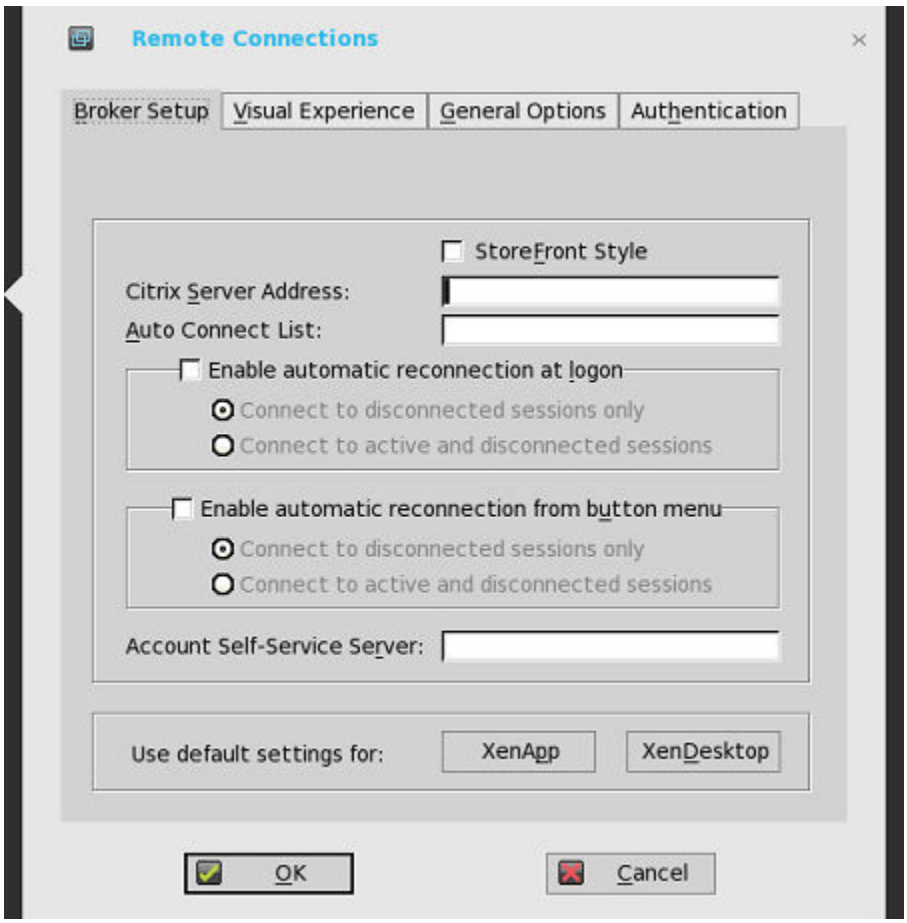


Figure 12. Broker setup

2 Select the **StoreFront Style** check box to enable the StoreFront style.

3 **Broker Server**— Enter the IP address / Hostname / FQDN of the broker server.

4 Select the **Enable automatic reconnection at logon** check box to enable automatic re-connection at logon.

> **NOTE: If you enable the automatic re-connection, you are able to select from the re-connection options. Click either of the options where you can connect to disconnected sessions only or both active and disconnected sessions.**

5 Select the **Enable automatic reconnection from the button menu** check box to enable automatic reconnection from the button menu. You can select any of the following options:

- Connect to disconnected sessions only.
- Connect to active and disconnected sessions.

6 **Account Self-Service Server**— Enter the IP address of the Account Self-service Server.

7 **XenApp** — Use this option if you want to set default settings to XenApp.

8 **XenDesktop**— Use this option if you want to set default settings as XenDesktop.

9 Click **OK** to save the settings.

Configuring the visual settings

To configure the visual settings:

1 From the floating bar menu, click the **System Setup** , and then click **Remote Connections**.
The **Remote Connections** dialog box is displayed.

2 Click **Visual Experience** tab and use the following guidelines:

NOTE: The Visual Experience tab is grayed out, if the StoreFront Style check box is selected for a Citrix Broker Server entered in the Broker Setup tab.

a Select the check box to enable Zero Toolbar activation in left pane.
   - Select the button if you want to enable Zero Toolbar activation in left pane when you pause a mouse on the screen.
   - Select the button if you want to enable Zero Toolbar activation in left pane only after clicking.

b Select the check box to disable hotkey to show toolbar.
c Select the check box to always disable toolbar when you have one session available.
d Select the check box to disable the Home Icon.

3 Click **OK** to save the settings.

Configuring the general options

To Configure the Remote Configurations to General Options:

1 From the floating bar menu, click the **System Setup** , and then click **Remote Connections**.
The **Remote Connections** dialog box is displayed.

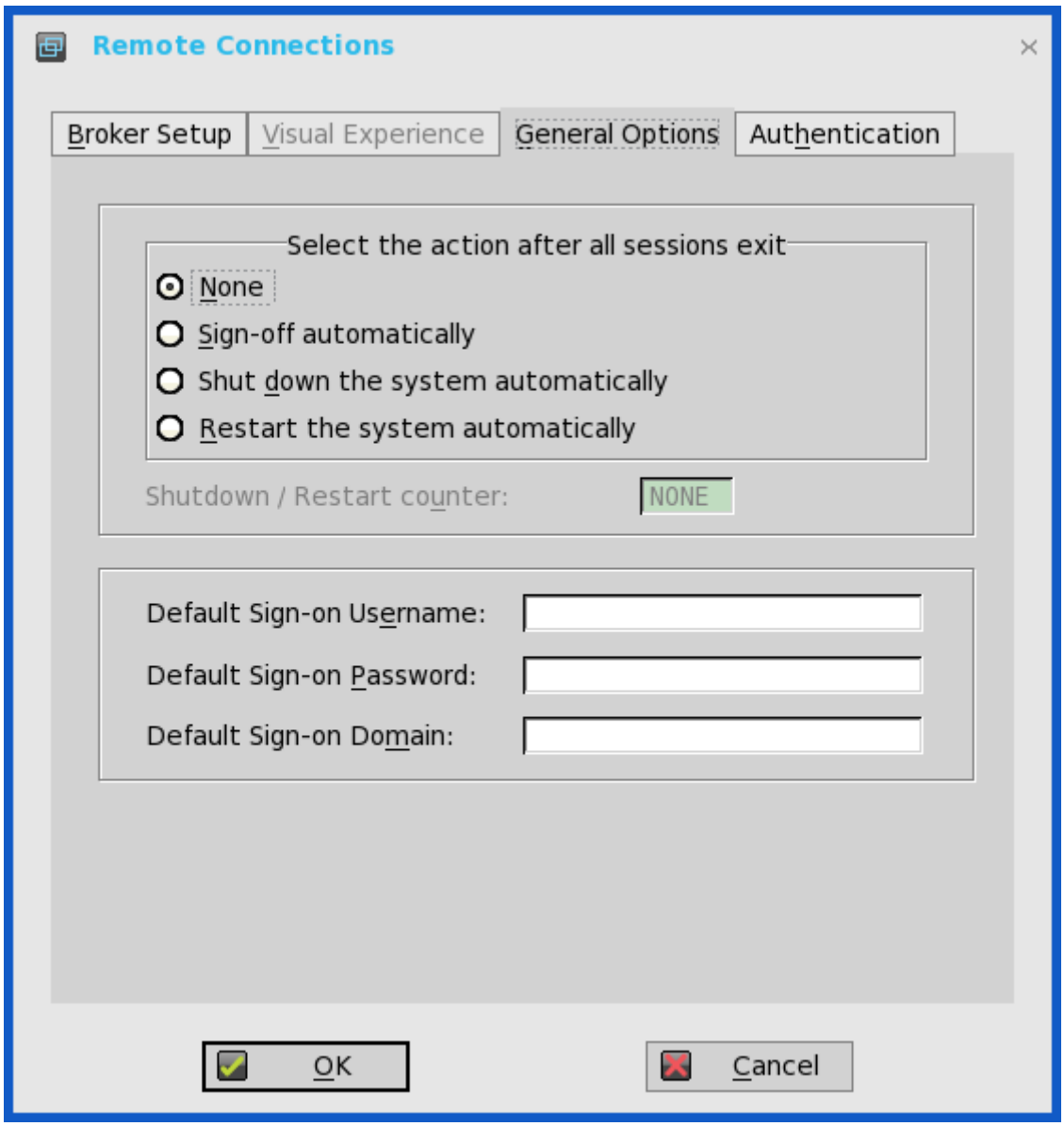


Figure 13. General options

2 Click **General Options** and use the following guidelines:

a Click the available options to select the action after you exit all open desktops. The available options are **None**, **Sign-off automatically**, **Shut down the system automatically** and **Restart the system automatically**.

NOTE: By default, None is selected and the zero client automatically returns to the terminal desktop.

b **Default Sign-on Username**— Enter the Default user name.

c **Default Sign-on password**— Enter the Default password.

d **Default Sign-on Domain**— Enter the Default Domain.

NOTE: If you enter all three Default Sign-on credentials (Username, Password and Domain), you are automatically logged on to your desktop upon system start.

Configuring the authentication settings

To configure the authentication settings:

1 From the floating bar menu, click the **System Setup**, and then click **Remote Connections**.
The **Remote Connections** dialog box is displayed.

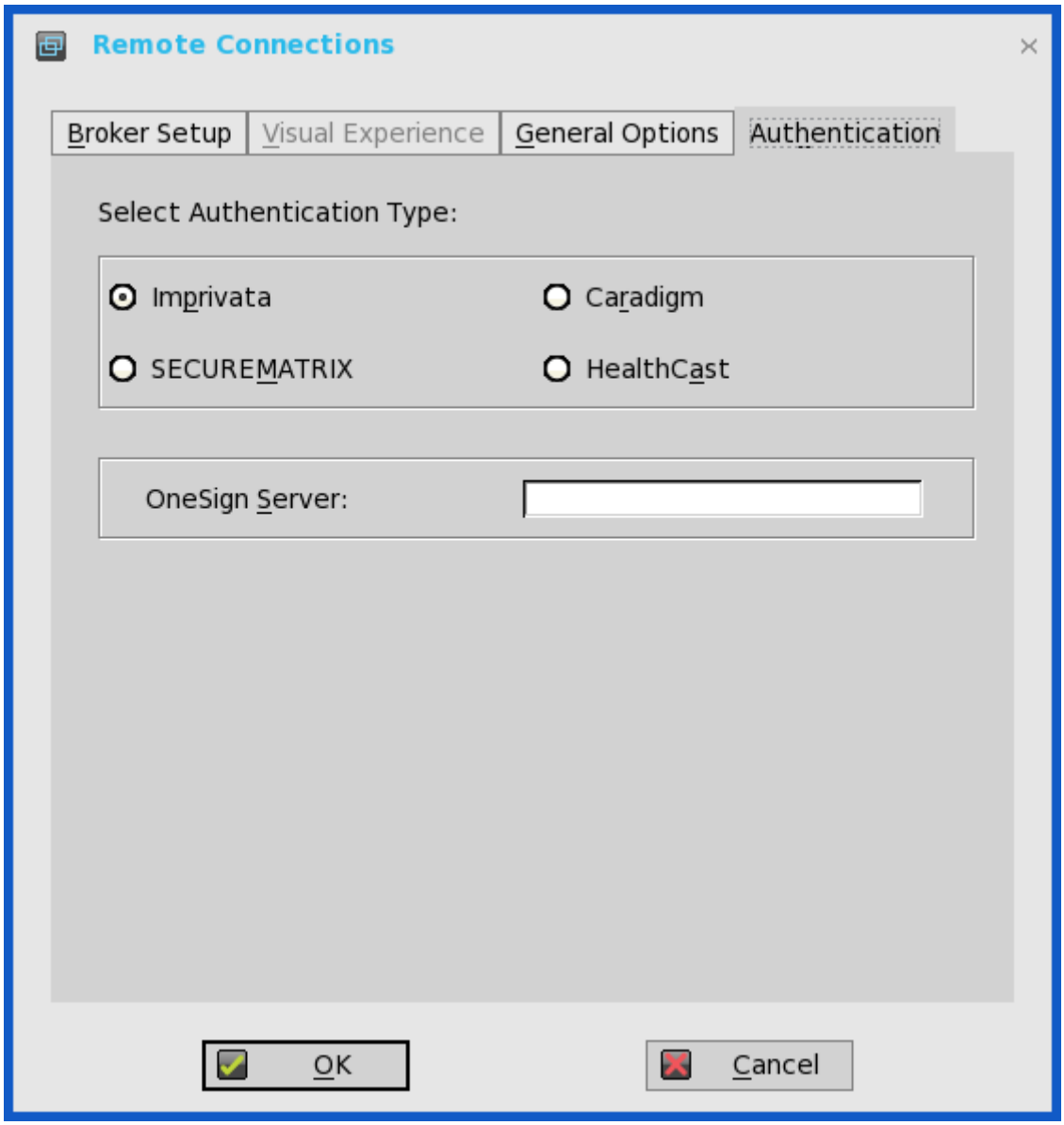


Figure 14. Authentication settings

2 Click the **Authentication** tab, and use the following guidelines:

a **Authentication type**— Click the button to select the Authentication type.

- **Imprivata** — OneSign Virtual Desktop Access provides a seamless authentication experience and can be combined with single sign-on for No Click Access to desktops and applications in a virtual desktop environment.

To configure the OneSign **Server**, enter either https://ip or https://FQDN values, reboot the client to display the logon dialog box, and then enter credentials to open the VDI broker dialog box for logon use. You can also set this feature in your INI file, see Parameters for a xen.ini File in this guide.

The following OneSign features/actions are supported:

- Client and Broker Authentication
  - Citrix Virtual Apps (formerly Citrix XenApp)
  - Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop)
- Kiosk Mode
- Fast User Switching
- Non-OneSign user VDI access
- Hotkey Disconnect
- Proximity card reader redirection
- Guided Question and Answer login
- Authenticate w/Password
- Authenticate w/Password + Password Change
- Authenticate w/Password + Password Change | New Password is Invalid
- Authenticate w/Proximity Card + Password
- Authenticate w/Proximity Card + Pin
- Authenticate w/Proximity Card + Pin | Pin not enrolled
- Authenticate w/Proximity Card Alone | Retrieve Password
- Retrieve User Identity Password
- Reset User Identity Password
- Update User Identity Password
- Enroll Proximity Card
- Lock/Unlock Terminal with Proximity CardLock/Unlock Terminal with Proximity Card

- **Caradigm** — Caradigm Single Sign-on and Context Management is the product of the Caradigm Company which provides Single Sign-on and Context Management Services.

  a **SSO & CM Server**— Enter the IP addresses of the Single Sign-On (SSO) and Context Management (CM) Servers.

  b **Default Group Name** —Type the name of the default group in the **Default Group Name** box.

  c **Enable logoff remote desktop**

  - Select the check-box to log off the current user from the session before system sign-off.
  - Clear the selection to disconnect from the session.

- **SECUREMATRIX** — SECUREMATRIX enhances the security of enterprise and cloud-based applications while providing seamless end user experience for a one-time password (OTP) that can be used for authentication with desktops, Windows, VPNs, intranets, extranets, web servers, e-commerce and other network resources.

  To configure the **SECUREMATRIX Server**, enter either https://ip or https://FQDN values, reboot the client to display the **log on** dialog box, and then enter credentials to open the **VDI broker** dialog box for logon use. You can also set this feature in your INI file, see the *INI section* in this guide. For details on SECUREMATRIX, see *SECUREMATRIX* documentation.

- **HealthCast Single Sign-On (SSO)**—HealthCast Single Sign-On (SSO) solution is designed to improve user convenience, streamline workflow, and strengthen security compliance in demanding environments. The same proximity cards used for physical access are used to tap-in and tap-out of unique user sessions and to tap-over any sessions unintentionally left open on the ThinOS Lite devices. Typically, you must type in your password only one time each day and use your proximity cards to streamline workflow and save time as they move between shared computers securely. Also, proximity cards can be secured

with a PIN, if configured by the organization. The HealthCast SSO solution also supports user self-service password reset so that you can reset your own passwords without the need to call the help desk.

- **OneSign Server**— Enter the IP Address of the OneSign Server.

3 Click **OK** to save the settings.

Configuring objects on Imprivata server

This version of ThinOS Lite supports Imprivata WebAPI version 5. This version supports Configuration objects to control different aspects of client behavior. User can experience the Imprivata WebAPI feature on OneSign server 4.9 or later versions.

This version supports configuration objects to control different aspects of the client behavior.

Use the following guidelines to configure the objects on Imprivata Server:

1 **Configuring the General configuration object**

a On the Imprivata server, click **Computer policy**, and then click **General** tab.

b Select the check box to allow users to shut down and restart workstation from lock screen.

NOTE: Display shutdown button and restarts commands to the user on the OneSign GINA.

The following configuration objects are supported on Imprivata server:

- **Shutdown Allow**
  - If you enable this feature by selecting the check box, the **shutdown** and **restart** icon is shown in ThinOS Lite login and locked windows.

Figure 15. Imprivata

- If you clear the check box, the **shutdown** and **restart** icon is grayed out.

- **FailedOneSignAuth Allow**—

  Only yes or no options are supported. Non-OneSign user can log in to the Broker by clicking **No** radio button.

- **Logging Allow**

  - OneSign logs could output on ThinOS Lite with this feature. An INI configuration is needed correspondingly.
  - Loglevel=0/1/2/3. The default value is 0. If set to 0, logs are not displayed.

- **Display name format** — Account name can be shown correctly with different formats in pop-up notifications.

2 **Configuring the Walkway configuration object**

On the Imprivata server, click **Computer policy**, and then click the **Walk Away** tab.

- **Key mouse inactivity enabled and behavior** — The check box **in addition to keyboard and mouse inactivity** is not supported.
- **Passive proximity cards**

  - If you want to use proximity card to lock the computer, select the **Tap to lock** check box.
  - If you want to lock the computer and log in as a different user. select the **Switch users** check box.
  - INI parameter is`TapToLock=0/1/2`.

- **Lock warning enabled and type—** The three types that are supported are: none, notification balloon and Screensaver.
  - None — No warning messages are displayed.
  - Notification balloon— ThinOS Lite displays a notification window.

- Screensaver— Hide the display contents before the workstation locks.

- **Warning message**— The message can be customized.
- **Lock Screen type** —Only obscure type is supported.
- **Hot key to lock workstation or log off user**— ThinOS Lite can support following keys:

  “F1 ~ F12”, "BKSP", “DEL”, “DOWN”, “END”, “ENTER”, “ESC”, “HOME”, “INS”, “LALT”, “LEFT”, “LCONTROL”, “NUMLOCK”, “PGDN”, “PGUP”, “RCONTROL”, “RIGHT”, RTALT”, “SPACE”, “TAB”, “UP”, “a~z”, “A~Z”, “0~9” and modifier “+”, “%”, “^” (Shift, Alt and Control)

- **Suspend action** — The server configuration controls this feature on ThinOS Lite. Therefore a new INI is added— `SuspendAction=0/1`; 0 means lock, 1 means signoff.

3 **Configuring the SSPR Configuration Object**

The SSPR configuration object controls the Self-Service Password Reset behavior for a user. The enabled attribute specifies whether the user is allowed to reset their password as part of emergency access. The mandatory attribute specifies whether the user must reset their password as part of emergency access.

4 **Configuring the RFIDeas configuration object**

The RFIDeas configuration object controls the behavior of the RFIDeas readers. The configuration can be configured by two ways, the computer policy of OneSign server and ThinOS Lite INI.

5 **Configuring the Custom background configuration object**

On the Imprivata server, click **Computer policy**, and then click the **Customization** tab.

Custom background image impacts the wallpaper of ThinOS Lite sign-on screen.

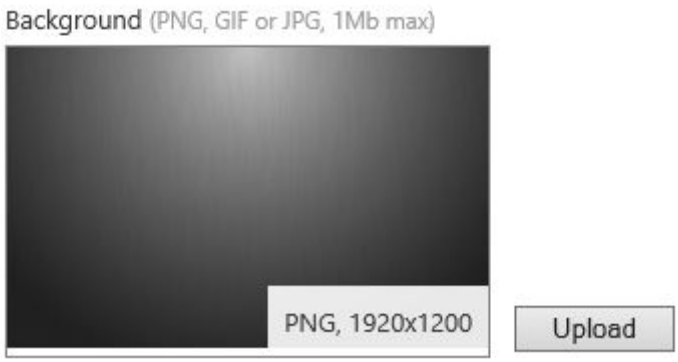


Figure 16. Background

6 **Configuring the Co-Branding configuration object**

On the Imprivata server, click **Computer policy** , and then click **Customization**.

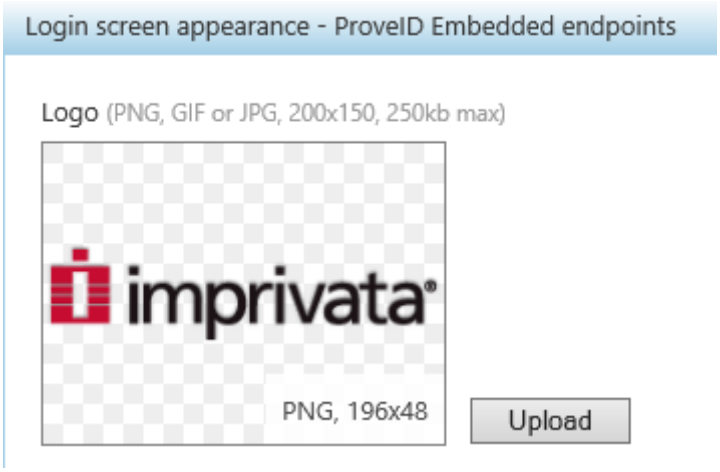


Figure 17. Login screen appearance

Logo image impacts all the dialog boxes in ThinOS Lite with raw logo.

7 **Configuring the SSPR Customization Configuration object**

- The text displayed in sign-on UI and lock window can be customized.
- The largest size supported by ThinOS Lite is 17 characters.

ThinOS Lite UI:

Figure 18. Imprivata OneSign

8 **Password Self-Services force enrollment feature**

Selecting this check box allows you to reset the primary authentication password.

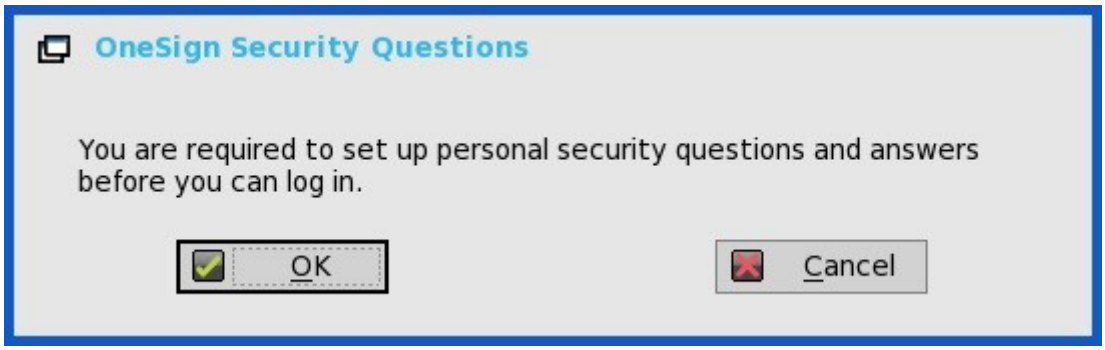


Figure 19. Security question

INI configuration for Imprivata OneSign Server

A new INI parameter is added to the `OneSignServer=AutoAccess=command`. The new value is `AutoAccess=Local`. When `AutoAccess`is set to local, the ThinOS Lite ignores the brokers that are set on the Imprivata OneSign Appliance and starts the broker/ connections which are defined in xen.ini or local defined on the client. You can start the ThinOS Lite connections while supporting Imprivata user authentication.

Proximity card enrollment

1 Tap the proximity card. The card enrollment page is displayed.

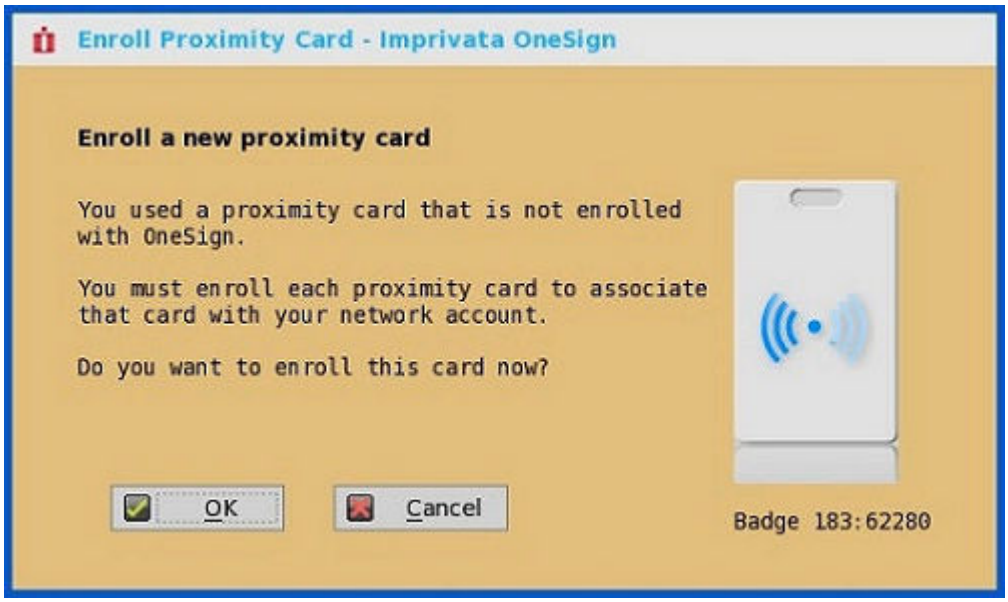


Figure 20. Enroll proximity card

2 Enter the credentials and then click **OK**.

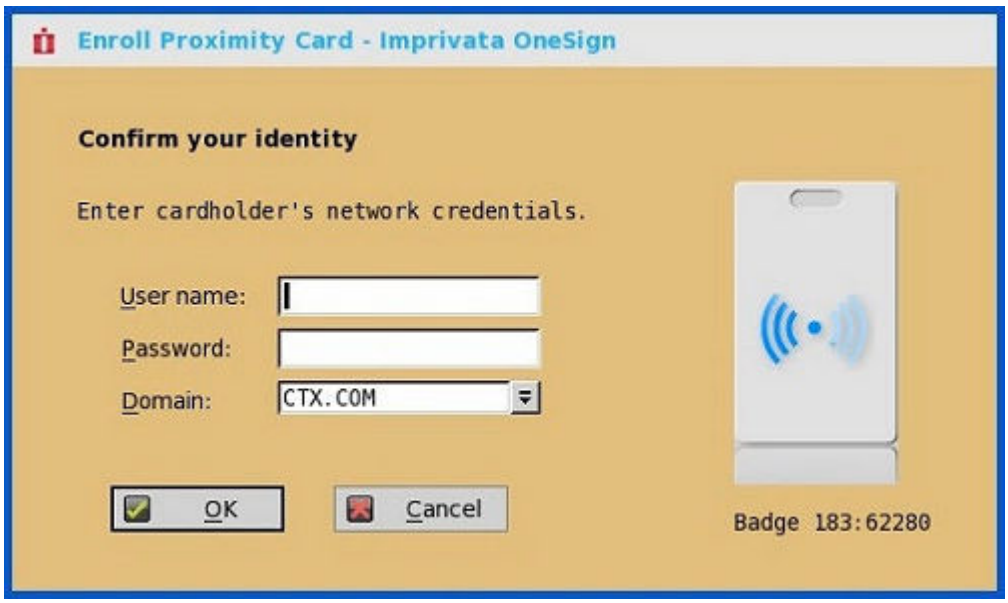


Figure 21. Confirm identity

Proximity card is enrolled successfully.

Figure 22. Proximity card success message

Imprivata bio-metric single sign-on

Imprivata WebAPI is updated to version 5. The key feature of this version is the Fingerprint identification feature. This feature is highly reliable, and cannot be easily replicated, altered, or misappropriated.
The prerequisites of OneSign server are:

- Imprivata v4.9 or later appliance version is needed that supports the WebAPI v5 and later versions.
- Fingerprint identification license is required.

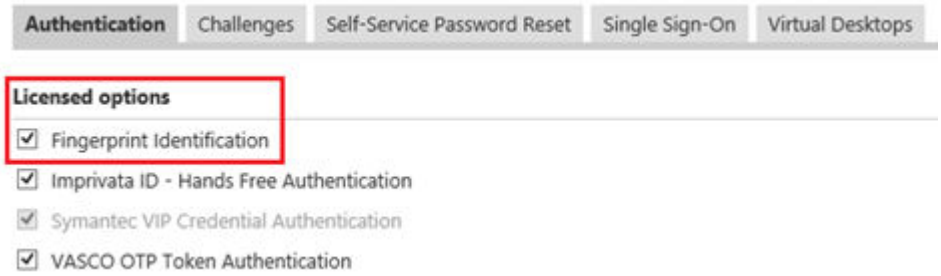
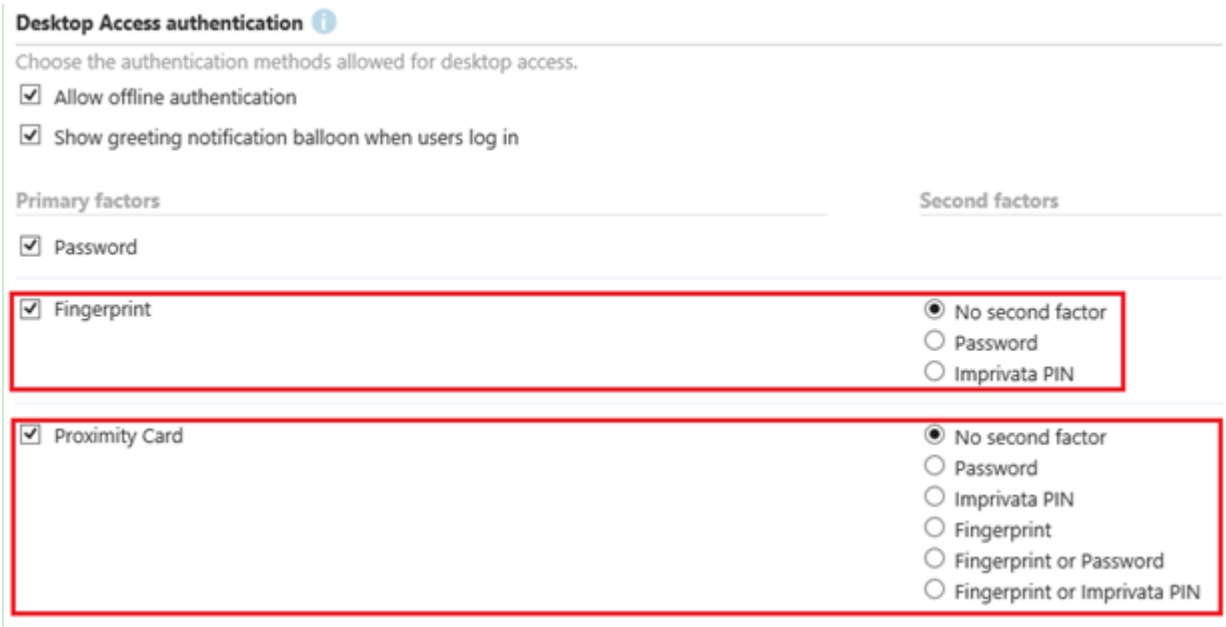


Figure 23. Licensed options



.

Figure 24. Desktop access authentication

Fingerprint authentication must be enabled in OneSign user policy

Following are the features of Imprivata Bio-metric Single Sign-On:

1 Supported protocol is ICA.

2 Required Fingerprint reader devices are:
   a ET710 (PID 147e VID 2016)
   b ET700 (PID 147e VID 3001)

3 Fingerprint authentication to sign-on/unlock for ThinOS Lite devices. For more information, see Signing in or Unlocking ThinOS Lite Devices using Fingerprint Authentication.

4 Fingerprint authentication to unlock the virtual desktop. For more information, see Unlocking Virtual Desktop using Fingerprint Authentication

5 ThinOS Lite supports the following Fingerprint authentication combinations:

Table 7. Fingerprint authentication combinations

Primary Factors	Secondary Factors
Fingerprint	No second factor
	Password

Primary Factors	Secondary Factors
	Imprivata PIN
Proximity Card	Fingerprint
	Fingerprint or Password
	Fingerprint or Imprivata PIN

Signing in or unlocking ThinOS Lite devices using fingerprint authentication

To sign-on/unlock the ThinOS Lite devices using fingerprint authentication, do the following:

1 Configure the OneSign server on ThinOS Lite, and then plug-in the fingerprint reader device.
The ThinOS Lite Fingerprint window is displayed automatically after OneSign server is initialized.

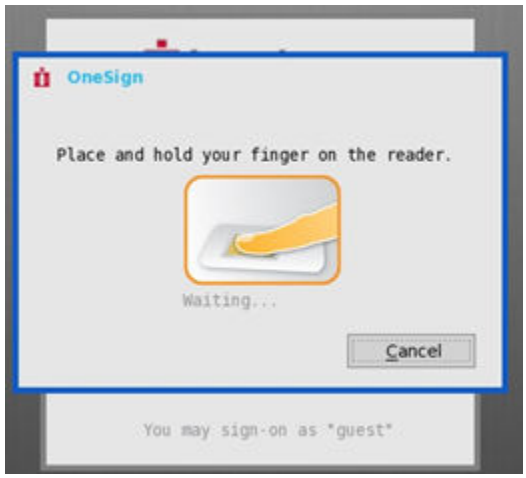


Figure 25. OneSign

2 Fingerprint authentication works on the ThinOS Lite unlock window.

Figure 26. Verifying administrator

Unlocking virtual desktop using fingerprint authentication

To unlock the virtual desktop using fingerprint authentication, do the following:

1 Enable the Imprivata Virtual Channel.

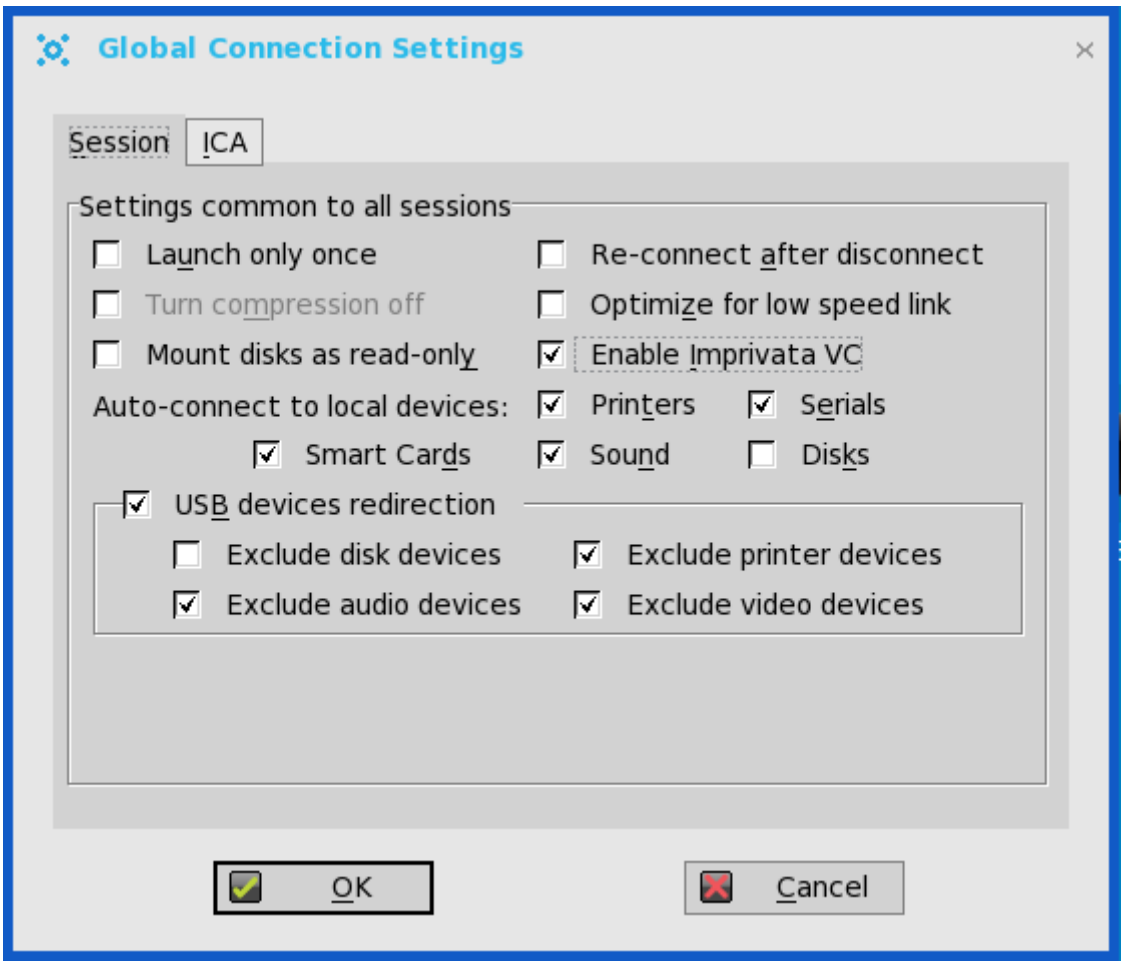


Figure 27. Global connection settings

2 When you lock the virtual desktop in the session, the Fingerprint window is displayed automatically

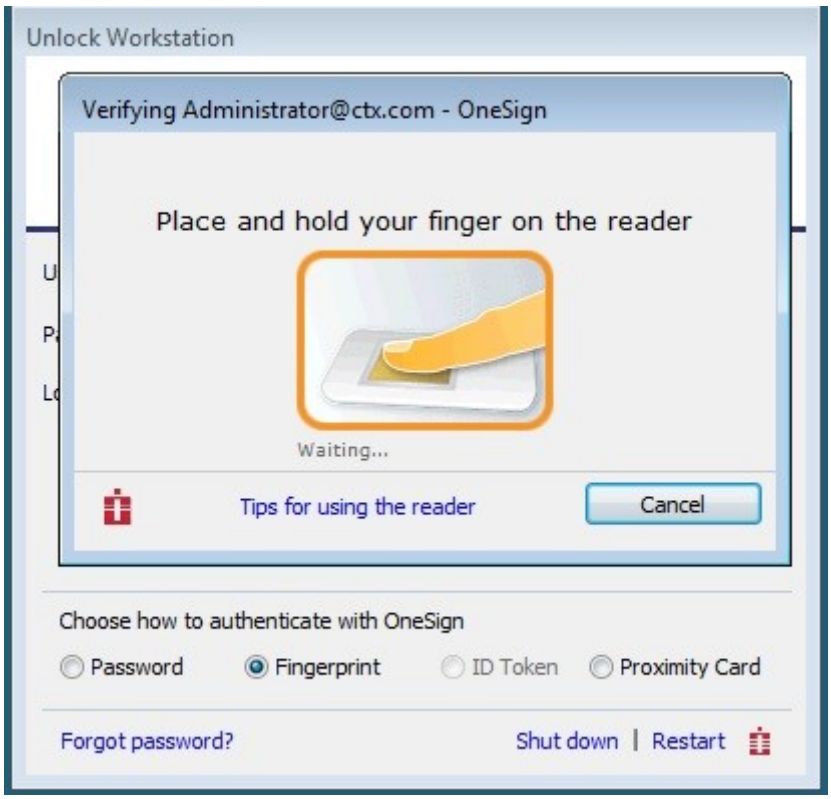


Figure 28. Verifying administrator

3 You can manage Fingerprints on virtual desktop. This requires OneSign agent v4.9. To manage Fingerprints, do the following:

a Right-click the OneSign agent icon in System tray.

b Click Manage Fingerprints, and enter the correct credentials in the displayed window to manage your Fingerprints.

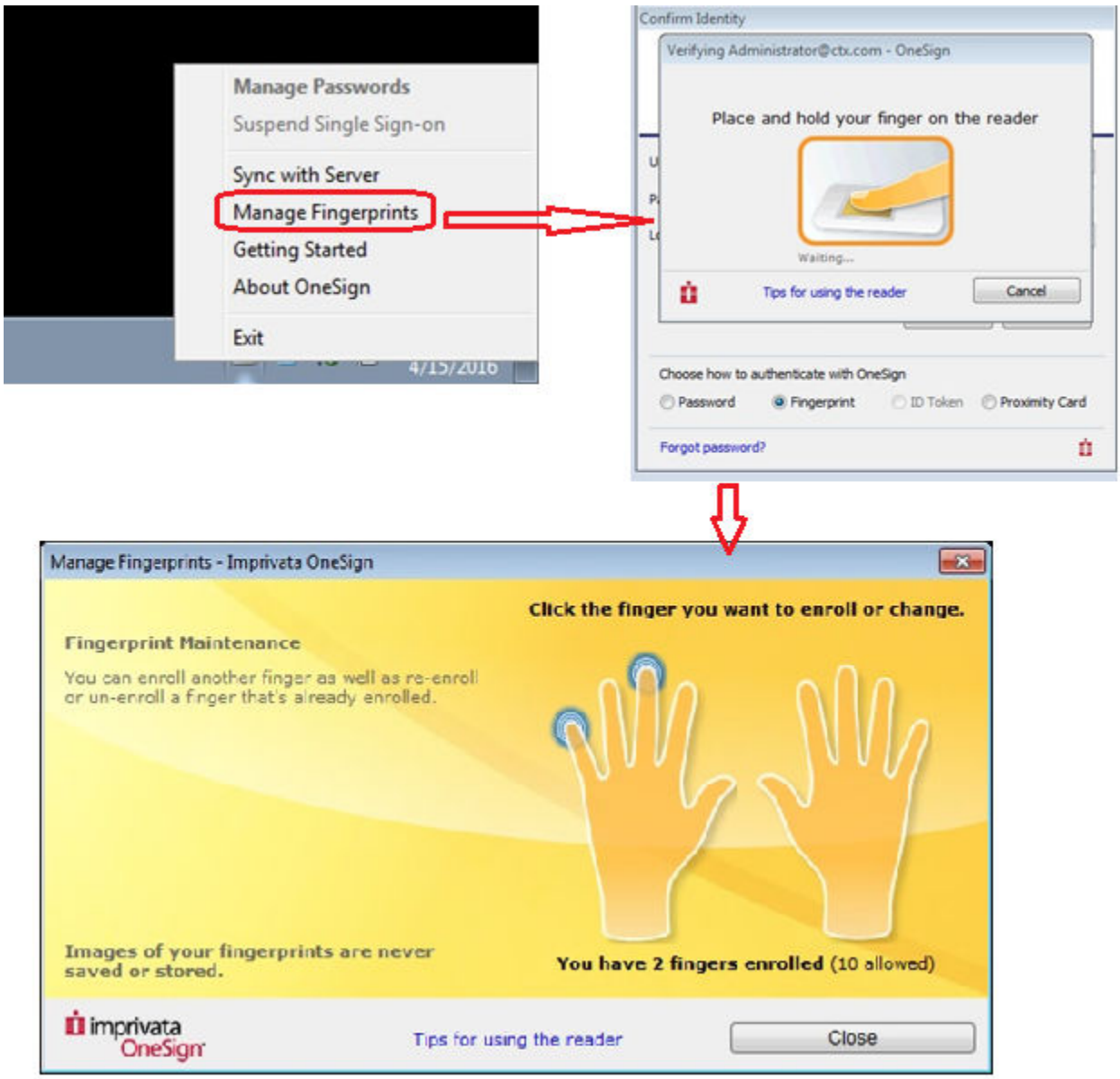


Figure 29. Manage fingerprints

Configuring the Caradigm Vault server

To configure the Caradigm Vault server on ThinOS Lite, do the following:

1 From the floating bar menu, click the **System Setup** , and then click **Remote Connections**.
The **Remote Connections** dialog box is displayed.

2 Click the **Authentication** tab, enter the IP address of the **SSO & CM Server** and then click **OK**.

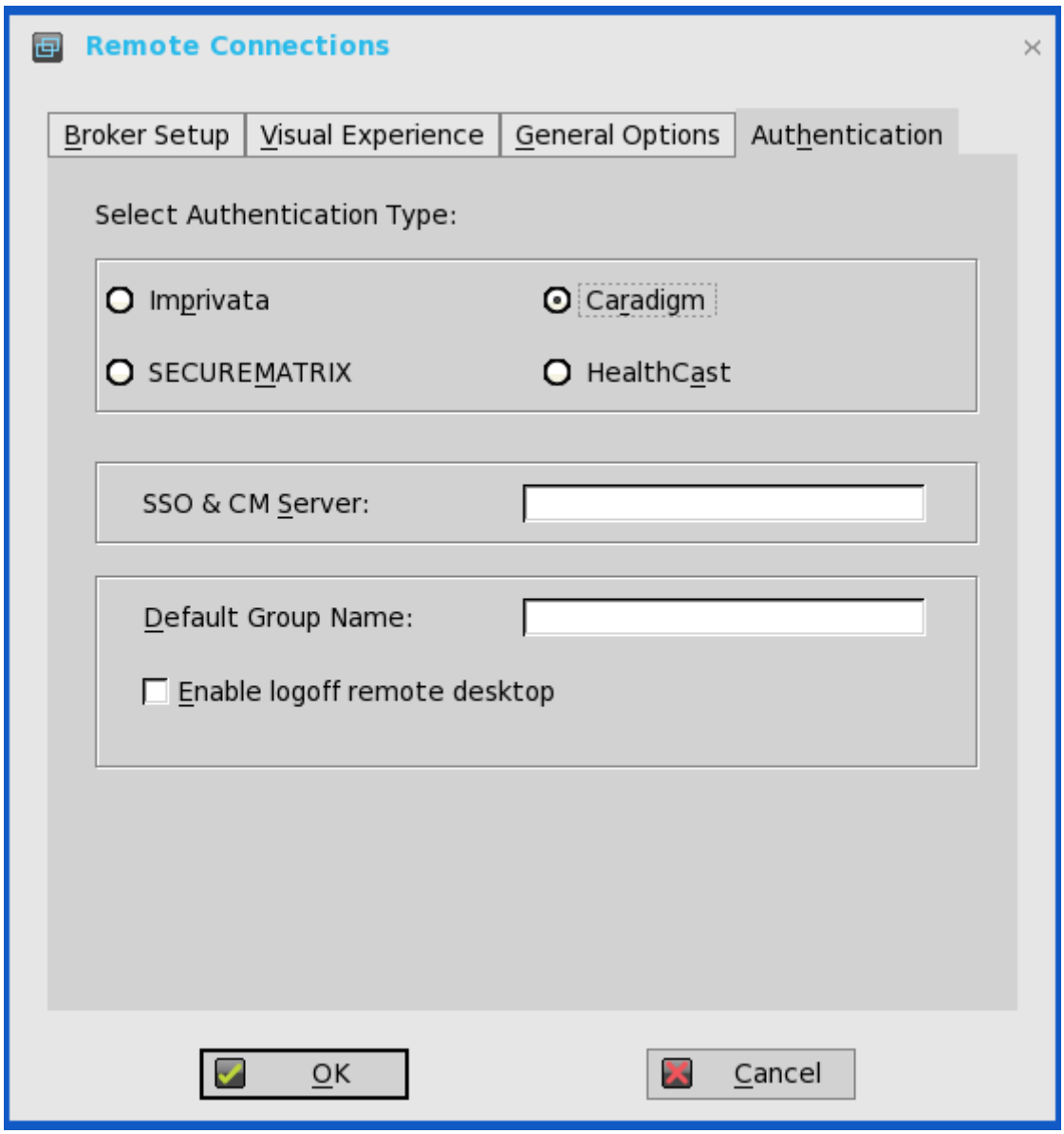


Figure 30. Remote Connections

3 On the Caradigm Vault Server, use the following guidelines:

- Ensure that the **Enroll unenrolled badges** option is checked.
- Make sure that all Badge ID mapping entries are deleted.

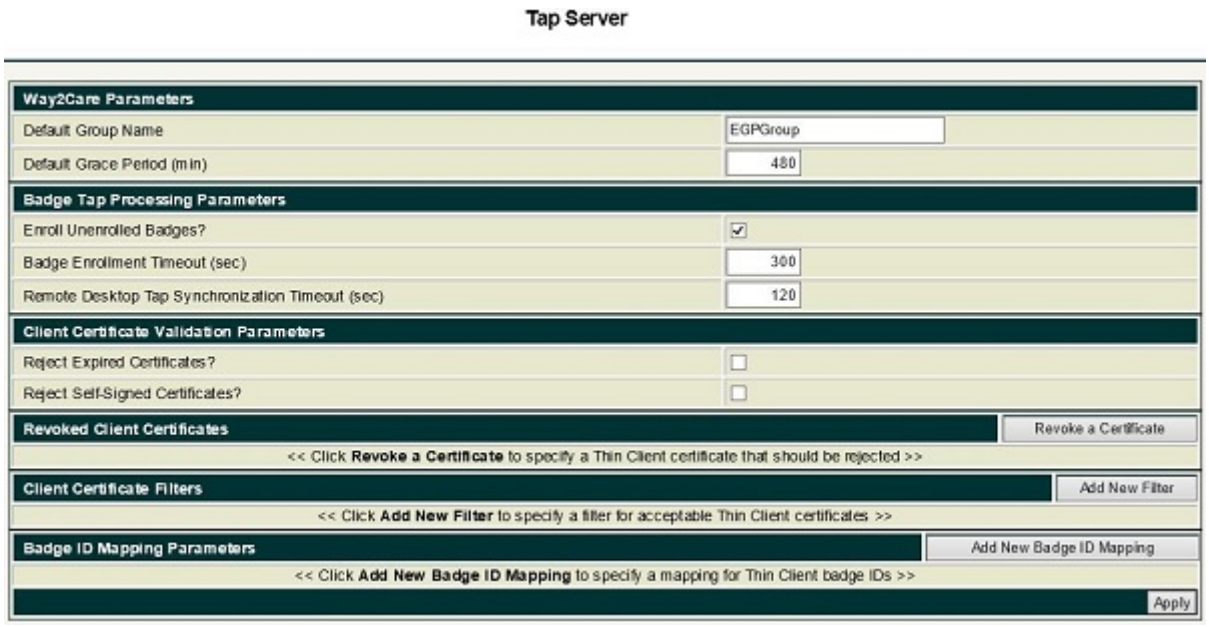


Figure 31. Tap server

4 Click **SSO&CM** > **Advanced Configurations** , and use the following guidelines:

Figure 32. Enable proximity server

a Ensure that the **Enable Proximity Support** check box is selected.

b Ensure that the **Enable way2care** check box is selected.

5 To prepare a certificate to the Caradigm Vault Server, use the following guidelines:

The Caradigm Vault Server uses the certificate to validate the connection between the Tap Server and the zero client.

a To raise a request for the certificate:
   - The certificate should be issued by your Certificate Authority.
   - Prepare the certificate in two formats:
     - PFX format which has a private key.
     - The other is PEM format which is text-based, Base64-encoded DER file. For Example, Caradigm.cer, Caradigm.pfx.

b To import a certificate to the zero client, use either of the following two options:
   - Click **System Setup** > **System tools** > **Certificates** to import certificates from USB storage or file server.
   - Use INI file to import certificate.

     ```
     AddCertificate=client_cert.pfx password=passpass
     ```

c To add a certificate to Vault server:

Figure 33. Thin client certificates

Use the **zero client Certificates** page to add certificates for the zero client devices. The certificate must be a text in PEM format, that is, a text-based Base64-encoded DER file.

- Open the DER cert file on Notepad.
- Log in to the Vault Server Admin Console, and then click **Appliance** > **zero client Certificates**.
- Copy the Notepad text to the Vault server

Configuration on VDI Server and Desktops

Caradigm solution of ThinOS Lite supports the multi-types of VDI server such as Citrix Virtual Apps 6.5, Citrix Virtual Apps and Desktops 5.6, and Citrix Virtual Apps and Desktops 7.6.

To configure the VDI server and desktop:

- Install the Caradigm desktop components in the servers and desktops.
- Indicate vault server IP, and then provide a valid security token.
- Add following lines to Service section of the**\programdata\sentillion\vergence\Authenticator.ini configuration file**.

```
TapServerIdentification=True
RemotePromptForPassword=Badge
```

Caradigm Way2Care

Way2Care is part of Caradigm Identity and Access Management (IAM) portfolio, and is designed to securely access patient information from multiple clinical applications.

In ThinOS Lite version 2.6, a new INI parameter `CaradigmServer=xxx UseWay2Care=yes` is added to support Way2Care. You can also set `DisableManualLogon=yes EGPGroup=xxx` along with the Caradigm Server parameter. This feature uses Way2Care API that is different from the TapServer API. Way2Care uses the decimal UID format.

For more information about the INI parameter, see the *Dell Wyse ThinOS Version 8.6 INI Reference Guide* at www.dell.com/support.

For more information about the Caradigm Way2Care feature, go to www.caradigm.com.

Introduction to HealthCast

HealthCast Single Sign-On (SSO) solution is designed to improve user convenience, streamline workflow, and strengthen security compliance in demanding environments. The same proximity cards used for physical access are used to tap-in and tap-out of unique user sessions and to tap-over any sessions unintentionally left open on the ThinOS Lite devices. Typically, you must type in your password only one time each day and use your proximity cards to streamline workflow and save time as they move between shared computers securely. Also, proximity cards can be secured with a PIN, if configured by the organization. The HealthCast SSO solution also supports user self-service password reset so that you can reset your own passwords without the need to call the help desk.

NOTE: HealthCast SSO Solution on ThinOS Lite is a client-server solution. ThinOS Lite provides the client-side functionality, but you must also install and configure the HealthCast Server components on a server system in order for the solution to work properly. Contact HealthCast on HealthCast website for one or more server installation executables, server requirements, and configuration information.

Configuring HealthCast on ThinOS Lite

HealthCast Web API Server is integrated with ThinOS Lite release to implement the HealthCast SSO solution. To use the HealthCast SSO solution, ThinOS Lite must be configured to use the HealthCast Web API Server. You can do this by using the INI file (wnos.ini), or using the ThinOS Lite UI. Dell recommends you to use the INI file for large deployments.

ThinOS Lite UI configuration

- To use the HealthCast Web API, configure the HealthCast settings on the zero client side. To configure, do the following:
  a From the desktop menu, click **System Setup** , and then click **Remote Connections**.
  The **Remote Connections** dialog box is displayed.
  b Click the **Authentication** tab, and then click **HealthCast**.

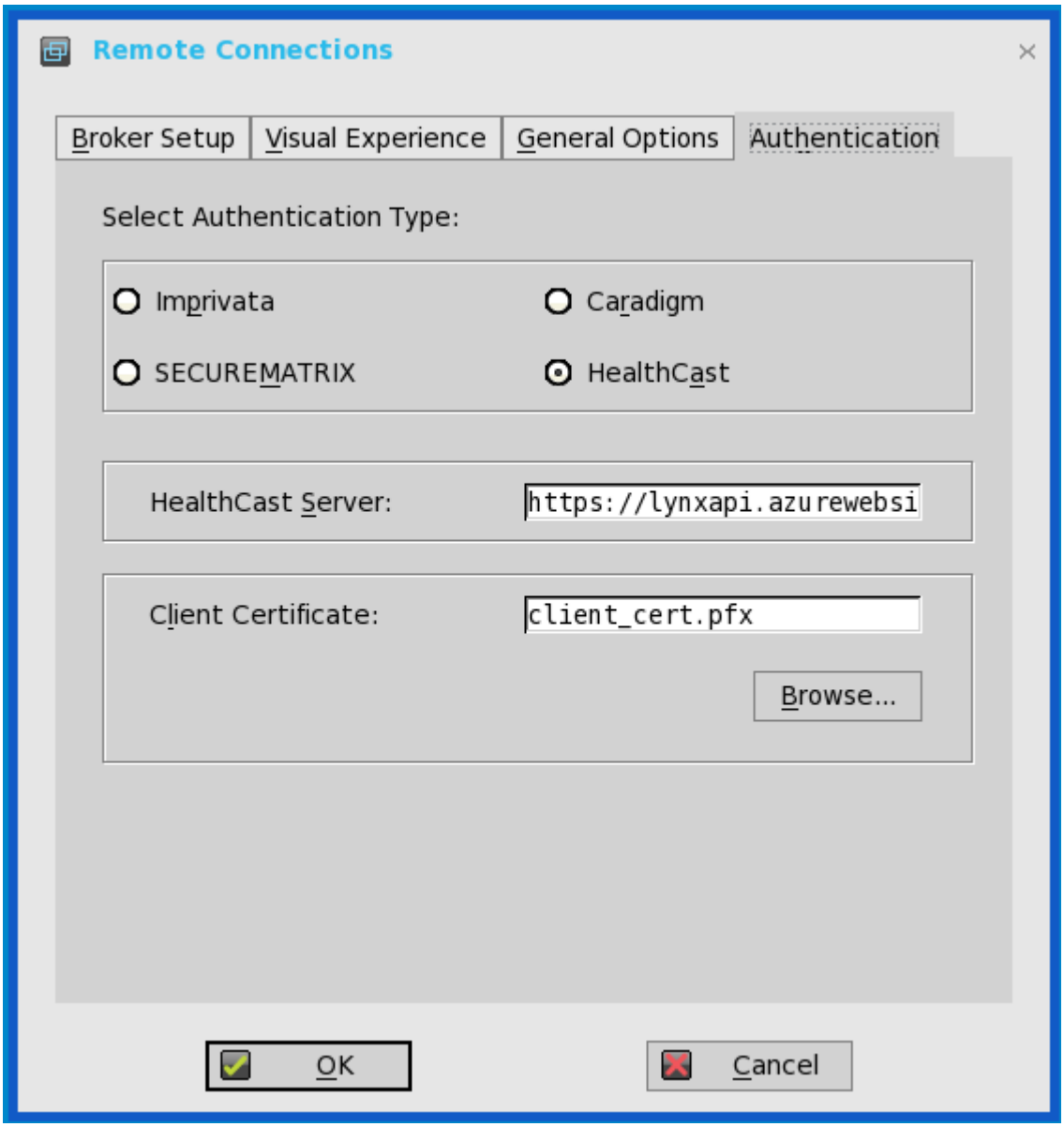


Figure 34. Remote connections

c Enter the HealthCast server details in the box provided.

d To import the client certificate, click **Browse**, and select the appropriate certificate you want to use.

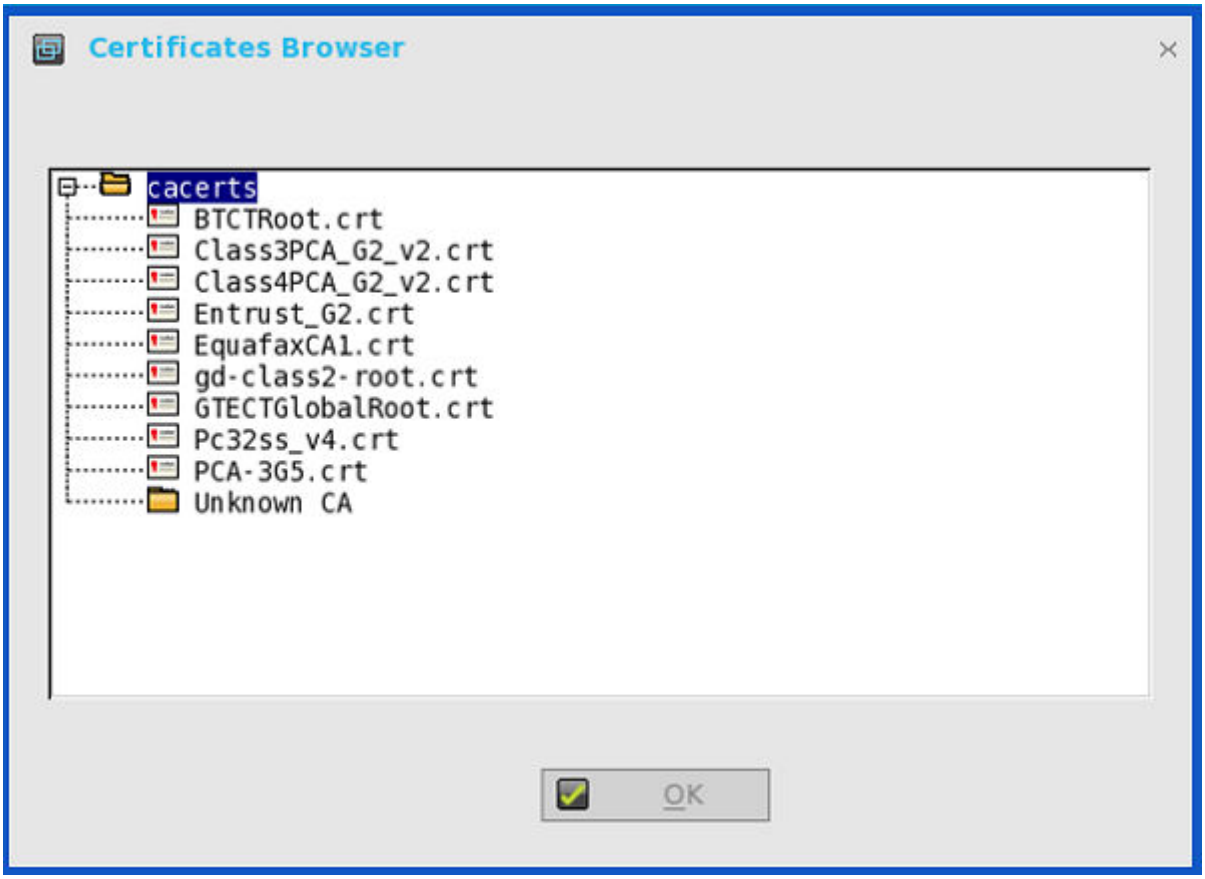


Figure 35. Certificates browser

e Click **OK** to save the settings.

INI configuration

To configure using INI parameters, add the following INI parameters to your wnos.ini file:

- HealthCastServer— The server address and options needed for the client to connect to the HealthCast Web API Server.
  HealthCastServer=<https address> SecurityMode=<default, full, warning, low> ClientCertificate=<cert-pfx-file-name>
  For example: HealthCastServer=https://server1.example.com SecurityMode=full ClientCertificate=client-cert.pfx.

  For more information on INI parameters, see INI parameters

HealthCast SSO features and functionality on ThinOS Lite

The following are the HealthCast SSO features and functionality on ThinOS Lite:

- **Proximity card enrollment**
  - HealthCast supports user self-enrollment. Therefore, there is no need to bring the proximity card to a special registration station, or for IT staff to be involved. Instead, you must only tap the disenrolled proximity card at a terminal and you can follow the easy registration process. This is a one-time event after which you can use the card wherever HealthCast is installed.

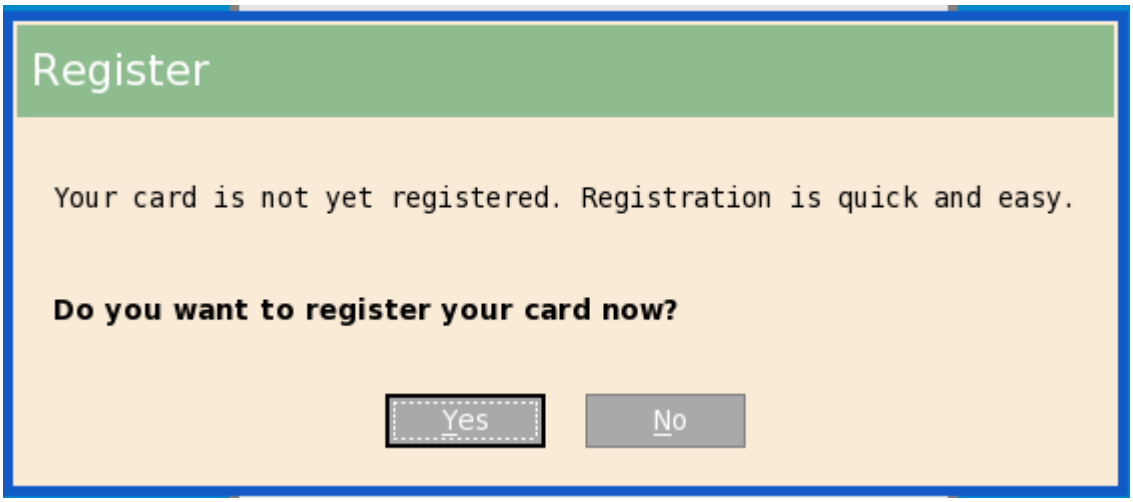


Figure 36. Proximity card enrollment

- **Manual login and lock/unlock terminal**
  - If you do not have a card, or choose not to use your card, then you can manually log in using your user name and password. Administrators can disable manual login, if they wish, so that users can sign on with their proximity cards. You can also lock or unlock the terminal, if you have signed on with a manual login.

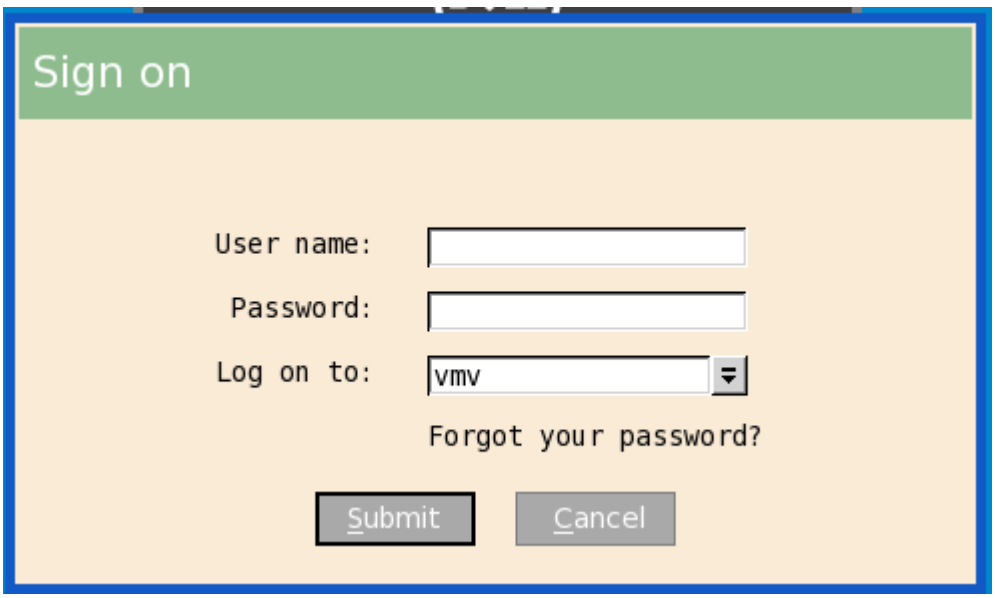


Figure 37. Manual login and lock/unlock terminal

- **Proximity card login and lock/unlock terminal**
  - After the proximity card is registered, tap the card at a terminal to login.

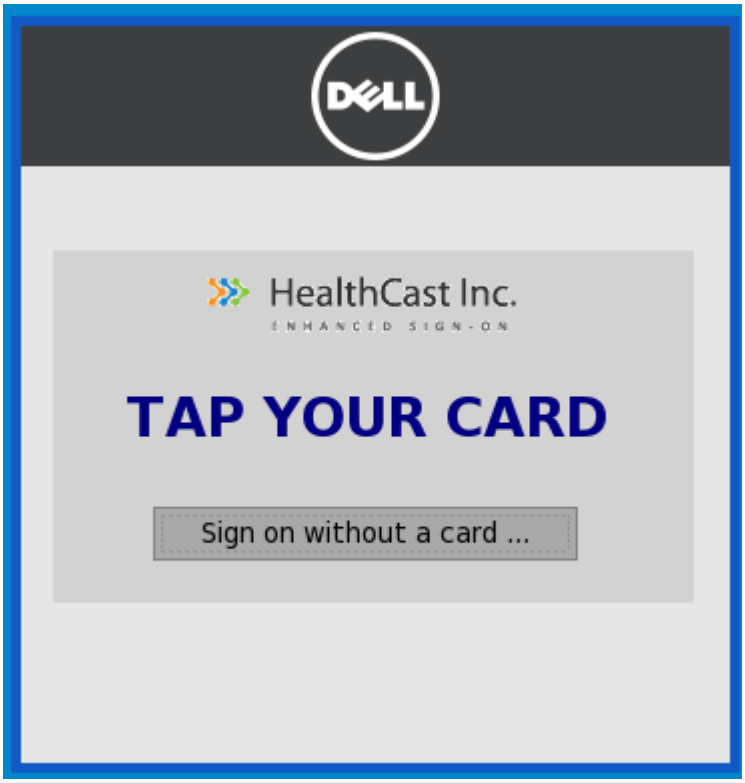


Figure 38. Login

You can lock the session to secure it, but leave the remote session connected for fast access when you return. To do this, tap the proximity card and the session is locked.

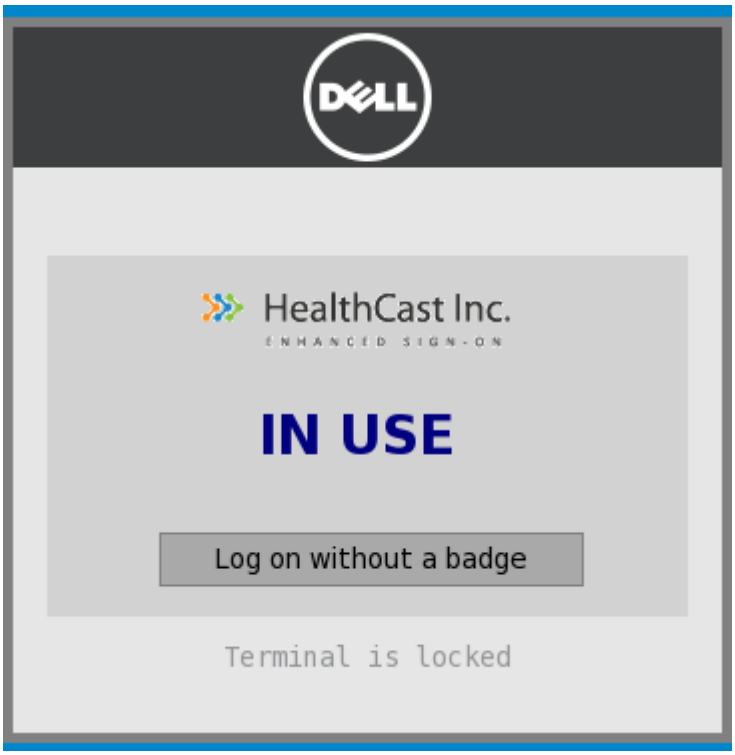


Figure 39. Lock terminal

To resume the session, tap the card again.

- **Walk away**
  - Terminals can be configured to lock or log off sessions that have been left open. The time that will elapse before automatic lock or log off can be set by an administrator using the convenient web administration application.
- **Tap-Over**
  - If a session is locked or left open, a second user can tap their own proximity card and this will disconnect the first session and log the second user into their own unique session.
- **Forgotten card**
  - If you forget your card at home, you can receive a temporary card and register it for the day using the same easy registration process mentioned above.
- **Lost or stolen card**
  - If you report a card as lost or stolen, an administrator can immediately disable the card using the convenient web administration application. This prevents anyone else from using it.
- **Self-Service Password Reset (SSPR)**
  - If SSPR enabled by an administrator, you can register for SSPR and reset your passwords without calling the help desk.

Figure 40. SSPR enrollment

- **Easy to use web-based administration tool**
  - Administrators can quickly and easily configure settings, manage proximity cards, and users using a web-based administration tool.

Configuring the central configurations

Use the Central Configuration dialog box to configure zero client central connection settings such as file server, optional WDM server settings, and optional Cloud Client Manager.

Use the following options to configure the Central Configurations:

- Configuring the General Central Configurations.
- Configuring the WDA Settings

Configuring the general central configurations

To configure the General Central Configurations:

1 From the floating bar menu, click the **System Setup** , and then click **Central Configuration**.
The **Central Configuration** dialog box is displayed.

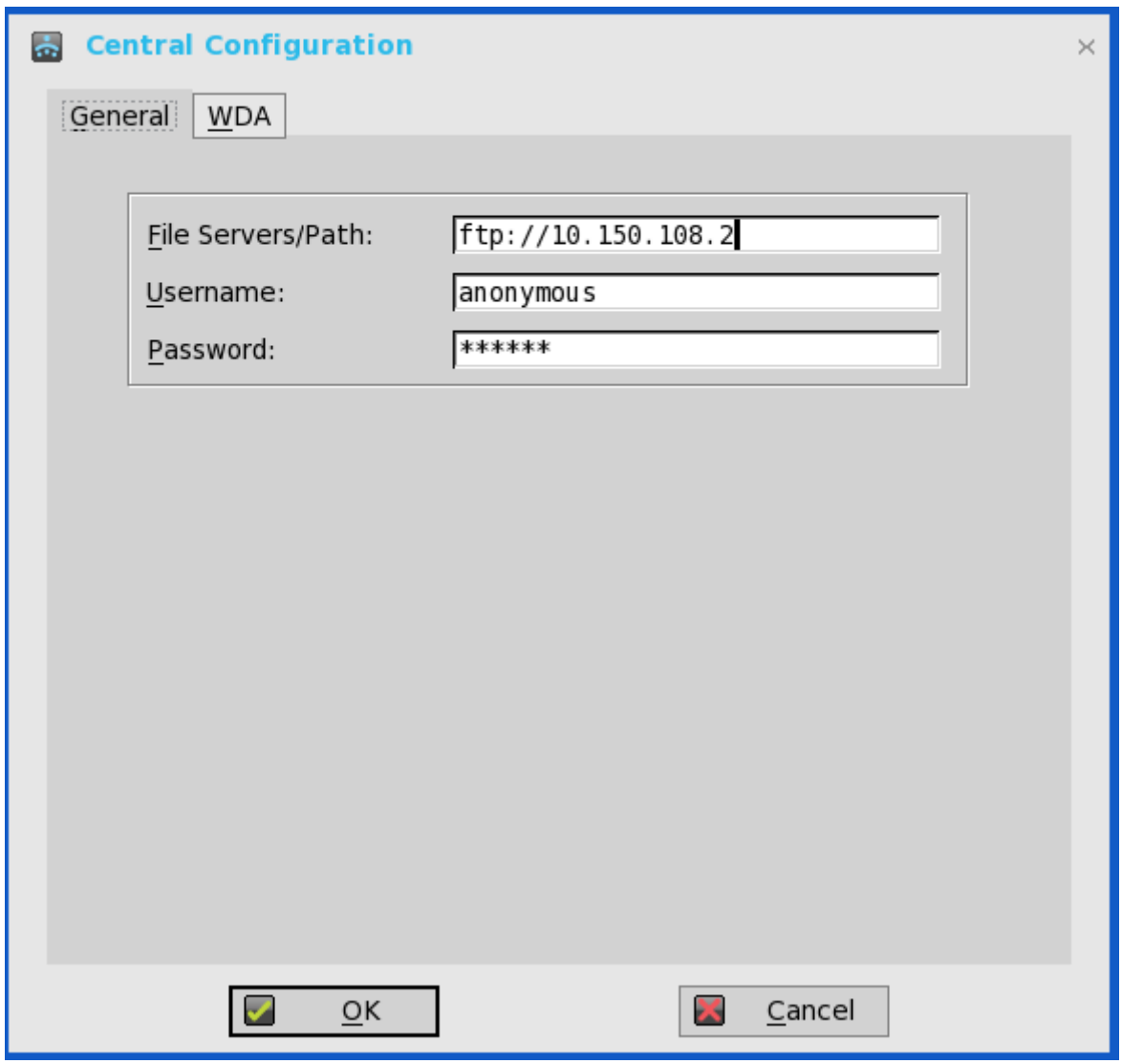


Figure 41. Central configuration

2 Click **General** tab and use the following guidelines:
File Servers/Path, **Username** and **Password** — IP address or host name of the file server that provides the system software and update images. The address can be supplied through DHCP, if DHCP is used.

   a **File Servers/Path** — Allows maximum of 127 characters for file server, and maximum of 127 characters for root path. The data specifies part of the path to be used when the server is accessed. Multiple file servers/paths may be named, as long as all data fits in the length limitation.
   b **Username** — To log in to the file server. Use maximum of 31 characters.
   c **Password** — To log in to the file server. Use maximum of 31 characters.

3 Click **OK** to save the settings.

Configuring the Wyse Device Agent settings

Use this tab to configure the Wyse Device Manager (WDA) and Wyse Management Suite settings.

ThinOS Lite supports all the Wyse Management Suite Group Policy settings. To configure the Wyse Management Suite settings, do the following:

1 From the desktop menu, click **System Setup**, and then click **Central Configuration**.

The **Central Configuration** dialog box is displayed.

2 Click **WDA** > **WMS**, and use the following guidelines:

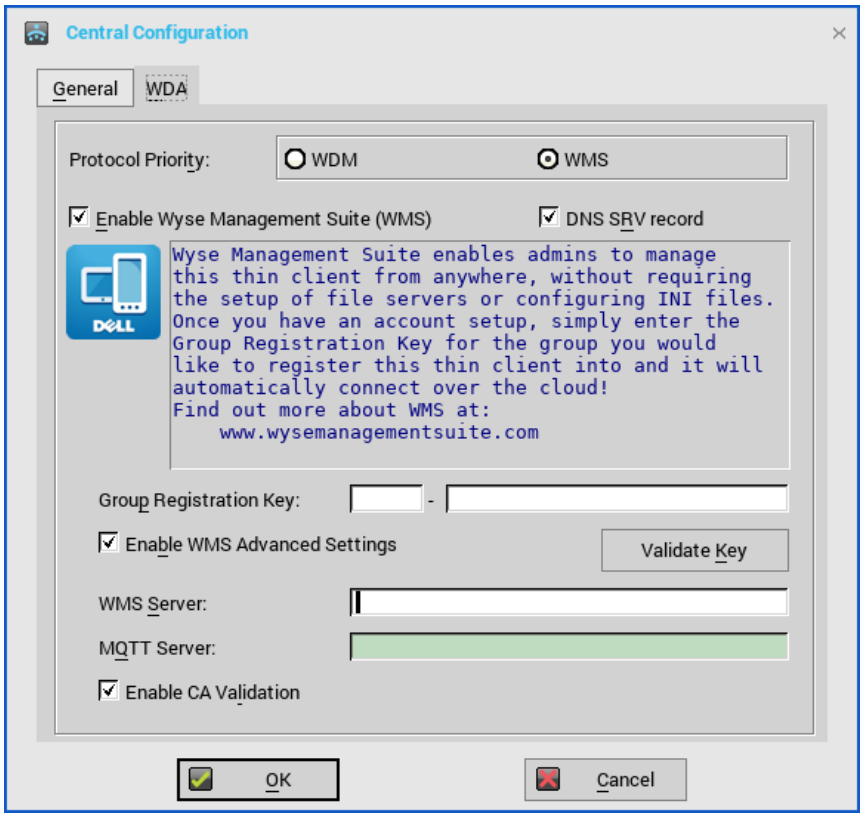


Figure 42. Central configuration

By default, the **WMS** option is selected. Wyse Management Suite service automatically runs after the client boot up.

If the first discovery, for example, the Wyse Management Suite service is not successful, it seeks for the next priority, for example, WDM service. This continues until a discovery is successful. If all discoveries fail, it is started again automatically after a fixed time—24 hours.

a **Enable Wyse Management Suite (WMS)**—Select the check box to enable the Wyse Management Suite to discover your thin client.

b **DNS SRV record**—Select this check box if you want the thin client to obtain the Wyse Management Suite values through DNS server, and then try to register into the Wyse Management Suite server. By default, the check box is selected. If the check box selection is canceled, the thin client cannot obtain the Wyse Management Suite values through DNS server.

To create DNS records in DNS server, use the following information:

WMS server URL

DNS Record Type: `DNS SRV`

Record Name: `_WMS_MGMT._TCP.<Domain>`

Value Returned: `WDMNG Server URL`

Example: _WMS_MGMT._TCP.WDADEV.com

MQTT Server URL

DNS Record Type: `DNS SRV`

Record Name: `_WMS_MQTT._TCP.<Domain>`

Value Returned: `WMS Server URL`

Example: _WMS_MQTT._TCP.WDADEV.com

Group Token

DNS Record Type: `DNS Text`

Record Name: `_WMS_GROUPTOKEN.<Domain>`

Value Returned: `Group Token` (as String)

Example: _WMS_GROUPTOKEN .WDADEV.com

CA Validation

DNS Record Type: `DNS Text`

Record Name: `_WMS_CAVALIDATION.<Domain>`

Value Returned: `TRUE or FALSE` (as String)

Example: _WMS_CAVALIDATION.WDADEV.com

c **Group Registration Key**—Enter the **Group Registration Key** as configured by your Wyse Management Suite administrator for the desired group. To verify the key, click **Validate Key**.

A Group Registration Key is not required for the private Wyse Management Suite server. You can provide the Wyse Management Suite server details to allow the device to check in to Wyse Management Suite. ThinOS Lite registers to a quarantine tenant in Wyse Management Suite.

d **Enable WMS Advanced Settings**—Select this check box to enter the Wyse Management Suite server, MQTT server details, and to enable the CA validation. By default, the MQTT server option is disabled. The MQTT server value is populated after the ThinOS Lite device is checked in to the Wyse Management Suite.

NOTE: If you enable the Wyse Management Suite, ensure that you have entered the Group Registration Key and configured the Wyse Management Suite advanced settings.

For more information about using Wyse Management Suite to manage the ThinOS Lite devices, see the Wyse Management Suite Administrator's Guide at Dell.com/manuals.

3 Click **OK** to save the settings.

When you modify the ThinOS Lite policy of the registered thin client using Wyse Management Suite, a dialog box is displayed prompting you to postpone or restart the thin client. To apply the settings immediately, click **Restart Now**. If you want to delay this task, click **Postpone**.

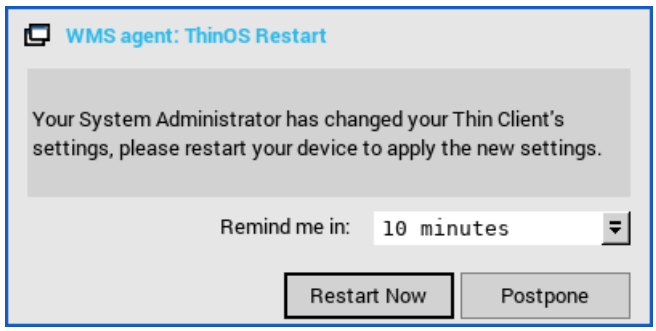


Figure 43. Wyse Management Agent: ThinOS Lite restart

To configure the WDM settings, do the following:

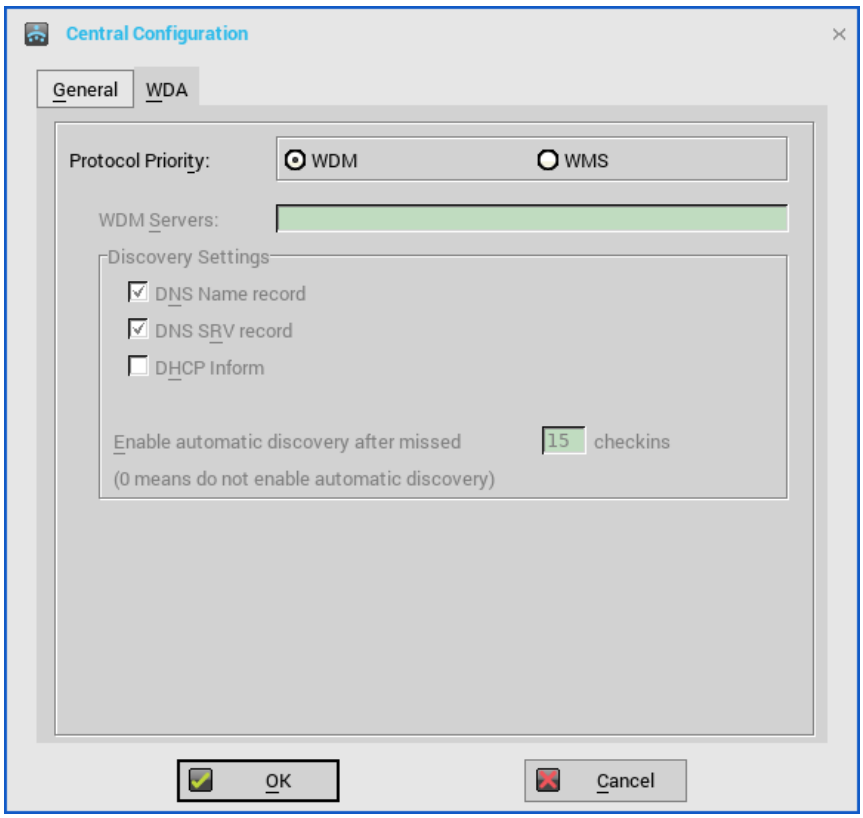


Figure 44. General central configuration

1 Click **WDM**, and use the following guidelines:

2 **WDM Servers**—Enter the IP addresses or host names, if WDM is used. Locations can also be supplied through user profiles, if user INI profiles are used.

3 **DNS Name Record**—(Dynamic Discovery) Allows devices to use the DNS hostname lookup method to discover a WDM Server.

4 **DHCP Inform**—(Dynamic Discovery) Allows devices to use DHCP Inform to discover a WDM Server.

5 **Enable Automatic Discovery After Missed Check-ins**—Select the number of missed check-ins after which you want the auto discovery options enabled.

6 Click **OK** to save the settings.

The Wyse Device Manager option can be disabled using the following INI parameters:

- WMSService=no
- Service=wdm disable=yes

- RapportDisable=yes

Configuring the VPN manager

The VPN Manager was included in ThinOS Lite to manage VPN connections. ThinOS Lite uses the OpenConnect client that is based on the SSL protocol for connecting to VPN. A virtual private network (VPN) extends a private network across a public network such as the Internet. It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if the devices are directly connected to the private network, while benefitting from the functionality, security and management policies of the private network.

To configure the VPN manager, do the following:

1 From the floating bar menu, click the **System Setup**, and then click **VPN Manager**.
The **VPN Manager** dialog box is displayed.

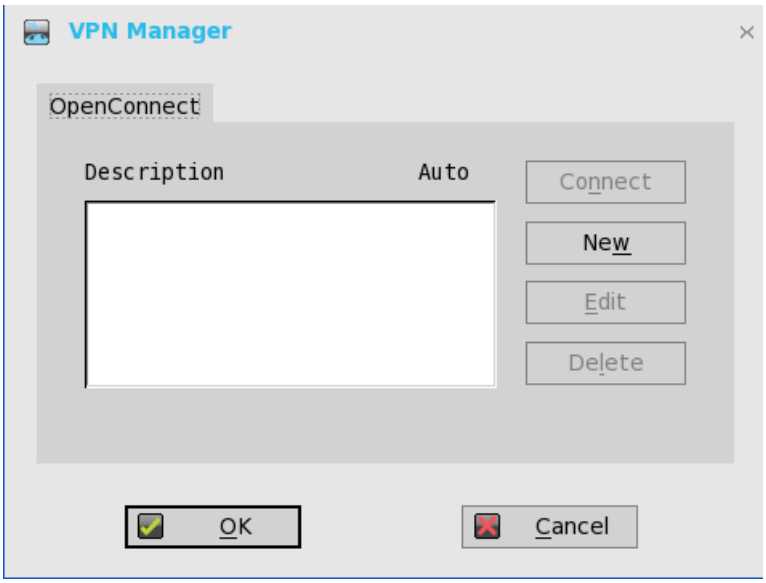


Figure 45. VPN manager

2 Click **New** tab to Create a new Connection.
The **OpenConnect Property** page is displayed.
- **Session Name** — Enter the name of the Session Name.
- **VPN Server** — Enter the IP address of the VPN Server.
- **Login Username**— Enter the Login Username.
- **Password**— Enter the password of the user.
- Select the check box to **Auto-connect on system startup**.
- Select the check box to **Show progress in detail**.

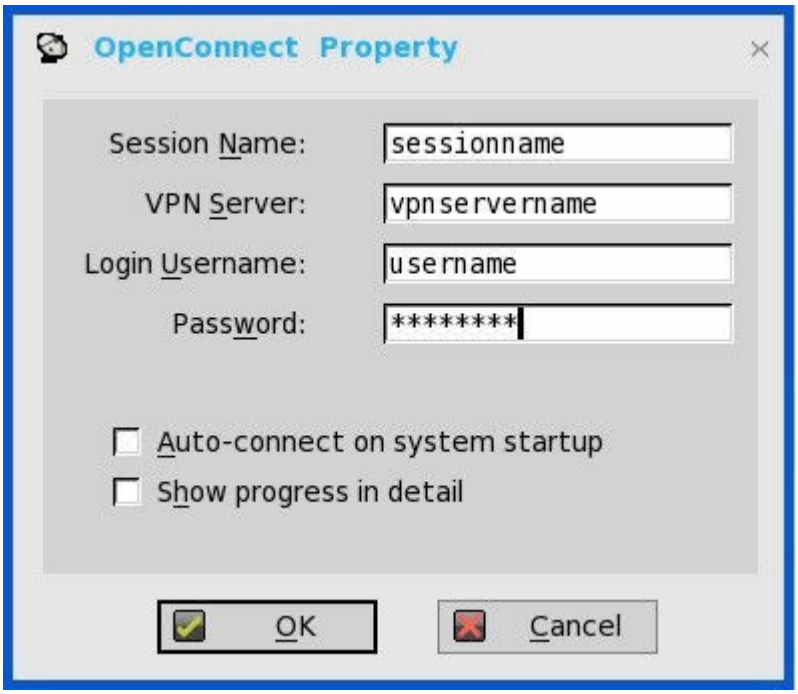


Figure 46. OpenConnect property

3 Click **Connect** to connect to the VPN Manager.

4 Click **Edit** to edit the to the VPN Manager connections.

5 Click **Delete** to delete the VPN Manager.

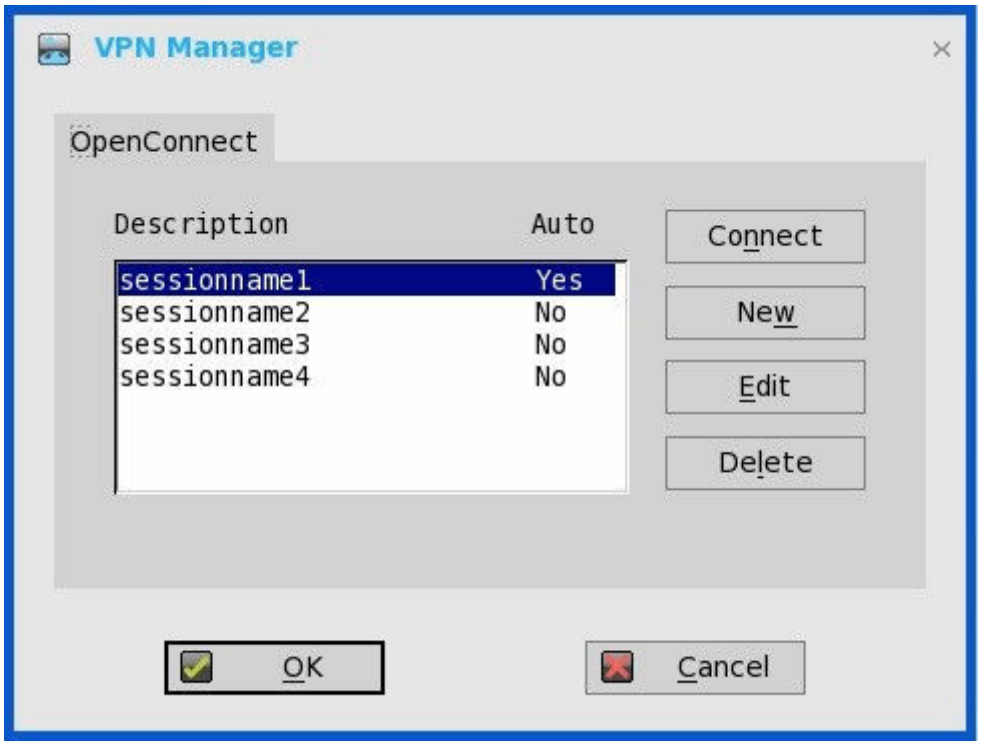


Figure 47. Delete VPN manager

6

Configuring the connection broker

In a Virtual Desktop Infrastructure (VDI) environment, a connection broker is a software entity that allows you to connect to an available desktop. The connection broker facilitates the VDI environment to securely and efficiently manage the centrally hosted desktop environments.

NOTE:

- Linux hosted desktop in the Citrix brokers is supported.
- Windows 10 desktop in multiple brokers is supported.
  - Windows 10 desktop is supported in the Citrix brokers.
- ICA multicast feature is not supported from ThinOS Lite 2.4. However, the URL redirection works.

Configuring Citrix

Citrix offers a complete virtualization solution, where all applications and resources are deployed on a centralized server, and published to remote devices. The Citrix Receiver client software installed on the thin client allows you to interact with the application GUI, while all of the application processes are performed on the server.

This section provides information about how to configure a Citrix broker connection on your ThinOS Lite device, and other Citrix features that you can configure on ThinOS Lite.

Configuring the Citrix broker setup

To configure the broker setup, do the following:

1 From the floating bar menu, click the **System Setup** , and then click **Remote Connections**.
The **Remote Connections** dialog box is displayed.

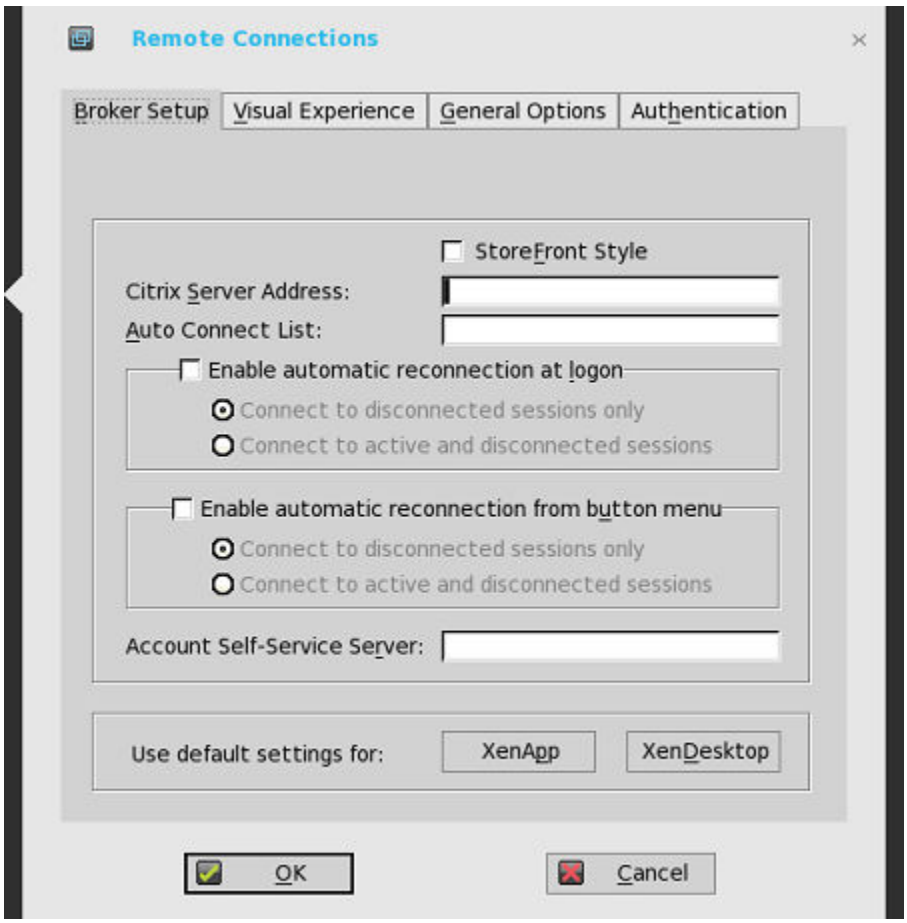


Figure 48. Broker setup

2 Select the **StoreFront Style** check box to enable the StoreFront style.

3 **Broker Server**— Enter the IP address / Hostname / FQDN of the broker server.

4 Select the **Enable automatic reconnection at logon** check box to enable automatic re-connection at logon.

> **NOTE: If you enable the automatic re-connection, you are able to select from the re-connection options. Click either of the options where you can connect to disconnected sessions only or both active and disconnected sessions.**

5 Select the **Enable automatic reconnection from the button menu** check box to enable automatic reconnection from the button menu. You can select any of the following options:

- Connect to disconnected sessions only.
- Connect to active and disconnected sessions.

6 **Account Self-Service Server**— Enter the IP address of the Account Self-service Server.

7 **XenApp** — Use this option if you want to set default settings to XenApp.

8 **XenDesktop**— Use this option if you want to set default settings as XenDesktop.

9 Click **OK** to save the settings.

Citrix HDX RealTime Multimedia Engine—RTME

RTME 1.8 was a new feature introduced in ThinOS Lite 2.2. This is the Citrix HDX RealTime Optimization Pack 1.8 for Lync. In ThinOS Lite 2.3 release, the **Citrix HDX RealTime Optimization Pack 2.0 (RTME 2.0)** is supported. Citrix RTME 2.0 is introduced to support Microsoft Skype for Business 2015 client/UI (only), in addition to RTME 1.8 supporting the Microsoft Lync 2010/2013 clients. From ThinOS Lite 2.4 release, RTME version is updated to a newer version 2.2– Citrix HDX RealTime Optimization Pack 2.2 for Microsoft Skype for Business

2016. This section provides information about supported platforms for RTME, installation of RTME package, Citrix remote Server/Desktop host preparation, configuration on ThinOS Lite, and RTME status check and troubleshooting.

- Installing the RTME package on ThinOS Lite.
- Setting up the RTME connector.
- Verifying the RTME 1.8 status.
- Verifying the RTME 2.2 status.

Introduction

The Citrix HDX RealTime Optimization pack offers high-definition audio and video calls on Lync. In every ThinOS Lite release, the RTME version may be updated to newer version and the latest RTME version coexists with RTME 1.8 version in the corresponding release packages. ThinOS Lite v2.6 supports RTME/RTOP version 2.5. However, you can still use RTME 2.2 package.

For more information about the Citrix RTME 1.8 feature, see the HDX RealTime Optimization Pack article at docs.citrix.com.

For more information about Citrix RTME 2.x feature, go to docs.citrix.com.

Supported Environments

- Citrix environment: XenDesktop and XenApp 5.6/6.5/7.x
- Desktop with RTME connector 1.8 (Lync server and client version 2010 and 2013; Skype for Business client in Lync 2013 GUI is supported).
- Desktop with RTME connector 2.2 (Skype for Business 2015 and 2016 is supported).
- Supported networks: LAN, WAN (VPN), wireless and so on.
- Supports calls between RTME clients or between RTME and standard Lync clients.
- Supports Microsoft Office 365 or Skype for Business Online. For more information, go to docs.citrix.com.

Installing the RTME package on ThinOS Lite

You are required to install the RTME.i386 package for the RTME 1.8 and 2.2 feature to work on ThinOS Lite.

To install the RTME.i386 package:

1 Upload the **RTME.i386.pkg** to directory **\wnos\pkg**.

> **NOTE: For RTME package version, see the latest *Dell Wyse ThinOS Lite Release Notes* available at www.dell.com/support.**

2 You must ensure that the INI `autoload` is not set to value 0.

3 Restart the thin client and wait till the auto-installation of packages is complete.
The installed RTME package is displayed in the **Packages** window in **System Tools**.

Setting up the RealTime Multimedia Engine connector

This section describes how to install and use Lync on a Citrix desktop.

1 Install Citrix HDX RealTime Connector version 1.8 or 2.2 on Citrix desktop VDA/Server. .

NOTE:

- HDX RealTime Multimedia Engine is the package installed on ThinOS Lite ; it is HDX RealTime Connector for Lync that needs to be installed or upgraded on the remote server and VDA.
- The upgrade option from 1.7 to 1.8 is discussed at docs.citrix.com/en-us/hdx-optimization/1-8/upgrade-1-7-to-1-8.html.
- The Firewall configuration is required on remote server and VDA. For more information, refer to docs.citrix.com/en-us/hdx-optimization/1-8/hdx-realtime-optimization-pack-configure-firewall.html.
- To know about the technical overview of RTME 2.2, go to docs.citrix.com/en-us/hdx-optimization/2-2/hdx-realtime-optimization-pack-about.html.

IMPORTANT: The RTME 1.8 feature on ThinOS Lite supports only HDX RealTime Connector 1.8 due to Citrix limitation.

2 Update the ThinOS Lite firmware to 2.4, and install the **RTME.i386.pkg** on the ThinOS Lite client. For information about installing the RTME package, see Installing the RTME Package on ThinOS Lite.

IMPORTANT: Since ThinOS Lite 2.3 RTME, 1.8 and 2.0 co-exist in the release package, supporting both versions of RTME connectors. In every ThinOS Lite release, RTME version may be updated to newer version and the latest RTME version co-exists with RTME 1.8 version in the corresponding release packages.

3 (This step is for RTME 1.8 only) Configure the Domain Name Server (DNS) settings on ThinOS Lite for Lync Server.

NOTE: You must ensure that the thin client does not have USB redirection for video/audio devices in order to have RTME working correctly.

4 Log in to your Citrix Desktop, and sign in to Lync client.

- For 1.8, the RTME icon is displayed in the lower-left corner of the Lync client window.
- For 2.2, the RTME icon is displayed on taskbar

Use the Lync Application or Skype for Business application to perform the following tasks:

- Start an audio or video call
  - Select user to call
  - Call from the IM window
  - Type a name or number to call
- Answer the call
  - Audio call
  - Video call
  - Headset button to answer the call
- Transfer call/ mute/ hold call
- Control the video: Pause/ End/ Picture in Picture (PiP)
- Set the volume levels
- Use Dial Pad
- Make a conference call
- Help and Hang up
- Minimize/maximize or close the call video window
- Perform Network Health check — For 1.8, press Ctrl+N to open the **Network Health** window. For 2.2, right click **RTME** icon on taskbar select **Call Statistics**.

  The attributes, such as received packets, sent packets, video frame rate, video resolution, audio codec, and video codec are displayed in the above described window.

  In RTME 2.2 version, USB Video Class (UVC) 1.1 and 1.5 Camera hardware encoding / H.264 (CAM) are supported. This is applicable for qualified cameras only, for example Logitech C930e.

In the **Call Statistics** window, **Video Codec = H.264 (CAM)** is displayed for P2P RTME video call in the **Sent** column. For group calls with standard SFB, the call statistics displays **Video Codec = H.264-UC (CAM)** in the **Sent** column. This improves video call quality/ resolution compared to Video Codec H.264 (SW); for example: P2P video call resolution upgrade from 480 x 270 to 640 x 360.

Verifying the RTME 1.8 status

The **Citrix HDX RealTime Connector for Microsoft Lync 2013** dialog box enables you to verify the RTME 1.8 status.
To view the **Citrix HDX RealTime Connector for Microsoft Lync 2013** dialog box:

1 Do any of the following to view the **Citrix HDX RealTime Connector for Microsoft Lync 2013** dialog box:
- Click the **RTME** icon in the lower-left corner of the Lync application window, and click **Audio Video Settings**.
- Click the **Lync menu** icon in the upper-right corner of the Lync application window, and click **Tools** > **Audio Video Settings**.

The **Citrix HDX RealTime Connector for Microsoft Lync 2013** dialog box is displayed.

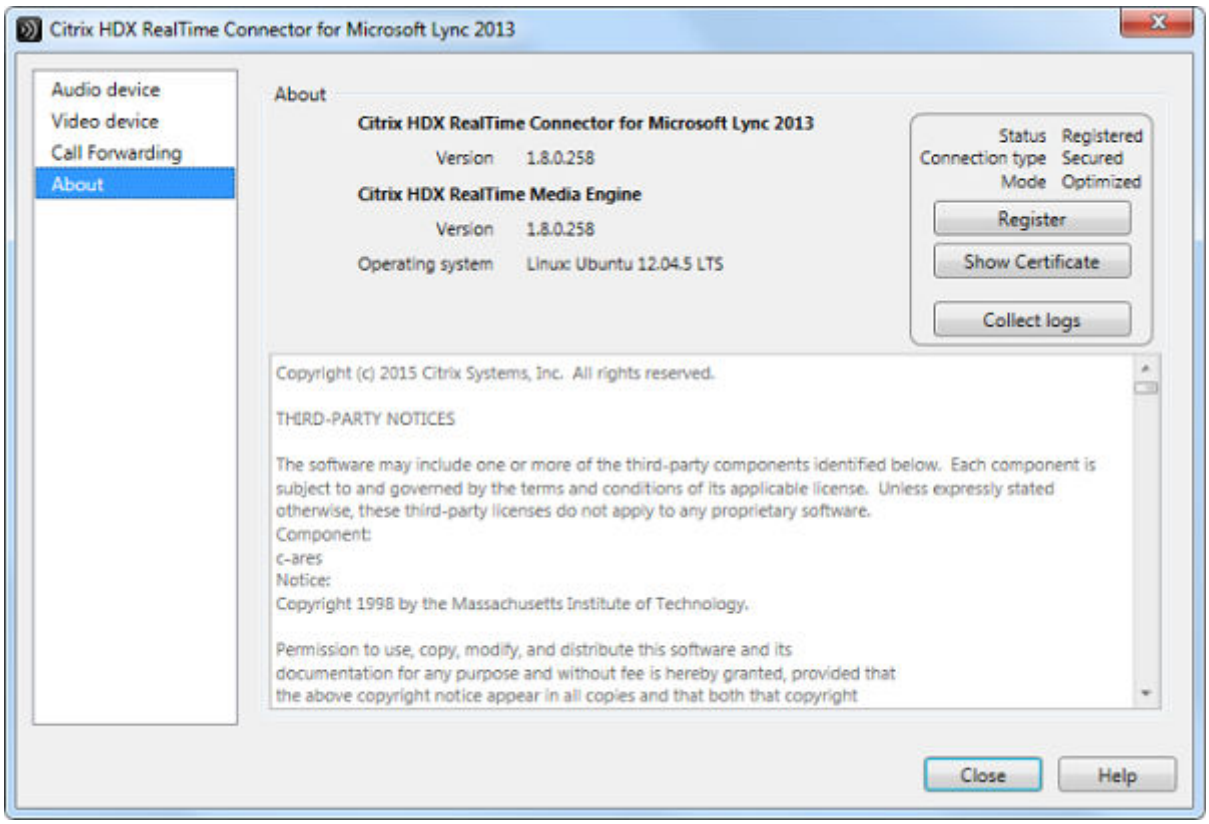


Figure 49. Citrix HDX RealTime Connector for Microsoft Lync 2013

2 Click the **About** tab in the **Citrix HDX RealTime Connector for Microsoft Lync 2013** dialog box.
The RTMS status is displayed in the upper-right pane of the dialog box. If the RealTime Multimedia Engine is successfully initiated between the ThinOS Lite client and Citrix Desktop, the RTME status is displayed as follows:

Table 8. RTME status

Status	Registered
Connection Type	Secured
Mode	Optimized

You can also view the **Citrix HDX RealTime Connector for Microsoft Lync 2013** version and **Citrix HDX RealTime Media Engine** version in the dialog box.

3 Click the **Audio Device** tab to configure the RTME audio settings, such as speakers, microphone, and ringer settings.

NOTE: The RTME audio device on ThinOS Lite shows only one device from ThinOS Lite local playback device. It can actually work the way they are configured at ThinOS Lite local playback device and record device. The RTME audio device for ringtone is limited to use ThinOS Lite local playback device. This is a known Issue.

4 Click the **Video Device** tab to configure the RTME video settings. From the drop-down list, select the webcam that you want to use for video calls.

5 Click the **Call Forwarding** tab to configure the call forwarding settings.

You can configure the following options:

- Turn off call forwarding
- Forward any call to a specific number
- Simultaneously ring

NOTE: The latest call forwarding settings configured by you are displayed in the lower pane of the dialog box.

Known Issues with RTME 1.8 feature

- RTME operation system on ThinOS Lite is displayed as Linux.
- The RTME 1.8 feature on ThinOS Lite does not work with other versions of HDX RealTime connector due to known Citrix limitation.
- If you change the audio device during an RTME call, the audio input or output might stop responding.
- Using similar hardwares, such as Dx0D, ThinOS Lite, Linux, and Windows (D90D7) produce similar video frame rate (20-30) and video resolution (320-400). It produces better video quality using laptop or PC because of better CPU capability.
- In a video conference call, when different user is speaking, the on-screen video switches to the active user, but takes a few seconds to switch over.

Tested devices—For information about the tested devices for RTME, see the latest Dell Wyse ThinOS Lite release Notes.

Verifying the RTME 2.x status

This section describes the working of RTME 2.x and how to verify the RTME status.

Salient Features

- Native SFB client menus and operations are available.
- Better initialization eliminates DNS confusions.
- Supports more call features, such as call delegation, and response group.
- Supports video codec H.264-UC, and audio codec SILK introduced by RTME 2.1.
- Call Admission Control support
- Bandwidth Policy Control
- DSCP/ QoS Configuration
- Ability to turn off version mismatch warnings for acceptable combinations of RealTime Connector and RealTime Media Engine.

To verify the RTME status, do the following:

1 Install the correct connector on the remote desktop.
2 Install the correct package on the ThinOS Lite device.
3 Plug-in the audio/video devices.

NOTE: USB redirection must be disabled for audio or video devices.

4 Connect to the remote desktop using SFB client 2015.
5 Verify the RTME connector 2.2 icon on taskbar. The status is displayed as **Connected**.
6 Verify the About, and Settings options from the RTME connector 2.2 menu.

7 Verify the audio/video devices from SFB client menus.

8 Establish the video/audio calls.

9 Pick up the calls by either clicking the mouse or using the headset button.

10 Verify the Call Statistics from the RTME connector 2.2 menu.

NOTE: RTME 2.2 supports various call scenarios. For more information, refer to *Citrix technical overview*.

In RTME 2.2 version, USB Video Class (UVC) 1.1 and 1.5 Camera hardware encoding / H.264 (CAM) are supported. This is applicable for qualified cameras only, for example Logitech C930e.

In RTME 2.3 version, the video performance of applications is designed for a lower CPU consumption. Therefore, the video resolution may be downgraded compared to v2.2.

In the **Call Statistics** window, **Video Codec = H.264-UC (CAM))** is displayed for P2P RTME video call in the **Sent** column. For group calls with standard SFB, the call statistics displays **Video Codec = H.264-UC (CAM)** in the **Sent** column. This improves video call quality/resolution compared to Video Codec H.264 (SW); for example: P2P video call resolution upgrade from 480 x 270 to 640 x 360.

Known Issues with RTME 2.2 feature

- RTME status dialog displays operation system as Linux.
- Only single device is supported in ThinOS Lite.
- Changing the video/audio device during RTME call results in issue with audio input or output.
- Volume: Dell recommends you to adjust the speaker volume in SFB 2015 call window to high, and the system local playback/record audio volume for better voice input/output. The default volume is a bit low.
- Camera/Video: The local camera setting does not affect/impact the RTME video output because of the RTME design.

Citrix Icon refresh

Citrix applications can be refreshed by clicking **Refresh** from the PNMenu.

There are two methods to refresh the Citrix applications:

- Manual refresh
- Auto refresh using the INI parameter

Refreshing Citrix applications manually

To refresh the Citrix application manually, do the following:

1 For single StoreFront or PNAgent server, change the application in broker, and then click **Refresh** from PNMenu.

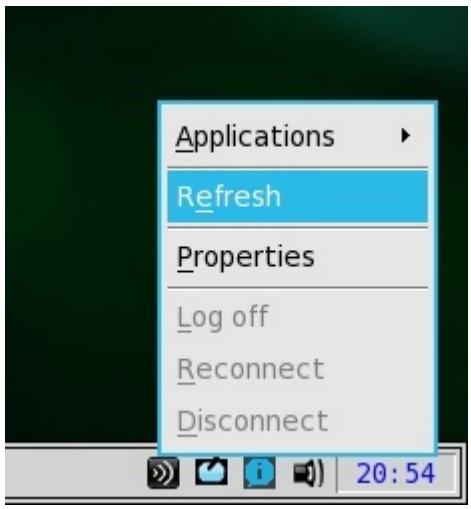


Figure 50. PNMenu

The following message is displayed in the lower right pane during application refresh.

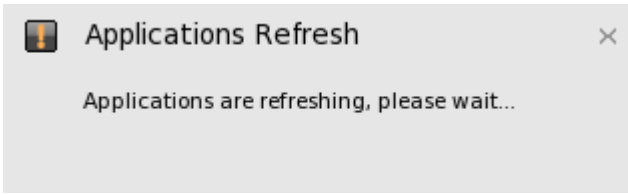


Figure 51. Applications refresh

2 Applications are refreshed in Session bar list, Connect Manager list and App menu list.

The following log is displayed in the Event Log window:

```
ICA: refresh store "xxx"…" or "ICA: refresh PNAgent"xxx"…
```

3 For MultiFarm (StoreFront or PNAgent servers) or Multilogon (StoreFront or PNAgent servers), select a single server to refresh or click **Refresh All** to refresh all servers.

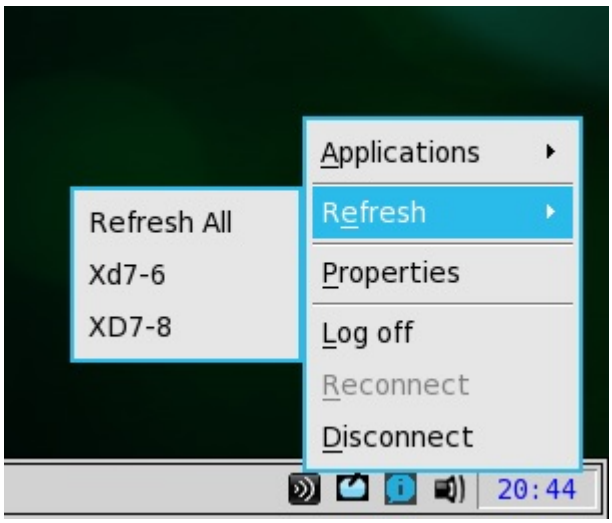


Figure 52. Refresh all

NOTE:
Warning message is displayed when you open or edit or remove applications when you refresh the applications.

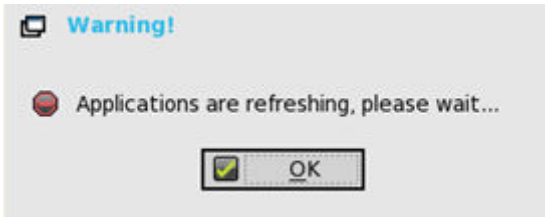


Figure 53. Warning

4 Refresh scope covers the aspects such as, application removed, added, duplicated, disabled, enabled, icon/title change, and on/off desktop.

Active sessions that are started are not affected by application refresh.

5 The disconnect session can be reconnected after application refresh, if **automatic reconnection at logon** is enabled in remote connection.

Refreshing the Citrix applications automatically using INI parameter

To automatically refresh the Citrix application, set the following INI parameter:

```
SessionConfig=ICA RefreshTimeOut=dd:hh:mm
```

For example, 01:01:22, means the application will start refresh automatically, every 1 day: 1 hour: 22 minutes.

Limitations of Citrix icon refresh

Following are the limitations of Citrix icon refresh:

- Citrix icon refresh is supported in classic mode and storefront mode only.
- Virtual Desktop Infrastructure (VDI) mode is not supported.

Using multiple audio in Citrix session

ThinOS Lite supports multiple audio device utilizations in the Citrix Virtual Apps and Desktops version 7.6 and later. You can connect or disconnect the audio devices anytime during the session, but the behavior is similar to a local desktop. With multiple device support, you can connect multiple audio devices and select a specific device for a specific application.

As a prerequisite, the **Audio Plug N Play** policy must be enabled on the Citrix Remote Desktop Session (RDS) desktop. The **Audio Plug N Play** policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is enabled by default.

NOTE: On the Citrix Virtual Desktop Infrastructure (VDI) desktop, preconfiguration is not required.

Supported devices—USB headset, webcam (without USB redirection), and analog headset devices are supported.

The following are valid working conditions for multiple audio:

- Using Citrix HDX generic audio:
  a Select the audio device as **PC Mic and Speaker**.
  b Configure the speaker or microphone.
  c For secondary ringer, select the audio devices excluding the HDX devices.
- Using Citrix RealTime Multimedia Engine (RTME):
  a Select the audio device as **HID headset with PC Mic and Speaker**.
  b Set **PC Mic and Speaker** to configure the speaker or microphone.
  c For secondary ringer, select the audio devices excluding the RTME devices.

The following scenarios must be considered during multiple audio settings:

- ThinOS Lite default audio must be set to latest plug-in audio device.
- Session default audio must be set to the ThinOS Lite default audio. However, this option can be changed.
- Restart Skype for Business/Lync client after you plug and remove the device connection.
- ICA RTP audio is supported with multiple audio connections.
- During a call, the audio device settings can be switched without connecting the device.
- Multiple audio can be shared across sessions.

Limitations

- Wyse 3010 zero client with Citrix and Wyse 3020 zero client with Citrix are not supported.
- Citrix multiple audio feature does not work with HDX generic audio. The resolution for the issue will be delivered in the next ThinOS release.

Using Citrix NetScaler with CensorNet MFA authentication

SMS PASSCODE is re-branded as CensorNet MFA. You can configure NetScaler Gateway to use a One Time Passcode/Password (OTP) in the form of a personal identification number (PIN) or passcode. To obtain this one-time password, you must install CensorNet app on your mobile. After you enter the passcode or PIN, the authentication server invalidates the one-time password. You cannot enter the same PIN or password again. For more information about configuring one-time passcode, see the Citrix documentation.

Prerequisites

- NetScaler v12.0 and later is installed on your client.
- SMS PASSCODE v9.0 SP1 is installed and configured in your network. You can download the SMS PASSCODE v9.0 file from download.smspasscode.com/public/6260/SmsPasscode-900sp1.
- Remote Authentication Dial-In User Service (RADIUS) authentication policy is configured and bind to the NetScaler gateway server.
- CensorNet app is installed and configured on your mobile device.

To use the one-time passcode on ThinOS Lite, do the following:

1 Log in to ThinOS Lite, and connect to the NetScalar Gateway URL.

2 Enter your credentials (user ID and password) and press Enter.

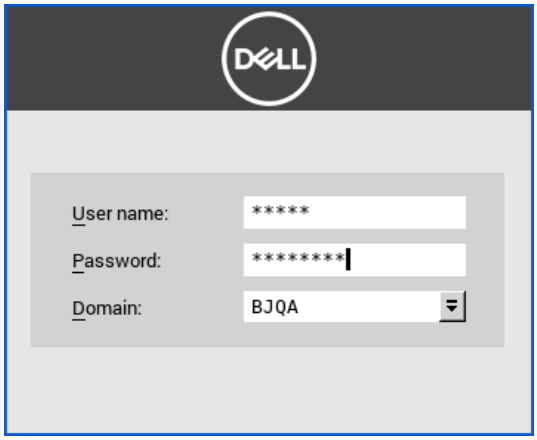


Figure 54. Credentials

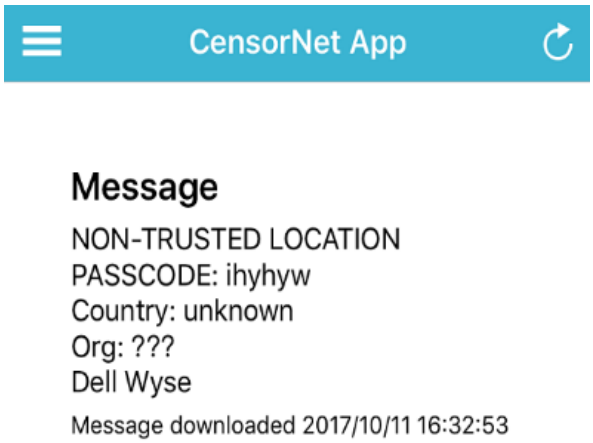


Figure 55. CensorNet App

The PASSCODE dialog box is displayed. You will receive a push notification from the CensorNet App on your phone with the code.

3 Click **OK**.

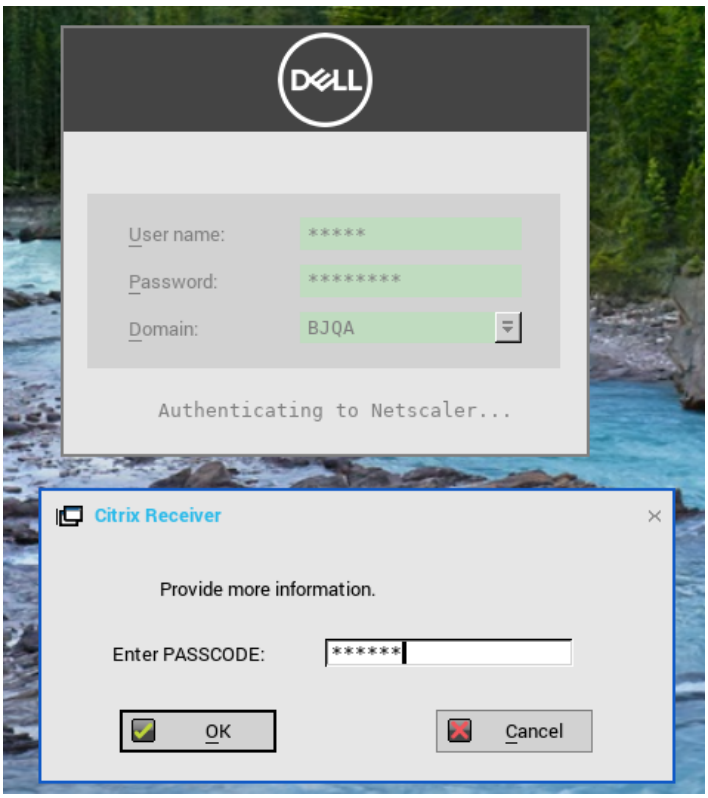


Figure 56. PASSCODE

If the authentication is successful, then you are logged into the Citrix session.

Okta Integration through Citrix NetScaler

Okta provides Single Sign-On (SSO) capability using Remote Authentication Dial-In User Service (RADIUS) for Citrix Virtual Apps and Desktops. ThinOS Lite supports Okta through the Citrix NetScaler Gateway 11.0 or later. The Okta RADIUS Agent is used for user authentication. The Okta RADIUS server agent assigns the user authentication to Okta using single-factor authentication (SFA) or multifactor authentication (MFA).

For more information about configuring Citrix NetScaler Gateway to use the Okta RADIUS Agent, see the *Citrix NetScaler Gateway Radius Configuration Guide* at help.okta.com.

NOTE:

- On the ThinOS Lite-based client, if you do not use `username@fqdn`, you must set the following INI parameter:

  ```
  pnliteserver=https://<fqdn of NS Server>
  CAGUserAsUPN=yes
  ```

  After you enable this INI parameter, the domain must use the **domain.com** format in the login window.
- Phone authentication by using Okta is supported only in US and Canada.

Configuring ICA connections

To configure the ICA connections, use the following guidelines:

NOTE: Set the INI `EnableLocal=yes` to show the Default ICA icon in connect manager.

1 Go to **Home icon** > **Connect Manager** > **Default ICA** > **Edit**.

2 Click the **Connection** tab, and use the following guidelines:

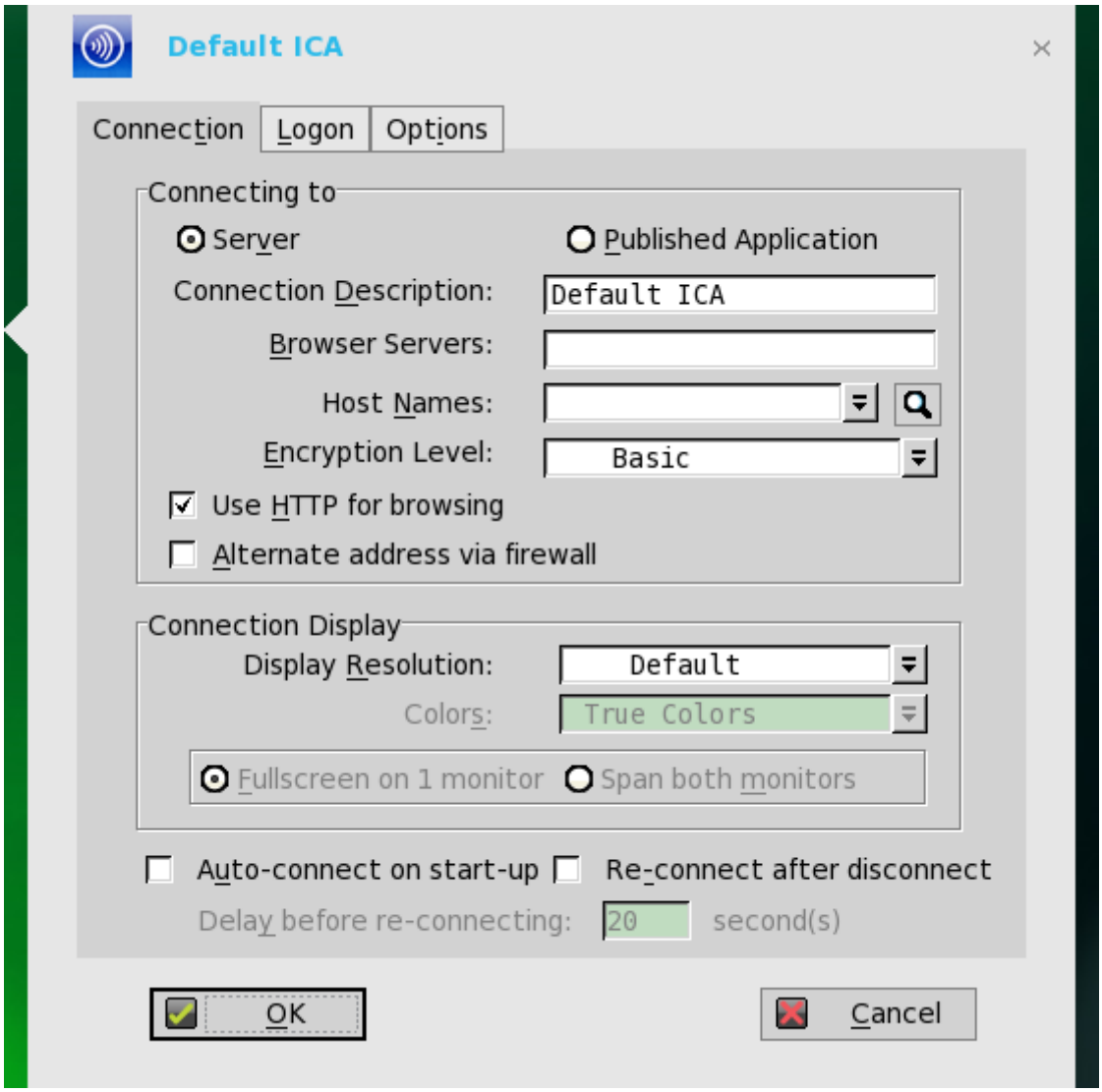


Figure 57. Default ICA

a **Server** or **Published Application**—Select the type of connection to which the settings apply.

b **Connection Description**—Enter the descriptive name that is to be displayed in the connection list (38 characters maximum).

c **Browser Servers**—Enter a delimited (comma or semicolon) list of IP addresses or DNS-registered names of ICA servers that contain the master browsers list, or that can direct to another server that contains the list.

The master browsers list is generated automatically by a browsing program on one of the ICA servers that are selected by negotiation between servers. It is used to provide the information that is displayed in the Server Name or IP box. No entry is needed if the list is on an ICA server in the same network segment as the zero client. No entry is necessary if the connection is to a server, or if the server name or IP contains the IP address of the server.

d **Host Name or Application Name** (title depends on the Server or Published Application option that is selected)—You can enter a delimited semicolon or comma-separated list of server host names or IP addresses, or you can select from the list of ICA servers or published applications that are obtained from the ICA master browser. You can also use **Browse** next to the box to make the selection you want.

If you enter a delimited list of servers, the zero client will attempt to connect to the next server on the list, if the previous server attempt fails. If you use the list and the selected connection fails, the zero client will attempt to connect to the next one on the list.

> **NOTE: The hostname may be resolved using one of three mechanisms: ICA master browser, DNS, or WINS. Master browser is the only mechanism that can resolve a published application unless manual entry is made in DNS for the application. DNS uses the default domain name in the network control panel to attempt to construct an FQDN but also tries to resolve the name without using the default.**

e **Encryption Level**—Allows you to select the security level of communications between the zero client and the ICA server.

Basic (the default option) is the lowest level of security. Basic allows faster communication between the device and the ICA server, because it requires less processing than the higher levels of encryption.

> **NOTE: The encryption selection applies to the security of communications between the zero client and the ICA server only. It is independent of the security settings of individual applications on the ICA server. For example, most web financial transactions require the zero client to use 128-bit encryption. However, transaction information could be exposed to a lower level of security if the zero client encryption is not also set to 128-bits.**

f **Use HTTP for browsing**—When this option is selected, by default the zero client uses HTTP when browsing.

g **Alternate address via firewall**—When selected, the zero client uses an alternate IP address that is returned from the ICA master browser to get through firewalls. This is used for the Windows login when the connection is activated.

h **Display Resolution**—Select the display resolution for this connection. Only Default option is available.

i **Colors**—Only **True Colors** option is available for Wyse 5010 zero client for Citrix (D00DX).

j **Autoconnect on start-up**—When selected, automatically connects the session on start-up.

k **Reconnect after disconnect**—When this option is selected, the zero client automatically reconnects to a session after a non operator-initiated disconnect. If selected, the wait interval is the time you set in the **Delay before reconnecting** box (enter the number of seconds 1–3600). If there is no INI file configured for this connection, or if you are a stand-alone user, the default value is set to 20 seconds.

3 Click the **logon** tab, and use the following guidelines:

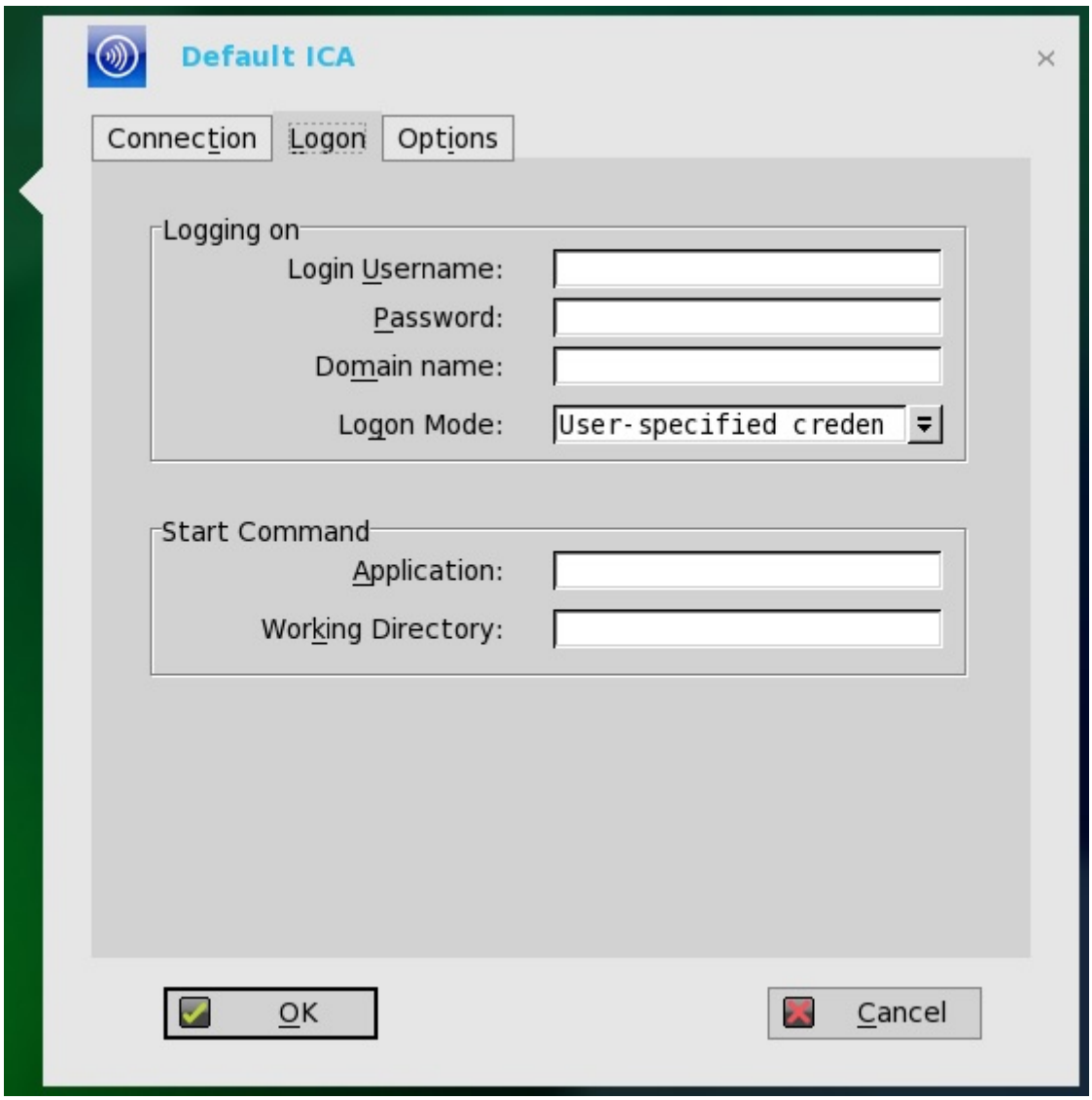


Figure 58. ICA Logon

a **Logging on area**—Enter the username, password, domain name, and logon mode.

If the Login username, password, and domain name boxes are not enabled, you can enter the information manually in the ICA server login screen.

- **Login Username**—Maximum limit is 31 characters.
- **Password**—Maximum limit is 19 characters.
- **Domain Name**—Maximum limit is 31 characters.
- **Logon Mode**—Select **User-specified credentials**, **Smart Card**, or **Local User**.

b **Start Command area**—Server Connection Option Only—This area is disabled for a Published Application option.

Application (127 characters maximum) and **Working Directory** (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

4 Click the **Options** tab, and use the following guidelines:

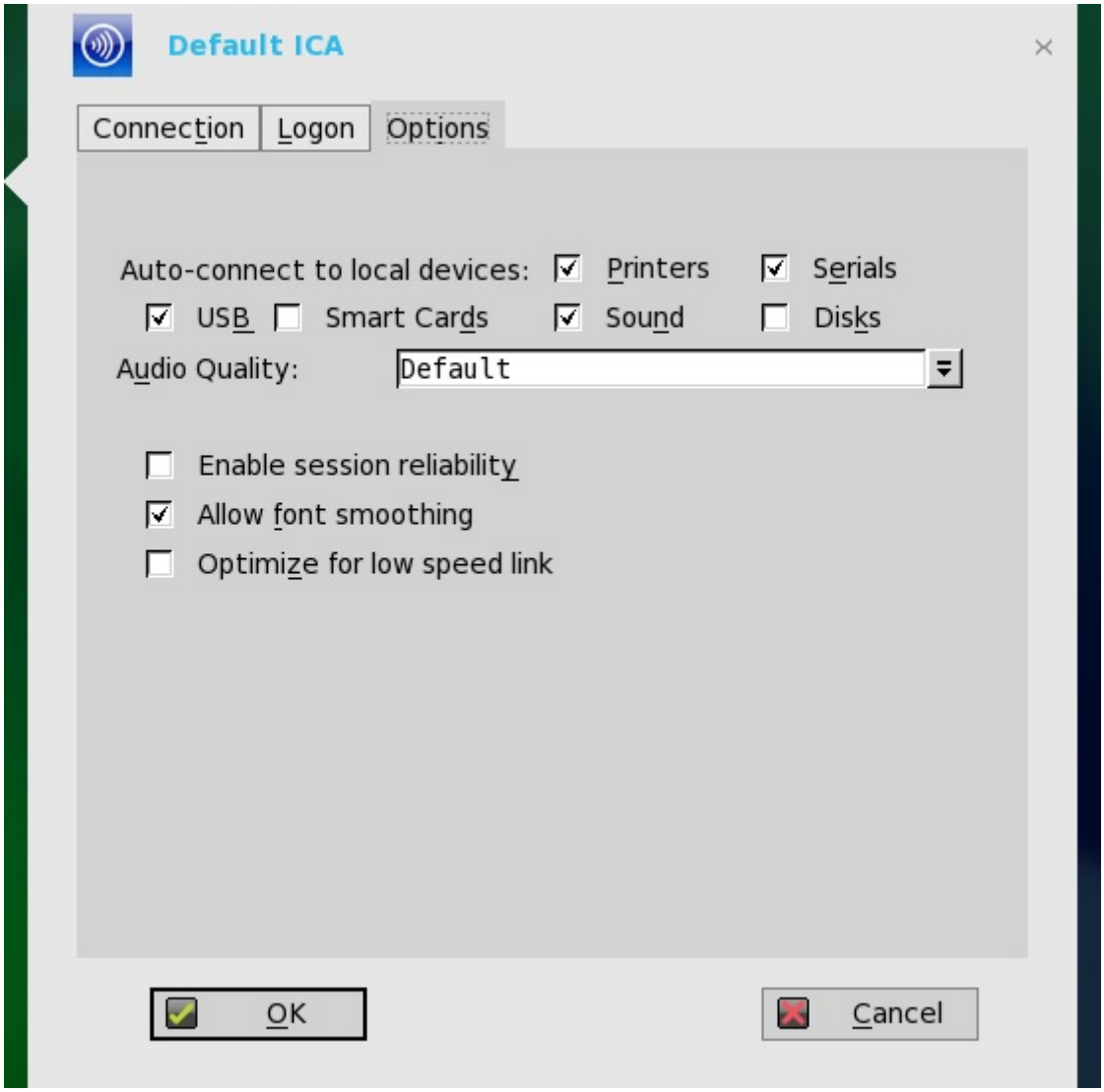


Figure 59. ICA options

a **Autoconnect to local devices**—Select any options (Printers, Serials, USB, Smart Cards, and Disks) to have the thin client automatically connect to the devices. An ICA session does not automatically connect to a device through a serial port.

b **Allow font smoothing**—When selected, enables font smoothing (smooth type).

c **Optimize for low speed link**—When selected, allows optimization for low-speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dial-up.

d **Enable session reliability**—When enabled, session reliability allows a user to momentarily lose connection to the server without having to reauthenticate upon regaining a connection. Instead of a connection time out, the session is kept active on the server and is made available to the client upon regaining connectivity. Session reliability is most relevant for wireless devices.

5 Click **OK** to save the settings.

If the session reliability is enabled in an active session, and your network connection is not configured properly, a warning message is displayed with time elapsed after warning issuance.

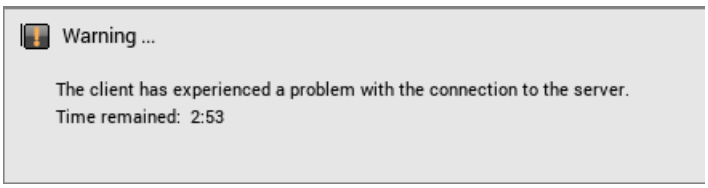


Figure 60. Warning

Advanced details on configuring ICA connections

Use the following information when configuring ICA connections. In this information assumes that the zero client does not have a locked down privilege level:

- **High-privileged user** — The additional functionality provided by the **Connection Settings** dialog box allows testing of connection definitions before they are entered by a network administrator into the user profile files.
- **Low-privileged user** — The settings for the selected connection can be viewed but cannot be edited, and new connections cannot be defined. Connection definitions are controlled by a network administrator and are accessed by the zero client from the user profiles on a remote server.
- **Stand-alone user** — The Connect Manager is available to Stand alone users because connection definitions cannot be accessed from remote user profiles. If user profiles are available on an FTP server but are not accessed because DHCP is not available or is not configured to provide the file server IP address, the file server IP location can be entered manually using the **Network Setup** dialog box.

ICA Self Service Password Reset—SSPR

You can reset the password or unlock the account after you complete the security questions enrollment.

Supported Environment

- Citrix Virtual Apps and Desktops 7.11 and later versions
- Support Storefront server 3.7 and later versions
- Self-Service Password Reset Server 1.0 and later versions

Supported Platforms

- All platforms are supported

Limitations

- Supports only storefront server
- The Legacy Account Self-Service (which needs Account Self-Service Server configured in ThinOS Lite Remote Connections) is independent with this storefront version. Storefront version will cover Legacy Account Self-Service.
- The security question enrollment is not supported in Virtual Desktop Infrastructure (VDI) mode.

Before resetting password or unlocking account

Before resetting your password or unlocking your account, you must register for the security questions enrollment. To register your answers for the security questions, do the following:

1 From the PNMenu, click the **Manage Security Questions** option (Classic and StoreFront only).

The **Security Questions Enrollment** window is displayed.

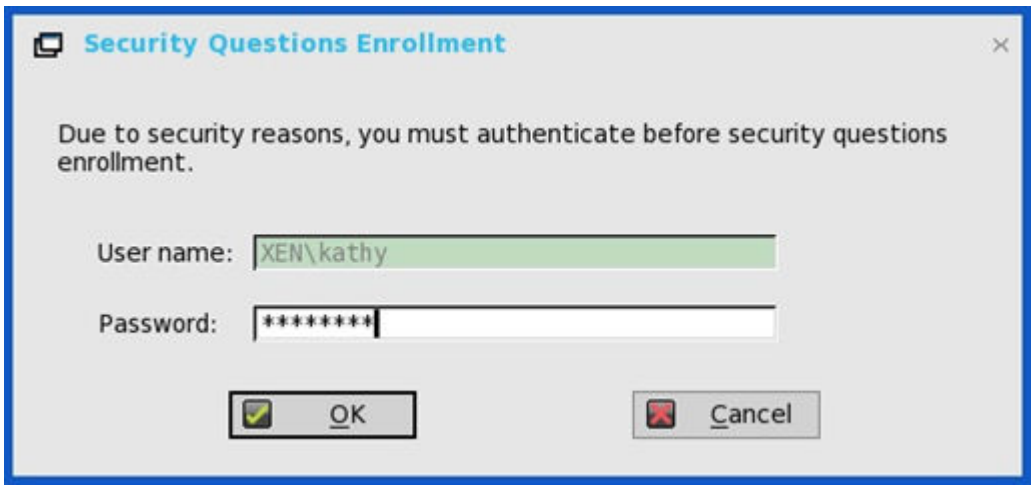


Figure 61. Security questions enrollment

2 Enter the appropriate answers to the question set.

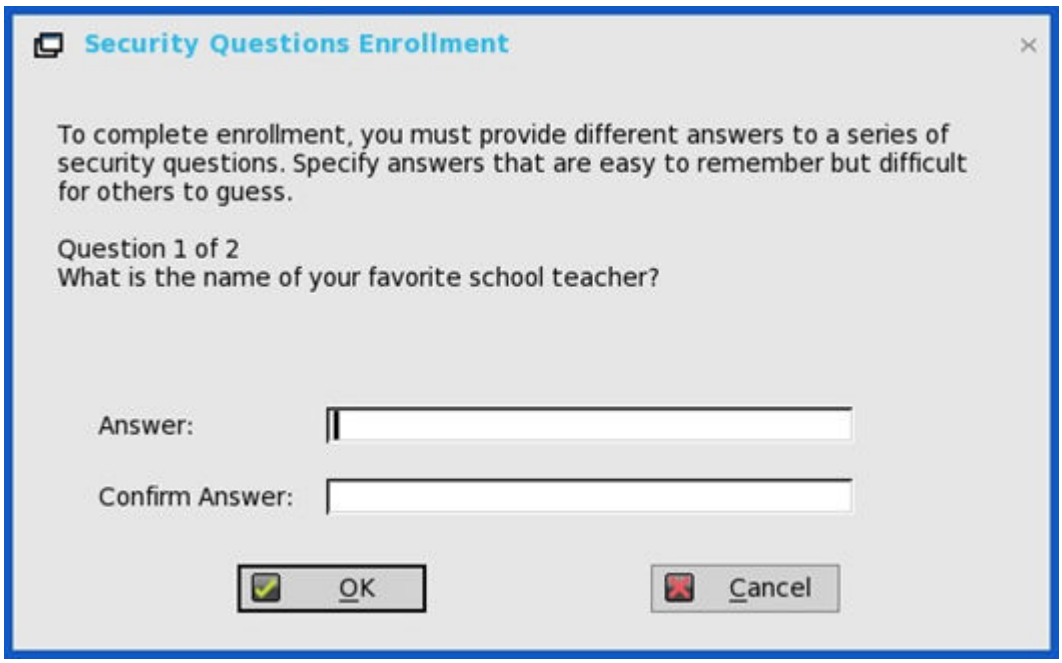


Figure 62. Security questions

Figure 63. Security questions

3 Click **OK** to register the security questions.

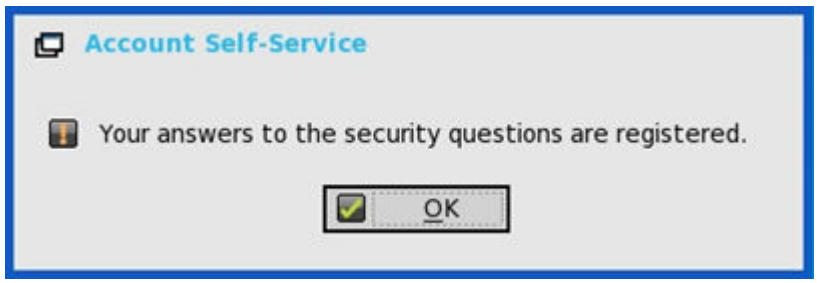


Figure 64. Account self-service

Using Account Self-Service

After the security questions enrollment is complete, when ThinOS Lite is connected to a StoreFront server with Self-Service Password Reset enabled, the **Account Self-Service** icon is displayed in the sign-on window.

NOTE: If you enter wrong password more than four times in the Sign-on window, the client automatically enters the unlock account process.

1 Click the **Account Self-Service** icon to unlock your account or reset your password.

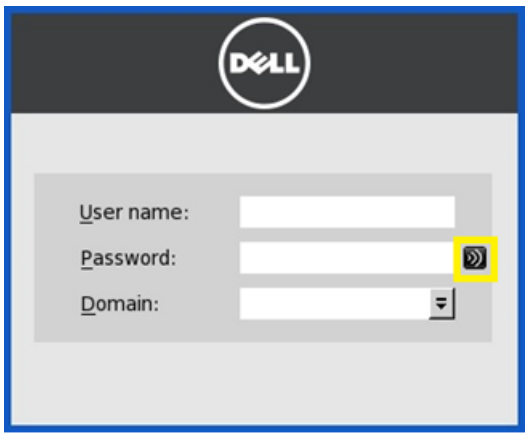


Figure 65. Account self-service icon

NOTE: **You need to register the security questions for the users before using unlock account or reset password.**

2 Click **Unlock account** or **Reset password** based on your choice, and then click **OK**.

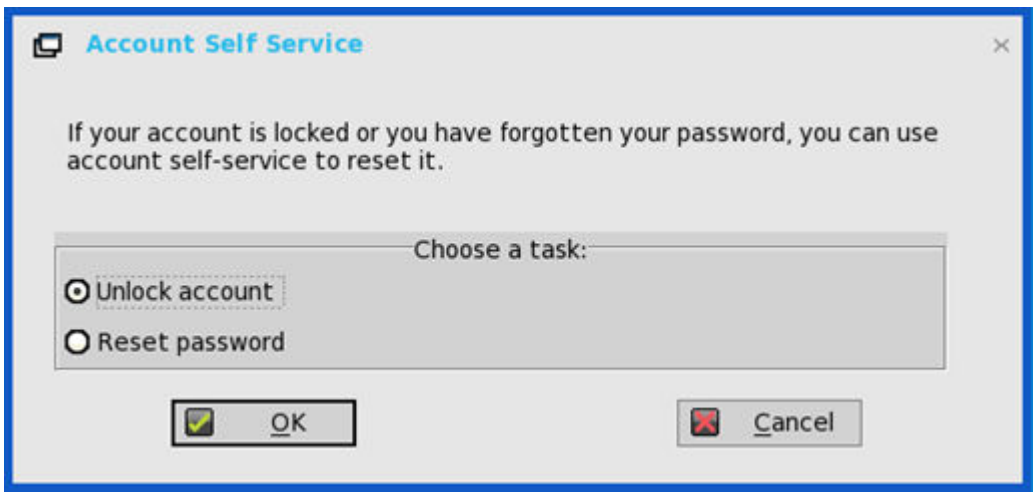


Figure 66. Account self-service icon

Unlocking account

After you register the security questions, do the following to unlock the account:

1 Choose a task (Unlock account) in **Account Self-Service** window.

2 Enter the user name.

The **Unlock Account** dialog box is displayed.

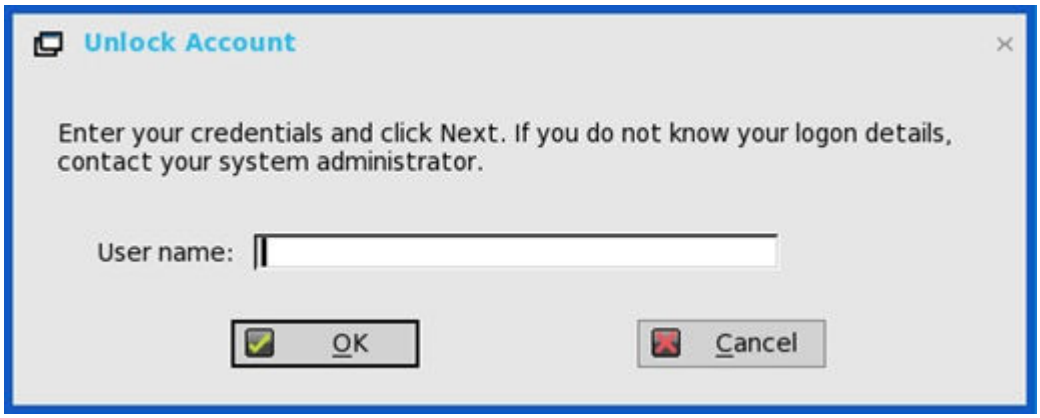


Figure 67. Unlock account

3 Enter the registered answers to the security questions.

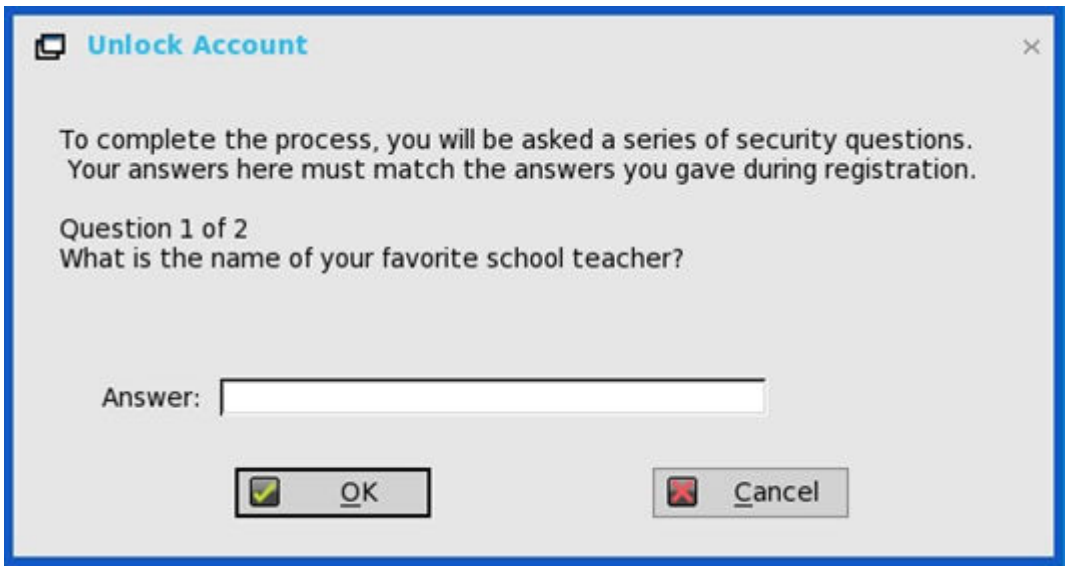


Figure 68. Unlock account

Figure 69. Unlock account

If the provided answers match the registered answers, then the **Unlock Account** dialog box is displayed.

4 Click **OK** to successfully unlock your account.

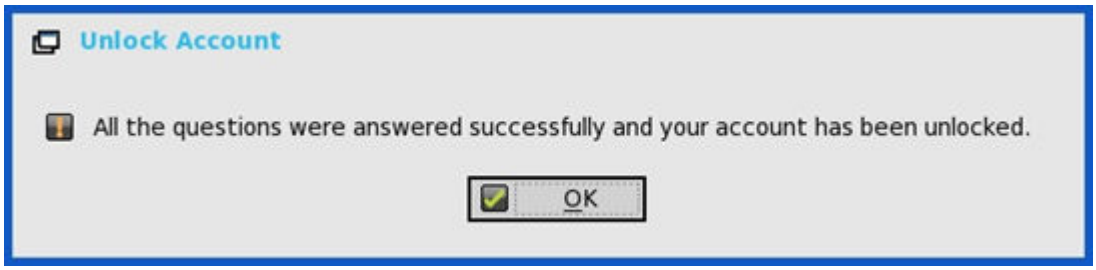


Figure 70. Unlock account success message

NOTE:

- If the provided answers are incorrect, the following error message is displayed.

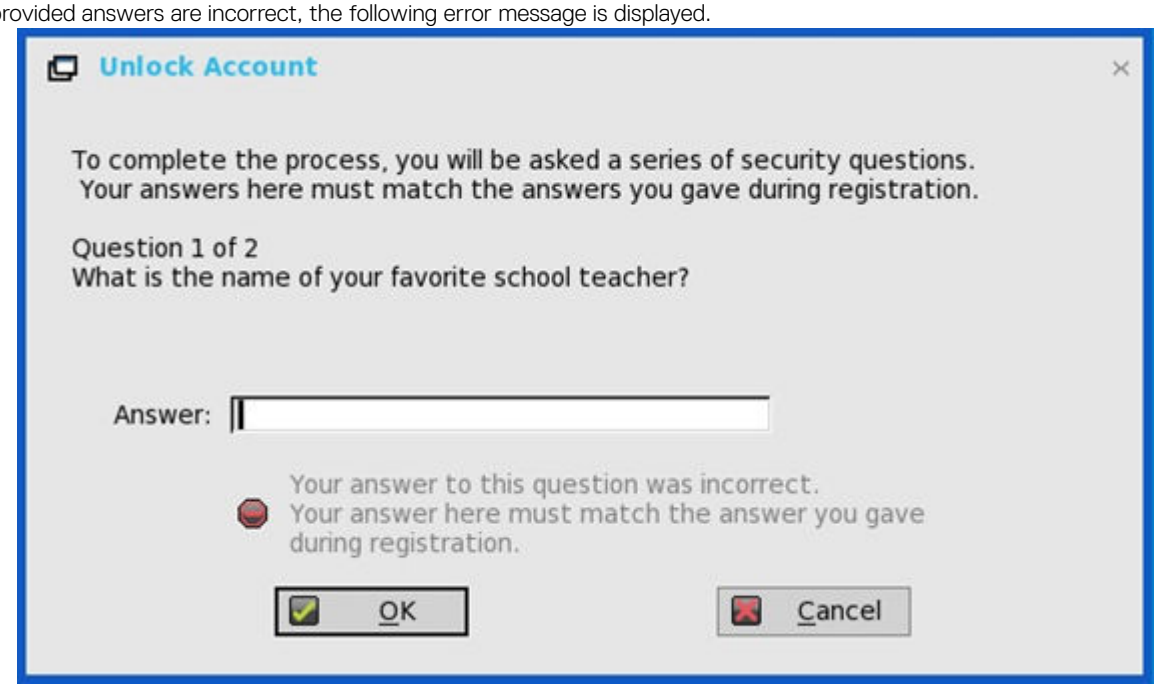


Figure 71. Error message

- If you provide the wrong answers more than three times, you can not unlock the account or reset the password, and the following error messages are displayed.

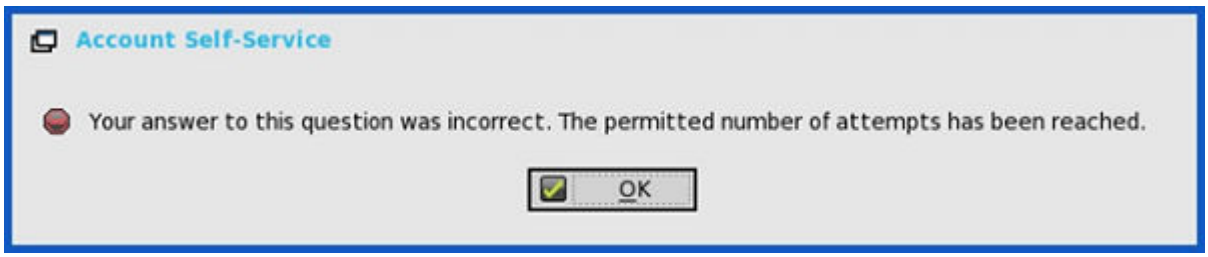


Figure 72. Attempts exceeded

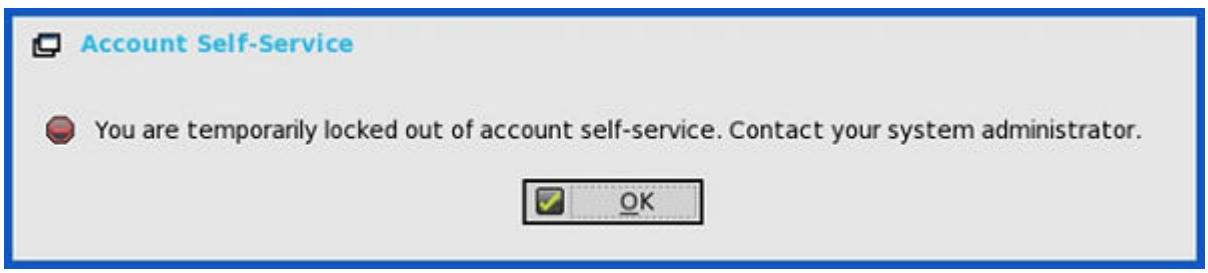


Figure 73. Account locked out

Resetting password

After you register the security questions, do the following to reset the password:

1 Choose a task (Reset password) in **Account Self-Service** window.

2 Enter the user name.

The **Reset Password** dialog box is displayed.

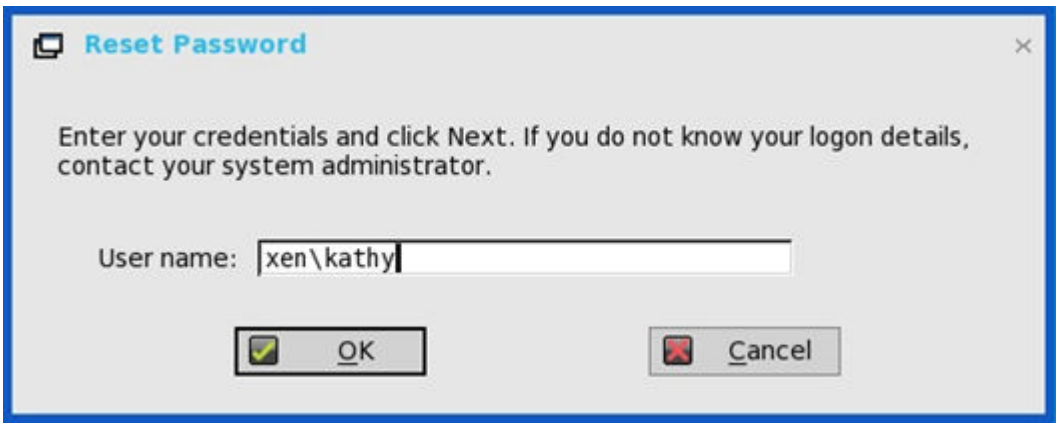


Figure 74. Reset password

3 Enter the registered answers to the security questions.

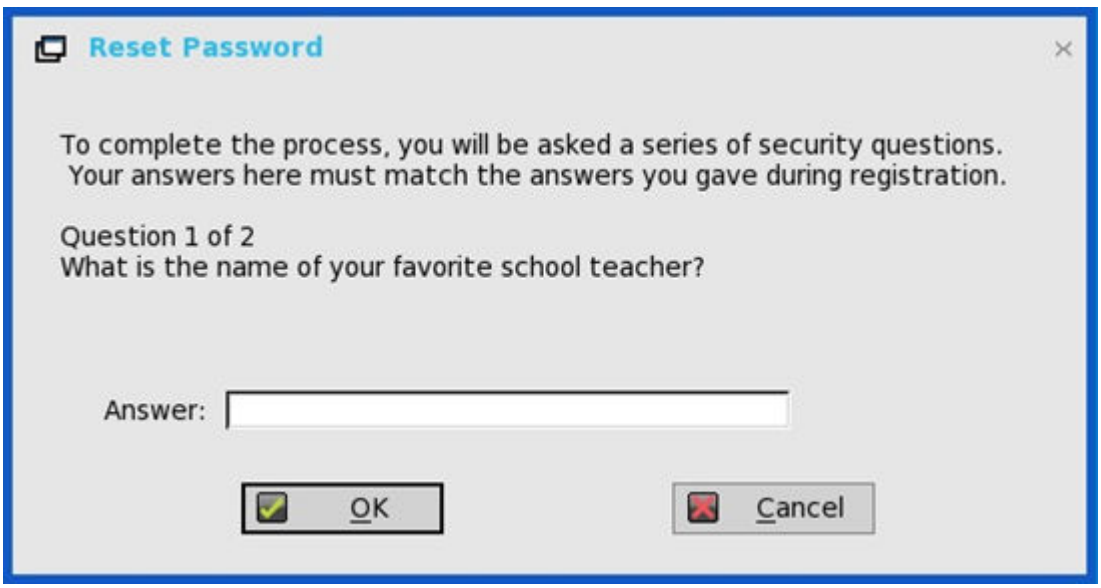


Figure 75. Security questions

Figure 76. Security questions

If the provided answers match the registered answers, then the **Reset Password** dialog box is displayed.

4 Enter and confirm the new password.

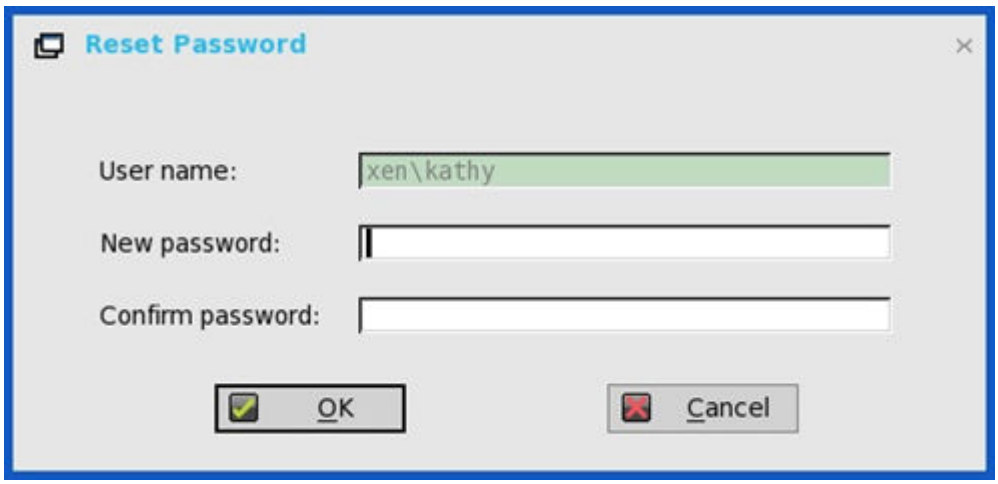


Figure 77. Set password

5 Click **OK** to successfully change the password.

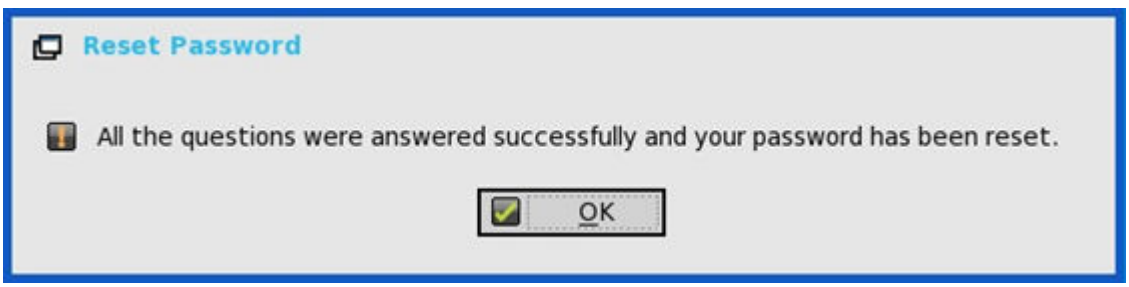


Figure 78. Password change successful

NOTE:
If you provide the wrong answers, you can not reset the password, and an error message is displayed.

QUMU or ICA Multimedia URL Redirection

QUMU utilizes ICA Multimedia URL Redirection. You are required to install a browser plug-in for this feature to work.

In earlier ThinOS Lite releases, ICA Multimedia URL Redirection was partially supported. In ThinOS Lite 2.4 release, a few enhancements are made to ICA Multimedia URL Redirection for better performance.

Supported protocols

- RTPS HLS
- HTTP

Verifying QUMU Multimedia URL Redirection: While the video is playing, a noticeable lag or jump in the video window is observed when you move the browser on the screen or scroll the browser. This behavior indicates that the video is being redirected.

To view the video sample, go to Kickoffdemo75.qumu.com/viewerportal/qumu/home.vp.

HTML5 Video Redirection

HTML5 Video Redirection controls and optimizes the way XenApp and XenDesktop servers deliver HTML5 multimedia web content to users. From XenApp and XenDesktop 7.12, this feature is available for internal web pages only. It requires the addition of JavaScript to the web pages where the HTML5 multimedia content is available, for example, videos on an internal training site.

The following server policies must be enabled:

- Windows Media redirection—By default this option is enabled.
- HTML5 video redirection—By default this option is disabled.

Verifying HTML5 Video Redirection—While the video is playing, a noticeable lag or jump in the video window is observed when you move the browser on the screen or scroll the browser. This behavior indicates that the video is being redirected.

ThinOS event log for RAVE MMR is also displayed.

Sometimes, the initial playback does not work. After several seconds, the video is refreshed automatically, and you need to click playback from start again. During this time, the video will redirect.

Reference documents

- Citrix sample video—www.citrix.com/virtualization/hdx/html5-redirect.html.
- ICA Multimedia policy settings—www.docs.citrix.com/en-us/xenapp-and-xendesktop/7-12/policies/reference/ica-policy-settings/multimedia-policy-settings.html.

ICA SuperCodec

ICA SuperCodec is a H.264 decoder integrated on ThinOS Lite ICA client side. Server encodes the session image into H.264 stream and sends it to client side. Client decodes the H.264 stream by SuperCodec and show the image on screen. It should improve user experience especially for HDX3DPro desktops.

Supported Environment

Citrix Virtual Apps and Desktops 7.5 or later versions

Supported Platforms

Wyse 5010 zero client for Citrix (D00DX) (ThinOS Lite Pro 2)

Wyse 3010 zero client for Citrix (T00X) (ThinOS Lite 2)

Wyse 3020 zero client for Citrix (T00DX) (ThinOS Lite 3)

Verifying the working status of the ICA connections

- **For Wyse 3010 zero client for Citrix (T00X) (ThinOS Lite 2) and Wyse 3020 zero client for Citrix (T00DX) (ThinOS Lite 3)**

  ICA SuperCodec is enabled by default when ThinOS Lite resolution is lesser than or equal to 1920 x 1080.

  a When the feature is working, the following results are displayed:

  ThinOS Lite event log ICA: SuperCodec enabled

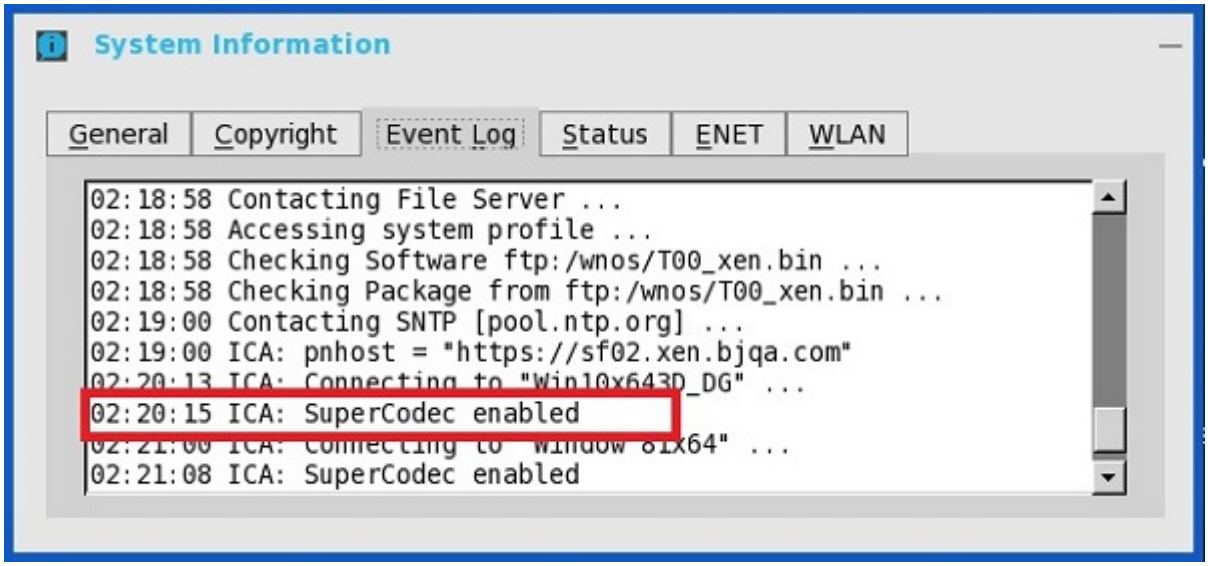


Figure 79. System information

Click **HDX Monitor** > **Graphics** > **Thinwire advanced** > **Encoder: DeepCompressionV2Encoder** for NON-HDX3DPro desktops or **DeepCompressionEncoder** for HDX3DPro desktops. From Citrix Virtual Apps and Desktops 7.11, the encoder is changed to Deprecated.

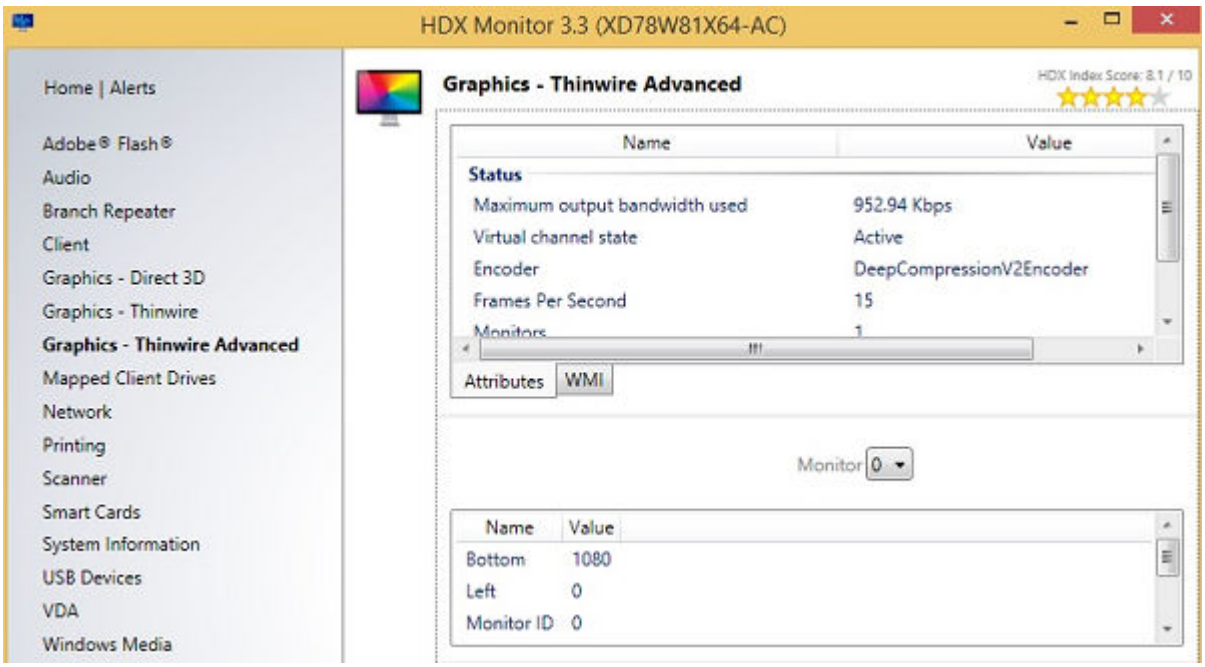


Figure 80. HDX Monitor 3.3

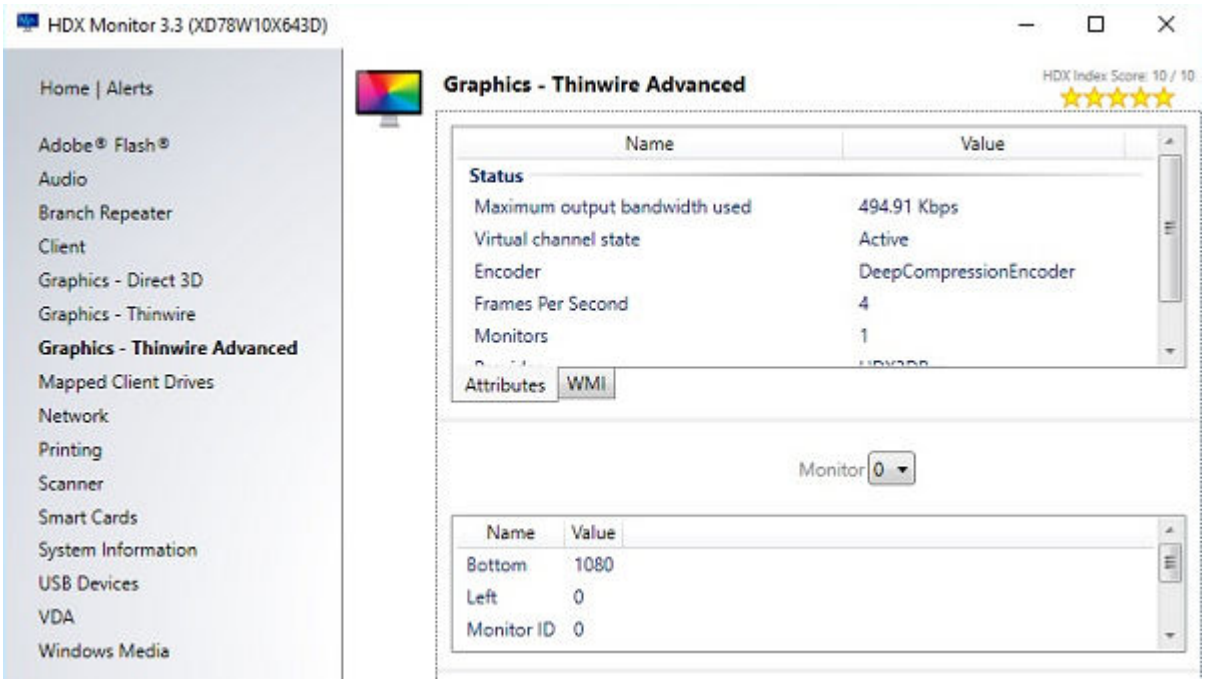


Figure 81. Graphics-Thinwire advanced

b When the feature is disabled, you can view the following results:

ThinOS Lite event log: System resolution exceeds hardware limitation (1920 x 1080), disable SuperCodec

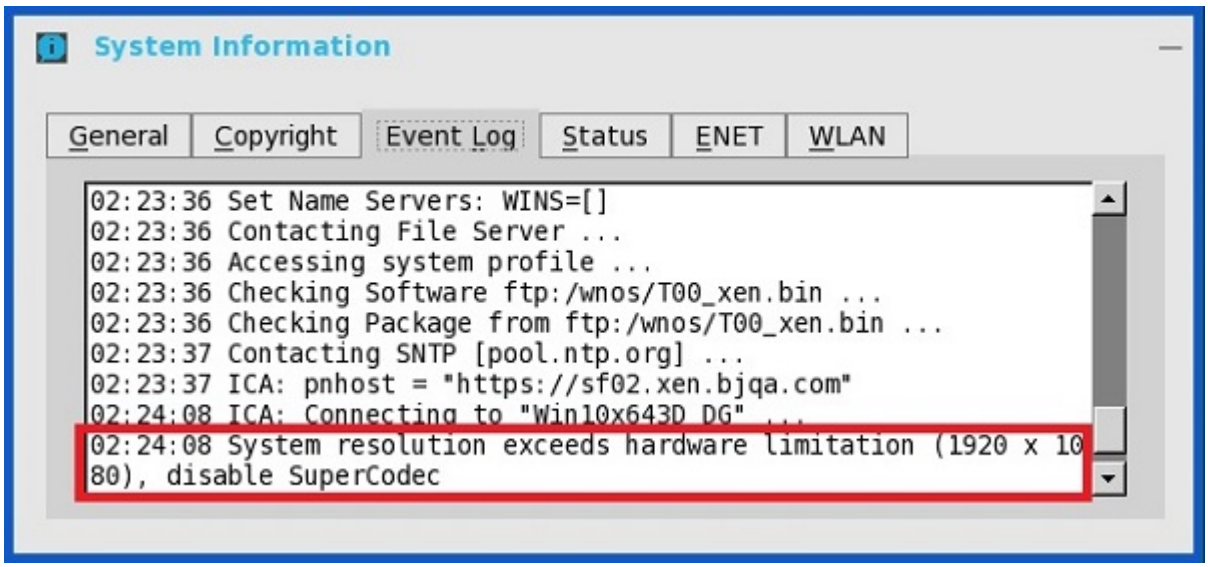


Figure 82. Event log

Click **HDX Monitor** > **Graphics** > **Thinwire Advanced** > **Encoder** > **CompatibilityEncoder; CompatibilityEncoder**. From Citrix Virtual Apps and Desktops 7.11, the encoder is changed to Deprecated

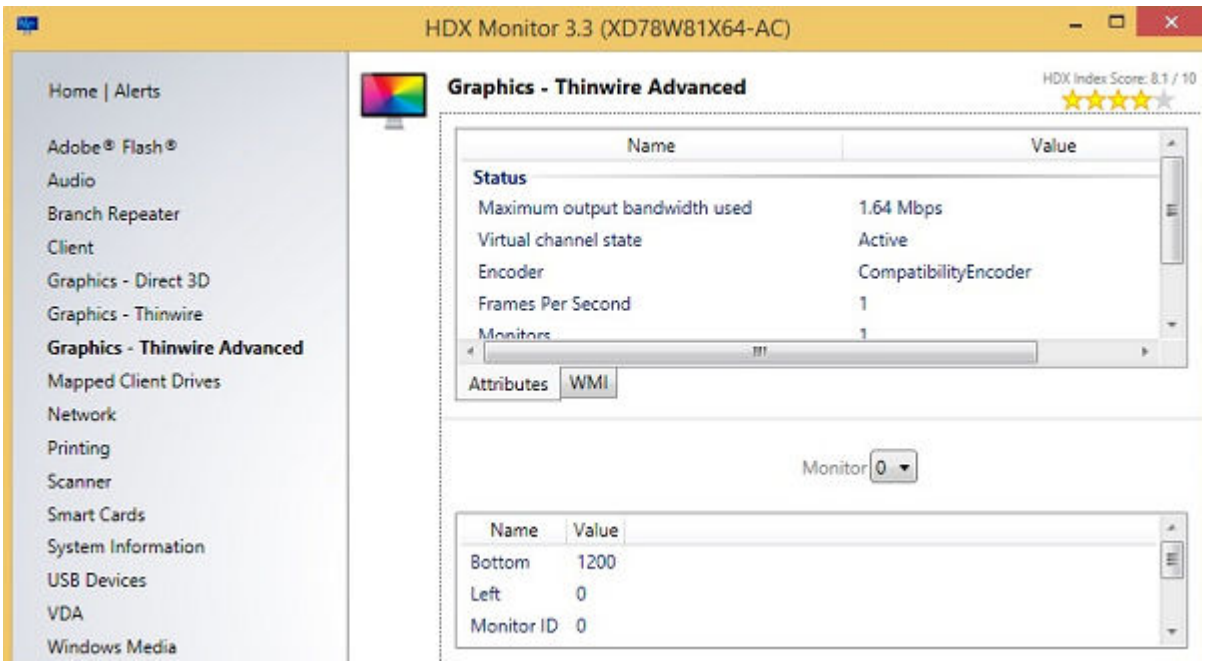


Figure 83. Status

- **For Wyse 5010 zero client for Citrix (D00DX) (ThinOS Lite Pro 2)**
  - ICA SuperCodec is always enabled without any limitation.
  - ThinOS Lite event log displays ICA: SuperCodec enabled.

NOTE: For ICA connections, there is no INI parameter.

Anonymous logon

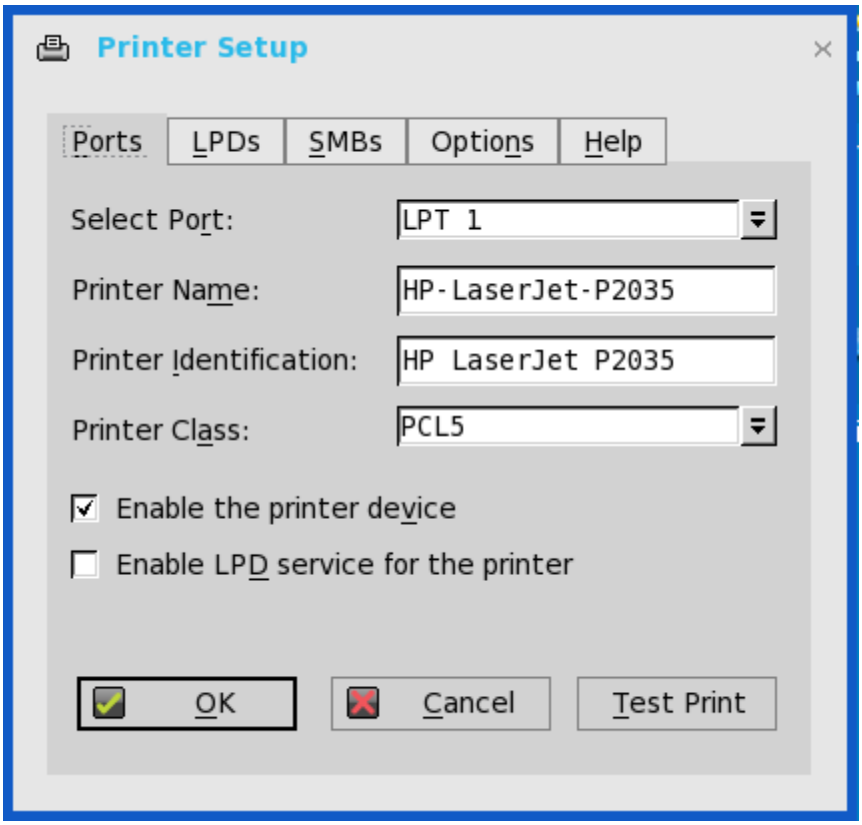
Anonymous logon—This feature enables the users to log in to the Storefront server configured with unauthenticated store without Active Directory (AD) user credentials. It allows unauthenticated users to access the applications instead of AD accounts.

Configuring the Citrix UPD Printer

Use of the Citrix Universal Printer Driver ensures that all printers connected to a client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center. Citrix Universal printer driver is the base of Citrix Universal Printer, it is an auto-created printer object that uses the Citrix Universal Print Driver and is not tied to any specific printer defined on the client.
To configure the Citrix UPD usage on ThinOS Lite:

1 Connect a printer to zero OS client, and from the floating bar menu click the **System Setup** , and then click **Printer Setup**.
The **Printer Setup** dialog box is displayed.

Figure 84. Printer setup



2 **Printer name** — Enter the name of the printer.
3 **Printer Identification**— Enter any string of the Printer identification.
4 Select the type of the printer class from the drop-down list and select the check box to enable the printer device, and then click **OK**.
5 Launch a Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) or Citrix Virtual Apps (formerly Citrix XenApp) application connection.
6 Open **Devices and Printers** in the desktop or application, notice the printer is mapped as UPD printer by default.

Citrix UPD Configuration on Server

Use the following guidelines for Citrix UPD configuration on Server:

1 To enable the printer policy in XenApp 6.5:
   a Go to the DDC Server.
   b Click **Start** > **Citrix AppCenter**.
   c Click **Citrix Resources** > **XenApp** > **Policies** > **User** > **Settings** > **Printing** > **Client Printers and enable the Auto-create generic universal printer**.
   d Click **Printing** > **Drivers**, and set the Universal print driver usage to use universal printing only from the drop-down menu available.
2 To enable the printer policy in XenApp/XenDesktop 7.5 and XenApp/XenDesktop 7.6:
   a Go to the DDC Server:
      1 Click **Citrix studio** > **Policies** and add a policy. Then enable the Auto-create generic Universal printer, set to from the drop-down menu.
      2 Set the Universal print driver usage to use universal printing only from the drop-down menu.
   b Check registry and make sure the same driver has been installed.
      1 Check the drivers in registry of the server or desktop which you want to connect. The server or desktop must have PS, PCL5, PCL4 drivers in the registry and the same driver must be installed on the server or desktop.
      2 Go to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\. ThinOS Lite does not support EMF and XPS.
   c If the server or desktop which you want to connect does not have these drivers, follow the steps mentioned here:
      1 For example, in XenApp A6.5+2008 R2, add PCL driver in Server. Go to **Device and Printers** > **Select any printer** > **Printer Server Properties** > **Driver** tab and then add HP LaserJet 2200 Series PCL 5 Driver.
      2 Under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\PCL5c\, change DriverAlias and DriverName HP LaserJet 2200 Series PCL 5.

Introduction to Flash Redirection

This solution is to offload Flash content to the ThinOS Lite client, and locally render and decode the flash playback. The offloading is conducted by Citrix HDX Flash Redirection. The local rendering and decoding process are conducted by customized flash player and other multimedia process that runs locally on ThinOS Lite.

Supported Environment—This release supports only Citrix Connections with XenApp 6.5 and later versions and XenDesktop 7.0 and later versions.

Supported Platforms—Wyse 5010 zero client for Citrix—D00DX (ThinOS Lite Pro 2).

Flash Redirection

Required packages

The below packages are required for the Flash Redirection to work correctly:

- `base.i386.pkg`— From the ThinOS Lite 2.2 release, the base package is integrated into the ThinOS Lite firmware image. You need not install or update this package manually.
- `FR.i386.pkg`

By default the packages should have been installed in system; if it is required to install the packages manually, follow the steps mentioned here:

1 Upload packages to directory `\wnos\pkg\`.
2 Ensure that the INI autoload is not set to 0.
   Set INI `AutoLoad=1 AddPkg=FR` in wnos.ini or xen.ini.

3 Restart the client to read File Server and wait till the auto installation of packages is complete.

4 User can view the installed packages in the **Packages** tab in the **System Tools** dialog box.

5 **Server configuration for Flash redirection**

To ignore the differences in flash player versions, user must add the `FlashPlayerVersionComparisonMask`registry key on the desktop.

If it is XenApp 6.5, `IEBrowserMaximumMajorVersion` registry key is required to ignore the differences in IE Browser versions.

6 **Client configuration for Flash redirection**

By default, no client configuration is required. New INI parameters are added to support HDX FR Client configurations, for example, to fetch the server side content. The newly added INI parameters are:

```
SessionConfig=ICA\
HDXFlashUseFlashRemoting=Never | Always (default) \
HDXFlashEnableServerSideContentFetching=Disabled (default) | Enabled \
```

How to verify it is working or not working

a Right-click the flash video to know the flash player version. It displays version information of the customized player at ThinOS Lite client side which is 11.1.102.59. If the flash player version is different, then it is unsuccessful server rendering.

b During the flash playback, it will display ThinOS Lite event logs for HDX FR in the System Information dialog box.

1 FR: Media type video/x-264

2 FR: Media type audio/mpeg

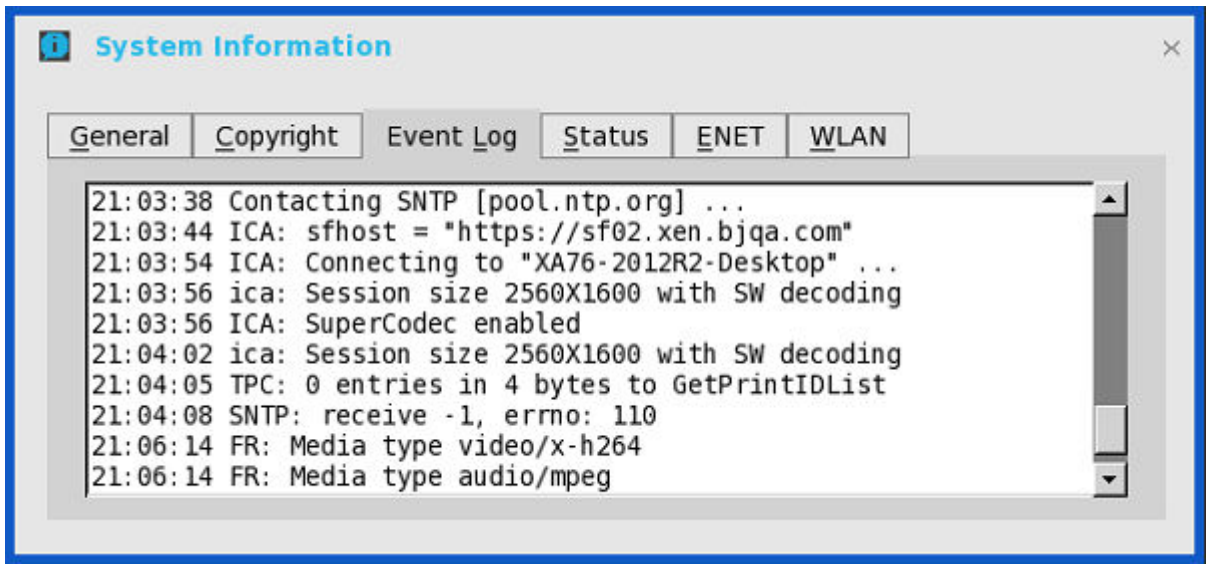


Figure 85. System information

Known Issues

a Playback flash videos in Internet Explorer browser with normal security settings.

b Playback with videos ≤ 720p; the 1080p video may show graphic issue.

c Playback full screen video with resolution ≤ 1920x1200; for example, full screen playback with ThinOS Lite resolution 1920 x 1200; in 2560 x 1600 full screen video there could be graphic issues.

d After flash video is loaded it will stay in initial size; for example, resizing browser will not resize the video content; it is same behavior with Citrix HDX FR Linux client.

e Only English font is supported; for example, subtitles in other languages will not be properly displayed.

f In some scenario the video shows no content initially; when user resizes browser the video appears normally; it is likely to happen with x86 desktops and is a known issue for Citrix HDX FR Linux client.

g Playback with videos that can work with HDX FR on Linux or Windows client: There are a number of videos/websites known as not working with Citrix HDX FR solution such as msn.com, espn.com, movies.yahoo.com, and dell.com. Flash videos simply cannot load with these websites using HDX FR solution. Some of them are working periodically; for example, videos on Dell.com were working well during this Feb/March but stopped working afterwards; the results can vary depending on user location as well (US/Europe/Asia). It is therefore recommended to make sure the target videos work with HDX FR on Linux or Windows, before working with it on ThinOS Lite.

h The solution on ThinOS Lite is based on Citrix HDX FR Linux version. It is advised to compare with Linux client in case of any issues.

i Playback YouTube.com videos may run into some issues; for example, cannot show video unless user copy the URL and paste it to the browser to visit again. In case any observation we recommend to compare with Linux client.

Citrix server configuration for Citrix HDX Flash Redirection

The following are the Citrix Server configurations for Citrix HDX Flash Redirection:

1 To disable flash version compatibility check, perform the following tasks:

NOTE: In common scenarios the flash player version installed on VDA/XenApp host is higher than the one in client (Windows/Linux or others). Citrix advised to disable flash version compatibility check to make HDX Flash redirection works between host and client.

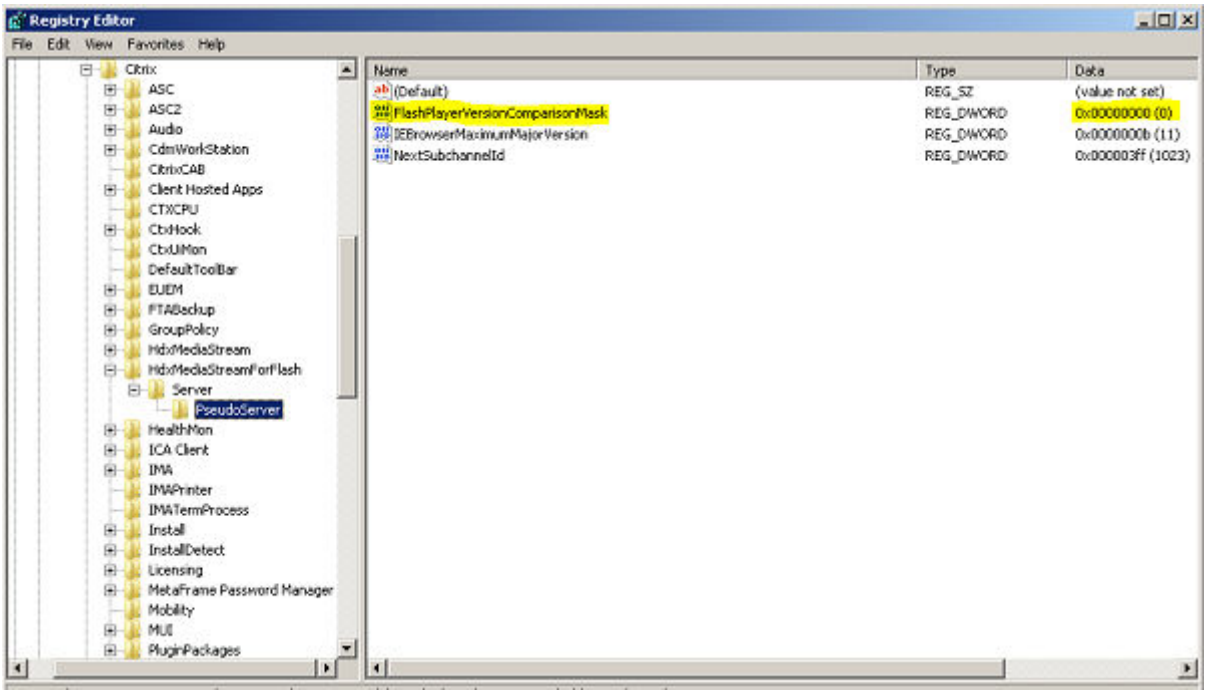


Figure 86. Registry Editor

a You can disable the version check by modifying Windows Registry Key on VDA/XenApp named "FlashPlayerVersionComparisonMask" which is a DWORD that must be set to zero.

b This needs to be set on each and every VDA/XenApp where the user needs the checking disabled.

- **For a 32 – bit operating system** :
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer.
  - Add the entry named FlashPlayerVersionComparisonMask with a DWORD value = 00000000
- **For a 64 – bit operating system**

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
- Add the entry named FlashPlayerVersionComparisonMask with a DWORD value = 00000000
- After making the modification you must restart IE on VDA/XenApp.

2 To modify maximum Internet Explorer version that HDX Flash supports:

a HDX Flash client side rendering feature does not work with Internet Explorer 11 with HDX Flash redirection enabled on XenApp 6.5 and XenDesktop 5.6 VDA.

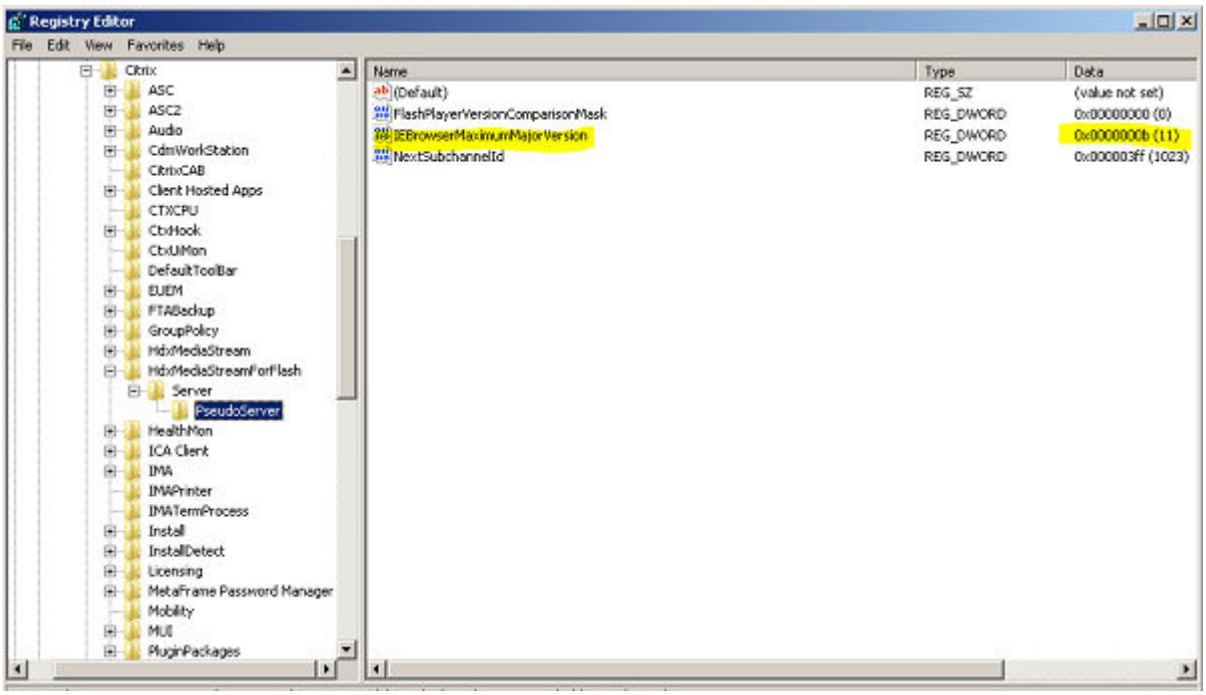


Figure 87. Pseudo server

b The registry key value IEBrowserMaximumMajorVersion is queried by the HDX Flash service to check for maximum Internet Explorer version that HDX Flash supports. For Flash Redirection to work with Internet Explorer 11, set the registry key value IEBrowserMaximumMajorVersion to 11 on the machine where HDX flash service is running. In case of XenApp it would be the XenApp Server and in case of XenDesktop it would be the machine where VDA is installed.

- For a 32-bit operating system:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  - Add the entry named IEBrowserMaximumMajorVersion with a DWORD value = 0000000b
- For a 64-bit operating system:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  - Add the entry named IEBrowserMaximumMajorVersion with a DWORD value = 0000000b

NOTE: This is applicable for XenApp 6.5 and XenDesktop 5.6 VDA.

3 To add a new policy:

a Launch **XenApp/XenDesktop Manage** console, go to **Policies** node pane.

b You can edit '**Unfiltered**' User Policy, that will apply to all connections.

c You can add a new personal policy, and assign it to your own Operating System (OS) and Domain User. For example, a new policy named '**Flash Test**' is added which can be viewed in the screenshot.

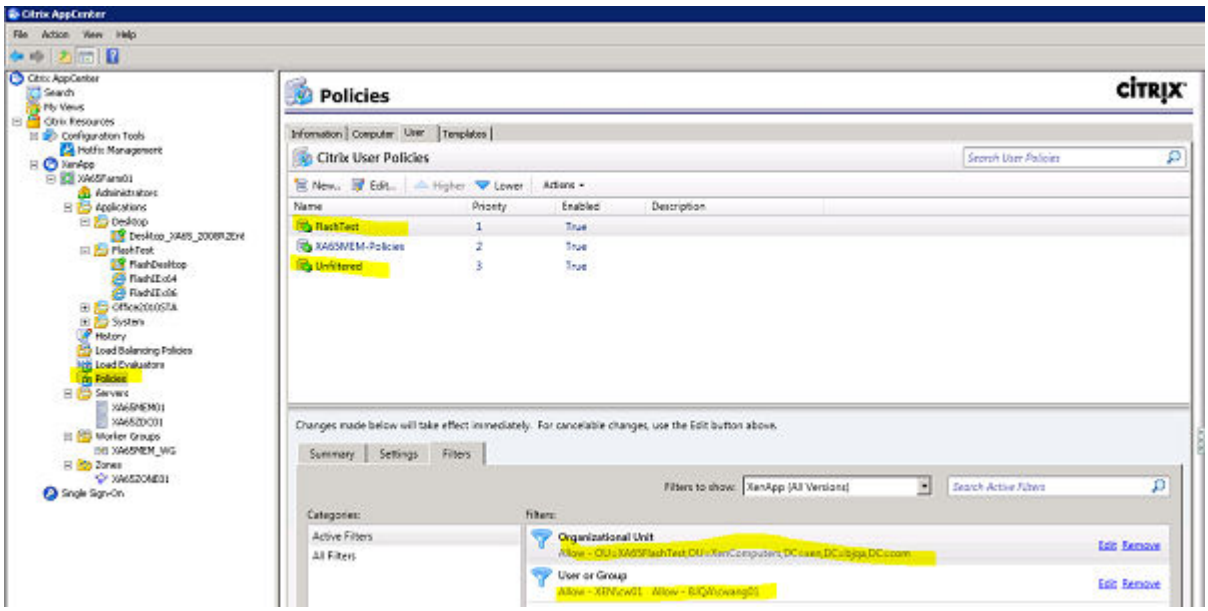


Figure 88. Policies

4 To view the list of Flash policies:

a Go to **Setting** tab, and select **Flash Redirection** category. All the Flash Redirection policies will be listed as shown in the following screenshot.

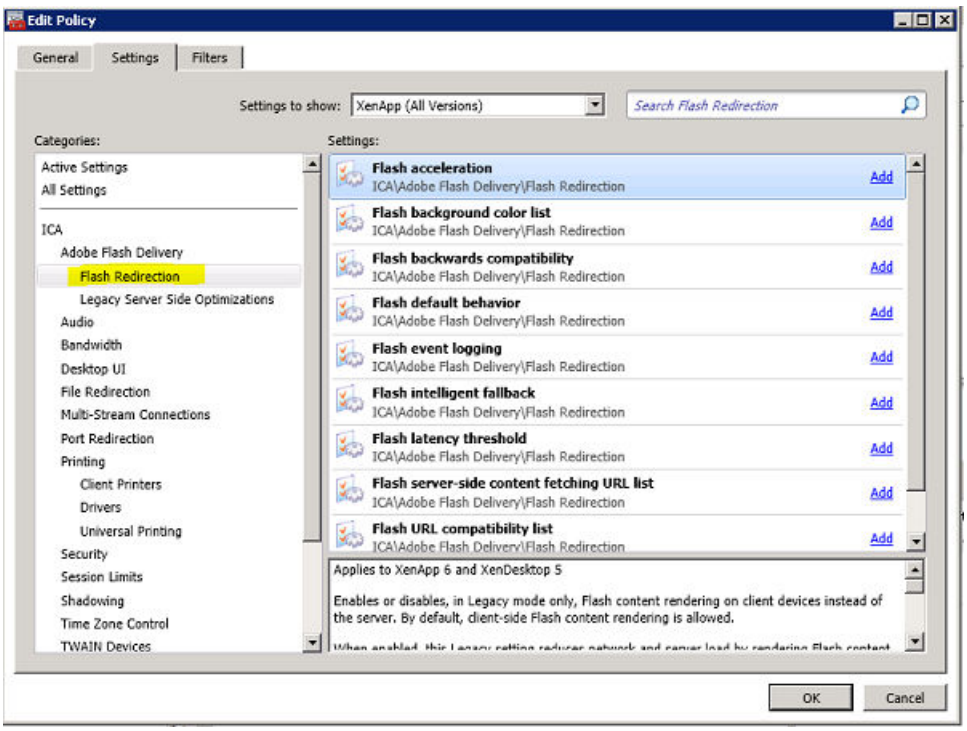


Figure 89. Edit Policy

5 To activate a policy:

a After modifying any Citrix policy, run the CMD command 'gpupdate /force' in the XenApp/VDA machine, and then reconnect the session. The policy will be updated immediately.

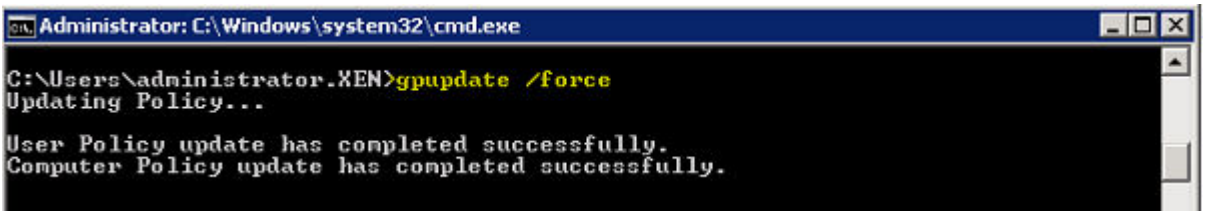


Figure 90. User policy update

6 To verify if Flash is getting client rendered OR HDX Flash redirection is working:

a Right-click on the Flash Region to view the Flash context menu. If the Flash context menu is same as native Linux menu, the ThinOS Lite built-in Adobe Flash Player version is 11.1. The following screenshot shows that the Flash is getting client rendered.

b When flash is client rendered, the event log will display “FR”.

7 To delete dynamic blacklist manually:

a Go to **Registry Editor**, right-click on HKEY_CURRENT_USER to find the keyword ‘**DynamicBlacklist**’, then delete the blacklist keys or blacklist records. For more information on Dynamic Blacklist, refer http://support.citrix.com/article/CTX126817.

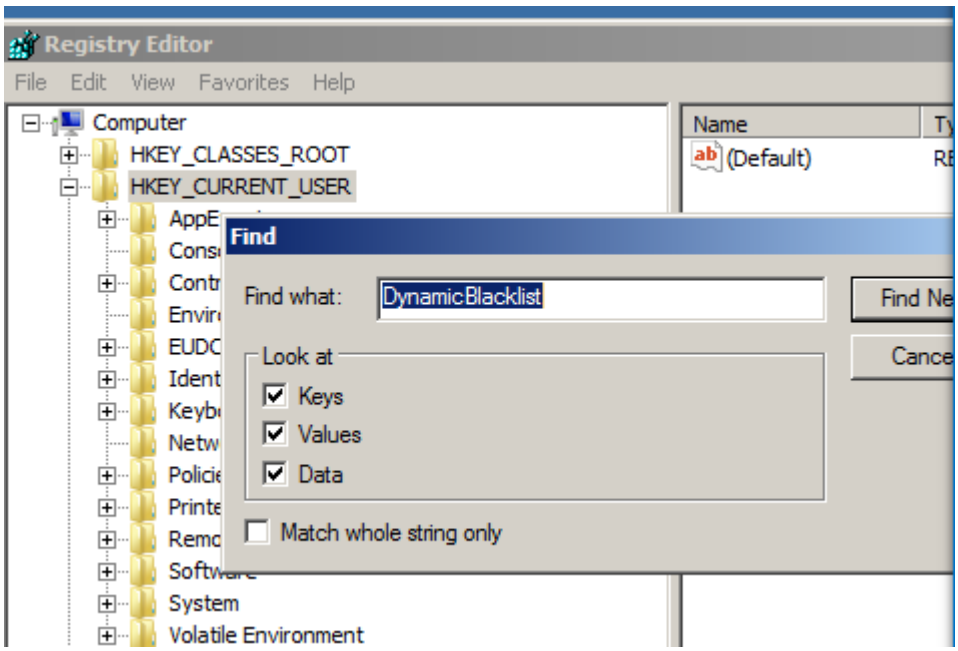


Figure 91. Registry Editor

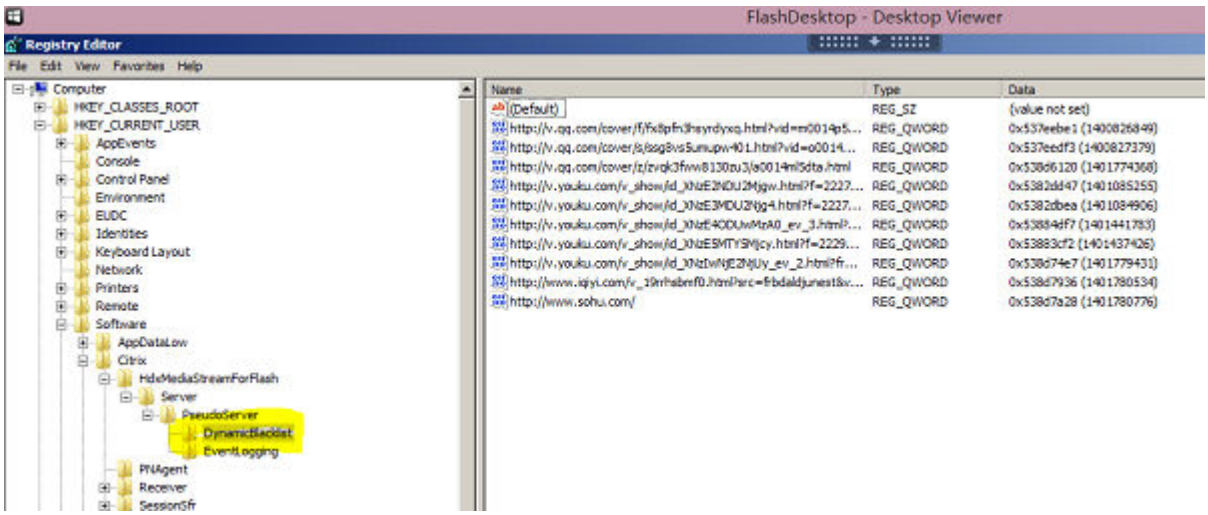


Figure 92. FlashDesktop

Citrix HDX Flash Redirection Policies Configurations

Policy - Flash default behavior

1 Remove all other active flash related policies in XenApp/XenDesktop server side.

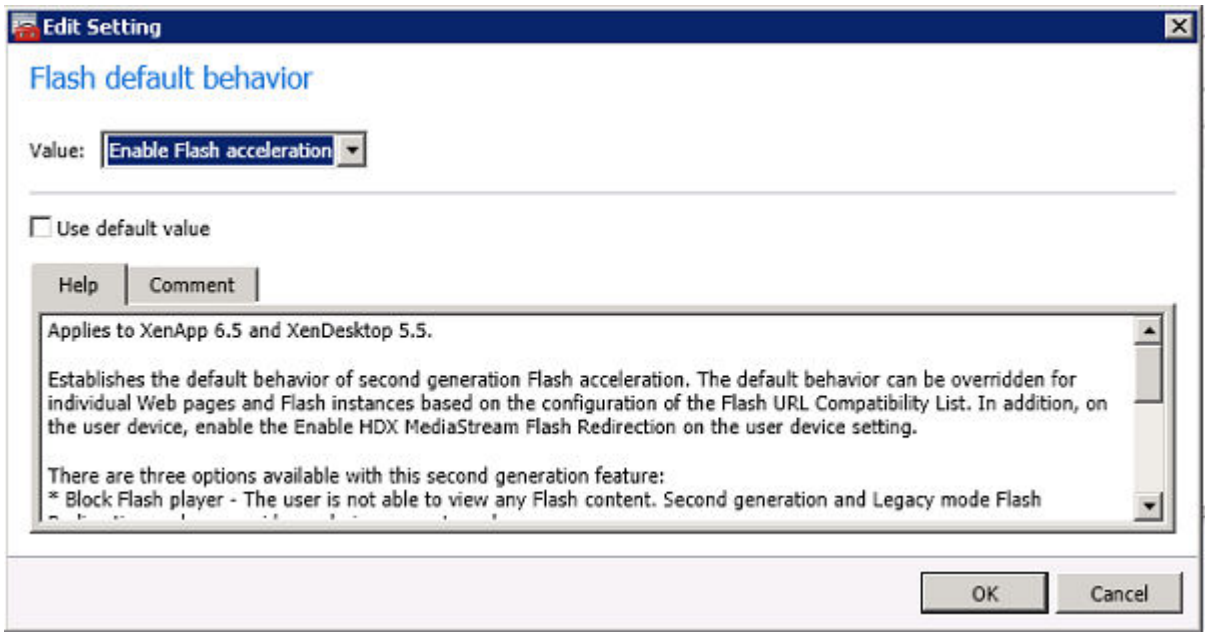


Figure 93. Enable Flash acceleration

2 Set Enable Flash acceleration for policy 'Flash default behavior' in XenApp/XenDesktop server side. Then run a web Flash video in ICA session for the client to render the flash video.

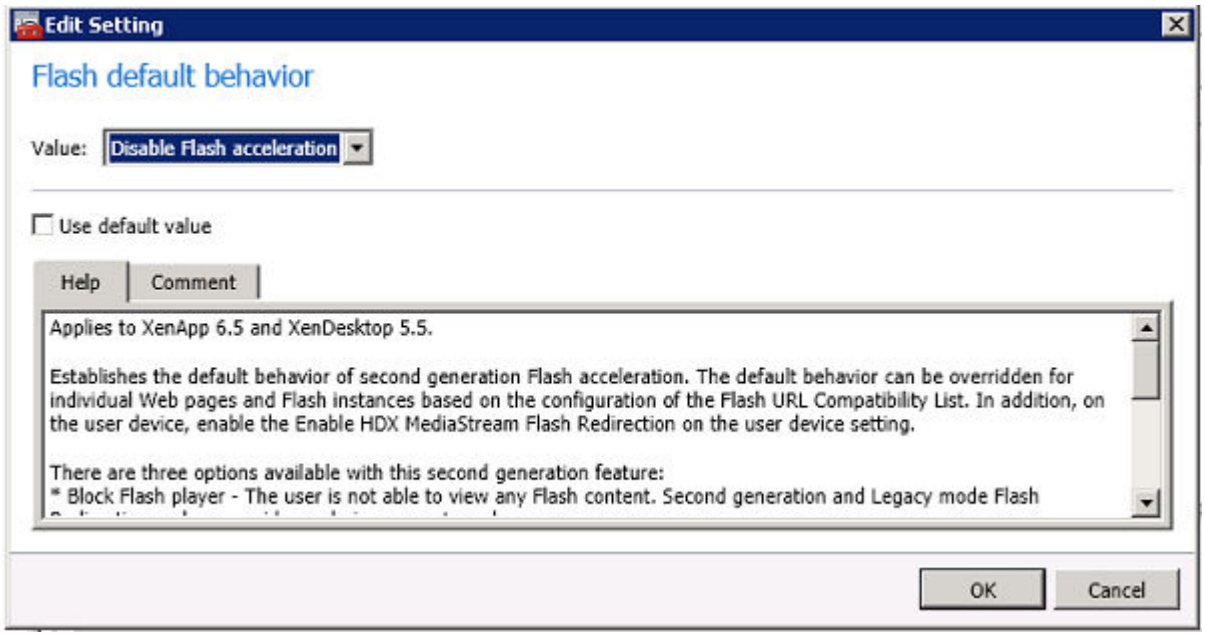


Figure 94. Disable Flash acceleration

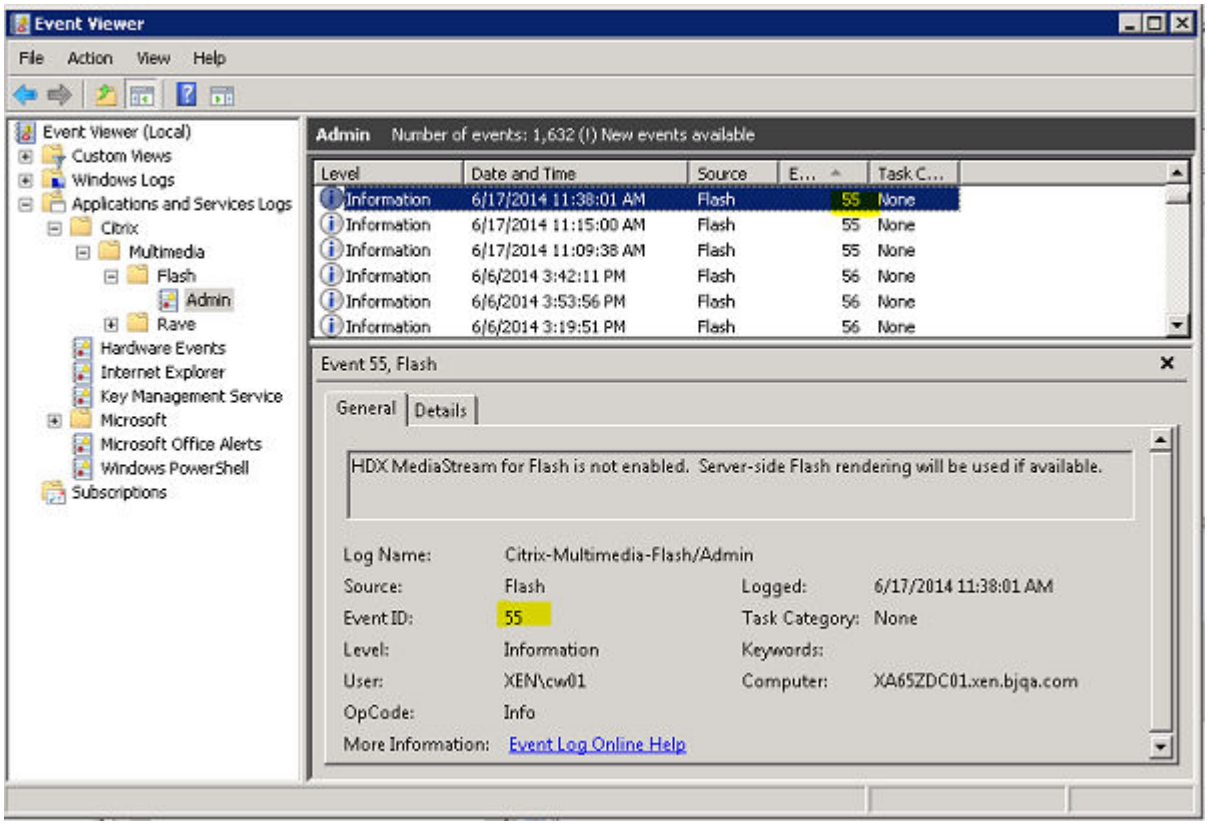


Figure 95. Event viewer

3 Set **Block Flashacceleration** for the policy **Flash default behavior** in the XenApp/XenDesktop server side, and then run a web Flash video in ICA session, the flash video will be server rendered and event 55 generates in **event viewer** > **ApplicationsAndServicesLogs** > **Citrix** > **Multimedia** > **Flash** > **Admin**.

4 Set **Block flashplayer** for policy 'Flash default behavior' in **XenApp/XenDesktop** server side, and then run a web Flash video in ICA session, the flash instances are blocked and event 63 generates in **event viewer** > **ApplicationsAndServicesLogs** > **Citrix** > **Multimedia** > **Flash** > **Admin**.

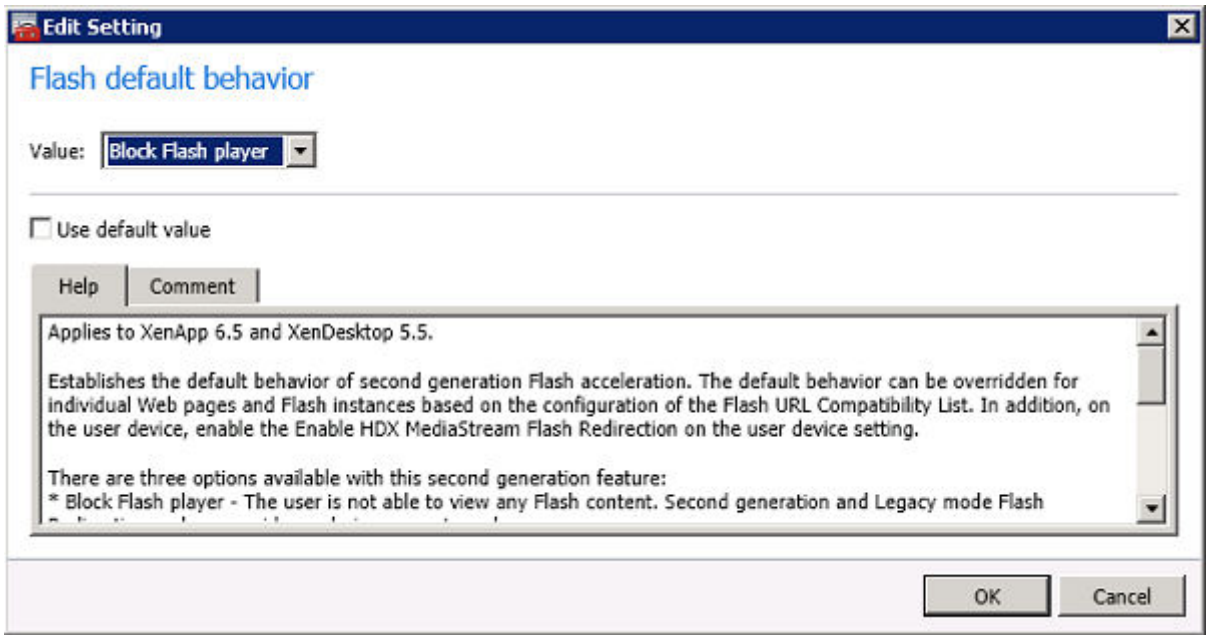


Figure 96. Block Flash player

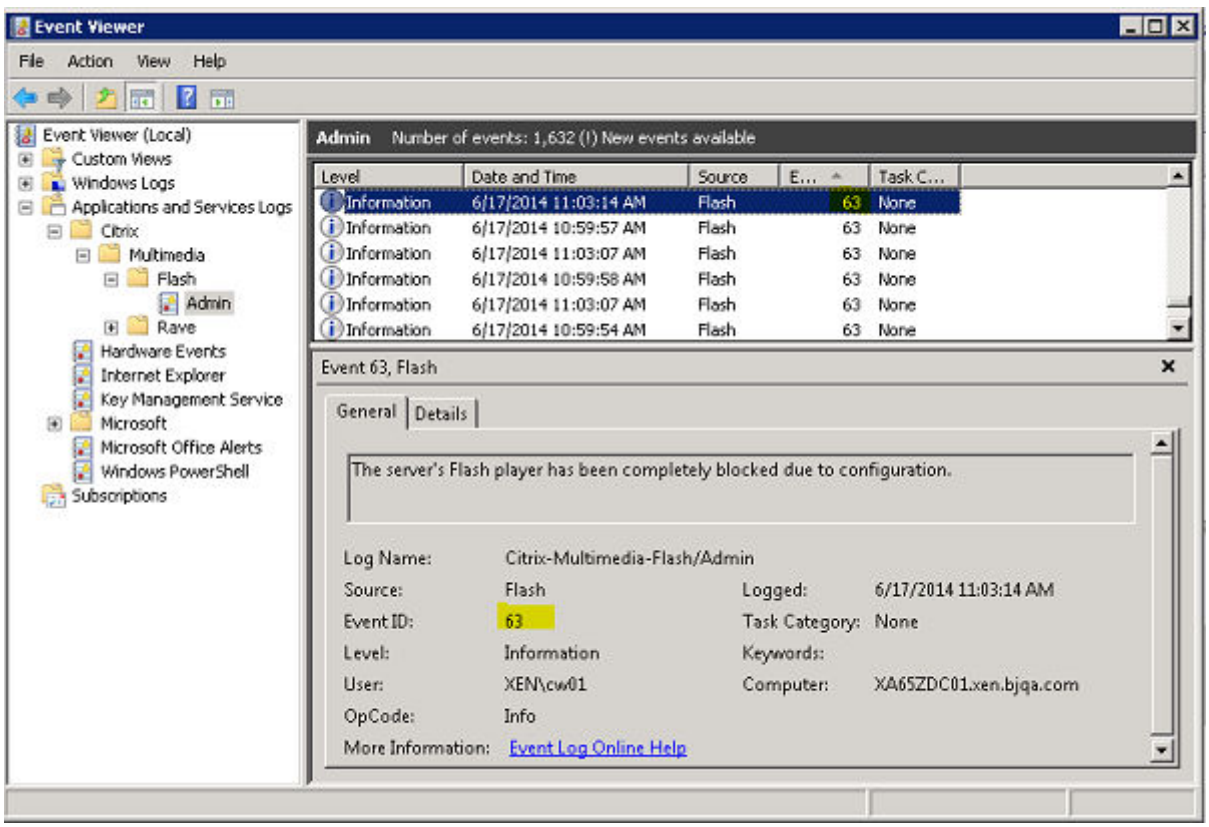


Figure 97. Event viewer

Policy - Flash URL compatibility list

1 Edit XenApp/XenDesktop policy 'Flash URL compatibility list', such as new item {Render On Client, *youku.com*, Any}, and then access the website (For example, www.youku.com). All flash instances on the website are client rendered.

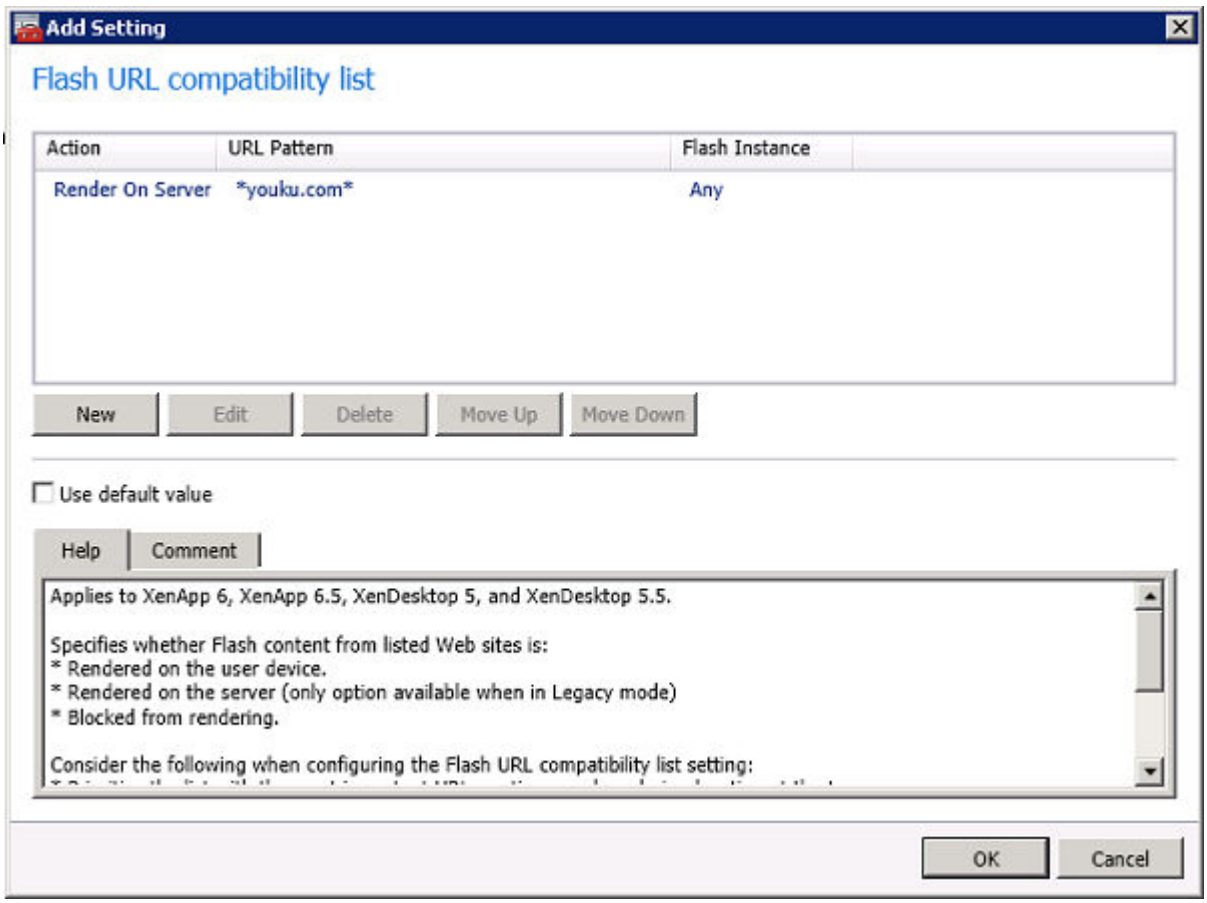


Figure 98. Flash URL compatibility list

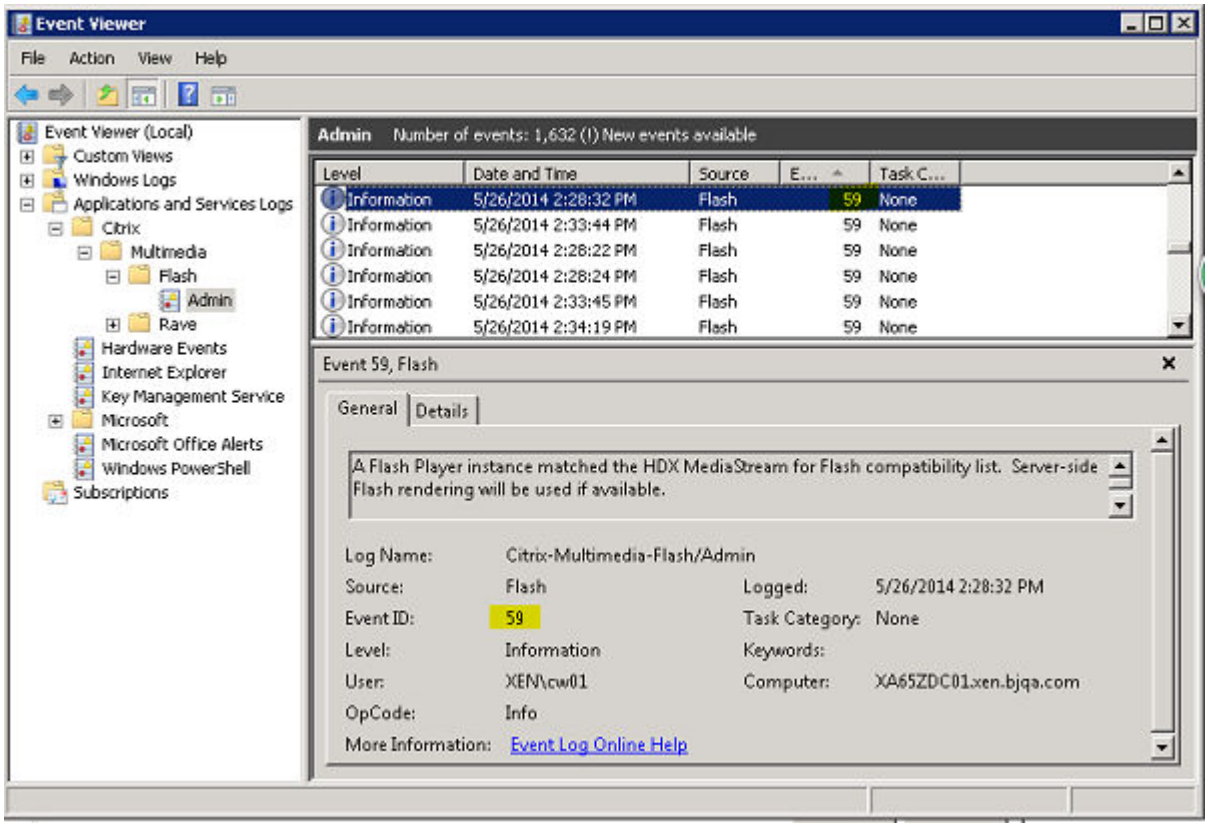


Figure 99. Event viewer

2 Edit XenApp/XenDesktop policy 'Flash URL compatibility list', such as new item {Render On Server,*youku.com*, Any}. And then access the website (For example, www.youku.com). All flash instances on the website are server rendered, and Event 59 generates in event viewer.

3 Edit XenApp/XenDesktop policy 'Flash URL compatibility list', such as new item {Block, *youku.com*, Any}. And then access the website (For example, www.youku.com). All flash instances on the website are blocked and Event 60 generates in event viewer.

Policy - Flash background color list

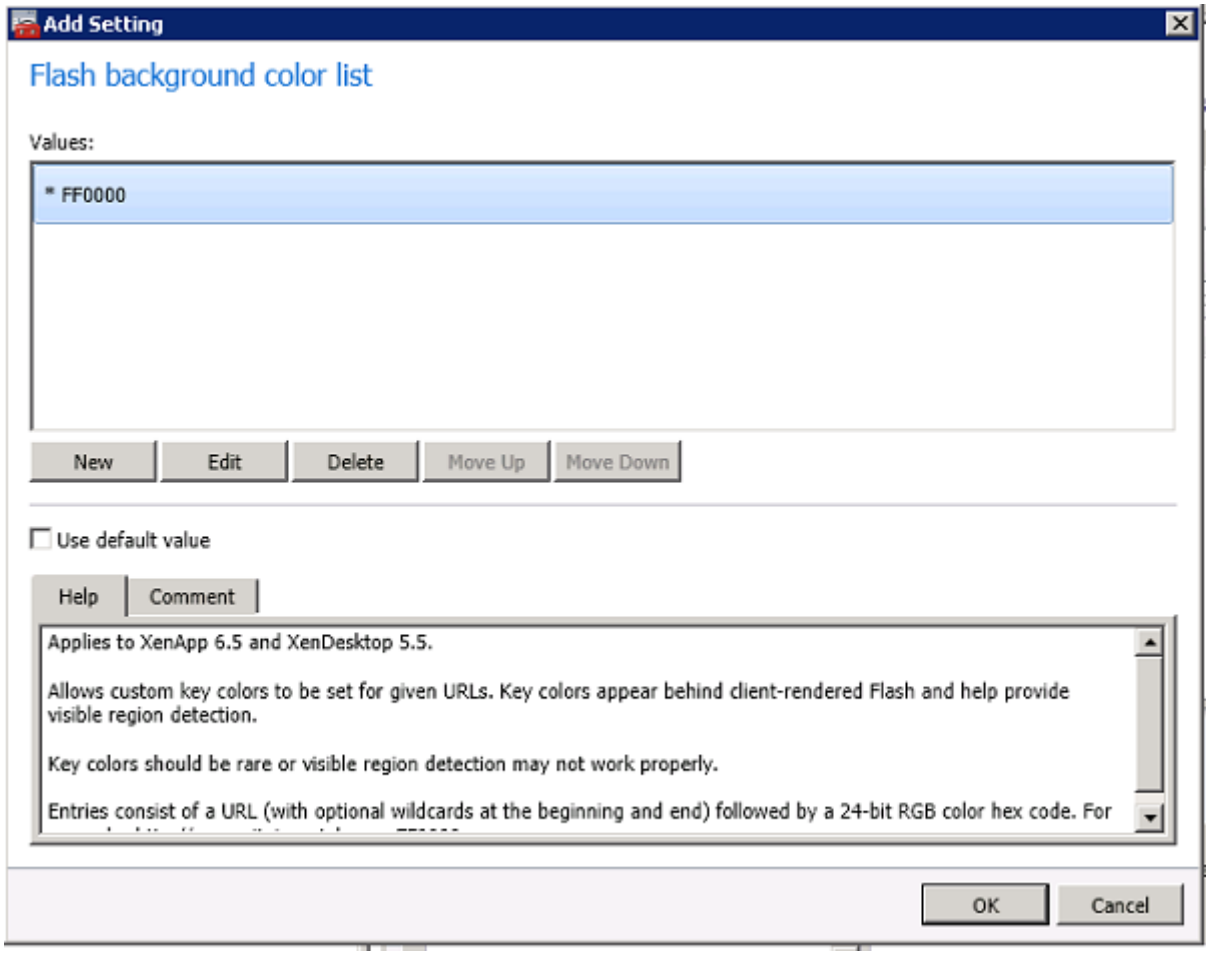


Figure 100. Flash background color list

1 Edit the Flash background color list in XenApp/XenDesktoppolicy, such as new item {*FF0000}.

2 Access any web site, for example . www.youku.com to play a flash video through HDX FR, when the flash background color is red.

Policy - Flash intelligent fallback

1 Enable the policy 'Flash intelligent fallback' in XenApp/XenDesktop server side. Run some flash websites in ICA session. Event 61 generates in **event viewer** > **Applications And ServicesLogs** > **Citrix** > **Multimedia** > **Flash** > **Admin** .

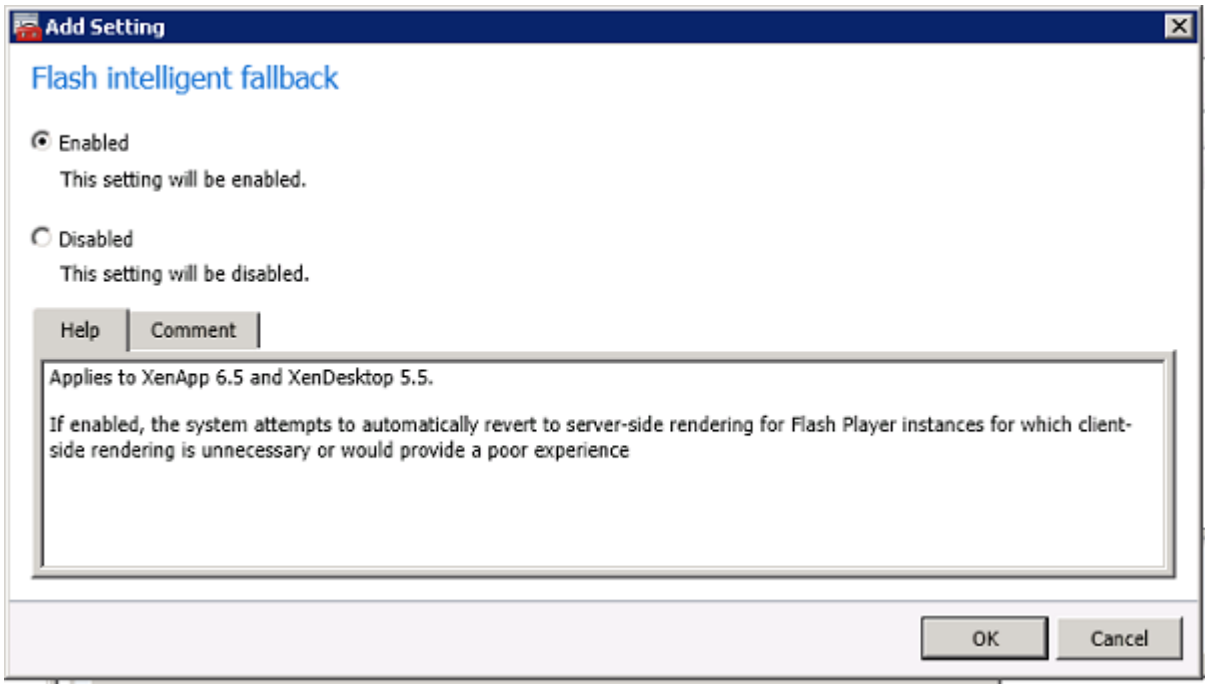


Figure 101. Flash intelligent fallback—Enabled

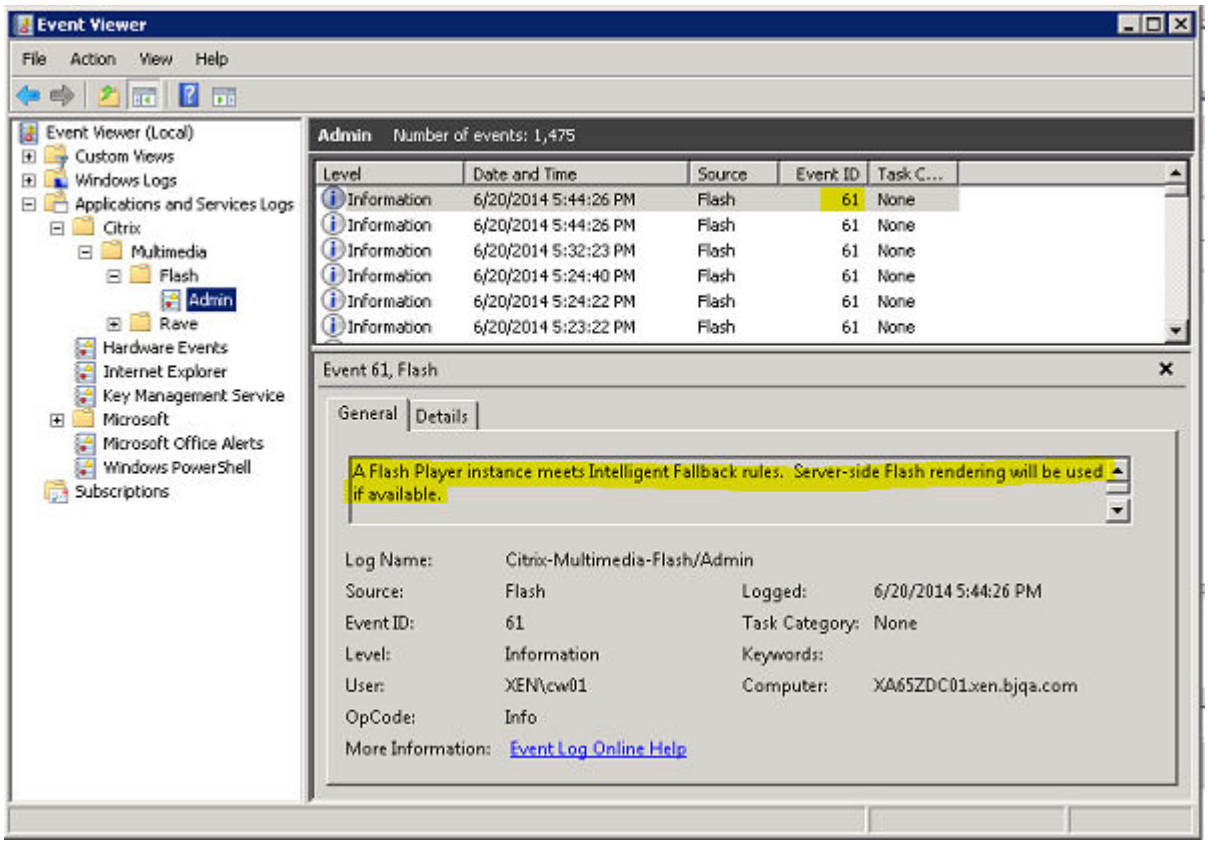


Figure 102. Event viewer

2 Disable the policy **Flash intelligent fallback** in XenApp/XenDesktop server side. Run some flash websites in ICA session. there will be no new event 61 in **event viewer** > **Applications And ServicesLogs** > **Citrix** > **Multimedia** > **Flash** > **Admin**.

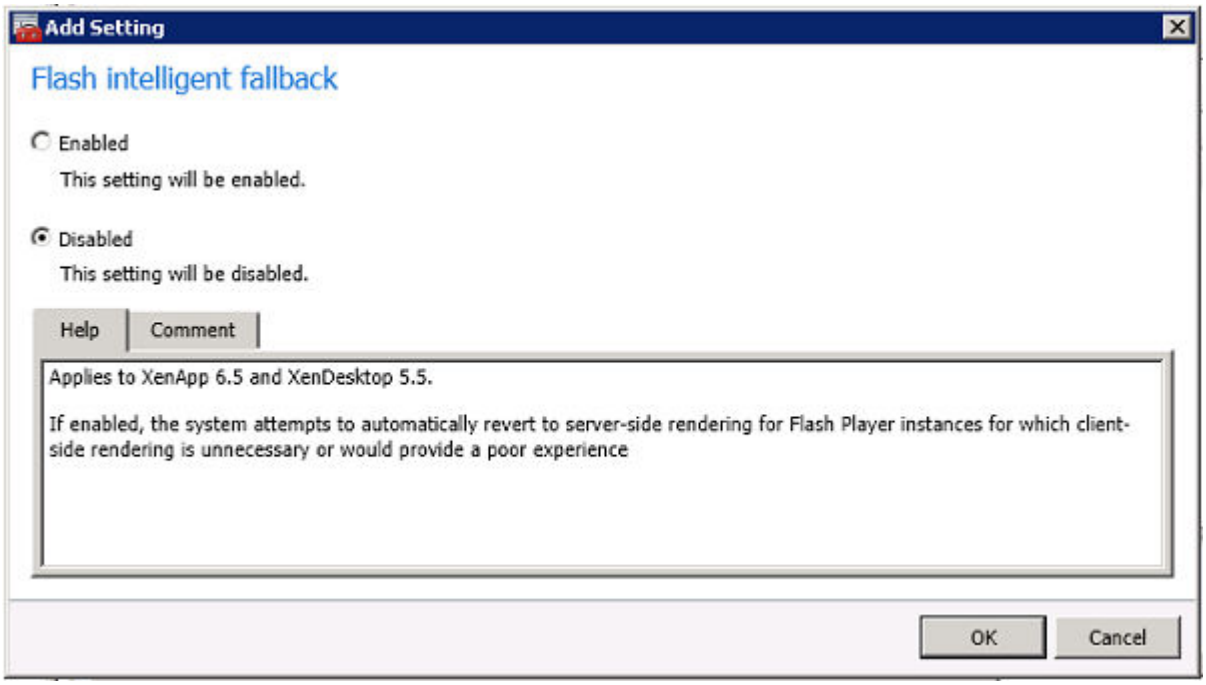


Figure 103. Flash intelligent fallback—Disabled

Policy - Flash server-side content fetching URL list

1 Edit the **Flash server-side content fetching URL list** in XenApp/XenDesktop policy, such as new item {*}

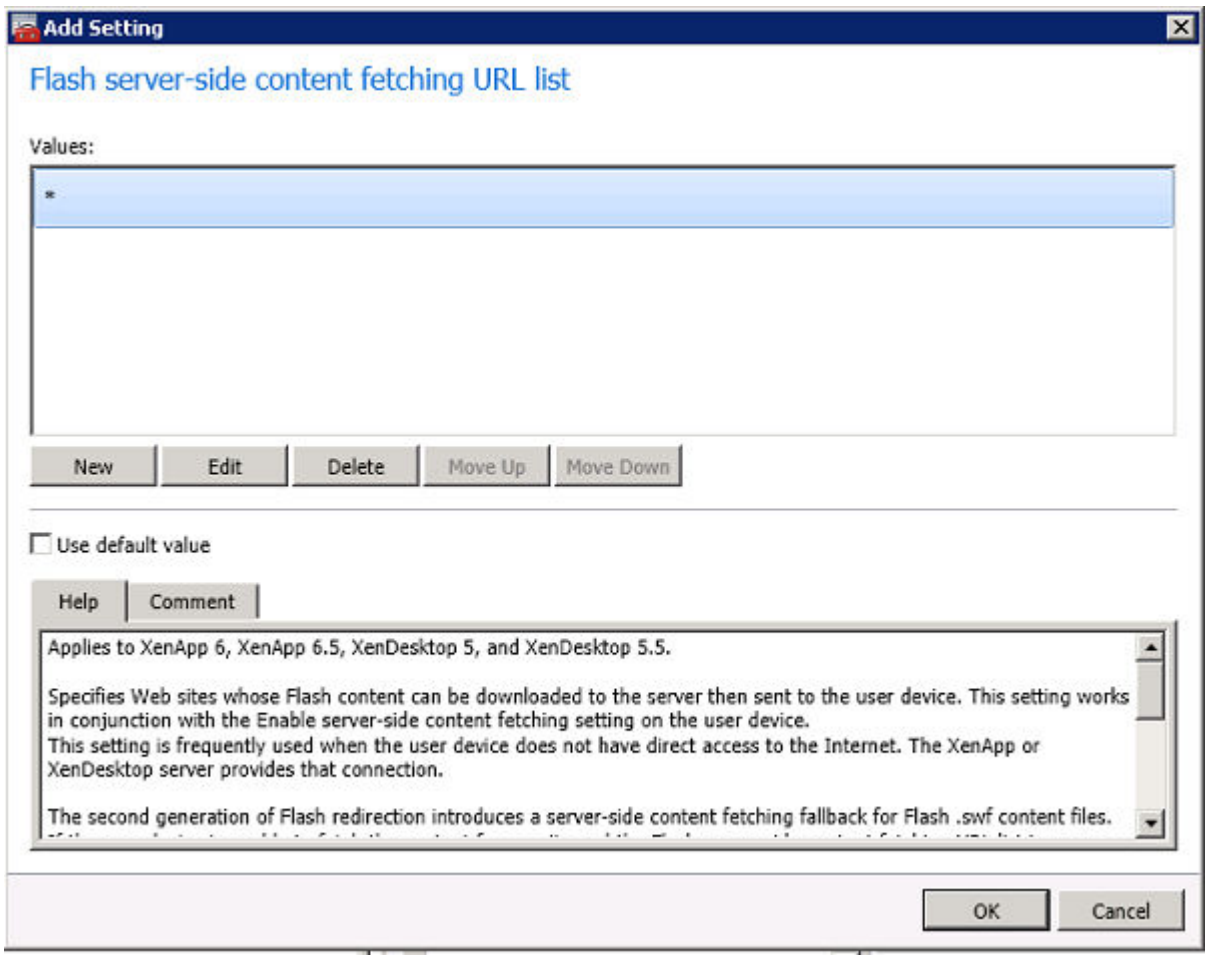


Figure 104. Flash server-side content fetching URL list

2 Set the ThinOS Lite INI using the {SessionConfig=ICA HDXFlashEnableServerSideContentFetching=Enabled}

3 Make sure that the client cannot access your testing Flash website, set an unreal DNS server to break client internet connection. You can try to ping your website domain name for example **www.youku.com** that request will be timed out.

4 Access any website for example **www.youku.com** to play a flash video through HDX FR. The flash video can still be client rendered employing server-side content fetching.

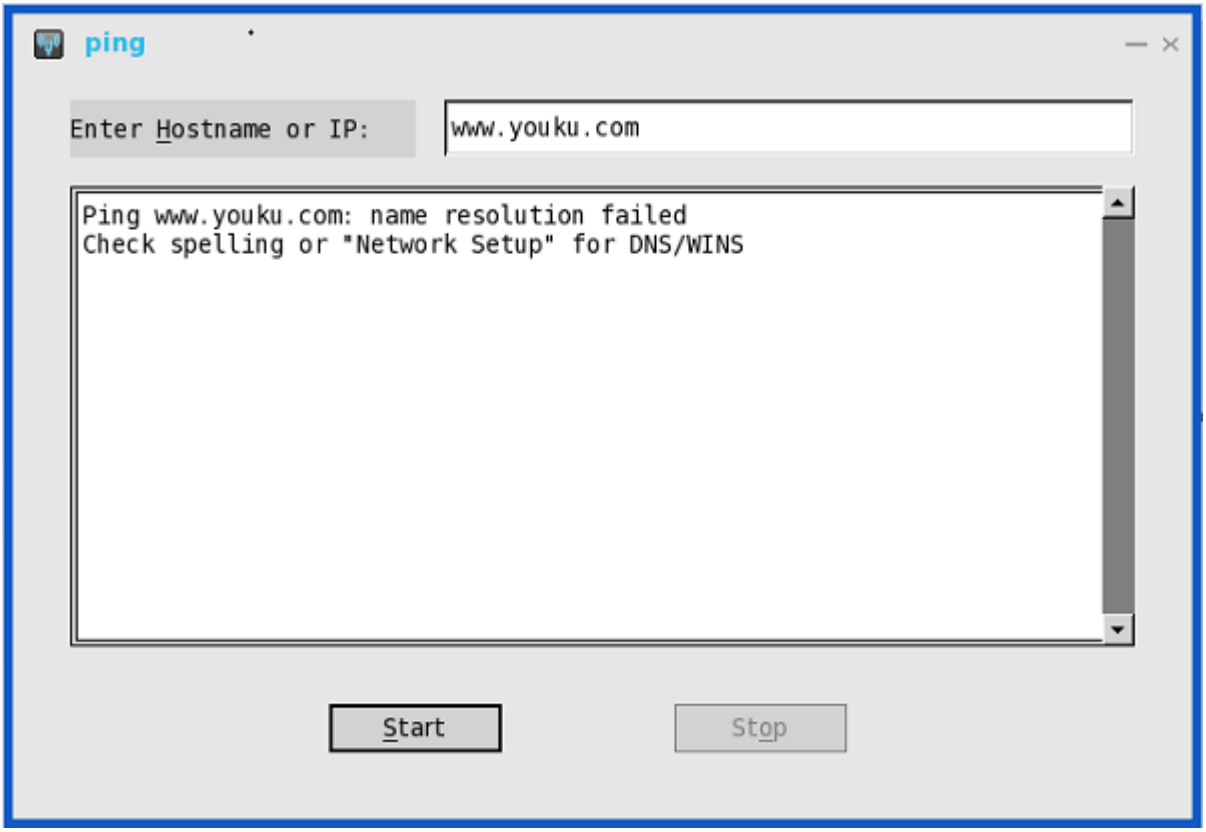


Figure 105. Ping

7

Configuring Zero Client Settings

You can configure available zero client settings on the zero client using the following. Depending on user privilege level, some dialog boxes and options may not be available for use.

- Local Settings Menu
- Reset Features

NOTE: While it is not recommended to use dialog boxes for configuring zero client settings, they are available in case you want to temporarily override central default configurations or you do not have the option to set up central configuration (smaller environments). In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all supported zero clients in your environment. For more information, see Central Configuration: Automating Updates and Configurations.

Local Settings Menu

Local Settings menu items include:

- Configuring the System Preferences
- Configuring the Display Settings
- Configuring the Peripheral Settings
- Configuring the Printer Settings

To access the Local Settings menu:

- **Zero Desktop** — Click the **System Settings** icon on the Zero Toolbar. Administrators can also click the **Admin Mode** button on the **Login** dialog box.

NOTE: User Name is the user who is logged-on and is at the lower-left pane of the taskbar.

Configuring the System Preferences

Use the **System Preference** dialog box to select personal preferences such as screen saver, time/date and custom information settings.

Use the following options to configure the System Preferences:

- Setting the General System Preferences
- Setting the Time and Date
- Setting the Custom Information

Setting the General System Preferences

To configure the General Settings for System Preference:

1 From the floating bar menu, click the **System Setup** , and then click **System Preferences**.
The **System Preference** page is displayed.

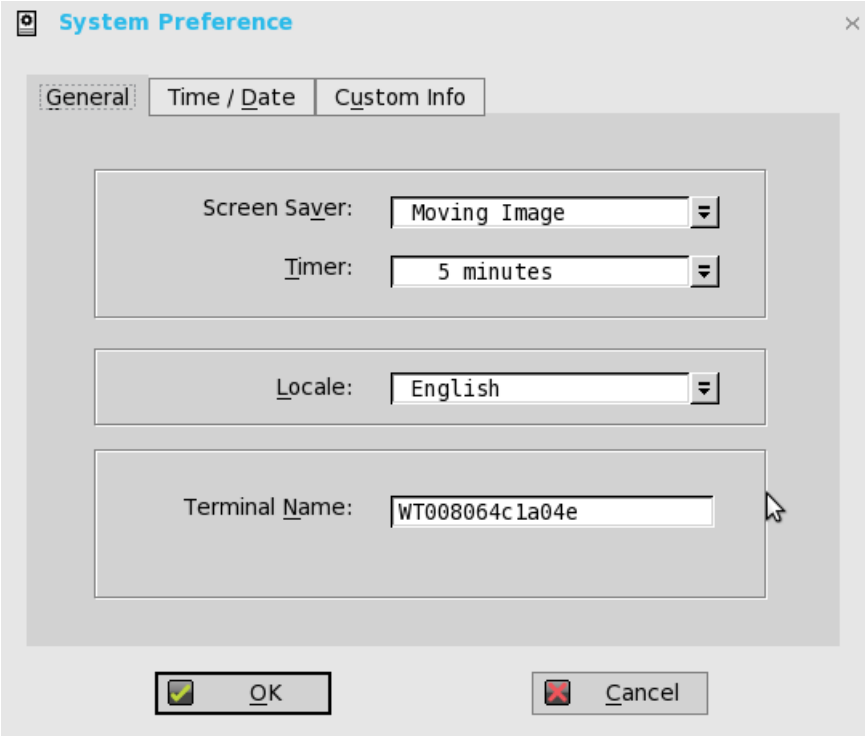


Figure 106. System preference

2 Click the **General** tab, and use the following guidelines:

a **Screen Saver** — Allows you to select the type of screen saver you want. The default is to **Turn Off Screen**.

Other available selections are **Flying Bubbles**, **Moving Image** ,**Showing Pictures** and **Playing Video** which are screen savers with the monitor remaining on.

b **Timer** — Select a time after which the screen saver is to be activated; either **disable**, **1 minute**, **3 minutes**, **5 minutes**, **10 minutes** (default), **15 minutes**, or **30 minutes**.

When the zero client is left idle for the specified idle time, the screen saver is initiated.

c **Locale** — Select a language to be activated for the user login-experience; either **French**, **German**, or default **English**.

> **NOTE: Locale changes the language for the user login-experience screens only displayed during boot-up and login and not the configuration or administrator screens.**

Only the following messages are applicable for French locales:

- Username/Password/Domain
- System Information
- Shut down the system, restart the system, reset the system setting to factory default
- OK, Cancel
- Initiating devices
- Looking up IP address from DHCP, Note: Pressing CTRL-ESC keys cancel out of network check
- Retry DHCP for an IP address
- Waiting for network link....Please verify that network cable is plugged into back of unit
- Check Cable, No Ethernet link
- Leave administrator mode
- Connecting...
- Sign off from account

- Lock Terminal, Unlock Password
- Terminal is locked, Invalid unlock password

d **Terminal Name** — Allows entry of a name for the zero client. The default is a 14-character string composed of the letters WT followed by the zero client Ethernet MAC address.

Some DHCP servers use this value to identify the IP address lease in the DHCP Manager display.

3 Click **OK** to save the settings.

Setting the Time and Date

To configure the Time and Date settings:

1 From the floating bar menu, click the **System Setup** , and then click **System Preferences**.

The **System Preference** dialog box is displayed.

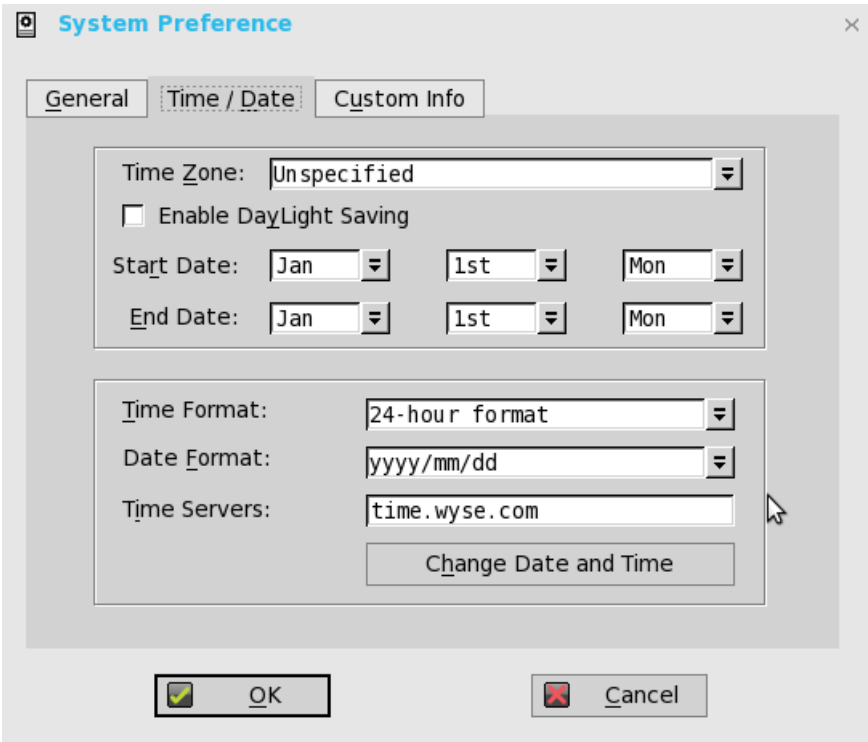


Figure 107. Time and Date

2 Click the **Time/Date** tab and use the following guidelines:

a **Time Zone**— Select a time zone where the zero client operates from the drop-down list. Default is **Unspecified**.

b **Enable Daylight Saving**— Allows you to enable the daylight saving settings. When selected, the **Start Date** and **End Date** boxes must be properly configured to define the daylight saving starting (month/week/day) and ending (month/week/day) periods.

Use the following guidelines to enter the Start Date and End Date:

- **Month**— Specifies the month in the year from **January** through **December**.
- **Week**— Select **1** through **4** for the week in the month. Week last denotes the last week in the month.
- **Day** — Specifies the day of the week from **Monday** through **Sunday**.

c **Time Format** — Allows you to select a 12 or 24-hour time format. Default is **24-hour** format.

d **Date Format** — Allows you to select a yyyy/mm/dd (year/month/day) or dd/mm/yyyy (day/month/year) date format. Default is **yyyy/mm/dd**.

e **Time Servers** — List of IP addresses or host names with optional TCP port number of Time Servers.

Each entry with optional port number is specified as Name-or-IP: port, where: port is optional. If not specified, port 80 is used. Locations can be supplied through user profiles if user profiles are used. The Time Servers provide the zero client time based on the settings of time zone and daylight saving information. If DHCP is used, locations can be supplied through DHCP.

f **Change Date and Time** — Allows you to change date and time for secure environments requiring a solution to outside server access. When connecting to a file server over HTTPS, the proper time must be defined on the zero client for SSL/ certification validation.

Setting the Custom Information

Use the **Custom Info** tab to enter configuration strings used by WDM software. The configuration strings can contain information about the location, user, administrator, and so on.
To configure the Custom Information:

1 From the floating bar menu, click the **System Setup** , and then click **System Preferences**.
The **System preferences** dialog box is displayed.

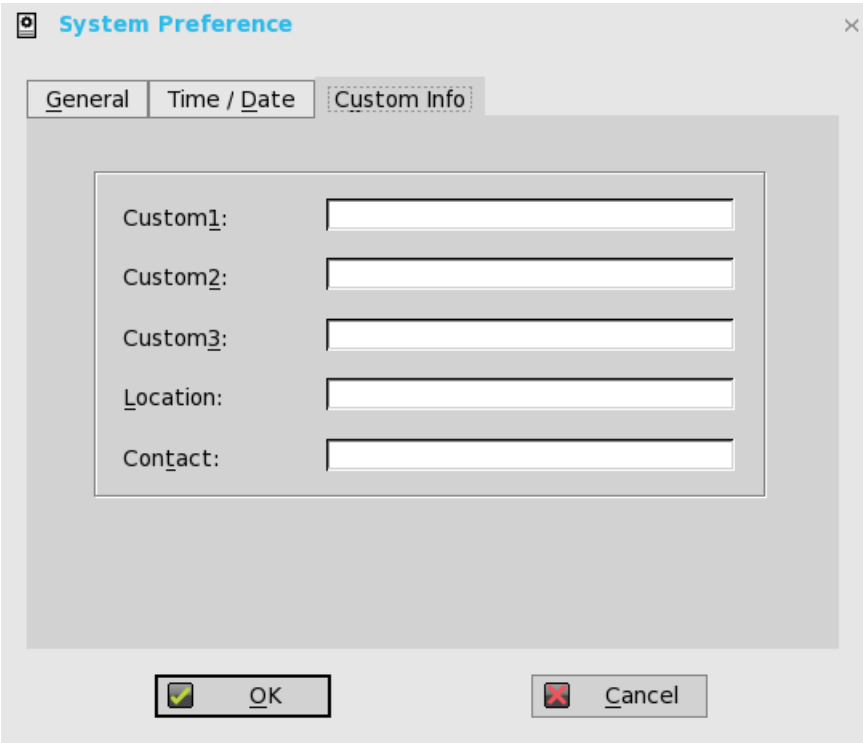


Figure 108. Custom info

2 Click the **Custom Info** tab to enter configuration strings for use by WDM software. The configuration strings can contain information about the location, user, administrator, and so on. Clicking **OK** transfers the custom field information you enter in the dialog box to the Windows registry. The information is then available to the WDM Client Manager. For more information on using Custom Fields and using WDM for remote administration and upgrading zero client software, see the *WDM documentation*.

3 Click **OK** to save the settings.

Configuring the Display Settings

Use the **Display** dialog box to select the resolution and refresh rate for the monitor used with the zero client.

Use the following options to configure the Display Settings:

- Configuring the General Display Settings

Configuring the General Display Settings

To configure the general display settings.

1 From the floating bar menu, click the **System Setup** , and then click **Display**.
The **Display** dialog box is displayed.

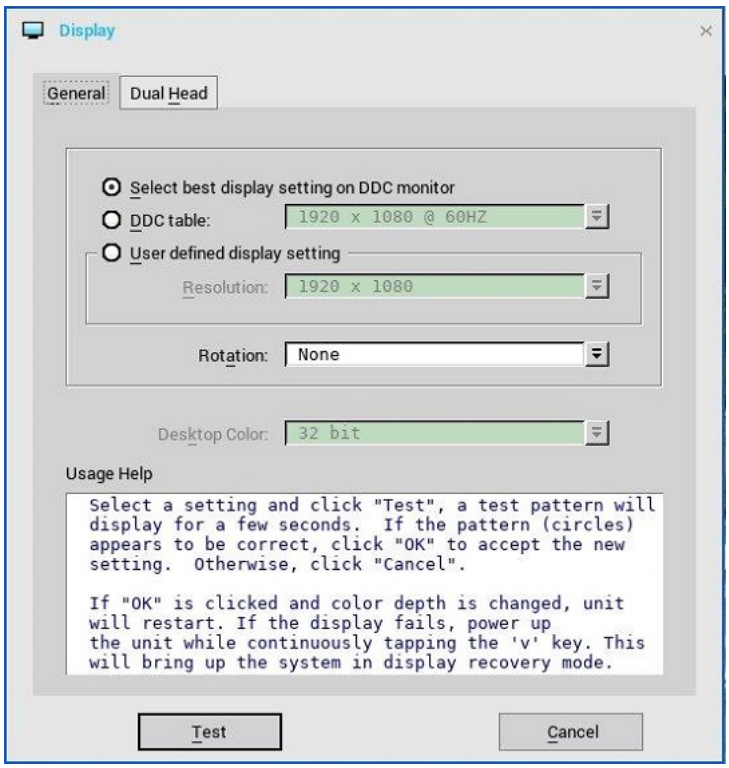


Figure 109. Display—General

2 Click **General** tab and use the following guidelines:

a **Select best display setting on DDC monitor**—If the monitor is VESA DDC2B (Display Data Channel) compatible, selection of this option allows the zero client to automatically select the best resolution and refresh rate.

If your monitor is not DDC compatible, then **Monitor does not support Plug and Play** message is displayed. Click **OK** to acknowledge the message, and remove it from the screen.

b **DDC table**— If the monitor is VESA DDC2B (Display Data Channel) compatible, selection of this option allows you to select the resolution and refresh rate you want from the list.

c **User defined display setting**— Select this option and select the resolution and refresh rate supported by your monitor. All combinations are allowed.

Resolutions include:

640 x 480 (not on Wyse 3020 zero client for Citrix-T00DX)

800 x 600 (not on Wyse 3020 zero client for Citrix-T00DX)

1024 x 768

1152 x 864

1280 x 720

1280 x 768 (not on Wyse 3010 zero client for Citrix-T00X)

1280 x 1024

1360 x 768 (not on Wyse 3010 zero client for Citrix (T00X)/ Wyse 3020 zero client for Citrix (T00DX) class)

1366 x 768

1368 x 768 (not on Wyse 3010 zero client for Citrix (T00X)/ Wyse 3020 zero client for Citrix (T00DX)T00X) class)

1400 x 1050

1440 x 900

1600 x 900

1600 x 1200

1680 x 1050

1920 x 1080

1920 x 1200

1920 x 1440 (R00LX (ThinOS Lite Pro) class only)

2560 x 1080 (Single monitor only; R00LX (ThinOS Lite Pro) class and Wyse 5010 Zero Client for Citrix (D00DX) class only)

2560 x 1440 (Single monitor only; R00LX (ThinOS Lite Pro) class and Wyse 5010 Zero Client for Citrix (D00DX) class only)

2560 x 1600 (Single monitor only; R00LX (ThinOS Lite Pro) class and Wyse 5010 Zero Client for Citrix (D00DX) class only)

3840 x 2160 (Single monitor only; Wyse 5010 Zero Client for Citrix (D00DX) class only)

d **Rotation** —Select a rotation option; either **None**, **Left turn 90 degrees**, or **Right turn 90 degrees**.

e **Desktop Color**— Only **32 bit** is permitted from ThinOS Lite 2.2. This value is selected by default.

NOTE:

f **Usage Help** —This section contains brief instructions for using the **Display** dialog box and running the test. No operator entry can be made in this box.

Make note of the instructions in the area regarding v-key reset usage in case of display failure.

3 Click **OK** to save the settings.

Configuring the Dual Head Display Settings

To Configure the Dual Head Display Settings:

1 From the floating bar menu, click the **System Setup** , and then click **Display**.

The **Display** dialog box is displayed.

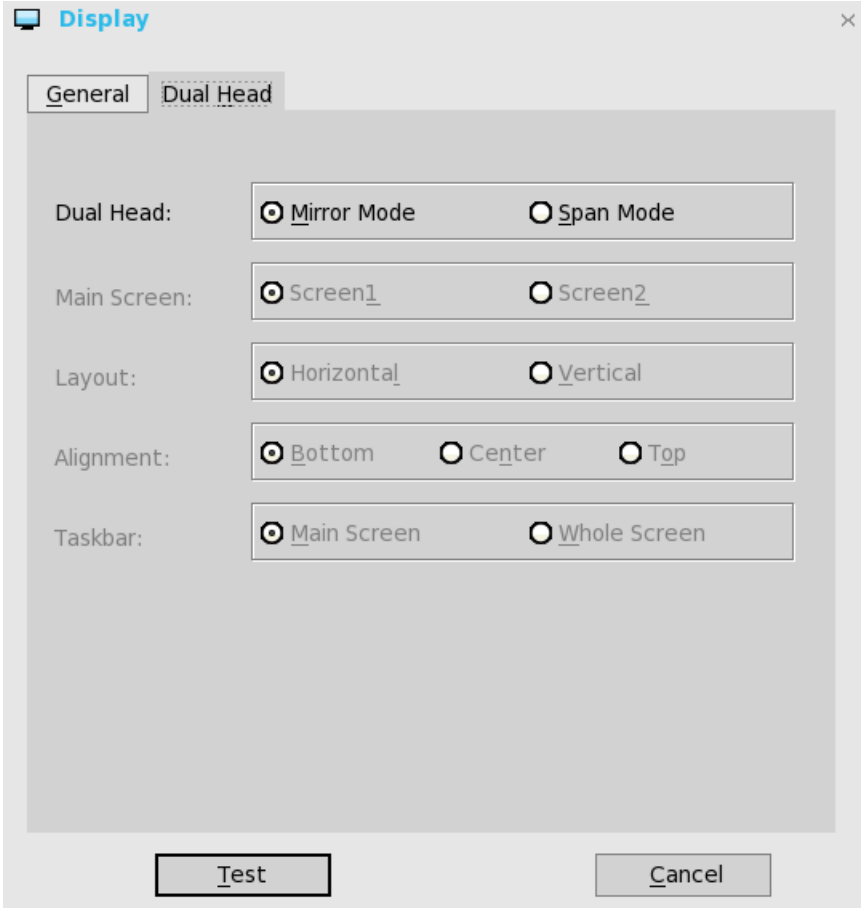


Figure 110. Display—Dual Head

2 Click **Dual Head** tab and use the following guidelines:

Supported Dual Monitor Capable Zero Clients Only.

a **Dual Head**—Select **Mirror Mode** to have the two monitors work in a matching state, or **Span Mode** to have the two monitors work separately second is extended from first.

b **Main Screen**—Select which of the two monitors you want to be the main screen (**Screen1** or **Screen2**). The other screen is extended from the main screen.

The other screen is extended from the main screen. Note that when using a DVI to DVI/VGA splitter with VGA and DVI monitors at the same time, the VGA monitor will be the primary monitor.

c **Layout**—Select how you want the two monitors to be oriented to each other.

Horizontal—Where you point the mouse device between the monitors from the left and right of the screens or **Vertical** where you point the mouse device between the monitors from the top and bottom of the screens.

d **Alignment**—Select how you want the monitors to be aligned **Bottom**, **Center**, or **Top**.

Bottom means screens are bottom-aligned in a horizontal orientation; Center means screens are center-aligned; Top means screens are top-aligned in a horizontal orientation.

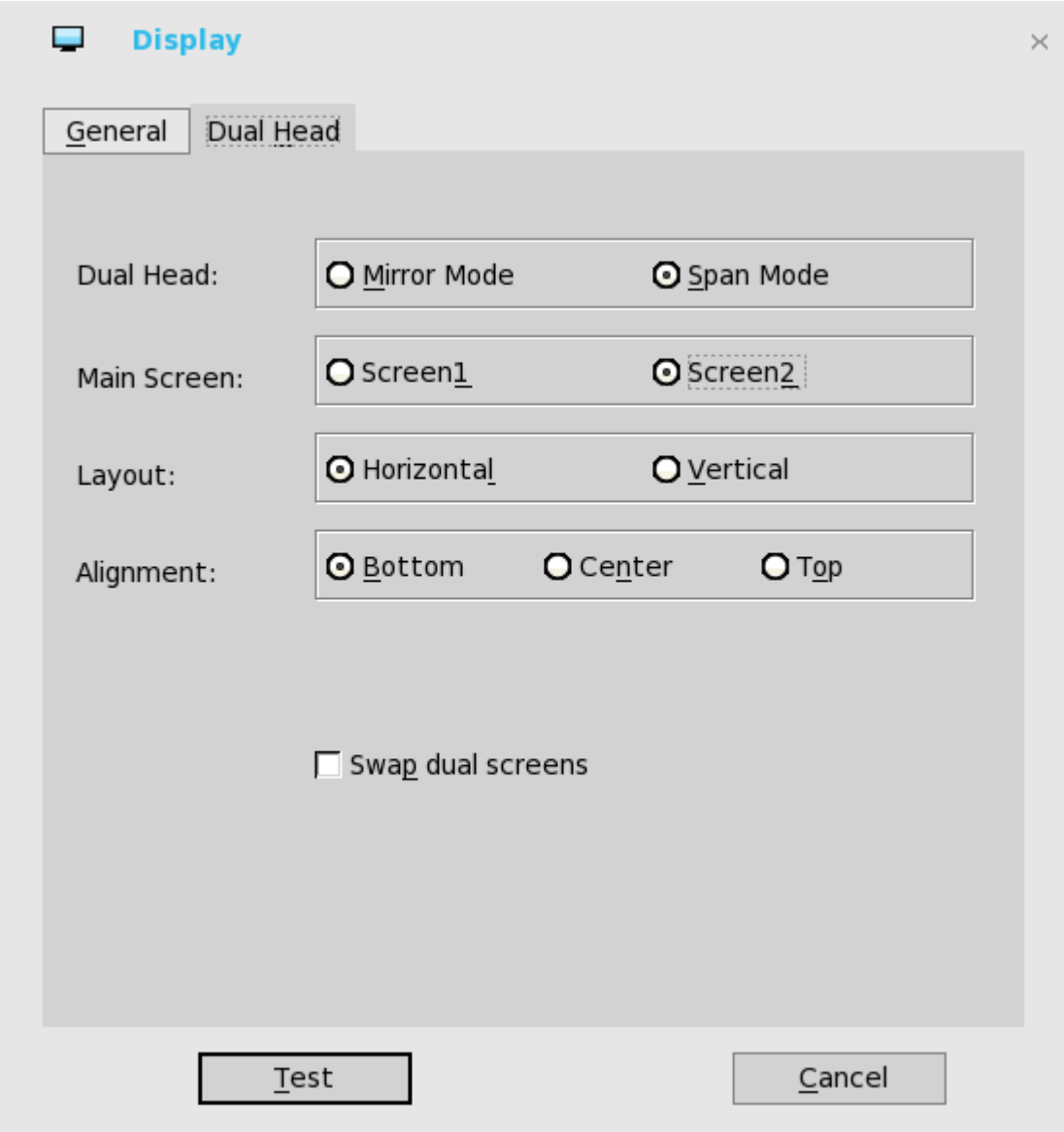


Figure 111. Display—Dual Head

e **Swap dual screens**—When you set Main Screen to Screen2, an additional check box is displayed at the bottom of the tab offering to swap dual screens; If the check box is cleared, the Screen1 is usually the left one or the top one in dual display. When you set Main Screen to Screen2 the main screen will be changed to the right screen or bottom screen; If the check box swap dual screens is selected, you are able to set Main Screen to Screen2 but still have it at the left side or the top side, which is considered more user friendly.

Changing display settings dynamically

From ThinOS Lite 2.4 release, after you change the display settings, the changes will take effect immediately without a system restart.

Single Mode user scenario

Go to **System Setup** > **Display** > **General** and do the following:

1 Change resolution from DDC table or User defined display settings.

2 Change rotation setting from User defined display settings.

When the display settings are changed, the modified settings are applied to the active sessions dynamically. But some of the active sessions disconnect and then reconnect.

Dual head user scenario

Go to **System Setup** > **Display** > **Dual Head** and change the settings.

Go to **System Setup** > **Display** > **General** and do the following:

1 Change resolution from DDC table or User defined display settings.
2 Change rotation setting from User defined display settings.

When the display settings are changed during active sessions, the active sessions do not resize dynamically in the following situations:

- Seamless sessions.
- For dual head mode, including:
  - Change from single mode to dual head.
  - Change from dual head to single mode.
  - Change display setting in dual head mode.

To apply the settings, disconnect the session and reconnect it.

Vertical Synchronization

Vertical Synchronization or V-Sync enables the zero client to synchronize the frame rate of a video with the monitor refresh rate to avoid screen tearing. Screen tearing occurs when the graphic processor delivers display frames more than your monitor can process. As a result, the image appears to be cut in half. Enabling VSync synchronizes the output video of the graphics card to the refresh rate of the monitor.

In ThinOS Lite version 2.6, V-Sync is enabled by default. For information about the supported platforms and limitations, see the *Dell Wyse ThinOS Lite Version 2.6 Release Notes* at www.dell.com/support.

Configuring the Peripherals Settings

The **Peripherals** dialog box enables you to configure the settings the Keyboard, Mouse, Audio, serial, camera, Touch screen and Bluetooth.

- Configuring the Keyboard Settings
- Configuring the Mouse Settings
- Configuring the Audio Settings
- Configuring the Camera Settings
- Configuring the Touch Screen Settings
- Configuring the Bluetooth Settings

NOTE: The Serial Settings tab is applicable only to those clients with serial ports hardware.

Configuring the Keyboard Settings

To configure the Keyboard Settings:

1 From the floating bar Menu, click **System Setup** , and then click **Peripherals**.
The **Peripherals** dialog box is displayed.

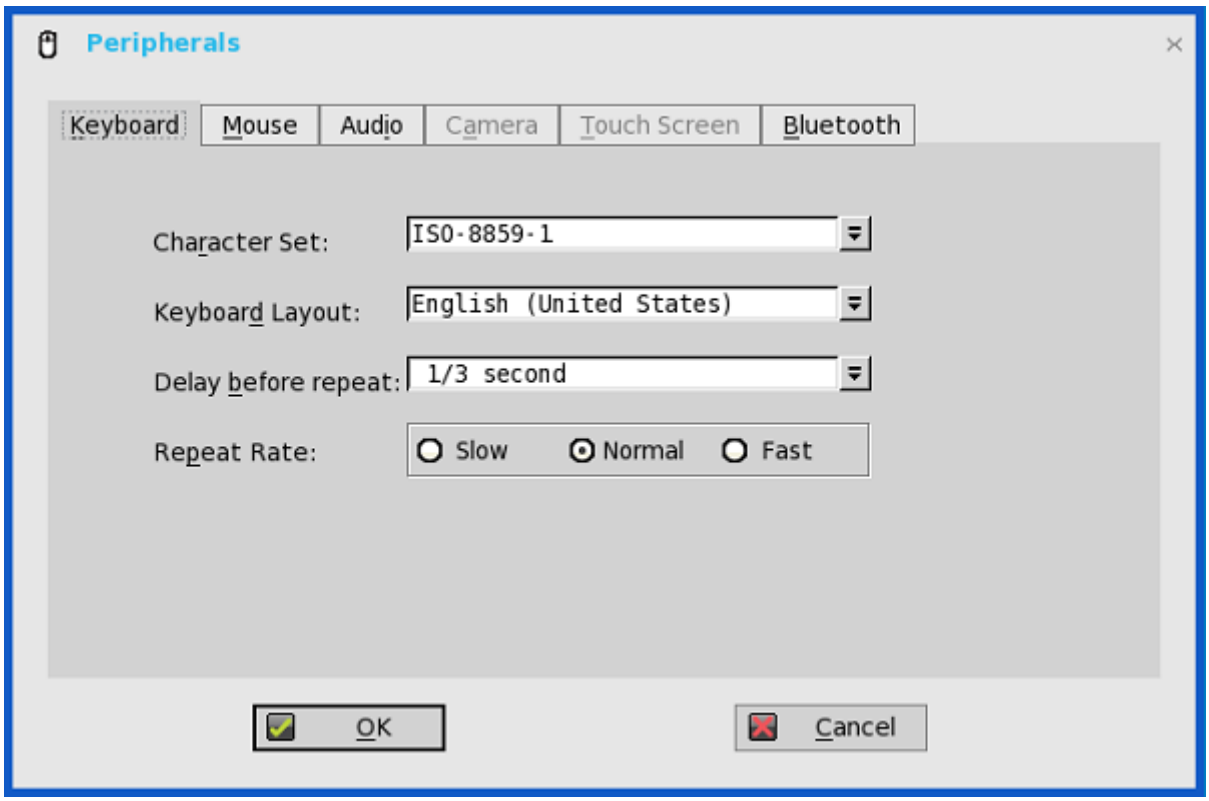


Figure 112. Peripherals—Keyboard

2 Click the **Keyboard** tab and set the Character Set, Keyboard Layout, Delay Before Repeat and Repeat Rate parameters. The following table explains the parameters present on the Peripherals page.

Table 9. Parameters on the Peripheral page

Parameter	Description
Character Set	Specifies the character set. Each character is represented by a number. The ASCII character set, for example, uses the numbers 0 through 127 to represent all English characters and special control characters. European ISO character sets are similar to ASCII, but they contain additional characters for European languages.
Keyboard Layout	Presently the keyboard languages listed in the **Keyboard layout** drop-down list are supported. The default value is **English (United States)**.
Delay Before Repeat	Specifies the repeat parameters for held-down key. Select the Delay before repeat value as either **1/5 second**, **1/4 second**, **1/3 second**, **1/2 second**, **3/4 second**, **1 second**, **2 seconds**, or **No Repeat**. The default is **1/3 second**.
Repeat Rate	Select **Slow**, **Normal**, or **Fast**. The default value is Medium.

3 Click **OK** to save the settings.

Configuring the Mouse Settings

To configure the Mouse Settings:

1 From the floating bar Menu, click the **System Setup** , and then click **Peripherals**.
The **Peripherals** dialog box is displayed.

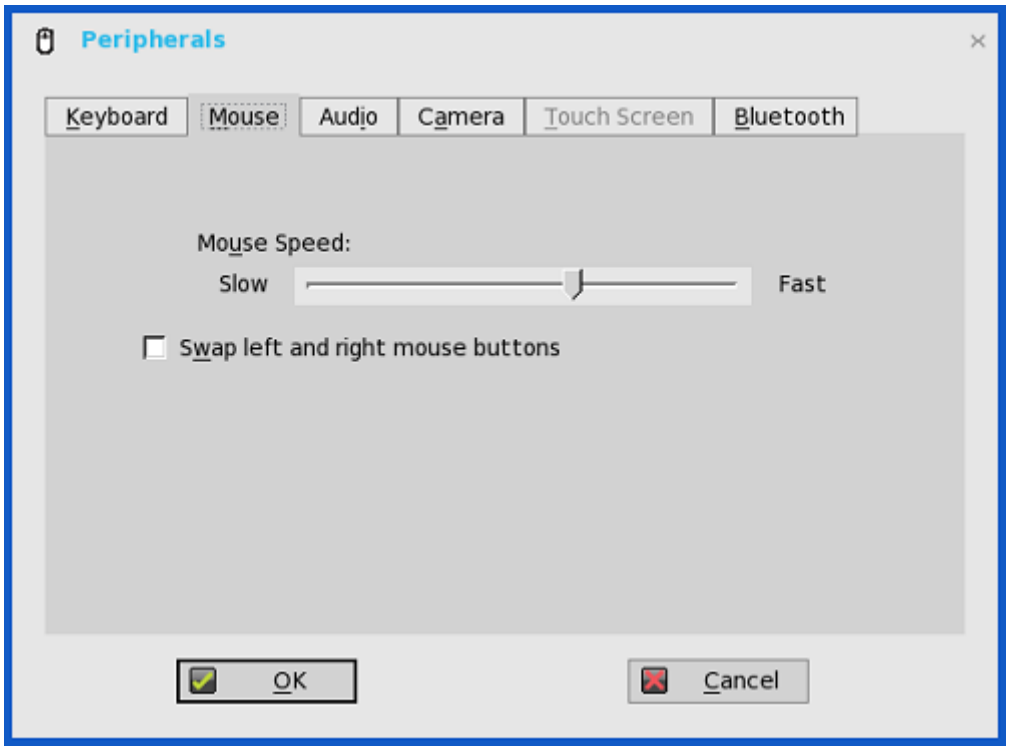


Figure 113. Peripherals—Mouse

2 Click the **Mouse** tab to select the mouse speed and mouse orientation.
3 Select the **Swap left and right mouse buttons** check box to swap mouse buttons for left-handed operations.
4 Select the **Reverse mouse wheel scroll direction** check box to invert the direction of the mouse scroll wheel.
5 Click **OK**.

Configuring the Audio Settings

To configure the Audio settings:

1 From the floating bar Menu, click **System Setup** , and then click **Peripherals**.
The **Peripherals** dialog box is displayed.

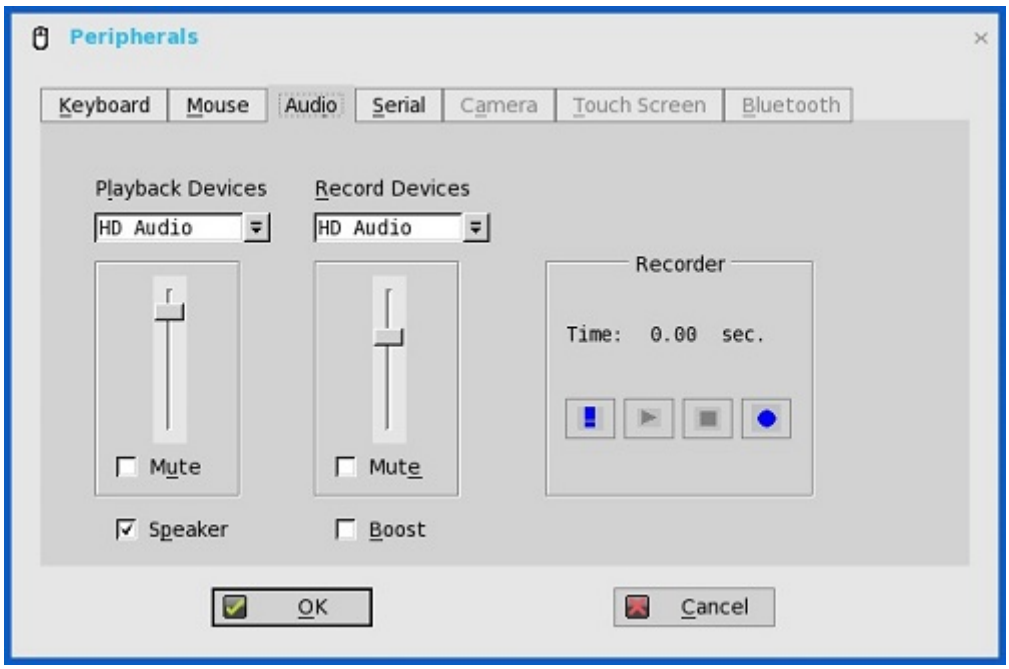


Figure 114. Peripherals—Audio

2 Click the **Audio** tab to select the volume settings for connected devices.

a Click the **Playback Devices** tab to select the type of the audio from the drop-down menu.

- Use **slider** to control the volume settings for the playback devices.
- Select the check box to mute.

b Click the **Recorded Devices** tab to select the type of the record from the drop-down menu.

- Use **slider** to control the volume settings for the record devices.
- Select the check box to mute.

c The **Recorder** tab allows you to do the following tasks:

- Collect information about the speaker and microphone currently being used.
- Examine the performance of the speaker and microphone currently being used.
- Export the recorded audio sample to a USB key for archiving and further analysis.

For example, the connected USB headsets are displayed in the drop-down. Select the HD Audio option for analog earphone use, the **Speaker** check box to enable the internal speaker, and the **Boost** check box for audio enhancement.

d Select the **Speaker** check box to connect the speaker.

e Select the **Boost** check box to boost the connected devices.

f Select the **Enable headset popup** check box if you want the headset popup dialog box to be displayed when you connect an analog headset to the front headset jack. In the headset popup dialog box, select any one of the following audio devices:

- Headset
- Headphone
- Speaker

NOTE: To disable the headset popup dialog box, select the Not show again check box, and click OK. You can also use an INI parameter to enable or disable the headset popup dialog box. For more information about INI parameters, see the latest *Dell Wyse INI Reference Guide*.

Configuring the Camera Settings

Use the **Camera** tab to interface with cameras that are locally connected to the zero client (USB) and supported by a UVC driver. When using the HDX RealTime webcam feature of Citrix Virtual Apps and Desktops, you can control options such as maximum resolution and frames per second (10 FPS is recommended).

By default, the format of USB camera is set to RAW.

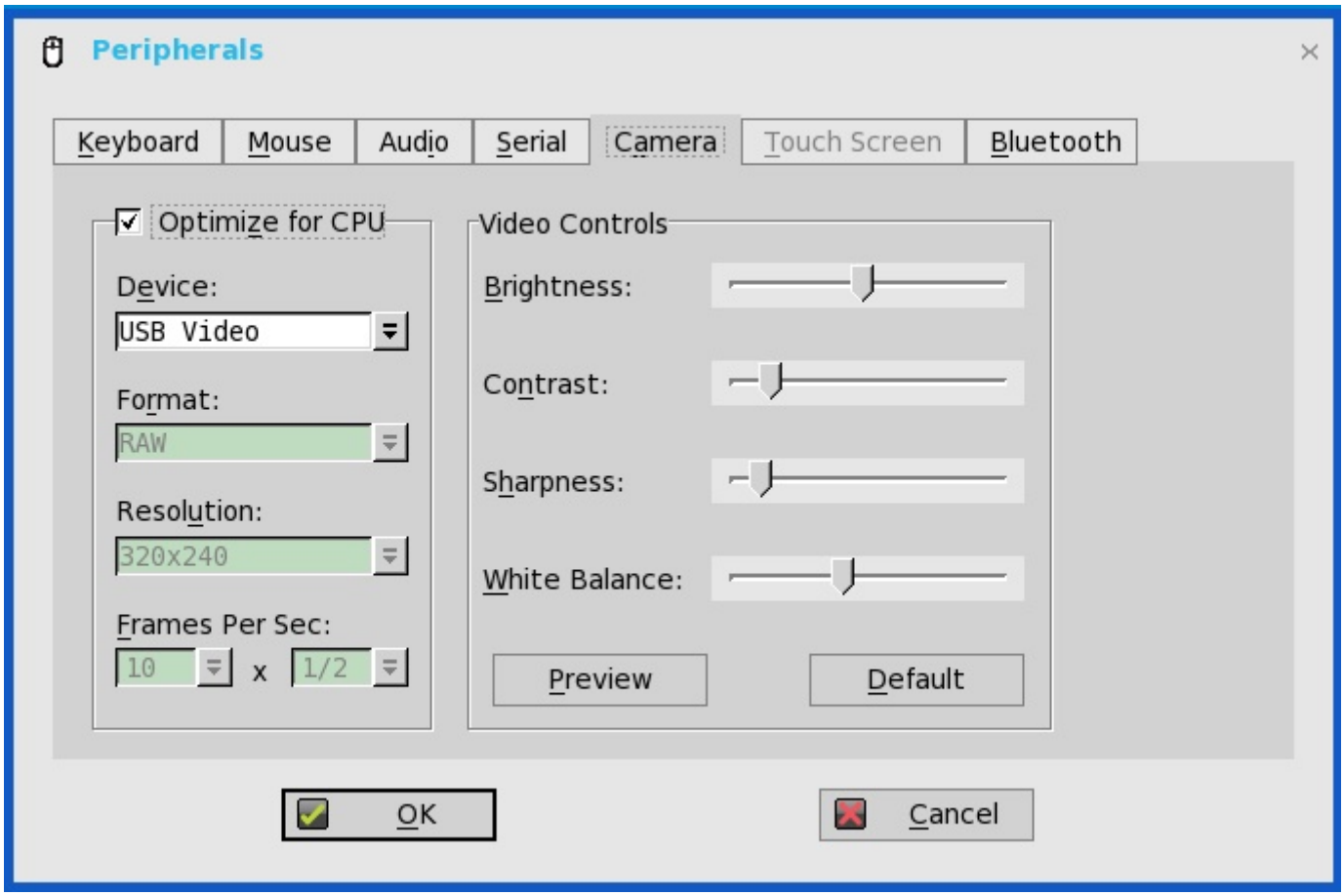


Figure 115. Peripherals—Camera

NOTE:
You can optimize performance and modify the frame rate per second, if the **Optimize for CPU** check box is NOT selected—supported values include 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 – directly from the zero client (if the webcam supports Universal Video Driver).

This feature is CPU intensive and is recommended for high performance products such as Wyse 5010 zero client for Citrix (D00DX).

Configuring the Touch Screen Settings

Use the Touch Screen tab to configure touch screens that are connected to the zero client. The tab is available (not grayed out) when the zero client detects that a touch screen is attached through a USB port or a serial port and the setup or calibration has not been performed. The Touch Setup window prompts you to touch two circles on the screen to make the necessary calibration adjustment. The adjusted calibrated values are saved in the local terminal NVRAM until the system is reset to factory default, or another type of touch monitor is connected.

NOTE: From ThinOS Lite version 2.5, the ELO touch screen does not work in certain scenarios. For more information, see the latest Dell Wyse ThinOS Lite Release Notes.

USB support

USB Hard disk—You should not plug in USB hard disk with 10 or more drives onto ThinOS Lite, or plug in more than 10 USB keys. ThinOS Lite does not accept USB disk with 10 or more drives.

Configuring the Bluetooth Settings

The Bluetooth feature helps you to connect your zero client with Bluetooth enabled devices such as headsets and mouses.

ThinOS supports both Intel wireless chipset 7260 and 7265. For mouse, headset, and keyboard, ThinOS supports both Bluetooth 3.0 and 4.0

Bluetooth 4.0 supports Classic and Bluetooth Low Energy (BLE). However, Bluetooth Alternate MAC/PHY (AMP) is not supported.

To configure the Bluetooth settings:

1 From the floating bar menu, click the **System Setup** , and then click **Peripherals**.
The **Peripherals** dialog box is displayed.

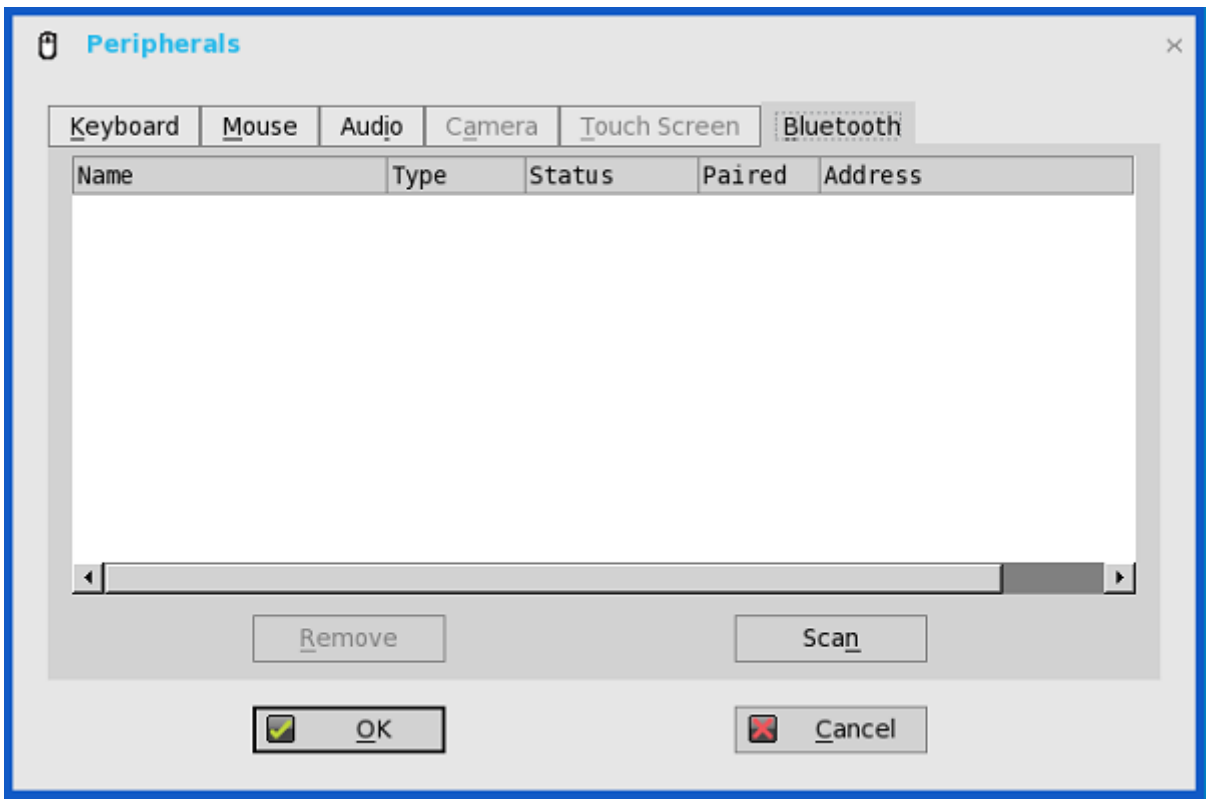


Figure 116. Peripherals—Bluetooth

2 Click **Bluetooth** tab and use the following guidelines:
Bluetooth enabled devices, such as headsets and mouses that are available in the zero Client environment are listed in the **Bluetooth** page. The following attributes are displayed in the list.

- **Name** — Specifies the name of Bluetooth enabled device.
- **Type** — Specifies the type of Bluetooth enabled devices, such as headsets, mouses or keyboards.

Both **Human Interface Devices (HID)** and **Headset** Bluetooth devices are supported from ThinOS Lite 2.2.

- **HID Type**:
  - HID include mouse and keyboard.
  - A maximim of seven HIDs is allowed.
- **Headset** type:
  - Bluetooth Headset is supported in this release.
  - The maximum number of Bluetooth headsets that can be connected is one.

IMPORTANT: Other types of Bluetooth devices are not scanned and supported. Call level audio quality on Headsets is supported. However, multimedia is still not supported.

- **Status**

— The **Bluetooth** page has two columns, namely, **Status** and **Paired**.

Table 10. Bluetooth—Status and Paired

Status	Connected	The Bluetooth device is connected to the ThinOS Lite device. It is ready to be used.
	Connecting	The Bluetooth device is connecting to the ThinOS Lite device.
	Disconnected	The Bluetooth device is not connected to the ThinOS Lite device.
Paired	YES	The Bluetooth device is paired with the ThinOS Lite device.
	NO	The Bluetooth device is not paired with the ThinOS Lite device.

- **Address**: Displays the address of the Bluetooth devices connected to your zero client.

The following are the user scenarios and corresponding Bluetooth statuses displayed on the Bluetooth page.

Table 11. User scenarios

User Scenario	Status
Close/power off device	Disconnected | Paired
Reopen/power on device	Connected | Paired
Disconnect device from ThinOS Lite	Disconnected | Not Paired

a **Connect**— Select a particular Bluetooth enabled device, and click **Connect** to connect the selected device automatically to the zero client. If the Bluetooth device is connected successfully, the status is displayed as **Connected** in the **Bluetooth** window.

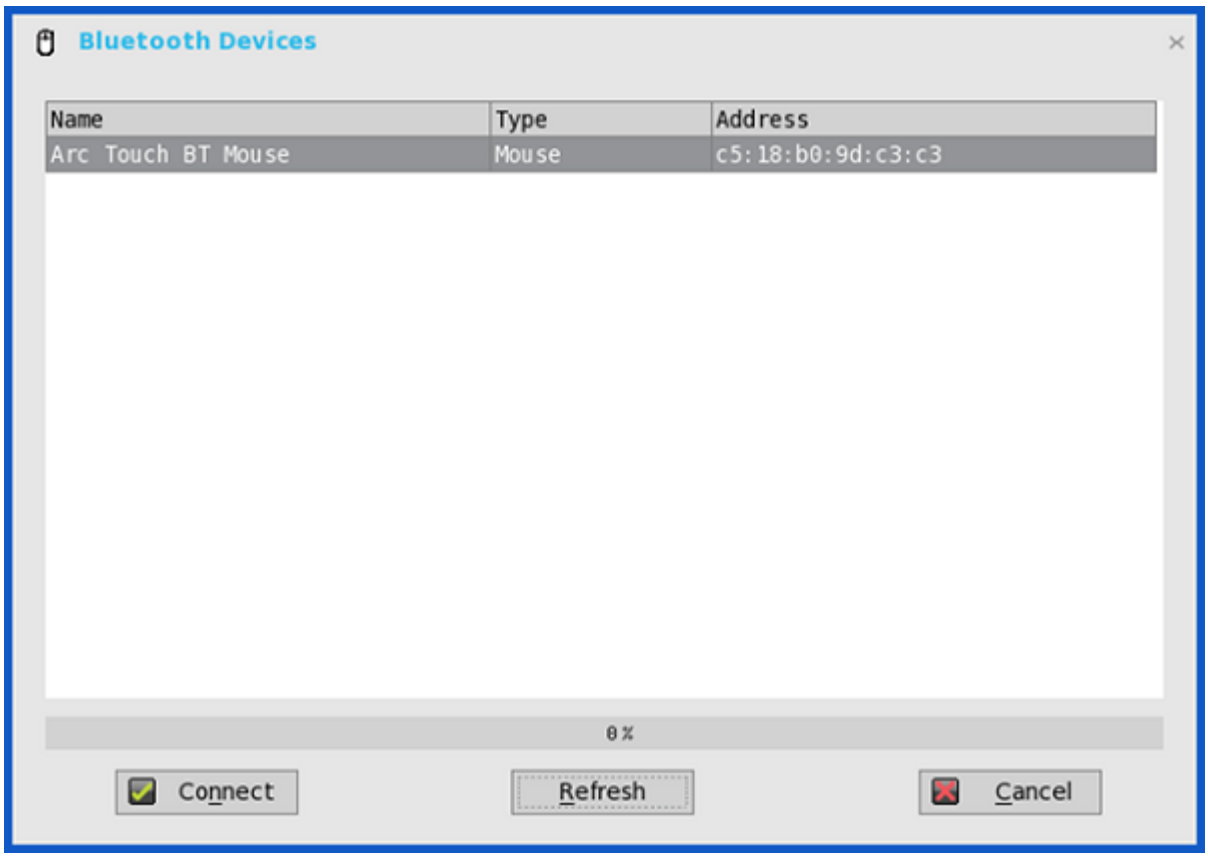


Figure 117. Bluetooth devices

b **Remove**— Select a particular Bluetooth device from ThinOS Lite and click **Remove** to disconnect and remove the device from the list.

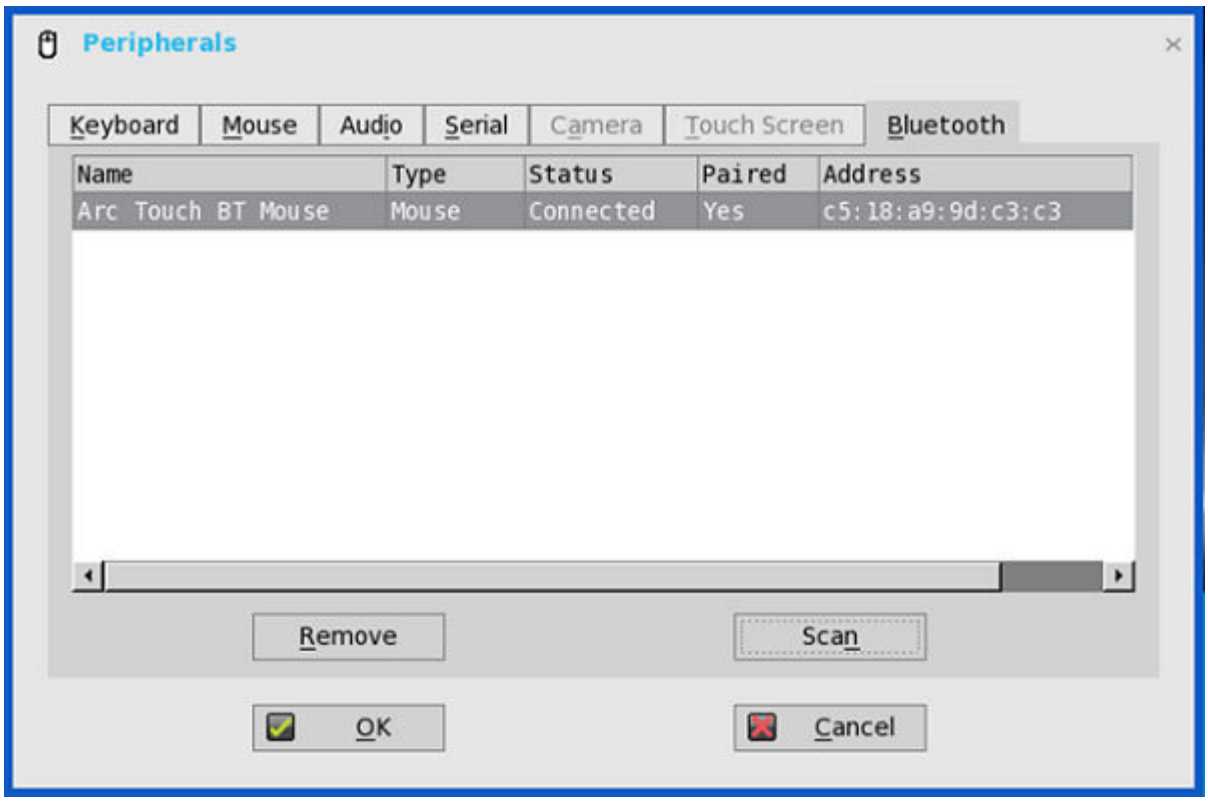


Figure 118. Peripherals—Bluetooth

c **Scan**— All Bluetooth devices enter into **Page Scan** mode. Different Bluetooth devices enter into the Page Scan mode at different instances such as when a specific button is pressed three times or a specific button is pressed and held until the LED turns blue.

> **NOTE:**
> **Auto Connect function**—The Auto Connect function is designed for HID devices.
>
> Prerequisites:
>
> - ThinOS Lite has no HID devices connected such as USB or Bluetooth HIDs.
> - The Bluetooth HID devices are configured as Page Scan mode.
>
> When you start the ThinOS Lite client, the Bluetooth HIDs can connect to ThinOS Lite automatically without scanning or pairing operations. The HID Bluetooth devices automatically reconnect upon ThinOS Lite reboot.
>
> **Reconnect function**—The Reconnect function is designed for HIDs and headsets
>
> When you restart the system with the Bluetooth device already paired and connected, the Bluetooth device automatically reconnects in a few seconds. For example, you can hover the Bluetooth mouse, and then click a few times, for the Bluetooth device to reconnect successfully. The Bluetooth headset reconnects automatically, but might require you to manually close or reopen the device on certain occasions.

To know about the certified devices, refer the latest Dell Wyse ThinOS Lite release notes.

Known Issues of the Bluetooth feature

1 If more than two Bluetooth mouse devices are connected to ThinOS Lite along with two other Bluetooth devices, it may cause low performance of Bluetooth connectivity.

Workaround: Dell recommends using one mouse and one keyboard in ThinOS Lite with Bluetooth connection.

2 The Bluetooth device name displays N/A sometimes.

Workaround: Remove this device from the list and rescan.

3 The Bluetooth device status is not refreshed sometimes when wireless chipset 7260 is shut down.

Workaround: Close the ThinOS Lite Bluetooth window and re-open it. The status is updated.

4 Only supports volume button and mute button on Bluetooth headset.

5 The performance of Bluetooth feature is low during wireless connection.

Configuring the Printer Settings

Use the **Printer Setup** dialog box to configure network printers and local printers that are connected to the zero client. Through its USB ports, a zero client can support multiple printers. If more than one printer is to be used and another port is not available on your zero client and the port that is to be used must be shared with a USB modem converter, connect a USB hub to the port.

Use the following options to configure the Printer Settings:

- Configuring the Ports Settings
- Configuring the LPDs Settings
- Configuring the SMBs Settings
- Using the Printer Setup Options
- Configuring the Citrix UPD Printer
- Using the Help

Configuring the Ports Settings

To configure the Ports Settings

1 From the floating bar Menu, click the **System Setup** , and then click **Printer**.
The **Printer Setup** dialog box is displayed.

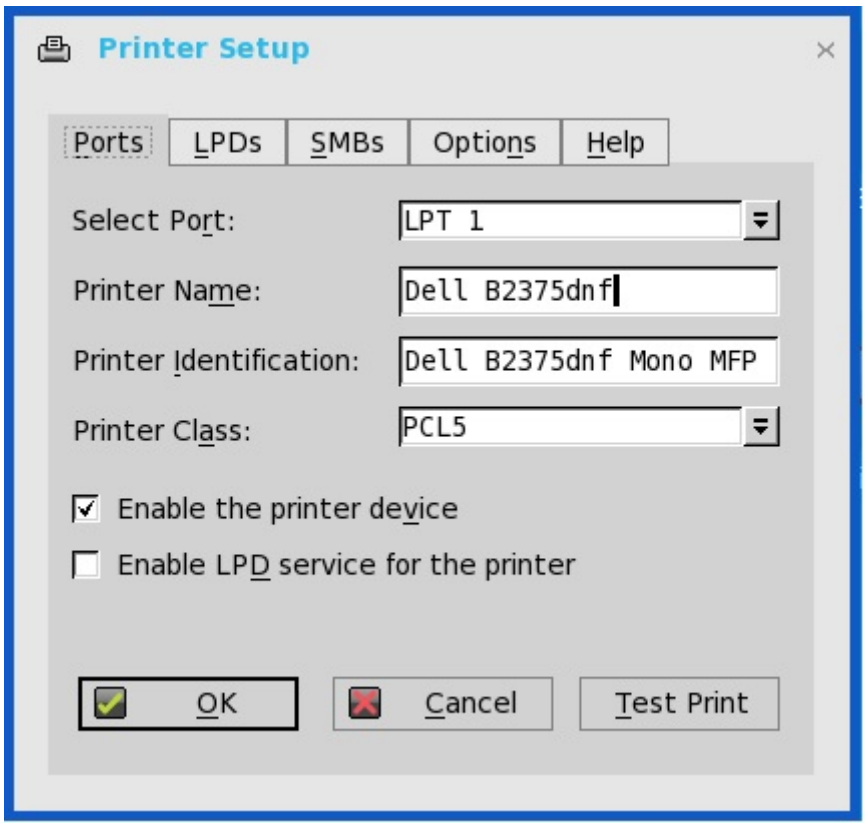


Figure 119. Printer setup—Ports

2 Click the **Ports** tab and use the following guidelines:

a **Select Port**—Select the port you want from the list. **LPT1** or **LPT2** selects the connection to a direct-connected USB printer.

b **Printer Name** — (Required) Enter name you want displayed in your list of printers.

most USB direct-connected printers report/fill in their printer name automatically.

> **NOTE: If Enable LPD service for the printer is selected, the printer name becomes the queue name for other clients using LPR to print to this printer.**

c **Printer Identification** — Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces, most USB direct-connected printers report/fill in their printer identifications automatically.

This entry must be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or **Generic / Text Only** for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

> **NOTE: The maximum characters of printer Identification filed is 31. If your printer driver string is more than 31 characters (Include space). Please create a txt file called "printer.txt", and input content like "HP Color" = "HP Color LaserJet CM1312 MFP PCL6 Class Driver"**

Then add below command line in your wnos.ini file:

printermap=printer.txt

Then you just enter "HP Color" in Printer Identification filed instead of the full driver string.

d **Printer Class**- (**Optional**) Select the printer class from the list **PCL5**, **PS**, or **TXT** or **PCL4.**

e **Enable the printer device** - Must be selected to enable the directly-connected printer. It enables the device so it displays on the remote host.

f **Enable LPD service for the printer** - Select this to make the zero client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network.

NOTE:
If the zero client is to be used as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the client.

3 Click **OK**.

Configuring the LPDs Settings

To configure the LPDs Settings:

1 From the floating bar Menu, click the **System Setup** , and then click **Printer**.
The **Printer Setup** dialog box is displayed.

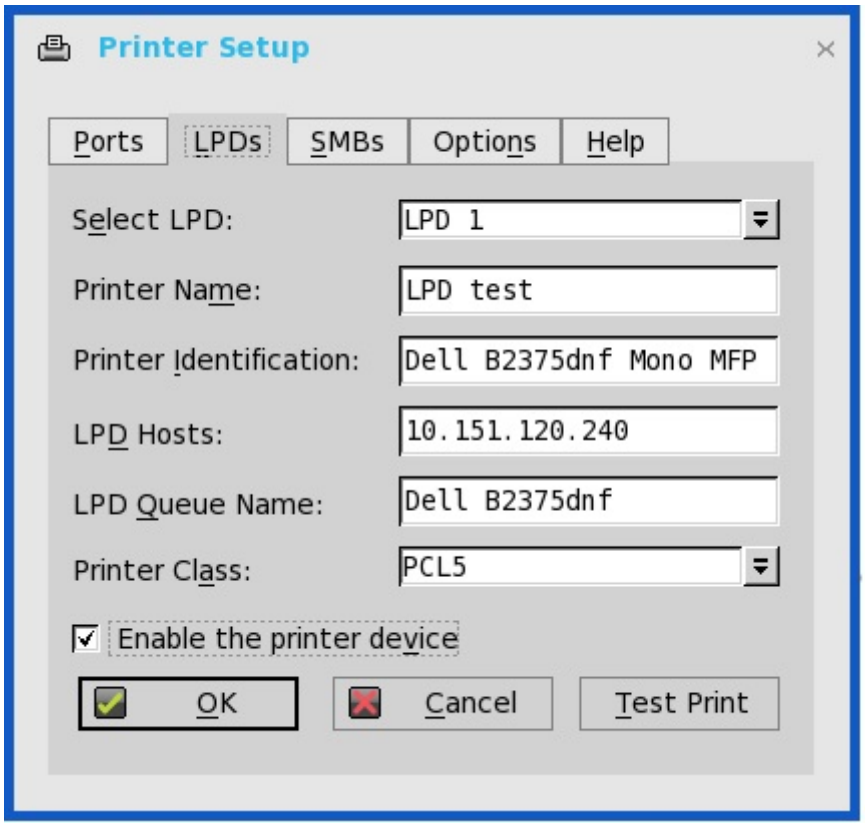


Figure 120. LPDs

2 Click **LPDs** tab and use the following guidelines when printing to a non-Windows network printer:

NOTE: Be sure to check with your vendor that the printer can accept Line Printer Request print requests.

a **Select LPD**—Select the port you want from the list.
b **Printer Name** —(Required) Enter name you want displayed in your list of printers.
c **Printer Identification**—Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.
This name must be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or **Generic / Text** for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).
d **LPD Hosts**—The DNS or WINS name of the server for the network printer. An IP address of the printer on the network can also be entered.

If the printer is attached to another zero client on your network, the entry in the LPD Hosts box is the name or address of that zero client.

e **LPD Queue Name** — An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer to be used.

This name can be different for each vendor. This field is required and must be correct so that the network printer accepts incoming print jobs properly. For example, auto can be used for HP LaserJet 4200n PCL6 as per documentation found on the HP Web site.

NOTE: If the printer is attached to another zero client on your network, the LPD Queue Name must match the content of the Printer Name box on the zero client with the printer attached.

f **Printer Class** — (Optional) Select the printer class from the list.

g **Enable the printer device** — Must be selected to enable the printer. It enables the device so it displays on the remote host.

3 Click **OK** to save the settings.

NOTE: When the LPD printer is mapped to a session and the LPD service host is not accessible, the TCP connection tries to connect to the LPD service host. The timeout period is 60 seconds. During the timeout period, you cannot close the session until the LPD printer initialization error log is displayed.

Configuring the SMBs settings

To configure the SMBs Settings:

1 From the floating bar Menu, click the **System Setup** , and then click **Printer**.

The **Printer Setup** dialog box is displayed.

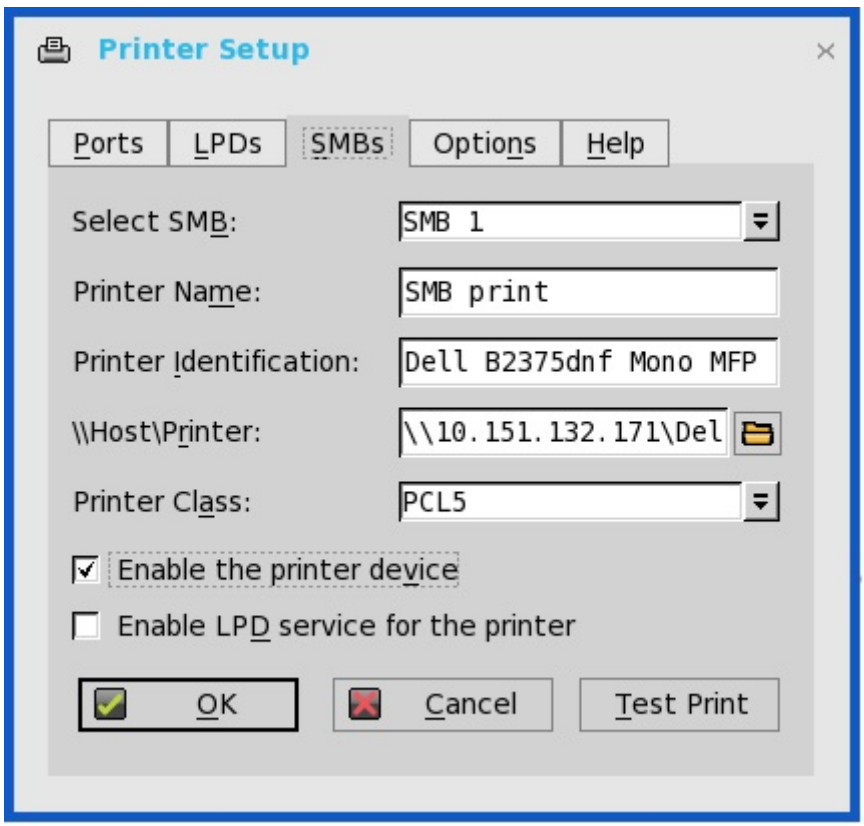


Figure 121. SMBs

2 Click **SMBs** tab and use the following guidelines when printing to a Windows network printer.

a **Select SMB** —Select the SMB you want from the list.

b **Printer Name** —(Required) Enter name you want displayed in your list of printers.

c **Printer Identification**- Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

This name must be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or **Generic / Text** for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

d **\\Host\Printer**—Enter the Host\Printer or use the browse folder icon next to the box to browse your Microsoft Networks and make the printer selection you want from the network printers available (The DNS name or IP address of the Windows print server on the network).

e **Printer Class** — (Optional) Select the printer class from the list.

f **Enable the printer device**— Must be selected to enable the printer. It enables the device so it displays on the remote host.

g **Enable LPD service for the printer**—Select this to make the zero client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network.

If the zero client is to be used as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the zero client.

3 Click **OK**.

Using the Printer Setup Options

To Configure the Printer Setup Options:

1 From the floating bar menu, click the **System Setup** , and then click **Printer Setup**.

The **Printer Setup** dialog box is displayed.

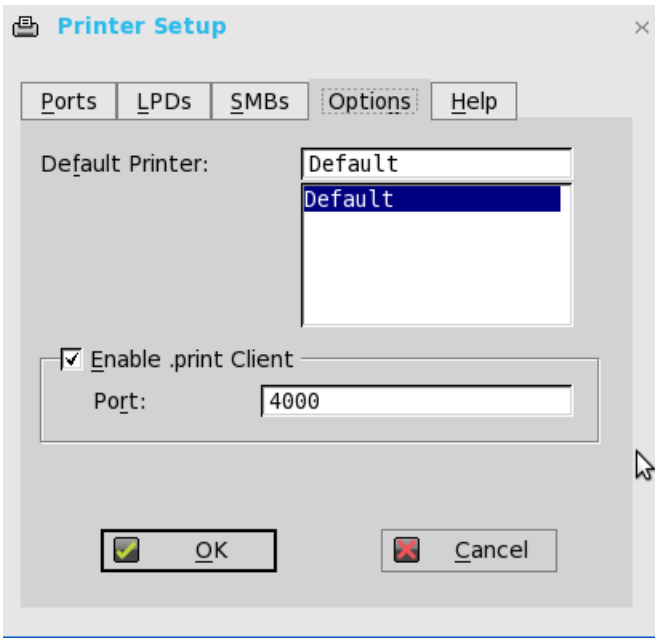


Figure 122. Printer setup—Options

2 Click the **Options** tab and use the following guidelines:

a **Default Printer** —Select the printer you want to be the default printer from your list of available printers.

b **Enable .print Client** and **Port** —If you want to enable .print Client, select **Enable print Client** and then enter the **port**.

Using the Help

When you click the **Help** tab, the following message is displayed in the text box.

Printer Identification is supplied by printer device. Change it to a Window's printer driver name or setup a driver mapping file.

Reset Features

Reset features include:

- Resetting to Factory Defaults Using G-Key Reset
- Resetting to Factory Defaults using Shutdown Reset
- Resetting Display Settings Using V-Key Reset
- Accessing Zero Client BIOS Settings

Resetting to Factory Defaults Using G-Key Reset

High-privileged or Stand-alone users can reset the zero client to factory default settings using the G-key reset feature.

To reset the zero client to factory default settings, restart the zero client and continuously tap the **G** key during the restart process. G-key reset impacts all configuration items, including, but not limited to, both network configuration and connections defined in local NV-RAM.

NOTE: G-key reset is disabled for Low-privileged and Non-privileged users in Lockdown mode.

Resetting to Factory Defaults Using Shutdown Reset

A High-privileged or Stand-alone user can reset the zero client to factory default settings from the **Shutdown** dialog box.
To reset the zero client to Factory Defaults:

1. Click **Shutdown** on the Floating Bar Menu.
   The **Shutdown** dialog box is displayed.
2. After starting your zero client you will see a **Dell logo** for a short period of time.
3. Click **Restart the system** to restart your zero client.
4. Select the **Reset the system setting to factory default** check box to restore your system settings to default factory settings.
5. Click **OK** to save the settings.
   Shutdown reset impacts all configuration items, including, but not limited to network configuration and connections defined in local NV-RAM. However, the terminal name will not be changed.

NOTE:
Shutdown reset is disabled for Low-privileged and Non-privileged users, regardless of lockdown state.

Resetting Display Settings Using V-Key Reset

If the display settings are inappropriate for the particular monitor that is connected, it is possible that the display will not function properly when the zero client restarts. To correct this, power-on the zero client while continuously tapping the **V** key. This will restart the zero client with a default/automatic display resolution.

8

Performing Diagnostics

Diagnostics include:

- System Tools
- Using the Trouble Shooting Options

System Tools

Use the **System Tools** dialog box to view device details, import certificates, view package details, and Global INI/User INI information.

1 From the floating bar menu, click **System Tools**.

The **System Tools** dialog box is displayed.

2 Click the **Devices** tab to display all the locally attached devices, including USB, Serial, and Parallel on applicable platforms. The details about the monitors connected to the zero client are also displayed.

The Device Viewer button was previously found in the **Devices** tab of the **System Information** dialog box.

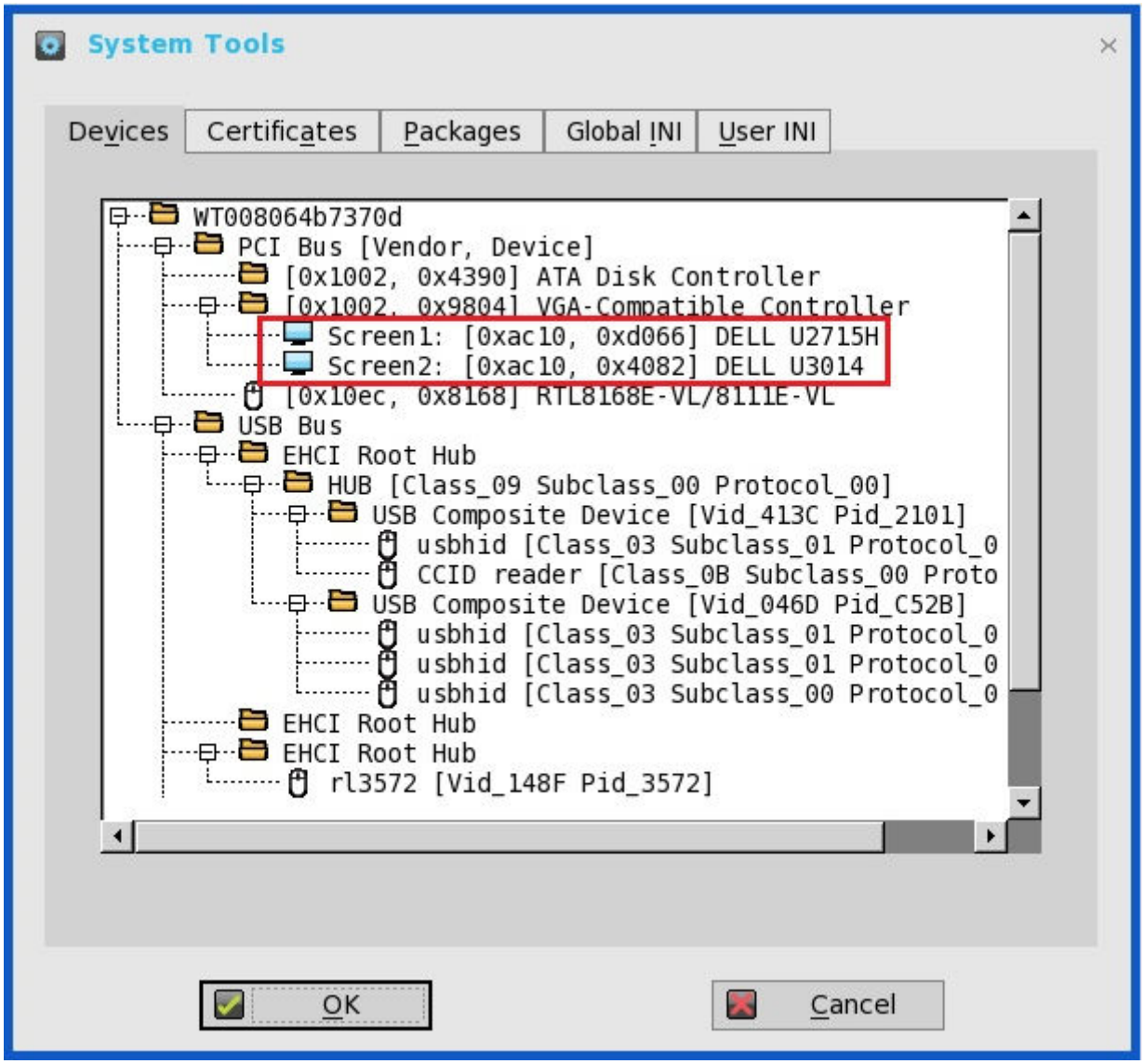


Figure 123. Peripherals—Audio

NOTE: The Mirror File Server tab has been removed from the System Tools dialog box as it can now be viewed in the Devices tab.

3 Click the **Certificates** tab and use the following guidelines:

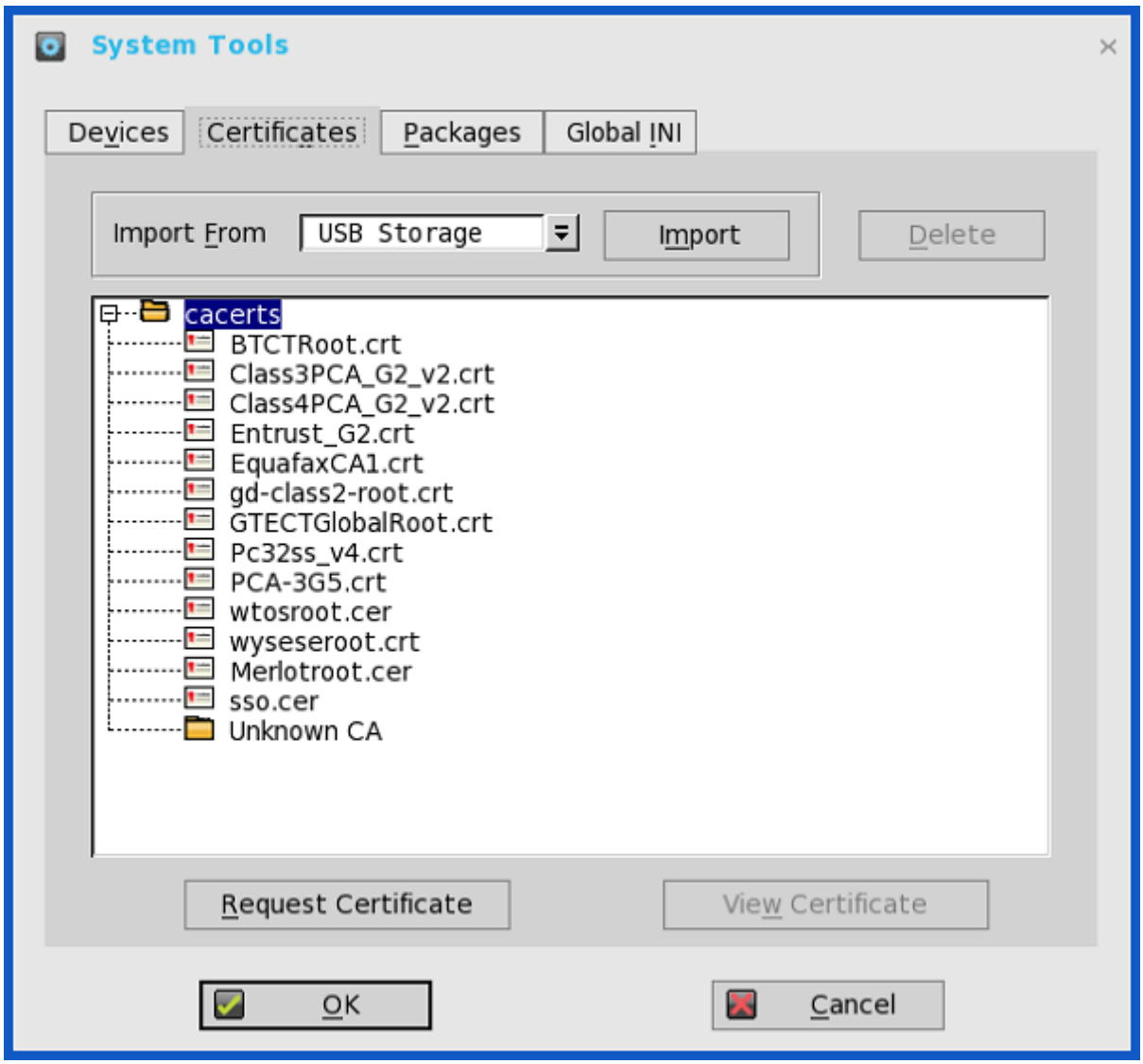


Figure 124. System tools—Certificates

a Import the certificates by selecting either USB Storage or File Server from the drop-down list, and then click **Import** to import the required certificate.

b Click **Delete** to delete the imported certificate.

c Click **View Certificate** to view the imported certificate information such as Version, Validity, and Serial number. You can also view the certificate path and certificate status.

For more information about certificate details, see About Default Certificates.

4 Click the **Packages** tab and use the following guidelines:

ThinOS Lite packages that are installed on zero client are listen in the **Packages** tab.

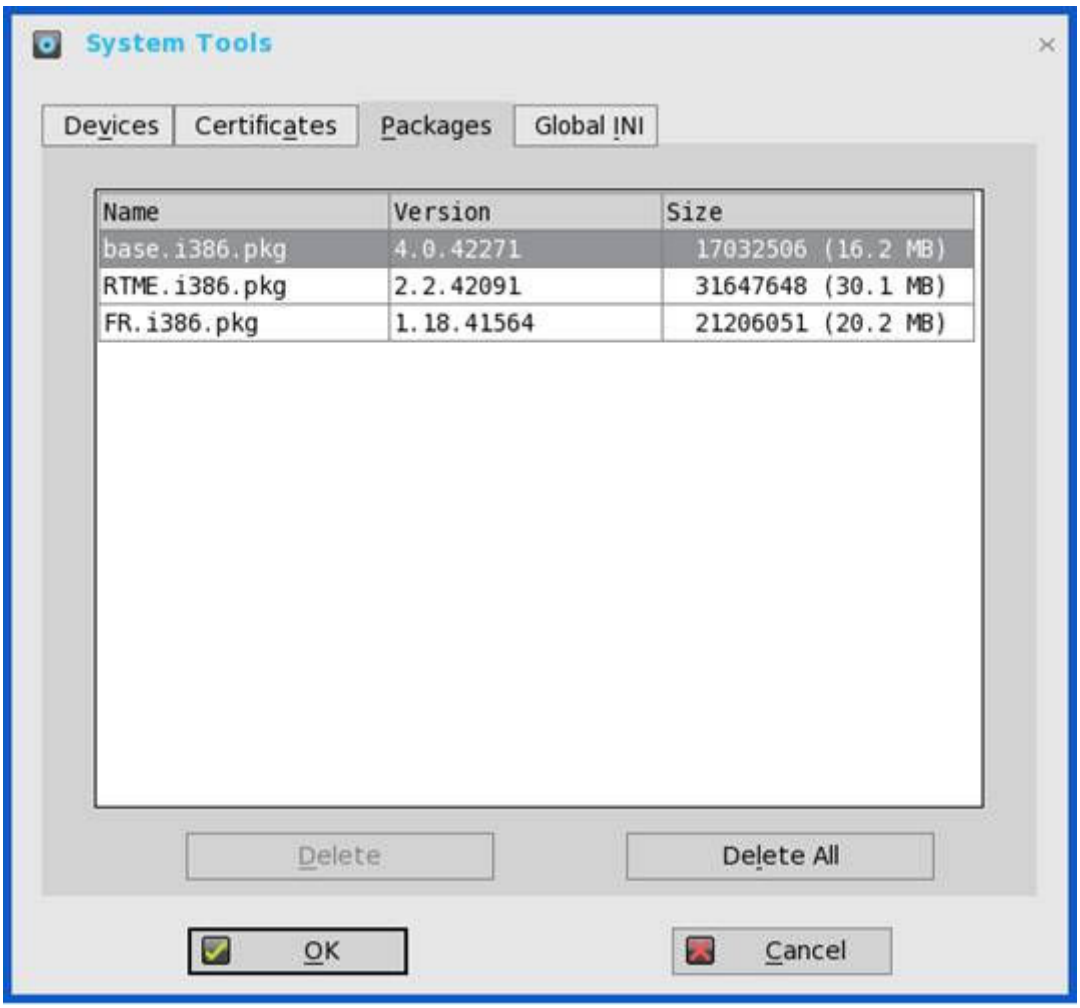


Figure 125. System tools—Packages

a Click the **Delete** button to delete the selected package.
b Click the **Delete all** button to delete all the packages.

The following packages are available in the **package tab**:

- `base.i386.pkg`
- `FR.i386.pkg`
- `RTME.i386.pkg package`

For information about updating the packages, see Firmware upgrade.

You cannot delete the base package separately. If u click**Delete All**, all packages are deleted including the base package.

The `base.i386.pkg` is mandatory for all zeo clients. This package is integrated into the ThinOS Lite firmware image. Other packages are optional. Installing the latest ThinOS Lite firmware image will automatically install the latest version of this packages on zero client. You cannot manually install or upgrade this embedded package. However, the package version detail is displayed in the **Packages** tab in System Tools for engineering information purpose only.

NOTE: When you install the packages or restart the client, the zero client verifies the version of the installed packages. If you have not installed the latest package version, the details about the current package version and the recommended package version are displayed in the Event Log tab. In every ThinOS Lite release, the packages may be updated to the latest version. For information about the latest package version, see the latest *Dell Wyse ThinOS Lite release notes*.

5 Click the **Global INI** tab to use to view xen.ini information.

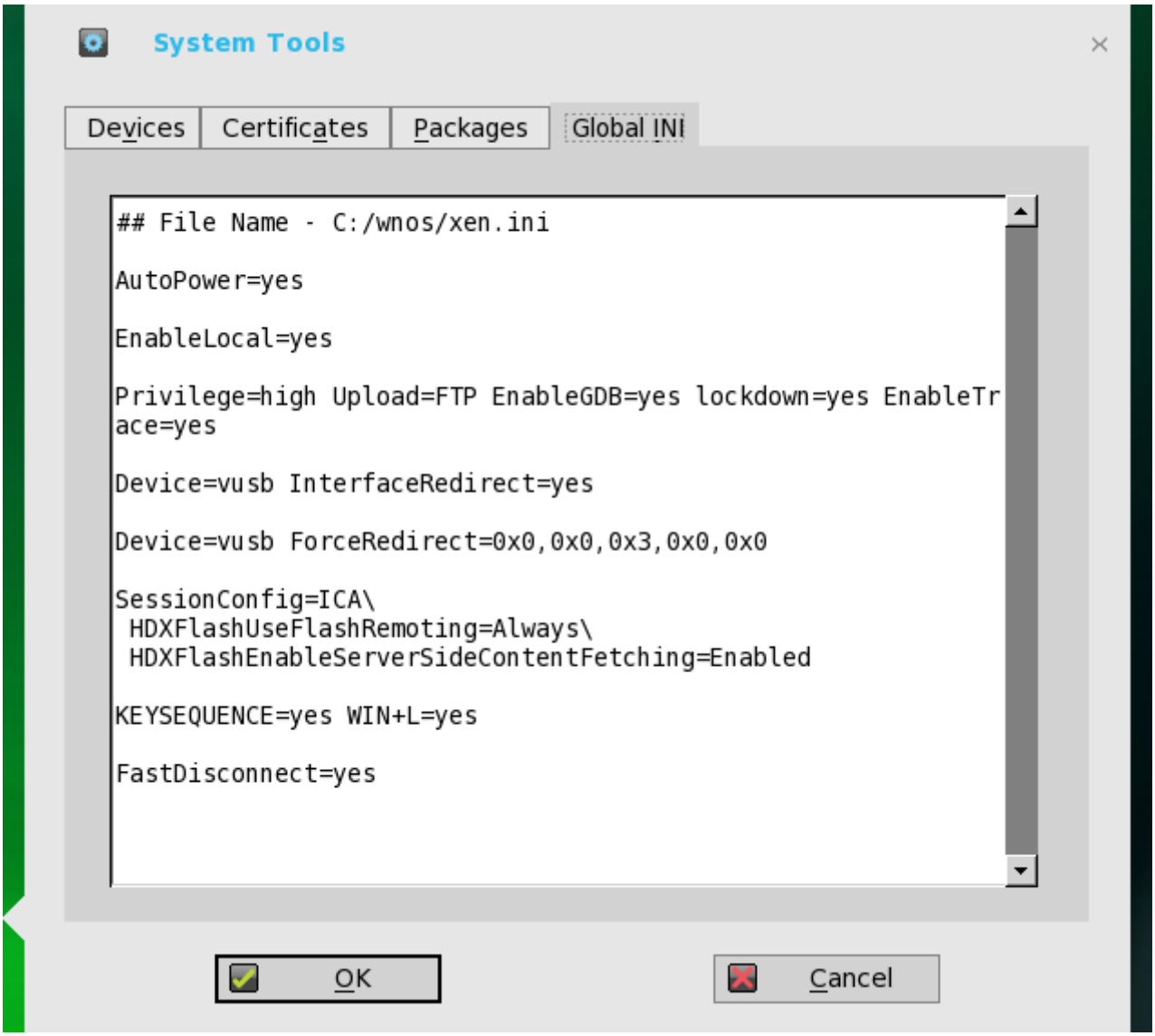


Figure 126. System tools—Global INI

6 Click the **WDM INI** to view the received WCM configurations.

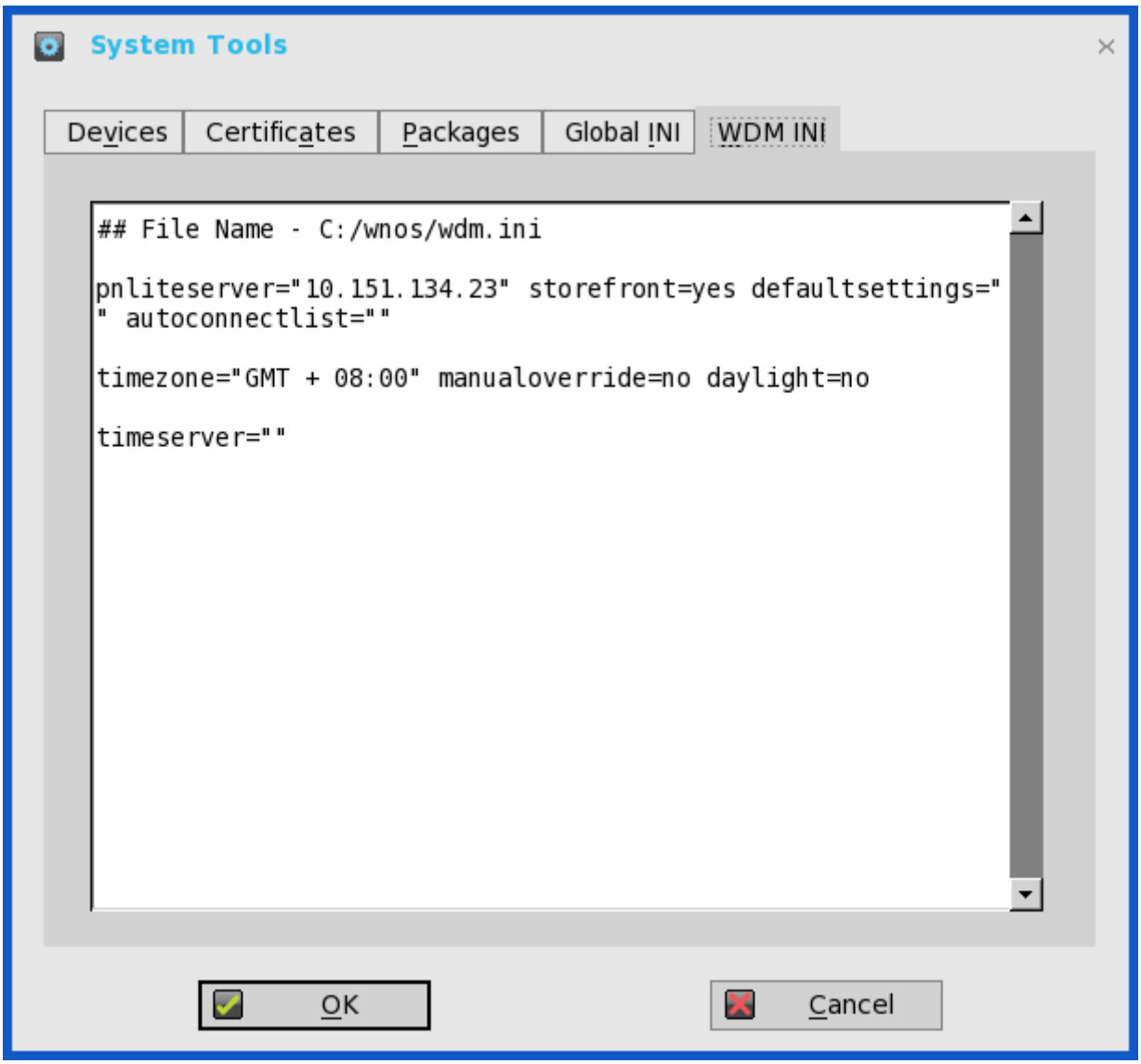


Figure 127. System tools—WDM INI

WCM function is supported from WDM for comprehensive client configuration. Without configuration from server, the client loads the cached settings (wdm.ini), if available.

Limitation

To upgrade or downgrade firmware/image through WCM, you are required to enable WDM file server function by selecting the **WTOS INI path upon checkin (FTP/HTTPS/HTTP/CIFS**) check box in the WTOS preferences in the WDM configuration manager.

User Scenario

a Create or edit client configurations from WCM (JSON).

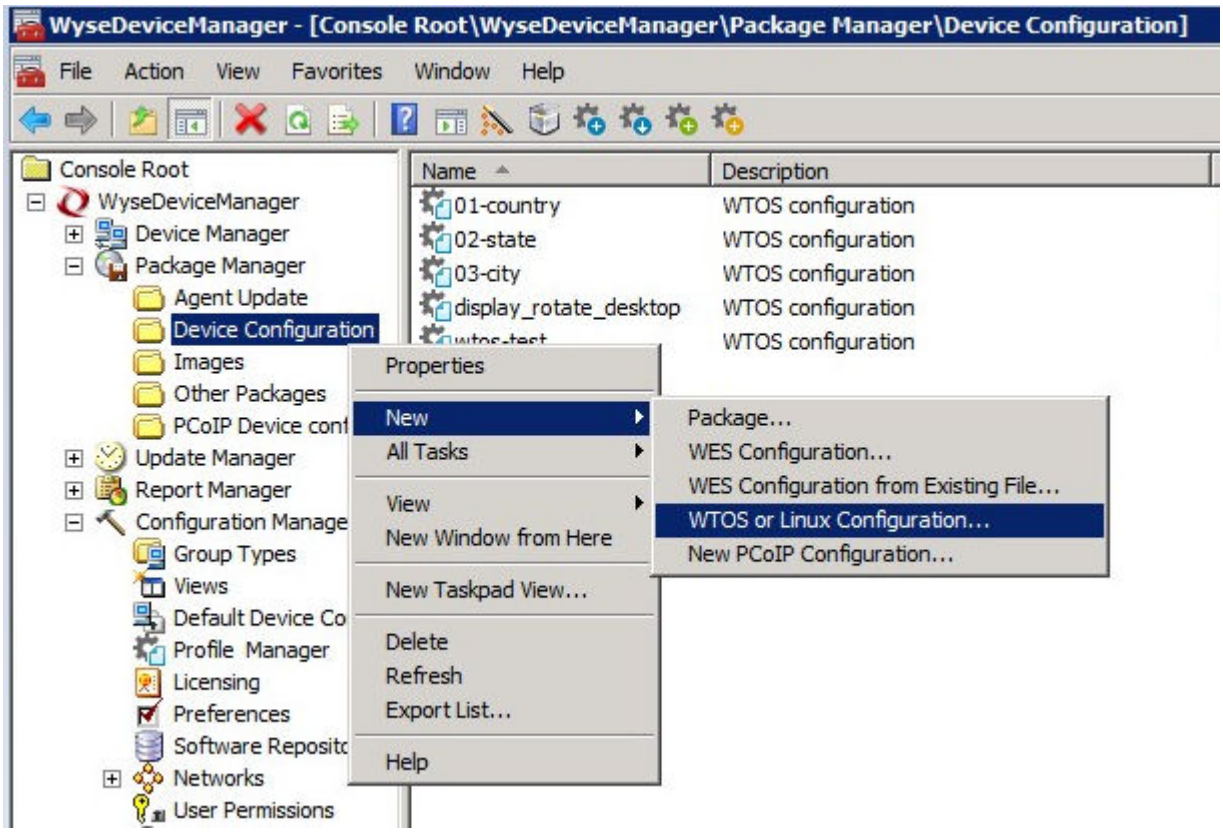


Figure 128. ThinOS or Linux configuration

b Select the target devices, and publish configuration settings through the **Package Distribution Wizard**.

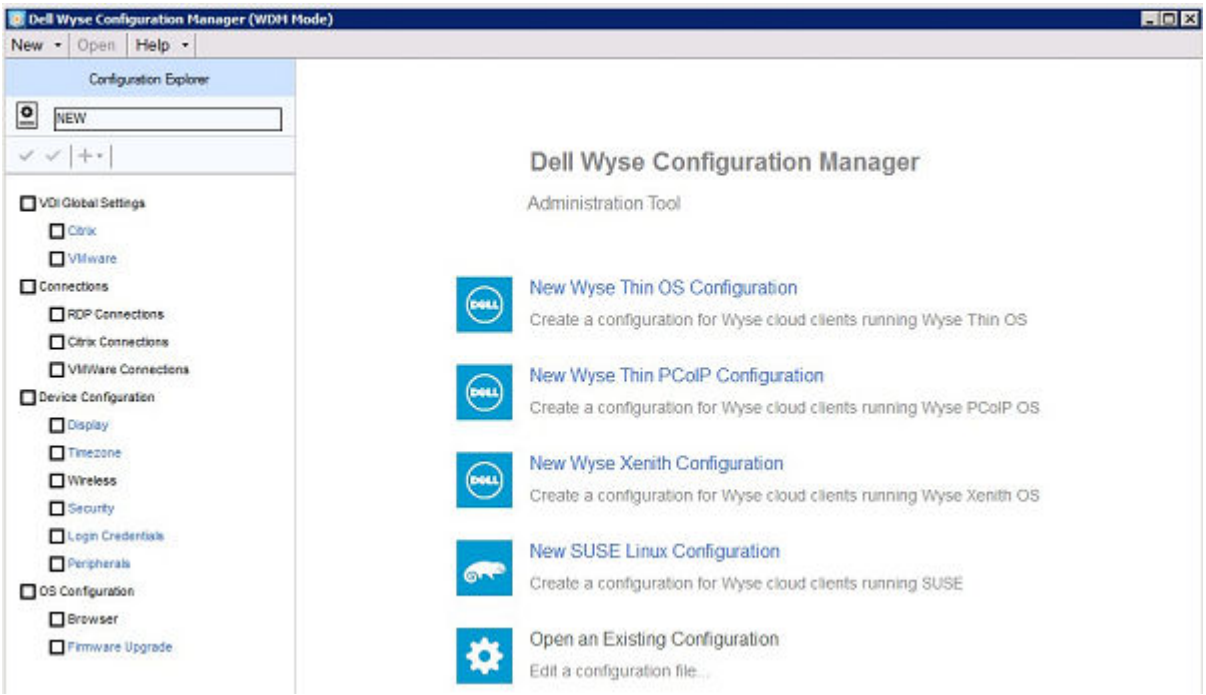


Figure 129. Dell Wyse Configuration Manager

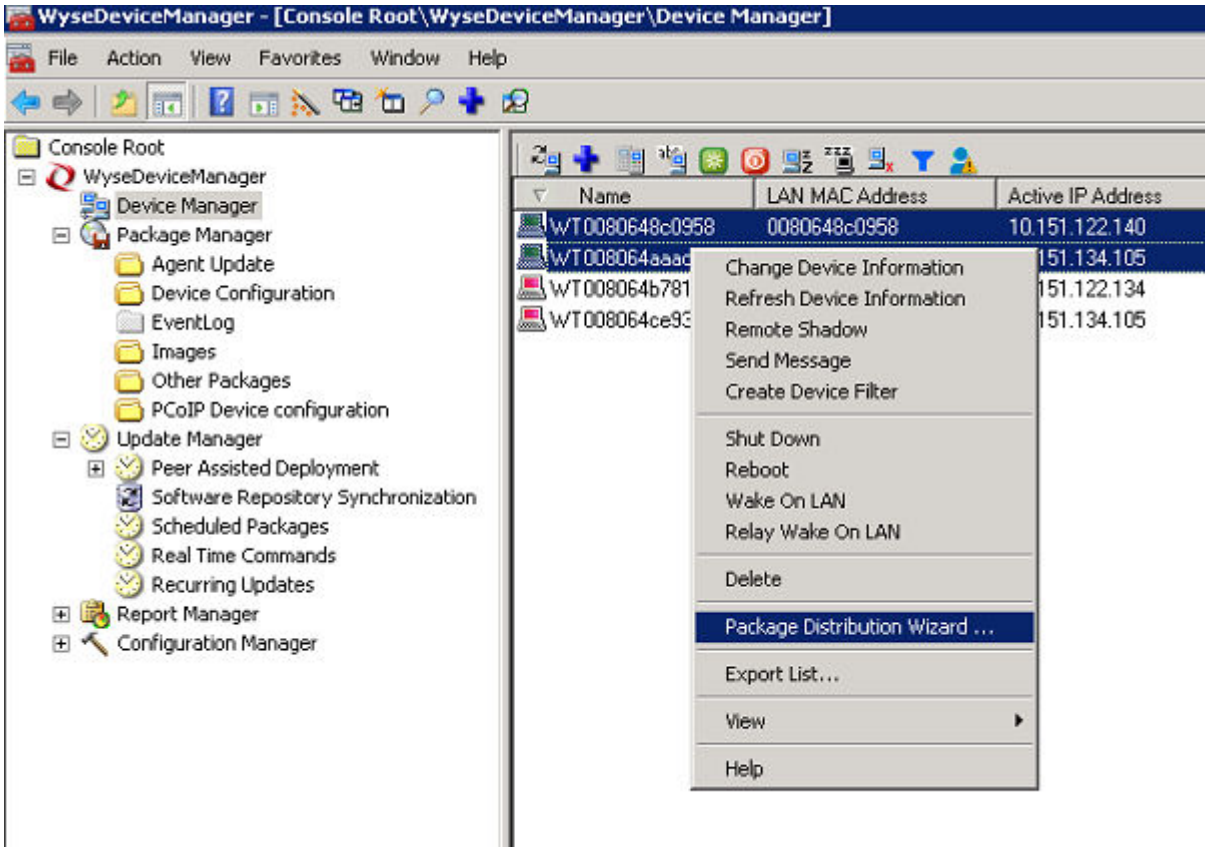


Figure 130. Package Distribution Wizard

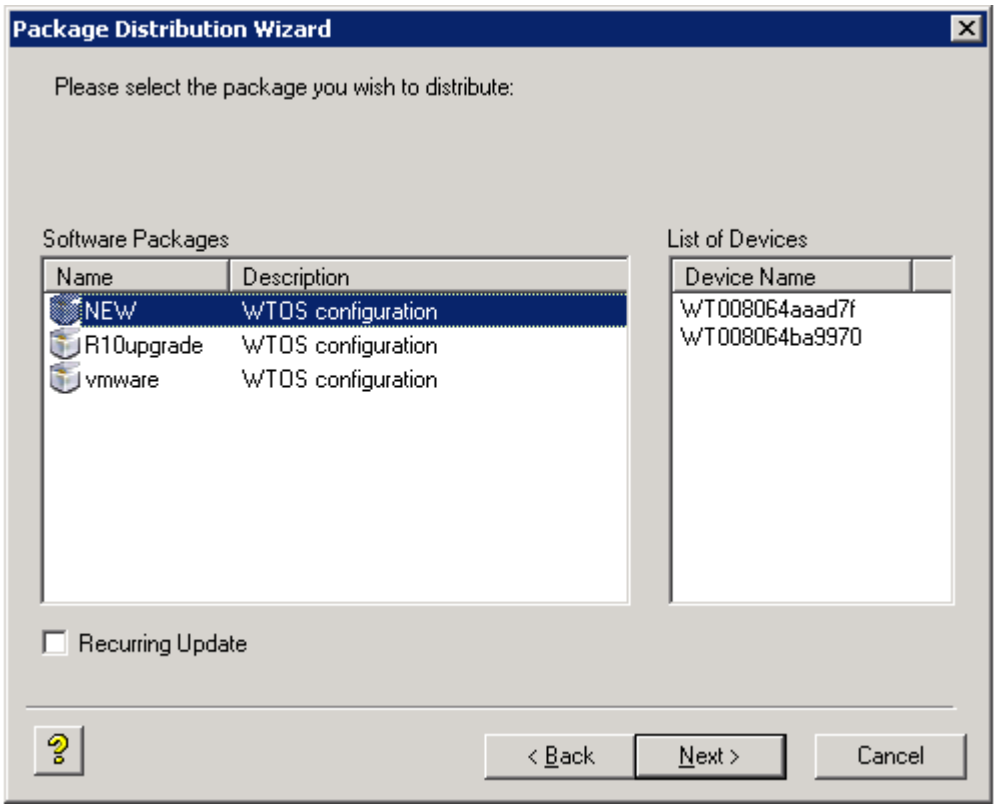


Figure 131. Package Distribution Wizard

For more information about WDM Package Manager and Profile Manager, refer to the *WDM Admin Guide*.

7 Click **OK** to save the settings.

Simplified Certificate Enrollment Protocol—SCEP

Simplified Certificate Enrollment Protocol (SCEP) was designed to be used in a closed network where all end-points are trusted. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner. Within an enterprise domain, it enables network devices that do not run with domain credentials to enroll for certificates from a Certification Authority (CA).

At the end of the transactions defined in this protocol, the network device will have a private key and associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

ThinOS Lite is treated as a network device. The functionalities of ThinOS Lite SCEP include manual certificate request, automatic certificate request, and automatic renewal of certificate.

Requesting certificate manually

To request the certificate manually, do the following:

1 Go to **System Tools** > **Certificates** > **Request Certificate**.
The **Request Certificate** dialog box is displayed.

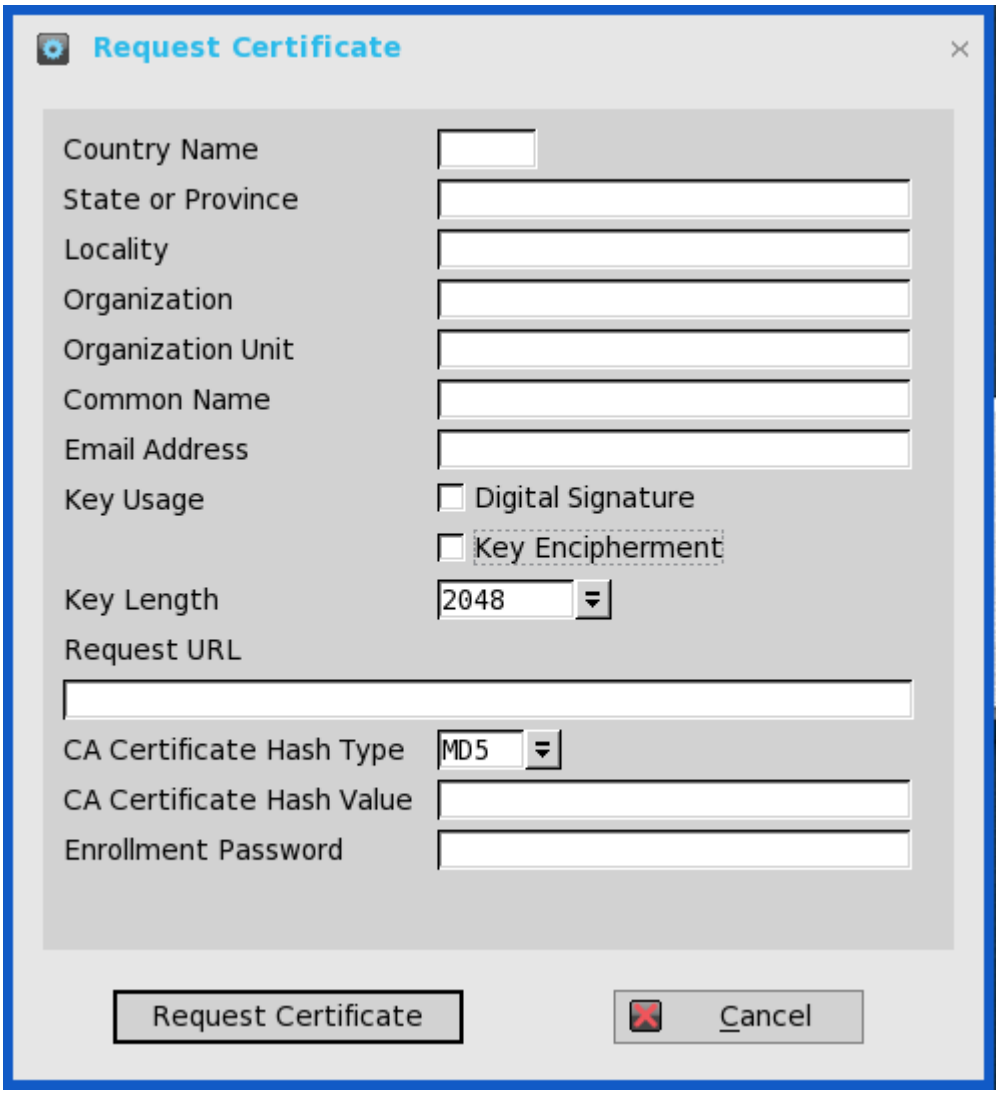


Figure 132. Request Certificate

2 Enter the appropriate values in the **Request Certificate** dialog box, and then click the **Request Certificate** button.

The certificate request is sent to the server and the client receives the response from server and installs both CA certificate and client certificate.

3 Click **Ok** to save the changes.

NOTE:

- The CA Certificate Hash type currently supports MD5, SHA1, and SHA256.
- The request server URL can be an HTTP or HTTPs link. You can add the protocol prefix before the URL.

Requesting certificate automatically

Use INI parameters to automate the **request and renew** certificate process. Related INI parameters are of global scope and should be used with INI parameter `ScepAutoEnroll`.

For more information about using the INI parameters, see INI Parameters

About Default Certificates

Default certificates embedded in the ThinOS are displayed in the **Certificate** dialog box. To view the default certificate, set ThinOS to factory default, and on the desktop click **System Settings** > **System Tools** > **Certificates**. The following default certificates are displayed in the **cacerts** folder, in an expandable tree structure format:

- BTCTRoot.crt
- Class3PA_G2_v2.crt
- Class4PA_G2_v2.crt
- Entrust_G2.crt
- EquafaxCA1.crt
- gd-class2–root.crt
- GTECTGlobalRoot.crt
- Pc32ss_v4.crt
- PCA-3G5.crt

To view each certificate, select the certificate you want to view, and then click **View Certificate**. In the **Certificate** dialog box, click any of the following tabs to view the corresponding certificate attributes:

1 **General**—The following values are displayed:
   - Purpose of the certificate
   - Certificate issued to
   - Certificate issued by
   - Certificate valid period
2 **Details**—The certificate details are listed along with the corresponding default values. For information about individual certificates, see the **Certificate Details** section.
3 **Certification Path**—The folder path where the certificate is stored is displayed. Certificate status can be viewed in the lower pane of the window.

Certificate details

This section lists the certificates with the valid attributes and corresponding default values.

Certificate name—BTCTRoot.crt

Table 12. BTCTRoot.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	02 00 00 b9
Signature algorithm	sha1RSA
Issuer	Baltimore CyberTrust Root CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore

Certificate field	Default value/format
	C=IE
Valid from	2000–05–12 18:46:00
Valid to	2025–05–12 23:59:00
Subject	Baltimore CyberTrust Root CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore C=IE
Public key	RSA (2048 bits). Key bits are displayed in the lower pane of the window.
Key usage	Certificate Sign, CRL Sign
Subject key ID	e5 9d 59 30 82 47 58 cc ac fa 08 54 36 86 7b 3a b5 04 4d f0
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	d4 de 20 d0 5e 66 fc 53 fe la 50 88 2c 78 db 28 52 ca e4 74

Certificate name—Class3PCA_G2_v2.crt

Table 13. Class3PCA_G2_v2.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	7d d9 fe 07 cf a8 le b7 10 79 67 fb a7 89 34 c6
Signature algorithm	sha1RSA
Issuer	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 3 Public Primary Certification Authority – G2 O=VeriSign, Inc C=US
Valid from	1998–05–18 00:00:00
Valid to	2028–08–12 23:59:59
Subject	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 3 Public Primary Certification Authority – G2 O=VeriSign, Inc

Certificate field	Default value/format
	C=US
Public key	RSA (1024 bits). Key bits are displayed in the lower pane of the window.
Thumbprint algorithm	sha1
Thumbprint	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

Certificate name—Class4PCA_G2_v2.crt

Table 14. Class4PCA_G2_v2.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	32 88 8e 9a d2 f5 eb 13 47 f8 7f c4 20 37 25 f8
Signature algorithm	sha1RSA
Issuer	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 4 Public Primary Certification Authority – G2 O=VeriSign, Inc C=US
Valid from	1998–05–18 00:00:00
Valid to	2028–05–01 23:59:59
Subject	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. – For authorized use only OU=Class 4 Public Primary Certification Authority – G2 O=VeriSign, Inc C=US
Public key	RSA (1024 bits). Key bits are displayed in the lower pane of the window.
Thumbprint algorithm	sha1
Thumbprint	0b 77 be bb cb 7a a2 47 05 de cc 0f bd 6a 02 fc 7a bd 9b 52

Certificate name—Entrust_G2.crt

Table 15. Entrust_G2.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	4a 53 8c 28
Signature algorithm	sha256RSA
Issuer	Entrust Root Certification Authority CN=Entrust Root Certification Authority—G2 OU=(c) 2009 Entrust, Inc. – For authorized use only OU=See www.entrust.net/legal-terms. O=Entrust, Inc. C=US
Valid from	2009–07–07 17:25:54
Valid to	2030–12–07 17:55:54
Subject	Entrust Root Certification Authority CN=Entrust Root Certification Authority—G2 OU=(c) 2009 Entrust, Inc. – For authorized use only OU=See www.entrust.net/legal-terms. O=Entrust, Inc. C=US
Public key	RSA (2048 bits). Key bits are displayed in the lower pane of the window.
Key usage	Certificate Sign, CRL Sign
Subject key ID	6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

Certificate name—EquafaxCA1.crt

Table 16. EquafaxCA1.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	04
Signature algorithm	md5RSA
Issuer	Equifax Secure eBusiness CN=Equifax Secure eBusiness CA-1 0=Equifax Secure Inc.

Certificate field	Default value/format
	C=US
Valid from	1999–06–21 04:00:00
Valid to	2020–06–21 04:00:00
Subject	Equifax Secure eBusiness CN=Equifax Secure eBusiness CA-1 0=Equifax Secure Inc. C=US
Public key	RSA (1024 bits). Key bits are displayed in the lower pane of the window.
Key usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign, Encipher Only, Decipher Only
Subject key ID	4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
Authority key ID	80 14 4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	da 40 18 8b 91 89 a3 ed ee ae da 97 fe 2f 9d f5 b7 d1 8a 41

Certificate name—gd-class2–root.crt

Table 17. gd-class2–root.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	00
Signature algorithm	sha1RSA
Issuer	Go Daddy Class 2 Certification Authority OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Valid from	2004–06–29 17:06:20
Valid to	2034–06–29 17:06:20
Subject	Go Daddy Class 2 Certification Authority OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Public key	RSA (2048 bits). Key bits are displayed in the lower pane of the window.

Certificate field	Default value/format
Key usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign, Encipher Only, Decipher Only
Subject key ID	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3
Authority Key ID	Key bits are displayed in the lower pane of the window.
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	27 96 ba e6 3f 18 01 e2 77 26 1b a0 d7 77 70 02 8f 20 ee e4

Certificate name—GTECTGlobalRoot.crt

Table 18. GTECTGlobalRoot.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	01 a5
Signature algorithm	md5RSA
Issuer	GTE CyberTrust Global Root CN=GTE CyberTrust Global Root OU=GTE CyberTrust Solutions, Inc. O=GTE Corporation C=US
Valid from	1998–08–13 00:29:00
Valid to	2018–08–13 23:59:00
Subject	GTE CyberTrust Global Root CN=GTE CyberTrust Global Root OU=GTE CyberTrust Solutions, Inc. O=GTE Corporation C=US
Thumbprint algorithm	sha1
Thumbprint	97 81 79 50 d8 1c 96 70 cc 34 d8 09 cf 79 44 31 36 7e f4 74

Certificate name—Pc32ss_v4.crt

Table 19. Pc32ss_v4.crt Certificate details

Certificate field	Default value/format
Version	V1
Serial number	70 ba e4 1d 10 d9 29 34 b6 38 ca 7b 03 cc ba bf
Signature algorithm	md2RSA

Certificate field	Default value/format
Issuer	Class 3 Public Primary Certification Authority OU=Class 3 Public Primary Certification Authority O=VeriSign, Inc. C=US
Valid from	1996–01–29 00:00:00
Valid to	2028–08–01 23:59:59
Subject	Class 3 Public Primary Certification Authority OU=Class 3 Public Primary Certification Authority O=VeriSign, Inc. C=US
Public key	RSA (1024 bits). Key bits are displayed in the lower pane of the window.
Thumbprint algorithm	sha1
Thumbprint	74 2c 31 92 e6 07 e4 24 eb 45 49 54 2b e1 bb c5 3e 61 74 e2

Certificate name—PCA-3G5.crt

Table 20. PCA-3G5.crt Certificate details

Certificate field	Default value/format
Version	V3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary Certification Authority — G5 CN=VeriSign Class 3 Public Primary Certification Authority — G5 OU=(c) 2006 VeriSign, Inc. – For authorized use only OU=VeriSign Trust Network O=VeriSign, Inc C=US
Valid from	2006–11–08 00:00:00
Valid to	2036–07–16 23:59:00
Subject	VeriSign Class 3 Public Primary Certification Authority — G5 CN=VeriSign Class 3 Public Primary Certification Authority — G5 OU=(c) 2006 VeriSign, Inc. – For authorized use only OU=VeriSign Trust Network O=VeriSign, Inc C=US

Certificate field	Default value/format
Public key	RSA (2048 bits). Key bits are displayed in the lower pane of the window.
Key usage	Certificate Sign, CRL Sign
Subject key ID	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	4e b6 d5 78 49 9b 1c cf 5f 58 le ad 56 be 3d 9b 67 44 a5 e5

Using the Troubleshooting Options

Use the **Troubleshooting** dialog box to configure Trace and Event log settings, performance monitor graphs that display client CPU, Memory, and Networking information, and for CMOS management extract and restore cmos settings. It also allows you to view wnos.ini cached information for troubleshooting purposes.

An additional option labelled Export Event Log is added to the Options window in Troubleshooting to enable logging of unexpected error messages.

To use the Troubleshooting options, do the following:

1 From the floating bar menu, click **Troubleshooting**.
The **Troubleshooting** dialog box is displayed.

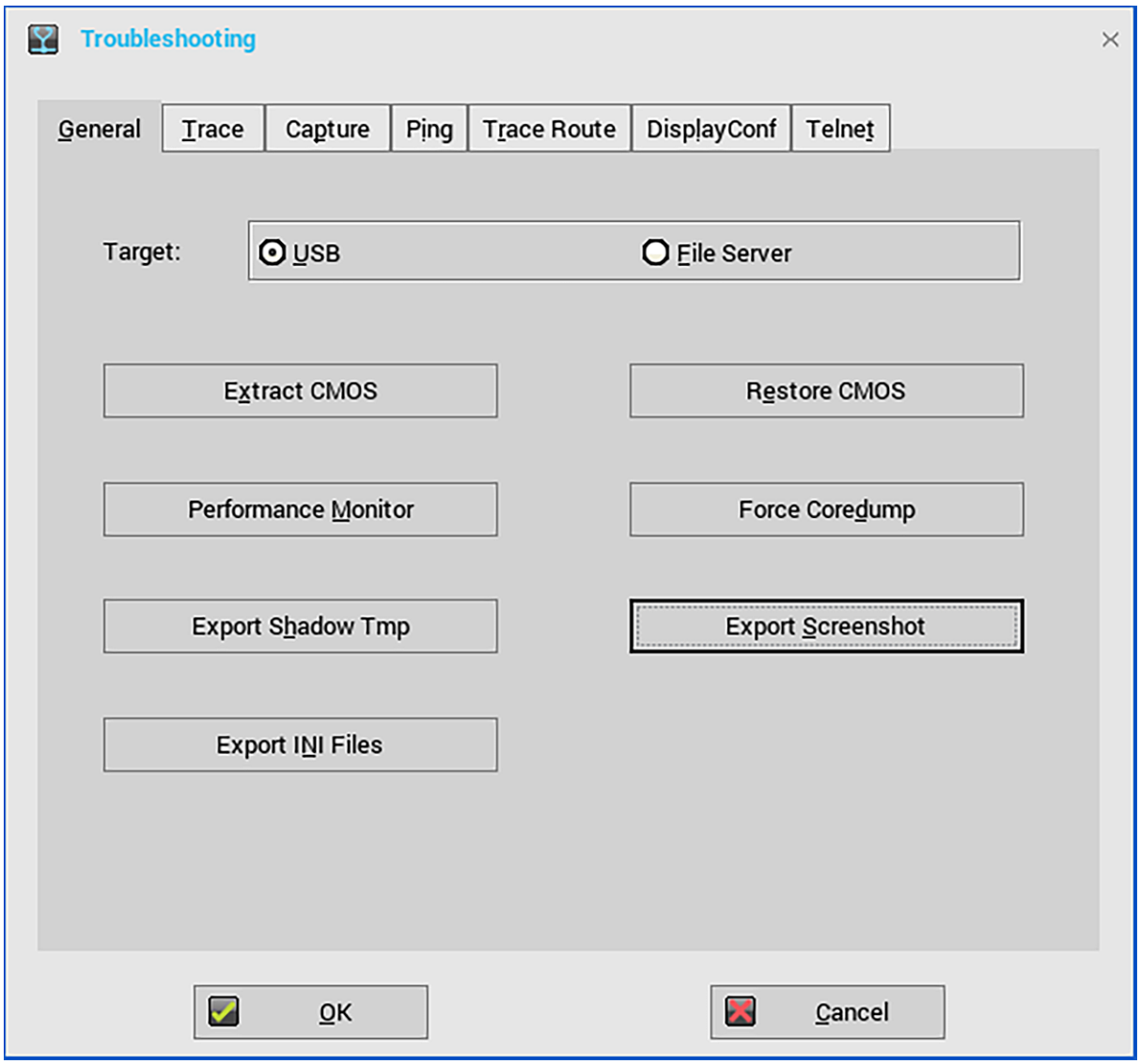


Figure 133. Trouble Shooting

2 Click the **General** tab and use the following guidelines:

a Click either **USB** or **File Server** to select your target device you want to use for CMOS management.

b **Extract CMOS** — Click this option to extract the CMOS settings to the USB Key or file server based on your target device selection.

c **Restore CMOS** — Click this option to write the CMOS settings from the USB Key to the target zero client.

d **Performance Monitor** — Click this option to display your zero client CPU, Memory, and Networking information. The graphs display on top of all windows.

e **Force Coredump** — Use this option to forcibly generate the debug information for technical investigation when your system is not responding.

f **Export Shadow Tmp**— Use this option to export temporary logs for debugging purpose. The log files can be exported to USB or File Server depending on the target configuration.

g **Export Screenshot**— Use this option to export screenshots to the file server or a USB drive. The exported file name is added with build information for a better troubleshooting. If a screenshot is present in the clipboard, then it is exported to the target location. If the screenshot is not available, then the full screen is copied automatically and exported to the target location.

h **Export INI files**—Use this option to export the global INI file (wnos.ini or xen.ini), wdm.ini, ccm.ini, mac.ini or other machine based INI file to the file server or a USB drive. Only username.ini file cannot be exported.

3 Click the **Trace** tab to configure the trace actions and delay on trace. The available options for trace action are **None**, **Capture**, and **Playback**.

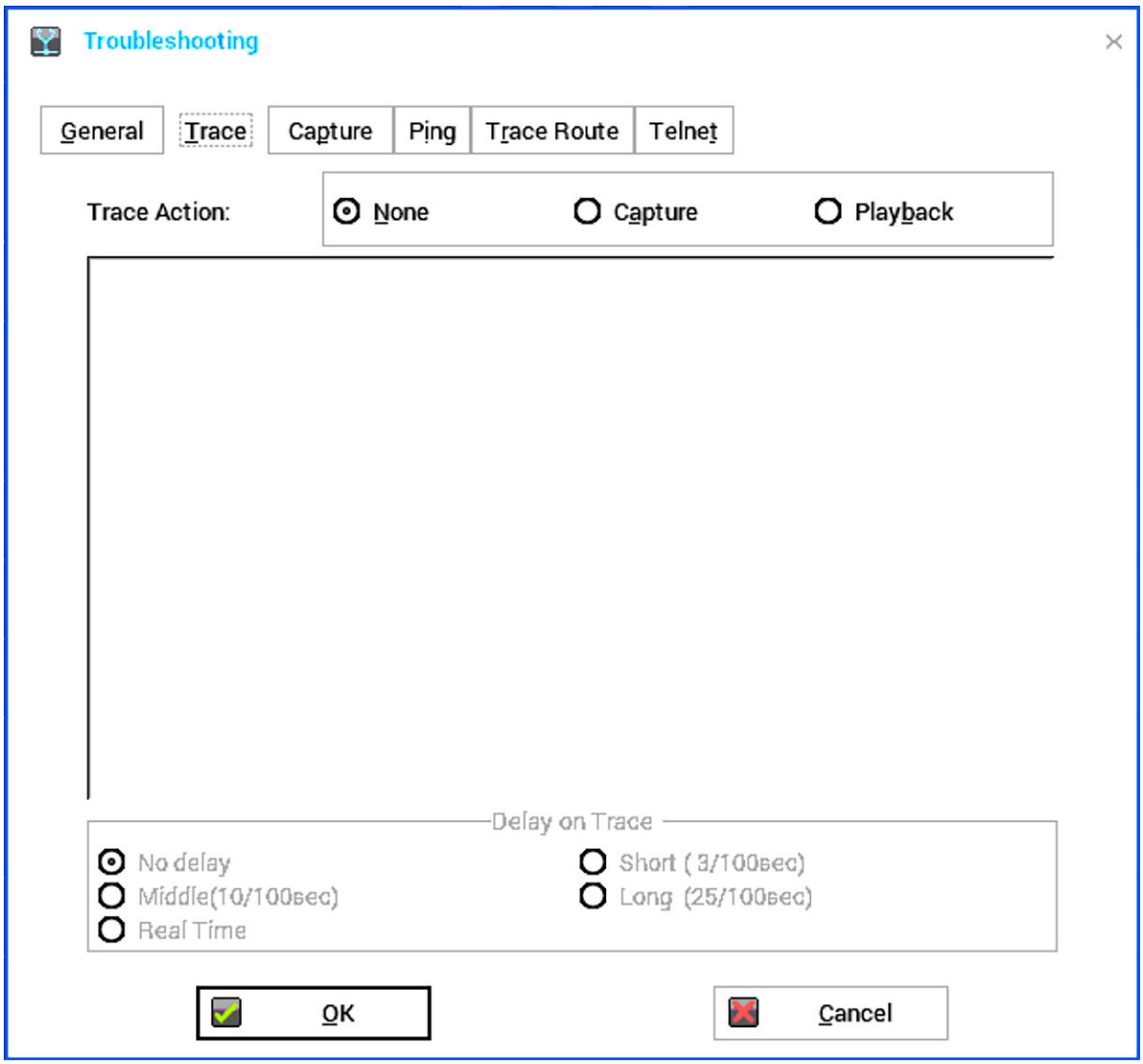


Figure 134. Trace

4 Click the **Capture** tab to configure the Export Event Log, Network Capture to USB, Wireless Capture to USB, and capture USB packets.

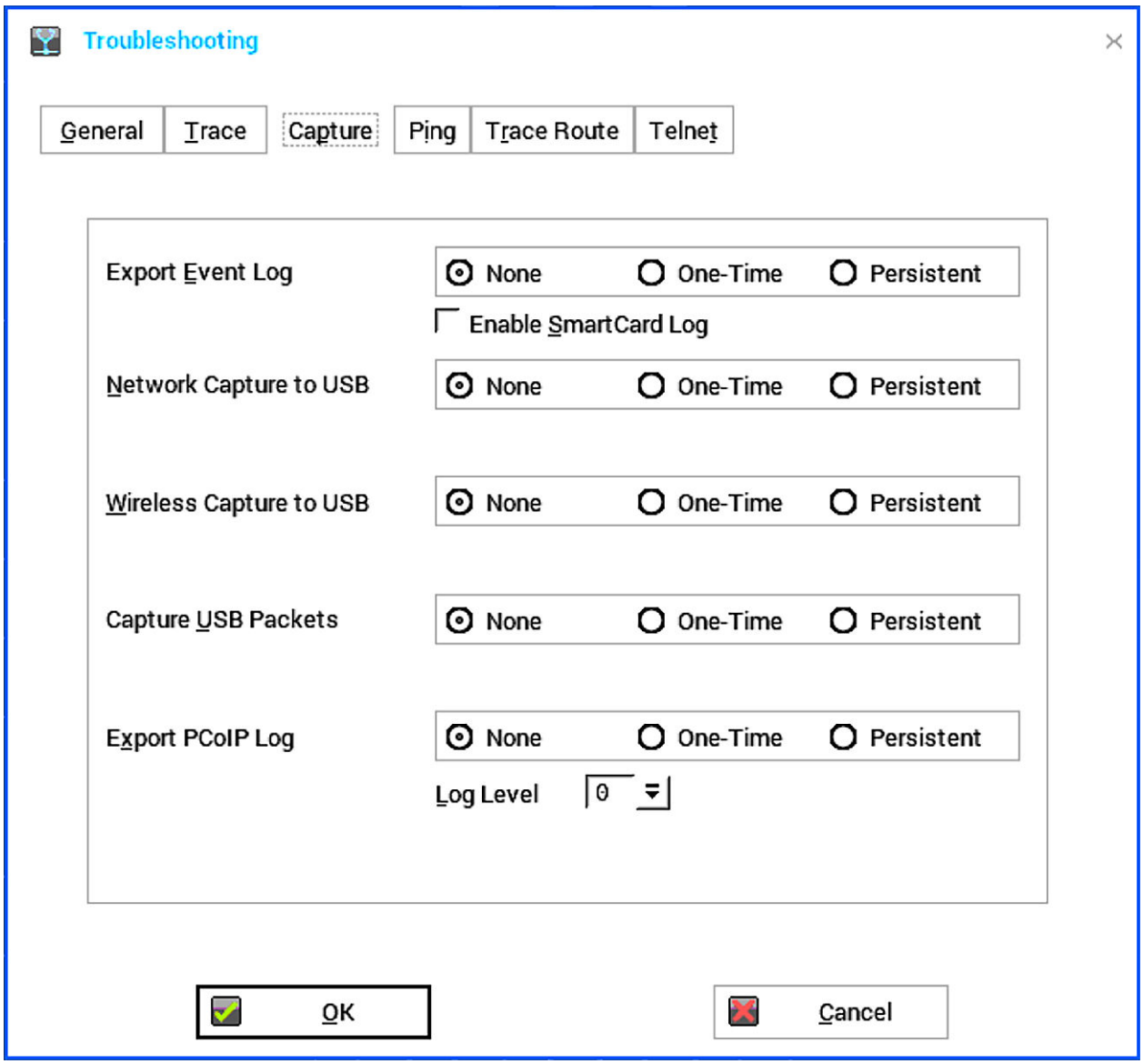


Figure 135. Capture

If you want to enable the error messages, use the following guidelines:

- Click either **One-time** or **Persistent** option to enable logging the unexpected error message.
- If you want to check the error messages, under Troubleshooting, turnoff the logging before checking.

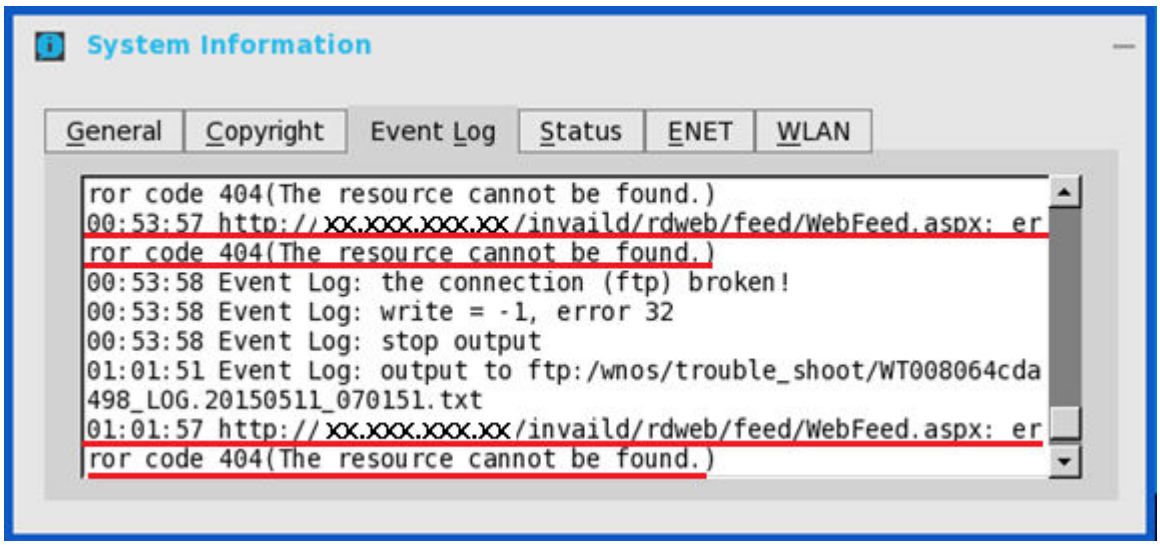


Figure 136. Event log

- Be sure to enable the EnableTrace option of the Privilege parameter in a `xen.ini` file. For more information, see *Dell Wyse ThinOS Lite INI Guide*.
- Use the **Network capture to USB** option to enable the capture of network information, that is, a network trace of all traffic coming in and out of the zero client to a USB drive that is inserted into the zero client.

  After you login and use the XenDesktop server or network, you will see a `/wnos/troubleshoot/[Terminal Name]_[ENET or WS].[Date_Time].pcap` file in the USB drive which you can analyze using software such as a packet analyzer used for network troubleshooting, and analysis.

  For example, for Ethernet, the file name is yx008064b2bfd7_ENET.20150415_064455.pcap. For wireless, the file name is yx008064b2bfd7_WS.20150415_064455.pcap.

  NOTE:
  Ensure that you have inserted the USB drive into the zero client before selecting the Network capture to USB option. The Network capture to USB option is automatically cleared if there is no USB drive inserted and you exit the dialog box, or after restarting the zero client; if needed, you must select the option again.

5 Click the **Ping** tab, and use the following guidelines to execute the ping diagnostic utility and display response messages:

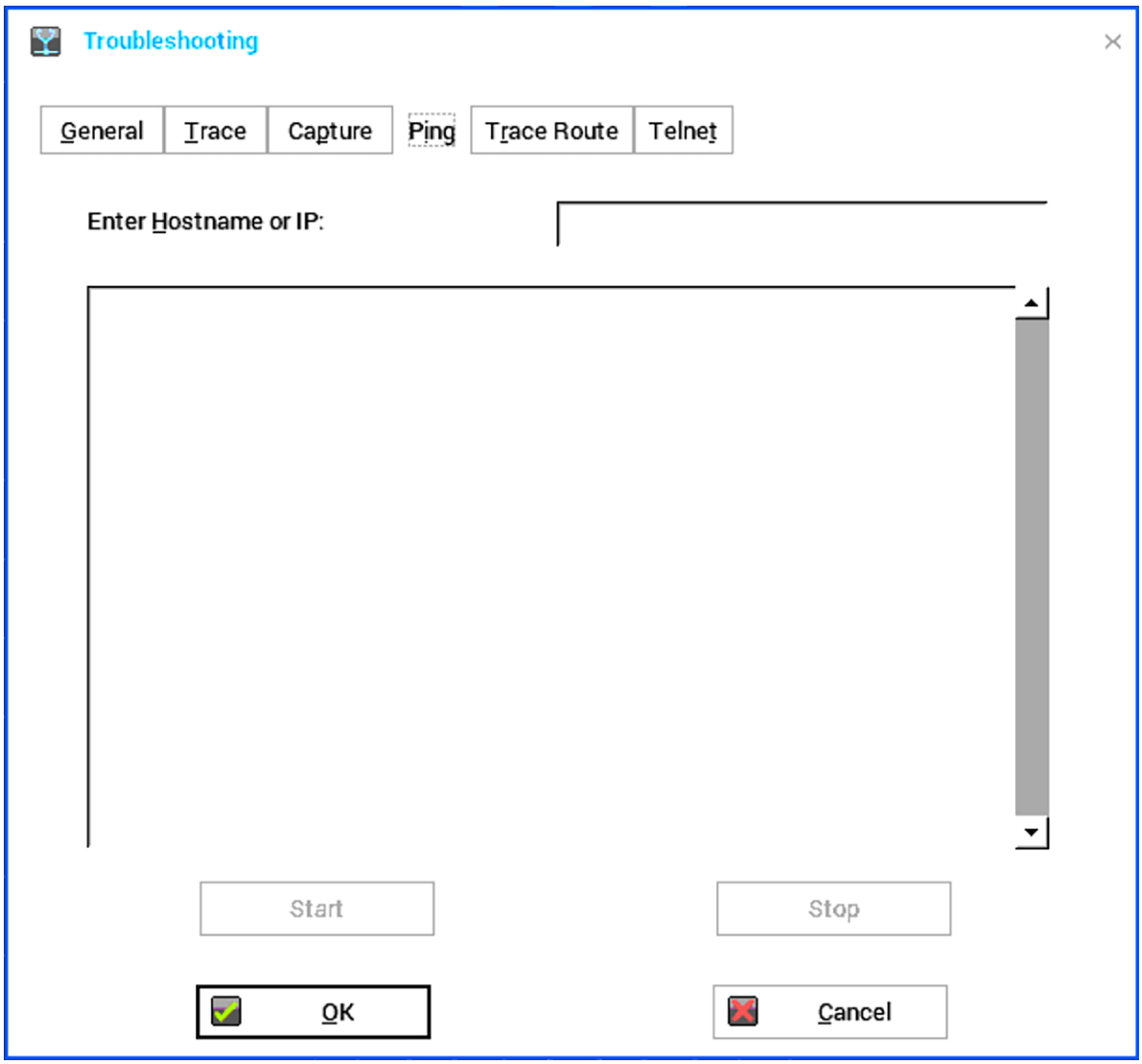


Figure 137. Ping

a **Enter Hostname or IP** — Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be pinged.

b **Data area** — Displays ping response messages. The ping command sends one echo request per second, calculates round trip times and packet loss statistics, and displays a brief summary upon completing the calculation.

c **Start** — Executes the ping command. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted by clicking **Stop**.

d **Stop** — Terminates the ping request and leaves the **Ping** dialog box open, so you can read the summary posted in the data area.

NOTE:

Ping sends an echo request to a network host. The host parameter is either a valid host name or an IP address. If the host is operational and on the network, it responds to the echo request. Ping sends one echo request per second and calculates round trip times and packet loss statistics. It displays a brief summary upon completion of the calculation.

The ping utility can be used to:

- Determine the status of the network and various foreign hosts.
- Track and isolate hardware and software problems.
- Test, measure, and manage networks.
- Determine the IP address of a host if only the host name is known.

IMPORTANT:

Not all network equipment will respond to ping packets, as this is a common mechanism used in denial-of-service attacks. Lack of response does not necessarily indicate that the target of the ping is unusable for other purposes.

6 Click the **Trace Route** tab to execute the tracert diagnostic utility and display response messages. Use the following guidelines:

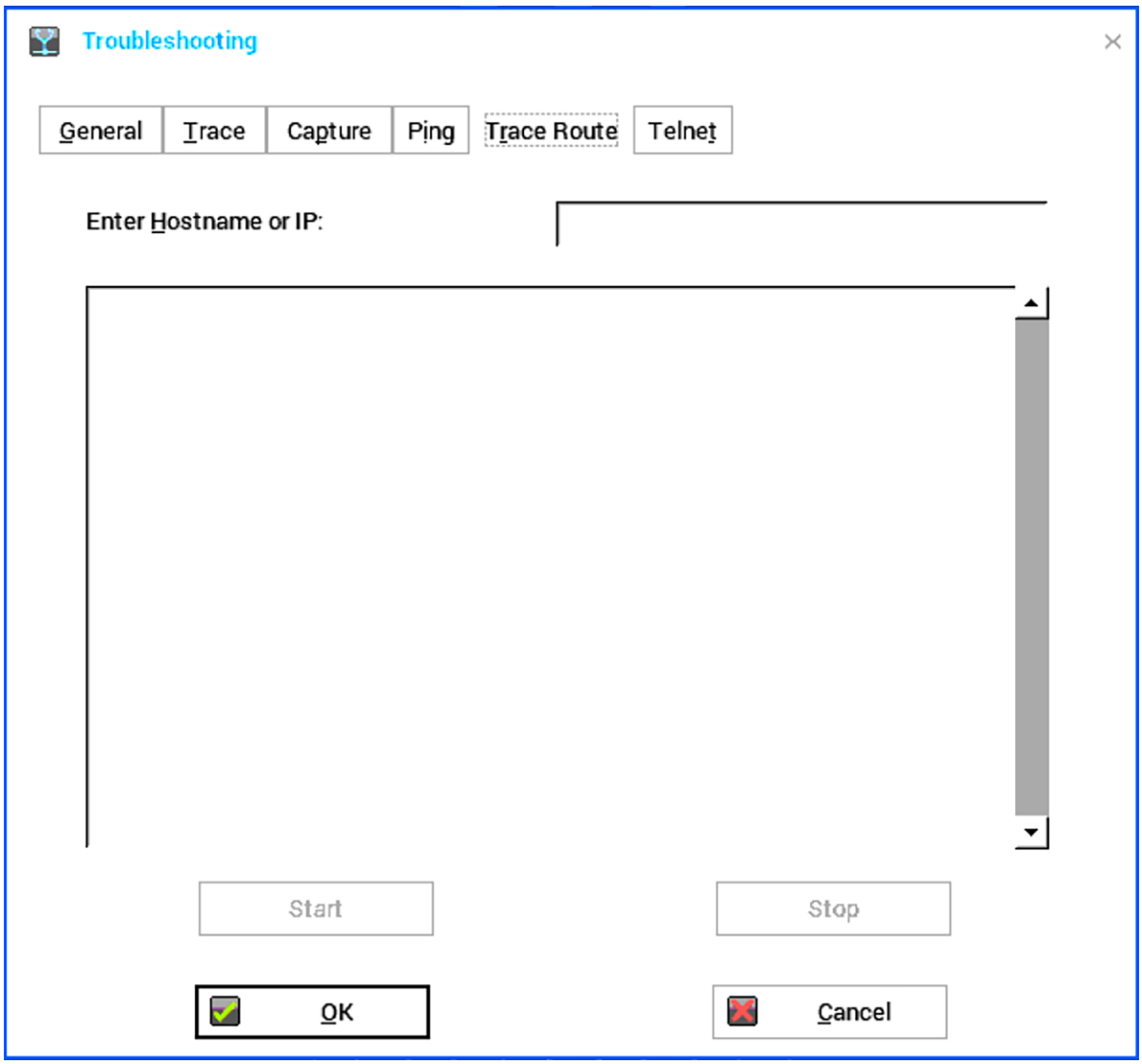


Figure 138. Trace Route

a **Enter Hostname or IP** — Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be traced
b **Data area** — Displays round-trip response time and identifying information for each device in the path.
c **Start** — Executes the tracert command.
d **Stop** — Terminates the tracert command and leaves the **Trace Route** dialog box open, so you can read the information posted in the data area.

The tracert utility traces the path from your zero client to a network host. The host parameter is either a valid host name or an IP address. The tracert utility sends out a packet of information three times to each device (routers and computers) in the path and displays the round trip response times and identifying information in the message box.

7 Click the **Telnet** tab, and do the following:

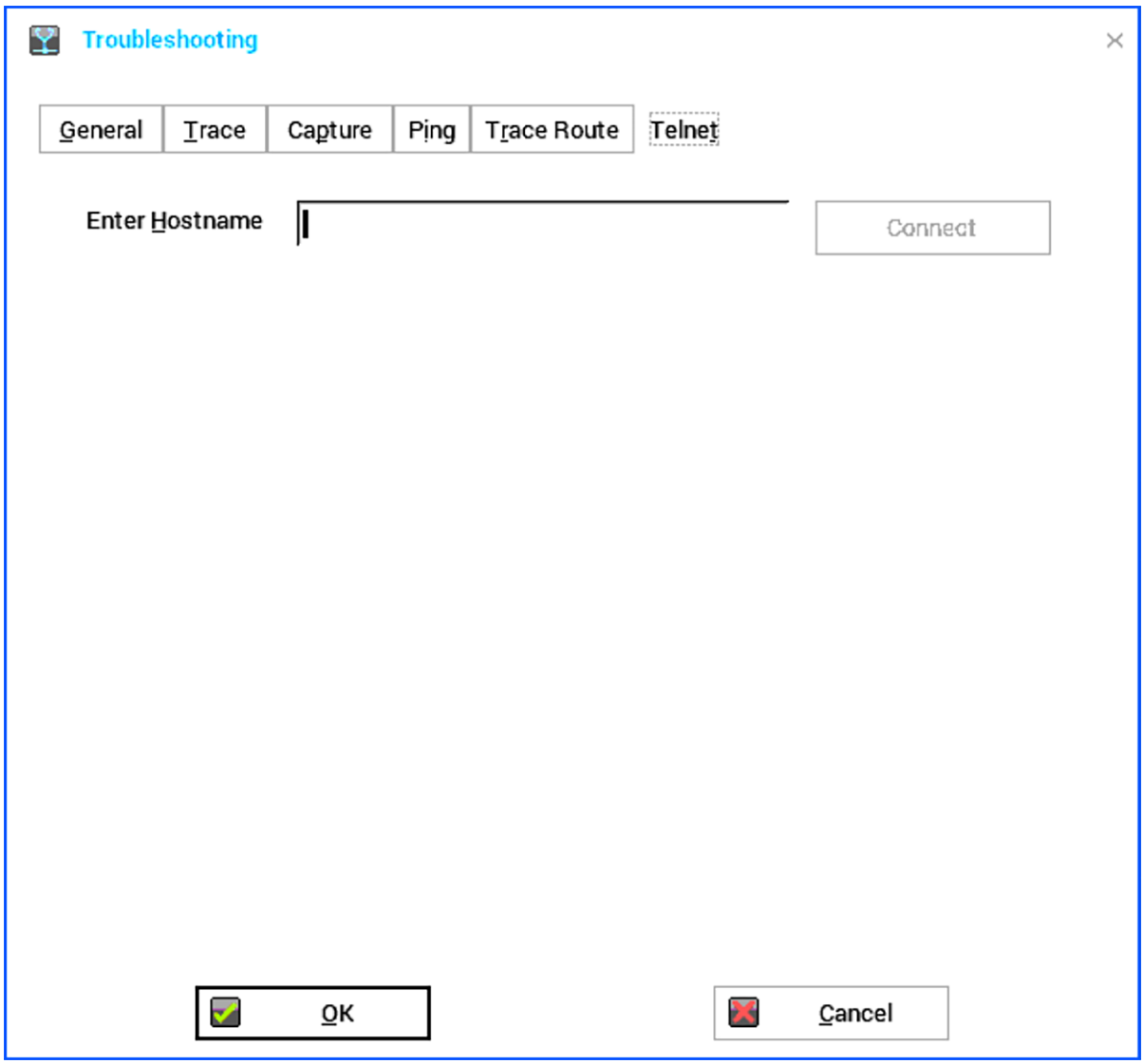


Figure 139. Telnet

a Enter the hostname.
b Click **Connect** to connect to a remote host or device.

The **Telnet** window is displayed, and the troubleshooting window is closed automatically.

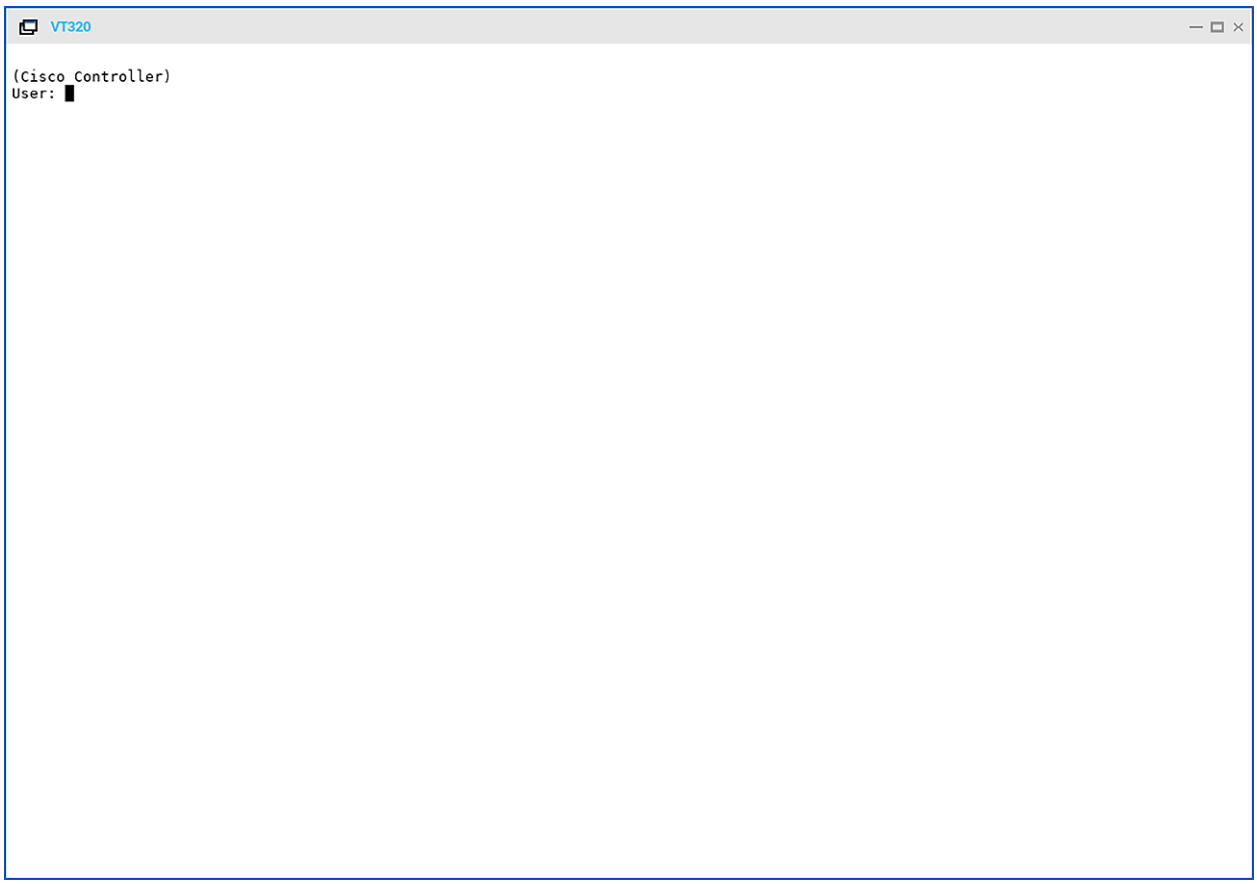


Figure 140. Telnet Window

8 Click **OK** to save the settings.

9

BIOS Management

The BIOS management information is used with the following supported versions:

- Wyse 5010 Zero Client for Citrix - D00DX (ThinOS Lite pro) BIOS version 3.0D or later

For BIOS configuration, if a password is configured, the password is required to update any settings. For example, the INI parameter to update settings must be same as CurrentPassword={}. This is mandatory for Dell BIOS, and will be implemented as mandatory for Wyse BIOS post this release.

After a File Server BIOS update to a Wyse 5010 thin client device, due to a CMOS mismatch, BIOS management may not be possible till the user manually enters and exits the BIOS configuration menu. This can be accomplished as follows:

- Boot unit and press **Delete** during boot to enter BIOS menu.
- Enter the BIOS password.
- Press **F10** to save BIOS configurations and resolve the CMOS mismatch.

The following table contains details on the main BIOS function and support matrix:

Table 21. BIOS function and support matrix

Major Requirement	INI example for BIOS management	Wyse 5010 zero client/ 3.0 U
Power on without beeps	NA	Yes
Update BIOS from file server	NA	Yes
Change BIOS password with INI	Device=Cmos CurrentPassword={} NewPassword={}	Yes
Change boot order with INI	Device=cmos BootOrder={PXE, HardDisk, USB}	Yes
Enable/Disable USB imaging with INI	Device=cmos BootFromUSB={yes, no}	Yes
Manage AC recovery with INI	Device=cmos AutoPower={yes, no}	Yes
Manage auto on time with INI	Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday	Yes
CMOS Extract and Restore	Device=cmos Action={extract, restore}	Yes
Audio management with INI	Device=cmos OnboardAudio={yes, no}	Yes
USB Port management with INI	Device=cmos USBController={yes, no}	Yes
Wake On LAN	Device=cmos WakeOnLan= {yes, no}	Yes

Depending on the method of distribution you want to use, there are two types of CMOS Management:

- CMOS Cental Management: Extracting CMOS Settings to a USB Key for Distribution
- CMOS Local Management : Extracting CMOS Settings to a USB Key for Distribution

CMOS Central Management—Extracting CMOS Settings to the File Server for Distribution

CMOS Central Management allows ThinOS Lite administrators to easily manage CMOS settings for large deployments of zero client devices using central configuration methodologies.
The following are the steps for extracting CMOS Settings to the File Server for Distribution for C00 BIOS version 1.0B_SPC001–0407:

1 To prepare a Reference Drive containing BIOS version 1.0B_SPC001-0407 or later:
   a The Reference Device is a golden image you use to distribute to other zero client devices. To access Reference Drive, enter the BIOS Setup Utility. Press the Delete key, enter the Password — Fireport (case sensitive) and press Enter. Configuring the CMOS settings, includes AutoPower, BootOrder, P-key setting, BiosPassword.
   b Save your CMOS Settings.
   c Restart your zero client device.
2 To create a CMOS INI File in a File Server:
   a In the file server, create a **cmos.ini** file and place it in the wnos directory/folder under the file server ini directory. Make sure that wnos directory on the file server has upload privilege.
   b Enter the following name in the cmos.ini file:**Device=cmos Action=extract**.
3 To reboot the Reference Device to the File Server containing the CMOS INI File:
   a Start the zero client, FOR which you want to use a Reference Device.
   b In the Login dialog box, enter the credentials you need to access the cmos.ini file.
   c After login, to view Event Log tab.

   To view **Event Log**, click System Information icon, System Information dialog box is displayed. In the System Information dialog box, select Event Log tab.

   You can open the event log to view a CMOS: extract to C00_cmos.1.0B_SPC001 event. This means that the CMOS central management file (containing the CMOS settings from your Reference Device) is now copied to the wnos directory/folder on the file server. As this is a C00 BIOS version 1.0B_SPC001-0407 example, the CMOS central management file name would be C00_cmos.1.0B_SPC001. These CMOS settings are now ready for distribution to other zero clients.
4 To prepare the File Server containing the CMOS INI File for Distribution:
   a Start the zero client devices for which you want to distribute the Reference Device CMOS Settings.
   b To access the **cmos.ini** file, enter your credentials in the Login dialog box.
   c To open Event Log, click System Information icon. In the System Information dialog box, select Event Log tab.

   You can view the CMOS: restore from C00_cmos.1.0B_SPC001 event. This means that your Central Management file containing the CMOS settings from your Reference Device is copied to the targeted zero client devices.

   NOTE: After you target your zero client devices contain the CMOS settings you want, do not log in to the file server containing the cmos.ini file with the restore action, unless you want to redo the restore process. Administrator can remove the cmos.ini file to prevent from unwanted CMOS overwrite.

   NOTE: It is recommended to initially complete these procedures on a file server designated to test the success of your CMOS central management settings/process. While the central configuration method can be used to enforce your CMOS settings in a production environment, be aware that any zero client device that logs in to the file server that contains the cmos.ini and its extract and restore commands are subject to those CMOS overwrite.

   NOTE: The above procedure is also applicable for other supported BIOS versions.

CMOS Local Management—Extracting CMOS Settings to a USB Key for Distribution

CMOS Local Management allows ThinOS Lite administrators to easily manage CMOS settings for small deployments of zero clients using USB Key distribution methods.
The following are the steps for extracting CMOS Settings to a USB Key for Distribution for C00 BIOS version 1.0B_SPC001–0407:

1 To prepare a Reference Drive containing BIOS version 1.0B_SPC001-0407 or later:

a The Reference Device is a golden image you use to distribute to other zero client devices. To access Reference Drive, enter the BIOS Setup Utility. Press the Delete key, enter the Password — Fireport (case sensitive) and press Enter. Configuring the CMOS settings, includes AutoPower, BootOrder, P-key setting, BiosPassword.

b Save your CMOS Settings.

c Restart your zero client device.

2 To extract the CMOS Settings to a USB Key:

a Attach a formatted USB key on the zero client device which you want to use as a Reference Device.

For example, to format on Windows 7 , attach the USB Key, right-click on the **USB Key** > **Format** > **Restore device defaults** > **Quick Format** and then click Start.

b After the extraction is complete, a pop-up message: **CMOS: extract to R00_cmos.1.0H_SPC** is displayed and then eject and detach the USB Key. The CMOS settings on the USB Key are now ready for distribution to other zero clients.

3 To restore the CMOS Settings to your Target Devices:

a Start the targeted zero clients, to distribute the Reference Device CMOS settings.

b To configure the CMOS settings from the USB Key to the targeted zero client, go to Restore CMOS from USB GUI feature of ThinOS Lite.

- For Wyse Zero Desktop: Click on System Settings icon, go to **System Tools** > **General tab** > **USB** > **Restore CMOS**.

c After the restoration is complete, a pop-up message: **CMOS: restore from R00_cmos.1.0H_SPC** is displayed and then eject and detach the USB Key. The CMOS settings on the USB Key are now reflected on the targeted zero clients.

NOTE: The above procedure is also applicable for other supported BIOS versions.

Accessing Zero Client BIOS Settings

After starting your zero client you will see a Dell logo for a short period of time. During this period you can press and hold the **Delete** key to enter the BIOS with **Fireport** as the password, to make your modifications. For example, you can use the F7 key to use Optimized Defaults (load optimal default values for all the items in the BIOS setup utility).

NOTE: These BIOS settings are not applicable to Wyse 3010 zero client for Citrix and Wyse 3020 zero client for Citrix, as there is no BIOS on ARM platform. To access the WLOADER on an ARM platform, press the power button for about four seconds until the power light turns green, and then press the Delete key.

10

Security Changes

A new global security policy has been defined for ThinOS Lite and this policy is applied to all secure connections (https/SSL connections) with a few exceptions.

Purpose – To improve the security level by default and add the global configuration. This security policy integrates security setting for each application.

```
SecurityPolicy={full, warning (default)|Low}

SecuredNetworkProtocol={yes | no (default)}

TLSMinVersion={1(default),2,3}

TLSMaxVesion={1,2,3 (default)}
```

The new INI parameter is independent and does not have any dependencies with other parameters. `SecurityLevel|SecureProtocol` from the Privilege segment is deleted.

ThinOS Lite supports SSL from TLSMinVersion onwards. `TLSMaxVersion` is the latest version of SSL supported by ThinOS Lite.

- If no value is set, then TLSMinVersion is set to TLS1.0 by default, and TLSMaxVersion is set to TLS1.2 by default.
- The values 1, 2, 3 refers to TLS1.0,TLS1.1,TLS1.2 respectively.

All applications running on the default SSL security mode follows the global mode. In the global mode, the default value is Warning. The affected applications include File Server, WDM, Caradigm, and OneSign. The following are the exceptions:

- File Server and WDM in factory reset state: Before loading any INI parameter, the SSL security mode is set to Low, and after loading the INI parameter, the value is changed to follow the global mode value. For example, the default value is set to Warning, if the value is not changed by the INI parameter.

  System with previous settings (default value is set to Low) follows the global mode after the unit is upgraded. For example, the default value is set to Warning, if the value is not changed by the INI parameter.
- Wyse Management Suite, Citrix broker, and SecureMatrix are always `Full`.

The following new INI parameters are added to support the changes mentioned:

- `CaradigmServer=SecurityMode={default,full,warning,none}`
- `OneSignServer=SecurityMode={default,full,warning,none}`
- `FileServer=SecurityMode={default,full,warning,none}`
- `RapportDisable=SecurityMode={default,full,warning,none}`
- `WDMService=SecurityMode={default,full,warning,none}`

File Server default protocol is retained as FTP without any setting from WDM/DHCP/INI and always displays the full address with protocol prefix. For example, `ftp://`.

New firmware/client deploy information is as follows:

- In a secured environment, such as file server and WDM using HTTPS, with clients in factory default or factory reset status, Dell recommends that IT administrator configures the proper file server address in WDM or DHCP, WDM address in DHCP, and uploads all necessary client certificates to a valid location before turning on the new client or upgrading to the new firmware with DHCP. This

automatically installs the required certificates. From the second boot up, without these configurations, the warning message is displayed with **OK** button for you to continue.

NOTE: For file server, the continue button is displayed with its own GUI.

- In a secured environment, such as file server and WDM using HTTPS, with previous clients upgraded to new firmware from file server, by default, the clients follow the new global SSL security mode, and the default value is set to Warning, if no value is set using the INI parameter. Dell recommends you to install required certificates on all clients before firmware upgrade. If required certificates are not propagated to clients, then you must see the displayed warning message during system boot up, such as click **OK** or continue, and select the preferred option.
- In an un-secured environment, such as file server and WDM using ftp/http protocol, after firmware update or boot up with factory default settings, the client connects to the file server in ftp protocol without any warning message.
- Dell recommends you to define the Security Policy before upgrading to version 8.3. If not, you may get warning messages that require intervention to proceed.

Improved user friendly messages are displayed for errors and warnings. The UI is not changed and only the message is modified for security errors/warnings.

In full security mode, the following warning message is displayed:

Figure 141. SSL Connection

Earlier when the connection to https file server fails in full security mode, a dialog box is displayed which prompts you to click OK. From ThinOS Lite 2.5 HF2 release, the feature is updated to display a tooltip at the bottom-right of the screen.

For warning security mode, the following warning messages are displayed:

Figure 142. Security alert

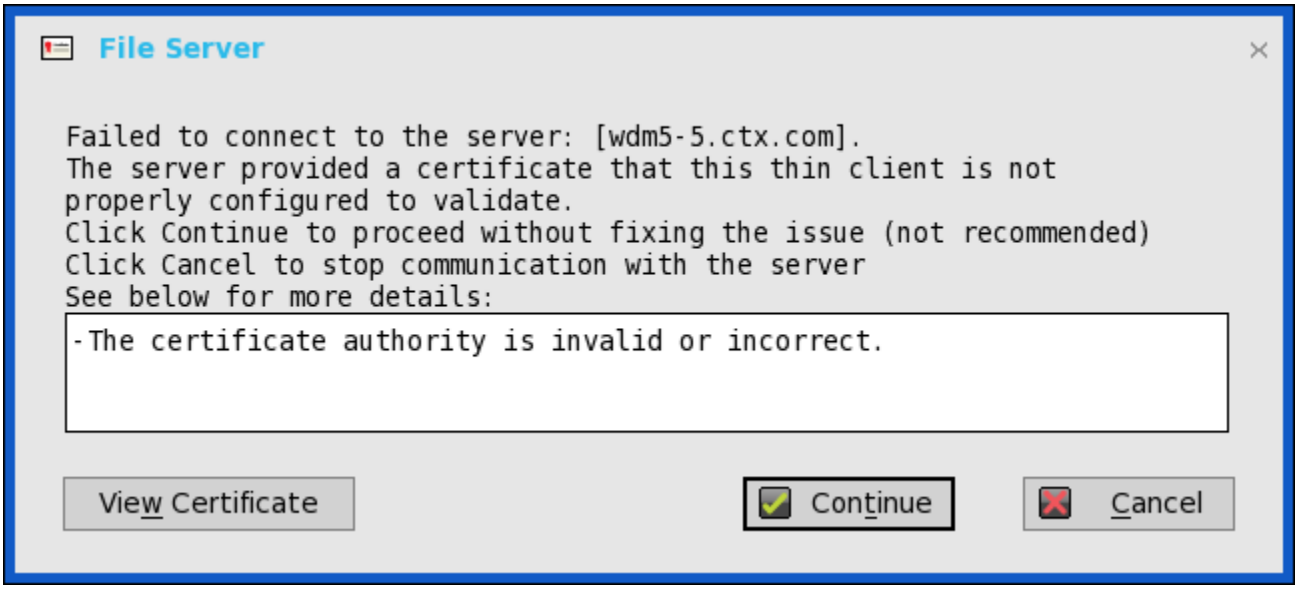


Figure 143. File Server

The server address does not convert to http, if WDM server is set as https.

- In the previous scenario, If WDM server is configured without HTTPS, and local WDM server address is specified in HTTPS, then the system converts it to HTTP address.
- In the current scenario, the system does not convert the WDM server address to HTTP.

Manual discovery is removed from WDM. In the **WDA** tab, the Manual discovery method option is removed.

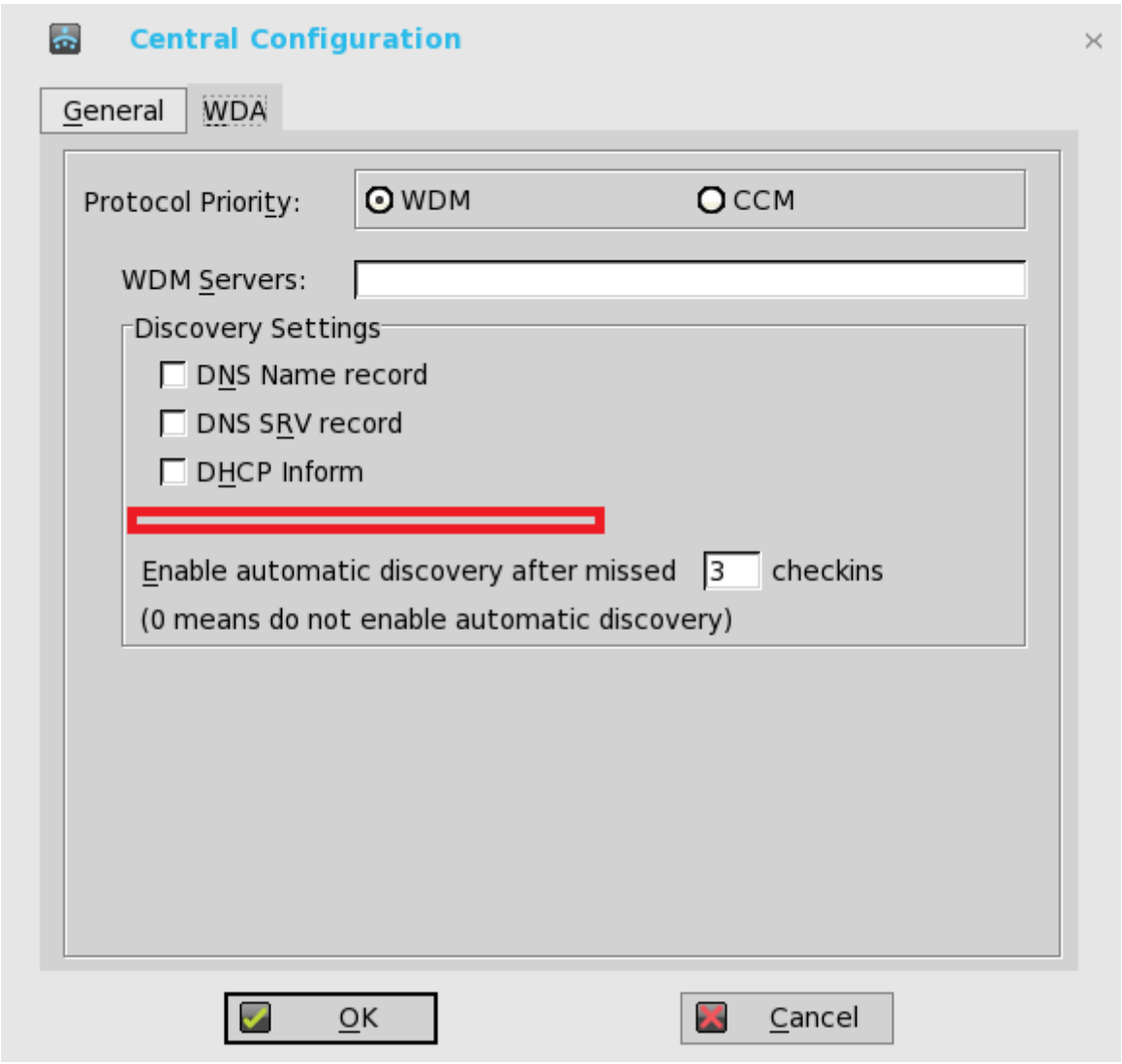


Figure 144. Central Configuration

By default, the SNMP is set to disabled. You can enable it by setting the INI parameter`Community=`

Security Enhancements—Firmware Signature

In ThinOS Lite 2.4 release, firmware signature verification is added to enhance firmware security. By default, signature verification is required on firmware downgrade/upgrade

Salient features

- By default, signature verification is required on firmware downgrade/upgrade.
- Provision to downgrade from 2.4 firmware to 2.3 firmware without signature.
- New INI parameter `verifysignature=no` is introduced to enable user downgrade firmware. For example: `autoload=101 verifysignature=no`. For more information about using INI parameters, see INI Parameters.

  The following scenarios are allowed without need of using INI parameters:
  - Upgrade from 2.3 firmware to 2.4 firmware.
  - Upgrade or Downgrade between 2.3 and/or earlier firmware.

- Upgrade or Downgrade between 2.4 and later firmware.

Transport Layer Security—TLS

Transport Layer Security (TLS) is a protocol that provides communication security between the client and server applications.

Upgrade to Transport Layer Security (TLS)— In the ThinOS 8.2 release, the TLS is upgraded from version 1.0 to version 1.2. By default, the ThinOS client uses TLS 1.2 to secure any communication protocols, connections, or applications upon SSL/ TLS in general and falls back to the previous SSL/ TLS version when negotiating with the server.

Smart cards and smart card readers

A smart card is a security token that has embedded integrated circuits. Smart cards allow you to store and transact data.

A smart card reader is an input device that reads data from a smart card.

- **Gemalto smart card IDPrime MD840**—Gemalto smart card IDPrime MD830 and MD840 are supported. IDGo 800 version 1.2.1 - 01 for the Windows middleware is required for supporting Gemalto smart card IDPrime MD840.

  The Secure Messaging feature is supported to enable the usage of latest MD830 Rev B cards.

  Known issue for Prime MD 840 smart card: If first container is used, then Xen broker logon fails.
- **OMNIKEY smart card readers**—The following OMNIKEY smart card readers are supported:
  - Omnikey 5427 CK (0x5427, 0x076b) reader supports iclass15693, 14443a, 125k card
  - Omnikey 5326 DFR(0x5326, 0x076b) reader supports iclass15693 card
  - Omnikey 5025 CL (0x502a, 0x076b) reader supports 125k card
  - Ominkey 5325 CL, 5125 (0x5125, 0x076b) reader supports 125k card
  - Omnikey 5321 V2 CLi (0x532a, 0x076b) reader supports 13.56 MHz card
  - Omnikey 5021 CL (0x5340, 0x076b) reader supports 13.56 MHZ card
  - Omnikey 5321 V2 CI Sam (0x5341, 0x076b) reader supports 13.56 MHz card
  - Omnikey 5421 (0x5421, 0x076b), reader supports 13.56 MHz card
  - Omnikey 5321 CR (0x5320, 0x076b)
  - Omnikey 5022 CL
- **On-board smart card reader**—On-board smart card reader works with regular smart cards. The functionality is similar to other external USB smart card readers and on-board smart card readers such as Dell KB-813.

For information about the complete list of the tested smart cards and smart card readers, see the latest Release Notes.

A

Creating and Using xen.ini Files

In this chapter you will learn how to construct and use a xen.ini file. The xen.ini file you create will provide your zero client with automatic updates and configurations.

Downloading and Using Sample INI Files

ThinOS Lite Sample INI files are available from Dell and can be modified to suit the individual connection profile needs for your users. These sample files are annotated to allow you to use them as a starter set, that you can modify to quickly get your file server up and running.
To download and use the files:

1 Go to Dell support site.
2 Click **Product Support**, and manually browse for your thin client model.
3 Click **Drivers and Downloads**.
4 From the **Operating system** drop-down menu, select **ThinOS Lite**.
5 Scroll down the page and download the sample INI file to the file server.
6 Open the text file by using an ASCII text editor, and modify the INI parameters as needed for your use. Be sure to rename the sample file to xen.ini for use.

Rules and Recommendations for Constructing a xen.ini File

In general, xen.ini files follow currently accepted "standard" INI file formatting conventions. The INI files consist of Dell Wyse parameters. If you are using an INI file, the only parameter you must use is the Connect parameter. For more information, see Connect in Parameters for a xen.ini File.

Any of the rest of the parameters can be used if you desire, but are not necessary unless you want changes from client and **other** defaults. For example, **other** can be the default resolution of your monitor. Every parameter has a name and a value, with the name appearing to the left of the equals sign (name=value). Number signs (#) indicate the start of a comment.

Comments can begin anywhere on a line. Everything between the # and the End of Line is ignored. Along with these general formatting conventions, use the following guidelines when constructing the INI files:

1 **Connect is the Only Required Parameter**

As stated earlier, if you are using an INI file, the only parameter you must use is the Connect parameter. Any of the rest of the parameters can be used if you desire, but are not necessary unless you want changes from client and **other** defaults.

2 **Continue Lines by using a Space and Backslash**

Placing a space and backslash (\) at the end of a line indicates line continuation; that is, the backslash means that the line and the following line are, for the purposes of reading code, the same line. No white space can appear after the backslash; the requirement of white space between parameter entries is maintained by the use of the space before the backslash.

In addition, starting all parameters at the left margin and placing at least one leading space (or tab) at the beginning of all (and only) continuation lines makes an INI file easier to read.

NOTE: In circumstances where you require string concatenation, you can use a backslash without a space before or after it to concatenate with the first set of characters from the previous line; for example the strings snow and ball may be concatenated to give snowball.

3 **Blank Lines Make Files Easy for Humans to Read**

Using blank lines is recommended for making code easier for you to read.

For example:

```
BootOrder=harddisk;usb;pxe

SessionConfig=ICA
PnliteServer=xxxxx
SessionConfig=ICA USBRedirection=HDX AudioQuality=High
DomainList="dellwyse.com"
Password=PCCOPIDIPKCKPGGC encrypt=yes


MaxVNCD=1
VncPassword="NCAOIIBOMPACMOAFMPBJ" Encrypt=yes
VncPrompt=No Accept=5
```

4 **Comment by using a # Sign**

As stated earlier, number signs (#) indicate the start of a comment. Comments can begin anywhere on a line. Everything between the # and the End of Line is ignored.

5 **Values with White Spaces Require Quotation Marks**

Values of parameters and their options containing white spaces must be placed inside quotation marks (use common-practice nesting rules).

6 **Separate Lists by using Semicolons or Commas**

Use semicolons or commas for list separators.

Parameters for a xen.ini file

The following table contains the most commonly used parameters in a xen.ini file.

IMPORTANT: Some parameters also have options shown within parenthesis [ ]. If an option has an underlined value (default), that option and default value will be automatically updated along with the parameter, options without underlined values can also be used if you want to, but are not automatically updated with the parameter.

In addition, when using parameters and options, you can retain the default value or change it to another value shown.

For example, in the following case where:

ParameterX={yes, no}

[Option1={0, 1}]

[Option2={1, 2, 3, 4}]

If you use ParameterX, then Option1 and its default value 0 will automatically updated as Option1 has been underlined (default of 0). You can still use Option2 if you want to, however, Option2 is not automatically along with the parameter as Option2 does not have a underlined (default) value.

Table 22. Parameters for a xen.ini File

Parameter	Description
AddCertificate=<filename> password=<plain text password> Password-enc=<encrypted password>	Specifies a certificate file residing in the subfolder cacerts under the xen folder to load on the nand flash device on platforms with nand flash, or on the memory.

Parameter	Description
	The length of the filename, including the trailing period and the file extension, is limited to 64 characters. This is required when configuring the Citrix Secure Gateway PNAgent Interface (PNAgent/Lite servers) in the Network Setup dialog box. Adding certificates are required if the user CSG environments use certificate agents that are not covered by the built-in certificates. The certificates are used to validate server identities by your zero client. Supported files include .crt file on ICA CSG; .cer and .pfx in 802.1x. password and Password-enc are used for .pfx files.
AddCertificate=client cert.pfx password=passpass	The Caradigm Vault server uses the certificate to validate the connection between the Tap Server and the zero client. Use this INI parameter certificate to Zero Client.
AdminMode={yes, no} [admin-username=<encrypted_username>] [admin-password=<encrypted_password>] [Username=<username>] [Password=<password>] [ShowAdmin]={yes, no} [Enc-username=encrypted_username] [Enc-password=encrypted_password] [ShowAESButton={yes, no}]	**Default is no.** **AdminMode** — Yes/no option to use the username and the password to obtain a high privilege zero client configuration when the Privilege parameter level is set to high (Privilege=high). **admin-username** — Specifies if admin-username=encrypted_username, then encrypted strings are used for admin-username, no minimum length; maximum length is 30 characters—15 characters convert to 30 characters encrypted. **admin-password** — Specifies if admin-password=encrypted_password, then encrypted strings are used for admin-password, no minimum length; maximum length is 30 characters—15 characters convert to 30 characters encrypted. **Enc-username** — Specifies if the username is encrypted, and encrypted strings are used for the Enc-username. **Enc-password** — Specifies if the password is encrypted, and encrypted strings are used for the Enc-password. **IMPORTANT:** · **Enc-password** — Specifies if the password is encrypted, and encrypted strings are used for the Enc-password. · **password** — Specifies the password, no minimum length; maximum length is 15 characters. **ShowAESButton=yes**—In this option **AES Encrypt** button populates in **System Admin**, when user enters the administrator mode. Click **AES Encrypt** to launch encrypted generator to generate enc-password for INI settings. You can hide AES Encrypt if **ShowAESButton=no**. If Enc-Username and Enc-Password is presented, the default value is **yes**. Otherwise, the default value is **no**.
AutoLoad=[0, 1, 2, 101, 102, 201, 202] [LoadPkg={0, 1, 2}] [AddPkg={pkg1_name, pkg2_name, ...}] [DelPkg={pkg1_name, pkg2_name, ...}] [VerifySignature={yes,no}] [UpgradeOrder=(bios,wtos)]	**Default is 1.** Specifies the firmware update mode. **0** — Disable checking for image. **1** — (Default) Enable a forced firmware upgrade/downgrade process. **2** — Enable a comparison/non-forced upgrade only process. **101** — Enable firmware upgrade/downgrade process, but have a popup message that identifies the firmware version, and then prompts with OK and Cancel buttons appearing before the process; completion message appears after process.

Parameter	Description
	102 — Enable upgrade only, but have a popup message that identifies the firmware version, and then prompts with OK and Cancel buttons appearing before the process; completion message appears after process. **201** — Enable a forced firmware upgrade/downgrade process, but have a popup message with OK button appearing before process although process will begin in 20 seconds in any case; completion message appears after process. **202** — Enable a comparison/non-forced upgrade only process, but have a popup message with OK and Cancel buttons appearing before the process; completion message appears after process. The option LoadPkg specifies how to update the external packages. If set to 0, this disables checking for packages. If set to 1 it enable packages upgrade/downgrade process, and if set to 2, it enables upgrade only. If LoadPkg is not in the statement, it will inherit the value of AutoLoad. For example, if the value is 0, and if AutoLoad=0, 1, and if AutoLoad=1, 101 or 201, and 2 if AutoLoad=2, 102 or 202.For example, if you set AutoLoad=1 LoadPkg=0, the firmware is checked, but the packages are not checked. From ThinOS Lite 2.3, the external packages update mechanism is changed. Some packages are default, and loaded according to value of LoadPkg. For example RTME. Some packages need additional parameter AddPkg to add. For example, FR and TCX.The option AddPkg is for adding packages. It depends on the value of LoadPkg. The packages check comes after firmware check.The option DelPkg is for deleting packages. It does not depend on the value of LoadPkg. The packages specified in DelPkg are always deleted when loading the ini file.The value of AddPkg and DelPkg is one package name or a package name list. For example, AutoLoad=1 AddPkg="FR, TCX" DelPkg=RTME. **NOTE: The AddPkg and DelPkg options depend on platforms which supports external packages. So far only Z/D and U class support it. The other legacy platforms does not support it.** The option VerifySignature specifies to verify the signature or not when updating the firmware and/or packages. It is introduced in ThinOS Lite 2.4 and above versions to make sure the security and integrity of the firmware and packages. If you set VerifySignature to no, it will not check the signature so that theo that the downgrade of the firmware and/or packages can happen which did not support signature. The default value is yes. The option UpgradeOrder is a control mechanism to enable BIOS and firmware upgrade in a specific order. If parameter is set to no, the default order is set to upgrade ThinOS firmware first, and then the BIOS. For the parameter UpgradeOrder you can set a single entity to upgrade or a list in order, (support value—bios and wtos) Example: AutoLoad=1 UpgradeOrder=bios Upgrades only the BIOS AutoLoad=1 UpgradeOrder=bios,wtos Upgrades BIOS first, then the ThinOS firmware AutoLoad=1 UpgradeOrder=wtos,bios Upgrades ThinOS firmware first, then the BIOS AutoLoad=1 UpgradeOrder=wtos Upgrades only the ThinOS firmware.
AutoSelectSingleCert={yes, no}	Yes/no option to select the single client certificate available.

Parameter	Description
	When HTTPS is configured to verify client certificate, one window pops up for the user to select the client certificate. If only one client certificate is available, set **AutoSelectSingleCert=yes** will not prompt the window and automatically select the client certificate.
AutoSignoff={yes, no, 2-60}	**AutoSignoff** —This option can be used to automatically sign-off a user when the last opened session is closed. The default value is **no**. A value ranging from 2 to 60 can be configured. This value represents the number of seconds a session must be active prior to calling AutoSignOff.
BootpDisable={no, yes}	**Default is no.** Yes/no option to support both DHCP and BOOTP to obtain the network configurations. In the first two tries, only DHCP is requested. Then, both DHCP and BOOTP are requested. For some environments, BOOTP requests will delay obtaining the IP from the DHCP server. Set BootpDisable=yes will only perform a DHCP request. This setting is only valid after the next reboot.

BootOrder={PXE, HardDisk, USB}	**Not supported on ThinOS Lite 2.**
	BootOrder — Sets the boot order for the BIOS. [Intro build 1.5.0_02] The boot order must follow these rules:
	
	1 The boot order is a list of these three options separated by a semi-colon (;)or a comma (,).
	2 Every option must be used.
	3 The options must be different.
	
	For example, the following settings are valid:
	`BootOrder=PXE;HardDisk;USB`
	`BootOrder=HardDisk;PXE;USB`
	`BootOrder=USB;PXE;HardDisk`
	
	However, the following settings are invalid:
	`BootOrder=PXE;HardDisk`
	`BootOrder=PXE;PXE;USB`
	`BootOrder=PXE;HardDisk;USB;PXE`
	
	If the first boot order is not Hard Disk, the system restart will boot from the BIOS setting.

CaradigmServer=vip list [EGPGroup=group name] [EnableLogOff={yes,**no**}] [SecurityMode={default, full, warning, low}] [DisableManualLogon=yes/no]	CaradigmServer=vip list contains a list of VIP addresses with optional TCP port number of Caradigm servers. EGPGroup defines the user group name. If EnableLogOff=yes is specified, the user is logged off from the session before system signs off. Otherwise the session is disconnected. The logged off user has a timeout value which can be set using SessionConfig parameter SessionLogOffTimeout. The default timeout value is 1, if no SessionLogOffTimeout is specified. SecurityMode specifies the SSL certification validation policy.If set to default, it applies the SecurityPolicy setting.If set to full, the SSL connection needs to verify server certificate. If it is untrusted, drop the connection.If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, the default value of the setting is default. DisableManualLogon=yes disables the manually entry of credentials to authenticate into the device. It only allows an already enrolled proximity

Parameter	Description
	badge and in active grace period to authenticate with a single badge tap. The default value is no.
CCMEnable={yes, no} [CCMServer=<server_address>[:port]] [GroupPrefix=<prefix>] [GroupKey=<hashkey>] [MQTTServer=<mqtt_address>[:<mqtt_port>]] [AdvancedConfig={no, yes}] [CCMDefault={no, yes}] [Override={no, yes}] [CAValidation=(yes, no)] [Discover=(yes, no)] [IgnoreMqtt=(yes, no)]	**Default is no.** **CCMEnable** — Yes/no option to enable the Cloud Client Manager **CCMServer** — Specifies a IP address or URL address for the Cloud Client Manager server. Default protocol is HTTPS. If "http://" or "https://" does not exist, default port is 443. Once specified, it is saved in the non-volatile memory. Default port is 80. For example, CCMEnable=yes CCMServer=http://xxx:8080. **GroupPrefix and GroupKey** — The options GroupPrefix and GroupKey compose the group code of the Cloud Client Manager server. Once specified, it is saved in the non-volatile memory. **MQTTServer** — Specifies a IP address or URL address for the MQTT server and MQTT port after the : (colon). Once specified, it is saved in the non-volatile memory. Default MQTT port is 1883. **AdvancedConfig** — **Default is no.** Yes/no option to enable the Cloud Client Manager server and MQTT server fields in the GUI. If AdvancedConfig=yes is specified, the Cloud Client Manager server and MQTT server fields in the Cloud Client Manager UI will be enabled. See also "PRIVILEGE=[None, Low, High] [LockDown= {no, yes}] [HideSysInfo={no, yes}] [HidePPP={no, yes}] [HidePN={no, yes}] [EnableNetworkTest={no, yes}]." **CCMDefault** — **Default is no.** Yes/no option to enable the Configure Cloud management dialog will display during boot up. If CCMDefault=yes is specified and both the CCMServer and GroupKey are NULL, the Configure Cloud management dialog will display during boot up. Input group code to connect to the default Cloud Client Manager server (us1.cloudclientmanager.com) and default MQTT server (us1-pns.cloudclientmanager.com). **Override** — **Default is no.** Yes/no option to allow a groupkey from the INI file to override the previous groupkey. If Override=yes is specified, the groupkey from the INI file will override the previous groupkey. Groupkey priority policy is listed as below: The Groupkey can technically be applied in many places. Below are the different places you can configure the group key in order of priority that is if #1 is defined it will override #2 etc. 1 Local GUI configuration or groupkey received from CCM in a Group Change command 2 Defined in INI file "ccmenable=yes groupkey=xxxx" 3 DHCP Option Tag #199 The Groupkey assigned in DCHP option #199 and INI parameter are only used for "first time deployment" that is they only take effect, if CCM is currently disabled,or if CCM is enabled but group-key is NULL. • If DCHP is defined and CCM is enabled or not NULL: The CCM Group key in the DHCP is ignored since it is configured manually in local UI or from CCM group change. • If INI is defined and CCM is enabled or not NULL: The CCM Group key in the INI is ignored since it is configured manually in local UI or from CCM group change.

Parameter	Description
	NOTE: There is an exception in the logic above when the 'override=yes' option is used in INI file. This will make #2 take priority over #1. For example `CCMEnable=yes CCMServer=xxx:8080 GroupPrefix=wlab GroupKey=TC-TEST-ENG MQTTServer=xxx:1883 AdvancedConfig=yes Override=yes` If IgnoreMqtt=yes is specified, CCM agent will not connect to MQTT server. The default value is no.
Community=community [Encrypt={yes, no}]	Specifies the SNMP community name. A string up to 31 characters is valid. After you specifythe community name, it is saved in the non-volatile memory. If you set the encrypt=yes, an encrypted string is used as a community name. You must use the Windows Password_Gen tool or built-in tool to generate the encrypted string. The default value is set to no.
CustomInfo={yes, no} [Custom1=<custom1_str>] [Custom2=<custom2_str>] [Custom3=<custom3_str>] [Location=<location_str>] [Contact=<contact_str>]	Yes no option to configure/store custom information. If CustomInfo=yes, the custom information configured by the following options will be stored into NVRAM. If CustomInfo=no, the custom information in NVRAM will be cleared. For example: `CustomInfo=yes custom1=11 custom2=2 custom3=3 location=contact=peter`
DefaultUser={username, $SYS_VAR} [Display={yes, no}] [disable={yes/no}]	Specifies the default sign-on user. **Display**—If the value is set to yes, the username field in sign-on window will be displayed. By default the value is set to no and the field will be obscured with asterisks (*). **disable**— If the value is set to yes, the user name field in sign-on window is disabled.
Password=<sign-on password> [disable={yes/no}] [encrypt={no, yes}]	**Password**— Specifies the password as the sign-on password. There is no minimum length. The maximum length is 64 characters. In xen.ini this sets as the default password. The system will sign on automatically and not wait for username, password, and domain entries. **Disable**—If the value is set to yes, the password field in sign-on window is disabled. Default is no. **encrypt** - The default value is no. The options are used to enable or disable an encrypted string for a password in the INI file instead of clear text. If the value is set to yes, the password in the INI is an encrypt string instead of clear text.
Desktop=<bitmap file> [Layout={center, tile, stretch}] [IconTextColor="<rrr ggg bbb>"]	**Desktop** — Specifies a bitmap file to be used as wallpaper for the local desktop. This file could be a 4-bit, 8-bit, or 24-bit BMP file or a standard GIF file or a standard JPEG file. The file must be located in the FTP server xen\bitmap directory. **Default is Wyse wallpaper.** To disable the parameter, leave value blank (Desktop=). When the parameter is set to **Desktop="**, the wallpaper is disabled.

Parameter	Description
	Layout — **Default is stretch.** Specifies the arrangement on the desktop background of the bitmap file specified by the Desktop parameter, if auto dial-up is set, Layout is invalid. • For center, the image is placed in the center of the desktop without image size change. • For tile, the image is replicated across the desktop. • For stretch, the image is modified to fill the desktop. **NOTE:** In dual-monitor mode, the wallpaper is replicated and specified separately for each monitor, instead of being shared by the two monitors. **IconTextColor** — Specifies the icon text color in RGB string format, must be enclosed in quotes, where rrr, ggg and bbb are decimal numbers in the range of 0 to 255.
DesktopColorDepth={16, 32}	**Default is 32.** **DesktopColorDepth** — Sets the desktop color to 16 or 32 bits.
Device=audio volume={low, middle, high} or {0 to 25} mute={0, 1, 2, 3} [mic_vol={high, middle, low} or {0-25}] [mic_mute={yes, no}] [mic_boost={yes, no, 1, 2, 3, 4}] [min_cache={1-50}] [EnableSpeaker={yes, no}][[playback={device name string}] [record={device name string}] [mic_gain_device={device name string}] [mic_gain={1~8}] [DPaudio={yes, no}] [local_button={yes, no}] [jack_popup={yes, no}]	Specifies the local thin client audio volume. **volume** — Default is **middle**. Specifies the volume level. high — maximum volume middle — medium volume low — minimum volume Values of 0-25 provide more exact volume level **mute** — Default is **0**. Option to enable/disable mute. 0 — no mute 1 — mutes audio 2 — mutes audio and system beep 3 — mutes system beep **mic_vol** — Default is **medium**. Option to set volume levels to high, middle or low. high — maximum volume middle — medium volume low — minimum volume Values of 0-25 provide more exact volume level. **mic_mute** — Default is **no**. no — no mute yes — mutes audio **mic_ boost** — This option increases the mic decibels.

Parameter	Description
	min_cache — Default is **1**. This option is for configuring ThinOS audio playback minimum buffering amount in ten millisecond units. This can be used when network bandwidth is not large enough to play audio smoothly. In such cases, set min_cache higher, so that ThinOS will buffer more audio data before playing the audio. 1 – ThinOS will buffer at least 10 ms of audio data when playing audio. 50 – ThinOS will buffer at least 500 ms (0.5s) of audio data when playing audio. **EnableSpeaker** — Default is **yes**. Yes/no option to enable the internal loud speaker. **playback** — You can set a playback device name. **record** — You can set the record device name. **mic_gain_device**— Specify the device name on which you want the mic gain. **mic_gain**—Enhances the mic gain by number of times the specified value. The default value is 1. **DPaudio=[yes, no]**— The default option is DPaudio=yes. DP audio may impact display on A10Q with certain screen resolutions such as 1920x1200, 2048x1152, 2048x1280, 2560x1080, 2560x1440 (U2718Q, UP3216Q) however not limited. User needs to disable DP audio using INI or GUI. This setting only works for terminals with DP audio support (A10Q, D10Q, and U10). **local_button=[yes, no]** The default option is yes, if the value is no, the mute/volume up/volume down buttons are disabled in ThinOS local, but it works during session **jack_popup**— The default option of jack_popup is **yes**. If the jack_popup is set to **no**, jack selection message display is disabled when the jack headset is plugged in.
Device=camera [format=raw] [width={camera supported width}] [height={camera supported height}] [fps={camera supported fps}] [samplerate={0, 1, 2, 3, 4, 5}] [optimize={yes, no}] [Disable={yes, no}] [Default={camera device name}]	Specify the ThinOS Lite local camera settings. **format** — Support only for raw video type; format=raw is fixed. **width** — The width of the resolution that the local camera supports. **height** — The height of the resolution that the local camera supports. **fps** — The frame per second (fps) of the resolution that the local camera supports. **samplerate** — The software level sample rate based on fps to optimize the performance, where the frame per second for the camera is actually equal to the fps value multiplied by the samplerate value. Samplerate values mean the following sample rates: 0 — 1/1 1 — 1/2 2 — 1/3

Parameter	Description
	3 — 1/4 4 — 1/5 5 — 1/6 **optimize** — Default is **no**. Yes/ no option to optimize the width, height, and fps at 320 x 240 at 10 fps. That is, if optimize=yes, then 320 x 240 at 10 fps will be used for the local camera settings regardless of the individual settings in width, height, and fps; as long as the camera supports the 320 x 240 at 10 fps. If optimize=yes and the camera does not support the 320 x 240 at 10 fps settings, an error will be present in the Event Log of ThinOS Lite. If optimize=no then the individual settings in width, height, and fps will be used as long as the camera supports them. **Disable**— When you specify Disable=yes, the device is disabled. For example, the **Camera** tab in peripherals setting is disabled, the **Exclude video devices** option in Global Connection Settings is disabled. The device cannot be accessed at local and remote sessions. **Default**—Enables you to set the default camera device settings.
Device=cmos [Action={extract, restore}] [Password=password] [encrypt={no, yes}] [BootOrder={PXE, HardDisk, USB}] [WakeOnLan={yes, no}] [AutoPower={yes, no}] [BootFromUSB={yes, no}] [USBController={yes, no}] [COMController={yes, no}] [PopupMenu={yes, no}] [OnboardAudio={yes, no}] [Bluetooth={yes, no}] [CurrentPassword= password NewPassword = password] [AutoPowerDate={yes,no}] [AutoPowerTime={hh:mm:ss} [AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}]	**Not supported on ThinOS Lite 2.0** CMOS management (extract and restore cmos settings). ThinOS Lite (C00X) BIOS version 1.0B_SPC001-0407 or later. ThinOS Lite Pro (R00LX) BIOS version 1.0H_SPC-0T51 or later. For more information, see BIOS Management. **Extract** — For extract action, CMOS content is saved to the file: $PF_cmos.$VER **IMPORTANT:** • $PF — denotes the name of the platform such as C10LE, C00X, R10L, R00LX, and VL10 • $VER — denotes the version of BIOS such as 1.0B_SPC001(1.0B_SPC001-0407), 1.0B-0407(Zilch), 1.0H_SPC-0T51(R10L, R00LX), 1.19R(VL10) **Restore** — For restore action, CMOS content is updated from the file: $PF_cmos.$VER The file is checked thoroughly and protected from corruption 1 The content is wrapped in a file header, including a field of magic number, checksum, timestamp, length and platform name. 2 The content is first checksum and then AES encrypted during save operation. 3 On restore operation, if the CMOS timestamp that is stored in nvram matches the timestamp on the file, the cmos content will not be written every time to avoid wearing out the cmos chip. For usage of this feature, there should be a special INI user name like "cmos". The associated ini/cmos.ini should include one line as "Device=cmos Action=extract". **NOTE: We do not recommend "Device=cmos Action=extract" to be written in global INI file, like xen.ini. This will take no effect, if it is written in global INI file.**

Parameter	Description
	After the administrator configures the CMOS on a template unit, the administrator should sign on to "cmos" account on ThinOS Lite to get the CMOS content saved to the cmos file on writable File Server xen directory. Then the xen.ini must be configured with "Device=CMOS action=restore", so all target units will get updated with the same CMOS setting as template unit after reboot. Once the restore action is finished, both "Device=cmos Action=extract" and "Device=CMOS action=restore" must be removed from the related INI files. The usage of other settings is self-explanatory. If the BIOS GUI has respective feature settings, then user can use these INI parameters to configure those settings. **[CurrentPassword= password NewPassword = password]**—This option is used to change the device BIOS password. CurrenPassword is required. The maximum count of the password string is 19 bytes. **[AutoPowerDate={yes,no}]**— This option is used to enable the system to turn on automatically on a scheduled time and day. If the value specified is no, the system does not turn on automatically. If the value specified is yes, the system turns on automatically at the time specified in AutoPowerTime and AutoPowerDays. **AutoPowerTime**—This option specifies the time for the system to turn on automatically. The value range for hh is 0 - 23 and the range for mm and ss is 0 - 59. **AutoPowerDays**—This option specifies the day to turn on the system automatically. For example, Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday;Saturday
Device=keyboard [numlockoff={no, yes}] [repeatrate={0, 1, 2}] [repeatdelay={0, 1, 2, 3, 4, 5, 6, 7}] [disabledKeys={PrtScn;SysRq}]	**Device**—Specifies the local keyboard.numlockoff — Default is no. Yes/no option to turn off the NumLock of the keyboard.repeatrate — Default is 1. Specifies the keyboard repeat rate. 0 — Slow 1 — Medium 2 — Fastrepeatdelay — Default is 2. Specifies the keyboard delay in seconds, before repeat. 0 — 1/5 1 — 1/4 2 — 1/3 3 — 1/2 4 — 3/4 5 — 1 6 — 2 7 — No Repeat

Parameter	Description
	NOTE: These settings are saved into NVRAM if EnableLocal is set to yes in the xen.ini file. **disabledKeys=PrtScn;SysRq**—You can use this parameter to disable keys in the keyboard. Use semicolon (;) to separate each key. Currently, only Prtscn and SysRq keys are supported.
Device=UsbTrace vid_pid={device vid/pin hex format} [max_len=500]	Specify the ThinOS Lite to trace USB device data to ftp or USB disk. For "vid_pid", that is, device Vendor ID and Product ID hex value, the VID is high 16 bit while Product ID is low 16 bit. This allows to trace maximum of 8 devices at one time. For "max_len", set a max len for capturing each USB transfer data. The default value is 128. After the user sets this, the user needs set option in Trouble shooting to start tracing the USB device data.
Device=Rfideas [DisableBeep={yes,no}] [DisableKeyStroke={yes,no}] [SetCardType={yes,no} Configuration1={*} Configuration2={*}] [DisableInitialization={yes,no}] [DisableLed={yes,no}]	Device=Rfideas — Specifies the local Rfideas readers. DisableBeep — Default is yes. Option disables the beep sound when the card is read. DisableKeyStroke — Default is yes. Option disables the keyboard movements and key strokes. SetCardType — Default is no. Used only for pcProx Plug readers. If set to yes, then the Configuration #1 initializes to HID Prox 608x compatibility and Configuration #2 initializes to RDR-758x Equivalent. If set to no, then the card type remains unchanged. DisableInitialization — Default is no. Option disables configurations to the card reader.
Device=mtouch [mult_touch={yes, no}] [mult_jitter={5-50}]	This parameter specifies the ThinOS multi-touch Monitor setting. For **mult-touch**, if the value is set as yes, multi-touch is supported. If the values is set as no, multi touch is not supported. The default value is yes. For **mult-jitter**, choose larger value if you prefer single click. Choose smaller value to have better user experience. The default value is 30.
DHCPOptionsRemap={yes, no} [DisableOption12={yes, no}] [FileServer={128-254}] [RootPath={128-254}] [FtpUserName={128-254}] [FtpPassWord={128-254}] [RapportServer={128-254}] [RapportPort={128-254}] [WDMServer={128-254}]	Default is **no.** **DHCPOptionsRemap** — Specifies whether or not the following options can be set. The value for each option must be from 128 to 254. Values for the options must be different for each option. These options are used to configure DHCP server tags for zero client booting. The option DisableOption12 sets if the option tag 12 in DHCP is accepted or not. As default, DHCP option 12 sets the hostname and domain name of the terminal. For example, the information of option 12 is terminal name.wyse.com, the terminal name will be set as terminalname and the domain name will be set as wyse.com. If you set different value for DisableOption12 from the value in NVRAM, the system will automatically reboot to make the value valid. (CIR36891)

Parameter	Description
[WDMPort={128-254}] [PnliteServer={128-254}] [DomainList={128 -254}] [VDIBroker={128-254}] [RapportSecurePort={128-254}] [Discover={yes, no}] [WDMSecurePort={128-254}] [WDMFQDN={128-254}] [CCMGroupKey={128-254}] [CCMServer={128-254}] [CCMMQTTServer={128-254}] [CCMCAValidation={128-254}]	**RapportSecurePort**— Specifies the HTTPS port of WDM server. It is in 6.3 to support WDM4.7. **Discover**—If Discover=yes, the device fetches Wyse DHCP options from DHCP server, otherwise, it prevents the device from fetching those information. Default value is yes. If the device receives FileServer/ WDMServer information through the DHCP server, then the associate User interface is protected. **NOTE:** WDMSecurePort is the specified HTTPS port of the WDM server. **WDMSecurePort**—Specifies the HTTPS port of WDM server. **WDMFQDN** — Specifies the Fully Qualified Domain Name (FQDN) of the WDM server. **NOTE: The CCMGroupKey, CCMServer and CCMMQTTServer options are specified to remap the tags for CCM configuration.** **NOTE:** • WDMServer (186) specifies ip address of WDM server. • WDMServer (192) specifies HTTP port of WDM server. • WDMSecurePort (190) specifies HTTPS port of WDM server. • WDMFQDN (194) specifies the FQDN of WDM server. • CCMGroupKey (199), CCMServer (165), CCMMQTTServer (166) and CCMCAValidation (167) specify to remap the tags for CCM configuration.
Device=Ethernet [Speed={Auto, 10M HD, 10M FD, 100M HD, 100M FD, or 1000M} [MTU=mtu] [KeepAlive={5-600}] [Warning={no, yes}] [StaticIPWaitFileServer={0-255}] [WirelessWaitEnet={1-60}]	**Device** — Specifies to use an ethernet. **Speed** — **Default is auto.** Specifies the ethernet speed to either Auto, 10M HD, 10M FD, 100M HD, 100M FD, or 1000M. If Speed is set in a xen.ini file, the Speed statement in the {username}.ini file will be disabled. **NOTE:** Device and Speed parameters can be replaced by the EthernetSpeed parameter. **MTU** — A maximum transmission unit value between 500 to 1500. **KeepAlive** — Specifies a time value in seconds between 5 and 600, to keep an idle connection alive. **Warning** — **Default is no.** Yes/no option to warn about an idle connection. In the seconds of the specified KeepAlive, if the tcp connection is idle and Warning=yes, one log will be printed for the session. For example: device=ethernet keepalive=20 warning=yes **StaticIPWaitFileServer** — **Default is 0.** Specifies the timeout threshold in seconds for cases of static IP. Note that the default 0 turns off this parameter and will allow the system to wait the system default 120 seconds. **CAUTION: If the Speed parameter value is changed, the client will require a reboot.**

Parameter	Description
	WirelessWaitEnet—This option specifies the wait period before the wireless initializes in case of Enet Up. The default value is 5.
Device=vusb [ForceRedirect=DeviceID] [ForceLocal=DeviceID] [Type={TCX, HDX}] [InterfaceRedirect={no, yes}]	**Device** — Specifies the ID of a local USB device that is not redirected by default. **ForceRedirect** — Specifies a forced redirect of the local USB device to the server. This parameter has priority over ForceLocal. The DeviceID can be found in the event log. For example, if you find "TCX USB: Local Device(0x04f2,0x0112,0x03,0x01,0x01)", set the parameter as: `Device=vusb ForceRedirect=0x04f2,0x0112,0x03,0x01,0x01` **Type** — (**Citrix Environments Only**) In Citrix environments, allows you to force the usage of HDX for USB virtualization instead of TCX. For example: Device=vusb Type=HDX **NOTE: To use the TCX option, TCX Suite must be install on the target server.** **InterfaceRedirect**— **Default is no.** Yes/no option to enable part of a composite device to run locally and part of the device to run on a remote session.
Device=Wireless [Mode={Infrastructure, AdHoc}] [SSID=ssid Channel={1-14}] [WepKey={None, 1-4}] [Key1=<k1>] [Key2=<k2>] [Key3=<k3>] [Key4=<k4>] [Key1Enc=<key1 encrypted>] [Key2Enc=<key2 encrypted>] [Key3Enc=<key3 encrypted>] [Key4Enc=<key4 encrypted>] [RoamSensitive={high, medium, low}] [Algorithm={Open, SharedKey}] [DisableBand={None, 2.4G, 5G}] [PreferBand={None, 2.4G, 5G}] [Priority=ssid_list] [DisableN={yes,no}] [DisableWlan={yes, no, EnetUp}	**Device** — Defines the wireless Ethernet device remotely and saves to the local NVRAM. Not all options are needed. For example, you can define Key1 to have a key of "k1" and leave out Key2 through Key4. **WEPKey** — **Default is None**. k1 to k4 are any real values of 5 to 13 characters or 10 to 26 Hex digits. Encrypted keys will overwrite unencrypted keys. Thus, if Key1 and Key1Enc are both configured, then Key1Enc will overwrite Key1. RoamSensitive — defines the sensitivity level of wireless roaming with respect to launching the Roaming daemon: high - signal lower than -60 dBm medium - signal lower than -70 dBm low - signal lower than -80dBm The RoamSensitive parameter is also used to enable wireless roaming. If it is not configured in the INI file, roaming will never be launched even if the signal is lower than -80dbm, unless it totally loses a wireless signal. **Algorithm** — specifies the authentication method of WEP between your zero client and the access point. If set to Open, open authentication will be selected. If set to ShareKey, shared key authentication will be selected. Algorithm=open wepkey={1,2,3,4} means open along with wep for wireless connection(Access typein GUI is displayed as Open(WEP)), while Algorithm=open wepkey=none means open.(Access type in GUI is displayed as Open) **DisableBand** — **Default is None.** Used to disable 2.4G or 5G 802.11 band. **Preferband**—**Default is none** Used to set the prioprity of wireless connection band, and select the 2.4G or 5G access point to connect. **Priority** — sets the priority of wireless profiles. The ssid list is separated by a semicolon or comma and the priority is from high to low. **DisableN** Used to disable 802.11n mode, and it is enabled by default.

Parameter	Description
	DisableWlan—Used to disable wireless. If DisableWlan=EnetUp, and the ethernet is on while booting, the wireless connection is disabled. For example, Device=Wireless Mode=Infrastructure SSID=ThinIsInIEEE8021X=yes network=wireless profile=ThinIsIn access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 Device=Wireless Mode=Infrastructure SSID=ThinOS Lite_95 roamsensitive=highIEEE8021X=yes network=wireless profile=ThinOS Lite_95 access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 Device=Wireless Mode=Infrastructure SSID=ThinOS Lite_11nIEEE8021X=yes network=wireless profile=ThinOS Lite_11n access=WPA2-PSK wpa2pskpwd=2wsx3edc Device=Wireless Priority="ThinOS Lite_11n,ThinOS Lite_95,ThinIsIn"
DEVICE_SECURITY=white_list/black_list vid_pid=[vvvv,pppp] class=name/[cc,ss,pp]	• When DEVICE_SECURITY=white_list is set, the security is in high level, and you need to add all the devices (on board devices including T10D's netcard, and internal hub) to the list that you want to use, and all other devices are denied when the device is plugged-in. • When DEVICE_SECURITY=black_list is set, the security is mid-level, and customer can add the device which is not present in the list. • About key value: all the value are hex, and vid_pid = 0xvvvvpppp, class value is =0xccsspp; where – vvvv=device vendor id – pppp=device product id – cc= device interface class – ss=device interface subclass – pp=device interface protocol • Class name is abbreviation for the defined class. Valid names are listed below: {Audio, CDC_control, HID, Pysical, Image, MASS_STORAGE, Hub, CDC_Data, Smart_Card, Content_Security, Video, Personal_Healthcare, AudioVideo, Billboard, Diagnostic_Device, Wireless, Miscellaneous, Application, VendorSpecific}. For detailed information, refer: www.usb.org/developers/defined_class • The max number of devices/class table is 16. Example: DEVICE_SECURITY=white_list class=HID class=Audio class=Video DEVICE_SECURITY=black_list vid_pid=0x0B0E2000 class=0x030101
DisableDomain={no, yes}	**Default is no.** Yes/no option to disable the drop-down domain list in the PNAgent/ PNLite Sign-on dialog box.
DNSIPVersion={ipv4, ipv6} [DNSServer=<server_list>] [DNSDomain=<dns_domain_url>] [Combined={yes,**no**}]	**Default is ipv4.** Specifies the DNS server and domain. Default IP version is ipv4. [Intro build 1.7_122] The DNSServer is an IP list separated by ";" or ",", max size of this list is

Parameter	Description
	If you set Combined=yes, the DNS server will combine the DNS server configured by DHCP and the static one. The DNS domain will use the value configured by DHCP in case the static DNS domain is empty.
DomainList=<List of NT domain names> [disable={yes/no}]	A list of domain names that will appear in the **Log on** dialog box as options to help users in selecting the domain to sign-on to PNAgent/ PNLite servers. Once specified, it is saved in non-volatile memory. **NOTE: Be sure to enclose in quotation marks if spaces are included.** For example: DomainList="North_America, SQA, test-domain" disable— If the value is set to yes, the domain field in sign-on window is disabled.
Dualhead={no, yes} [ManualOverride={yes, no}] [Mainscreen={1, 2}] [Orientation={hort, vert}] [Align={Top, Center, Bottom}] [MonitorAutoDetect={yes,no}] [EnsureDpIsOn ={yes, no}]	**Default is no.** **Dualhead** — Yes/no option to support a dual-monitor display. **CAUTION: If Dualhead is changed to yes, your zero client will require a reboot to change the monitor display.** **ManualOverride** — Yes/no option to have all the parameters only valid in factory default. It is helpful to configure the display setting manually if both single monitor and dual monitor exist in an environment. **Mainscreen** — Sets which screen is used as the main screen. **NOTE: When using a DVI to DVI and VGA cable, the DVI connected monitor will be the default mainscreen=1 in a dual-monitor configuration. When using a zero client with a DP and DVI ports, the DP is Screen 1 and DVI is Screen 2.** **Orientation** — Default is **hort**. Sets which style is used for display. **NOTE: hort means horizontal and vert means vertical.** **Align** — Sets how screens are aligned: · Top means screens are top aligned in "hort" orientation. · Center means screens are center aligned. · Bottom means screens are bottom aligned in "hort" orientation. **MonitorAutoDetect** — Determines whether or not the system will detect how many monitors are connected. If only one monitor is connected, Span mode will be transfered to Mirror mode. The optional keyword EnsureDpIsOn is only used for D-class. When EnsureDpIsOn is set to yes, D-class will halt at boot time until DP monitor is plugged in.
FileServer=<List of IP address or DNS name> [Username=<username>] [Password=<password>] [SecurityMode= {Low, Warning, Full, Default}] [Username-Enc={encrypted_password_string}] [Password-Enc={encrypted_password_string}]	**FileServer** — Specifies the FTP or Web (http://) server IP address or DNS name that is entered into the zero client local setup (non-volatile memory); your zero client immediately uses this server to access files. **Username** — Specifies the username of the file server. **Password** — Specifies the password of the file server. **NOTE: The target file server must support access using the same user credentials used in the INI files.**

Parameter	Description
	The option SecurityMode specifies these security modes. It is only valid when connected to https fileserver, the details of which are shown below: • Client checks the server certificate in the following phases except in Low mode: – Certificate has to have a Valid Date. – Issuer is valid and correct. – Certificate verification should pass. – CN and SAN on cert match DNS naming. • Set SecurityMode=Full to indicate that the client verifies the server's certificate in highest security mode. If any error is detected, client prompts a pop-up box. • Set SecurityMode=Warning to indicate that the client allows continuation if any error is detected. follows SecurityPolicy setting to check the certificate. • Set SecurityMode=Low to indicate that the client allows connection without any certificate verification. • Set SecurityMode=Default to indicate that the client follows SecurityPolicy setting to check certificate. • Default value of the setting is Default. If the settings are factory default or if you are upgrading to ThinOS Lite 2.3 for the first time, the value is temporarily set to None. After loading any INI, it goes to default. • If the security mode value in xen.INI is not the same as the one saved in Client NVRAM, client shows a reboot dialog box. Example: FileServer=https://10.151.122.66:444 SecurityMode=warning **NOTE:** • The sub parameter SecurityMode of FileServer is only validated when the FileServer is set to https:// as its prefix. • When you configure the https file server, the sub parameters Username and Password of FileServer can be omitted. The option **Username-Enc** specifies AES encrypted username of the file server. The option **Password-Enc** specifies AES encrypted password of the file server.

Hosts=<hosts file name>	Specifies the file name of the hosts. This file is a simple text file that associates IP addresses with hostnames, one line per IP address. The length of the file name is limited to 63 characters.
	The file must be placed in file server and can be cached if set MirrorFileServer=yes in the xen.ini. When resolving a host name, the system will initially look in the file and if not found, will search DNS, WINS, and so on. The following is an example of format in the hosts file:
	`10.151.122.1 gateway.ctx.com`
	`10.151.122.123 myvm.ctx.com`

IEEE8021X={yes, no} network={wired, wireless} [Profile=ssid] [access={WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT}]	If IEEE8021X is set to no, then all parameters following it is ignored. If network is not configured, the configuration is ignored. The key left of equal is case sensitive, and the value right of equal case is not case sensitive except for credential information; for example username, password or certificate filename.

Parameter	Description
[eap={yes,no}] [eaptype={None, EAP-LEAP, EAP-TLS, EAP-PEAP,EAP-FAST}] [leapun=<username for EAP-LEAP>] [leappwd=<password for EAP-LEAP>] [leappwdEnc=<password encrypted for EAP-LEAP>] [tlsauthtype=<user or machine>] [tlsclntcert=<client certificate filename for EAP-TLS>] [tlsclntprikeypwd=<password for privatekey>] [tlsclntprikeypwdEnc=<password encrypted for private key>] [peapeap=<EAP-MSCHAPV2, EAP-GTC>] [peapidentity=<identity/username for PEAP>] [peapmschapun=<username for EAP-PEAP/EAP-MSCHAPV2>] [peapmschappwd=<password for EAP-PEAP/EAP-MSCHAPV2>] [peapmschappwdEnc=<password encrypted for EAP-PEAP/ EAP-MSCHAPV2>] [peapmschapdm=<domain for EAP-PEAP/ EAP-MSCHAPV2>] [peapmschaphidedm={yes,no}] [peapsinglesignon={yes, no}] [peapgtcun=<username for EAP-PEAP/ EAP-GTC>] [peapgtcpwd=<password for EAP-PEAP/ EAP-GTC>] [peapgtcpwdEnc=<password for encrypted for EAP-PEAP/ EAP-GTC>] [servervalidate={yes, no}] [servercheck={yes, no}] [servername={"servername for EAP-TLS, EAP-PEAP, EAP-FAST"}] [wpapskpwd=<passphrase for WPA-PSK>] [wpapskpwdEnc=<passphrase encrypted for WPA-PSK>] [wpa2pskpwd=<passphrase for WPA2-PSK>] [wpa2pskpwdEnc=<passphrase encrypted for WPA2-PSK>] [encryption=<TKIP|CCMP>]	If two entries exist in an INI file, one each for wired and wireless, both will take effect; for example IEEE8021X=yes network=wired EAP=yes … IEEE8021X=yes network=wireless access=WPA-ENT … All EAP credential information is stored whatever the eaptype setting. All passwords here should be encrypted. The wildcard server include three entries in INI file. If both the servervalidate entry and severcheck entry are set to yes, the servername entry is valid. Server certificate validation is mandatory in EAP-TLS authentication. If the eaptype entry is set to EAP-TLS, the servercheck entry must be set to yes. Server list must be included in double quotation marks. For example IEEE8021X=yes Network=wireless access=WPA2-ENT eap=yes servervalidate=yes servercheck=yes servername=";test.com;wireless98; test.com" eaptype=eap-peap peapeap=eap-mschapv2 peapmschapun=administrator peapmschappwd=password Additional option timeoutretry specifies the retry times when 8021x authentication times out, which means that it is only validated when the optional network type is wired. For example, timeoutretry=3 allows you to retry thrice after 8021x authentication times out. Additional option Profile specifies the type of ssid authentication to be configured. When we support multiple ssid wireless settings, the statement ieee8021x must be after the statement device=wireless, and one additional profile parameter is needed to identify the type of ssid authentication which is configured. For example,#ThinIsInDevice=Wireless Mode=Infrastructure SSID=ThinIsInIEEE8021X=yes network=wireless profile=ThinIsIn access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 peapmschapdm=wyse#wtos_95Device=Wireless Mode=Infrastructure SSID=wtos_95IEEE8021X=yes network=wireless profile=wtos_95 access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2. Example:IEEE8021X=yes network=wireless access=wpa-ent eap=yes eaptype=eap-tls tlsclntcert=user.cer tlsclntprikey=user.pfx tlsclntprikeypwd=12345678 Or IEEE8021X=yes network=wireless access=wpa-ent eap=yes eaptype=eap-tls tlsclntcert=user.cer tlsclntprikey=user.pfx tlsclntprikeypwd=12345678 leapun=user1 password=1234 peapmschapun=user1 peapmschappwd=12345 peapmschapdm=wyse.com IEEE8021X=yes network=wired eap=yes eaptype=eap-tls tlsclntcert=user.cer tlsclntprikey=user.pfx tlsclntprikeypwd=12345678 By default, peapidentity is same as peapmschapun. If peapmschaphidedm is set to yes, the domain will use saved peap MSCHAP domain name and the prompts dialog will not include the domain field when you perform ieee8021x authentication. The following example describes wildcard server validation: IEEE8021X=yes network=WIRED access=WPA2-ENT servervalidate=yes eap=yes eaptype=EAP-PEAP servercheck=yes servername=w2k8-ACS-64.sqawirelsess.com peapmschapdm=EAP-MSCHAPV2 peapgtcun=sqawirless2 peapmschappwd=123!@#qwe The username of ieee8021x (fastmschapun, peapmschapun, peapgtcun, leapun) can be configured as system variables like $mac, $sn etc. By default, fastidentity is same as fastmschapun.

Parameter	Description
[timeoutretry=<number value of retry times when 8021x authentication timeout>] [fasteap={EAP-MSCHAPV2, EAP-GTC}] [fastidentity={Identity for EAP_FAST}] [fastmschapun={username for EAP-FAST/EAP-MSCHAPV2}] [fastpmschappwd={password for EAP-FAST/EAP-MSCHAPV2}] [fastmschappwdEnc={password encrypted for EAP-FAST/EAP-MSCHAPV2}] [fastmschapdm={domain for EAP-FAST/EAP-MSCHAPV2}] [fastmschaphidedm={yes,no}] [fastsinglesignon={yes, no}] [fastgtcun={username for EAP-FAST/EAP-GTC}] [fastgtcpwd={password for EAP-FAST/EAP-GTC}] [fastgtcpwdEnc={password for encrypted for EAP-FAST/EAP-GTC}] [wiredreset={yes, no}]	If fastmschaphidedm is set to yes, the domain uses saved EAP_FAST MSCHAP domain name, and the prompts dialog does not include the domain field when you perform ieee8021x authentication. The following example describes wildcard server validation:IEEE8021X=yes network=WIRED access=WPA2-ENT servervalidate=yes eap=yes eaptype=EAP-FAST servercheck=yes servername=w2k8-ACS-64.sqawirelsess.com fastmschapdm=EAP-MSCHAPV2 fastgtcun=sqawirless2 fastmschappwd=123!@#qwe The option **wiredreset** is used to reset MII when **authenticate cancel** occurs. This option is only for wired-network and is disabled by default.
INACTIVE = minutes [NoSessionTimer=minutes] [LockTimer=seconds]	**Default is 0.** There is no Idle timeout. The range is 0 minutes to 480 minutes. If the value given is bigger than 480, 480 is set instead. If the value given is smaller than 0, 0 is set instead. When the system idle is time out in the configured minutes, the system will automatically sign off, reboot or shutdown which are based on the setting of AutoSignoff. The parameter NoSessionTimer has the same range as INACTIVE and it is valid only if INACTIVE value is not 0. If there is a session use the value of Inactive, otherwise use the value of NoSessionTimer, if NoSessionTimer is configured. If AutoSignoff=yes Shutdown=yes is configured, then this statement can work before sign on. f the parameter LockTimer is set, the terminal is locked and the system idle is timeout in the configured seconds, system will automatically sign off, reboot or shutdown which are based on the setting of AutoSignoff.
IPProto=ICMP [DisableTStamp={yes, no}] [DisableEcho={yes, no}]	Configures the ICMP protocol. **DisableTStamp** — If DisableTStamp=yes, the system will not reflect the ICMP timestamp (13) request. **DisableEcho** — If DisableEcho=yes, the system will not reflect the ICMP echo (8) request. In this case, the unit cannot be pinged.
KeySequence={no, yes} [Ctrl+Alt+Del={no,yes}]	**Default is yes.**

Parameter	Description
[Ctrl+Alt+Up={no, yes}] [Ctrl+Alt+Down={no, yes}] [Ctrl+Alt+Left={no, yes}] [Ctrl+Alt+Right={no, yes}] [Win+L key={no,yes}] [Alt+Tab={yes,no}]	**keySequence** — Yes/no option to enable the following supported combined keys options • KeySequence=yes enables all of these options, each having a default of yes that you can change individually to no if desired. • KeySequence=no disables all of these options regardless of the individual settings. **Ctrl+Alt+Del** — **Default is no.** Yes/no option to enable use of Ctrl+Alt +Del key to display the windows menu. **Ctrl+Alt+UP**—**Default is yes.** Yes/no option to enable Ctrl+Alt+Up to toggle between task selections. **Ctrl+Alt+Down** —**Default is yes.** Yes/no option to enable Ctrl+Alt+Down to toggle between task selections. **Ctrl+Alt+Left** —**Default is yes.** Yes/no option to enable Ctrl+Alt+Left Arrow to lock the zero client if the user is logged in with a password, if the user is logged in without a password, this key sequence does not work. **Ctrl+Alt+Right** —**Default is yes.** Yes/no option to enable Ctrl+Alt+Right Arrow to lock the zero client if the user is logged in with a password, if the user is logged in without a password, this key sequence does not work. **[Win+L key={no,yes}]** —**Default is no.** Yes/no option to enable use of Win+L key to lock the client. **Alt+Tab**—Default is yes. This option is used for task selection.
Language=code [Charset={ISO-8859-1, ISO-8859-2, ISO-8859-5, ISO-8859-7}] [ImageSuffix={us, fr, de, gb, b5, jp, ko, la, default]	**Default is Us.** **NOTE: The preferred method is to use the Locale parameter as an easy way to support multiple languages instead of this Language parameter.** **Language** — Specifies the keyboard language to use. Once specified in a xen.ini file, it is saved in non-volatile memory. The code used must be exactly the same as the character string shown in the keyboard language list below. **Charset** — **Default is ISO-8859-1.** Specifies which ISO option to use: • ISO-8859-1 — (Default) Supports part 1 of the standard character encoding of the Latin alphabet. • ISO-8859-2 — Supports the Czech, Hungarian, Polish, Romanian, and Slovenian languages on the desktop display. • ISO-8859-5 — Supports Cyrillic characters on the desktop display. • ISO-8859-7 — Supports the Greek language on the desktop display. Keyboard Language List - Description and Code: Arabic (Saudi Arabia) — Ar_sau Arabic (Iraq) — Ar_ira Arabic (Egypt) — Ar_egy Arabic (Libya) — Ar_lib Arabic (Algeria) — Ar_alg

Parameter	Description
	Arabic (Morocco) — Ar_mor Arabic (Tunisia) — Ar_tun Arabic (Oman) — Ar_oma Arabic (Yemen) — Ar_yem Arabic (Syria) — Ar_syr Arabic (Jordan) — Ar_jor Arabic (Lebanon) — Ar_leb Arabic (Kuwait) — Ar_kuw Arabic (U.A.E.) — Ar_uae Arabic (Bahrain) — Ar_bah Arabic (Qatar) — Ar_qat Brazilian — Br Canadian Multilingual — ca_ml Chinese (Simplified) — Gb Chinese (Traditional) — b5 Croatian — Croat Czech — Cz Danish — Dk Dutch — Nl Dutch (Belgian) — Nl_be Dutch (Belgian Comma) — Nl_be_c English (Australian) — Au English (3270 Australian) — au3270 English (New Zealand) — Nz English (United Kingdom) — Uk **English (United States) (default) — Us** Estonian (Estonia)-Et_ee Finnish — Fi French (Belgian) — fr_be French (Belgian Comma) — fr_be_c French (Canadian) — fr_ca French (France) — Fr

Parameter	Description
	French (Swiss) — fr_sf German — De German (IBM) — de_ibm German (Swiss) — de_sg Greek — el Hungarian — Hu Icelandic – Is Italian — It Italian (Swiss) — it142 Japanese — Jp Japanese — Jp_109a Korean — Ko Korean (MS-IME2002) — ko_ime Latvian (Latvia)-lv_lv Latvian (Qwerty)-lv_lv_q Lithuanian (Standard)-lt_lt Lithuanian (IBM)-lt_lt_i Lithuanian (MS)-lt_lt_m Norwegian — No Polish (214) — Pl Polish Programmers — pl_prog Portuguese — Pt Portuguese (Brazil) — Pt2 Romanian — Ro Slovakian — Slovak Slovakian (Qwerty) — sk_q Slovenian — Sloven Spanish — Es Spanish (Mexican) English — La(us) Spanish (Mexican) Localized — La Swedish — Se Turkish — Turk

Parameter	Description
	Turkish (QWERTY) — turk_q U.S. International — us_int **NOTE: Japanese refers to Japanese Input system (MS-IME2000), not JP. Russian keyboard is supported for server input; not local input.** **ImageSuffix** — Localization builds have different suffixes according to the keyboard language as follows Japanese — jp Simplified Chinese — gb Traditional Chinese — b5 Korean — ko Spanish Mexican — la By default, with the above keyboard languages, the system will update the standard image according to the suffixes with the language code. With other keyboard languages, the system will update the standard image without the suffix specified. For example, if you set Language=jp on a ThinOS Lite, the system will update the image named C10_xen.jp which is the Japanese localization build. If you set Language=us on a ThinOS Lite, the system will update the image named C10_xen. The option ImageSuffix can specify the suffix of the image name when you do not want the default behavior.
INACTIVE=minutes [NoSessionTimer=minutes]	Default is 0. There is no Idle timeout. The range is 0 minutes to 480 minutes.If the value given is bigger than 480, 480 is set instead. If the value given is smaller than 0, 0 is set instead. When the system idle is time out in the configured minutes, the system will automatically sign off, reboot or shutdown which are based on the setting of AutoSignoff. The parameter NoSessionTimer has the same range as INACTIVE and it is valid only if INACTIVE value is not 0. If there is a session use the value of Inactive, otherwise use the value of NoSessionTimer, if NoSessionTimer is configured. If "AutoSignoff=yes Shutdown=yes" is configured, then this statement can work before signon.
MMRConfig={VIDEO} [flashingHW={0, 1}]	This parameter specifies whether to show the “HW” label at the top left corner of video or not when HDX is hardware decoded. The default value is 0. Set flashingHW to 0, if you want to hide HW. Set flashingHW to 1, if you want to show HW.
Locale=<value> [load={yes | no}]	Locale — Specifies the system language. **NOTE: Locale changes the language for the user logon-experience screens only, displayed during boot-up and logon and not the configuration or administrator screens.**

Parameter	Description
	Values include: English, us, French, fr, German, de, Chinese Simplified, gb, Chinese Traditional, b5, Japanese, jp, Korean, ko, Latin, la load=yes/no specifies whether or not to load the language file. The language file must end with the locale name and be placed under the folder xen/locale in the file server. For example, if you want to specify French and load the localized messages, you must place a file named French.msg under the folder xen/locale in the file server, and then add Locale=French load=yes in the INI file **NOTE: You can use Local=fr instead of Locale=French.** **IMPORTANT: For Chinese Simplified, Chinese Traditional, Japanese, and Korean localization, a font file must also be placed under the folder xen/font in the file server.** For example, if you want to specify the system language to be Japanese, you must place a file named Japanese.msg under the folder xen/locale in the file server, place a file named Japanese.fnt under the folder xen/font in the file server, and then add Locale=Japanese load=yes in the INI file. If you are under a Dell maintenance contract, you can download .fnt and .msg files from your My Downloads page in the Self-Service Center. For more information, see **"Technical Support"**. If you are not under maintenance and wish to gain access to these files, you must complete a product registration.
LocaleList=<value>	**LocaleList** — Specifies a list of locale, so that a user can switch the system language as needed. Be to place the required files, for example German.msg, Japanese.msg, Japanese.fnt, and so on under the correct folders as described in the Locale parameter description.
Lpdspool={0–50}	Specifies the size of spool to buffer all the data before sending them to the LPD printer. The range of value is 0 to 10. It means 0 MB to 10 MB. If the specified value is over the range, then it is set to 5. The range of value is extended to 50. In build 2.2_001 or after, the LPD data is spooled to a file in a ram disk instead of a buffer. So the value of the parameter will not be related to the spool size as before. If Lpdspool=0, the function is disabled, otherwise the function is enabled.
ManualOverride=[no, yes] [Components={None, display, keyboard, mouse, timezone, network, audio, printer, language, All}]	The parameter **ManualOverride** allows the end users to keep their personalized settings. The default value is **No**. If the value is set to **No**, personalized setting is not allowed. If the value is set to **Yes**, the personalized settings are saved in the device component which can be specified using the **components** option. The parameter **Components** specifies the component that is allowed as a personalized setting. Currently the options supported are None, display, keyboard, mouse, timezone, network, audio, printer, language, all. The default value is **None**.

Parameter	Description
	NOTE: • If the parameter ManualOverride is set, a warning message is displayed when the users try to reset the device to allow them to retain the personalized settings or revert to default settings. The components set using the INI statements are ignored. For example, ManualOverride=Yes Components="display,timezone" This INI statement allows the user to customize display and timezone settings, and these personalized settings are not overridden by wnos.ini after the device restart.
MaxVNCD={0, 1} [VNCD_8bits={yes,no}] [VNCD_Zlib={yes, no}]	**Default is 0.**Option to enable VNC shadowing. Default value is 0 means VNC shadowing is disabled. Set to 1 to enable shadowing. **NOTE: Only one VNC client session is allowed and a password is required.** See also VNCPrompt to enable a VNC shadowing prompt to a user. See also VncPassword to specify a string of up to 8 characters as the password used for shadowing.
OneSignServer=onesign_server [DisableBeep={yes,no}] [KioskMode=yes,no}] [TapToLock={0,1,2}] [EnableWindowAuthentication={yes,no}] [AutoAccess={VMW,XD,XA,LOCAL}] [NetBIOSDomainName={yes,no}] [SuspendAction={0, 1}] [DisableHotKey={yes,no}] Loglevel=0/1/2/3 [DisablePromptToEnroll={**yes**,no}]	A list of host names or IP addresses with optional TCP port number or URLs of Imprivata OneSign servers. It should use https protocol. If OneSignServer="" is defined, then only imprivata virtual channel can work.If DisableBeep is set to yes, then Rfideas reader can be set to mute when a card is tapped. Default is no. If KisokMode is set to yes, then different OneSign user can unlock the client desktop. Default is no. Optional keyword TaptoLock is only active when KioskMode=yes. If TapToLock=0, then tap a card to lock terminal is disabled. If TapToLock=1(Tap to lock), then use the proximity card to lock the terminal. If TapToLock=2(Tap over), then lock the terminal and log in as a different user. Default is 2. If EnableWindowAuthentication is set to yes and OneSign signon fails, then continue to sign-on with windows credential to pre-define broker. Default is yes. If AutoAccess is defined, then auto launch the corresponding type of broker. Otherwise, get the broker type from the Imprivata Server setting of computer and user policy. If none of them is defined, then launch the first available broker server from the Imprivata server. If AutoAccess=LOCAL is set, then launch the broker from the zero client setting; the broker getting from the Imprivata Server is ignored. **NOTE:** • AutoAccess can be set in [username].ini and xen.ini. The xen.ini has priority over [username].ini. If NetBIOSDomainName is set to yes, then Imprivata domain list will show NetBIOS domain name and card user will authenticate to the broker server using NetBIOS domain name. Default is no. If SuspendAction is set to 0, then lock the terminal when you tap the card or press the hotkey. If set to 1, then signoff the terminal. If 'no' is defined, then lock the terminal in KioskMode and sign-off the terminal in none KioskMode.

Parameter	Description
	If DisableHotKey is set to yes, then no action when you press the hotkey defined in Imprivata Server. Only WebAPI 4 and later versions support the hotkey function. Loglevel— While configuring the Imprivata server, user can view the OneSign logs on ThinOS Lite by enabling the Agent Logging feature. An ini configuration is needed correspondingly. Default value is 0. If set to 0, logs are not displayed. If DisablePromptToEnroll is set to yes, then ThinOS does not prompt you to enroll their security answers after OneSign sign-on. Default value is yes.

SelectGroup={yes, no}
 	
[Default=default_desc]
 	
description=group1
 	
[groupname=name1]
 	
[description=group2]
 	
[groupname=name2]
	User can choose the group list from sign-on window to log in.
	
	The description is displayed in the group list box in sign-on window.
	
	The groupname is used to identify the group including the directory and file name.If it is not defined, the description will become the groupname.
	
	The Default option following "SelectGroup=yes" can specify the default group. The value is one of group description defined after that. After the user selects another group and signs off, this default group is selected.
	
	If there is no Default option, the last selected group is selected in the next sign on.
	
	For example,
	`SelectGroup=yes \`
	`  default="Sus team" \`
	`description="Dev team" groupname=dev \`
	`  description="Sus team" \`
	`description="SQA team" groupname=sqa \`
	`  description="guest"`
	
	1 **Group 1 :** Description="Dev team" groupname=dev. The file \xen\ini \dev\dev.ini needs to be created in the file server. In the dev.ini, the broker, domain list or connections can be defined for dev team.
	2 **Group 2 :** Description="Sus team" . The file \xen\ini\Sus team\Sus team.ini needs to be created in the file server. In the Sus team.ini, the broker, broker list or connections can be defined for Sus team.
	
	After the user selects the group, the system will load the group ini file at first, and then load the \xen\ini\{group_name}\username.ini.If the username.ini in the group directory is not found, the system will try to load \xen\ini\username.ini as before.
	
	If SelectGroup=yes, the Select Server List statement is invalid because the group list may define different brokers.

SelectServerList= {PNA, VDI} [Default=default_desc] list of servers {Server1 Server2 ServerN} SelectServerList= {PNA, VDI}; list of servers {Server1; Server2; ServerN}	User can choose one PNA or VDI server from sign-on window to log in. This format must be used in newer build. For server's format: description = <server's description> host = <server's url> [<options>]. **NOTE:** 1 There must be "description" and "host" key words on each server. 2 For PNA Server: about "options", please reference the options of parameter "PnliteServer". 3 For VDI Server: If user wants to use VDM VDI broker, please specify "ConnectionBroker=VDM "in xen.ini. About "options", refer the options of parameter "VDIBroker".

Parameter	Description
	The default option following "SelectServerList={PNA, VDI}" specifies the default server. The value is one of the server description defined. After the user selects different server and signs off, this default server is selected. If there is no default option, the last selected server is selected in the next sign on. The Default option following "SelectServerList={PNA, VDI}" can specify the default server. The value is one of server description defined after that. After one selects another server and sign off, this default server will be selected.If no Default option, the last selected server will be selected in the next sign on. For Example: 1 For PNA: SelectServerList=PNA Default=test3 description = test1 host = 192.168.0.10 autoconnectlist =* reconnectfrombutton=0 description = test2 host = HostName2.wyse.com TimeOut=200 descriprion = test3 host = https://server3.wyse.com 2 For VDM: ConnectionBroker=VDM SelectServerList=VDI Default=test5 description = test4 host = 192.168.0.11 description = test5 host = host2.wyse.com
MicBoost={no, yes}	**Default is no.** Yes/no option to enable on-board microphone boost. [Intro build 1.5.0_02]
MirrorFileServer={no, yes}	**Default is no.** Yes/no option to enable the cache all server files functionality. Cache all server files such as INI files, wallpaper, bitmap, font, local messages and so on to the local flash when files are changed in the file server. The device would use the cached files when files on the file server are unavailable. **NOTE:** • Not supported on ThinOS Lite 2 • With ThinOS Lite 1.7 build or later, the original function of the ini cache is discarded and the mirror file server replaces it. **NOTE:** For ThinOS Lite 2, use the depreicated EnableCacheIni parameter to locally cache the xen.ini ONLY. EnableCacheIni={no, yes}. Default is no.
MultiLogon={no, yes}	**Default is no.** Yes/no option to support multiple log ons. If MultiLogon=yes, the PNAgent/PNLite sign-on authenticating window can input a different username, password, and domain while signing on to different PNAgent/PNLite servers. For backward compatibility, the following format is supported: MultiLogon=yes PNAgentServer=10.1.1.30;10.2.2.60

Parameter	Description

	The SelectServerList statement is also supported:
	`MultiLogon=yes`
	`SelectServerList=pna \`
	`description=store host=http://proper-storefront-url.ctx.com`
	`description="Floor 3" host=10.1.1.30 \`
	`description=""Floor 1" host=10.2.2.60 \`
	`description="All Users" host=10.3.3.90`
	
	NOTE:
	The Select Server List takes precedence over PNAgentServer.
	
	The PNA server description or name can be displayed on the signon window so that the user knows which and what server is logging on.

NoReducer={no, yes} [Encryption={Basic, 40, 56, 128, Login-128, None}]	**Default is no.** **NoReducer** — Yes/no option to turn off compression. Default is no, which enables compression. To turn off compression, enter yes. Used here this parameter is a global statement for all connections. It sets the default value of NoReducer. **NOTE: By default the ICA protocol compresses its data to minimize the amount of data that needs to traverse the network. This compression can be as much as 50% for text-based applications such as Microsoft Word and 40% less for graphics applications than the uncompressed data streams.** **Encryption** — (**Citrix Environments Only**) **Default is Basic.** Specifies the default setting of encryption level for all ICA connections. The highest level is 128-bit security. The lowest is Basic.
NoticeFile=filename [Resizable={no, yes}] [Timeout={0, 10 to 600}] [Title="notice_title"] [ButtonCaption="button_caption"]	**NoticeFile** — Specifies a legal notification file residing in the home directory folder. The file is displayed in a dialog box and the user is prompted to accept it before the sign-on process continues. **Resizable** — Default is **no**. Yes/no option to resize the dialog box to fit the text size. **Timeout** — Default is **0**. After the notice is accepted, if Timeout is specified in seconds, and if no mouse or keyboard is used, then the dialog box will display again after the seconds set. 0 means no timeout. **Title and ButtonCaption** — Specifies the notification window title and button that can be customized. For example, `NoticeFile=filename Title=Problem ButtonCaption=Ok`
OneSignServer=onesign_server [DisableBeep={no, yes} [KioskMode={no, yes}] [EnableFUS={no, yes}] [TapToLock={0, 1, 2}] [EnableWindowAuthentication={yes,no}] [AutoAccess={VMW,XD,XA}] [NetBIOSDomainName={no, yes}]	Specifies a list of host names or IP addresses with optional TCP port number or URLs of Imprivata OneSign servers. **IMPORTANT: An https protocol must be used.** OneSign virtual desktop access offers a seamless authentication experience and can be combined with single sign-on for no click access to desktops and applications in a virtual desktop environment. The following inputs are acceptable values: https://ip or

Parameter	Description
	https://FQDN **DisableBeep** — Default is **no**. Yes/no option to set the Rfideas reader to mute when a card is tapped. **KisokMode** — Default is **no**. Yes/no option to allow the OneSign user to share the client desktop. **EnableFUS** — Default is **no**. Yes/no option to set the Citrix client to remain running when switch users. **TaptoLock** — Default is **2**. Only active when KioskMode=yes. Specifies tap to lock. If TapToLock=0, then tap a card to lock terminal is disabled. If TapToLock=1 (Tap to lock), then use the proximity card to lock the terminal. If TapToLock=2 (Tap over), then lock the terminal and log in a different user. **EnableWindowAuthentication** — Default is **yes**. Yes/no option to sign-on with the user's Windows credentials to pre-defined broker if the OneSign sign-on fails. **AutoAccess** — Specifies the corresponding type of broker to automatically start. If not defined, the broker type is obtained from the Imprivata Server setting of the computer and user policy. If none of them is defined, then the first available broker server from the Imprivata server is started. **NOTE:** AutoAccess can be set in [username].ini and xen.ini, however, the xen.ini, has priority over [username].ini. **NetBIOSDomainName** — Default is **no**. Yes/no option to enable the authentication to the broker server using the NetBIOS domain name. If set to yes, the Imprivata domain list will show NetBIOS domain name and the card user will authenticate to the broker server using the NetBIOS domain.
PasswordServer=<password_server> [AccountSelfService={no, yes}] [connect=<ica sever>] [encryption={Basic, 40, 56, 128, Login-128, None}]	**PasswordServer** — (**Citrix Environments Only**) Specifies the IP Address of the password server (which can be defined as an Account Self Service server (AccountSelfService=yes) or a direct connection (connect=) - if no option is specified, it will connect with the ICA protocol). **AccountSelfService** — **Default is no.** Yes/no option to define the password server as an Account Self Service server. AccountSelfService=yes also displays the Account Self-Service icon on the Log on dialog box. If AccountSelfService=yes option follows the PasswordServer parameter, the password server specified will be defined as the account self-service server and the connect option will be invalid. **connect** — Defines the password server as a direct connection to an ICA server that can be logged on to modify a password for a user sign-on with a password timeout. An encryption option can also be set for this direct connection.
PlatformConfig=all [EncryptFS=yes]	Encrypts local flash, specifically cached INI files and credentials that are stored, if using signon=yes.

Parameter	Description
	NOTE: Event log will display new statements stating that FileSystem encryption has been enabled.
PnliteServer=<List of {IP address, DNS names, or URLs} > [ReconnectAtLogon={0, 1, 2}] [ReconnectFromButton={0, 1, 2}] [AutoConnectList={*/ appname1;appname2; appname3...}] [Timeout=5...300] [CAGRSAAuthMethod={LDAP, RSA}] [CAGAuthMethod={LDAP, RSA, LDAP+RSA, RSA+LDAP}] [RequestIconDataCount={0-65535}] [DefaultSettings={XenApp, XenDesktop}] [SmartcardPassthrough={yes, no}] [StoreFront={no, yes}] [HttpUserAgent={UserAgent}] [CAGSendDomain= {yes, no}] [IgnoreDefaultGateway={yes, no}] [CAGUserAsUPN={yes, no}] [CAGExternal={yes, no}] [DisableSFInit={yes, no}]	**PnliteServer**—Specifies the list of IP addresses or host names with optional TCP port number or URLs of PNAgent/PNLite servers. The list is empty by default. Each entry with optional port is specified as Name-or-IP:port, where port is optional; if not specified, port 80 is used as the default. If a port other than 80 is used, the port number must be specified explicitly with the server location in the form IP:port or name:port. Once specified, it is saved in the non-volatile memory. The statement PNAgentServer and Web interface for Citrix MetaFrame Server is equal to this statement. **NOTE:** PnliteServer and the DomainList parameters can be used in a {username}.ini file, but generally are used only in a xen.ini file. The PNAgent/PNLite server list and associated domain list optionally can be entered in DHCP server options 181 and 182, respectively. If entered in both places, the entries from the **Connection Settings: xen.ini files, {username} INI, and $MAC INI Files** section will take precedence. However, the {username}.ini file will override the xen.ini file if the identical parameters with different values exist in the {username}.ini file. **NOTE:** When Multifarm=yes, use # to separate failover servers, and use a comma (,) or a semicolon (;) to separate servers that belong to different farms. **ReconnectAtLogon** — Specifies the reconnection function at log in. Default is **0** — disables the option. 1 — reconnects to disconnected sessions only. 2 — reconnects to active and disconnected sessions. **ReconnectFromButton** — Specifies the reconnection function from the reconnect command button. Default is **0** — disables the option. 1 — reconnects to disconnected sessions only. 2 — reconnects to active and disconnected sessions. **AutoConnectList** — Specifies the PNA applications that will be automatically started when using PNA to sign on. If AutoConnectList=*, then all the PNA applications will be automatically connected. The autoconnectlist is the connection description of application or host name which can use the wildcard * to match the string. **IMPORTANT: Appname values are case sensitive.**

Parameter	Description
	Timeout — Specifies the time in seconds where a client will try to establish a connection before reporting that it is unreachable. **CAGRSAAuthMethod** or **CAGAuthMethod** — CAGAuthMethod option is used for CAG authentication configuration. **NOTE: This option replaces CAGRSAAuthMethod. If CAGAuthMethod=RSA which is same as the prior CAGRSAAuthMethod=RSASecurid, an extra passcode field needs to be input except username/password/domain. If CAGAuthMethod=LDAP, no passcode field is needed.** • CAGAuthMethod={LDAP+RSA, RSA+LDAP} — Used for CAG authentication configuration. • If CAGAuthMethod = LDAP+RSA, an extra passcode field needs to be input except username/password/domain. If the CAG server is configured for a double authentication policy, this ini corresponds to the first auth LDAP and second auth RSA. • If CAGAuthMethod = RSA+LDAP, it has the same result with CAGAuthMethod = RSA, compared to LDAP+RSA. If CAG server configure double authentication policy, this ini correspond to First auth RSA and Second auth LDAP. **RequestIconDataCount** — RequestIconDataCount is used for requesting 32-bit color icons. It is a counter which means that only the count of the icons will be requested. The default number is **10**. For example, if set RequestIconDataCount=0, no icon data will be requested. If set RequestIconDataCount=5, only 5 icons are requested. **DefaultSettings** — Specifies the default settings for XenApp or XenDesktop. **Xen App Default Settings:** 1 SignOn=Yes 2 PnliteServer= RequestIconDataCount=20 3 desktopcolordepth=32 4 LongApplicationName=yes 5 sessionconfig=ica progressivedisplay=yes ondesktop=yes 6 device=audio volume=high 7 Seamless=yes FullscreenReserved=yes 8 sessionconfig=all mapdisks=yes 9 Enabled by default: Disks, Serials, Sound 10 Disabled by default: USB, Printers, Smart Cards **Xen Desktop Default Settings:** 1 SignOn=Yes 2 sysmode=vdi toolbarclick=yes toolbardelay=3 3 sessionconfig=ica progressivedisplay=yes 4 PnliteServer= 5 AutoSignoff=yes 6 Enable by default: Printers, Serials, USB, Sound 7 Disabled by default: Disk, Smart Cards **SmartcardPassthrough** — Default is **yes**. Yes/no option to enable/ disable the smartcard pass through mode.

Parameter	Description
	StoreFront — Default is **no**. Yes/no option to support Citrix StoreFront Authentication. The value will be saved into NVRAM. **HttpUserAgent**—The option will replace the default "CitrixReceiver WTOS/1.0" during Netscaler login. If you are using "WTOS/1.0" as Netscaler Session Policy, set this INI parameter to retain your Netscaler policy configuration. **CAGSendDomain**—This option sends domain as domain\user to external network Netscaler to support Netscaler and DUO passcode authentication. The default value is no. **IgnoreDefaultGateway**—This option ignores default gateway of the current selected store during Netscaler login. Always use pnliteserver to continue. The value **Yes** ignores the default gateway. **No** is the default value. When the value is set to **no** Netscaler server is used as default gateway to reset login again. **CAGUserAsUPN**—This parameter enables you to send user details to server in the format similar to an email address—username@fqdn. Certain third party authentication for Netscaler requires this format. For example, Okta authentication. **CAGExternal**—This value allows CAG login with external network mode directly without verifying beacons. This reduces the login time. **DisableSFInit**—This value disables storefront initialization process during the system bootup. Storefront initialization can be disabled using this parameter as it is not required during login.
FastDisconnect={yes, no, Signoff} [CtrlKey={yes, no}] [AltKey={yes, no}] [PowerButton=signoff]	Default value is set to **yes**. If the value is set to yes, pressing the **F12** (default) key or the key defined in FastDiconnectKey= statement will close the active window of the session. If the active window is a seamless window, the action will only close the window. If the window is not a seamless window, then the session will be disconnected. If the option CtrlKey and/or AltKey is set to yes, the function key should be combined with **Ctrl key** and/or **Alt key**. If the value is set to Signoff, pressing the **F12** (default) or the key defined in FastDisconnectKey= statement will disconnect all sessions and return to the signon window. If PowerButton is set to signoff, pressing the power button of the unit after you sign on will disconnect all sessions and return to the logon window. Otherwise, the unit will shut down normally.
FastDisconnectKey={F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Pause/Break}	Specifies the disconnect key that will close the active window from the session.
Printer={COM1, COM2, LPT1, LPT2} [Name=<name>] [PrinterID=window_driver] [Class=classname] [Enabled={no, yes}] [EnableLPD={no, yes}]	Default is **COM1**. **Printer** — Specifies the local printer to configure. **Name** — Specifies the name of the printer. **This option must be used**. **PrinterID** — If not specified, the default Generic/Text Only is used. **Class** — Used in ThinPrint print for TPAutoconnect; the ThinPrint technology of mapping the printer from the client side. It can group printers to use the same template on the ThinPrint server side. The strings PCL5, PS, and TXT are pre-defined classes. Class can be a string with 7 characters. **Enabled** — Default is **yes**. Yes/no option to enable the printer.

Parameter	Description
	EnableLPD — Default is **no**. Yes/no option to enable the LPD service. **NOTE: The parameters must be specified in the order shown.**
Printer={LPD1, LPD2, LPD3, LPD4} [LocalName=name] [Host= host] [Queue=queue] [PrinterID=window_driver] [Class=classname] [Enabled={no, yes}]	Default is **LPD1**. **Printer** — Specifies the LPD printer to configure. **LocalName** — Specifies the name of the printer. If LocalName is not specified, the Queue name is used. **Host** — Specifies the host name of the printer. **Queue** — Specifies the queue name of the printer. **PrinterID** — Specifies the windows driver to use for the printer. If not specified, the default Generic/Text Only is used. **Class** — Used in ThinPrint print for TPAutoconnect; the ThinPrint technology of mapping the printer from the client side. It can group printers to use the same template on the ThinPrint server side. The strings PCL5, PS, and TXT are pre-defined classes. Class can be a string with 7 characters. **Enabled** — Default is **yes**. Yes/no option to enable the printer. These settings in a xen.ini file will be saved into NVRAM if EnableLocal=yes is set in the xen.ini file. **NOTE:** The parameters must be specified in the order shown. For backward compatibility, LPD is accepted as LPD1.
Printer={SMB1, SMB2, SMB3, SMB4} [LocalName=name] [Host=\[domain]\host] [Name=share_name] [PrinterID=window_driver] [Class=classname] [Enabled={no, yes}] [EnableLPD={no, yes}] [Username=username] [Password=password] [Domain=domain name]	Default is **SMB1**. **Printer** — Specifies the shared Microsoft network printer to configure. **LocalName** — Specifies the name of the shared printer. **Host** — Specifies the host name of the shared printer specified as \domain\host when the host is configured within a Microsoft domain, otherwise, host can be specified as \\host. **Name** — Specifies the shared name of the shared printer. **PrinterID** — Specifies the windows driver to use for the printer. If not specified, the default Generic/Text Only is used. **Class** — Used in ThinPrint print for TPAutoconnect; the ThinPrint technology of mapping the printer from the client side. It can group printers to use the same template on the ThinPrint server side. The strings PCL5, PS, and TXT are pre-defined classes. Class can be a string with 7 characters. **Enabled** — Default is **yes** . Yes/no option to enable the printer. **EnableLPD** — Default is **no**. Yes/no option to enable the LPD printer. **Username** — Specifies the username of a user who can use the SMB printer. **Password** — Specifies the password of a user who can use the SMB printer.

Parameter	Description
	Domain — Specifies the domain name of the SMB printer.
** PRIVILEGE=[None, Low, High] [LockDown= {no, yes}] [HideSysInfo={no, yes}] [HidePPP={no, yes}] [HidePN={no, yes}] [HideConnectionManager={no, yes}] [EnableNetworkTest={no, yes}] [EnableTrace={no, yes}] [ShowDisplaySettings={no, yes}] [EnableKeyboardMouseSettings={no, yes}] [KeepDHCPRequestIP={no, yes}] [SuppressTaskBar={no, yes, auto}] [EnablePrinterSettings={no, yes}] [CoreDump={ide, disabled] [EnableNetworkSetup={yes, no}] [DisableNetworkOptions={yes, no}] [EnableSystemPreferences={yes,no, TerminalNameOnly}] [DisableTerminalName={yes, no}] [DisableSerial={yes, no}] [DisableRotate={yes, no}] [DisableChangeDateTime={yes,no}] [EnablePeripherals={keyboard,mouse,audio,serial,camera,touchscreen,bluetooth}] [FastDHCP={yes,no}] TCPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF] UDPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF] [HideWlanScan={yes,**no**}]	Default is **high**. Privilege controls operator privileges and access to zero client resources. See also CCMEnable={yes, no}. None — This level of access is typical for kiosk or other restricted-use deployment. The System Setup selection on the Floating Bar menu is disabled and the Setup submenu is not displayed. The Connect Manager is disabled by default. The Connect Manager can be enabled by using the HideConnectionManager=no option, however, the user cannot create a new connection or edit an existing connection. The user cannot reset the zero client to factory defaults. Low — This access level is assigned to a typical user. The Network selection on the Setup submenu is disabled and the Network Setup dialog box cannot be opened. The user cannot reset the zero client to factory defaults. High — Administrator access level allows all zero client resources to be available with no restrictions. A user can reset to factory defaults. **NOTE:** If None or Low is used, the Network Setup dialog box is disabled. If it is necessary to access this dialog box and the setting None or Low is not saved into NVRAM, remove the network connector and reboot. **LockDown** — Default is **no**. Yes/no option to allow lockdown of the zero client. If yes is specified, the system saves the privilege level in flash. If no is specified, the system clears the privilege level from flash to the default unlocked state. **NOTE:** If the zero client is set to LockDown without a High privilege level, it will disable the G key reset on power-up. LockDown can be used to set the default privilege of the zero client. For example • If LockDown=yes, then the privilege is saved in permanent registry. • if LockDown=no, then the privilege level is set to the default high in the permanent registry. That is, the system has a default high privilege level, which is stored in the permanent registry. • If you do not specify a privilege in either the xen.ini file or the {username}.ini file or the network is unavailable, the setting of LockDown will take effect. It can be modified by a clause. For example, privilege=<none|low|high>lockdown=yes in a xen.ini file or a {username}.ini file sets the default privilege to the specified level. **HideSysInfo** — Default is **no**. Yes/no option to hide the System Information from view. **HidePPP** — Default is **no**. Yes/no option to hide the Dialup Manager, PPPoE Manager, and PPTP Manager from view.

Parameter	Description
	HidePN — Default is **no**. Yes/no option to hide the PNAgent or PNLite icon from view on the taskbar. **HideConnectionManager** — Default is **no**. Yes/no option to hide the Connect Manager window from view. **NOTE:** As stated earlier, although the Connect Manager is disabled by default if Privilege=none, the Connect Manager can be enabled by using HideConnectionManager=no; however, the user cannot create a new connection or edit an existing connection. **EnableNetworkTest** — Default is **no**. Yes/no option to enable the Network Test. **EnableTrace** — Default is **no**. Yes/no option to enable trace functionality. The active items are added to the desktop right-click menu in Privilege=Highlevel. **ShowDisplaySettings** — Default is **no**. Yes/no option to enable the Display Settings in a popup menu. **EnableKeyboardMouseSettings**. Yes/no option to enable the keyboard and mouse configuration preferences. **KeepDHCPREquest** — Default is **no**. Yes/no option to keep the same IP address that is requested from the DHCP server after a request fails and does not invoke the Network Setup dialog box. **SuppressTaskBar** — Default is **no**. Yes/no/auto option to hide the taskbar. If set to auto the taskbar will automatically hide/display the taskbar. When using this parameter in a xen.ini file, it will be saved to NVRAM if EnableLocal is set to yes in the xen.ini file. **EnablePrinterSettings** — Default is **no**. Yes/no option to enable printer configurations when a user Privilege=None. **CoreDump** — The option CoreDump=disabled will disable the core dump function. **EnableNetworkSetup** — This option is used to enable and disable the network setup. **DisableNetworkOptions** — This option is used to enable and disable the network options. **EnableSystemPreferences** — This option is used to enable and disable the system preferences. If the optional parameter EnableSystemPreferences=TerminalNameOnly is set with Privilege=none, then the System Preferences menu is enabled, and only Terminal Name field can be accessed. **DisableTerminalName**— This option is used to enable and disable the terminal name. **DisableSerial** — This option is used to enable and disable the serial table in peripherals. **DisableRotate** — If the optional DisableRotate=yes is set, the rotate setting in the display setup will be disabled. This is only valid for C class clients because the rotation performance in C class may not be desirable.

Parameter	Description
	DisableChangeDateTime—If the option DisableChangeDateTime is set, the function of changing the date and time locally is disabled. For example, when you right-click the time label in taskbar, nothing is displayed. The Change Date and Time button in System Prefernce is invisible. **NOTE:** If the optional EnableNetworkSetup=yes is set with Privilege={none, low}, the network setup will be enabled. If the optional DisableNetworkOptions=yes is set at the same time, the Options table will be disabled. If the optional EnableSystemPreferences=yes is set with Privilege={none, low}, the system preferences setup will be enabled. If the optional DisableTerminalName=yes is set at the same time, the terminal name field will be disabled. If the optional DisableSerial=yes is set with Privilege={none, low}, the serial table in peripherals setup will be enabled. If the optional EnablePeripherals= is set with Privilege=none, the specified peripherals tab will be enabled. The value of the option can be a list of any valid value separated with "," or ";". For Camera, Touchscreen and Bluetooth, they can be enabled only if the devices are available. For example, Privilege=none lockdown=yes EnablePeripherals=mouse,audio,camera,bluetooth, then mouse and audio tab will be enabled, if there are camera and/or bluetooth devices, the camera and/or bluetooth tab will be enabled too. The optional EnableKeyboardMouseSettings=yes can be replaced as below:Privilege=none lockdown=yes EnablePeripherals=keyboard,mouse. **FastDHCP**— FastDHCP identifies the gateway first. If the gateway is same as the network before disconnection and the previous DHCP information is valid, the same information is used. The default value is yes. **TCPTosDscp**—Use this option to set the TOS field of all TCP packets when the fields are not pre-configured by other INI settings. **UDPTosDscp**—Use this option to set the TOS field of all UDP packets when the fields are not pre-configured by other INI settings.Added new sheet TOS_Priority_settings for TosDSCP INI, which is merged from TOS_Priority_settings.docx. **HideWlanScan**—Use this option to disable WIFI scan in lockdown mode. The default value is no.
Proxy={yes, **no**} AppList={ccm;fr;rtme;wms} [Type={Global, http, https, socks5}] [Server=_host_port_] [User=_user_name] [Password=_password_] [Encrypt={yes, no}]	Specifies the proxy settings which are saved in non-volatile memory. If Proxy=no, all proxy settings are cleared and all the followed options are ignored. If Proxy=yes, the option AppList must be followed. It specifies which applications are applied to connect through proxy. WMS, CCM, FR, and RTME are supported. The application name is separated with semicolon. **NOTE: Wyse Management Suite is the successor to Cloud Client Manager (CCM).** The following options are used to configure one or several proxy server setting. The option Type specifies the proxy protocol including http, https and socks5. The option Server specifies the url of the proxy server. The

Parameter	Description
	option User and Password specify the credentials of this proxy server. The option Encrypt specifies if the password is encrypted or not. The option User and Password can support system variables. Because CCM runs before sign on, it is not appropriate to use $UN and $PW. If Type=Global, the proxy settings are saved into http proxy setting, and the https and socks5 proxy settings use the same setting as http proxy. And the followed proxy settings will be ignored. For example, Proxy=yes AppList=fr \ Type=http Server=server1:1234 user=$UN password=$PW (OR) Proxy=yes AppList=ccm \ Type=http Server=server1:1234 user=abc password=xyz \ Type=socks5 Server=server2:4321 user=abc password=1234 (OR) Proxy=yes AppList=ccm;fr \ Type=Global Server=server_global user=user_global password=password_global_encrypted Encrypt=yes
RapportDisable={yes, no} [DHCPinform = {yes, no}] [DNSLookup = {yes, no}] [QuickMode = {yes, no}] [Discover={yes, no}] [SecurityMode= {default, full, warning, low}]	If this option is set to yes, the Rapport agent will be disabled. We support to discover WDM server by the following options: 1 DHCP option tag values received from standard or WDM proxy DHCP service for vendor class “RTIAgent”. 2 DNS service location record "_wdmserver._tcp". 3 DNS host name lookup "wdmserver". When RapportDisable=no, setting DHCPinform=yes will do #1, and setting DNSLookup=yes will do #2 and #3. If QuickMode is set to yes, then the rapport agent will not block any other process during ThinOS Lite boot up and increases the boot time of ThinOS Lite . If Discover=yes is specified, rapport will discover WDM server information from DHCP option tag, DNS service location record, and DNS host name. If the WDM server is discovered, the WDM server UI is protected on the device. **Default=yes.** **IMPORTANT: If file server is changed by WDM server, device will reboot automatically to make sure all settings from WDM server take effect. Default is yes.** SecurityMode specifies the SSL certification validation policy.If set to default, SecurityPolicy setting is applied.If set to full, the SSL connection

Parameter	Description
	needs to verify server certificate. If it is untrusted, drop the connection.If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection.If set to low, the server certificate is not checked. The value is persistent, and the default value of the setting is default. If the settings are factory default or if you are upgrading to ThinOS Lite 2.3 for the first time, the value is temporarily set to low. After loading any INI, it goes to Default.
RapportServer=<server_list> [Retry=<retry number value>]	**IMPORTANT: DISCONTINUED. DO NOT USE. Use WDMService parameter.**
Reboot={no, yes} Time=hh:mm [-hh:mm] [Wday={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}] [Idle=minutes] [Week={Current, Other, 0, 1, 2, 3, 4}]	Default is **no**. **Reboot** — Yes/no option to enable automatic daily reboot of all ThinOS Lite devices. **Time** — Specifies the time to reboot and must be in a 24-hour format. For example: Reboot=Yes Time=17:30 will reboot all ThinOS Lite devices at 5:30 P.M. daily. The option **Wday** specifies the weekday of scheduled reboot The option **Week** specifies the minimum weeks required to reboot the client after configuring an INI parameter. The value **Current** is equal to 0 and the value **Other** is equal to 1. **Idle**—Specifies the idle minutes. Once the scheduled reboot time is reached, the system reboots if there is no active session or the terminal is idle for the specified idle minutes. If the session is still active, the reboot is delayed till the idle time is reached or log off the sessions. For example, If you set Reboot=yes time=20:30, the unit reboots on local time 20:30. If you set Reboot=yes time=20:30-4:30, the unit reboots on random time through 20:30 to 4:30. If you set Reboot=yes time=23:00 Wday=Friday,Monday, the unit reboots on local time 23:00 of Friday and Monday. If you set Reboot=yes time=1:00 Idle=10, the unit reboots on 1:00, if there are no sessions. If there is any active session, the reboot happens only if the unit is idle for 10 minutes or the system logs out from the session. If you set Reboot=yes time=1:45 Wday=Sunday Week=1, the unit will reboot at 1:45 on a Sunday only after 1 week of setting the INI parameter.
Reconnect={no, yes, seconds}	**Default is no.** Yes/no option to enable automatic reconnection to an application after a server disconnection. This setting in a xen.ini file will be saved into NVRAM if EnableLocal=yes is set in the xen.ini file. The value of seconds is the interval to wait before automatically restarting the connection after disconnect. If the value is negative, it will reconnect only during startup Valid range of the absolute value is 1 to 3600. If the absolute value is over 3600, it is set to 20.
Resolution=[DDC, 640X480, 800X600, 1024X768, 1152X864, 1280X720,	Default is **DDC**. **Resolution** — Specifies the local display resolution. Option DDC can be specified to select default display resolution.

Parameter	Description
1280X768, 1280X1024, 1360X768, 1366X768, 1368X768, 1400X1050, 1440X900, 1600X900, 1600X1200, 1680X1050, 1920X1080, 1920X1200] [Refresh=60, 75, 85} [rotate={right}]	**NOTE:** When using the Wyse Y Cable, DDC will properly work on both monitors by default. However, if connected to R10L/R00x clients and you are using Dual DVI, then you must add the following DualHead INI parameter and DualHead option for DDC to properly work on both monitors: Parameter: DualHead=yes Option: ManualOverride=yes **Refresh** — Specifies the local display refresh rate. **NOTE:** If the Resolution or Refresh parameter values are changed, the zero client will reboot without notice to the user. **rotate** — Rotate allows you to rotate monitors for viewing in Portrait mode. For example: `screen=1 resolution=1280x1024 refresh=60 rotate=none` **NOTE:** Due to processing power requirements, rotate is not recommended and supported on the C class platforms at this time. **IMPORTANT:** The Screen parameter must be placed before the Resolution parameter. For example: `screen=1 resolution=1280x1024 refresh=60 rotate=none`
RootPath=<file server root path>	This file server root path is entered into the zero client local setup (non-volatile memory). The zero client immediately uses this path to access files. The directory name \xen will be appended to the file server root path entry before use.
**ScreenSaver=value{0, 1, 3, 5, 10, 15, 30} [LockTerminal={0, 1, 2, 3}] [Type={0, 1, 2, 3, 4}] [VideoLink=httplink] [VideoSpan=no] [Unit=hour] [Image=imagefile] [PictureTimer={2-60}] [PictureOrder=random] [PictureCheck=always] [PictureLayout={stretch, tile, center}]	**Screensaver**— Specifies to put the thin client in a screensaver state when the time limit for inactivity is reached, that is delay before starting is reached. Default value is **10**. Value and delay before starting the screensaver: 0 — Disabled 1 — 1 Minute 3 — 3 Minutes 5 — 5 Minutes 10 — 10 Minutes 15 — 15 Minutes 30 — 30 Minutes The default screen saver value is 10 minutes and the maximization value is 30 minutes.

Parameter	Description
[Sleep={0-180}]	**LockTerminal**— This is an optional parameter and specifies to put the thin client in LOCK state when the screen saver is activated. Default is **0**. **0** — Disabled. **1** — Puts the thin client in a LOCK state when the screen saver is activated. The wallpaper is shown and the user is prompted with an unlock dialog box to enter the sign-on password to unlock the thin client. **LockTerminal** settings are saved into NVRAM if **LockTerminal=1**and **EnableLocal=yes** is set in the xen.ini file. **2**— Puts the thin client in a LOCK state when the screen saver is activated, however, the wall paper cannot be viewed when the user is prompted with an unlock dialog box to enter the sign-on password to unlock the thin client. **3**— Puts the thin client in a LOCK state when the screen saver is activated, and the username and password are needed to unlock the terminal. The wallpaper is not shown and the Password field in the Unlocking window is invisible until you have entered the username. When you click **OK** or press the Return key, a message box pops up to input the username and password to unlock the terminal. **NOTE:** The user must be signed on with a password for a Lock action to take effect. If set in KeySequence, users can lock the thin client at any time by pressing Ctrl+Alt+Left arrow or Ctrl+Alt+Right arrow. **Unit** — This parameter converts the screen saver timer value from minutes to hours to set longer time. **Type** — Specifies which type of screensaver to use. 0 — Blank the Screen 1 — Flying Bubbles 2 — Moving Image 3 — Showing Pictures 4 — Playing Video **VideoLink** — Specifies the video link address of the video file. Links with only http are supported. The mp4 video format is supported. **VideoSpan** — Specifies the video displayed mode in the screen. If the dual head is in span mode and VideoSpan=yes, it is spanned across all the screens. If VideoSpan=no, it is displayed in the main screen. **Imagefile** — This is an optional parameter and specifies an image file residing in the **bitmap** sub-folder under the home folder to be used as a **Moving Image** screensaver. If Type is set to 2 and no image file is present then the default Dell Wyse logo is used. If Type is set to 3, pictures residing in **picture** subfolder under the home folder are displayed.

Parameter	Description
	If **SelectGroup=yes**, then the pictures residing in the **picture** subfolder under the group folder are displayed. For example, `/xen/ini/{group_dir}/picture` If group pictures do not exist, global pictures are used. Supported formats include JPG, GIF, PNG and BMP. **PictureTimer** — Specifies the interval to wait in seconds to display another picture. Default value is **6 seconds**. **PictureOrder** — Specifies the order of picture files to display. **The default is to use the order of sort from A to Z**. If set to random, pictures are displayed randomly. **PictureCheck** — Specifies whether to check for picture files servers or not. **NOTE:** If set to always, the picture files in file servers are checked when the screen saver starts every time. By default, the system checks for picture files only when the screen saver starts for the first time to decrease network traffic. **PictureLayout**— The optional parameter is used to specify the arrangement on the desktop when pictures are displayed. For the tile selection, the image is replicated across the desktop. For the center selection, the image is placed at the center of the desktop without any image size change. For the stretch selection, the image is either expanded or shrinked to fill the desktop. The default value is stretch. **Sleep**—The optional parameter is used to specify the interval minutes to stop soft screen saver and turn off monitor. After the specified minutes, since software screen saver starts up, the software screen saver is stopped and turns off the monitor until screen saver is off. The value range is 0 to 180. The value 0 is default which disables this function.
SecureMatrixServer=<SecureMatrix Server Host name or IP address/FQDN or URL>	Specifies the Host name or IP address/FQDN or URL of the Secure Matrix server. Http or https protocol usage is decided by the server configuration. If SecureMatrixServer is defined, the user must pass authentication with the Secure Matrix server first, and then there is a seamless log in to the brokers if the server can provide the correct broker credentials, if not, the user must enter broker credentials to log in. For Example: SecureMatrixServer=https://gsb01.bjqa.com **NOTE:** Before using this parameter, use the Secure Matrix documentation to set up the Matrix Server. Also, be sure you import the relevant GSB Server Certificate file when using https.
SecurityPolicy={full, **warning**, low} [SecuredNetworkProtocol={yes, **no**}] [TLSMinVersion]={1,2,3}] [TLSMaxVesion={1,2,3}] [DNSFileServerDiscover={yes,no}]	Specifies the global security mode for SSL connection. If application SecurityMode is default, application applies the setting. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, connection is dropped.If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, and the default value is **warning**. For those SSL connections with their own security policy, this does not impact.

Parameter	Description
	For example, Fileserver follows global security policy. Citrix broker, and SECUREMATRIX are forced to high security mode. If the optional SecuredNetworkProtocol=yes is set, the unsecure protocols including ftp, http and tftp are disabled. The value is persistent, and the default value is no. Option TLSMinVersion and TLSMaxVersion allows you to configure the SSL connection.TLSMinVersion sets the minFallbackMinorVersion. Server uses the version equal or above to communicate with the client. TLSMaxVersion sets the advertisedMinorVersion. Server uses this version equal or above to communicate with the client. If no value is set for TLSMinVersion then the default value is set to TLS1.0 and TLSMaxVersion is set to TLS1.2. The value 1, 2, 3 corresponds to TLS1.0, TLS1.1, TLS1.2 respectively. These parameters are used by engineers for internal tests. In classic mode, a DNS name wyseftpfbc4tc is resolved to discover the file server, if the global INI file in remote file server and local cache cannot be loaded. If the optional DNSFileServerDiscover=no is set, the function is disabled. The value is persistent, and the default value is yes.
SessionConfig=ALL [unmapprinters={no, yes}] [unmapserials={no, yes}] [smartcards={no, yes}] [mapdisks={no, yes}] [disablesound={no, yes, 2}] [unmapusb={no, yes}] [DisksReadOnly={no, yes}] [MouseQueueTimer={0–99}] [WyseVDA={no, yes}] [WyseVDA_PortRange=startPort, endPort] [WyseVDAServerPort=serverPort] [OffScreen={yes, no}] [UnmapClipboard={no, yes}] [DefaultColor={0,1,2}] [VUSB_DISKS={yes, no}] [VUSB_AUDIO={yes, no}] [VUSB_VIDEO={yes, no}] [VUSB_PRINTER={yes, no}] [FullScreen={no, yes}] [Resolution={default, vga_resolution}] [DisableResetVM={no, yes}]	Set ALL to establish default settings for all sessions. If connection parameters are set to yes, the default settings will be changed accordingly. The optional keyword DisksReadOnly specifies the mount mass storage as read-only. (CIR38166) The optional keyword MouseQueueTimer specifies the default queue timer of mouse event in ICA session. The unit is 1/100 second. It can adjust the bandwidth of network (CIR40532). If Disablesound =2 is set, it disables sound at remote computer. Set WyseVDA=yes to enable WYSE Virtual Desktop Accelerator for all /ICA sessions. Default is disabled. If WyseVDA is disabled, ICA sessions, including MMR and USB, will not go through WYSE VDA. Set WyseVDA_ENABLE_MMR=no, to disable TCX MMR over WyseVDA. Set WyseVDA_ENABLE_USB=no, to disable TCX USB over WyseVDA. Set WyseVDA_PortRange for ThinOS Lite VDA client port range. The port range must follow the rules mentioned here: 1 The port range is a list of start port and end port separated by a semicolon (;) or a comma (,). 2 Both ports must be between 1 and 65535. 3 The end port must be greater than start port. For example, "WyseVDA_PortRange=3000,3010", the start port is 3000, the end port is 3010.Set WyseVDAServerPort for ThinOS Lite VDA client. The default port is 3471, the port range must be from 1029 to 40000. For example, "WyseVDAServerPort=3000", set VDA server port to 3000, client will connect VDA server with this port. Set OffScreen=yes, to enable offscreen support for all sessions. Currently only ICA is supported. (CIR45080) Set UnmapClipboard=yes, to disable clipboard redirection for all sessions.This setting in xen.ini is saved into nvram, if EnableLocal is set to yes in xen.ini. The optional keyword DefaultColor specifies the default color depth of the session.

Parameter	Description
[WyseVDAServerPort=serverPort] [FontSmoothing={yes, no}] [AutoConnect={yes, no}] [MultiMonitor={yes, no}] [EnableImprivataVC={yes,no}] [Locale=LocaleID] [SessionLogoffTimeout=seconds] [GroupSession={yes,no}]	The options VUSB_DISKS, VUSB_AUDIO, VUSB_VIDEO, VUSB_PRINTER are specified, if these USB devices are redirected to the server using TCX Virtual USB or ICA USB redirection when USB redirection is enabled.By default, these devices are handled as local devices. For example, If you want to use USB disks as a network disk, you can set “SessionConfig=all mapdisks=yes VUSB_DISKS=no". If you want to use USB disks as server side device which are displayed in session device manager, you can set "SessionConfig=all mapdisks=no VUSB_DISKS=yes". The option FullScreen specifies the default screen mode. The option Resolution specifies the session resolution. It can be default or vga_resolution, for example, 640 x 480, 1024 x 768 and so on. For more information, refer to resolution in connection parameters. Set DisableResetVM=yes to disable the Reset VM function. By default, this function is controlled by server side including Citrix PNA. Set FontSmoothing=no to disable font smoothing option. By default, font smoothing is allowed. Set AutoConnect=no to disable auto connection function. Set MultiMonitor=no to disable multiple monitor layout function. The session has the same desktop width and height with local virtual desktop size, spanning across multiple monitors, if necessary. If EnableImprivataVC is set to no, the Imprivata Virtual Channel is disabled. The user can use vusb redirect instead of Imprivata Virtual Channel mode to use the Rfideas or finger print device in session as server side remote device. Set Locale=LocaleID to set Locale in session to make some localization configuration to work.) Set SessionLogoffTimeout to force all sessions to logoff after you sign-off from the broker. It only supports Citrix Xen brokers. Without this INI, all sessions are simply disconnected after you sign-off from the broker. The default value is 0. So when you log off from the broker, we used to disconnect all active sessions. Now the system will also force those sessions to be logged off, so that next time you can have a clean session. From this release, when this INI value is not 0, for example 30, and when you sign off from broker with active sessions, client sends sign-off command to active sessions instead of asking disconnect, and client waits for 30 seconds, if all active sessions successfully log off within 30 seconds, for example finish by 20 seconds, system will sign out users from broker immediately after that. If any active sessions fail to log off within 30 seconds, system will close the session and sign out users from broker immediately. During the awaiting time, system will prompt user a message to ask them to check and save all work to make the session log off smoothly. Set GroupSession=yes to enable the function of grouping sessions and the menu item of Group Sessions is checked when you right click on the desktop. The default value is no and the original state of Group Sessions is unchecked.
**SessionConfig=ICA [desktopmode={fullscreen, window}]	**SessionConfig** — Specifies the ICA default settings of the optional connection parameters for all ICA sessions.

Parameter	Description
[mapdisksunderz]: DISCONTINUED. DO NOT USE. [TosIpPrecedence={0–5}] [TosDscp={Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF}] [DiskMapTo=a character sequence] [SysMenu={remote, local}] [SessionReliability={no, yes}] [WarnPopup={yes, no}] [ondesktop={no, yes, all, none, desktops, applications, ondesktop_list}] [AudioQuality={default, high, medium, low}] [USBRedirection={TCX, ICA|HDX}] [ZLKeyboardMode={0, 1, 2}] [ZLMouseMode={0, 1, 2}] [SucConnTimeout=seconds] [HDXFlashUseFlashRemoting={Never,Always}] [HDXFlashEnableServerSideContentFetching={Disabled,Enabled}] [EnableRTME={Yes, No}] [FlipByTimer={0, 1}] [RefreshTimeOut={dd:hh:mm}] [Timeout={Yes, No}] [PasswordExpireNotify={yes, no}] [RefreshPopupNotice={yes, no}] [DisableReceiverLogo={Yes, No}] [MMRClientFetchDisabled={Yes, No}]	**desktopmode** — Default is **fullscreen**. Specifies the display mode of an ICA published desktop when using an ICA PNAgent logon; the default is **fullscreen mode for a PNA desktop application**. **mapdisksunderz** — DISCONTINUED. DO NOT USE. **TosIpPrecedence** — Allows you to set IP Precedence in the TOS fields. **TosDscp** — Sets IP DSCP in the TOS fields. **DiskMapTo** — Specifies to map disks to a character sequence. **NOTE:** A sequence of characters can be used by DiskMapTo, with each letter mapped to one disk in order. For example, if RTNM is the sequence, R is mapped to the first disk (in ThinOS, it will be D:/), T is mapped to the second disk (in ThinOS, it will be E:/), and so on. Only the letters “a” through “y” and “A” through “Y” are accepted; All lowercase letters are changed to uppercase, other characters will be skipped, and duplicate characters will be omitted. For example, #GGefZzedAF1JaE will be mapped to GEFDAJ. The number of disks mapped to the session depends on the number of valid letters provided. If no letter is provided, all disks will be mapped to the session using default driver letters. **SysMenu** — Default is **local**. Specifies the system menu mode when right-clicking the taskbar button of a seamless window. If it is remote, the system menu will come from the remote server; otherwise, it will be the local menu. **SessionReliability** — Default is **no**. Yes/no option to enable session reliability. **WarnPopup**— If WarnPopup=no, the option can disable the warning message when session reliability happens in order to decrease the administrative support calls. **ondesktop**— This option specifies the connections that are displayed on the desktop. It enhances ondesktop options for SessionConfig=ICA so that the VDI brokers can work with ondesktop options too. • If AutoConnectList is set in the VDIServer statement, all connections configured in AutoConnectList parameter are displayed. • The connections show on desktop as default. • The connections can be controlled by using the values available. • The connection is added to the connection manage list even if the connection is not displayed on the desktop. all - show all, same as default none - don't show any desktops - only show desktops applications - only show applications The others will be handled as a ondesktop_list. For example, if set ondesktop="word; excel", only show the applications "word" and "excel". all—display all connections. none—no connections are displayed. desktops—display only the desktop connections. applications — display only applications, the connections are handled as an ondesktop_list. For example, if you set ondesktop=word; excel, then only the applications word and excel are displayed. The ondesktop_list also supports wildcard when the star * is used, similar to the AutoConnectList parameter in VDIServer. For example, if the value

Parameter	Description
	is set as **ondesktop=*IE***, any application which includes the string IE is displayed. **AudioQuality** — Default is **default**. Specifies the audio quality of ICA sessions. **NOTE: Medium quality is recommended for Speech scenarios. For example: SessionConfig=ICA AudioQuality=high** **USBRedirection** — Default is **ICA|HDX**. Option to select the channel of usb devices redirection. This option is recommended to replace the older setting device=vusb type={TCX, HDX}. **ZLKeyboardMode** — Specifies to accelerate the display of the input text on the client device over a high latency connection. 0=off, 1=on, 2=auto **ZLMouseMode** — Specifies to accelerate the visual feedback for mouse-clicks on the client device over a high latency connection. 0=off, 1=on, 2=auto **SucConnTimeout**— This option will enhance the seamless session share. During the first session logon, immediately start second or later sessions, which will wait for the time set with SucConnTimeout (or the logon success) to make sure new applications share with the first logon session. **HDXFlashUseFlashRemoting**— Default is **Always**, which means the HDX is enabled always. The value Never is to disable HDX. **HDXFlashEnableServerSideContentFetching**— Default is **Disabled**, which means the server side fetching content is not enabled. The value enabled is to enable this function. **EnableRTME**— This option controls the launch of RTME service. The default value is enabled. **FlipByTimer**— This option selects the screen refresh method. For some old server, there is no EndOfFrame transferred to the client. Then we can use this option to fix such issues. **RefreshTimeOut**—RefreshTimeOut triggers auto-refresh which updates ICA applications automatically. The value format dd:hh:mm, indicate days&&hours&&minutes as the auto-refresh interval. The default value is 0, that disables auto-refresh. **Timeout**– This option controls the credential prompt after ICA broker logon was timeout. Session ticket is invalid now. If yes, users have to enter their credential to re-login to launch session, if no, ThinOS will use the default credential to do login in background. The default is yes. **NOTE: Other Citrix INI parameters are not listed here. However, these Citrix INI parameters are supported on ICA connection by using INI `SessionConfig=ICA`.** **PasswordExpireNotify** —This option enables the password expire notification, which should configure in storefront server side, Authentication, password change set as At any time. Then before the password expires, logon prompts a message displaying the number of days after which the password will expire and let you change the password. The option WarnPopup=no can disable the warning message when session reliability happens to decrease the administrative support calls. **RefreshPopupNotice** — This option enables or disables the popup notice during refresh in progress. The default value is yes.

Parameter	Description
	DisableReceiverLogo—Hides the CitrixReceiver logo in left top corner in storefront style. The default value is No. **MMRClientFetchDisabled** — This option disables RAVE client content fetching. The default value is No.
SessionConfig=ICA KeyboardTimer=1000	This is a Citrix INI. This specifies the amount of time, in milliseconds, the client queues keystrokes before passing them to the server.
Shutdown={standby, turnoff}	Default is **standby**. Specifies the system state when shutting down the unit. If set to standby, the ThinOS Lite system is suspended. When the unit starts up, it is resumed. It does not go to the BIOS and thus turns on quickly. If set to turnoff, the system is turned off. When the unit starts up, it first starts the BIOS then ThinOS Lite.
SignOn={yes,no, NTLM} [MaxConnect=max] [ConnectionManager={maximize, minimize, hide}] [EnableOK={no, yes}] [DisableGuest={no, yes}] [DisablePassword={no, yes}] [LastUserName={no, yes}] [RequireSmartCard={no, yes}] [SCRemovalBehavior= {-1, 0, 1}] [SaveLastDomainUser={yes, no, user, domain}] [DefaultINI=filename] [IconGroupStyle={default, folder}] [IconGroupLayout={Vertical, Horizontal}] [PasswordVariables={yes, no} [LockTerminal={yes, no}] [ExpireTime={0, 1 - 480}] [UnlockRefresh={yes, no}] [SCShowCNName={yes,no}] [SCSecurePINEntry={no, yes}] [AutoConnectTimeout={10-300}] [DisableEditDomain={yes, no}] [AdGroupPrefix=adgrpnameprefix]	Yes/no option to enable the sign-on process. Default is yes. If set to NTLM, user can be authenticated with NTLM protocol. The user must be a domain user and the same sign-on user credentials must be available in the ftp://~/xen/ini/ directory. The optional keyword **MaxConnect** sets the maximum number of connects that are allowed to be specified in the xen.ini and username.ini together. The range allowed for the “max” is 100 to 2000. If the value is greater than 2000, 2000 is set instead. If the value is lesser than 100, 100 is set instead. The default maximum value is 216 entries. (CIR37285) The optional keyword **ConnectionManager** sets the state of connection manager while sign on (After 5.0.006). The following optional keywords are valid after 5.0.010. The optional keyword EnableOK is set to display OK and Cancel button in sign-on window The optional keyword AutoConnectTimeout sets the timeout for auto connect published applications. The range is 10 seconds to 300 seconds. The default is 30 seconds The optional keyword DisableGuest sets whether guest sign-on is disabled or not. The optional keyword DisablePassword is set to disable password box and new password check box in sign-on window. The optional keyword LastUserName is set to display the last sign-on username after the user logs off. The optional keyword RequireSmartCard is set to enable force logon with smartcard The optional keyword SaveLastDomainUser is set to save the username and domain into NVRAM, after successful sign on. So during the next reboot, the username and domain saved in the NVRAM is displayed in sign on server as default username and domain, if no Default User is set in xen.ini.

Parameter	Description
[RequireSmartCard ={yes or force, optional, no}] [CitrixSignonStyle={default, xenith, thinos}] [SignonStatusColor="rrr ggg bbb"]	The size of domain\username is limited to 32. If input domain\username size is greater than 32, it will be truncated and then saved into NVRAM. If SaveLastDomainUser=user, only username is saved into NVRAM. If SaveLastDomainUser=domain, only domain name is saved into NVRAM. (CIR57726) The optional keyword SCRemovalBehavior configures the behaviors after the smart card is plugged out from the terminal. **SCRemovalBehavior** — Default is **0**. Specifies what happens after a smart card is removed. **-1** — If smartcard is removed then client has no action. Whether the session can be used or not, totally depends on the server policy. **0** — System logs off. **1** — System locks and can be unlocked only when the same certificate is used with the smart card. The optional keyword DefaultINI configures a file name which is in default folder of username ini files. If the {username}.ini is not found, this file will be loaded by default. (CIR51869) The optional keyword IconGroupStyle configures the icon group style on the desktop. PNAgent published applications can be configured with client folder in PNA server. If set IconGroupStyle=folder, the PNAgent published applications which are specified to display on the desktop will display with the folder. After clicking the folder icon, the subfolder or applications in this folder will display on the desktop. In this case, there is an Up to 1 Level icon on top. Clicking the icon will display the up one level folder contents. In this case, there is an "Up to 1 Level" icon on top. Clicking this icon will get back to the up level folder contents. (CIR54333) The optional keyword IconGroupLayout configures the direction of the icon group on desktop. The default is vertical. The optional keyword PasswordVariables l s set to support variable mapping ($TN, $UN etc) for password. The optional keyword LockTerminal configures the lockup terminal. The default is yes. If LockTerminal=no, the function of locking terminal is disabled. You can right-click on the desktop or click the Shutdown option --> Lock Terminal, to disable the Lock Terminal. Also, it disables the lock terminal even if "ScreenSaver=_minutes_ LockTerminal=yes" is set. The option keyword ExpireTime configures the expiration time. The range is 1 minute to 480 minutes. The default is 0 which means no expiration. If the value is greater than 480, 480 is set instead. If the value is smaller than 0, 0 is set instead. After sign on or launching a connection, start counting the expiration time. After the expiration time is reached, launch a session by clicking icon or menu or connection manager. The user will view a message box to enter password. But the open sessions still remain open. Only if the password is same as original sign on password, the session will be launched.

Parameter	Description
	If the terminal is locked and unlocked by using password, start counting the sign on expiration time again. If the default value yes is set, then when you unlock the system, the system will refresh PNA list to verify the password. Set the value to no to disable the behavior of refresh. (CIR63666) The optional keyword SCShowCNName is set to yes to forcibly use the CN name of the certificate as the user name when using smartcard sign on. By default, the UPN name is used as the user name. The optional keyword SCSecurePINEntry is set to yes to enable Secure PIN entry function for pkcs15 card with Cherry keyboard. The default value is no. The optional keyword DisableEditDomain is set to yes to stop typing in the domain box manually. Typing the character @ or \ as the format domain \user and user@domain in username box are not allowed. The option **AdGroupPreFix** is only valid, when you configure SignOn=NTLM. If the option is configured, then zero Clinet will verify all AD group names to which the sign-on user belongs, to get the first group name so that its prefix matches adgrpnameprefix, and load adgroup/the_whole_ad_group_name.ini if the configuration file exits, before loading user specific ini. For example, if the sign no user is user_111 in a domain, user_111 belongs to group domain user and group tc_grp1_ad, the option is configured as AdGroupPrefix=tc_grp1. If the configuration file adgroup/tc_grp1_ad.ini exists, it will be loaded. RequireSmartCard is used for authentication of smartcard. If optional RequireSmartCard=yes or force, only smartcard authentication is allowed. If optional RequireSmartCard=no, smartcard authentication is disabled. If optional RequireSmartCard=optional, smartcard authentication is optional. The default value is optional. The optional keyword CitrixSignonStyle specifies the sign on window style for ThinOS Lite build. By default, CitrixSignonStyle=default, the citrix receiver store front style sign on window is used if StoreFront Style is checked in Xen Broker GUI, otherwise, the legacy ThinOS Lite sign on window style is used. If you set CitrixSignonStyle=thinos, the ThinOS Lite sign on window style is used. If set CitrixSignonStyle=Xenith, the legacy ThinOS Lite sign on window style is used. CitrixSignonStyle specifies the signon window style for ThinOS Lite build. By default, CitrixSignonStyle=default, the citrix receiver store front style signon window is used. If StoreFront Style is checked in Xen Broker GUI, otherwise, the legacy Xenith signon window style is used. If you set CitrixSignonStyle=thinos, the ThinOS signon window style is used. If set CitrixSignonStyle=Xenith, the legacy ThinOS Lite signon window style is used.
ScepAutoEnroll = { yes | **no** } AutoRew = { yes | **no** } InstallCACert = {yes | **no** } [CountryName = county] [State = state]	This option is to allow client automatically get certificates and renew certificates using SCEP protocol. **ScepAutoEnroll**—Set this keyword to yes to enable client's functionality to automatically obtain certificate. Set **AutoRenew**—Set this keyword to yes to enable certificate auto renew. Client only tries to renew certificates requested either manually or automatically through SCEP from this client, and the renewal is performed only after a certificate's 1/2 valid period has passed.

Parameter	Description
[Locality= locality] [Organization = organization_name] [OrganizationUnit = organization_unit] [CommonName = common_name] [Email = email_address] KeyUsage = kay_usage KeyLength = {1024, 2048, 4096 } [subAltName = subject_alt_name_list] RequestURL = scep_request_url CACertHashType = { MD5, SHA1, SHA256 } CACertHash = CA_HASH_VALUE [EnrollPwd = enrollment_password] [EnrollPwdEnc = encrypted_enrollment_password] [ScepAdminUrl = scep_administrator_page_url] [ScepUser = scep_enrollment_user] [ScepUserDomain = scep_enrollment_user_domain] [ScepUserPwd = scep_enrollment_user_password] [ScepUserPwdEnc = encrypted_scep_enrollment_user_password]	Set **InstallCACert**—Set this keyword to yes to install the root CA's certificate as trusted certificate after successfully getting a client certificate. **CountryName, State, Locality, Organization, OrganizationUnit, CommonName, Email**—These keywords together compose the subject identity of the requested client certificate. Country Name should be two letter in uppercase, other fields are printable strings with a length shorter than 64 bytes, and email_address should have a '@' in it. At least one of the above fields must be configured correctly to form the client certificate's subject identity. **KeyUsage** —This option is to specify key usage of the client certificate and should be set to a digitalSignature, keyEncipherment or both using a ';' concatenating these two as digitalSignature;keyEncipherment. **KeyLength**—This option is to specify the key length of the client certificate in bits, must one of the value in the list. **subAltName**—This option is to specify the client certificate's subject alternative names. It is a sequenced list of name elements, and every element is either a DNS name or an IP address. Use ';' as delimiter between them. **RequestURL**—The RequestURL option is to specify the SCEP server service URL. This field must be set correctly. The default protocol for SCEP services is HTTP, which also ensures data security. You can also add the prefix https:// if SCEP service is deployed on HTTPS in your environment. **CACertHashType**—CACertHashType is the hash type used to verify certificate authority's certificate, should be set to MD5, SHA1 or SHA256. **CACertHash**—This is the hash value used to verify certificate authority's certificate. Client will not issue a certificate request to a SCEP server and cannot pass certificate chain checking through a valid certificate authority. **EnrollPwd** or **EnrollPwdEnc**—These keywords are used to set the enrollment password from a SCEP administrator. **EnrollPwd** is the plain-text enrollment password and **EnrollPwdEnc** is the encrypted form of the same enrollment password. Use only one of these two fields to set the used enrollment password. As a substitute of using EnrollPwd or EnrollPwdEnc to directly specify an enrollment password, client allows using a SCEP administrator's credential to automatically get an enrollment password from a Windows SCEP server. In this case, the **ScepUser**, **ScepUserDomain**, **ScepUserPwd** (or ScepUserPwdEnc, in encrypted form instead of plan-text) are used to specify the SCEP administrator's credential, and ScepAdminUrl must be set correctly to specify the corresponding SCEP admin web page's URL. If neither EnrollPwd nor EnrollPwdEnc is set, client will try to use these set of settings to automatically get an enrollment password and then use that password to request a certificate. If communication security is necessary in your environment during this phase, please add https:// as the prefix for ScepAdminUrl to use HTTPS instead of the default HTTP protocol. Use ScepAutoEnroll=no AutoRenew=yes to only enable SCEP auto renew; all other parameters are not needed if ScepAutoEnroll is set to no. **NOTE: SCEP server's URL must be an HTTP link. Do not add protocol prefix to RequestURL and ScepAdminURL.**

Parameter	Description
SysinfoOntop=[yes,no]	This parameter enables the **System Information** window to be displayed at the top in the Z-Order and overlaps on the nonmode switched full screen session window.
SysMode={classic, vdi, Citrix} [toolbardisablemouse={yes, no}] [toobarclick={yes, no}] [toolbardelay={0-4}] [toolbar_no_conmgr={yes, no}] [toolbardisablehotkey={yes, no}] [ToolbarEnableOneSession={no, yes}] [ToolbarAutoQuit={yes, no}] [ToolbarStay=<value from 1 through aproximately 20>] [EnableLogonMainMenu={no, yes}] [LightGray="r g b"] [MediumGray="r g b"] [DarkGray="r g b"] [DisableAddConnection={yes, no}]	**SysMode** — Specifies the Zero interface optimized for VDI or the Classic interface. This value will be remembered across reboots until changed. If not defined and an INI is present, Classic mode is the default. If no INI is present, VDI mode is the default. Classic mode has full taskbar, desktop and connection manager and is recommended for a terminal server environment and for backward compatibility with WTOS 6.x. VDI mode (Zero interface) has a new launchpad-style interface optimized for full-screen sessions that is Desktops. Everything you need is accessed through an always available overlay interface. Citrix mode makes the client turn to Xenith. Xen.ini is preferred in the next reboot. **toolbardisablemouse** — **Default is no.** By default, the toolbar is hidden until a user hovers their mouse over the left side of the screen. The toolbardisablemouse=yes will disable this function. **toolbarclick** — **Default is no.** If toolbarclick=yes will pop up a toolbar only when a user clicks on the left side of the screen. **toolbardelay** — **Default is 4.** Specifies the number of seconds the toolbar will stay visible. The value 0 will have no delay. Other values 1-4 will delay 0.5, 1, 1.5 and 2 seconds respectively. **toolbar_no_conmgr** — **Default is no.** The toolbar_no_conmgr=yes will make the Connections icon invisible. **toolbardisablehotkey** — **Default is no.** By default, pressing Ctrl+Alt+Up also pops up the toolbar regardless of the settings of toolbarclick and toolbardelay.The toolbardisablehotkey=yes will disable this function. **ToolbarEnableOneSession** — **Default is no.** Yes/no option to enable the toolbar when only one session is available. **ToolbarAutoQuit** — **Default is yes.** ToolbarAutoQuit=no will prevent the sub-window from being closed. The toolbar will auto-hide after a certain amount of time after user moves the mouse pointer away from the toolbar. **ToolbarStay** — ToolbarStay={1~20} controls the auto-hide duration, 0.5s per value. Thus if ToolbarStay=1, the Toolbar will auto-hide after 0.5 second; If ToolbarStay=10, the Toolbar will auto-hide after 5 seconds. **EnableLogonMainMenu** — **Default is no.** Yes/no option to enable the main menu if you click the mouse button on the desktop prior to logon in Zero mode. **DisableAddConnection** — Yes/no option to disable the add connection option.
[RTPTosDscp={Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF}]	The RTPTosDscp can set RTP/UDP audio channel in the TOS fields. For more information, see *TOS_Priority_settings.docx*.

Parameter	Description
TcpMaxRetransmission=<value from 2 through aproximately 12>	**Default is 5.** Configures the retransmission of a TCP connection.
TerminalName=<name> [reboot={no, yes}]	User can set a string up to 15 characters as terminal name. It can be configured as system variable like $MAC, $SN or $IP etc. If reboot is set to yes and the terminal name is changed, the terminal will reboot. If "TerminalName=$DNS" is set, the system will do reverse DNS lookup to configure the terminal name. For example, if the DNS server configures the terminal IP as reverse DNS name p12345.wysespt.com, the terminal name will be configured as p12345.
TimeServer=<server_list> [TimeFormat=24-hour format, 12-hour format}] [DateFormat={yyyy/mm/dd, mm/dd/yyyy, dd/mm/yyyy}] [GetBiosDT={no, yes}]	**TimeServer** — Specifies the SNTP time servers to use for time retrieval. If a time server is not defined, the client CMOS/BIOS internal clock will be used as a reference. **TimeFormat** — **Default is 24-hour format.** Specifies the time format to use. **DateFormat** — **Default is yyyy/mm/dd.** Specifies the date format to use. **GetBiosDT** — **Default is no.** Yes/no option to obtain time from BIOS/CMOS when the timeserver is not available or cannot be contacted. Example: TimeServer=time.nist.com TimeFormat="24-hour format" DateFormat=mm/dd/yyyy OR TimeServer=time.nist.com \ TimeFormat="24-hour format" \ DateFormat=mm/dd/yyyy
TimeZone=<zone value> [ManualOverride={no, yes}] [daylight={no, yes}] [start=MMWWDD end=MMWWDD] [TimeZoneName=<timezonename>] [DayLightName=<daylightname>]	**TimeZone** — Specifies the time zone if the zone is unspecified on the zero client or is used with ManualOverride. Supported zone values s are listed in the System Preference dialog box on the zero client and in TimeZone Parameter: Values. **NOTE:** The TimeZone parameter is dependent on the TimeServer=parameter. If a time server is not defined, the client CMOS/BIOS internal clock will be used as a reference. **ManualOverride** — Default is **no**. Yes/no option to override the zero client System Preference Menu setting with this TimeZone setting. TimeZone settings in the xen.ini file will be saved into NVRAM if EnableLocal=yes is set in the xen.ini file. **Daylight** — Default is **no**. Yes/no option to enable daylight saving time; MMWWDD is a 6 digit number to specify the start and the end of daylight saving time.

Parameter	Description

	IMPORTANT: The Start and End options are in the MMWWDD format, where:
	MM = Month of the year. Values are 01 to 12 for the months of the year from January to December. For example, 01 = January, 12 = December
	
	WW = Week of the Month. Values are 01 to 05 for the week of the month, 05 is the last week. For example, 01 = 1st week, 05 = the last week of the month.
	
	DD = Day of the week. Values are 01 to 07 for the day in the week from Monday to Sunday. For example, 01 = Monday, 07 = Sunday.
	
	NOTE:
	For the 2013 year, DST dates are Sunday, March 10, 2:00am and ends Sunday, November 3, 2:00am.
	
	TimeZoneName — Display name sent to the ICA session such as Eastern Standard Time.
	
	DayLightName — Display name for daylight saving time. If daylight saving time is enabled, DayLightName should be named something similar to Eastern Daylight Time, otherwise it should be the same as TimeZoneName.
	
	Overall Example:
	
	`TimeZone="GMT - 08:00" \`
	`ManualOverride=Yes Daylight=Yes Start=030107 End=110107 \`
	`TimeZoneName="Pacific Standard Time" \`
	`DayLightName="Pacific Daylight Time"`

VncPassword=<password> [encrypt={no, yes}]	**VncPassword=password** — Specifies a string of up to 8 characters as the password used for shadowing. **encrypt** — **Default is no.** Yes/no option to encrypt the password; an encrypted string is used as a password ensures US HIPPA and Congress Acts compliance. See also MaxVNCD parameter.
VNCPrompt={yes, no} [{Accept, Reject}=<value from 10 through 600>] [ViewOnly={no, yes}] [ActiveVisible={no, yes}]	**Default is yes.** **VNCPrompt** — Yes/no option to enable a VNC shadowing prompt to a user (VNCPrompt set to yes means the user will always be prompted before shadowing starts and the user will then decline or accept VNC shadowing; VNCPrompt set to no means the user will not be able to decline or accept shadowing. See also MaxVNCD parameter. **Accept, Reject** — **Default is 10.** Specifies the amount of time (in seconds) a user has to accept or reject the VNC shadowing prompt before the client desktop is shadowed. **ViewOnly** — **Default is no.** Yes/no option to specify that the desktop being shadowed can only be viewed by the person who is shadowing no keyboard or mouse events are allowed to interfere with the zero client being shadowed. **ActiveVisible** — **Default is no.** Yes/no option to display a VNC session-end notice after the VNC session ends.

Parameter	Description
VPN=openconnect [Description=string_description] [Server=server_ip_or_name] [Username=username_string] [Password=password_string] [Autoconnect={yes,no}] [Username-enc=encrypted_username_string] [Password-enc=encrypted_password_string] Folder=[folder]	The INI **openconnect** enables you to connect to Cisco AnyConnect VPN servers, that use standard TLS protocols for data transport. **Description** specifies the session name. The length of the string is limited to 21 characters. **Server** specifies the VPN server IP or the VPN server name. The length of the string is limited to 63 characters. **Username** specifies the login username. The length of the string is limited to 31 characters. **Password** specifies the login password. The length of the string is limited to 31 characters. **Autoconnect** specifies the option to enable or disable auto-connect on system startup. **Username-enc**— Specifies AES encrypted Login Username **Password-enc**— Specifies AES encrypted Login Password **Folder**— Specifies the grouping of connections. Displays the folder on ThinOS Lite desktop only if the mode is classic mode and the parameter signon is set as signon=yes icongroupstyle=folder. The folder can include sub folders.
WDMFlash=flash_size	The specified value will be saved into NVRAM, and then reports to the WDM server. This statement ensures that all the units would function with DDC regardless of flash size. This statement is valid for all platforms and replaces the previous S10WDMFlash statement.
WakeOnLAN={yes, no}	**Default is yes.** Wake-on-LAN allows a ThinOS Lite to be turned on or woken up by a network message. If WakeOnLAN=yes, ThinOS Lite will respond for the Wake-On-LAN packet for a remote wake up. If WakeOnLAN=no, ThinOS Lite will not respond for the Wake-On-LAN **NOTE: To use the WakeOnLAN parameter with a ThinOS Lite, the ThinOS Lite must use BIOS version 1.0B_SPC001 or later.**
WDAService=yes [Priority ={WDM, WMS, “WDM;WMS”, “WMS;WDM”}] [interval = {0-65535}] [disableNotice={yes, no}] [disableCancel={yes, no}] [noticeTime={0-255}] [enableReminder={yes, no}]	WDA Service always runs in the background. If priority is available, WDA discovers the protocol according to it. **Priority**—There are only two protocols available now - WDM, and Wyse Management Suite. For example, if priority=WDM; WDM, WDA tries to discover the WDM server and tries to check-in, and if it fails to check-in to WDM server, it tries to check-in the device to Wyse Management Suite server. **interval**—If interval is available, WDA rediscovery delay after a failed check-in (both Wyse Management Suite and WDM failed) is changed to interval minutes. The default value is 0. (WDA rediscovery delay is 24 hours). For example, if you set WDAService=yes interval=30, WDA rediscovery delay is set as 30 minutes.

Parameter	Description
	disableNotice—If disableNotice=yes, and the configuration from WDM is received, the count down prompt window is not displayed. The default value is no. **disableCancel**—If disableCancel=yes, there is no possibility to cancel count down prompt for WDM (device is going to reboot). **noticeTime**—If noticeTime is available, the time of countdown prompt is changed to time set using this parameter. Default value is 20. For example, WDAService=yes disableNotice=no disableCancel=yes noticeTime0 **enableReminder**—If enableReminder is set to yes, the reboot warning window is displayed and the user has an option to postpone the reboot. The default value is no. Example: WDAService=yes enableReminder=yes Whenever a reboot is required from Wyse Management Suite agent, a warning dialog window is displayed. The user can postpone the reboot for as many times set by the admin.
WDMService={yes, no} [DHCPinform={no, yes}] [DNSLookup={no, yes}] [QuickMode={yes, no}] [Discover={yes, no}] [SecurityMode={default, full, warning, low}]	The value is set to no, to disable the WDM agent. The default is yes. Discovering the WDM server is supported by the following: 1 DHCP option tag values received from standard or WDM proxy DHCP service for vendor class “RTIAgent” 2 .DNS service location record "_wdmserver._tcp" 3 DNS host name lookup "wdmserver"If WDMService=yes, set DHCPinform=yes will do #1, set DNSLookup=yes will do #2 and #3. If QuickMode is set to yes, the rapport agent will not block any other process during ThinOS Lite boot up and increases the boot time of ThinOS Lite. If Discover=yes is specified, rapport discovers WDM server information from the DHCP option tag, DNS service location record, and DNS host name. If the WDM server is discovered, the WDM server UI is protected on device. **Default=yes.** **NOTE: if "file server" is changed by WDM server, device will reboot automatically to make sure all settings from WDM server take effect. Default = yes.** SecurityMode specifies the SSL certification validation policy. If set to default, it will apply SecurityPolicy setting.If set to full, the SSL connection needs to verify server certificate. If it is untrusted, then drop the connection. If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it's up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, and the default value of the setting is default. If the settings are factory default, or if you are upgrading to ThinOS Lite 2.3 for the first time, the value is temporarily set to low. After loading any INI, it goes to Default.
WDMServer=<server_list> [Retry=<retry number value>]	**WDMServer** — Specifies a list of IP addresses or DNS name, separated by using a comma for the WDM servers. Once specified, it is saved in non-volatile memory. [Intro build 2.0_013] **Retry** — Determines the number of attempts to retry a contact to WDM servers.

Parameter	Description
WINSServer=<server_list>	Specifies the WINS server address. The WINSserver is an IP list separated by ";" or ",", with a maximum list size of 2.

Connect Parameter: Options

This topic provides the supported options for the Connect parameter in ICA supported connections.

ICA connect options

Table shown here contains the supported options used for ICA connections (after you use the **Connect=ICA** parameter/selection).

IMPORTANT:

If an option has an underlined value (default), that option and default value will automatically be used with Connect=ICA; options without underlined values can also be used if you want to, but are not automatically used with Connect=ICA. In addition, when using options, you can leave the default value or change it to another value shown.

For example, in the following case where:

Connect=ICA

[Option1={0, 1}]

[Option2={1, 2, 3, 4}]

Since you are using Connect=ICA, then Option 1 and its default value 0 will automatically be used as Option 1 has an underlined value (default of 0). You can still use Option 2 if you want to, however, Option 2 is not automatically used with the parameter as Option 2 does not have a default value.

NOTE:

Any option in ICA Connect Options that is used in a {username}.ini file will return to the default value set for that option in the wnos.ini file after a user sign-off. For example, if your {username}.ini file contains the option Reconnect=yes so that a lost connection will restart 20 seconds after disconnection; and you sign off the thin client, then the Reconnect value will return to the original default value of no (Reconnect=no) contained in the wnos.ini file—so that others who sign in can use their own user profile; assuming the administrator has not changed the default values in the wnos.ini.

ICA connect: options

Table 23. ICA connect: options

Option	Description
Alternate=[no, yes]	**Default is no**. Yes/no option to use an alternate IP address returned from an ICA master browser to get through firewalls.
AudioQualityMode={0, 1, 2, 3}	**Default is 0**. Specifies the audio quality of a session. 0 – Default 1 – High Quality

Option	Description
	2 – Medium Quality 3 – Low Quality
Autoconnect={0 to 99}	**Default is 0**. Use for automatically starting a session after you sign in, if sign-on is enabled. The value of 0 – 99 is the delay in seconds before auto-starting the session.
AppendUsername=1	This enhancement allows user names to display in the title bar of an ICA session at the client side.
Browserip=list of browsers	List of IP addresses or DNS registered names to specify ICA browsers. List items must be separated by semicolons or commas.
Colors={256, 32k, 64k or high, 16m, true}	**Default is high**. Session color mode. For faster display performance, use 256 colors for the session. • 256 is 8-bits • 32k is 15-bits • 64k or high is 16-bits • 16m is 24-bits • true is 32-bits **NOTE:** • 64k is the same value as high. • 16m — 24-bits over ICA is only supported by Windows XP and Windows 2003 server. It is not supported by Windows Server 2008 or newer. • true — 32-bit remote connections are not supported by Windows XP or Windows 2003 server. It requires Windows Vista, Windows Server 2008, or newer with ICA.
Command=start command	A string of commands to be executed after logging on to the server. This entry is limited to 127 characters.
Description=string description	Connection description. Enclose the string description in quotation marks if there are embedded blanks or single quotes. For quotation marks, use common-practice nesting rules. Maximum of 38 characters are allowed.
Directory=working directory	A directory to be used as the working directory after logging on to the server. Maximum of 63 characters are allowed.
Disablesound={no, yes, 2} or {**0**, 1, 2}	**Default is no**. Specifies whether or not to disable remote sound upon connection start.
Domainname={domain name,$DN}	Domain name to use in a Windows network. $DN specifies that the thin client sign-on domain name is used. Maximum of 19 characters are allowed.

Option	Description
Encryption={None, Basic, 40, 56, 128, Login-128}	**Default is Basic**. Connection security encryption level. The highest level is 128-bit security (Login-128 option is 128 bit encryption for login only).The lowest is None. **NOTE:** The server must support the specified level of encryption or the connection will fail.
Fullscreen={no, yes}	**Default is no**. Yes/no option to run the session in full screen. If Fullscreen=no then the session runs in a windowed screen.
Host=[name, IP, $SYS VAR] or Application=published application	**Host** — A list of server hostnames or IP addresses to which the thin client will attempt to connect. The next server on the list is attempted if the previous one failed. List items must be separated by semicolons or commas. **NOTE:** $UN (see System Variables) specifies that the sign-on user name is used and should be set in a {username}.ini file. If set to Host=$UN in a {username}.ini file, the hostname will display as the sign-on user name. If set to Host=$UN in a wnos.ini file, the hostname will display as the default start. **Application** — Defines the published application to launch. Application is required if no host is specified.
HttpBrowsing={no, yes}	**Default is no**. Yes/no option to select an http browsing protocol. Use HttpBrowsing=no for User Datagram Protocol (UDP). **NOTE:** This option is used to override the default method of browsing established in the ICABrowsing parameter.
Icon={default, bitmap file}	Specifies an icon to appear on the thin client desktop for a connection. Use Icon=default to display a system default icon for a connection. To use an icon other than the default icon, enter the name with extension of the bitmap file; ensure that the file is located in the FTP server wnos\bitmap directory. If Icon= is not specified and the icon is not specified by a PNAgent/PNLite server, no icon is displayed for a connection.
KeepAlive={0 to 127}	Specifies the number of minutes to keep a session connected after the session is inactive. During this period, one dummy packet will be sent to the server if network traffic is lost. Default is **10**.
LocalCopy={no, yes}	**Default is no**. Yes/no option to save the connection to the local NVRAM.

Option	Description
	The connection description of the Description option is used as the index key into the local connection table. If a match is found, then the entry is updated. Otherwise, a new entry is created. Maximum total of local entries is 16.
Logon_mode={local-user, smartcard, user-specified}	**Default is local-user**. Specifies how users authenticate to the selected application set or ICA connection.
Lowband={no, yes}	**Default is no**. Yes/no option to enable optimization for low speed connections such as reducing audio quality and/or decreasing protocol-specific cache size.
Mapdisks={no, yes}	**Default is no**. Yes/no option to auto-connect and map any connected USB flash drive upon connection start.
Mapdisksunderz	**IMPORTANT: : DISCONTINUED. DO NOT USE** .
[NO_FontSmoothing={no, yes}]	**Default is no**—font smoothing is enabled by default. Yes/no option to disable font smoothing. If set to yes, the font smoothing is disabled.
NoReducer={no, yes}	**Default is no**. Yes/no option to turn off compression. Default is no, which enables compression. To turn off compression, enter yes. Used here is an option of the Connect statement. It sets the value of NoReducer only for this specified connection. **NOTE:** By default the ICA protocol compresses the data to minimize the amount of data that needs to traverse the network. This compression can be as much as 50 percent for text-based applications such as Microsoft Word and 40 percent less for graphics applications than the data streams that are not compressed.
OnScreen={1-6}	In multi monitor span mode, this value indicates which screen session must display fullscreen.
Password={password, $SYS_VAR}	Password to log-in to the application server. Either a conventional login password or a variable can be used. Maximum of 19 characters are allowed. The value of password is a conventional login password. The value of $SYS_VAR is a system variable found in Table: System variables.

Option	Description
	IMPORTANT: The application server password is not encrypted; it is strongly recommended not to specify it. The user will be prompted to enter the password when the connection is made. This application server password directive never starts a line, so it can be distinguished from the thin client user sign-on password which does starts a line. **NOTE:** The Password option is not written into a {username}.ini file by a user. When the **New Password** check box is selected, the system writes the new, changed password into the {username}.ini file with encryption. This password is then checked against the sign-on password with encryption to determine whether sign-on is successful.
Password-enc=an encrypted password	Specifies an encrypted string as a password for a connection.
Reconnect={no, yes, 1 to 3600 (seconds)}	**Default is no**. Controls automatic reconnection to an application after a server disconnection. yes — Use to restart the connection; the default delay time for yes reconnect is 20 seconds. no — Use to prevent reconnection after a disconnect. 1 to 3600 — Use an integer value of 1 to 3600 seconds to restart the connection after the delay you want. For example, use 50 and the automatic reconnection to an application will occur after 50 seconds.
Resolution=[default, Seamless, <monitor resolution>]	**Default is default**. Specifies the connection display resolution. default — Starts the connection using the current desktop display setting with no window frame and border. Seamless — Available for use if the connection is to a published application. For Seamless connections, the MetaFrame hosts select the best-fit connection window for applications. <monitor resolution> — Resolution values you can use in the form X x Y depending on your client. Example for monitor resolution: 1024 x 768. See the Release Notes of your client.
SessionReliability={no, yes}	**Default is no**. Yes/no option to enable session reliability. **NOTE:** ThinOS thin clients do not support UDP browsing to obtain a new configuration about session reliability on the server. The thin client always connects to the default port.
UniSession={no, yes}	**Default is no**.

Option	Description
	Yes/no option to use a unisession. The connection will launch only once at a time.
UnmapClipboard={no, yes}	**Default is no**. Yes/no option to disable clipboard redirection for an ICA session if redirecting the clipboard.
UnmapPrinters={no, yes}	**Default is no**. Yes/no option to not auto-connect to local printers when the connection starts.
UnmapSerials={no, yes}	**Default is no**. Yes/no option to not auto-connect to local serials when the connection starts.
UnmapUSB={no, yes}	**Default is no**. Yes/no option to not auto-connect to local USB devices (Virtual USB) when the connection starts.
Username=[username, $SYS_VAR]	Username to log-in to the application server. Either a conventional login username or a variable can be used. Maximum of 31 characters are allowed. The value of username is a conventional login username. The value of $SYS_VAR is a system variable. **NOTE:** The combination of all the variables such as $IP@$DN are also supported.
Username-enc=an encrypted username	Specifies an encrypted string as a username for a connection.
[WyseVDA={no, yes}]	**Default is no**. Yes/no option to enable Wyse Virtual Desktop Accelerator for all ICA sessions.

TimeZone Parameter—Values

Using the TimeZone parameter, Table “TimeZone Parameter: Values” contains the zone value options that can be used.

For Example:

```
TimeZone="GMT - 08:00" ManualOverride=Yes Daylight=Yes \
Start=030207 End=110107 TimeZoneName=Pacific \
DaylightName=Pacific
```

Remember to use quotation marks (" ") since the option includes spaces. The example above uses the " \" to break a single continuous line into multiple likes for easier reading with no" \" on the last line of the parameter.

NOTE:

The Start and End options are in the MMWWDD format, where:

MM = Month of the year. Values are 01 to 12 for the months of the year from January to December.

For example, 01 = January, 12 = December

WW = Week of the Month. Values are 01 to 05 for the week of the month, 05 is the last week.

For example, 01 = 1st week, 05 = the last week of the month.

DD = Day of the week. Values are 01 to 07 for the day in the week from Monday to Sunday.

For example, 01 = Monday, 07 = Sunday

U.S. Only:

For the 2013 year, DST dates are Sunday, March 10, 2:00am and ends Sunday, November 3, 2:00am.

Start=030207 End=110107

For the 2014 year, DST dates are Sunday, March 9, 2:00am and ends Sunday, November 2, 2:00am.

Start=030207 End=110107

TimeZone Parameter—Values

Table 24. TimeZone Parameter Values

Geographic time zones	Time zones name
(GMT-12:00) International Date Line West	Dateline
(GMT-11:00) Coordinated Universal Time-11	UTC-11
(GMT-10:00) Hawaii	Hawaiian
(GMT-09:00) Alaska	Alaskan
(GMT-08:00) Pacific Time (US & Canada)	Pacific
(GMT-07:00) Arizona"	US Mountain
(GMT-07:00) Chihuahua, La Paz, Mazatlan	Mountain (Mexico)
(GMT-07:00) Mountain Time (US & Canada)	Mountain
(GMT-06:00) Central America"	Central America
(GMT-06:00) Central Time (US & Canada)	Central
(GMT-06:00) Guadalajara, Mexico City, Monterrey	Central (Mexico)
(GMT-06:00) Saskatchewan	Canada Central

Geographic time zones	Time zones name
(GMT-05:00) Bogota, Lima, Quito, Rio Branco	SA Pacific
(GMT-05:00) Chetumal	Eastern (Mexico)
(GMT-05:00) Eastern Time (US & Canada)	Eastern
(GMT-05:00) Indiana (East)	US Eastern
(GMT-04:30) Caracas	Venezuela
(GMT-04:00) Asuncion	Paraguay
(GMT-04:00) Atlantic Time (Canada)	Atlantic
(GMT-04:00) Cuiaba	Central Brazilian
(GMT-04:00) Georgetown, La Paz, Manaus, San Juan	SA Western
(GMT-03:30) Newfoundland	Newfoundland
(GMT-03:00) Brasilia	E. South America
(GMT-03:00) Cayenne, Fortaleza	SA Eastern
(GMT-03:00) City of Buenos Aires	Argentina
(GMT-03:00) Greenland	Greenland
(GMT-03:00) Montevideo	Montevideo
(GMT-03:00) Salvador	Bahia
(GMT-03:00) Santiago	Pacific SA
(GMT-02:00) Coordinated Universal Time-02	UTC-02
(GMT-01:00) Azores	Azores
(GMT-01:00) Cape Verde Is.	Cape Verde
(GMT) Casablanca	Morocco
(GMT) Coordinated Universal T+A35:A98ime	UTC
(GMT) Dublin, Edinburgh, Lisbon, London	GMT
(GMT) Monrovia, Reykjavik	Greenwich
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	W. Europe
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	Central Europe
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	Romance

Geographic time zones	Time zones name
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb	Central European
(GMT+01:00) West Central Africa	W. Central Africa
(GMT+01:00) Windhoek	Namibia
(GMT+02:00) Amman	Jordan
(GMT+02:00) Athens, Bucharest	GTB
(GMT+02:00) Beirut	Middle East
(GMT+02:00) Cairo	Egypt
(GMT+02:00) Damascus	Syria
(GMT+02:00) E. Europe	E. Europe
(GMT+02:00) Harare, Pretoria	South Africa
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	FLE
(GMT+02:00) Istanbul	Turkey
(GMT+02:00) Jerusalem	Israel
(GMT+02:00) Kaliningrad (RTZ 1)	Russia TZ 1
(GMT+02:00) Tripoli	Libya
(GMT+03:00) Baghdad	Arabic
(GMT+03:00) Kuwait, Riyadh	Arab
(GMT+03:00) Minsk	Belarus
(GMT+03:00) Moscow, St. Petersburg, Volgograd (RTZ 2)	Russia TZ 2
(GMT+03:00) Nairobi	E. Africa
(GMT+03:30) Tehran	Iran
(GMT+04:00) Abu Dhabi, Muscat	Arabian
(GMT+04:00) Baku	Azerbaijian
(GMT+04:00) Izhevsk, Samara (RTZ 3)	Russia TZ 3
(GMT+04:00) Port Louis	Mauritius
(GMT+04:00) Tbilisi	Georgian
(GMT+04:00) Yerevan	Caucasus

Geographic time zones	Time zones name
(GMT+04:30) Kabul	Afghanistan
(GMT+05:00) Ashgabat, Tashkent	West Asia
(GMT+05:00) Ekaterinburg (RTZ 4)	Russia TZ 4
(GMT+05:00) Islamabad Karachi	Pakistan
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	India
(GMT+05:30) Sri Jayawardenepura	Sri Lanka
(GMT+05:45) Kathmandu	Nepal
(GMT+06:00) Astana	Central Asia
(GMT+06:00) Dhaka	Bangladesh
(GMT+06:00) Novosibirsk (RTZ 5)	Russia TZ 5
(GMT+06:30) Yangon Rangoon	Myanmar
(GMT+07:00) Bangkok, Hanoi, Jakarta	SE Asia
(GMT+07:00) Krasnoyarsk (RTZ 6)	Russia TZ 6
(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi	China
(GMT+08:00) Irkutsk (RTZ 7)	Russia TZ 7
(GMT+08:00) Kuala Lumpur, Singapore	Singapore
(GMT+08:00) Perth	W. Australia
(GMT+08:00) Taipei	Taipei
(GMT+08:00) Ulaanbaatar	Ulaanbaatar
(GMT+08:30) Pyongyang	North Korea
(GMT+09:00) Osaka, Sapporo, Tokyo	Tokyo
(GMT+09:00) Seoul	Korea
(GMT+09:00) Yakutsk (RTZ 8)	Russia TZ 8
(GMT+09:30) Adelaide	Cen. Australia
(GMT+09:30) Darwin	AUS Central
(GMT+10:00) Brisbane	E. Australia
(GMT+10:00) Canberra, Melbourne, Sydney	AUS Eastern

Geographic time zones	Time zones name
(GMT+10:00) Guam, Port Moresby	West Pacific
(GMT+10:00) Hobart	Tasmania
(GMT+10:00) Magadan	Magadan
(GMT+10:00) Vladivostok, Magadan (RTZ 9)	Russia TZ 9
(GMT+11:00) Chokurdakh (RTZ 10)	Russia TZ 10
(GMT+11:00) Solomon Is., New Caledonia	Central Pacific
(GMT+12:00) Anadyr, Petropavlovsk-Kamchatsky (RTZ 11)	Russia TZ 11
(GMT+12:00) Auckland, Wellington	New Zealand
(GMT+12:00) Coordinated Universal Time+12	UTC+12
(GMT+12:00) Fiji	Fiji
(GMT+13:00) Nuku'alofa	Tonga
(GMT+13:00) Samoa	Samoa
(GMT+14:00) Kiritimati Island	Line Islands

Examples of Common Printing Configurations

This section provides examples on using the **Printer Setup** dialog box and ThinOS Lite INI parameters for common printing situations. Use the following guidelines mentioned below in addition to the information provided in Connecting to a Printer.

IMPORTANT: Host-based printers are not supported.

It includes:

- Printing to Local USB or Parallel Printers
  - Using the Printer Setup Dialog Box for Local USB or Parallel Printers
  - Using INI Parameters for Local USB or Parallel Printers
- Printing to Non-Windows Network Printers (LPD)
  - Using the Printer Setup Dialog Box for Non-Windows Printers (LPD)
  - Using INI Parameters for Non-Windows Network Printers
- Printing to Windows Network Printers (SMB)
  - Using the Printer Setup Dialog Box for Windows Network Printers (SMB)
  - Using INI Parameters for Windows Network Printers (SMB)
- Using Your Zero Client as a Print Server (LPD)
  - Using the Printer Setup Dialog Box for Configuring LPD Services
  - Using INI Parameters for Configuring LPD Services
- Configuring ThinPrint

Local USB for Printing

You can use locally attached printers through USB ports to print.

IMPORTANT:
Citrix XenApp each has own printing policies that must be configured properly to allow client side for printing. For more information on configuring printing in Citrix XenApp environment, see your vendor instructions.

Using the Printer Setup Dialog Box for Local USB Printers

Consider a following scenario, you have an HP LaserJet 4000 attached to a zero client USB port. When you connect USB printers, few printers display the Printer Name and Printer Identification fields for you.
To Configure the Printer to print locally attached printers through USB ports :

1 From the floating bar menu, click the **System Setup** , and then click **Printer**.
The **Printer Setup** dialog box is displayed.

2 Click the **Printer Setup** , and use the following guidelines for each tab :
   a **Select Port** — Select LPT1 port or LPT2 port.
   b **Printer Name** — Enter the name you want to be displayed in your list of printers, most USB direct-connected printers display their printer name automatically.

c **Printer Identification** — Enter the type or model of the printer in the exact text of the Windows printer driver name — including capitalizations and spaces most USB direct-connected printers display their printer identification automatically. In the above mentioned scenario, enter HP LaserJet 4000 Series PCL.

d **Printer Class** — You can leave this as default.

e **Enable the printer device** — Enable this option, as it enables the printer device to display on the remote host.

3 Click **OK** to save the settings.

Using INI Parameters for Local USB Printers

The INI parameters for Local USB Printers:

```
Printer=LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled=yes
```

NOTE: The PrinterID is same as that of the Windows printer driver name. For example, if a printer driver is named HP LaserJet 4000 Series PCL in Windows, then the PrinterID is same as that of the printer driver mentioned in the INI parameters including capitalizations and spaces.

Printing to Non-Windows Network Printers—LPD

ThinOS Lite can print to non-Windows network printers, if ThinOS Lite can accept LPR print requests. Most workgroup printers and large network printers provides an option to check with your vendor whether the printer can accept Line Printer Request print requests.

Once your zero client is configured to print to an LPR capable printer, the client will then redirect this printer through an ICA connection to your back end infrastructure. In this way the client will connect to your back end infrastructure and this network printer will appear as a client local printer.

Using the Printer Setup Dialog Box for Non-Windows Network Printers—LPD

To configure the Printer Setup Dialog Box for Non-Windows Network Printers (LPD):

1 From the the floating bar menu, click the **System Setup** , and then click **Printer**.

In this example we have an HP LaserJet 4200n attached to a zero client through LPR.

The **Printer Setup** dialog box is displayed.

2 Click the **LPDs** tab and use the following guidelines when printing to a non-Windows network printer:

a **Select LPD** — Select LPD1 port or LPD2 port.

b **Printer Name** — Enter name you want to be displayed in your list of printers.

c **Printer Identification** — Enter the type or model of the printer in the exact text of the Windows printer driver name — including capitalizations and spaces.

In this example, enter HP LaserJet 4200n PCL6.

d **LPD Hosts** — The DNS or WINS name of the server for the network printer. An IP address of the printer on the network can also be entered as we have used in our case example.

NOTE: If the printer is attached to another zero client on your network, the entry in the LPD Hosts box is the name or address of that zero client.

e **LPD Queue Name** — An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer used. This name can be different for each vendor. This field is required and must be correct so that the network printer accepts incoming print jobs properly. In our case example, **auto** can be used for HP LaserJet 4200n PCL6 as per documentation found on the HP website.

NOTE: If the printer is attached to another zero client on your network, the LPD Queue Name must match the content of the Printer Name box on the zero client with the printer attached.

f **Printer Class** — (Optional) You can leave this as default.

g **Enable the printer device** — Enable this option, as it enables the printer device to display on the remote host.

Using INI Parameters for Non-Windows Network Printers—LPD

The INI parameters for Non- Windows Network Printers (LPD) :

```
Printer=LPD1 \
LocalName="HP LaserJet 4200n" \
Host=10.10.10.1 \
Queue=auto \
PrinterID="HP LaserJet 4200 PCL6" \
Enabled=yes
```

NOTE: The PrinterID is same as that of the Windows printer driver name. For example, if a printer driver is named HP LaserJet 4200n PCL6 in Windows, then the PrinterID is same as that of the printer driver mentioned in the INI parameters including capitalizations and spaces.

Windows Network Printers for Printing—SMB

ThinOS Lite can print to printers that are shared by Microsoft print servers. There are some configuration requirements that need to be considered while configuring SMB printing from ThinOS Lite which may require changes to your zero client setup.

Since connecting to a Microsoft Windows Print Server requires domain credentials, you must provide the credentials to ThinOS Lite either on demand as the printer is used or by administrator setup providing credentials cached from the Dell Wyse login screen ,see **"Example 3: Defining an SMB Printer to Use User Credentials Cached by ThinOS Lite (Advanced)".** This section will discuss both methods.

Using the Printer Setup Dialog Box for Windows Network Printers—SMB

Configuring an SMB printer is this manner forces users to enter their credentials before each printing; this means they will be temporarily pulled out of their remote session to enter their credentials (this can be avoided by using an INI file as discussed in the Using INI Parameters for Windows Network Printers (SMB) section.

1 From the floating bar menu, click the **System Setup** , and then click **Printer**.

The **Printer setup** dialog box is displayed.

2 Click the **SMBS** tab and use the following guidelines when printing to a Windows network printer:

NOTE: The printer name shared by Windows must not contain any spaces or ThinOS Lite will not be able to use it.

a **Select SMB** — Select the SMB you want from the list.

b **\\Host\Printer** — Click the browse folder icon next to the box to browse your Microsoft Networks and make the printer selection you want from the network printers available the DNS name or IP address of the Windows print server on the network. After entering required domain credentials, the **Printer Setup** dialog box will display

c **Printer Name** — Enter name you want displayed in your list of printers.

d **Printer Identification** — Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

In example case, enter HP LaserJet 4100 Series PCL.

e **Printer Class** — You can leave this as default.

f **Enable the printer device** — Must be selected to enable the printer.

It enables the device so it displays on the remote host.

Click **Test Print** and you will be prompted to enter your Windows credentials, these credentials will be used to access the printer share. This is also the same dialog box that will display for a user when they attempt to print to this printer.

Using INI Parameters for Windows Network Printers—SMB

Configuring SMB printing using ThinOS Lite INI parameters is simple and an easy way to configure printers shared by a Windows server for all clients in your environment. The primary advantage of configuring SMB printing using ThinOS Lite INI parameters is that you can pre-define the domain account to use to authenticate the printer. The following examples discuss how the credentials can be supplied.

1. To Define a SMB Printer with Generic User Credentials in Plain Text

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=Username1 \
Password=Password \
Domain=contoso
```

2. To define a SMB Printer with Generic User Credentials that are Encrypted

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username-enc=PACGOGDBPKDOPGDGKC \
Password-enc=PFDBOHDBODCJPODP \
Domain=contoso
```

NOTE: In order to create the encrypted passwords for use in an INI file you will want to use a program such as ConfGen. This application has built in support for creating the encrypted strings. ConfGen can be downloaded from http://technicalhelp.de.

IMPORTANT: This is a non-supported tool that is linked solely for the purpose of this example.

3. To Define a SMB Printer to Use User Credentials Cached by ThinOS Lite (Advanced)

NOTE: This method requires that the user log in to ThinOS Lite so that the credentials can be cached for later use. The example INI section provided below provides the minimum requirements you need.

Signon=NTLM

```
Connect=ICA \
Host=1.2.3.4 \
Username=$UN \
Password=$PW \
Domain=$DN \
AutoConnect=1
```

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=$UN \
Password=$PW \
Domain=$DN
```

Using Your Zero Client as a Print Server—LPD

A ThinOS Lite zero client can be configured as a basic network print server, to share local printers with other zero clients.

Using the Printer Setup Dialog Box for Configuring LPD Services

A zero client can be configured to provide LPD (Line Printer Daemon) services making the zero client a printer server on the network. Set up the zero client that is to provide LPD print services as follows:
To configure LPD Services using the Printer Setup Dialog Box :

1 From the floating bar menu, click **System Setup** > **Network Setup** to open the **Network Setup** dialog box.
2 Enter a static IP address for the zero client.
3 From the floating bar menu, click **System Setup** > **Printer** to open the **Printer Setup** dialog box and select any of the listed ports.
4 Select LPT.
5 Name the printer in the Printer Name box.
6 Enter the **Printer Identification** type or model of the printer in the exact text of the Windows printer driver name — including capitalizations and spaces. In our example case, enter HP LaserJet 4000 Series PCL.
7 You can leave **Printer Class** as default.
8 Select **Enable the Printer Device**.
9 Select **Enable LPD service for the printer**.
10 For Setting Up Windows 2003/2008 Servers, see Setting Up Windows 2003/2008 Servers.

Setting Up Windows 2003 or 2008 Servers

To Configure Setting the Windows 2003/2008 Servers :

1 Navigate to **Control Panel** > **Administrative Tools** > **Services** and ensure the Microsoft TCP/IP Printing service is installed. If it is not, install it using the Microsoft installation instructions.
2 Add the zero client as the LPD printer by completing the following:
   a Navigate to **Control Panel** > **Printers** > **Add Printers** > **Local Printer** > **Create a new port** and select **LPR PORT**.

      NOTE: If you do not see LPR Port, ensure that the Microsoft TCP/IP Printing service is installed correctly.

   b Type the zero client IP address or DNS name in the **Name or address of host providing LPD** box.
   c Type the printer name assigned in Using the Printer Setup Dialog Box for Configuring LPD Services in the **Name of printer on that machine** box.
   d Click **OK**, and then click **NEXT**.
3 After you have selected the printer, you can perform your normal printer setup for the application server. For example, select the manufacturer printer type and printer name.

Using INI Parameters for Configuring LPD Services

Configuring LPD printing using ThinOS Lite INI parameters is simple and an easy way to configure a ThinOS Lite zero client to be a basic network print server, to share local printers with other zero clients.

Your INI parameters will look something like the following:

```
Printer=LPT1 \
Name="HP LaserJet 4000" \
```

```
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled=yes \
EnableLPD=yes
```

NOTE: The PrinterID is the exact text of the Windows printer driver name, so if a printer driver is named HP LaserJet 4000 Series PCL in Windows, then it must be exactly the same in the PrinterID field in the INI parameters including capitalizations and spaces.

Configuring ThinPrint

No ThinPrint specific configuration is available on the zero clients. Thus to be able to use ThinPrint, users must first set up their printers according to the user documentation, and then configure ThinPrint on the zero client using the Printer Setup dialog box.

To Configure the ThinPrint use the following guidelines:

- Use the **Printer Identification** field to enter a printer class (you can change the printer name as needed).
- Printer IDs are assigned (depending on the physical port) as follows:
  - COM1 = 1
  - COM2 = 2
  - LPT1 = 3 — USB printers are detected automatically on LPT1
  - LPT2 = 4
  - LPD0 = 5– The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - LPD1 = 6 — The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - LPD2 = 7 — The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - LPD3 = 8 — The LPD Queue name is transmitted as the printer name; the Printer Identification as class
  - SMB1 = 9 — In the form \\host\printershare
  - SMB2 = 10
  - SMB3 = 11
  - SMB4 = 12

To install the relevant ThinPrint product on the server use the following guidelines:

- **Printer Objects Created Manually by the Administrator** — After you install.print Engine, create a printer object on the server to use the native driver and ThinPort as a printer port. You can use any protocol (TCP or ICA) because ThinOS Lite has.print clients for all of the protocols. The printer object needs to observe ThinPrint naming conventions, for example, *HPLJ5#_:2*, in which case print jobs are sent to the local printer that has ID number *.2* by referring to.print client port ID. If no ID number is present, the.print client sends the print job to the printer set as current.
- **Printer Objects Created Automatically by ThinPrint AutoConnect** — When using ThinPrint AutoConnect, the zero client identifies with the zero client ID number 84 and thus is recognized as a zero client without a local spooler. You can also set up a template on the server that uses a native driver example, *HPLJ5*) and ThinPort, and then name this template as you want in the form _#AnyName.

  You can then make sure that the rules on ThinPrint Autoconnect [1] have been set to assign the desired local printers to use this server template. The assigned printer will then be shown in the user session using the HPLJ5 driver and ThinPort; it is named automatically according to ThinPrint naming convention with the printer name from the client side included. Alternatively, you can also define a template name according to the client printer name (replace.AnyName. with printer name 4. and 5. above for example, *_#HP Laserjet 5* so that the local printer object.HP Laserjet 5. is mapped to this template without any rules defined on the ThinPrint Autoconnect.

C

Important Notes

VNC RFB version upgrade—Since ThinOS Lite 2.0, the VNC RFB version has been upgraded to 3.8. This version upgrade provides support for applications like DameWare. Thus, an administrator can now remote into a ThinOS Lite device using either DameWare or VNC Viewer. Prior to 2.0, you could only use VNC Viewer.

D

Troubleshooting

- ThinOS Lite devices allow secure SSL connections—`SecurityMode=Full`—only after verifying the certificates. In the present scenario, the devices enforce the warning policy after you define a server using a valid IP address. The resolution for the issue will be delivered in the next ThinOS Lite release.

  The following are the workarounds to avoid the SSL connection issue:

  – Ensure that the device has a valid certificate and the correct time is selected on the device.
  – Define the server by name instead of IP address.
  – Set the value of the global security policy to high.
  – Use the following INI parameter to enforce the high security mode:
    `SecurityPolicy=high TLSCheckCN=Yes`
- Firmware/Package update—When the packages fail to update or cannot function (cannot connect desktop) after update with new version firmware; if there is further failure, a work around would be to remove all packages and re-install all of them on reboot.
- Boot up unit without monitor or with monitor power off.
  – If the thin client waits for 15 to 20 seconds and the monitor is attached or powered on within 20 seconds, the display is turned on. If the monitor is attached or powered on after 20 seconds, the monitor displays the black screen. Turn on the monitor first, and then turn on the thin client.