Dell Wyse ThinOS

Version 8.5.1 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 - 12

Rev. A03

Contents

Introduction

Thin clients running Dell Wyse ThinOS firmware are designed solely for optimal thin client security and performance. These efficient purpose-built thin clients are virus and malware resistant and offer ultrafast access to applications, files and network resources within Citrix, Microsoft, VMware and Dell vWorkspace environments, and other leading infrastructures. ThinOS based thin clients are self-managed, go from power-on to fully productive in seconds, and with no published API, locally accessible file system or browser, require no local McAfee Anti-Virus software or firewall to protect against viruses or malware.

About this guide

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

Supported products

Table 1 lists the supported Dell Wyse ThinOS products.

Table 1. Supported platforms

Platform	Processor
Wyse 5070 thin client	Celeron
Wyse 5070 thin client	Pentium
Wyse 5070 Extended thin client	Pentium

Table 2. Firmware and BIOS version

Platform	ThinOS	ThinOS with PCoIP	BIOS version	BIOS BIN file name
Wyse 5070 thin client (Celeron Processor)	X10_wnos	PX10_wnos	Dell BIOS 1.1.1	X10_bios.bin
Wyse 5070 thin client (Pentium Processor)	X10_wnos	PX10_wnos	Dell BIOS 1.1.1	X10_bios.bin
Wyse 5070 Extended thin client (Pentium Processor)	X10_wnos	PX10_wnos	Dell BIOS 1.1.1	X10_bios.bin

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, contact information and so on, visit www.dell.com/wyse/support.

What is new in this release

The following are the updates or new features in the ThinOS 8.5_115 release:

- Updated the VMware Horizon package on ThinOS to version 4.6.51718 to resolve the user trap issue on Blast protocol.
- UI enhancement that allows you to restart the client immediately or delay the restart when Wyse Management Suite policy changes need to be applied to ThinOS. See, Configuring the WDA settings.
- Updated the display priority on Wyse 5070 Extended thin client to support the latest AMD vBIOS firmware. See, Hardware capability.
- Added new INI parameters. See, *Dell Wyse ThinOS Version 8.5.1 INI Reference Guide* at www.dell.com/support.

Getting started

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

- Configuring ThinOS using the first boot wizard
- Connecting to a remote server
- Using your desktop
- Configuring thin client settings and connection settings
- Connecting to a printer
- Connecting to a monitor
- Locking the thin client
- Signing off and shutting down
- Additional getting started details

NOTE:

ThinOS is centrally managed and configured using INI files to automatically push updates and any desired default configuration to all supported thin clients in your environment — see Central configuration: Automating updates and configurations.

If no INI files are detected, you can use local dialog boxes on each thin client to make available configurations. ThinOS will save 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 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 using the First Boot Wizard

The First Boot Wizard runs the first time you start a new thin client with the ThinOS version 8.5.1. The thin client starts the First Boot Wizard application before you enter the ThinOS system 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.

You can also reset your thin client to factory default settings to enter the First Boot Wizard.

The following flowcharts depict the workflow of First Boot Wizard:

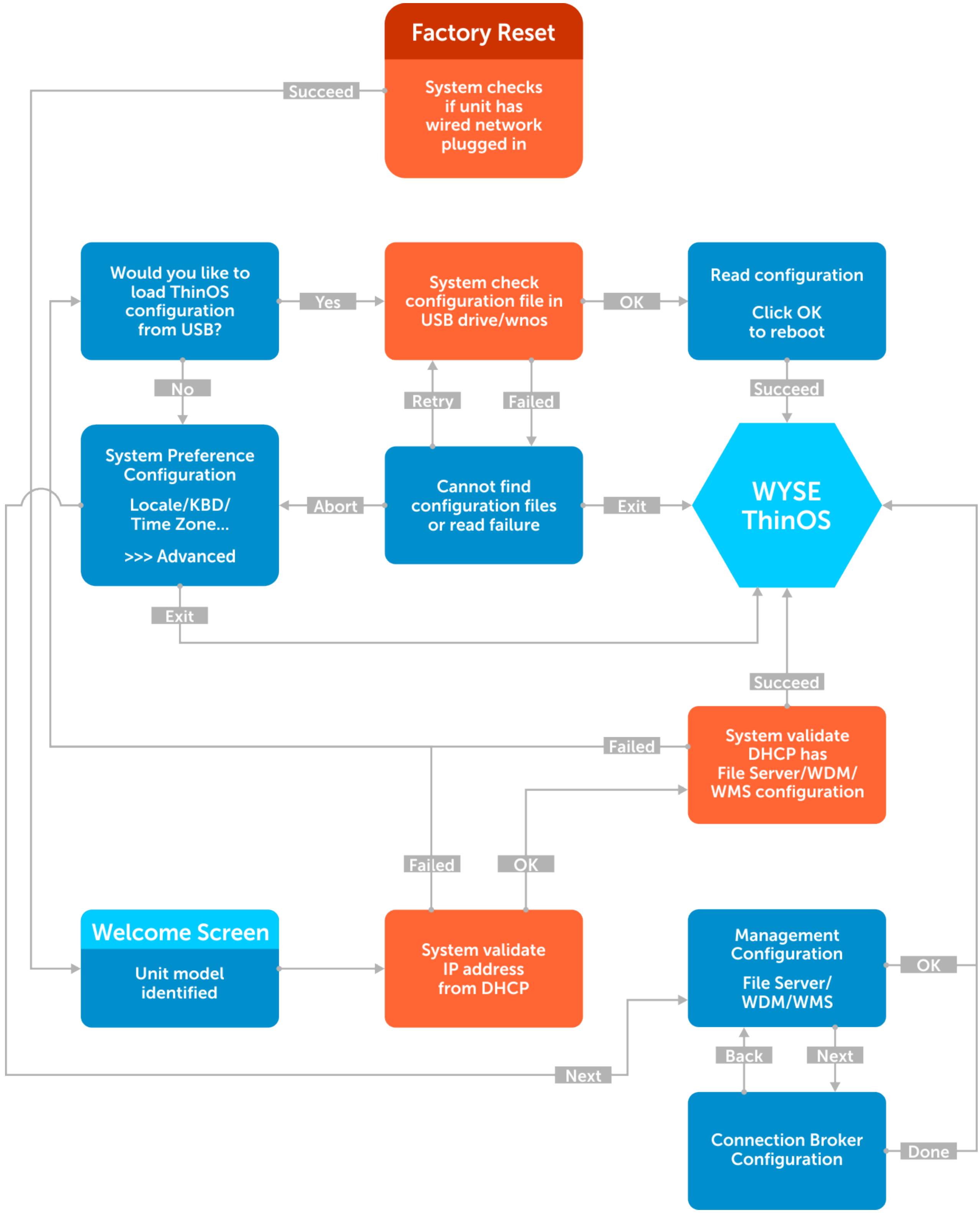

Factory Reset
System checks if unit has wired network plugged in
Succeed
Would you like to load ThinOS configuration from USB?
Yes
System check configuration file in USB drive/wnos
OK
Read configuration
Click OK to reboot
No
Retry
Failed
Succeed
System Preference Configuration
Locale/KBD/ Time Zone...
>>> Advanced
Abort
Cannot find configuration files or read failure
Exit
WYSE ThinOS
Exit
Succeed
Failed
System validate DHCP has File Server/WDM/ WMS configuration
Failed
OK
Welcome Screen
Unit model identified
System validate IP address from DHCP
Management Configuration
File Server/ WDM/WMS
OK
Back
Next
Next
Connection Broker Configuration
Done

Figure 1. First Boot Wizard—network successful

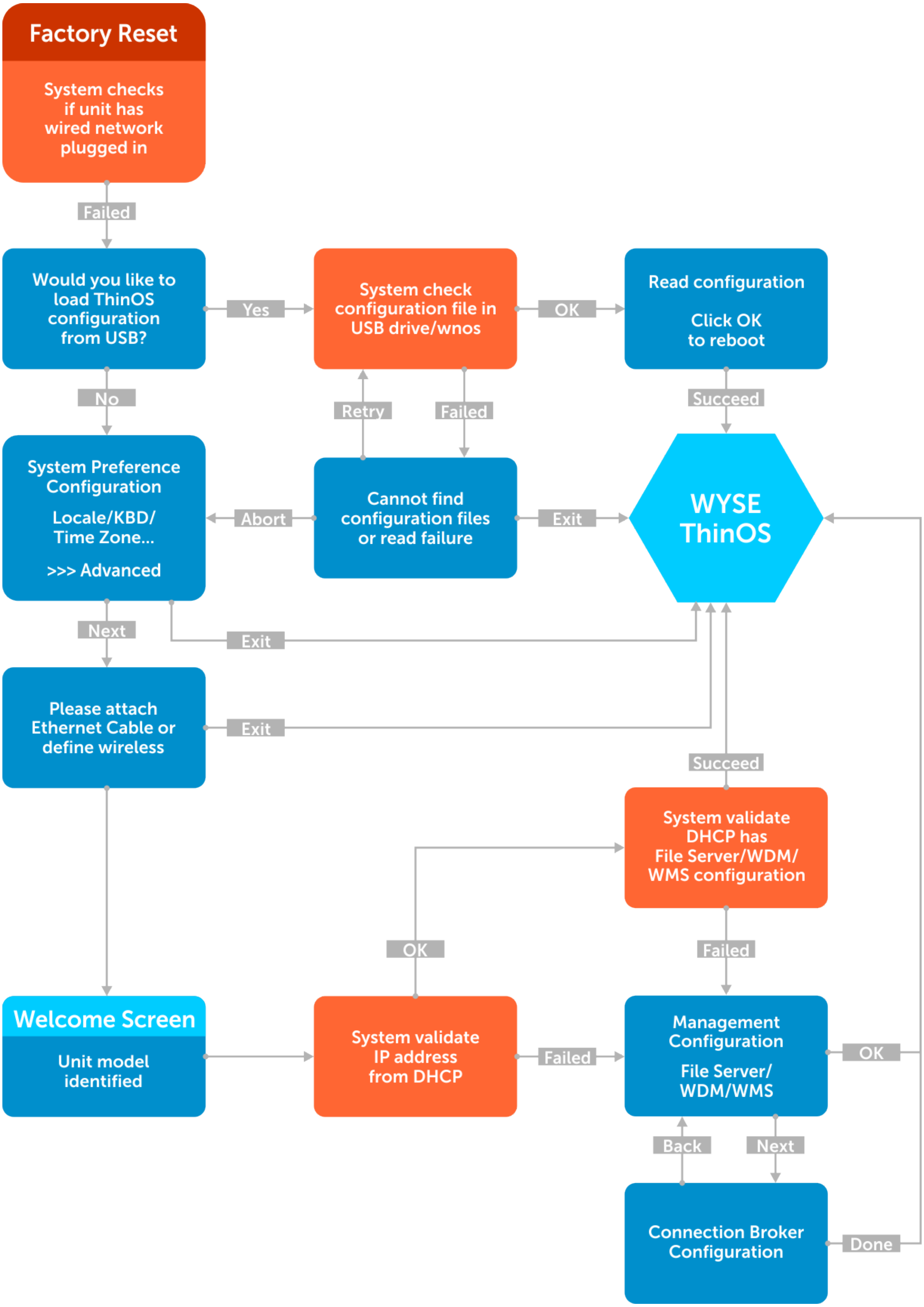

Factory Reset
System checks if unit has wired network plugged in
Failed
Would you like to load ThinOS configuration from USB?
Yes
System check configuration file in USB drive/wnos
OK
Read configuration
Click OK to reboot
Succeed
No
Retry
Failed
System Preference Configuration
Locale/KBD/ Time Zone...
>>> Advanced
Abort
Cannot find configuration files or read failure
Exit
WYSE ThinOS
Next
Exit
Please attach Ethernet Cable or define wireless
Exit
Succeed
System validate DHCP has File Server/WDM/ WMS configuration
OK
Failed
Welcome Screen
Unit model identified
System validate IP address from DHCP
Failed
Management Configuration
File Server/ WDM/WMS
OK
Back
Next
Connection Broker Configuration
Done

Figure 2. First Boot Wizard—network failure

To configure the First Boot Wizard:

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

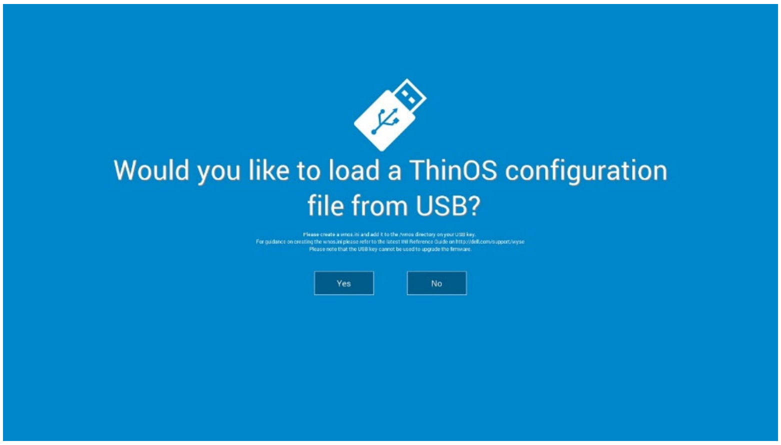
2 Turn on your thin client.

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

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

> ⓘ NOTE: **To exit the 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 configuration file from USB?** screen, do either of the following:



Would you like to load a ThinOS configuration file from USB?

Please create a wnos.ini and add it to the /wnos directory on your USB key.
For guidance on creating the wnos.ini please refer to the latest INI Reference Guide on http://dell.com/support/wyse
Please note that the USB key cannot be used to upgrade the firmware.

- To load a ThinOS configuration file from the USB drive, ensure that you create a **wnos.ini** file and add the file to the **/wnos directory** on the USB drive. Using this option, you can load packages, and wallpapers that are specified in the INI file. Plug in the USB drive to thin 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 thin client validates the configuration file in the USB drive.

  – If the ThinOS configuration file in the USB drive is correct, the **Read configuration success** message is displayed. Click **OK** to exit the First Boot Wizard, and log in to the ThinOS system desktop.

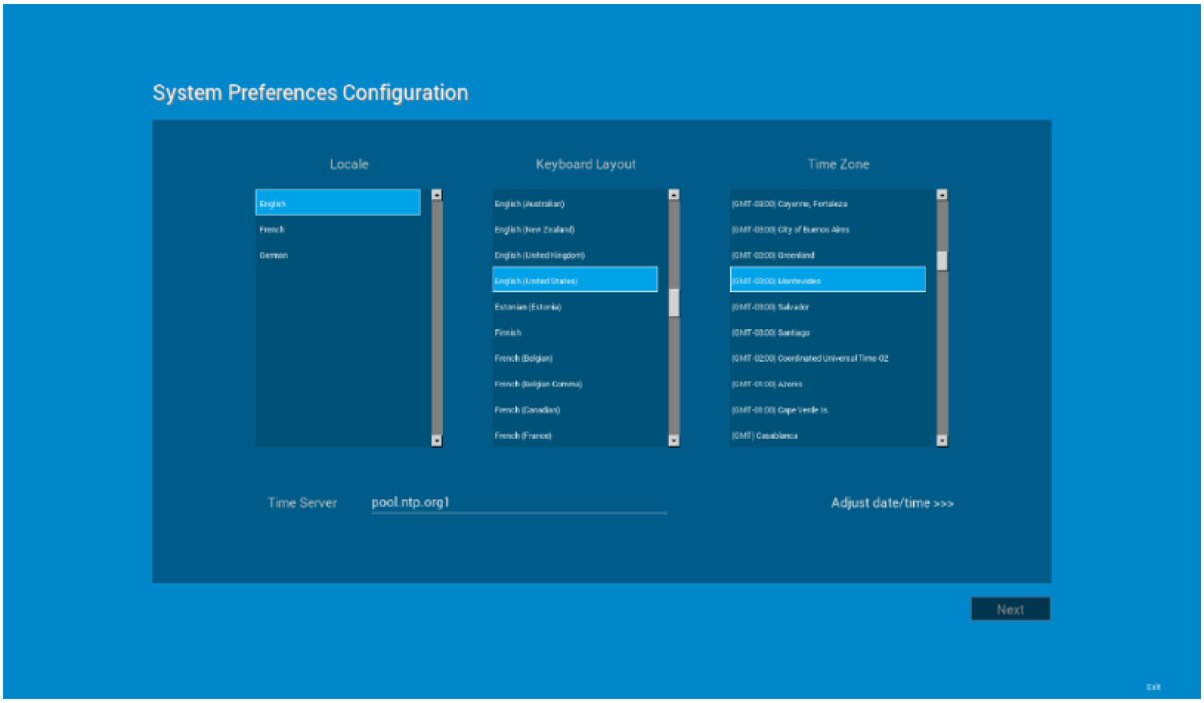
  – If the ThinOS configuration file in the USB drive is corrupted or the appropriate file is not available, then the **Cannot find configuration files, or read configuration failure** message is displayed. Upload the correct file on the USB drive, plug the USB drive again, and then click **Retry**. If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

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

    > ⓘ NOTE: **To exit the Cannot find configuration files, or read configuration failure message screen, and load the ThinOS system desktop, click Exit.**

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

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



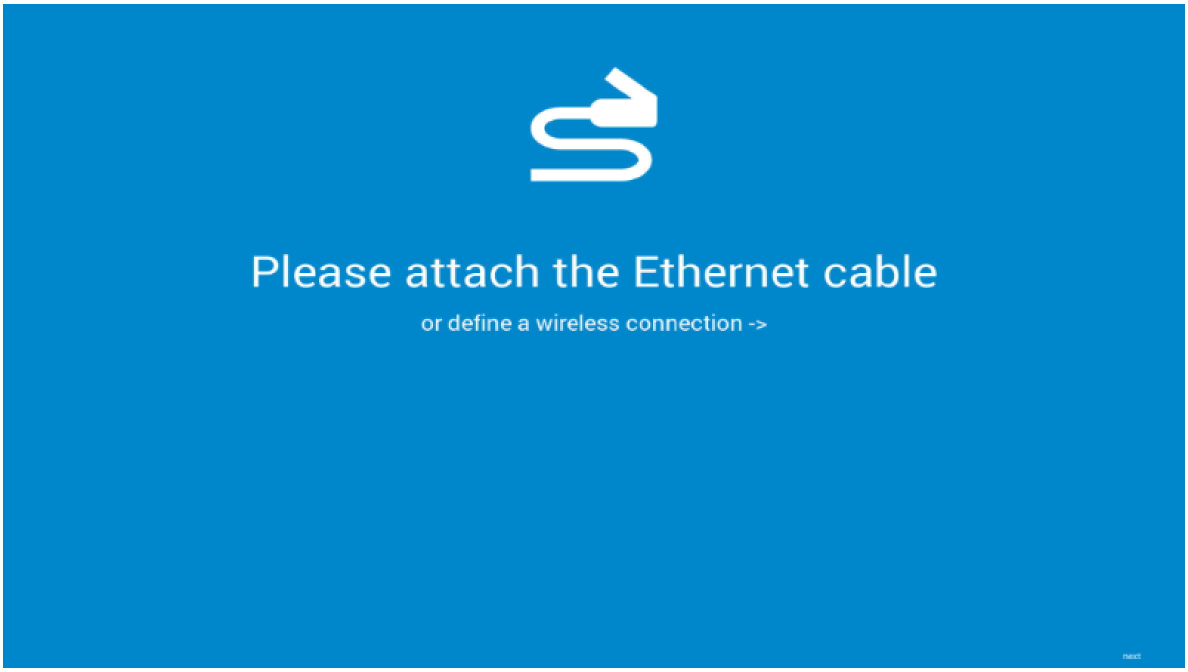
System Preferences Configuration

Time Server pool.ntp.org1

- **Locale**—Select a language to start ThinOS 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 thin 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 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.



Please attach the Ethernet cable

or define a wireless connection ->

Do either of the following:

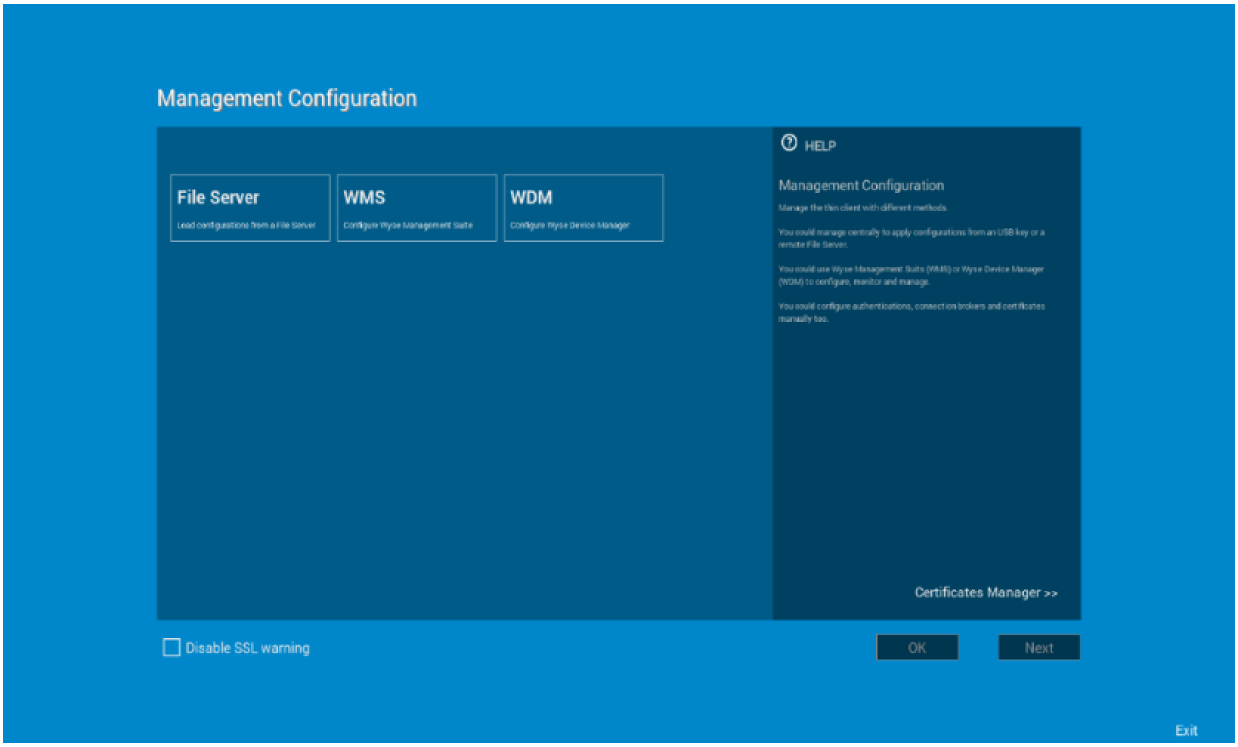
- Connect the Ethernet cable to the thin client.

- 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 thin clients without a WLAN module.
  > - To exit the **Attach the Ethernet cable** screen, and load the ThinOS system desktop, click **Exit**.

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

5. Click **Next** to enter the **Management Configuration** setup.
6. On the **Management Configuration** screen, configure the following:



Manage the thin client with different methods.

You could manage centrally to apply configurations from an USB key or a remote File Server.

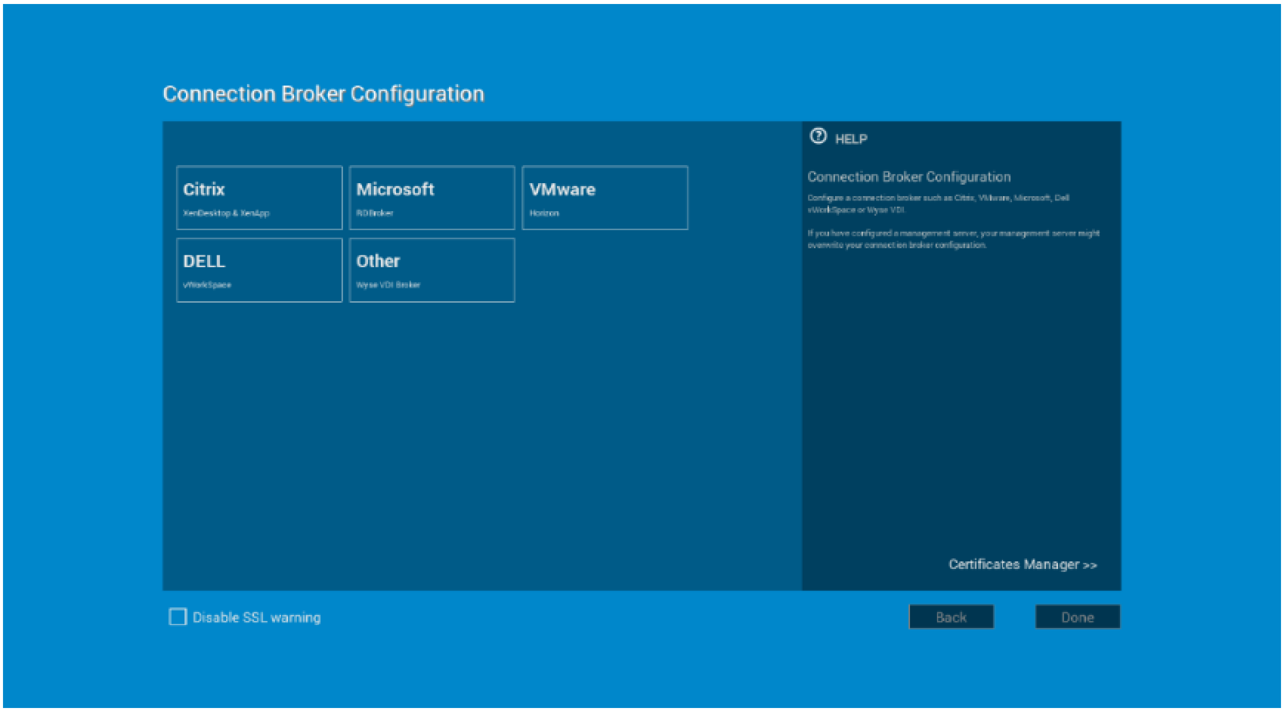
You could use Wyse Management Suits (WMS) or Wyse Device Manager (WDM) to configure, monitor and manage.

You could configure authentications, connection brokers and certificates manually too.

- **File Server**—Enter the file server details to apply configurations including INI files, firmware, packages, and so on, from a file server.
- **WMS**—Enter the group registration key and the Wyse Management Suite server URL to register the thin 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 system desktop, click Exit.**

7. Click **Done** to exit the First Boot Wizard or click **Next** to enter the **Connection Broker Configuration** setup.
8. On the **Connection Broker Configuration** screen, configure the following:



Connection Broker Configuration

Configure a connection broker such as Citrix, VMware, Microsoft, Dell vWorkSpace or Wyse VDI.

If you have configured a management server, your management server might overwrite your connection broker configuration.

- **Citrix**—The broker allows you to connect to full desktops using XenDesktop or individual applications using 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 thin 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 thin client.
- **Microsoft**—The broker allows you to connect to the virtual desktops using RemoteApp and Desktop connection. Enter the host name or IP address of the broker connection.
- **VMware**—The broker allows you to connect to the remote desktops using VMware Horizon Client.
  - **Server Address**—Enter the host name or IP address of the broker connection.
  - **Enable theme: VMware View**—Select this check box to set the ThinOS desktop theme to VMware View mode.
- **DELL**—The broker allows you to connect to the virtual desktops or applications using Dell vWorkspace. Enter the host name or IP address of the broker connection.
- **Amazon WorkSpaces**—The broker allows your PCoIP clients to connect to virtual desktops that run on AWS. Enter the host name/IP address/FQDN of the broker connection.

  > NOTE: **Amazon WorkSpaces option is applicable only to the PCoIP clients.**
- **Other**—The broker allows you to connect to the virtual desktops or applications using other supported protocols. Enter the host name or IP address of the broker connection.
- **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 steps 6 and 7.**

The device exists from the First Boot Wizard mode, and the ThinOS 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 thin client before starting the thin 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. For more information, see Configuring the Network Settings.

Central Configuration — If you are configured for automatic detection using INI files — see *Dell Wyse ThinOS INI Guide* , your thin client will automatically detect and connect to the configured remote services during the boot-up process. Press the power button to turn on your thin 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.

> ⓘ NOTE:
>
> Although the thin client will default to the Classic Desktop for INI backward compatibility, you can configure the thin client to display the Zero Desktop by using the SysMode=VDI parameter in the INI files or by selecting the desktop option in the dialog box. For more information, see Using Your Desktop.

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 thin client knows the location of your server, it automatically connects to the server for login when you start the thin 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. Click the **System Settings** icon on the Zero Toolbar to open the System Settings menu, and then click **Remote Connections** to open the **Remote Connections** dialog box.
2. Click the **Broker Setup** tab of the **Remote Connections** dialog box to configure one of the following connections:
   - ICA or RDP connection —Select **None**, select **ICA** or **RDP**, click **Configure Connection**, and then follow the wizard.
   - A specific broker server connection — Select Microsoft, Citrix Xen, Dell vWorkspace, VMware View, Amazon WorkSpaces or Other, and then enter the IP Address for the server in the **Broker Server** box.

   > ⓘ **NOTE: For more details, see Configuring the Remote Connections.**
3. Click **OK**, and then restart the thin client.

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

   > ⓘ NOTE:
   >
   > - If an ICA or RDP connection is configured— After thin client restarts, click the **Home** icon on the Zero Toolbar to open the list of available connections. Click the ICA or RDP connection you created, and then log in.
   > - If a specific Broker Server connection is configured— After thin 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 see after logging on to the server depends on the administrator configurations.

- **Users with a Classic Desktop**—will see the classic ThinOS desktop with full taskbar, desktop, and Connect Manager familiar to ThinOS users. This option is the default out-of-the-box experience and is recommended for terminal server environments with published applications and for backward compatibility with ThinOS 6.x versions. For more information on using the Classic Desktop, see Classic Desktop Features.

- **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.

In any desktop case, you can select the desktop option you want (Classic Desktop or Zero Desktop) and create the connections you need using the Visual Experience tab on the **Remote Connections** dialog box.To open the **Remote Connections** dialog box, perform one of the following tasks:

- **Classic Desktop** — Click User Name, and then select **System Setup** > **Remote Connections**.

  ⓘ NOTE: **User Name is the user who is logged-on and is located at the lower-left pane of the taskbar**
- **Zero Desktop** — Click the **System Settings** icon on the Zero Toolbar, and then select **Remote Connections**.

Configuring thin client settings and connection settings

While the use of INI files is recommended to configure thin client settings and connection settings available to users, see How to set up automatic updates and configurations, you can use dialog boxes on a thin client to:

- Set up your thin client hardware, look and feel, and system settings, see Configuring thin client settings locally.
- Configure connection settings, see Configuring thin client settings locally.

Connecting to a printer

To connect a local printer to your thin 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. For information on connecting to printers, see Configuring the printer setup.

Connecting to a monitor

Depending on your thin 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. For information on configuring multi-display settings, see Configuring the display settings.

ⓘ NOTE:

For dual-monitor supported thin 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 thin client

To help ensure that no one else can access your private information without permission, ThinOS allows you to lock your thin client so that credentials are required to unlock and use the thin 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 thin client, then the thin client will lock. To unlock the thin 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 thin 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 thin client.
- **Use Lock Terminal from the Shortcut Menu and Shutdown dialog box** — On the Classic Desktop, right-click on the desktop and select **Lock Terminal**, or use the **Shutdown** dialog box, see Classic Desktop features. On the Zero Desktop, use the **Shutdown** dialog box, see Signing off and shutting down. To use the thin client, you must use your correct password.
- **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:

- **Classic Desktop** — Click **Shutdown** in the Connect Manager or Desktop Menu.
- **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 on the following:

- Zero Desktop features
- Classic Desktop features
- Login dialog box features
- Accessing 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 3. 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 thin 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 thin 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.

Administrators can configure the toolbar settings using either a dialog box, see Configuring the remote configurations or the SysMode parameter in the wnos.ini file, see *Dell Wyse ThinOS INI Guide*.

Table 4. Toolbar icons

Icon	What It Does
Home	Opens the list of available connections, see List of connections.
System Information	Displays thin client system information, see Accessing system information.
System Settings	Opens the System Settings menu to configure thin client system settings and perform diagnostics, see Configuring the connectivity, Configuring thin client settings locally, Central configuration: Automating updates and configurations.
Shutdown Terminal	Click the **Shutdown Terminal** icon to use the Shutdown options available on the thin client, see Signing off and shutting down. 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 thin 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. Sometimes, the list contains only default connections.

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

Table 5. 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 to change the connection options. ⓘ NOTE: **Depending on user privilege level, editing options may not be available for use.**
Add Connection	Allows you to configure or add new connections.
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 the connection in the list.

Using Zero theme

Use the zero theme option to customize the look and feel of your ThinOS for Citrix, VMware, Classic or VDI mode. To enable a zero theme, deploy the INI parameters based on your zero theme preference, and restart your thin client. The **Visual experience settings are changed** message is displayed, and the thin client loads the selected zero theme.

```
ZeroTheme={Classic,VDI,Citrix,VMware}
```

```
SysMode={Classic,VDI,Citrix,VMware}
```

INI parameters work with wnos.ini file. You can also use Wyse Management Suite to manage the configuration.

- **Citrix zero mode**—When you configure ThinOS in Citrix zero mode, the device searches for xen.ini file, and loads the Citrix zero mode. If the xen.ini file is not available, then the wnos.ini file is used during configuration. If you need to switch from the Citrix zero mode, then you must use the wnos.ini file during configuration.
- **VMware zero mode**—When you configure ThinOS in VMware zero mode, the device loads the VMware zero mode.

  ⓘ NOTE: **VMware wallpaper is used in the VMware zero mode.**

Classic desktop features

This section includes information on:

- Classic interactive desktop guidelines
- Using the Shortcut menu
- Using the Desktop menu
- Using the Connect Manager

Classic interactive desktop guidelines

The Classic desktop has a Dell Wyse default background with a horizontal task bar at the bottom of the screen.

Use the following guidelines:

- Icons representing available server connections and published applications are displayed on the background. If you pause the mouse pointer over an icon, the information about the connection will be displayed. Right-clicking on an icon opens the **Connection Settings** dialog box which displays additional information about the connection. The number of icons that can be displayed on the desktop depends on the desktop resolution and administrator configuration.
- A server connection and published application can be opened by double-clicking a desktop icon or a user can navigate to the desktop icon they want by using tab key and pressing **Enter** to initiate the connection.

- Right-clicking on the desktop provides a shortcut menu, see Using the shortcut menu.
- Clicking the User Name or clicking on the desktop, opens the desktop menu, see Using the desktop menu.

NOTE:

- User Name is the user who is logged-on and is located at the lower-left pane of the task bar.
- If configured to display by an administrator, the volume control is displayed in the right corner of the taskbar and the current time and date are shown when the cursor is placed on the time; the thin client is capable of synchronizing its clock to time provided by a Simple Network Time Protocol (SNTP) server.

Using the Shortcut menu

To use the Shortcut menu:

1. Log in as administrator.
2. Right-click on your desktop

   The **Shortcut** menu is displayed.
3. On the **Shortcut** menu, you are able to view and use the following options:
   a. **Administrator Mode**—Allows administrators to configure various settings locally on thin client.
   b. **Hide all windows**—Brings the full desktop to the foreground.
   c. **Copy to clipboard**—Copies an image of the full screen, current window or event log to the clipboard. The clipboard contents can then be pasted to an ICA or an RDP session. You can copy full screen or current window to clipboard, and can export the screenshots using the **Export Screenshot** option in Troubleshooting.
   d. **Purge clipboard**—Discards the contents of the clipboard in order to free up memory.
   e. **Lock Terminal**—Puts the thin client in a locked state if the user has signed on to the system with a password. The thin client can only be unlocked using the same password.
   f. **Group Sessions**—Enables you to open more than three ICA, RDP, PCoIP, Blast or ICA seamless sessions. The sessions are displayed as a group on the taskbar.

Using the desktop menu

To use the desktop menu:

1. Click your desktop or click your User Name.

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

   The Desktop menu is displayed.
2. On the desktop menu, you are able to view and use the following options:
   a. **System Setup** —Provides access to the following local system setup dialog boxes:
      - **Network Setup** —Allows selection of DHCP or manual entry of network settings, as well as entry of locations of servers essential to thin client operation. This menu selection is disabled for Low-privileged users. See Configuring the network settings.
      - **Remote Connections**—Allows you to configure thin client Broker connections including Microsoft, Citrix Xen, Dell vWorkspace, VMware View, Amazon WorkSpaces or Other broker server connections. For more information, see Configuring the remote connections.
      - **Central Configuration**—Allows you to configure thin client central connection settings such as file server and optional WDA server settings. For more information, see Configuring the central configurations.
      - **VPN Manager** —Allows you to configure thin client VPN manager. For more information, see Configuring the VPN manager.
      - **System Preference**—Allows user selection of thin client parameters that are matter of personal preference. For more information, see Configuring the system preferences.
      - **Display**—Allows you to configure the monitor resolution and refresh rate. For more information, see Configuring the display settings.
      - **Peripherals**—Allows you to select the peripherals settings such as audio, keyboard, mouse, serial, camera, bluetooth, and touchscreen settings. For more information, see Configuring the peripherals settings.

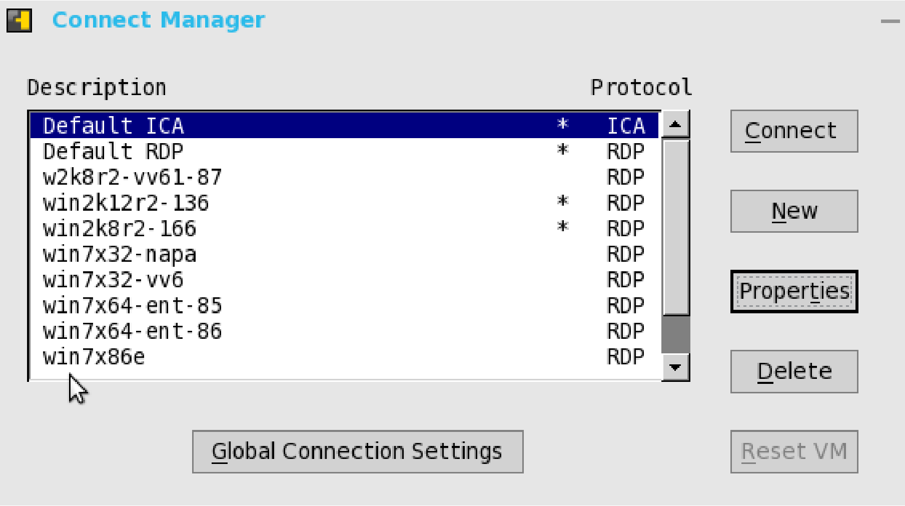
    - **Printer**—Allows configuration of network printers and local printers that are connected to the thin client. For more information, see Configuring the printer settings.
  b. **System Information**—Provides thin client system information. See Accessing system information.
  c. **System Tools**—Provides information about devices, certificates, packages, global INI, user INI, wdm or ccm.ini. See System tools.
  d. **Troubleshooting options**—Displays Performance Monitor graphs that display client CPU, Memory and Networking information, Trace and Event log settings, CMOS management extract and restore settings, and other options that are useful for ThinOS troubleshooting. For more information, See Using the troubleshooting options and System tools.
  e. **Applications**—Contains a submenu of all locally configured applications and is populated with published applications when a user is signed on using either PNLite or PNAgent.
  f. **Shutdown**—Opens the **Sign-off/LockTerminal/Shutdown/Restart the System** dialog box. See Signing off and shutting down.

Using the Connection Manager

To use the Connection Manager:

1. Click **Connect Manager** on the Taskbar.
   - The Connect Manager has a list of connection entries and a set of command buttons available for use with the connections.
   - Non-privileged users cannot view the Connect Manager.

   The **Connection Manager** dialog box is displayed.



Description		Protocol
Default ICA	*	ICA
Default RDP	*	RDP
w2k8r2-vv61-87		RDP
win2k12r2-136	*	RDP
win2k8r2-166	*	RDP
win7x32-napa		RDP
win7x32-vv6		RDP
win7x64-ent-85		RDP
win7x64-ent-86		RDP
win7x86e		RDP

2. In the Connection Manager dialog box, use the following buttons to configure the Connection Manager settings:
   a. Click **Connect** to select a connection from the list and make a connection.
   b. Click **New** to open the **Connection Settings** dialog box either directly or through the Connection Protocol menu selection for creating a new connection definition.

      The locally defined connections are added to the connection list. Be aware of the following information:

      - **High-privileged user**—Typically, all locally defined connection definitions are temporary and are lost when the user logs off and when the thin client restarts or is shut down. However, if configured by an administrator (enablelocal=yes), locally defined connection definitions can be saved in these cases.
      - **Stand-alone user**—Locally defined connections are retained when the thin client restarts or is shut down and there is no individual logon. Network configuration settings must be made locally.
   c. Click **Properties** to open the **Connection Settings** dialog box for the selected connection.

      Be aware of the following information:

      - **High-privileged user**—Can view and edit the definitions for the currently selected connection. Edits are not permanently retained when the user signs-off.
      - **Low-privileged user**—Cannot create or edit connections, but can view connection definitions.
      - **Stand-alone user**—Can permanently modify the persistent connections except when PNAgent/PNLite services are used.
   d. Click **Sign-off** to sign off from the thin client.
   e. Select a connection from the list, and click **delete** to delete the selected connection.

f Select a Virtual connection from the list, and click **Reset VM** to reset a selected virtual connection.

g Click **Global Connection Settings** tab to open and use the **Global Connection Settings** dialog box to configure settings that affect all the connections in the list.

For more information on the **Global Connection Settings** dialog box, see Global connection settings.

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 thin 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 thin client system information such as System Version, IP Address, information on devices connected to your thin client, event logs and so on. For more information, see Accessing system information.
- **Admin Mode**—Click the **Admin Mode** button to configure various settings locally on the thin client other than broker desktop configurations. For example, you can choose to manually configure the Citrix XenBroker 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**.
  - **Classic desktop**—Use the **Leave Administrator Mode** option in the Shutdown dialog box.
  - **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.**

  ⓘ **NOTE: By default there is no password needed for the 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 Dell Wyse ThinOS INI Guide.**
- **Shutdown**—Click the **Shutdown** button 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 Dell Wyse ThinOS INI Guide.

This process assumes that the security questions and answers have been pre-registered by the user inside 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. For more information, see Configuring the remote connections. After the security questions are answered, your new password will be set or your account will be unlocked.

Accessing system information

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

- **Classic desktop**—Click **System Information** from the desktop menu.
- **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 the Serial ports.
- **Copyright tab**—Displays the software copyright and patent notices.

  Acknowledgments button is added in the **Copyright** tab in System Information. This button is related to third party software.
- **Event Log tab**—Displays the thin 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 and USB connected to the thin client, and bluetooth initialization are also displayed.

- **Status tab**—Displays status information about TCP performance-related parameters, UDP performance-related parameters, CPU Busy, System Up Time, Wyse Management Suite status, Free Memory, Active sessions, and WDM status.
- **IPv6 tab**—Displays IPv6 information such as Link-local Address, IPv6 Address, and IPv6 Default Gateway.

  > ⓘ NOTE: **This tab is displayed when IPv6 is enabled in the General tab of the Network Setup dialog box, see Configuring the network settings.**

- **ENET tab**—Displays information about wired network connections.

  If Wyse 5070 thin client contains either RJ-45 module or SFP module, the Dual NIC feature is supported. In the **ENET** tab, click **Details** to view the network information of both Ethernet connections.
- **WLAN tab**—Displays information about wireless network connections.
- **About tab**—Displays information about the ThinOS operating system. The following attributes are listed:
  - Platform name
  - Operating system type
  - ThinOS build name
  - ThinOS build version
  - BIOS name
  - BIOS version
  - Citrix Broker or Receiver version—This represents ICA revisions between the ThinOS versions.
  - Dell vWorkspace version
  - VMware Horizon version—This represents the Horizon revisions between the ThinOS versions.
  - Microsoft Broker or RDP version
  - Teradici PCoIP version—This represents the PCoIP revisions between the ThinOS versions, and is applicable to the PCoIP devices only.
  - Imprivata version
  - Caradigm version
  - SECUREMATRIX version
  - HealthCast version

  > ⓘ NOTE:
  >
  > - **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 Microsoft RDP protocol version is 10.0, 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. 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. Using the ThinOS specified version, you can identify the changes between different revisions. For example, the Citrix Receiver version is 14.0.44705, the VMware Horizon version is 4.6.45422, and so on. The components are matched to the installed packages. If the packages are removed, the field remains empty in the **About** tab.

ENERGY STAR compliance

ENERGY STAR is a standard label on devices that meet energy-efficiency requirements by Environmental Protection Agency (EPA). Wyse 5070 thin clients with ThinOS are ENERGY STAR compliant. For more information about the ENERGY STAR program, see www.energystar.gov. For information about the supported ThinOS build version, see the *Dell Wyse ThinOS 8.5_113 Release Notes* at www.dell.com/support.

IPv6 certification

All networks are required to be Internet Protocol version 6 (IPv6) capable. Wyse 5070 thin clients with ThinOS are certified for IPv6 capability. For information about the supported ThinOS build version, see the *Dell Wyse ThinOS 8.5_113 Release Notes* at www.dell.com/support.

3

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:

- Zero desktop—Click **Global Connection Settings** in the list of connections.
- Classic desktop—Click **Global Connection Settings** in the Connect Manager.

To configure the Global Connection settings:

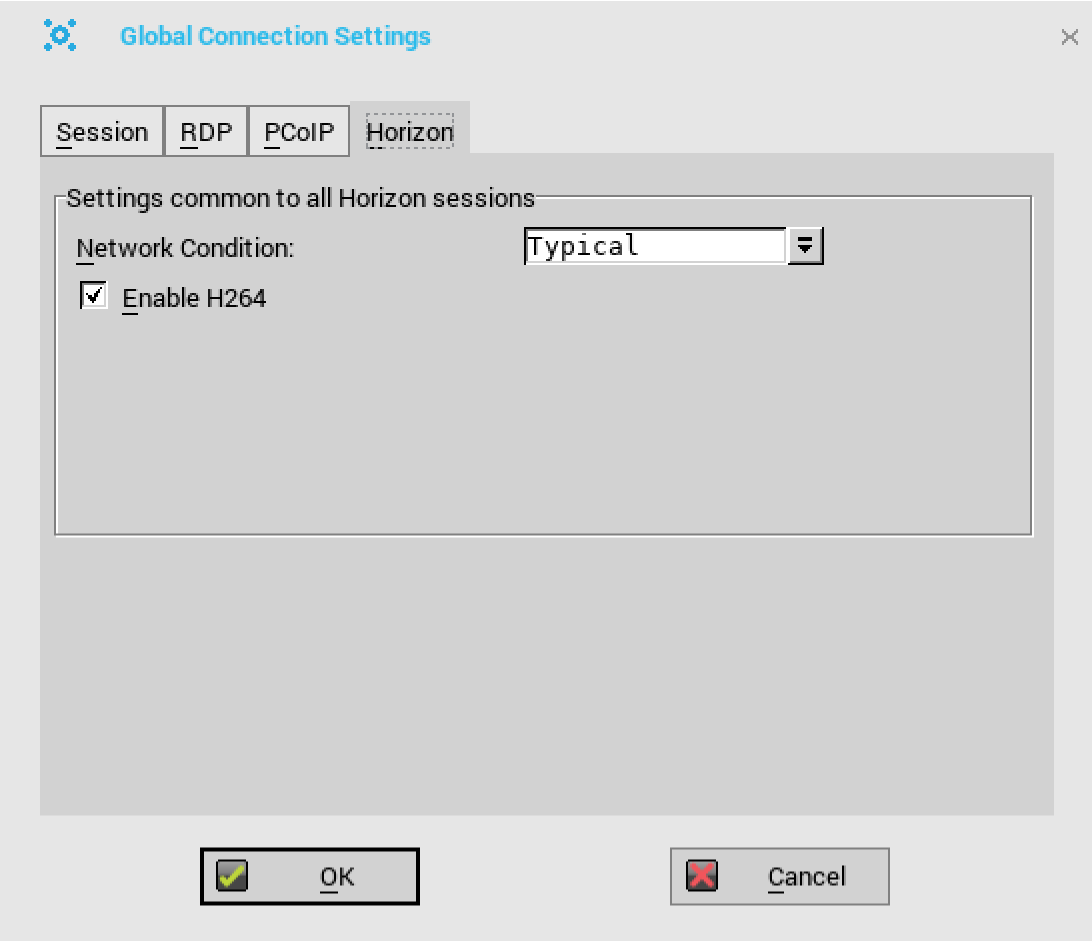
1. On the desktop taskbar, click **Connect Manager** > **Global Connection Settings**.

   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.

   > ⓘ NOTE:
   >
   > ICA sessions always have automatic connection to attached smart card readers. 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.

   > ⓘ 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 the **ICA** tab, and do the following:
   a. Select the check boxes you want for the options that are available to all ICA sessions.
   b. Select an audio quality optimized for your connection.
   c. Use the **Map to** option to map a disk. When a drive is entered, the disk is mapped under that particular drive.
4. Click the **RDP** tab and do the following:
   a. Enable or disable Network Level Authentication (NLA)—The NLA authentication method verifies users before they are allowed to connect with a full Remote Desktop connection.
   b. Enable or disable ForceSpan—This option allows you to span a session across all the connected monitors. All the monitors that are spanning is considered as one large monitor. You must connect to the session in a full screen mode.
   c. Enable or disable Terminal Service multimedia Redirection (TSMM).
   d. Enable or disable Record from Local (recording from local microphone).
   e. Enable or disable RemoteFX.
   f. Select the USB Redirection Type (TCX USB or RDP USB)—TCX USB is the default. To use RDP USB, you must use a RemoteFX session for Windows 7/Windows 2008 R2 session. However, RDP USB is not supported using a standard Windows 7/ Windows 2008 R2 session. For Windows 8 session and above, RDP USB is supported.
5. In PCoIP enabled clients, an extra tab named **PCoIP** is available. Select the **USB device redirection** type from the drop-down list. The available values are **PCoIP USB** and **TCX USB**.
6. Click the **Horizon** tab, and do the following:



Settings common to all Horizon sessions

Network Condition: Typical

☑ Enable H264

a Select the **Enable H264** check box. This option allows H.264 decoding in Horizon Client.

To validate the H.264 decoding, do the following:

- Configure the INI parameter `BlastDebugClientH264=yes`.
- Launch a VMware Blast session.
- On the upper-left corner of the screen, verify if the H264 basic watermark is displayed.

NOTE: A performance tracker is introduced by VMware for performance evaluation and data collection.

b From the **Network Condition** drop-down list, select whether to use a condition for your Blast connection.

NOTE: Blast Extreme protocol is part of BEAT (Blast Extreme Advanced Transport).

- Select **Excellent** to allow the Blast connection to use Transmission Control Protocol (TCP).
- Select **Typical** to allow the Blast connection to use Transmission Control Protocol (TCP). By default, this value is selected.
- Select **Poor** to allow the Blast connection to use User Datagram Protocol (UDP). UDP uses the available bandwidth to deliver the end-user experience.

  To enable UDP, you need to make a few changes to the VMware View Connection Server, the Agent host desktop, and the VMware Horizon Client. For information about the necessary configuration on server and agent desktop, see VMware Certificate Guide at code.vmware.com/group/euc/thin-client/certs/4.6.

4

Configuring 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 VPN manager.

ⓘ NOTE: **To configure the settings on Classic desktop, click System Setup from the desktop menu, and use the configuration tabs.**

To configure the settings on Zero desktop, click the **System Settings** icon on the zero toolbar, and then use the configuration tabs.

Configuring the network settings

To configure the network settings use the following options:

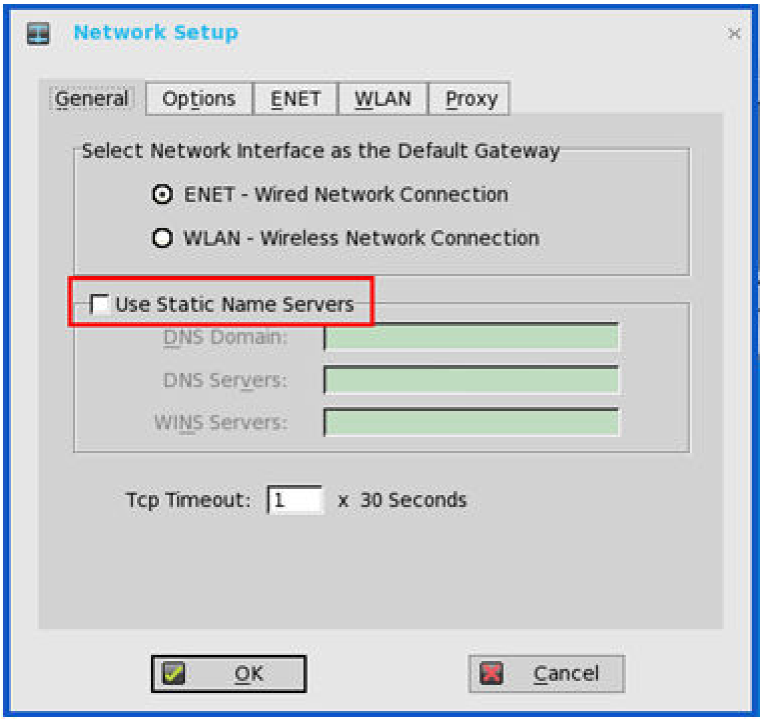
- Configuring the General settings.
- Configuring the Options settings.
- Configuring the ENET settings.
- Configuring the WLAN settings.
- Configuring the Proxy settings.

Configuring the general settings

ⓘ NOTE: **This section is applicable if Wyse 5070 thin client contains Wireless LAN (WLAN) module. If Wyse 5070 thin client contains any of the optional modules—Registered Jack 45 (RJ45) or Small form-factor pluggable (SFP) module, see Configuring the general settings.**

To configure the general network settings:

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


Network Setup

General | Options | ENET | WLAN | Proxy

Select Network Interface as the Default Gateway

● ENET - Wired Network Connection

○ WLAN - Wireless Network Connection

□ Use Static Name Servers

DNS Domain:

DNS Servers:

WINS Servers:

Tcp Timeout: 1 x 30 Seconds

The **Network Setup** dialog box is displayed.

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.

NOTE: The User Interface (UI) will not be changed automatically.

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

b **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.

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

2 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 up to 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.

3 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 thin 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.

c Enter the digit multiplier of 30 seconds in the **TCP Timeout** box to set the time-out value of a TCP connection. The value must be **1** or **2** which means the connection time-out 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 time-out 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.

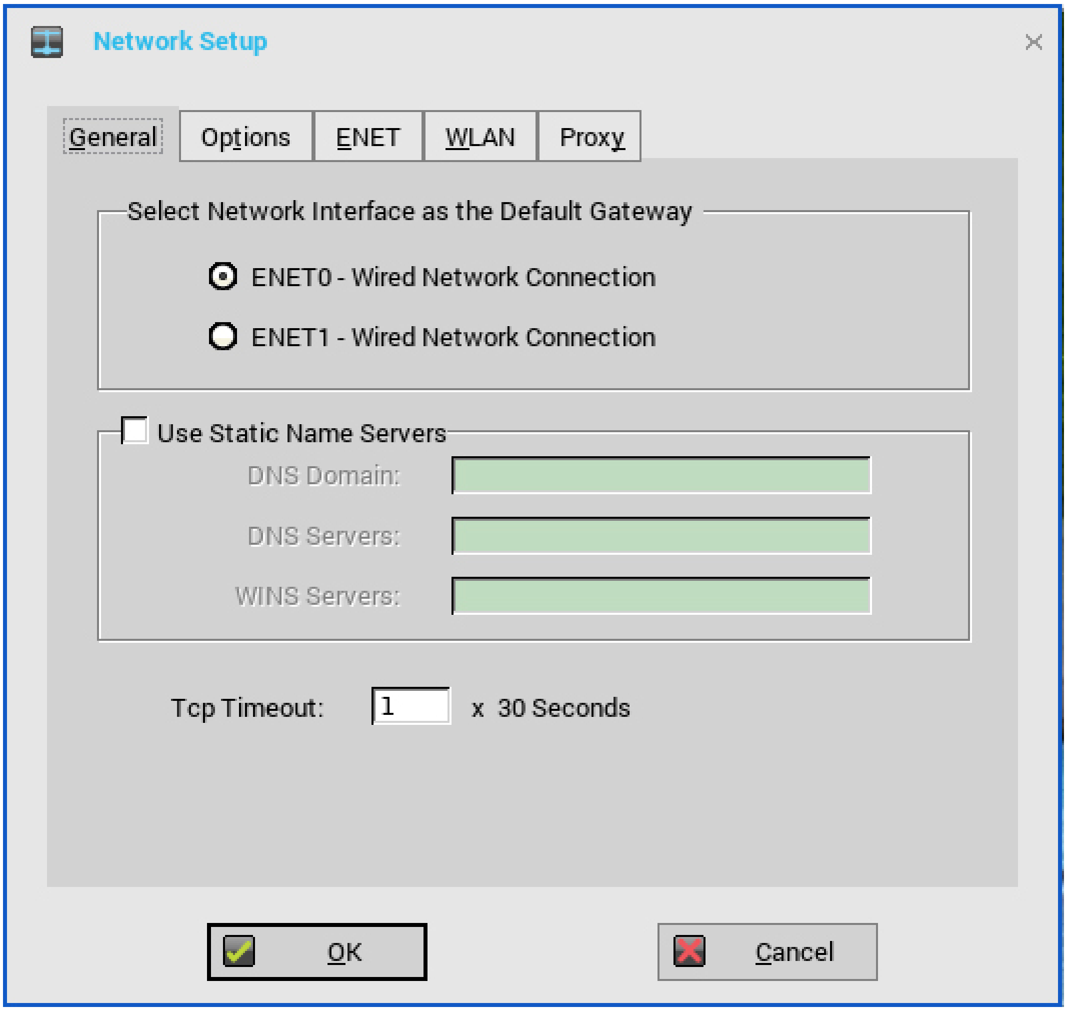
Configuring the general settings

ⓘ NOTE: **This section is applicable if the Wyse 5070 thin client contains any of the optional modules—Registered Jack 45 (RJ45) or Small form-factor pluggable (SFP) module. If the Wyse 5070 thin client contains Wireless LAN (WLAN) module, see Configuring the general settings.**

To configure the general network settings:

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

The **Network Setup** dialog box is displayed.



Network Setup

Select Network Interface as the Default Gateway

● ENET0 - Wired Network Connection

○ ENET1 - Wired Network Connection

□ Use Static Name Servers

DNS Domain:

DNS Servers:

WINS Servers:

Tcp Timeout: 1 x 30 Seconds

Figure 3. General settings

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

a To set the default gateway, select the type of network interface from the following options:

- **ENET0**— Enables you to set up the first Ethernet Wired Network connection.
- **ENET1**—Enables you to set up the second Ethernet Wired Network connection.

ⓘ NOTE: **You can connect your thin client to two wired network connections at the same time. The default gateway is determined by the UI settings. However, UI will not be changed automatically.**

b **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 0 and Ethernet 1, if network is not working.

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

2 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 up to 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.**

3 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 thin 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.

c Enter the digit multiplier of 30 seconds in the **TCP Timeout** box to set the time-out value of a TCP connection. The value must be **1** or **2** which means the connection time-out 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 time-out 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.

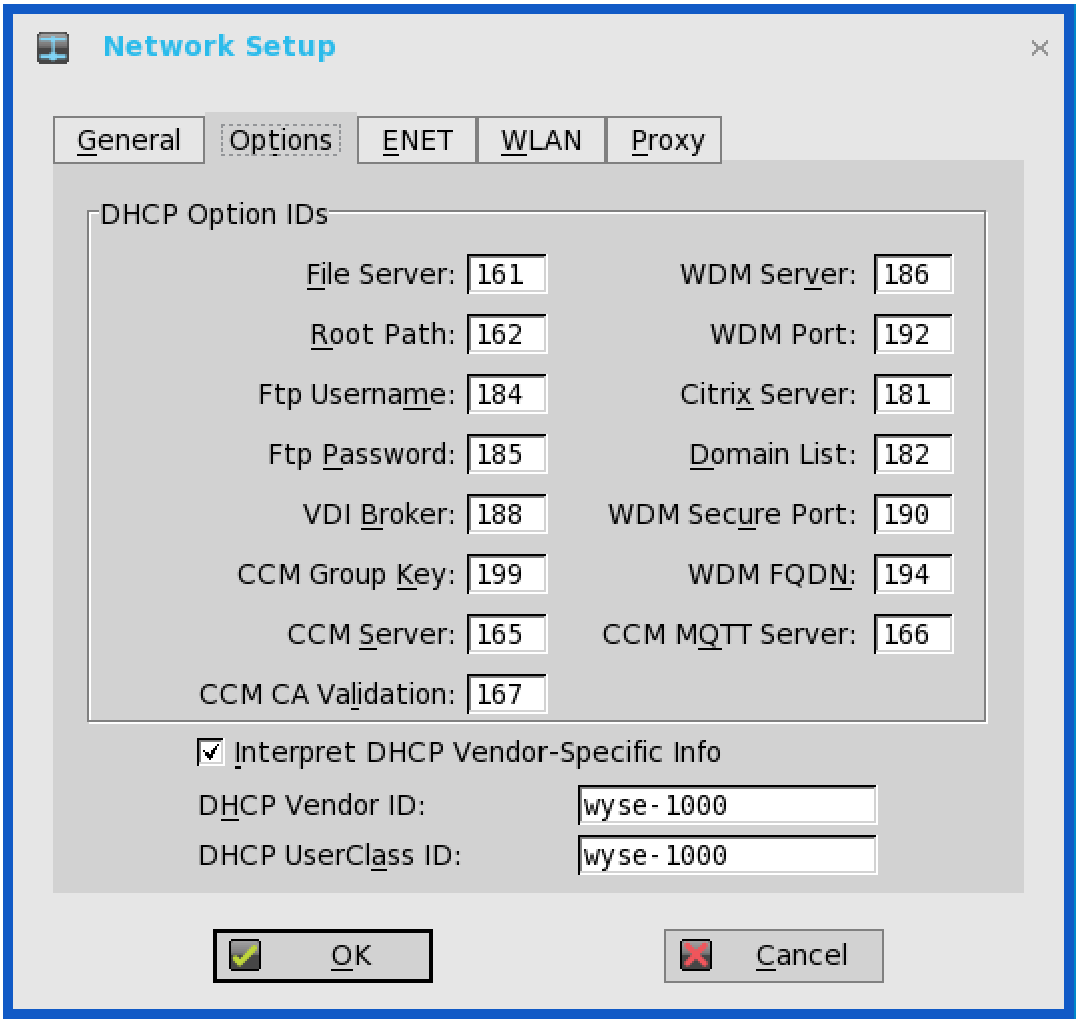
Configuring the DHCP options settings

To configure the options settings:

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

The **Network Setup** dialog box is displayed.

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



DHCP Option IDs

File Server:	161	WDM Server:	186
Root Path:	162	WDM Port:	192
Ftp Username:	184	Citrix Server:	181
Ftp Password:	185	Domain List:	182
VDI Broker:	188	WDM Secure Port:	190
CCM Group Key:	199	WDM FQDN:	194
CCM Server:	165	CCM MQTT Server:	166
CCM CA Validation:	167		

☑ Interpret DHCP Vendor-Specific Info

DHCP Vendor ID: wyse-1000

DHCP UserClass ID: wyse-1000

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 about DHCP options, see 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.

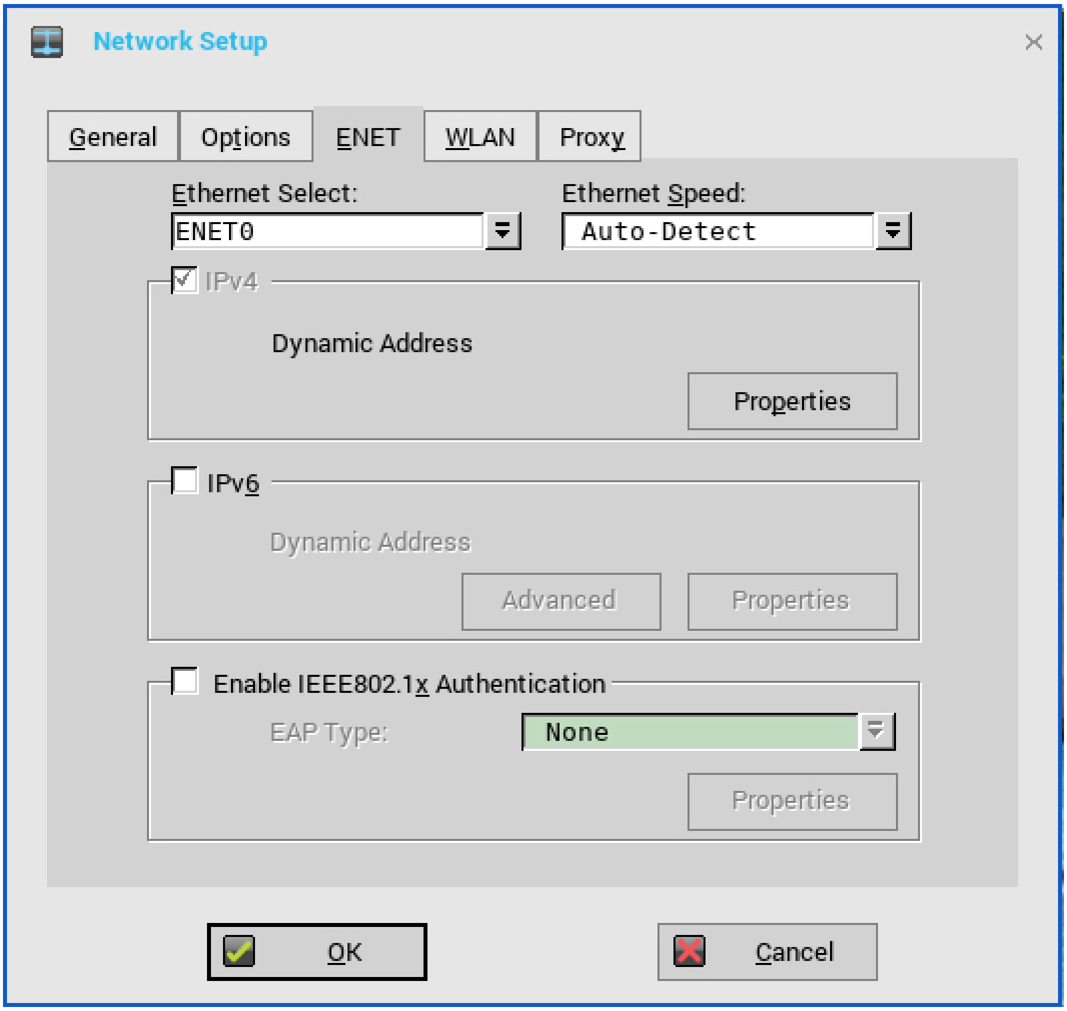
Configuring the ENET settings

To configure the ENET settings:

1 From the desktop 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:



Ethernet Select: ENET0

Ethernet Speed: Auto-Detect

☑ IPv4

Dynamic Address

□ IPv6

Dynamic Address

□ Enable IEEE802.1x Authentication

EAP Type: None

Figure 4. ENET tab

a. **Ethernet Select**—Allows you to select the wired network connection. For Wyse 5070 thin client without SFP or RJ-45 module, the **ENET0** option is selected by default. For Wyse 5070 thin client with SFP or RJ-45 module, select either **ENET0** or **ENET1** based on your network preference.

b. **Ethernet Speed**—The default value is **Auto-Detect**. If your network equipment does not support the automatic negotiation, select any of the available options—**10 MB Half-Duplex**, **10 MB Full-Duplex**, **100 MB Half-Duplex**, **100 MB Full-Duplex**, or **1 GB Full-Duplex**.

   The **10 MB Full-Duplex** option can be selected locally. However, this mode can be negotiated through **Auto-Detect**.

c. The **IPv4** check box is selected by default. Click **Properties** to configure the following options:

   - **Dynamically allocated over DHCP/BOOTP**—Select this option to enable your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server by using DHCP options to provide information. Any value that is entered locally in the **Options** tab is replaced by the DHCP value. If the DHCP server fails to provide replacement values, the locally entered value is used.
   - **Statically specified IP Address**—Select this option to manually enter the IP address, subnet mask, and default gateway.
     - **IP Address**—Enter 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 a different subnet, messages that are sent to that address must be sent through the default gateway. This does not depend on the value that is 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.

d 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 autoconfiguration (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**—Select this option to enable your thin client to consider IPv6 DHCP before you log in. If you do not select this option, and DHCP is enabled, the system still waits for IPv4 DHCP.
- **Dynamically allocated over DHCP/BOOTP**—Select this option to enable 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 that is entered locally in the **Options** tab is replaced by the DHCP value. If the DHCP server fails to provide replacement values, the locally entered value is used.
- **Statically specified IP Address**—Select this option to manually enter the IP address, subnet mask, and default gateway.
  - **IP** Address—Enter a valid network address in the server environment. The network administrator must provide this information.
  - **Subnet Prefix Len**—Enter the prefix length of the IPv6 subnet.
  - **Default gateway**—Use of gateways is optional. For more information, see various IPv4-supported options 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 provides this value, it replaces any locally configured value. If the DHCP server does not provide this value, the locally configured value is used.

> ⓘ NOTE: **If you enable IPv6 for both ENET0 and ENET1, IPv6 routes through the Ethernet connection that fetches the IPv6 address first.**

e Select the **Enable the IEEE802.1x authentication** check box, and from the **EAP type** drop-down list, select **TLS**, **LEAP**, **PEAP** or **FAST**.

- **TLS**—Select this option, and click **Properties** to 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. The server certificate text field supports a maximum of approximately 255 characters, and supports multiple server names.**

  - Select the **Connect to these servers** check box, and enter the IP address of server.
  - Click **Browse** to find and select the client certificate file and the private key file you want.

    > ⓘ NOTE: **Ensure that you select the PFX file only.**

  - From the **Authenticate** drop-down list, select either user authentication or machine authentication that is based on your choice.

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

    - *.dell.com
    - *dell.com
    - *.com

ⓘ **NOTE: Using only the FQDN, that is, company.dell.com does not work. Use one of the options, for example servername.dell.com (*.dell.com is the most common option as multiple authentication servers may exist).**

- **LEAP**—Select this option, and click **Properties** to 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**—Select this option, and click **Properties** to 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**—Select this option, and click **Properties** to 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.

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

  ⓘ **NOTE: 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 validated forcibly. When EAP-MSCCHAPV2 is selected for PEAP or FAST authentication, an option to hide the domain is available. Username and Password boxes are available for use, but the **domain** text box is disabled.

  When EAP-MSCHAPV2 is selected for PEAP or FAST authentication, a check box to enable the Single Sign-On feature is available.

  From ThinOS 8.3, 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. The first-time connection always fails, and the subsequent connections succeed. Only automatic PAC provisioning is supported. The user/machine PAC provisioning that is generated with CISCO EAP-FAST utility is not supported.

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

   ⓘ **IMPORTANT: From ThinOS version 8.5, client reboot is not required to change the network settings. All the changes take effect immediately.**

   For example, ThinOS connects to the new wireless SSID immediately without reboot.

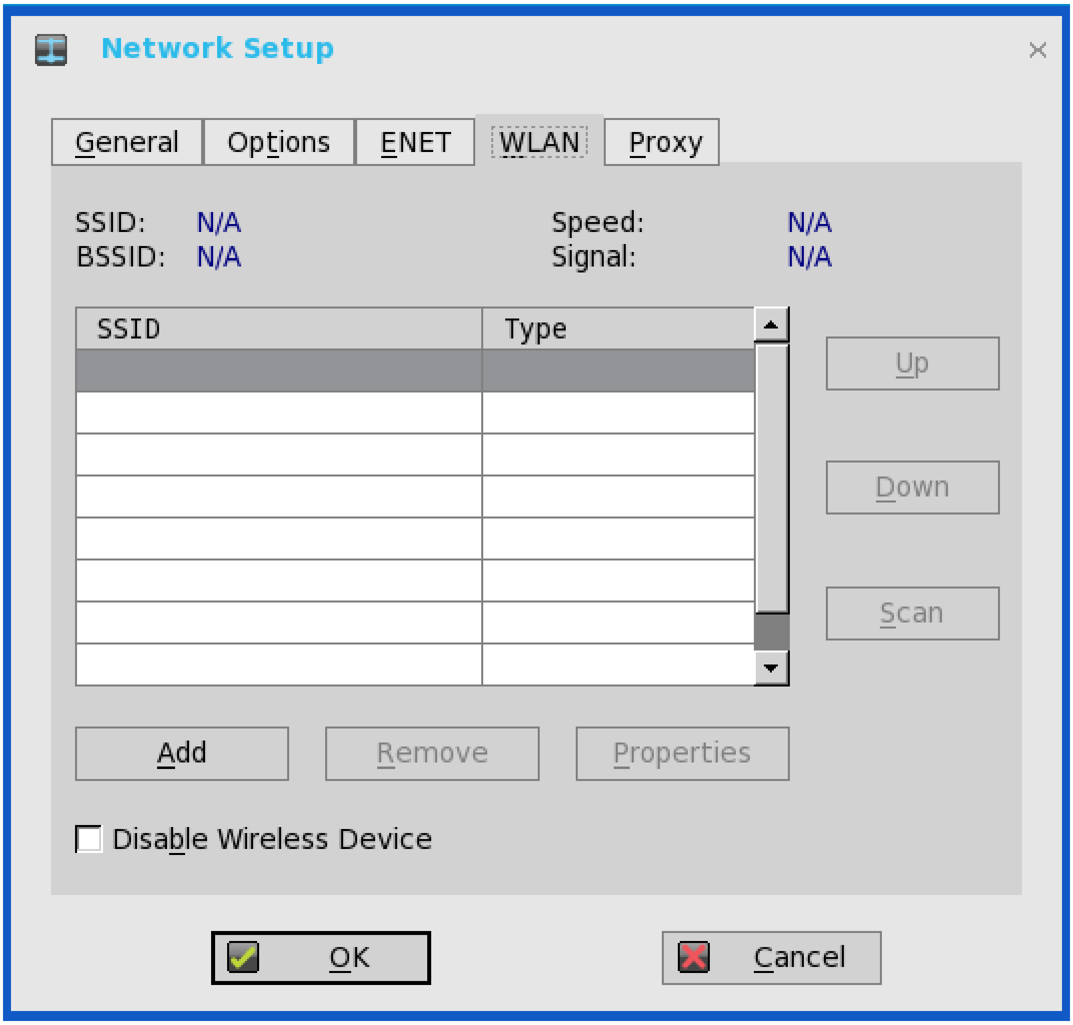
Configuring the WLAN settings

ⓘ **NOTE: On Wyse 5070 thin client with an optional SFP module or RJ45 module, you cannot configure the wireless settings.**

To configure the WLAN settings:

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

   The **Network Setup** dialog box is displayed.
2. Click the **WLAN** tab, and do the following:



SSID: N/A

BSSID: N/A

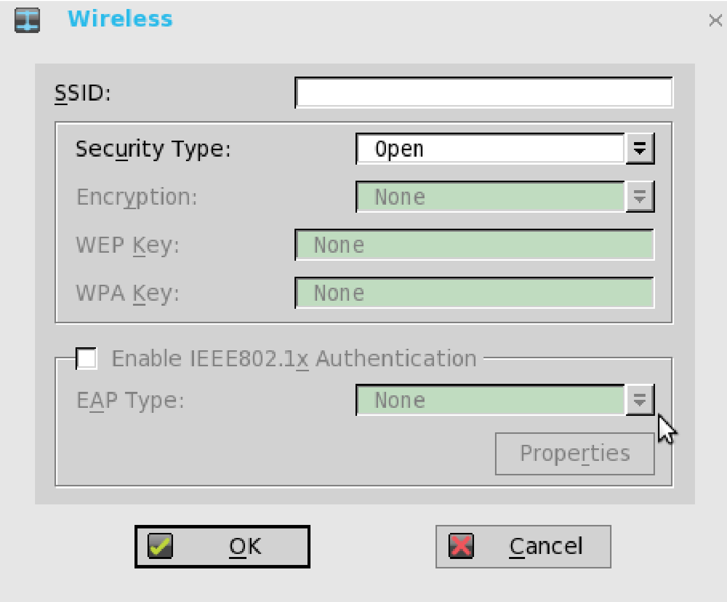
Speed: N/A

Signal: N/A

□ Disable Wireless Device

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.



SSID:

Security Type: Open

Encryption: None

WEP Key: None

WPA Key: None

□ Enable IEEE802.1x Authentication

EAP Type: None

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

b **Remove**—Use this option if you want to remove a SSID connection by selecting the SSID connection from the list.

c **Properties**—Use this option to view and configure the authentication properties of a SSID connection that is displayed in the list.

d 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.

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

> ⓘ IMPORTANT: **Device reboot is not required to change the network settings. All the changes take effect immediately.**
>
> For example, ThinOS connects to the new wireless SSID immediately without reboot. However for ARM platforms—Wyse 3010 thin client, and Wyse 3020 thin client—the requires reboot.

> ⓘ NOTE:
>
> - Supported chipset: Intel Dual Band Wireless AC 9560
> - Supported standards: 802.11 a/b/g/n/ac

Configuring the proxy settings

The network **Proxy** tab supports Wyse Management Suite, HDX Flash Redirection, and RealTime Multimedia Engine (RTME).

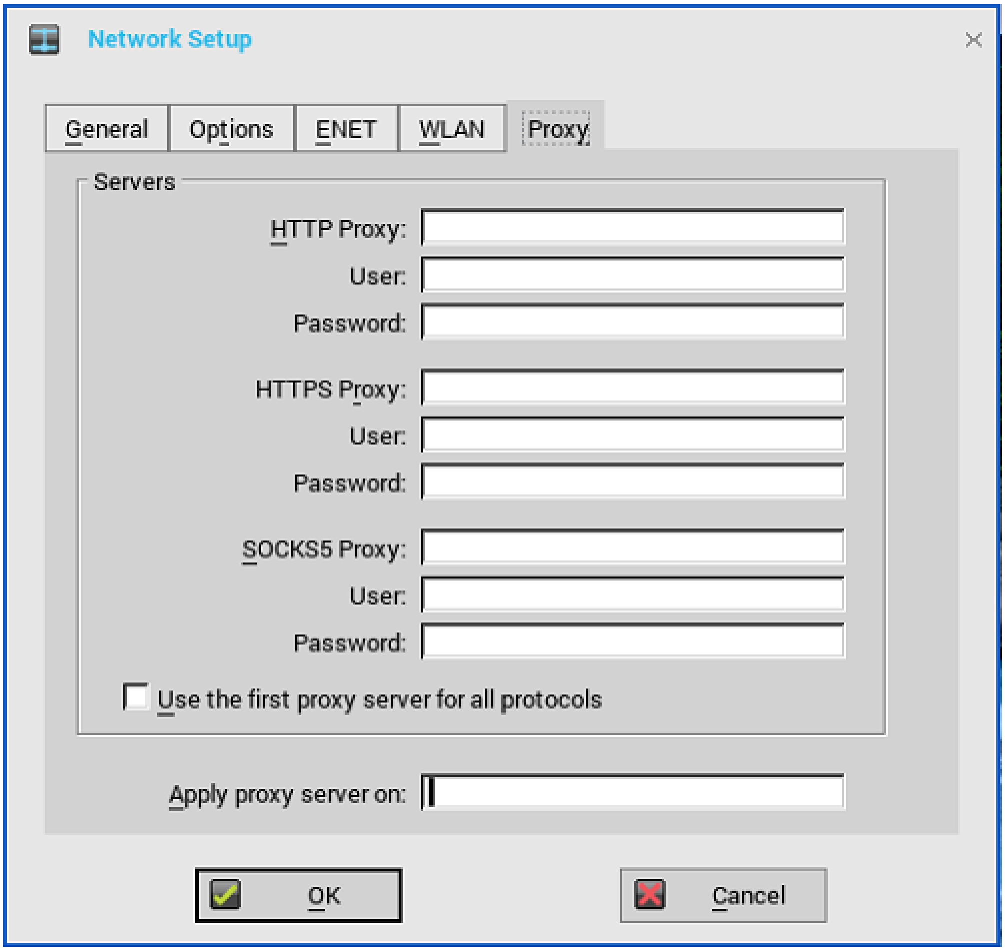
Supported protocols—HDX FR, WMS and RTME

- For **HDX FR**: HTTP and HTTPS protocols are supported.
  - If both HTTP and HTTPS are configured, the HDX FR works with HTTPS proxy.
  - User credential pass through is possible with $UN/$PW.
- For **Wyse Management Suite**: 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 do the following:



a Enter the **HTTP proxy** port number or **HTTPS proxy** port number, **User** name 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 the WMS/MQTT server. However, the HTTP proxy cannot redirect TCP packages to the MQTT server which requires a SOCKS5 proxy server. If there is only HTTP server available, then the real-time command that requires MQTT does not work.

HTTP/HTTPS proxy default port is 808, and **SOCKS5 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 the **HTTP Proxy** fields. Both HTTP and HTTPS proxy use the same host and port, and SOCKS5 proxy agent uses HTTP host with default Socks5 port (1080).

If **SOCKS5 proxy** is configured, then WMS proxy uses the SOCKS5 only. If SOCKS5 is not configured, then WMS proxy searches for alternative protocols, for example, HTTP in the configuration.

c Specify the supported applications as Wyse Management Suite, FR and RTME separated by a semicolon in the **Apply proxy server on** field.

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

User scenario

1 Configure correct proxy server host and port.

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

On system restart, the client checks in to the Wyse Management Suite server through SOCKS5 proxy server. MQTT connection is established through SOCKS5 proxy server. Real-time commands work fine through SOCKS5 proxy server.

3 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 thin client remote connections including ICA, RDP, Citrix XenDesktop, Microsoft, VMware View, Dell vWorkspace, and other broker server connections. This dialog box also enables you to configure visual options, and general connection settings.

- Configuring the Broker setup
- Configuring the Visual settings
- Using the General options
- Configuring the Authentication settings

ⓘ **NOTE: In the Classic Desktop option, the Remote Connections dialog box allows you to create the default RDP connections for use. If you want to create more than the default connections, use the Connect Manager, For more information see Using the Connect Manager.**

Configuring the broker setup

To configure the broker setup:

1 From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

2 In the **Broker Setup** tab, from the drop-down list, select the **Broker type**.

a Select **None**, and click either of the following connection protocols:

- **ICA**—For more information, see Configuring ICA connections.
- **RDP**—For more information, see Configuring RDP connections.

b Select any one of the available broker connections, and configure the broker setup to connect to the respective virtual desktop environments. For instructions about configuring a particular broker setup, see Configuring the connection brokers.

The available broker connections that you can configure on ThinOS are:

- **Citrix Xen**
- **VMware View**
- **Microsoft**
- **Dell vWorkspace**
- **Amazon vWorkspace**—This is applicable only to the PCoIP clients.

c Select **Other**, and use the following guidelines:

- **Broker Server**—Enter the IP address of the Broker server.
- **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be listed. Each desktop name is separated by a semi-colon, and is case-sensitive.

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

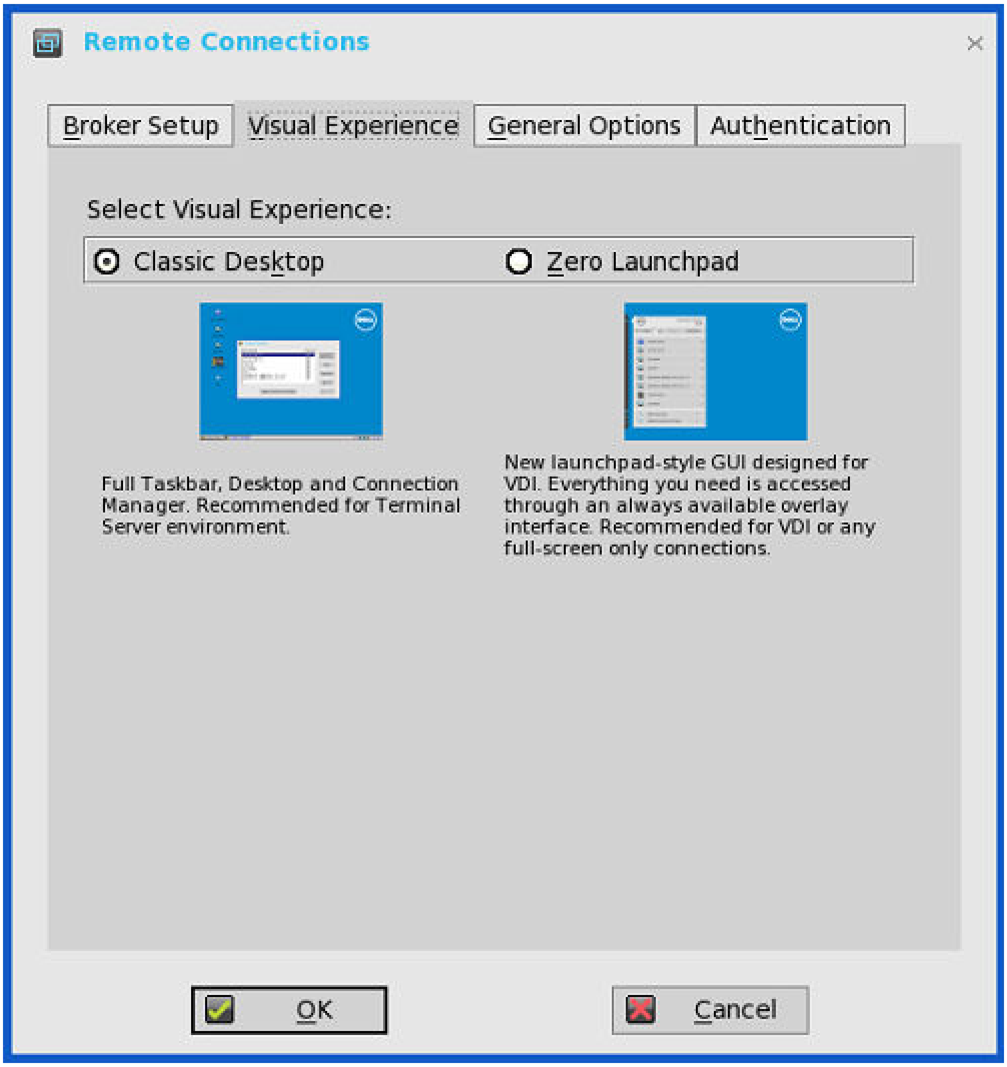
Configuring the visual settings

To configure the visual settings:

1 From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** tab is displayed.

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



Select Visual Experience:

● Classic Desktop ○ Zero Launchpad

Full Taskbar, Desktop and Connection Manager. Recommended for Terminal Server environment.

New launchpad-style GUI designed for VDI. Everything you need is accessed through an always available overlay interface. Recommended for VDI or any full-screen only connections.

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 **Classic Desktop** — Displays the full taskbar, desktop and Connect Manager familiar to ThinOS users. This option is recommended for terminal server environments and for backward compatibility with ThinOS 6.x versions.

b **Zero Launchpad** — Displays the new launch pad style GUI designed for VDI use. Functionality is accessed through an always available interface. This option is recommended for VDI and any full-screen only connections. Toolbar, hotkey and connection icon options are also available for configuration.

If you select the **Zero Launchpad**, then use the following guidelines:

- 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. You must select the time duration—0. 0.5 or 1 second—after which the Zero toolbar is activated.
  - Select the button if you want to enable Zero Toolbar activation in left pane only after clicking.
- Select the check box to disable hotkey to show toolbar.
- Select the check box to always disable toolbar when you have one session available.
- Select the check box to disable the Home icon.

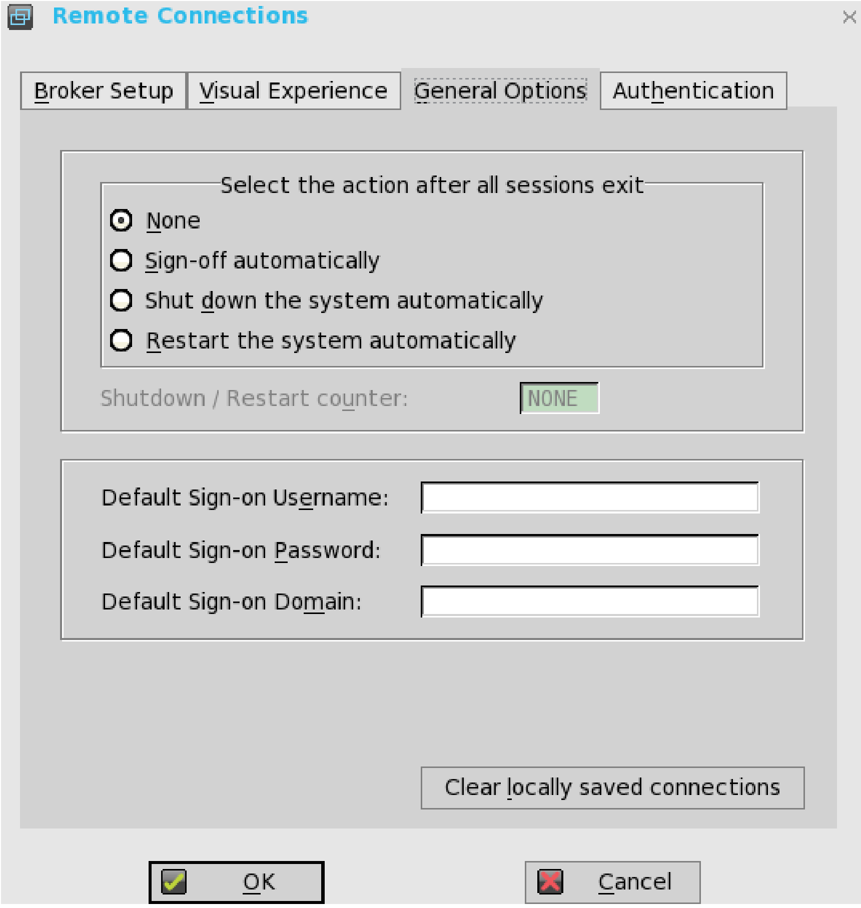
3 Click **OK** to save the settings.

Configuring the general options

To configure the general options:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.



Select the action after all sessions exit

● None
○ Sign-off automatically
○ Shut down the system automatically
○ Restart the system automatically

Shutdown / Restart counter: NONE

Default Sign-on Username:

Default Sign-on Password:

Default Sign-on Domain:

2. Click the **General Options** tab, 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 thin 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.

   e. Click **Clear locally saved connections** to clear locally saved connections.

      ⓘ 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:

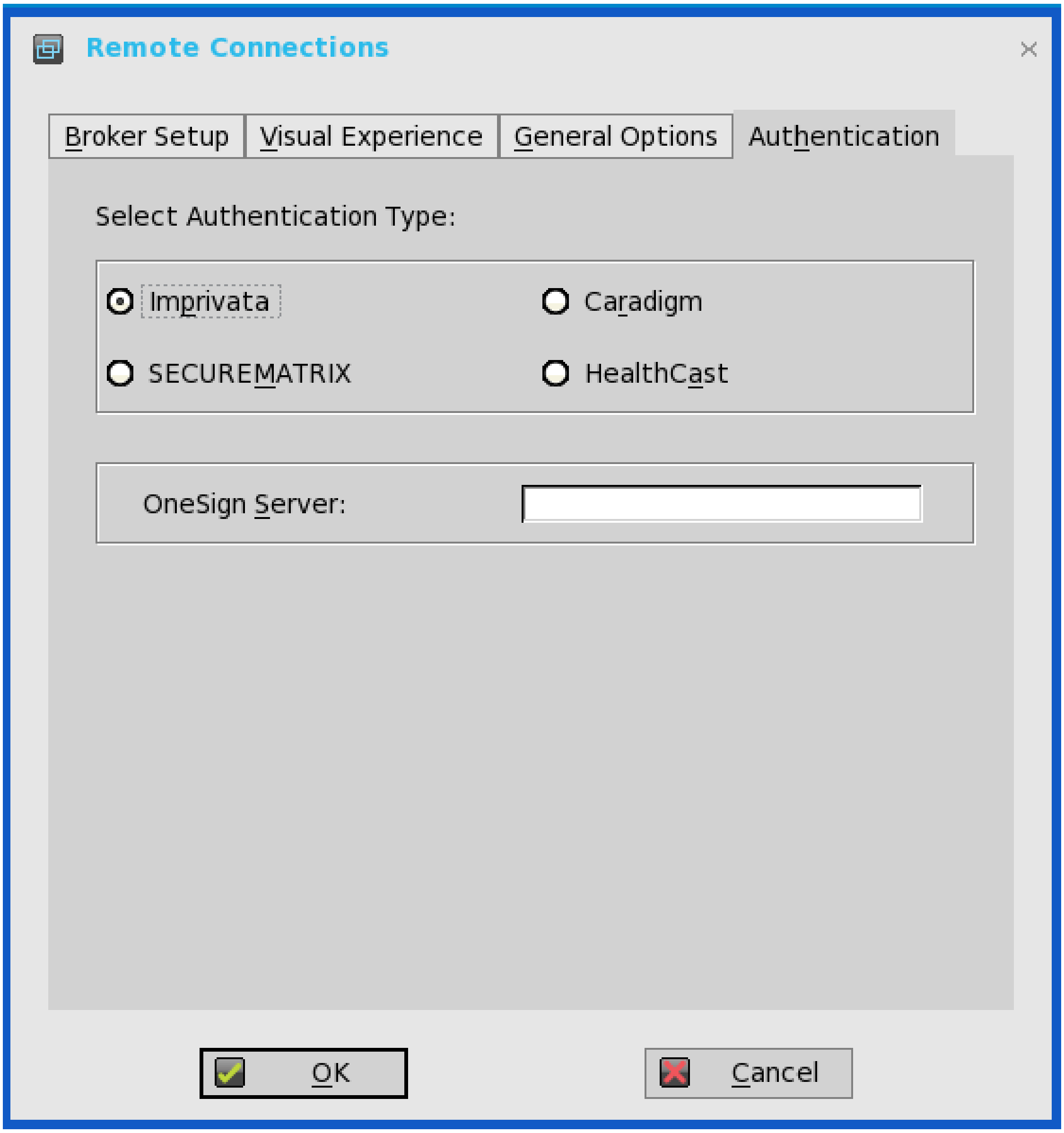
1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.

2 Click the **Authentication** tab, and select the authentication type.

The following authentication options are displayed:

- Imprivata— Configuring Imprivata OneSign server.
- Caradigm—Configuring Caradigm server.
- SECUREMATRIX— Configuring SECUREMATRIX.
- HealthCast—Introduction to HealthCast.



Select Authentication Type:

● Imprivata ○ Caradigm

○ SECUREMATRIX ○ HealthCast

OneSign Server:

3 After configuring your preferred authentication, click **OK** to save the settings.

Configuring Imprivata OneSign server

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 the details of the OneSign Server (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 *Dell Wyse ThinOS INI Reference Guide*.

The following OneSign features or actions are supported:

- Client and Broker authentication
  - Citrix XenApp
  - Citrix XenDesktop
  - VMware View
- 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

ThinOS supports latest Imprivata WebAPI version 5. It includes OneSign Objects (WebAPI v4) and Fingerprint Authentication (WebAPI v5).

Configuring objects on Imprivata Server

Imprivata WebAPI is updated from version 4 to version 5. From earlier version, supports configuration objects are supported that enables you to control different aspects of client behavior. The Imprivata WebAPI feature is available on OneSign server 4.9 and later versions. The Configuration objects 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.

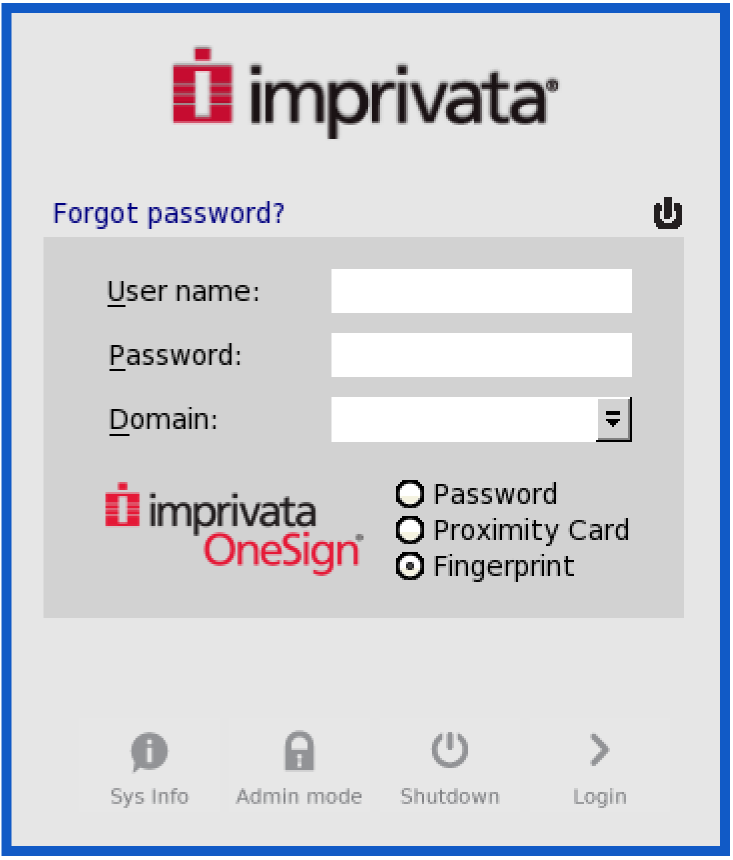
b Select the check box to allow users to shut down and restart workstation from lock screen.

ⓘ | **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 login and locked windows.



○ Password
○ Proximity Card
● Fingerprint

- 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 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 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 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. Therefore a new INI is added—`SuspendAction=0/1`; 0 means lock, 1 means signoff.

3 **Configuring the SSPR Configuration Object**

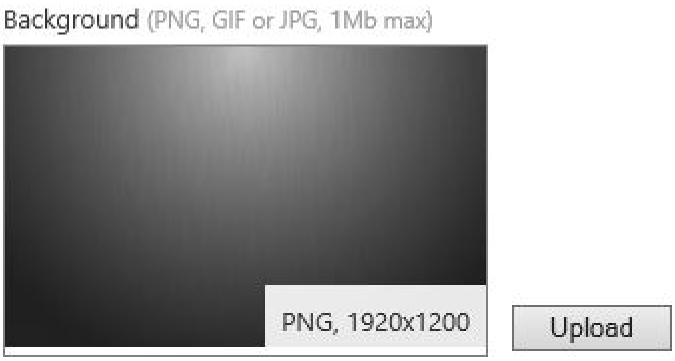
The SSPR configuration object controls the Self-Service Password Reset behavior for a user. The enabled attribute specifies whether the user is allowed to reset their password as part of emergency access. The mandatory attribute specifies whether the user must reset their password as part of emergency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

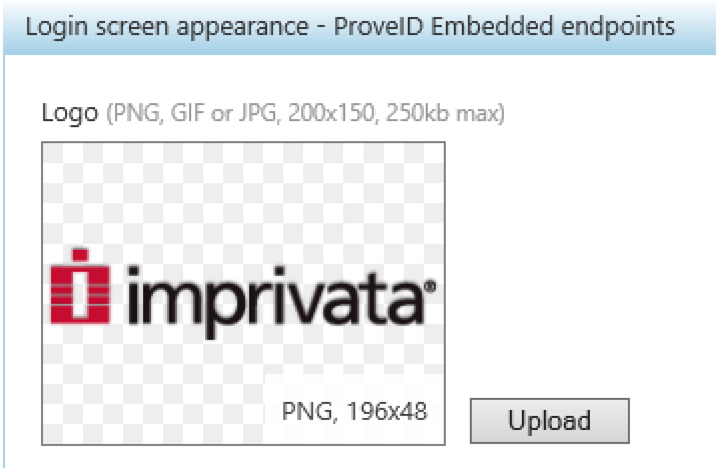
5 **Configuring the Custom background configuration object**

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



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

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

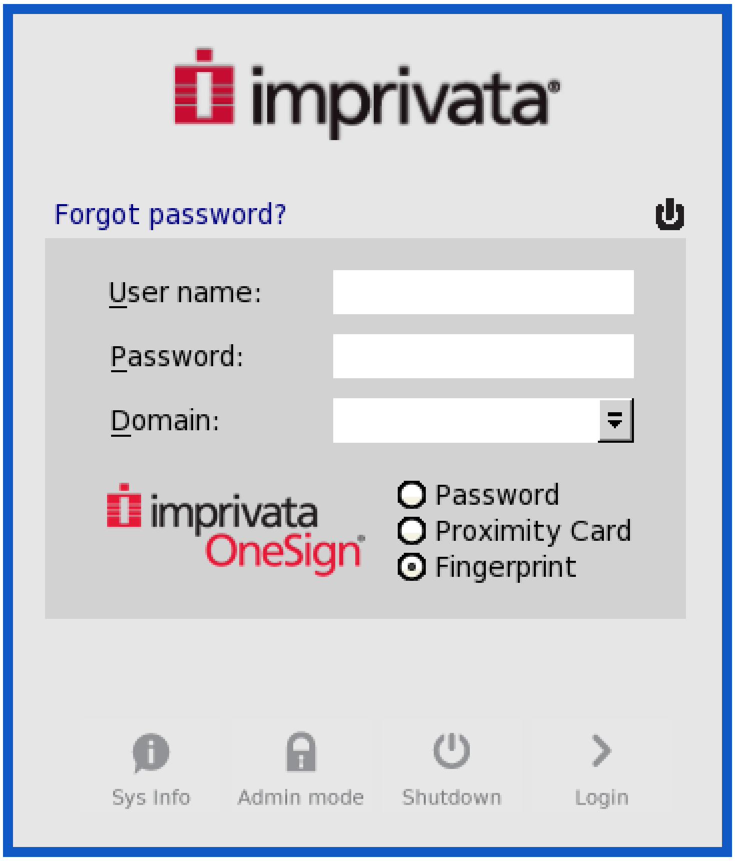

Login screen appearance - ProveID Embedded endpoints
Logo (PNG, GIF or JPG, 200x150, 250kb max)
imprivata
PNG, 196x48
Upload

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

7 **Configuring the SSPR Customization configuration object**

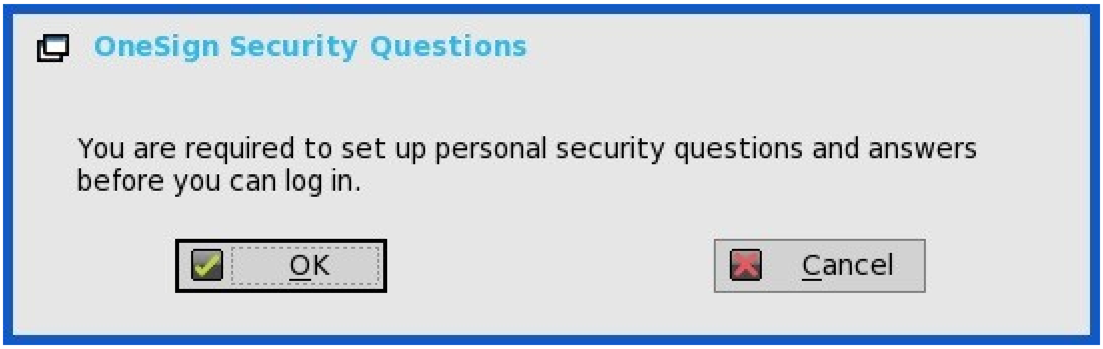
- The text displayed in sign-on UI and lock window can be customized.
- The largest size supported by ThinOS is 17 characters.

ThinOS UI:



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

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


OneSign Security Questions

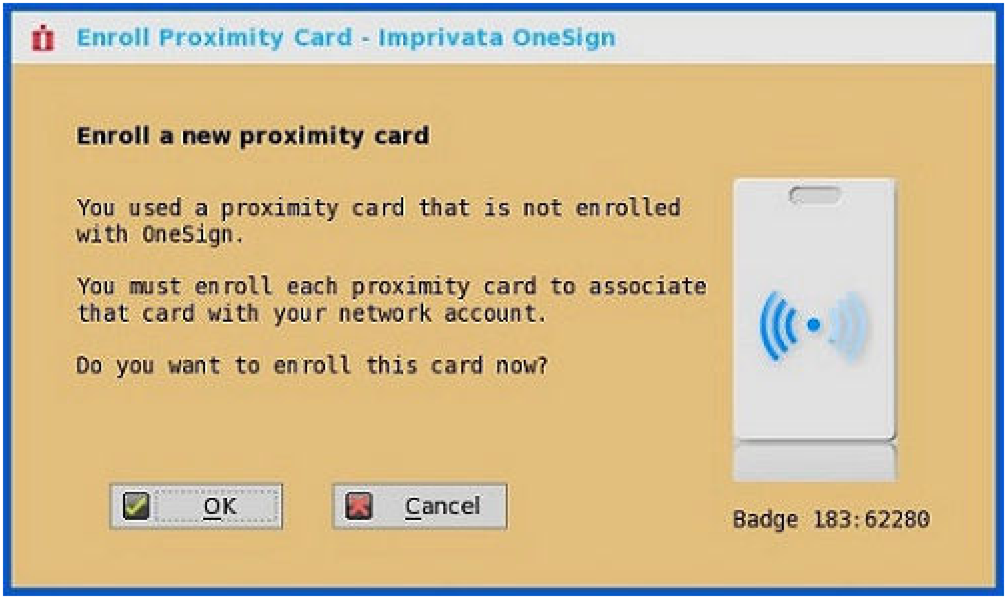
You are required to set up personal security questions and answers before you can log in.

INI configuration for Imprivata OneSign Server

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

Proximity card enrollment

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



Enroll Proximity Card - Imprivata OneSign

Enroll a new proximity card

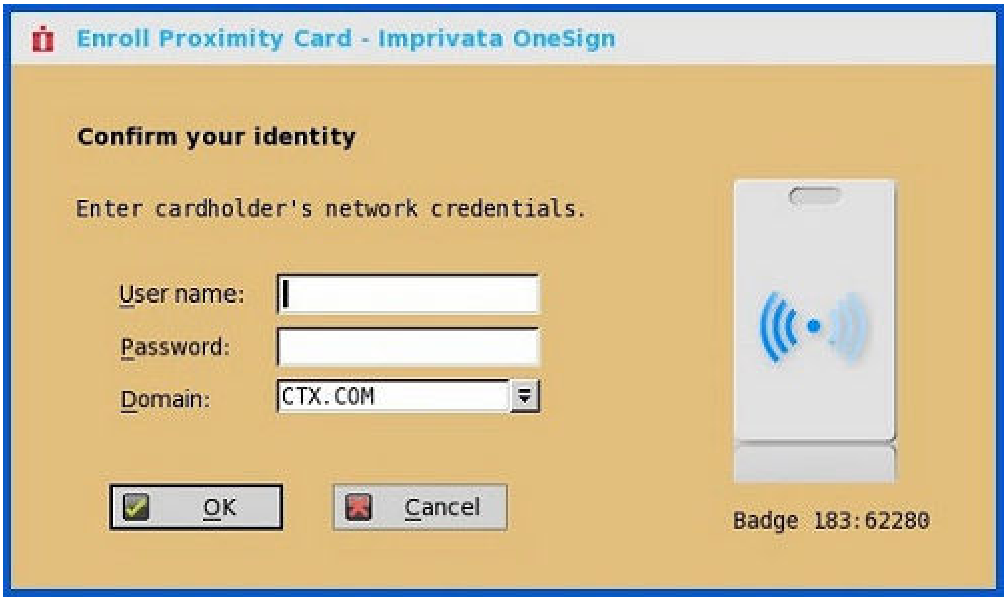
You used a proximity card that is not enrolled with OneSign.

You must enroll each proximity card to associate that card with your network account.

Do you want to enroll this card now?

Badge 183:62280

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



Enroll Proximity Card - Imprivata OneSign

Confirm your identity

Enter cardholder's network credentials.

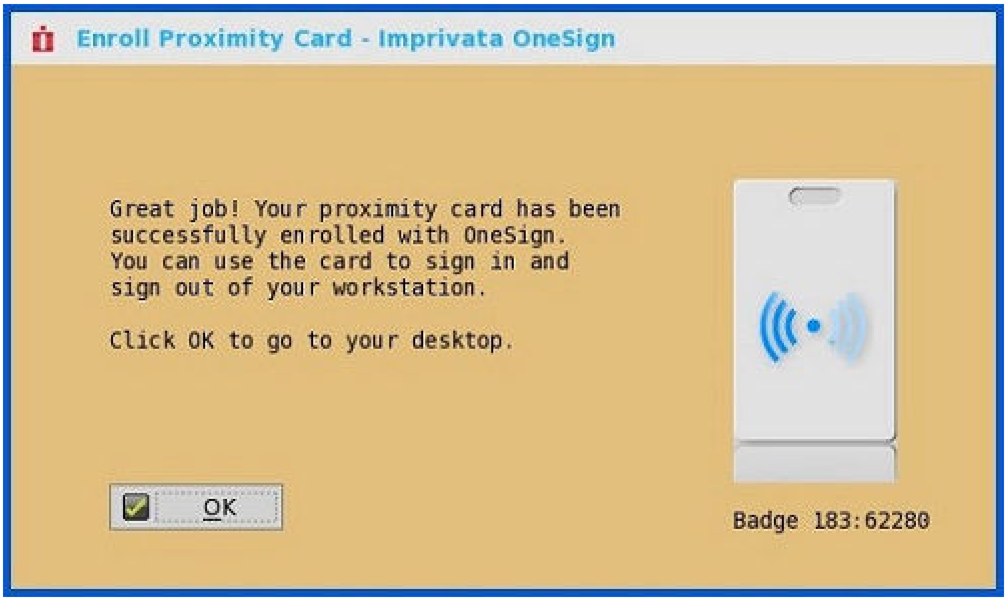
User name:

Password:

Domain: CTX.COM

Badge 183:62280

Proximity card is enrolled successfully.



Great job! Your proximity card has been successfully enrolled with OneSign. You can use the card to sign in and sign out of your workstation.

Click OK to go to your desktop.

Badge 183:62280

Imprivata Bio-metric Single Sign-On

Fingerprint identification 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.

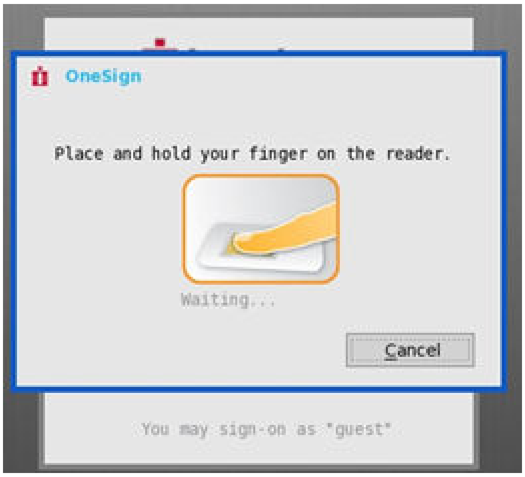
ⓘ **NOTE:**

- Supported protocols are RDP, ICA, and PCoIP.
- Required Fingerprint reader devices are:
  - ET710 (PID 147e VID 2016)
  - ET700 (PID 147e VID 3001)

Supported scenarios

1 Signing in or unlocking the ThinOS devices using Fingerprint Authentication.

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

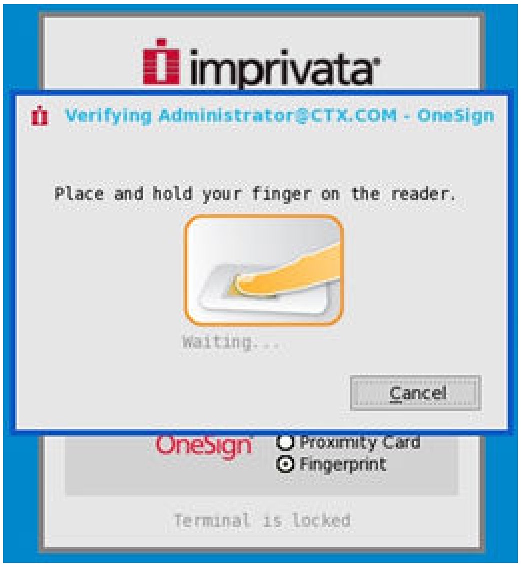


Place and hold your finger on the reader.

Waiting...

You may sign-on as "guest"

- Fingerprint authentication works on the ThinOS unlock window.



Verifying Administrator@CTX.COM - OneSign

Place and hold your finger on the reader.

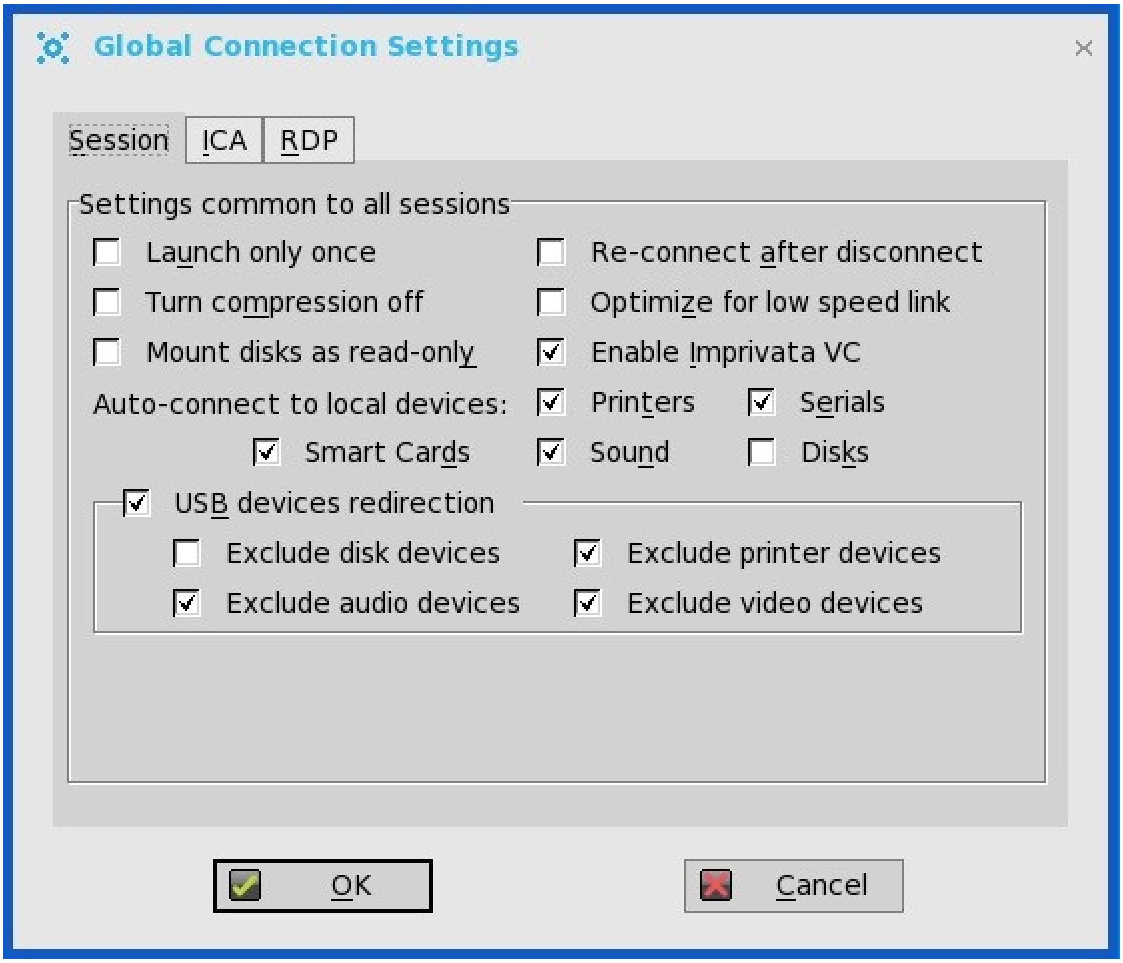
Waiting...

○ Proximity Card
● Fingerprint

Terminal is locked

2 Unlocking the Virtual Desktop using Fingerprint Authentication.

- Enable the Imprivata Virtual Channel from ThinOS Global Connection Settings.



Global Connection Settings

Settings common to all sessions

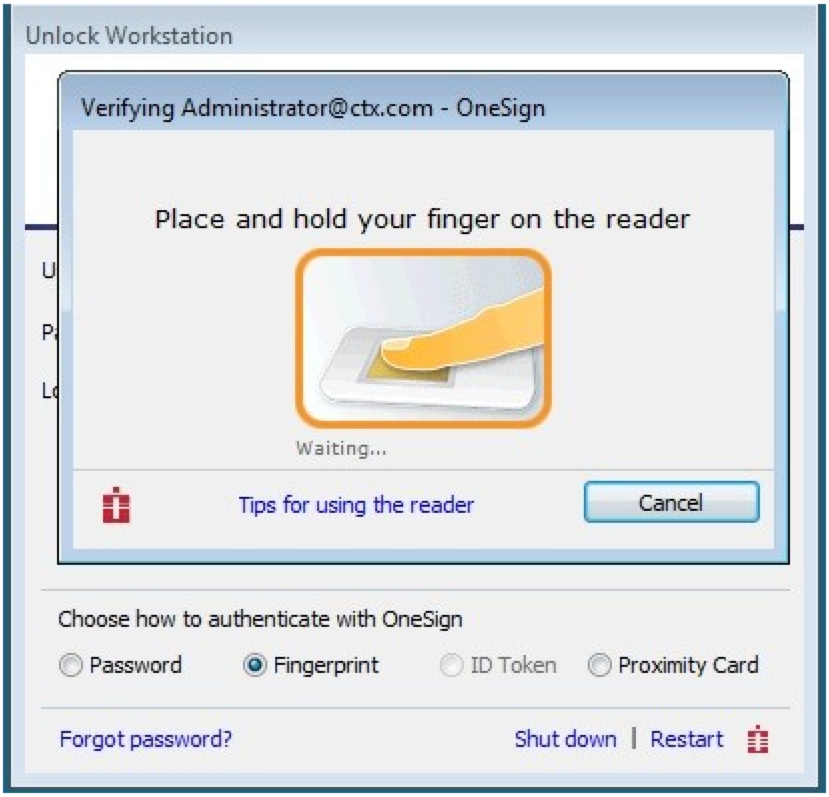
- □ Launch only once
- □ Re-connect after disconnect
- □ Turn compression off
- □ Optimize for low speed link
- □ Mount disks as read-only
- ☑ Enable Imprivata VC

Auto-connect to local devices: ☑ Printers ☑ Serials ☑ Smart Cards ☑ Sound □ Disks

☑ USB devices redirection

- □ Exclude disk devices
- ☑ Exclude printer devices
- ☑ Exclude audio devices
- ☑ Exclude video devices

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


Unlock Workstation

Verifying Administrator@ctx.com - OneSign

Place and hold your finger on the reader

Waiting...

Choose how to authenticate with OneSign

○ Password ● Fingerprint ○ ID Token ○ Proximity Card

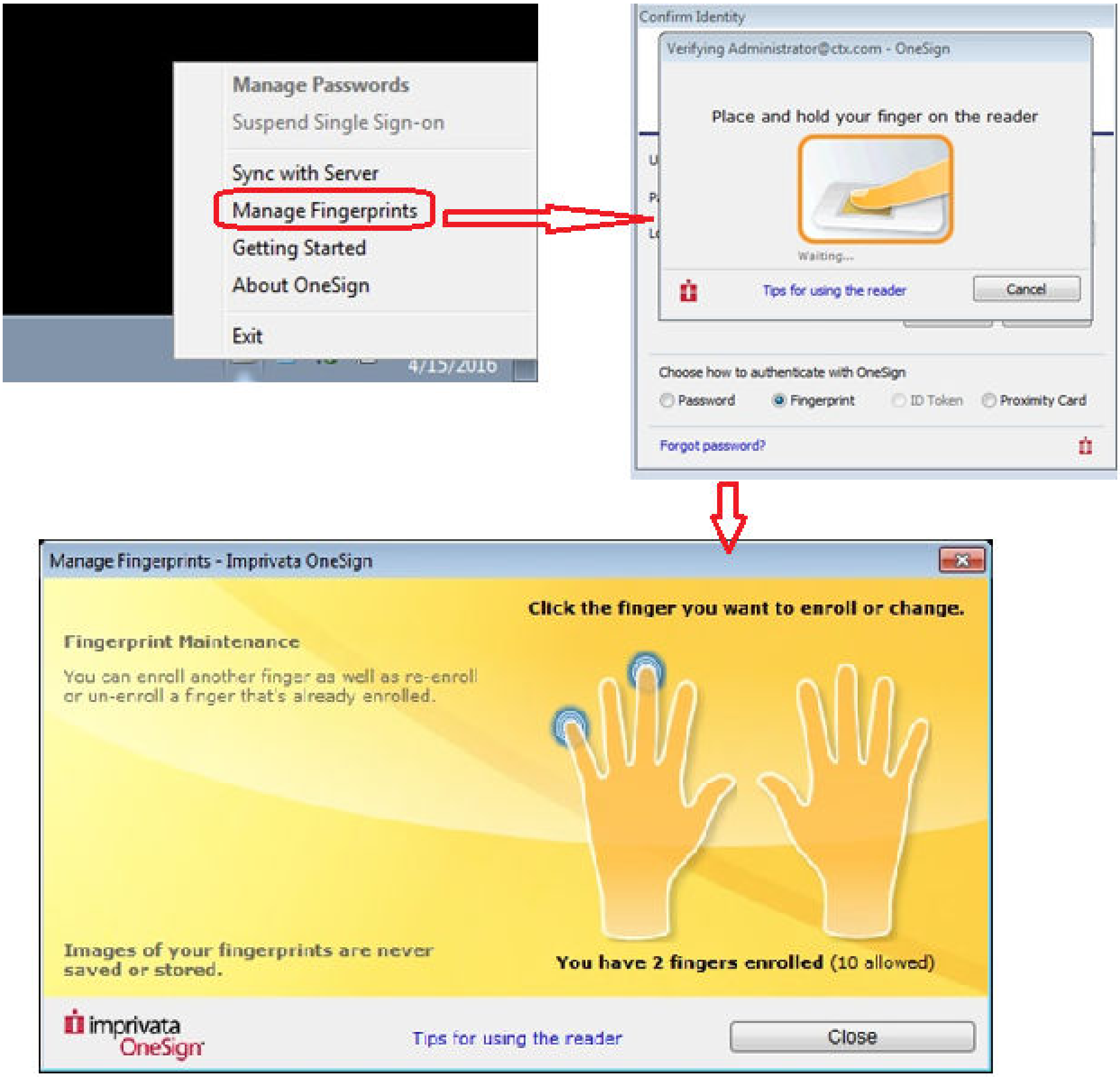
3 Managing Fingerprints on virtual desktop.

- Legend Fingerprint Management is supported.
- Fingerprint management with Imprivata Confirm ID enabled is not supported. This requires both supervisor and user to finish the enrollment and it is recommended to use Windows platform to perform this action.

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.



Verifying Administrator@ctx.com - OneSign

Place and hold your finger on the reader

Waiting...

Choose how to authenticate with OneSign

○ Password ● Fingerprint ○ ID Token ○ Proximity Card

Click the finger you want to enroll or change.

Fingerprint Maintenance

You can enroll another finger as well as re-enroll or un-enroll a finger that's already enrolled.

Images of your fingerprints are never saved or stored.

You have 2 fingers enrolled (10 allowed)

Configuring the Caradigm server

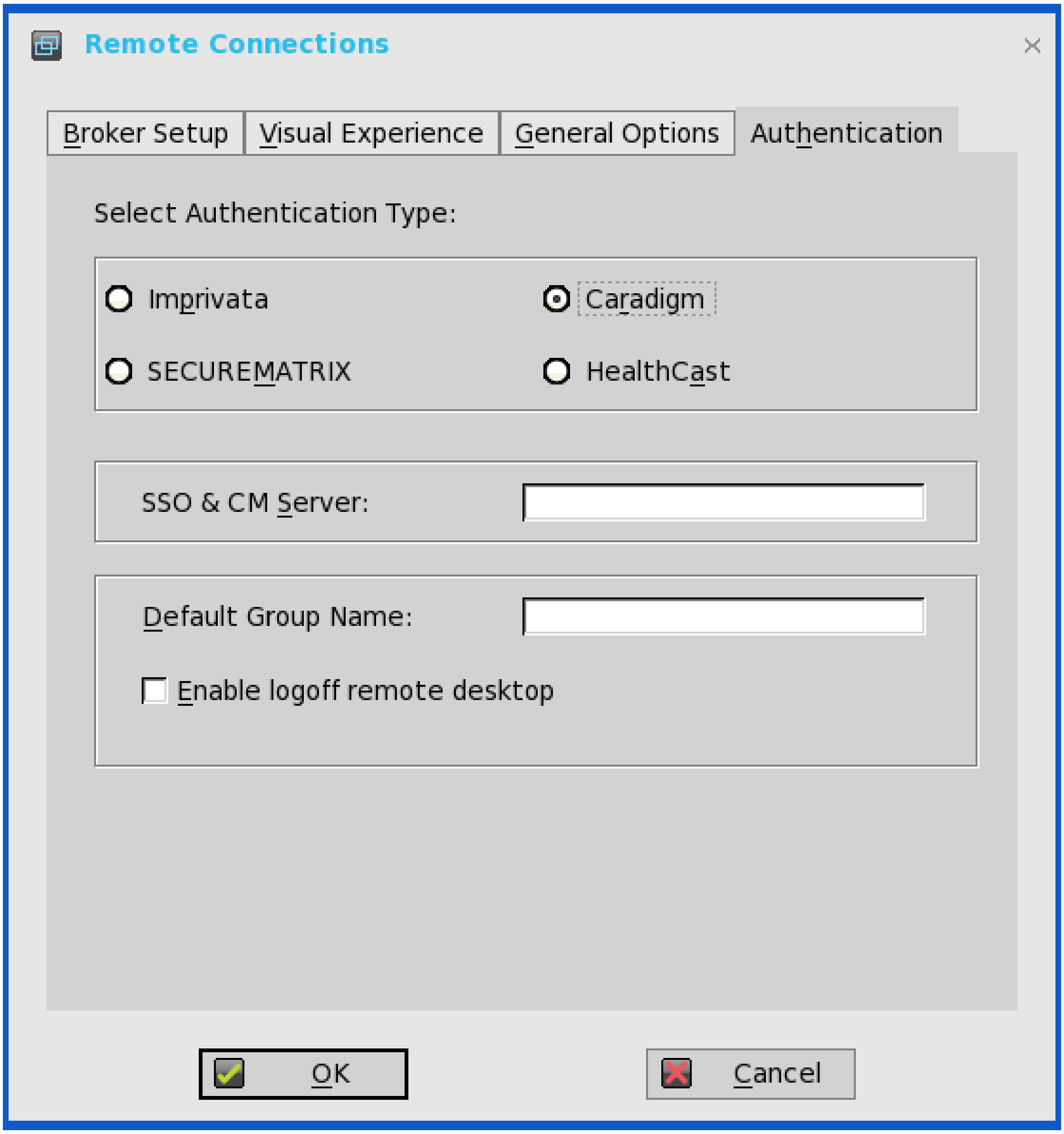
Caradigm Single Sign-on and Context Management (SSO & CM) is the product of the Caradigm Company which provides Single Sign-on and Context Management Services. Caradigm solution has been integrated since ThinOS 8.1.

To configure the Caradigm integration on ThinOS, do the following:

1 From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

2 Click the **Authentication** tab, and then click **Caradigm**.



Remote Connections

Select Authentication Type:

○ Imprivata ● Caradigm

○ SECUREMATRIX ○ HealthCast

SSO & CM Server:

Default Group Name:

□ Enable logoff remote desktop

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.

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

Configuring the Caradigm Vault server

To configure the Caradigm Vault server on ThinOS:

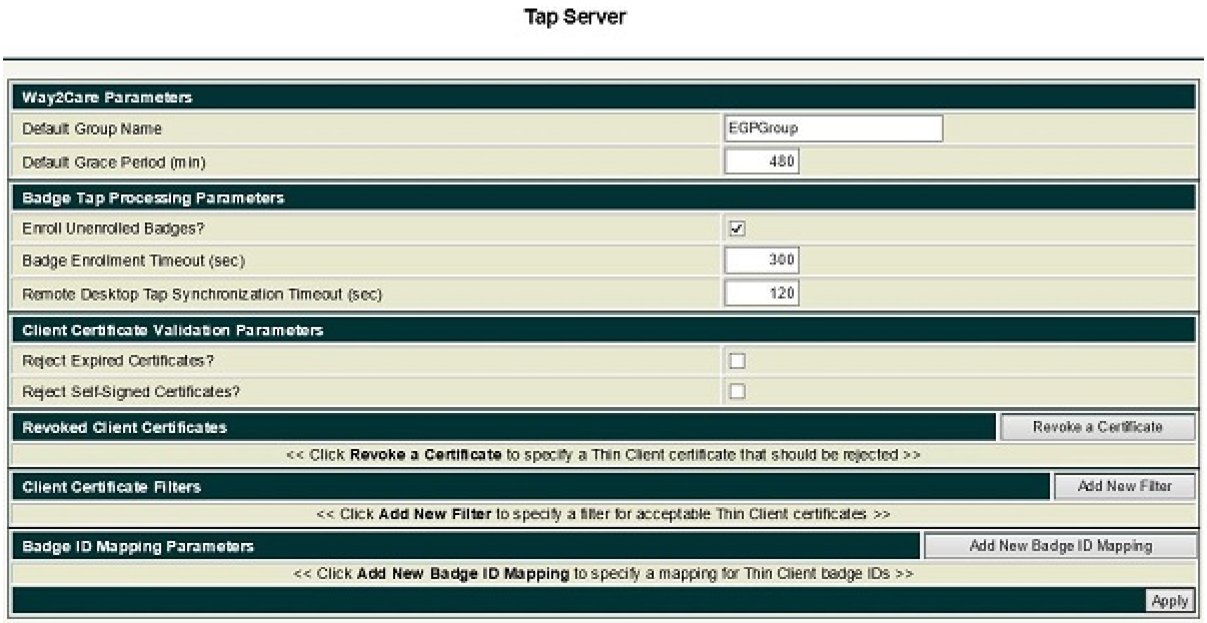
1 From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

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

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

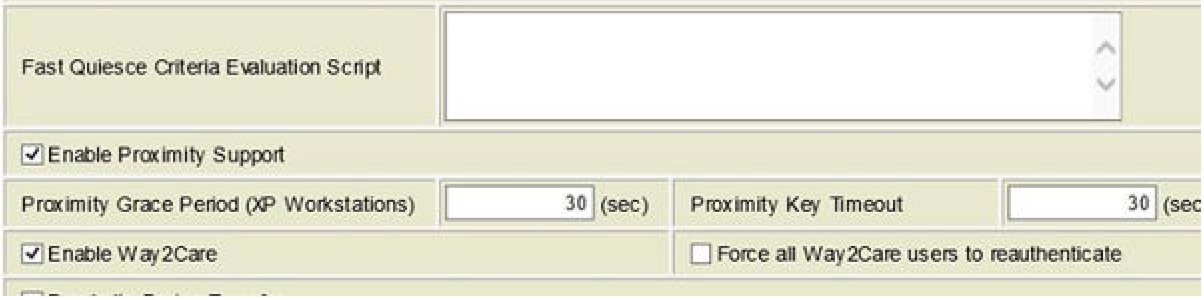
- Ensure that the **Enroll unenrolled badges** option is checked.
- Make sure that all Badge ID mapping entries are deleted.



Tap Server

Way2Care Parameters	
Default Group Name	EGPGroup
Default Grace Period (min)	480
Badge Tap Processing Parameters	
Enroll Unenrolled Badges?	☑
Badge Enrollment Timeout (sec)	300
Remote Desktop Tap Synchronization Timeout (sec)	120
Client Certificate Validation Parameters	
Reject Expired Certificates?	□
Reject Self-Signed Certificates?	□
Revoked Client Certificates	Revoke a Certificate
<< Click **Revoke a Certificate** to specify a Thin Client certificate that should be rejected >>	
Client Certificate Filters	Add New Filter
<< Click **Add New Filter** to specify a filter for acceptable Thin Client certificates >>	
Badge ID Mapping Parameters	Add New Badge ID Mapping
<< Click **Add New Badge ID Mapping** to specify a mapping for Thin Client badge IDs >>	
	Apply

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



Fast Quiesce Criteria Evaluation Script			
☑ Enable Proximity Support			
Proximity Grace Period (XP Workstations)	30 (sec)	Proximity Key Timeout	30 (sec
☑ Enable Way2Care		□ Force all Way2Care users to reauthenticate	

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 thin client.

a To raise a request for the certificate:

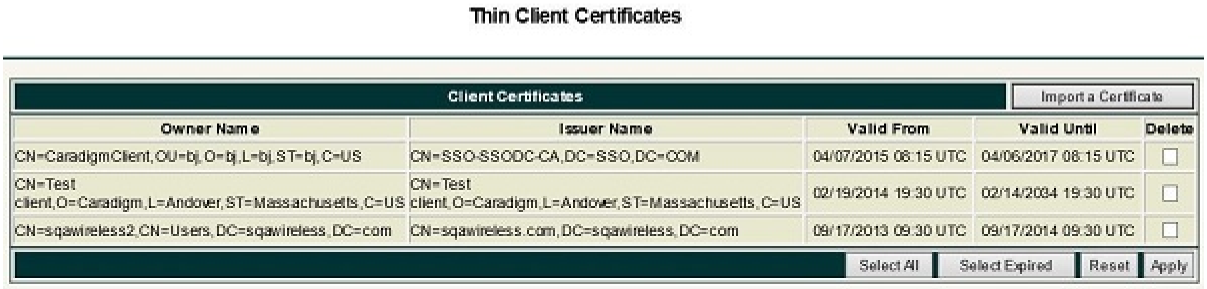
- The certificate should be issued by your Certificate Authority.
- Prepare the certificate in two formats:
  - PFX format which has a private key.
  - The other is PEM format which is text-based, Base64-encoded DER file. For Example, Caradigm.cer, Caradigm.pfx.

b To import a certificate to the thin 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:



Thin Client Certificates

Client Certificates — Import a Certificate

Owner Name	Issuer Name	Valid From	Valid Until	Delete
CN=CaradigmClient,OU=bj,O=bj,L=bj,ST=bj,C=US	CN=SSO-SSODC-CA,DC=SSO,DC=COM	04/07/2015 08:15 UTC	04/06/2017 08:15 UTC	□
CN=Test client,O=Caradigm,L=Andover,ST=Massachusetts,C=US	CN=Test client,O=Caradigm,L=Andover,ST=Massachusetts,C=US	02/19/2014 19:30 UTC	02/14/2034 19:30 UTC	□
CN=sqawireless2,CN=Users,DC=sqawireless,DC=com	CN=sqawireless.com,DC=sqawireless,DC=com	09/17/2013 09:30 UTC	09/17/2014 09:30 UTC	□

Use the **Thin Client Certificates** page to add certificates for the thin 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** > **Thin Client Certificates**.
- Copy the Notepad text to the Vault server

Configuration on VDI server and desktops

Caradigm solution of ThinOS supports the multi-types of VDI server such as VMware View Horizon 6, Citrix XenApp 6.5, Citrix XenDesktop 5.6 and Citrix XenDesktop 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
```

SSO and CM client installed on your VDI server and desktops must be upgraded to latest version 6.2.5 in order to support this feature.

Configuring 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 Dell Wyse ThinOS INI Guide. For details see SECUREMATRIX documentation.

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 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 is a client-server solution. ThinOS 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

HealthCast Web API Server is integrated with ThinOS release to implement the HealthCast SSO solution. To use the HealthCast SSO solution, ThinOS 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 UI. Dell recommends you to use the INI file for large deployments.

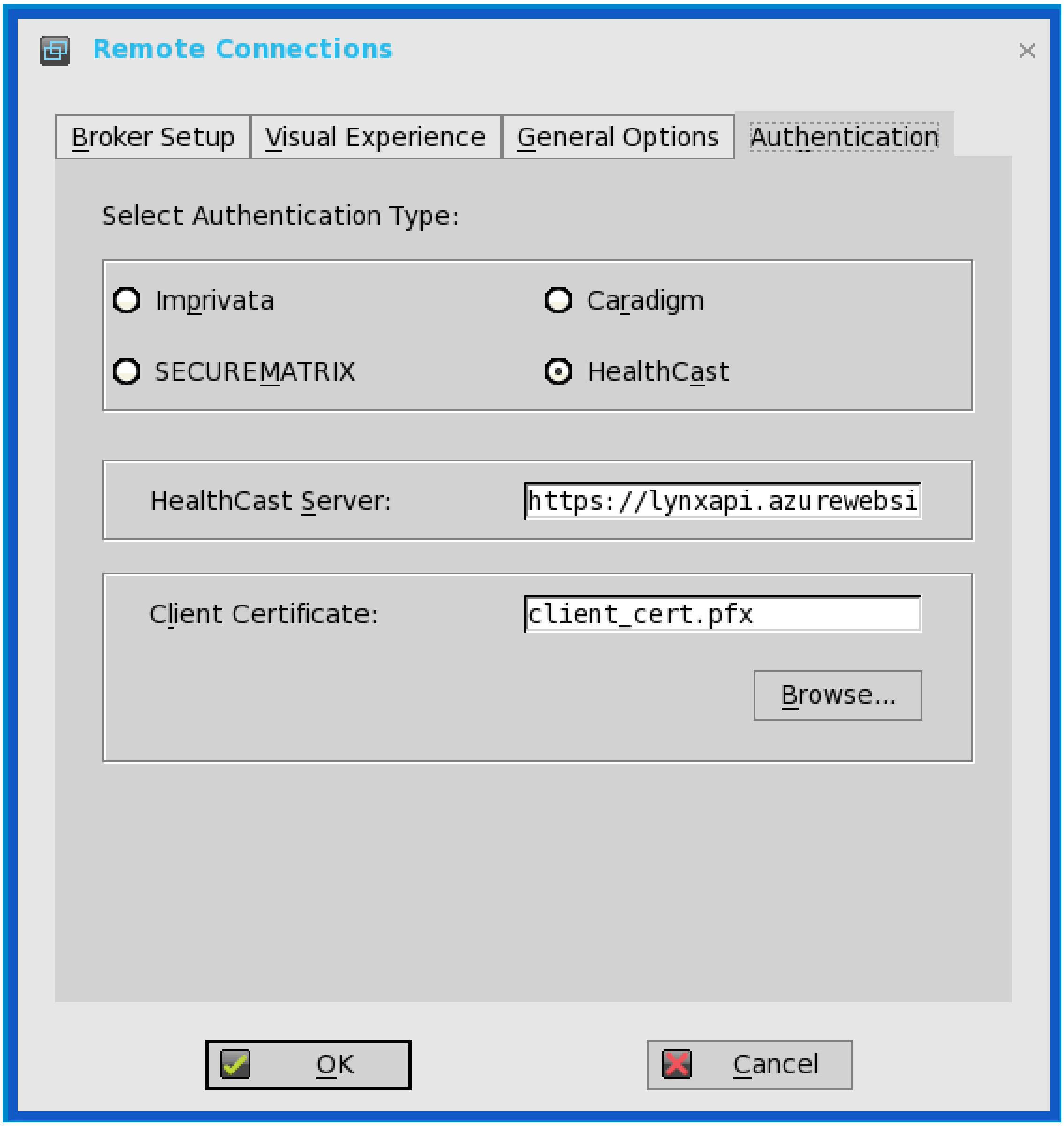
ThinOS UI configuration

- To use the HealthCast Web API, configure the HealthCast settings on the thin 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**.



Select Authentication Type:

○ Imprivata ○ Caradigm

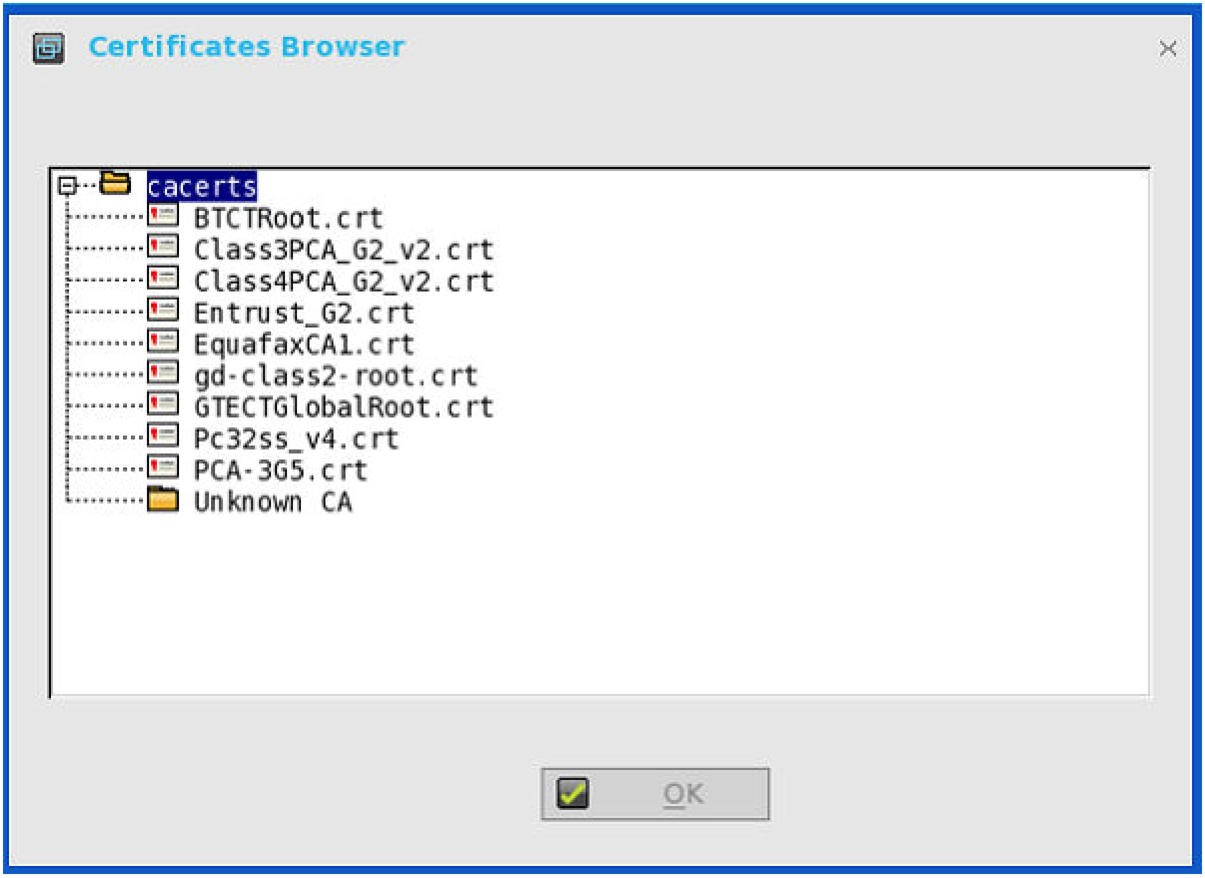
○ SECUREMATRIX ● HealthCast

HealthCast Server: https://lynxapi.azurewebsi

Client Certificate: client_cert.pfx

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.



Certificates Browser

cacerts
- BTCTRoot.crt
- Class3PCA_G2_v2.crt
- Class4PCA_G2_v2.crt
- Entrust_G2.crt
- EquafaxCA1.crt
- gd-class2-root.crt
- GTECTGlobalRoot.crt
- Pc32ss_v4.crt
- PCA-3G5.crt
- Unknown CA

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>

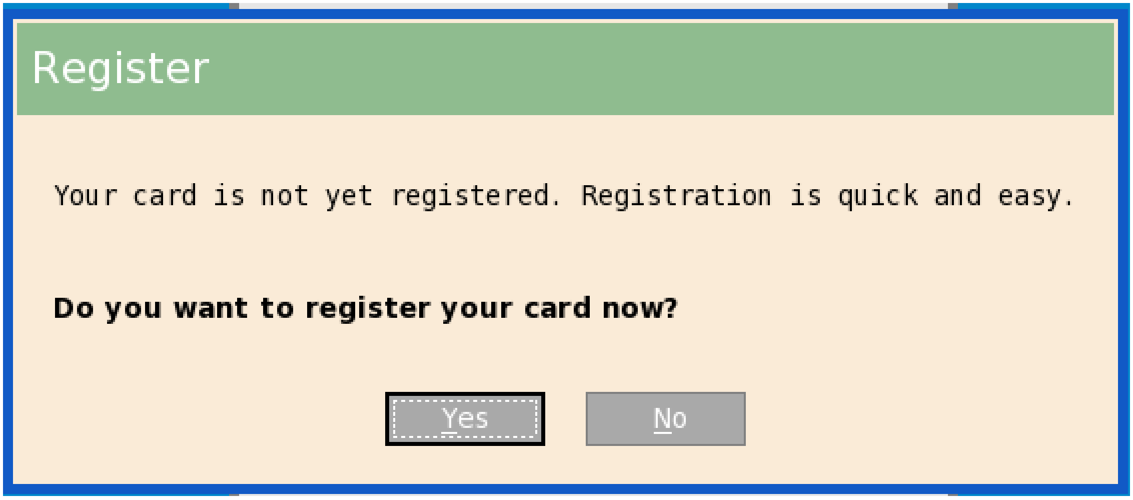
For example: HealthCastServer=https://server1.example.com SecurityMode=full ClientCertificate=client-cert.pfx.

For more information on INI parameters, see Dell Wyse INI Reference Guide.

HealthCast SSO features and functionality on ThinOS

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

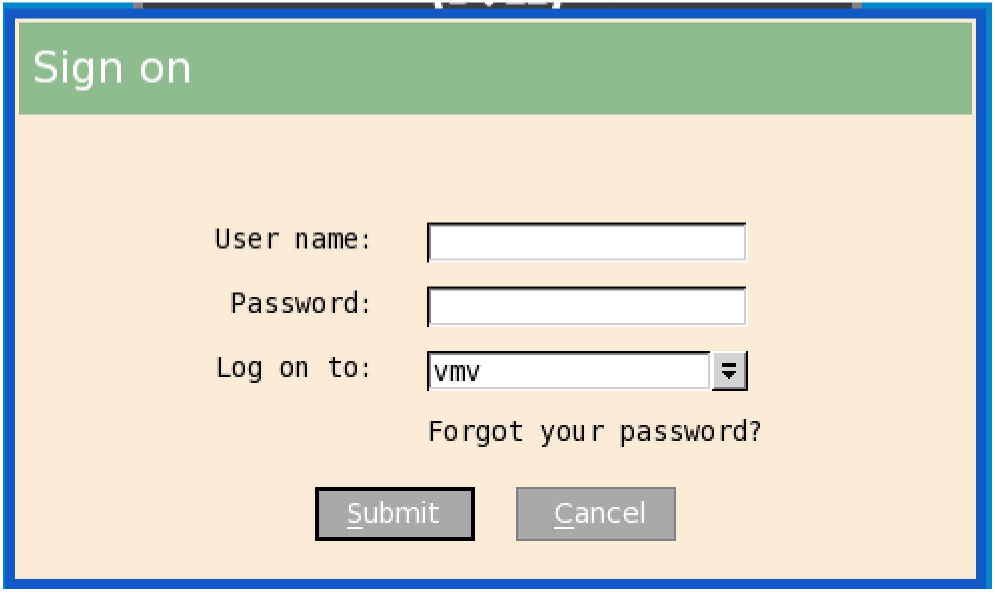
- **Proximity card enrollment**—HealthCast supports user self-enrollment. Therefore, there is no need to bring the proximity card to a special registration station, or for IT staff to be involved. Instead, you must only tap the disenrolled proximity card at a terminal and you can follow the easy registration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



Your card is not yet registered. Registration is quick and easy.

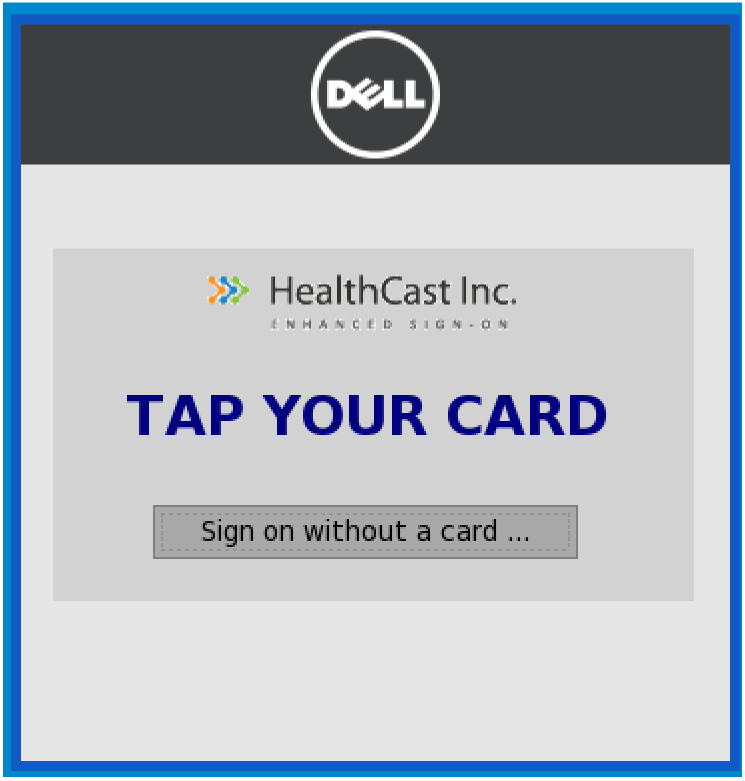
Do you want to register your card now?

- **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.



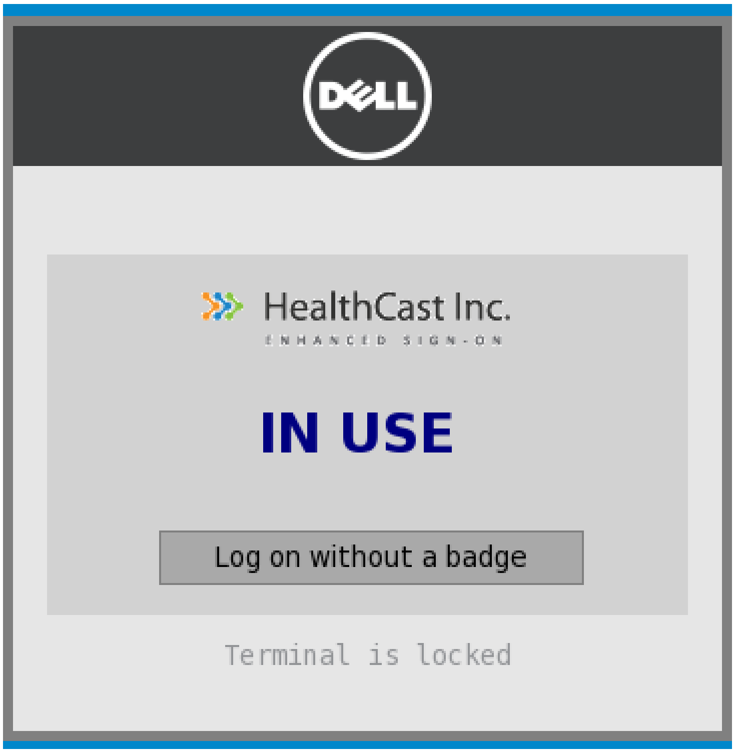
Log on to: vmv

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



TAP YOUR CARD

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.



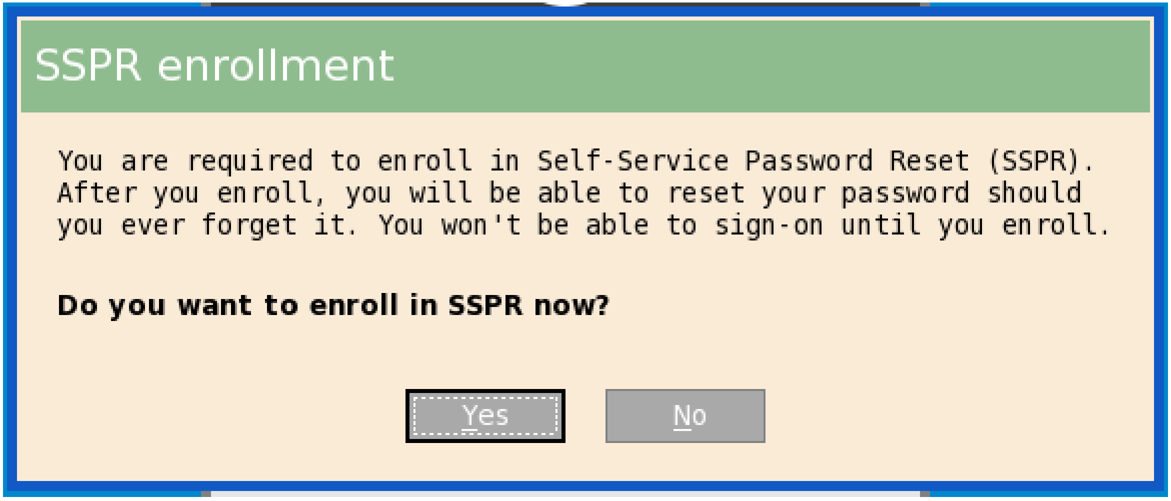
IN USE

Terminal is locked

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 in this section.
- **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.



SSPR enrollment

You are required to enroll in Self-Service Password Reset (SSPR). After you enroll, you will be able to reset your password should you ever forget it. You won't be able to sign-on until you enroll.

Do you want to enroll in SSPR now?

- **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 thin 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:

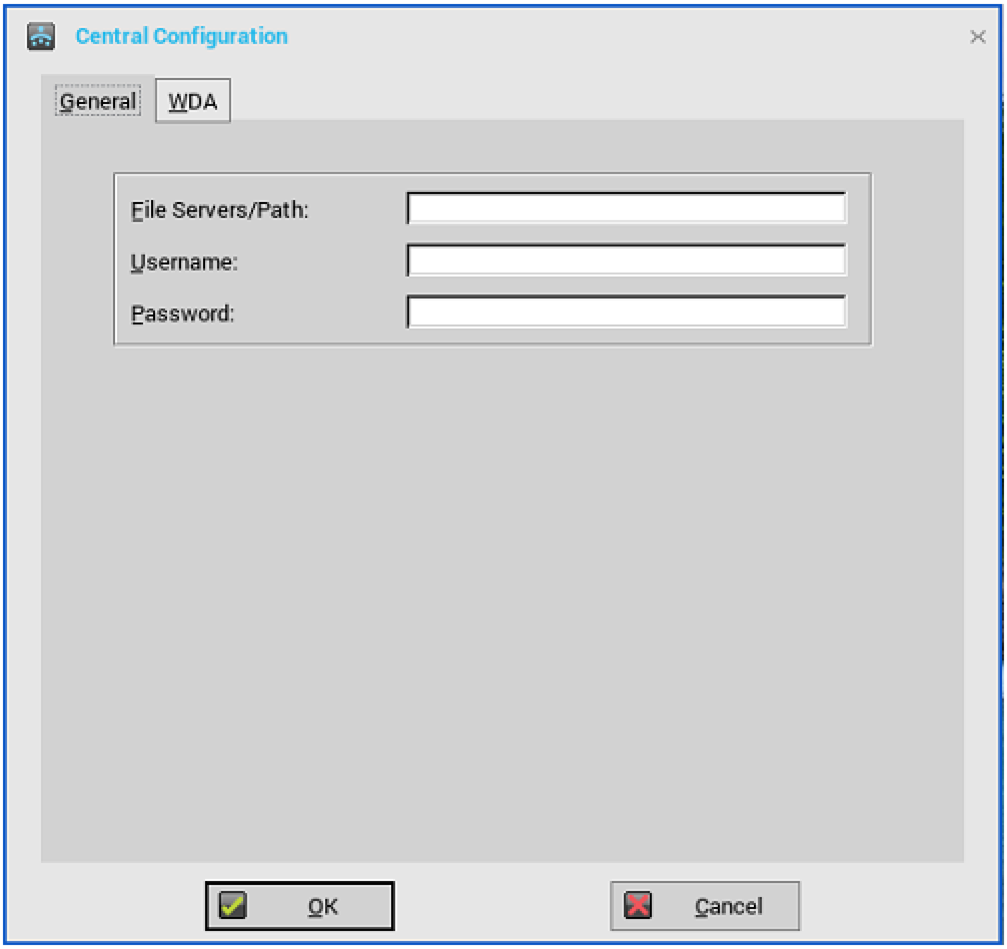
- Configuring the general central configurations.
- Configuring the WDA settings.

Configuring the general central configurations

To configure the general central configurations:

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

   The **Central Configuration** dialog box is displayed.
2. Click **General** tab, and use the following guidelines:



File Servers/Path, **Username** and **Password** — Enter the 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** — Enter the username to log in to the file server. Use maximum of 31 characters.

c **Password** — Enter the 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

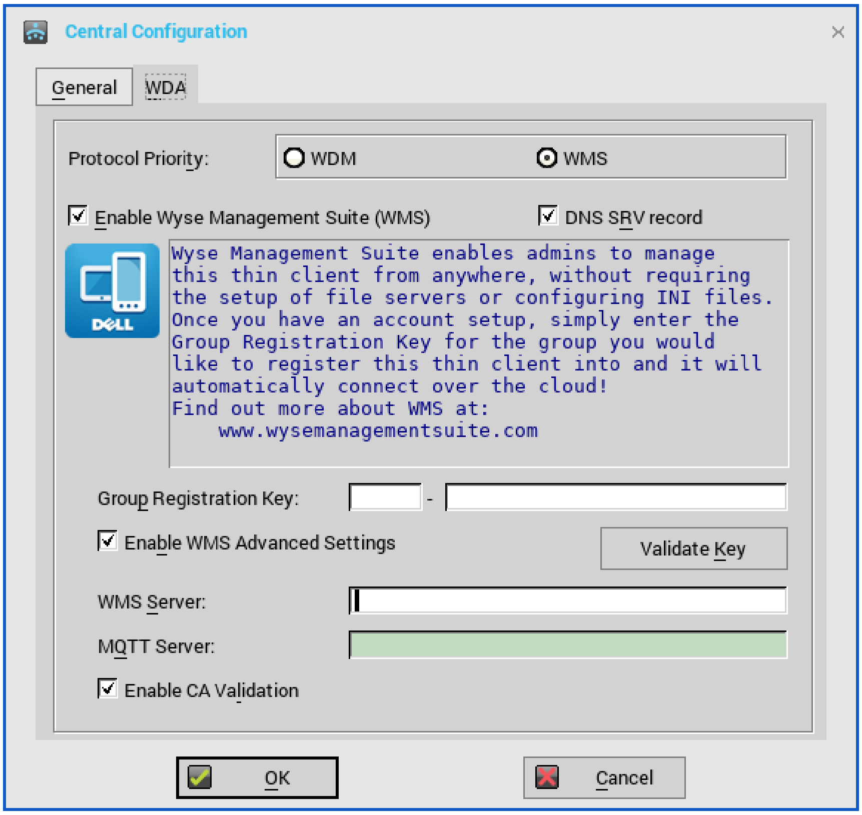
Use this tab to configure the Wyse Device Manager and Wyse Management Suite settings.

ThinOS 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:



Protocol Priority: ○ WDM ● WMS

☑ Enable Wyse Management Suite (WMS) ☑ DNS SRV record

```
Wyse Management Suite enables admins to manage
this thin client from anywhere, without requiring
the setup of file servers or configuring INI files.
Once you have an account setup, simply enter the
Group Registration Key for the group you would
like to register this thin client into and it will
automatically connect over the cloud!
Find out more about WMS at:
    www.wysemanagementsuite.com
```

Group Registration Key: -

☑ Enable WMS Advanced Settings

WMS Server:

MQTT Server:

☑ Enable CA Validation

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, then 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 registers to a quarantine tenant in Wyse Management Suite.

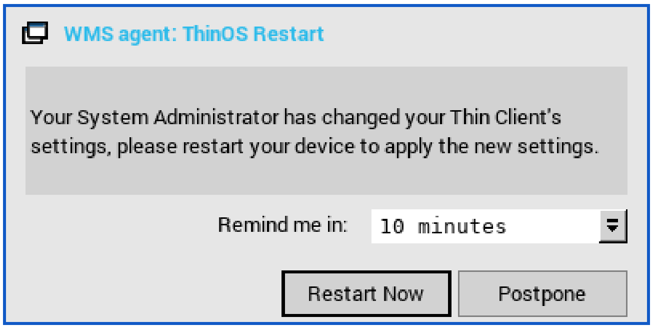
d **Enable WMS Advanced Settings**—Select this check box to enter the Wyse Management Suite server, MQTT server details, and to enable the CA validation. By default, the MQTT server option is disabled. The MQTT server value is populated after the ThinOS device is checked in to the Wyse Management Suite.

ⓘ 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 devices, see the Wyse Management Suite Administrator's Guide at www.dell.com/manuals.

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

When you modify the ThinOS 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**.



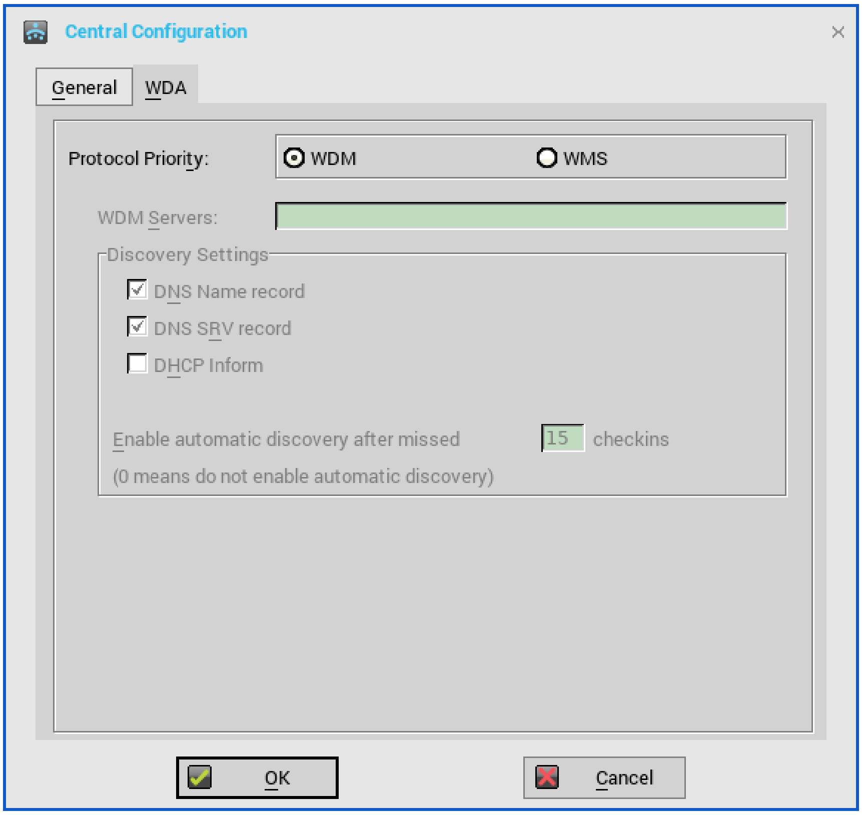
WMS agent: ThinOS Restart

Your System Administrator has changed your Thin Client's settings, please restart your device to apply the new settings.

Remind me in: 10 minutes

Figure 5. Wyse Management Agent: ThinOS restart

To configure the WDM settings, do the following:



Protocol Priority: ● WDM ○ WMS

WDM Servers:

Discovery Settings

☑ DNS Name record

☑ DNS SRV record

□ DHCP Inform

Enable automatic discovery after missed 15 checkins

(0 means do not enable automatic discovery)

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

   a **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.

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

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

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

2 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

VPN Manager is included to manage VPN connections. 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 benefiting from the functionality, security and management policies of the private network.

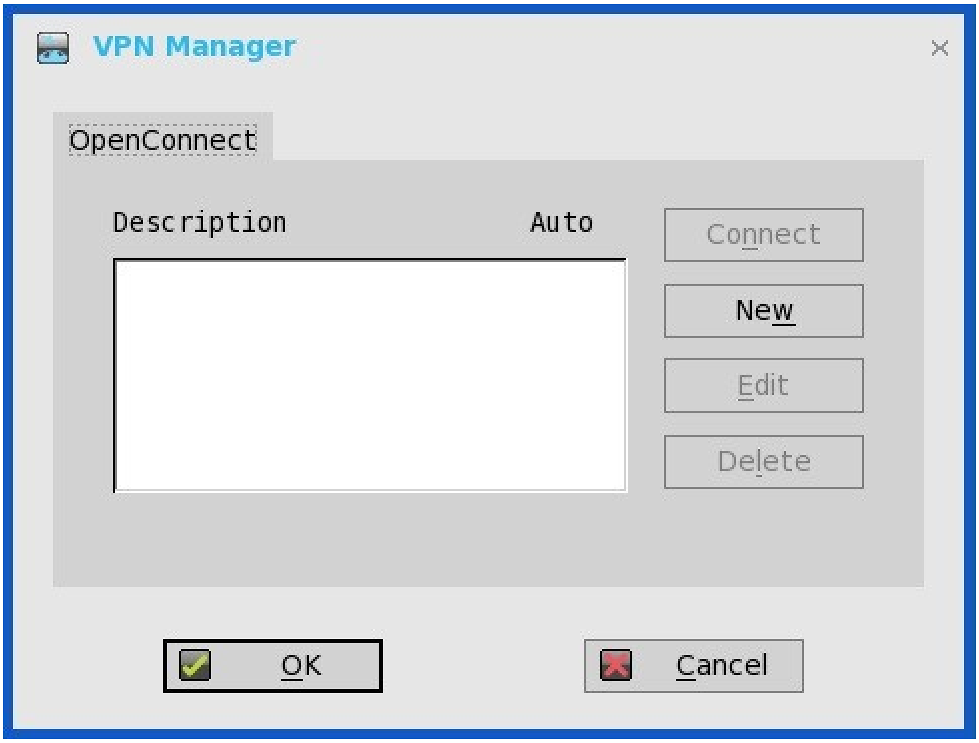
To configure the VPN Manager, use the following guidelines:

1 In Classic Mode, from the desktop menu, click **System Setup** > **VPN Manager**.

   In Zero Mode, user can view the **VPN Manager** tab in System Settings panel.

2 Click **VPN Manager**.

   The **VPN Manager** dialog box is displayed.



3 Click **New** to create a new session.

a Session Name (up to 21 characters)—Enter the name of the Session Name. This is not a mandatory option. If the field is left blank, the VPN server name will be used as the session name.

b VPN server (up to 63 characters)—Enter the IP address of the VPN Server. This is defined as either an IP address or a host name. This is a mandatory option.

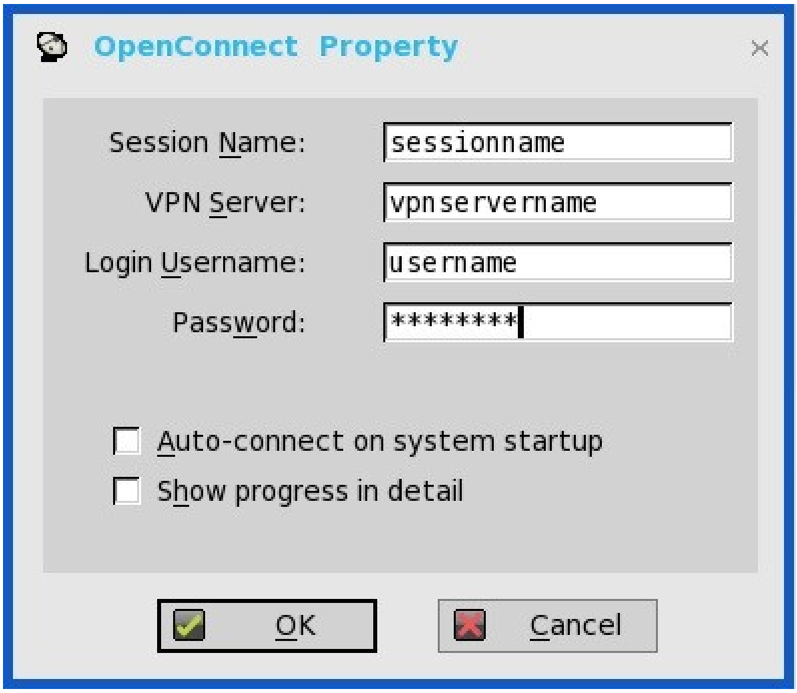
c Login Username (up to 31 characters)—Enter the Login Username. This is a mandatory option.

d Login Password (up to 31 characters)—Enter the password of the user. This is not a mandatory option.

e Select the check box to Auto-connect on system startup.

f Select the check box to show progress in detail.

g Click **OK**.



Session Name: sessionname

VPN Server: vpnservername

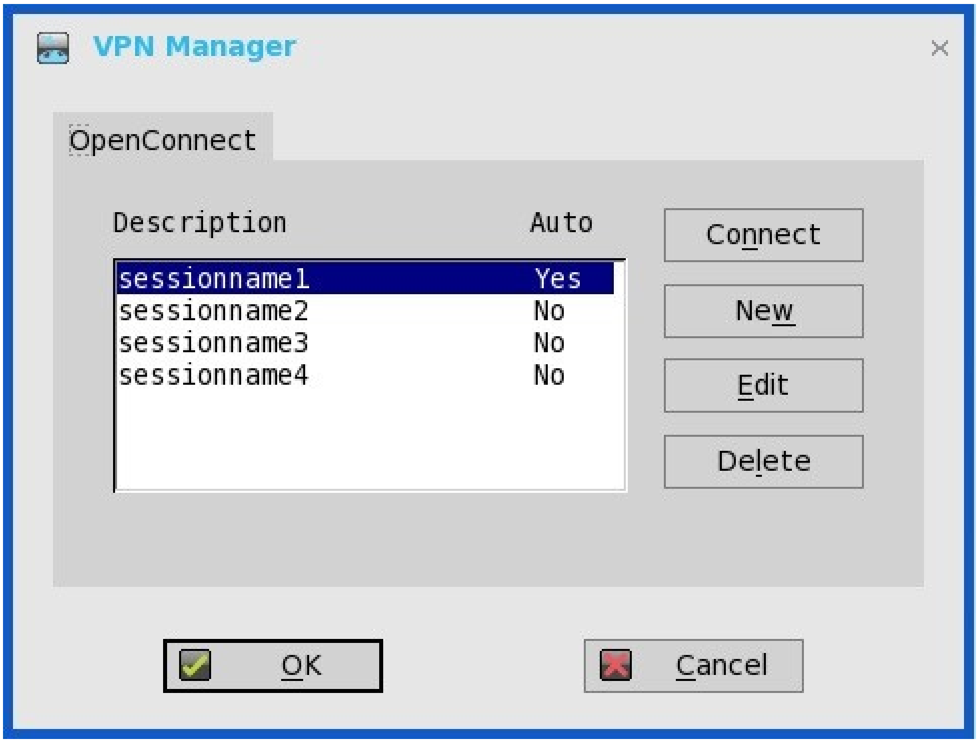
Login Username: username

Password: ********

□ Auto-connect on system startup

□ Show progress in detail

When the connections are created, the description column lists the session name and the Auto column shows which connection is automatically connected when the unit restarts. Only one session can be set to auto-connect.



Description	Auto
sessionname1	Yes
sessionname2	No
sessionname3	No
sessionname4	No

4 Click **Connect**.

The connection status is displayed.

Configuring the connection brokers

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 Citrix, VMware, and Dell vWorkspace brokers are supported.
- Windows 10 desktop in multiple brokers is supported.
  - Windows 10 desktop is supported in Citrix, VMware, and RDS brokers.
  - Windows 10 remote desktop published from Microsoft RDS does not support MMR. Windows 10 remote desktops published from VMware Horizon and Citrix Xen support MMR.
- ICA multicast feature is not supported from ThinOS 8.4. 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 device, and other Citrix features that you can configure on ThinOS.

Configuring the Citrix broker connection

To configure the Citrix broker setup:

1 From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

2 In the **Broker Setup** tab, from the drop-down list, select **Citrix Xen**, and do the following:

- Select the check box to enable the **StoreFront style**.
- **Broker Server**— Enter the IP address/Hostname/FQDN of the Broker Server.
- **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semi-colon, and is case-sensitive.
- Select the check box to enable automatic reconnection at logon.

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

- Select the check box to enable automatic reconnection from the button menu.

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

- **Account Self-Service Server**— Enter the IP address of the Account self-service server.
- **XenApp** — Use this option, if you want to set default settings to **XenApp**.
- **XenDesktop**— Use this option, if you want to set default settings to **XenDesktop**.

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

Citrix HDX RealTime Multimedia Engine or RealTime Optimization Pack

HDX RealTime Optimization Pack (RTOP) provides a scalable solution to deliver audio-video conferencing and Voice over Internet Protocol (VoIP) enterprise telecommunication by using Microsoft Skype for Business. The Optimization Pack supports XenDesktop and XenApp environments to users on ThinOS devices. For more information about HDX RealTime Optimization Pack, see Citrix documentation.

This section provides information about supported platforms for RealTime Multimedia Engine (RTME), installation of RTME package, Citrix remote server/Desktop host preparation, configuration on ThinOS, and RTME status check and troubleshooting.

- Introduction
- Installing the RTME package on ThinOS
- Setting up the RTME connector
- Verifying the RTME 1.8 Status
- Verifying the RTME 2.x Status

Introduction

Citrix HDX RealTime Optimization pack offers high-definition audio and video calls. In every ThinOS release, the 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. ThinOS supports RTME/RTOP version 2.3. However, you can still use RTME 2.2 package.

For more information about Citrix RTME 1.8, and 2.x features, see the Citrix documentation at www.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.x (Both Skype for Business 2015 and Skype for Business 2016 are 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, See the Citrix documentation.

Installing RTME package on ThinOS

You are required to install the RTME.i386 package for the RTME feature to work on ThinOS.

To install the RTME.i386 package:

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

   ⓘ **NOTE: For the latest RTME package version, see the latest Dell Wyse ThinOS Release Notes.**
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 or Skype for Business (SFB) on a Citrix desktop.

1 Install Citrix HDX RealTime Connector on Citrix desktop VDA/Server. HDX RealTime Multimedia Engine (RTME) is the package installed on ThinOS. It is HDX RealTime Connector that needs to be installed or upgraded on the remote server and VDA.

> ⓘ NOTE: **The following are applicable to RTME 1.8 only:**
>
> - 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.
> - The RTME 1.8 feature on ThinOS supports only HDX RealTime Connector 1.8 due to Citrix limitation.

2 Update the ThinOS firmware, and install the **RTME.i386.pkg** on the ThinOS client.

> ⓘ IMPORTANT: **Since ThinOS 8.3.1 HF release, the RTME 1.8 and 2.1 co-exist in the release package, supporting both versions of RTME connectors. In every ThinOS release, the 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 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 or Skype for Business (SFB) client.

- For RTME 1.8, the RTME icon is displayed in the lower-left corner of the Lync client window.
- For RTME 2.x, 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 RTME 1.8, press **Ctrl+N** to open the **Network Health** window.
  - For RTME 2.x, right-click the RTME icon on taskbar and 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.

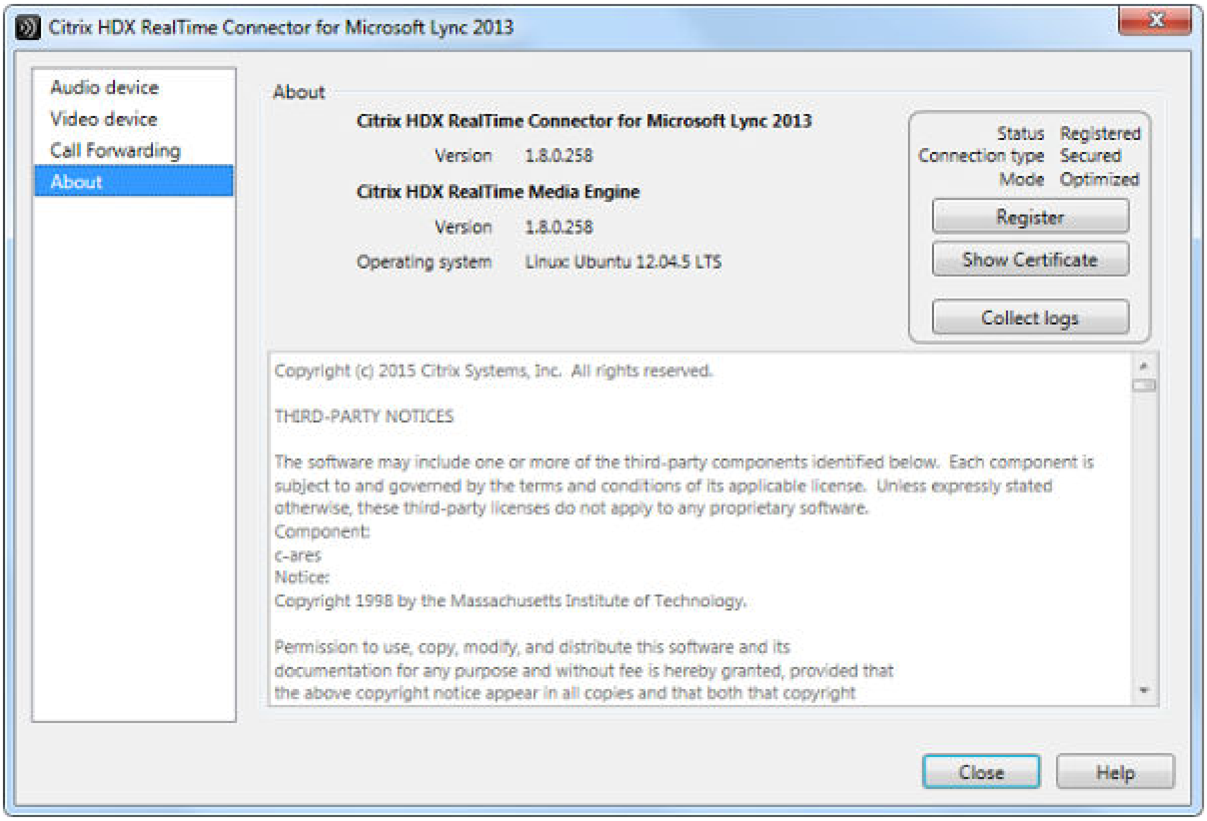
Verifying the RTME 1.8 status

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.



Citrix HDX RealTime Connector for Microsoft Lync 2013

Version 1.8.0.258

Citrix HDX RealTime Media Engine

Version 1.8.0.258

Operating system Linux Ubuntu 12.04.5 LTS

Status Registered
Connection type Secured
Mode Optimized

Copyright (c) 2015 Citrix Systems, Inc. All rights reserved.

THIRD-PARTY NOTICES

The software may include one or more of the third-party components identified below. Each component is subject to and governed by the terms and conditions of its applicable license. Unless expressly stated otherwise, these third-party licenses do not apply to any proprietary software.
Component:
c-ares
Notice:
Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright

2 Click the **About** tab in the **Citrix HDX RealTime Connector for Microsoft Lync 2013** dialog box.

   The RTME status is displayed in the upper-right pane of the dialog box. If the RealTime Multimedia Engine is successfully initiated between the ThinOS client and Citrix desktop, the RTME status is displayed as follows:

Table 6. RTME status

Attribute	Value
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 shows only one device from ThinOS local playback device. It can actually work the way they are configured at ThinOS local playback device and record device. The RTME audio device for ringtone is limited to use ThinOS 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.**

For more information about trouble shooting, go to docs.citrix.com/en-us/hdx-optimization/1-8/hdx-realtime-optimization-pack-troubleshooting.html.

Known Issues with RTME 1.8 feature

- RTME operation system on ThinOS is displayed as Linux.
- The RTME 1.8 feature on ThinOS 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.
- 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 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 Skype For Business 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 device.
3 Connect the audio or video devices.

ⓘ **NOTE: USB redirection needs to be disabled for audio or video devices.**

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

ⓘ **NOTE: RTME 2.2 and later versions support various call scenarios. For more information, refer to Citrix documentation.**

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

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 or Limitations

- The video sent from client in call is decided by capabilities of both endpoints in the call. Sending higher video from one client does not mean that the client has better capability than the other one in call.
- RTME status dialog displays operation system as Linux.
- 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 audio settings of SFB client to high. By default, the SFB client audio volume is set to 40 percent. 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.
- In Citrix RTME version 2.3, the video performance of applications is designed for a lower CPU consumption. Therefore, the video resolution may be downgraded compared to version 2.2.

Citrix icon refresh

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

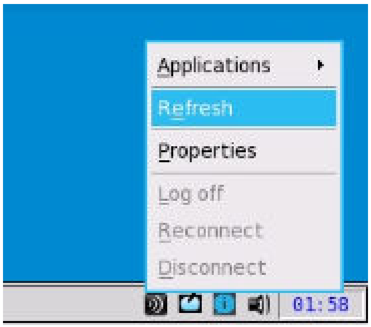
There are two methods to refresh the Citrix applications:

- Manual refresh
- Auto refresh using the INI parameter

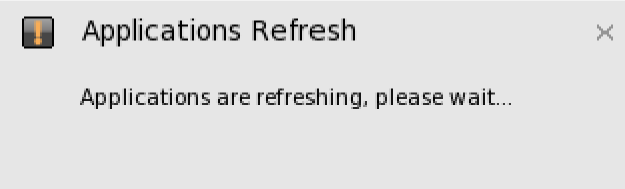
Refreshing Citrix applications manually

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.



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



Applications Refresh

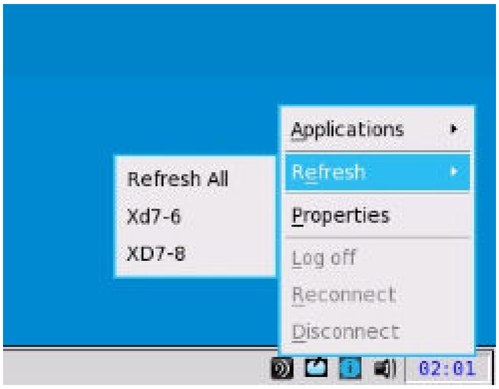
Applications are refreshing, please wait...

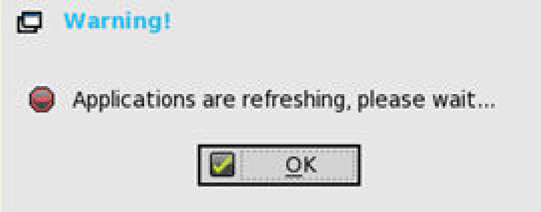
2 Applications are refreshed in Session bar list, Connect Manager list and App menu list.

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.



> NOTE:
> Warning message is displayed when you open or edit or remove applications when you refresh the applications.
>
> 
> Warning!
>
> Applications are refreshing, please wait...
>
>

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 by 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 supports multiple audio device utilizations in the XenDesktop or XenApp 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.

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, pre-configuration 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 devices that are already selected.
- 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 devices that are already selected.

The following scenarios must be considered during multiple audio settings:

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

Using Citrix NetScaler with CensorNet MFA authentication

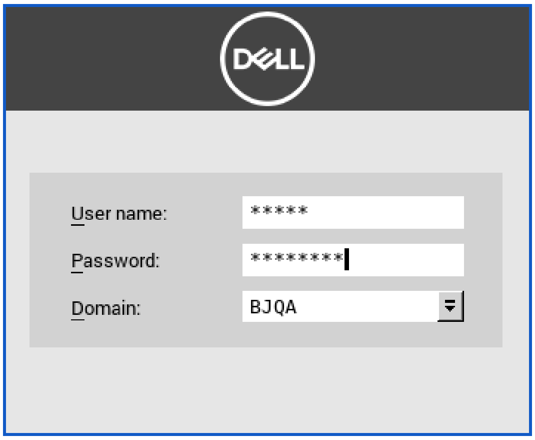
SMS PASSCODE is re-branded as CensorNet MFA. You can configure NetScaler Gateway to use a One Time Passcode/Password (OTP) in the form of a personal identification number (PIN) or passcode. To obtain this one-time password, you must install CensorNet app on your mobile. After you enter the passcode or 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, do the following:

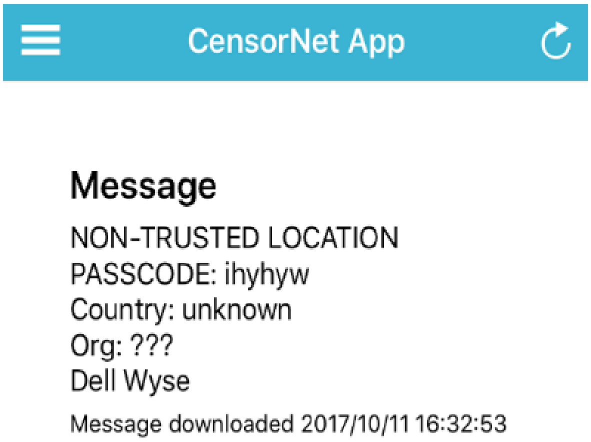
1 Log in to ThinOS, and connect to the NetScalar Gateway URL.
2 Enter your credentials (user ID and password), and press Enter.
  The PASSCODE dialog box is displayed. You will receive a push notification from the CensorNet App on your phone with the code.



User name: *****

Password: ********

Domain: BJQA



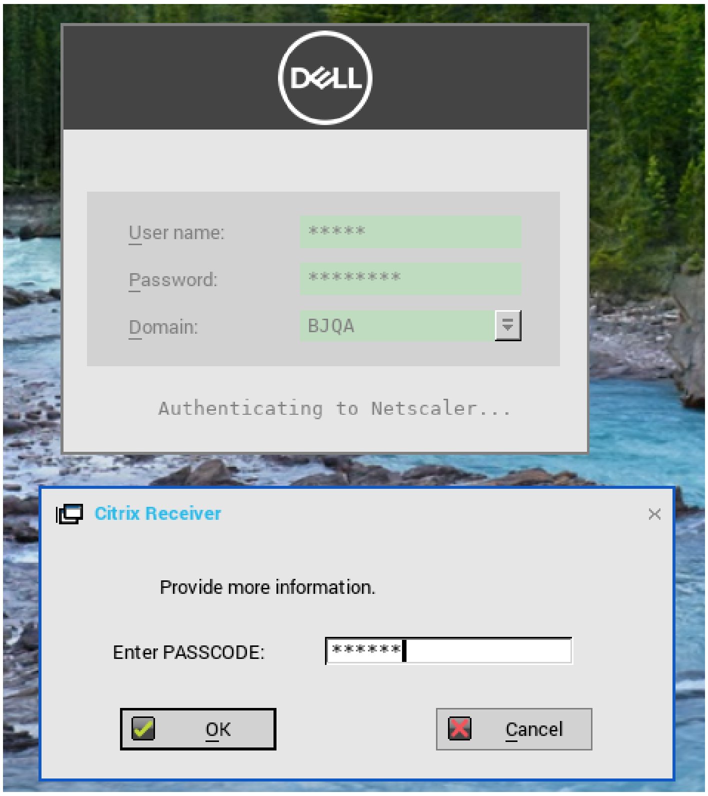
Message

NON-TRUSTED LOCATION
PASSCODE: ihyhyw
Country: unknown
Org: ???
Dell Wyse

Message downloaded 2017/10/11 16:32:53

3 Click **OK**.

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



User name: *****

Password: ********

Domain: BJQA

Authenticating to Netscaler...

Citrix Receiver

Provide more information.

Enter PASSCODE: ******

Configuring ICA connections

To configure the ICA connections:

1 From the desktop menu, click **System Setup**, and then click **Remote Connections**.

The **Remote Connections** dialog box is displayed.

2 In the **Broker Setup** tab, from the drop-down list, select the **Broker type** as **None**.

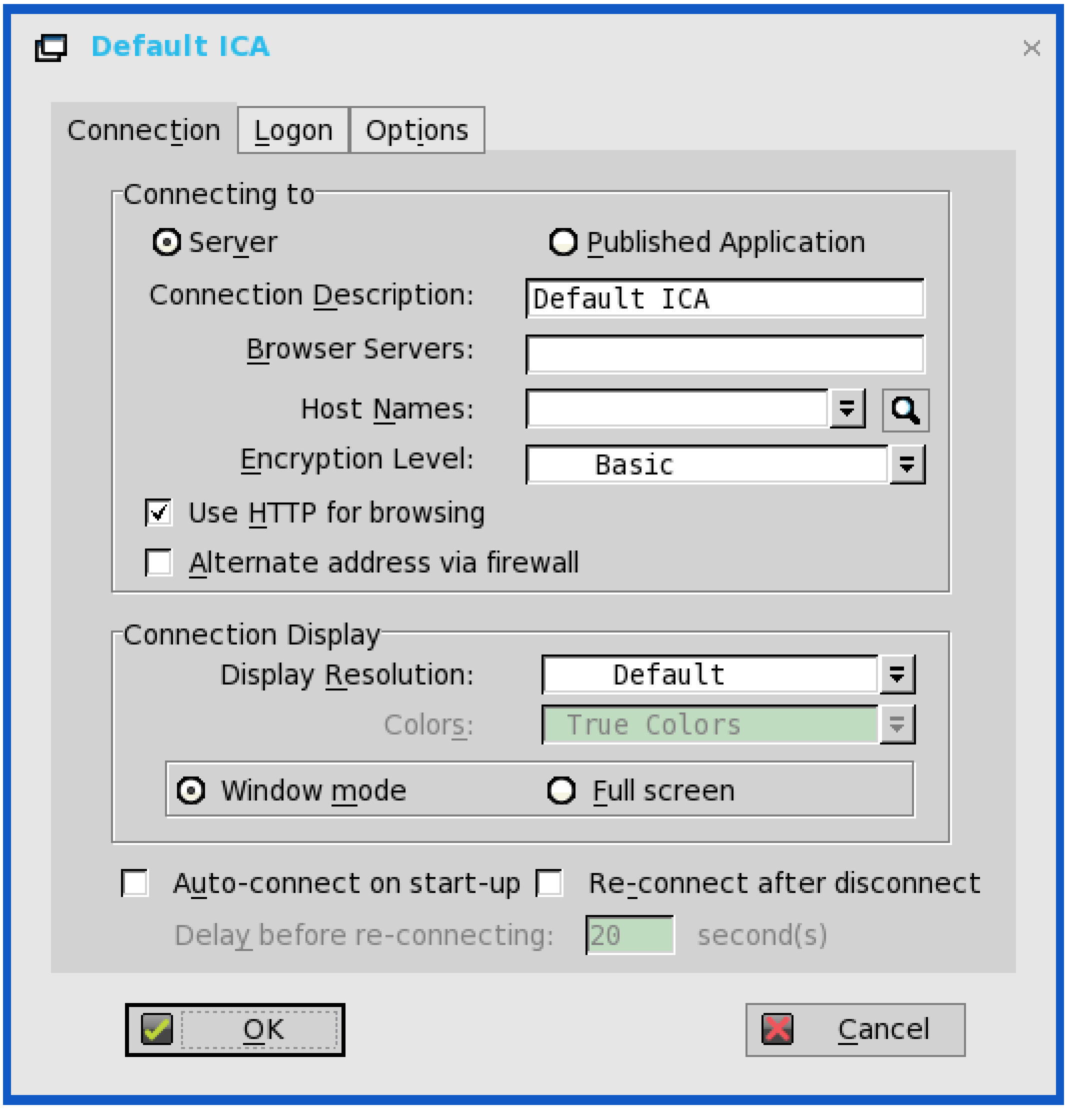
3 Click **ICA** connection protocol, and click **Configure**.

The **Default ICA** dialog box is displayed.

> ⓘ NOTE: **Default ICA is always used for direct connection to a published application and not for StoreFront or PNAgent.**

4 Click the **Connection** tab.

To configure the ICA connections, do the following:



Connecting to

● Server ○ Published Application

Connection Description: Default ICA

Browser Servers:

Host Names:

Encryption Level: Basic

☑ Use HTTP for browsing

☐ Alternate address via firewall

Connection Display

Display Resolution: Default

Colors: True Colors

● Window mode ○ Full screen

☐ Auto-connect on start-up ☐ Re-connect after disconnect

Delay before re-connecting: 20 second(s)

Figure 6. 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 appear 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 contains the master browsers list, or that could refer to another server that contains the list.

The master browsers list is generated automatically by a browsing program on one of the ICA servers (selected by negotiation between servers). It is used to provide the information 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 thin 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 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 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 thin 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 thin client will attempt to connect to the next one on the list.

ⓘ NOTE: **The Host Name 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 will also try to resolve the name without using the default.**

e **Encryption Level**—Allows you to select the security level of communications between the thin 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 thin 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 thin client to use 128-bit encryption. However, transaction information could be exposed to a lower level of security if the thin client encryption is not also set to 128–bits.**

f **Use HTTP for browsing**—When selected, the thin client, by default, uses HTTP when browsing.

g **Alternate address via firewall**—When selected, the thin client uses an alternate IP address returned from the ICA master browser to get through firewalls. Used for the Windows log on when the connection is activated.

h **Display Resolution**—Select the display resolution for this connection.

If you select the **Published Application** option, the Connection Display allows you to select the **Seamless Display Resolution** option.

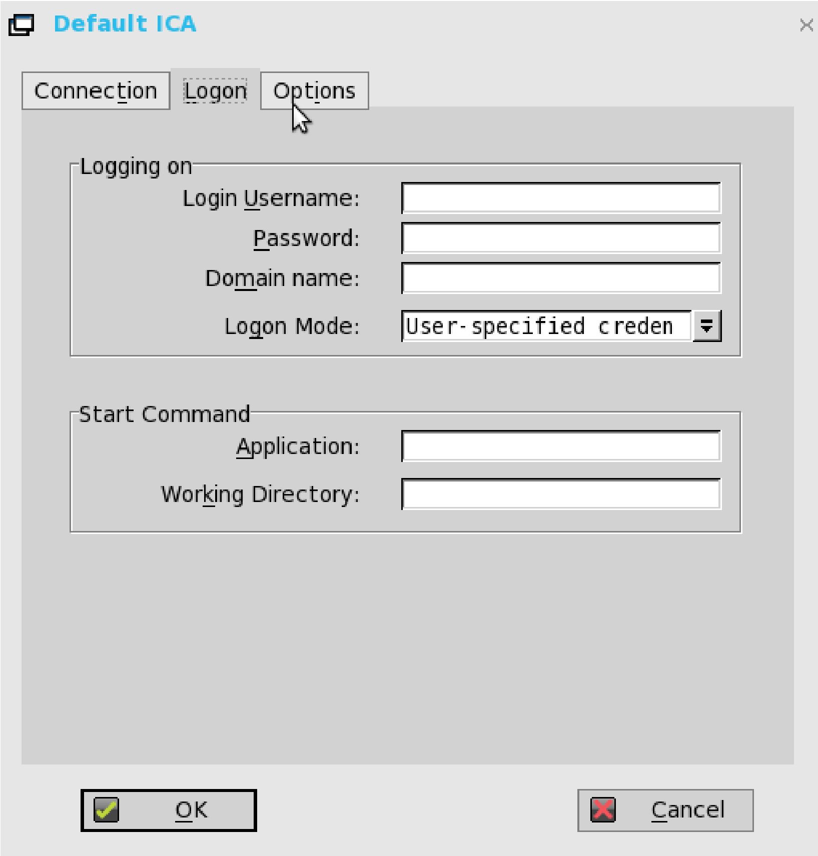
Colors — Select the color depth of the ICA session. If High Colors (16 bits) or True **Colors** is selected and the ICA server does not support this color depth, the thin client renegotiates the color depth to the lower value, for example, 256 Colors [8–bits].

i **Window mode** and **Full screen mode**—Select the initial view of the application and desktop in a windowed screen or full screen.

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

k **Reconnect after disconnect**—When selected, causes the thin client to automatically reconnect to a session after a non operator-initiated disconnect. If selected, the wait interval is that set in the **Delay before reconnecting** box (enter the number of seconds 1–3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds, if there is no INI file description of this connection, or is a Stand-alone user, or simply omitted.

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



Logging on

Login Username:

Password:

Domain name:

Logon Mode: User-specified creden

Start Command

Application:

Working Directory:

Figure 7. Default ICA—Logon

a **Logging on area**—Enter Login User name, Password, Domain name, and Logon Mode.

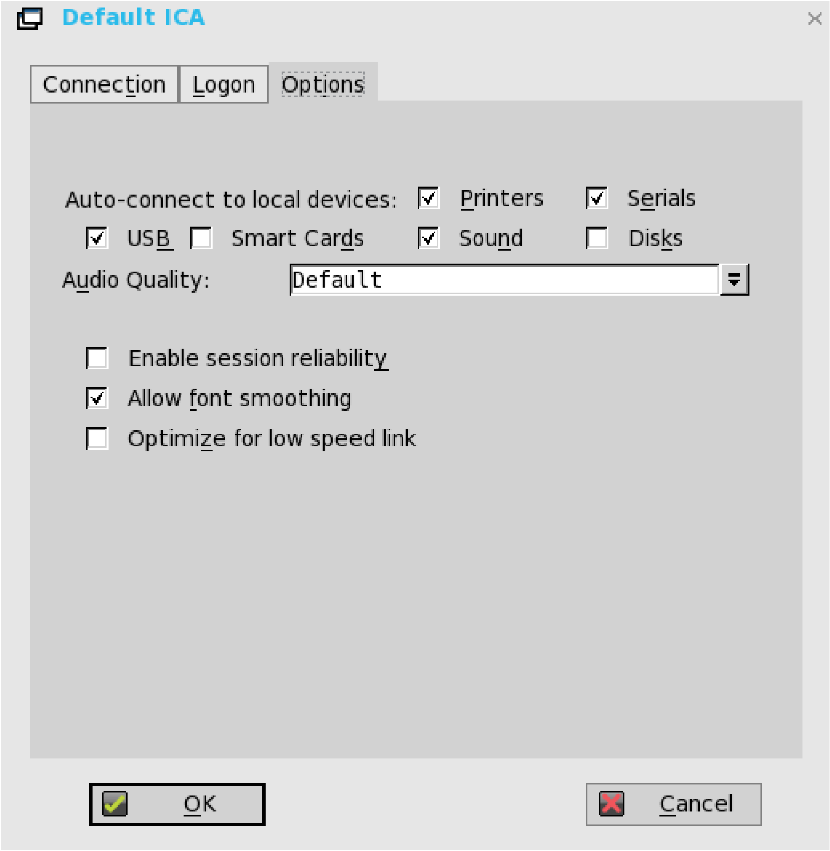
If the Login User name, Password, and Domain name boxes are not populated, you can enter the information manually in the ICA server login screen when the connection is made:

- **Login Username**—Maximum of 31 characters is allowed.
- **Password**—Maximum of 19 characters is allowed.
- **Domain Name** — Maximum of 31 characters is allowed.
- **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.

6 Click **Options** tab and use the following guidelines:



Auto-connect to local devices: ☑ Printers ☑ Serials

☑ USB □ Smart Cards ☑ Sound □ Disks

Audio Quality: Default

□ Enable session reliability

☑ Allow font smoothing

□ Optimize for low speed link

Figure 8. Default 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.

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 dialup.

d **Enable session reliability**—When enabled, session reliability allows a user to momentarily lose connection to the server without having to re-authenticate upon regaining a connection. Instead of a user's connection timing out after X seconds, the session is kept alive on the server and is made available to the client upon regaining connectivity. Session reliability is most relevant for wireless devices.

Support for multi-monitors in Citrix session

ThinOS supports ICA desktop multiple monitors in XenDesktop/XenApp 7.6 and later versions.
Prerequisites:

- Increase the value of **MaxVideoMemoryBytes** REG_DWORD to support one or more 4K resolution monitors. For more information, see Citrix documentation at support.citrix.com.
- Increase the display memory limit to support more color depth and higher resolution. For more information, see Citrix documentation citrix.com.

User scenario:

1 Connect multiple monitors to ThinOS device.

2 In the **Display Setup** dialog box, disable **Mirror Mode**, and configure the display layout.

3 Launch an ICA desktop with full screen.

Table 7. Display details

Platforms	Best Display resolution	Maximum number of system displays	
		Standard or RDS desktop—Windows 10 /2012 R2/ 2016	**HDX 3D Pro desktop—Windows 10 with GRID K1/K2 GPU**
Wyse 5070 Extended thin client	1920 x 1080	6	4
	2560 x 1440	6	4
	3840 x 2160	6	Not supported, due to GRID K1/K2 vGPU profile limitation.
Wyse 5070 thin client—Pentium processor	1920 x 1080	3	3
	2560 x 1440	3	3
	3840 x 2160	3	Not supported, due to GRID K1/K2 vGPU profile limitation.
Wyse 5070 thin client—Celeron processor	1920 x 1080	2	2
	2560 x 1440	2	2
	3840 x 2160	2	Not supported, due to GRID K1/K2 vGPU profile limitation.

Limitations

- For standard or RDS desktop (Windows10/ 2012 R2 /2016) on Wyse 5070 Extended thin client, Dell recommends that you use up to four 4K monitors and remaining monitors with 1920 x 1080 resolution.
- For HDX 3D Pro desktop using vGPU or GPU Passthrough, the supported resolution and number of supported monitors is based on the NVIDIA's GRID support matrix.

ⓘ NOTE: **For more information about the Citrix official multiple monitors support, see Citrix documentation at support.citrix.com.**

ICA Self Service Password Reset

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

Supported Environment

- XenDesktop 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

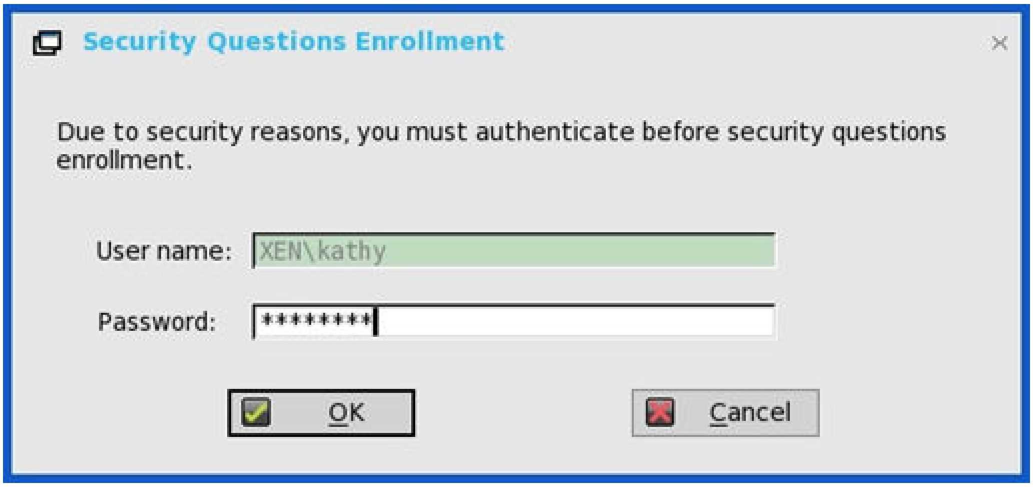
- Supports only storefront server
- The Legacy Account Self-Service (which needs Account Self-Service Server configured in ThinOS Remote Connections) is independent with this storefront version. Storefront version will cover Legacy Account Self-Service.
- The security question enrollment is not supported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



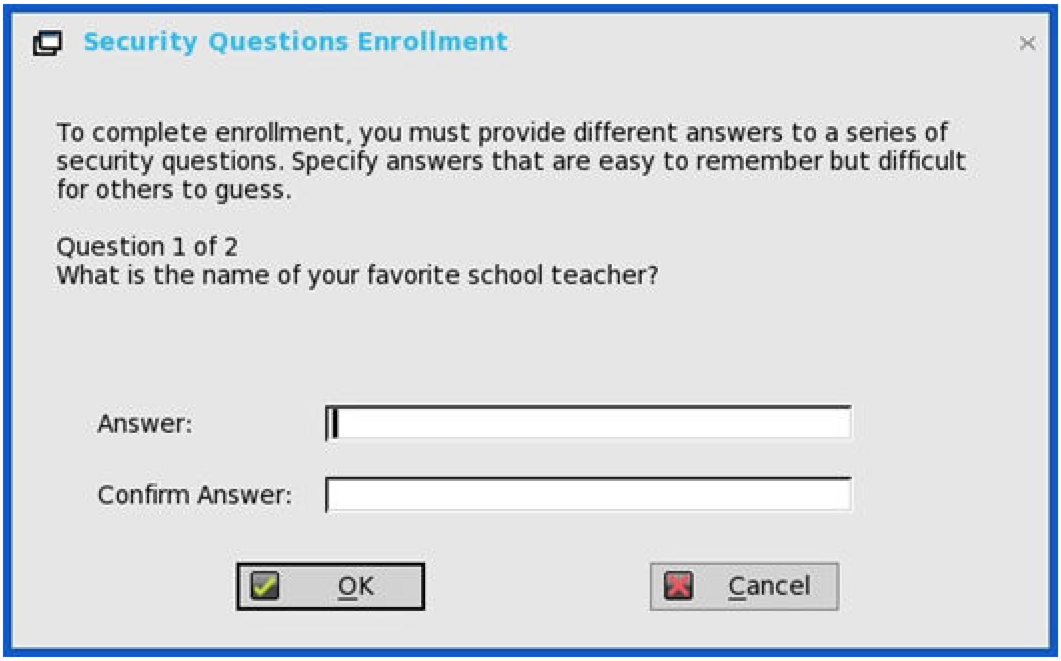
Security Questions Enrollment

Due to security reasons, you must authenticate before security questions enrollment.

User name: XEN\kathy

Password: ********

2 Enter the appropriate answers to the question set.



Security Questions Enrollment

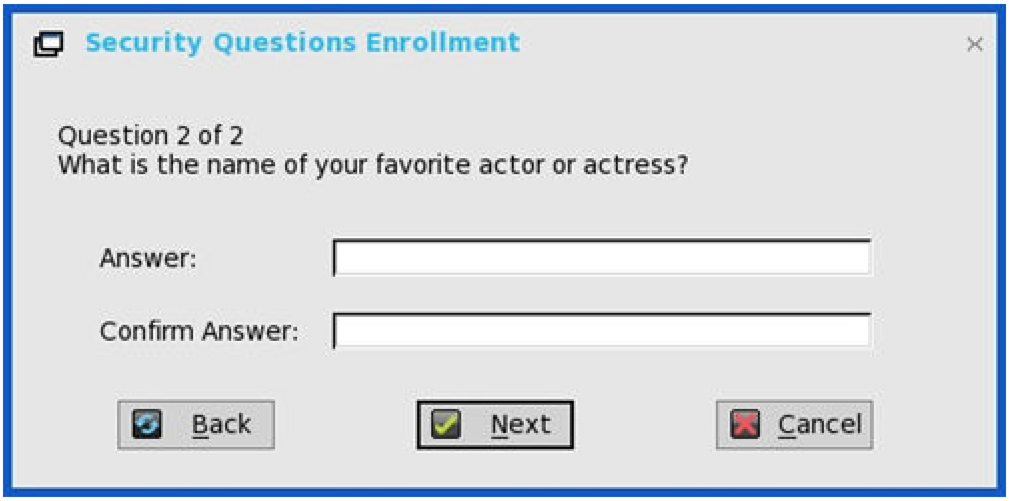
To complete enrollment, you must provide different answers to a series of security questions. Specify answers that are easy to remember but difficult for others to guess.

Question 1 of 2

What is the name of your favorite school teacher?

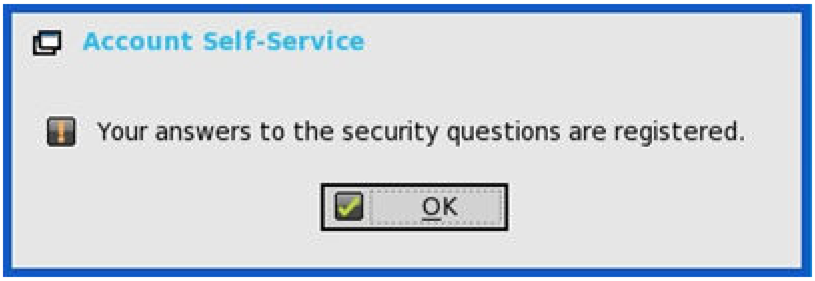
Answer:

Confirm Answer:


Security Questions Enrollment

Question 2 of 2
What is the name of your favorite actor or actress?

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


Account Self-Service

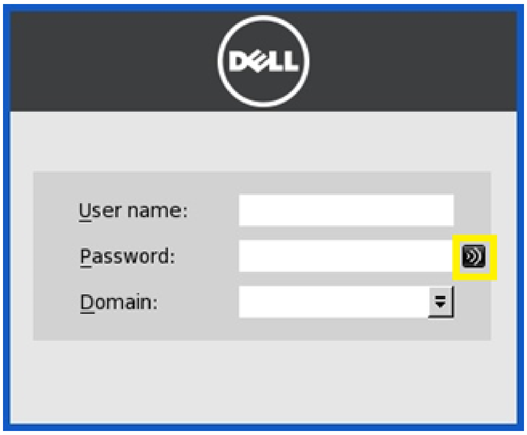
Your answers to the security questions are registered.

Using Account Self-Service

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

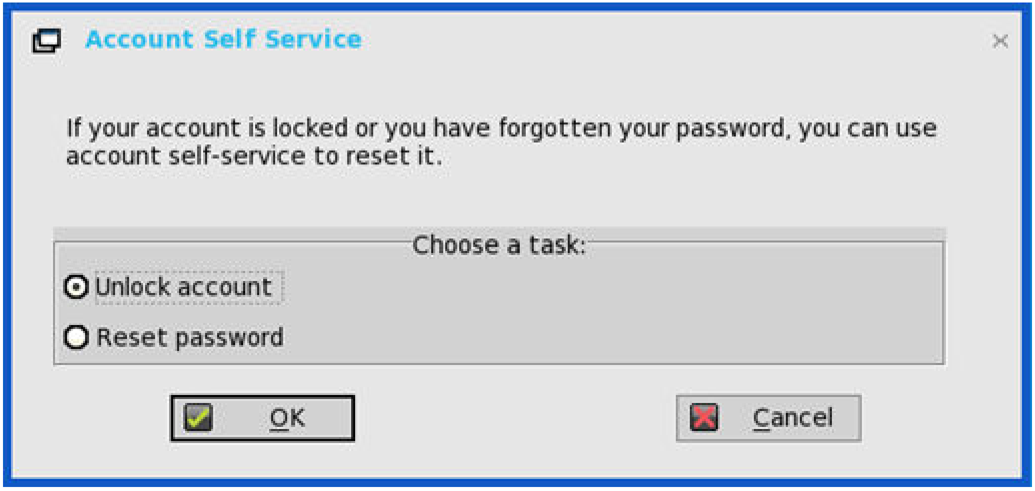
NOTE: **If you enter wrong password more than four times in the Sign-on window, the client automatically enters the unlock account process.**

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



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**.



Account Self Service

If your account is locked or you have forgotten your password, you can use account self-service to reset it.

Choose a task:

● Unlock account

○ Reset password

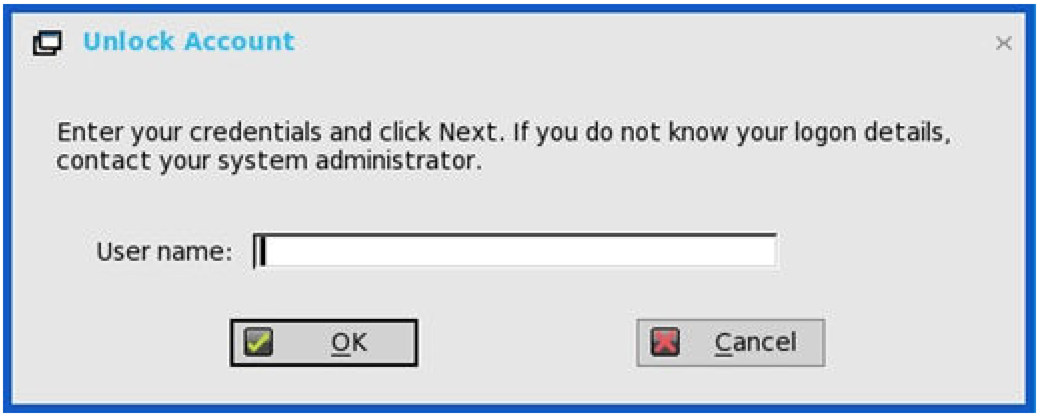
Unlocking account

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

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

2 Enter the user name.

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

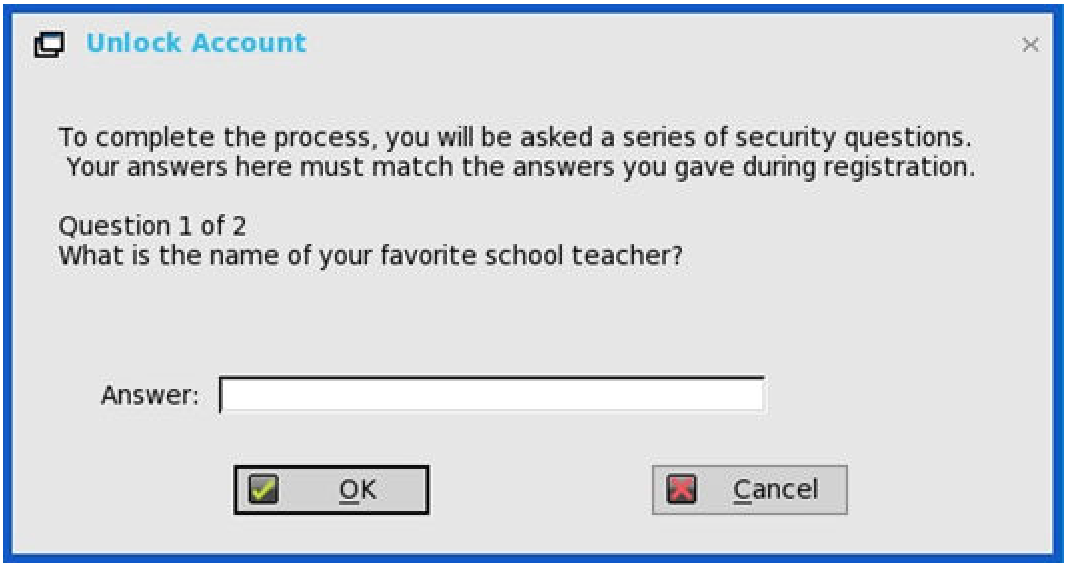


Unlock Account

Enter your credentials and click Next. If you do not know your logon details, contact your system administrator.

User name:

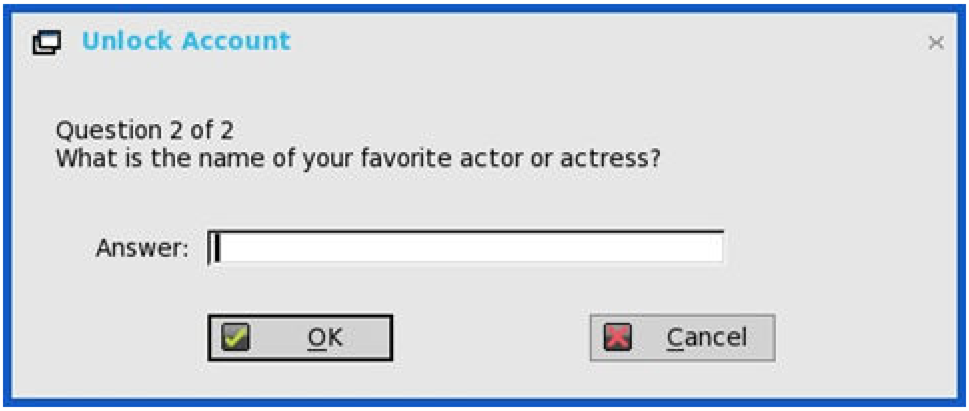
3 Enter the registered answers to the security questions.


Unlock Account

To complete the process, you will be asked a series of security questions. Your answers here must match the answers you gave during registration.

Question 1 of 2
What is the name of your favorite school teacher?

Answer:

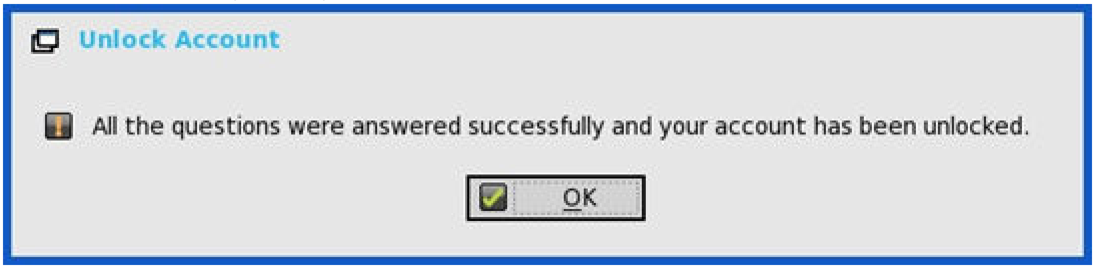

Unlock Account

Question 2 of 2
What is the name of your favorite actor or actress?

Answer:

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

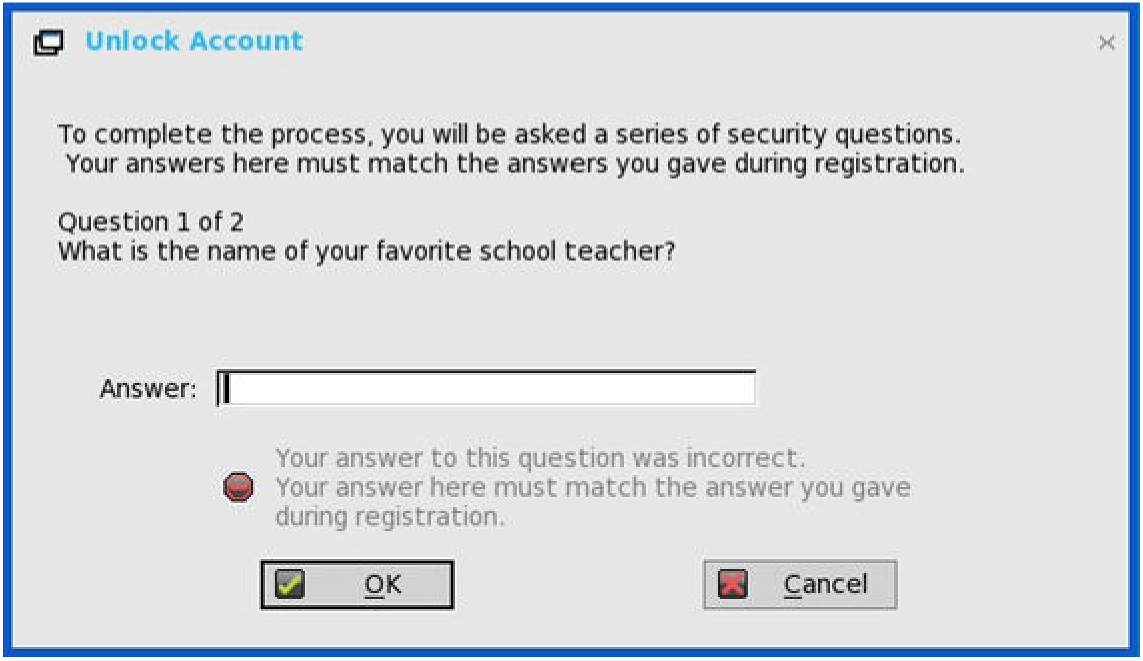
4 Click **OK** to successfully unlock your account.


Unlock Account

All the questions were answered successfully and your account has been unlocked.

ⓘ NOTE:

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



Unlock Account

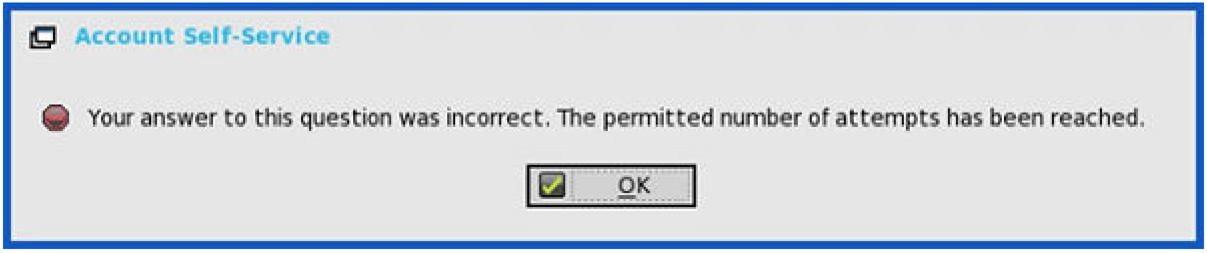
To complete the process, you will be asked a series of security questions.
Your answers here must match the answers you gave during registration.

Question 1 of 2
What is the name of your favorite school teacher?

Answer:

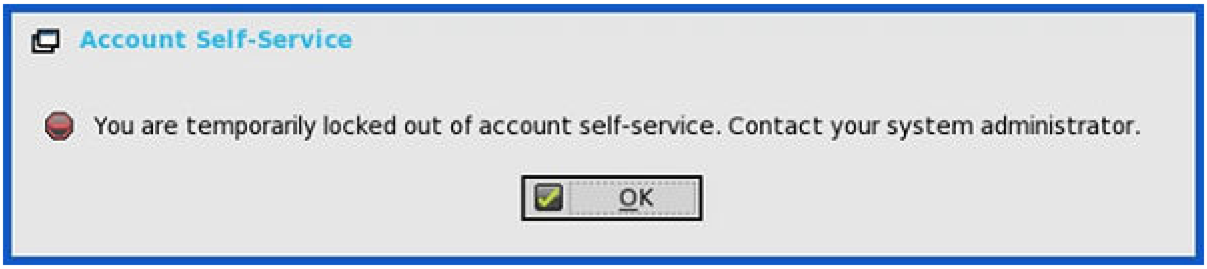
Your answer to this question was incorrect.
Your answer here must match the answer you gave during registration.

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



Account Self-Service

Your answer to this question was incorrect. The permitted number of attempts has been reached.



Account Self-Service

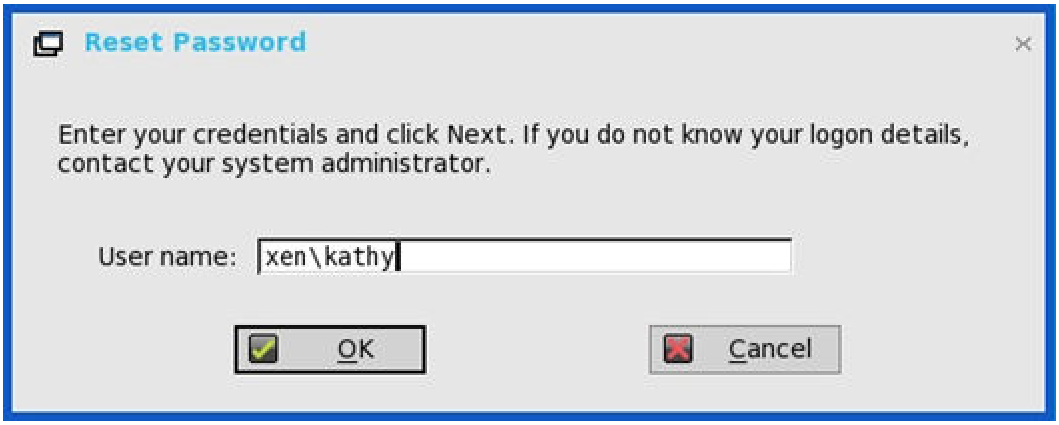
You are temporarily locked out of account self-service. Contact your system administrator.

Resetting password

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

1. Choose a task (Reset password) in **Account Self-Service** window.
2. Enter the user name.

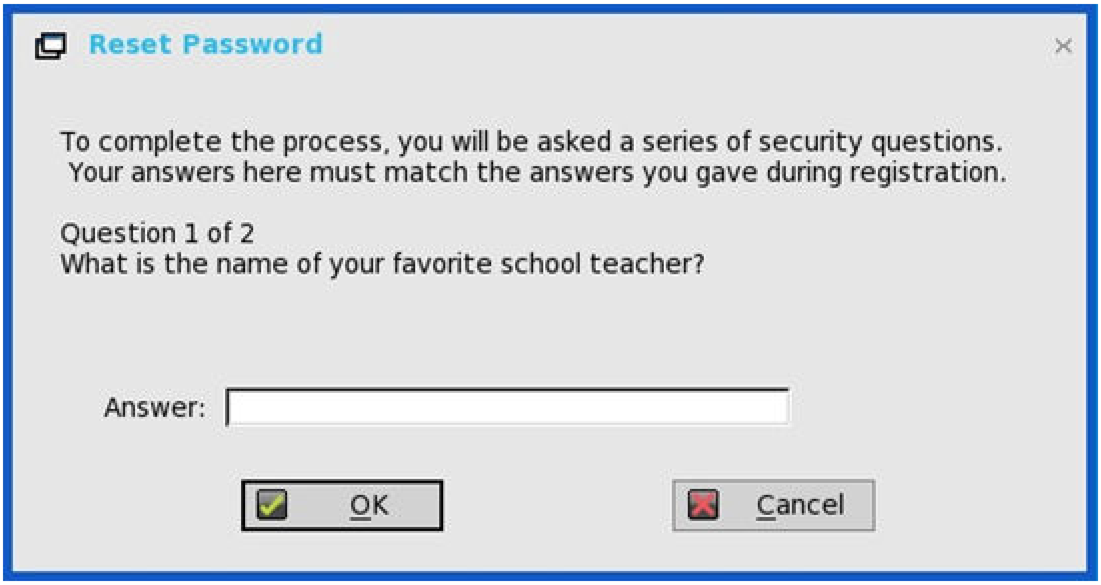
   The **Reset Password** dialog box is displayed.


Reset Password

Enter your credentials and click Next. If you do not know your logon details, contact your system administrator.

User name: xen\kathy

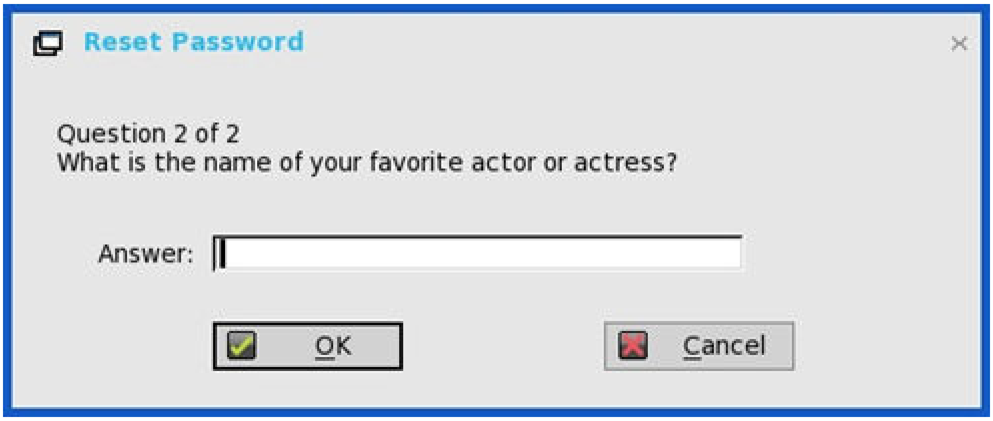
3 Enter the registered answers to the security questions.


Reset Password

To complete the process, you will be asked a series of security questions. Your answers here must match the answers you gave during registration.

Question 1 of 2
What is the name of your favorite school teacher?

Answer:

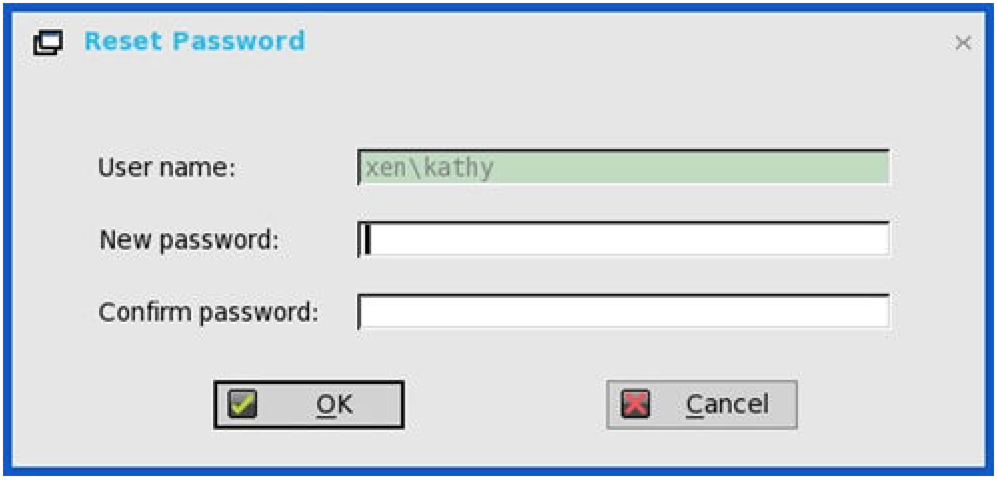

Reset Password

Question 2 of 2
What is the name of your favorite actor or actress?

Answer:

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

4 Enter and confirm the new password.



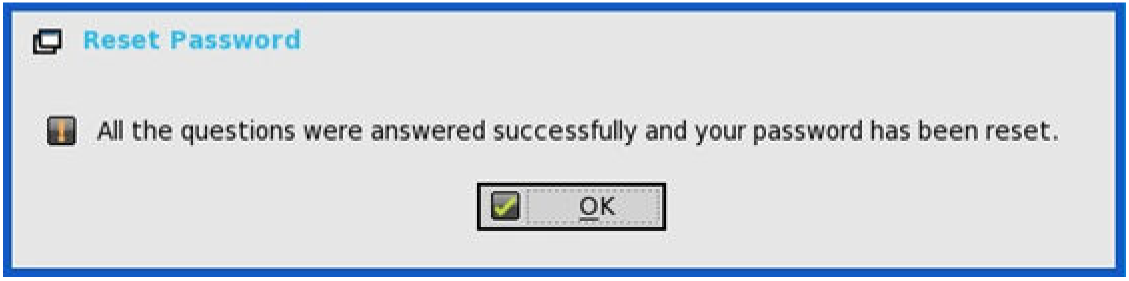
Reset Password

User name: xen\kathy

New password:

Confirm password:

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



Reset Password

All the questions were answered successfully and your password has been reset.

If you provide the wrong answers, you cannot 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 releases, ICA Multimedia URL Redirection was partially supported. From ThinOS 8.4 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.

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.

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

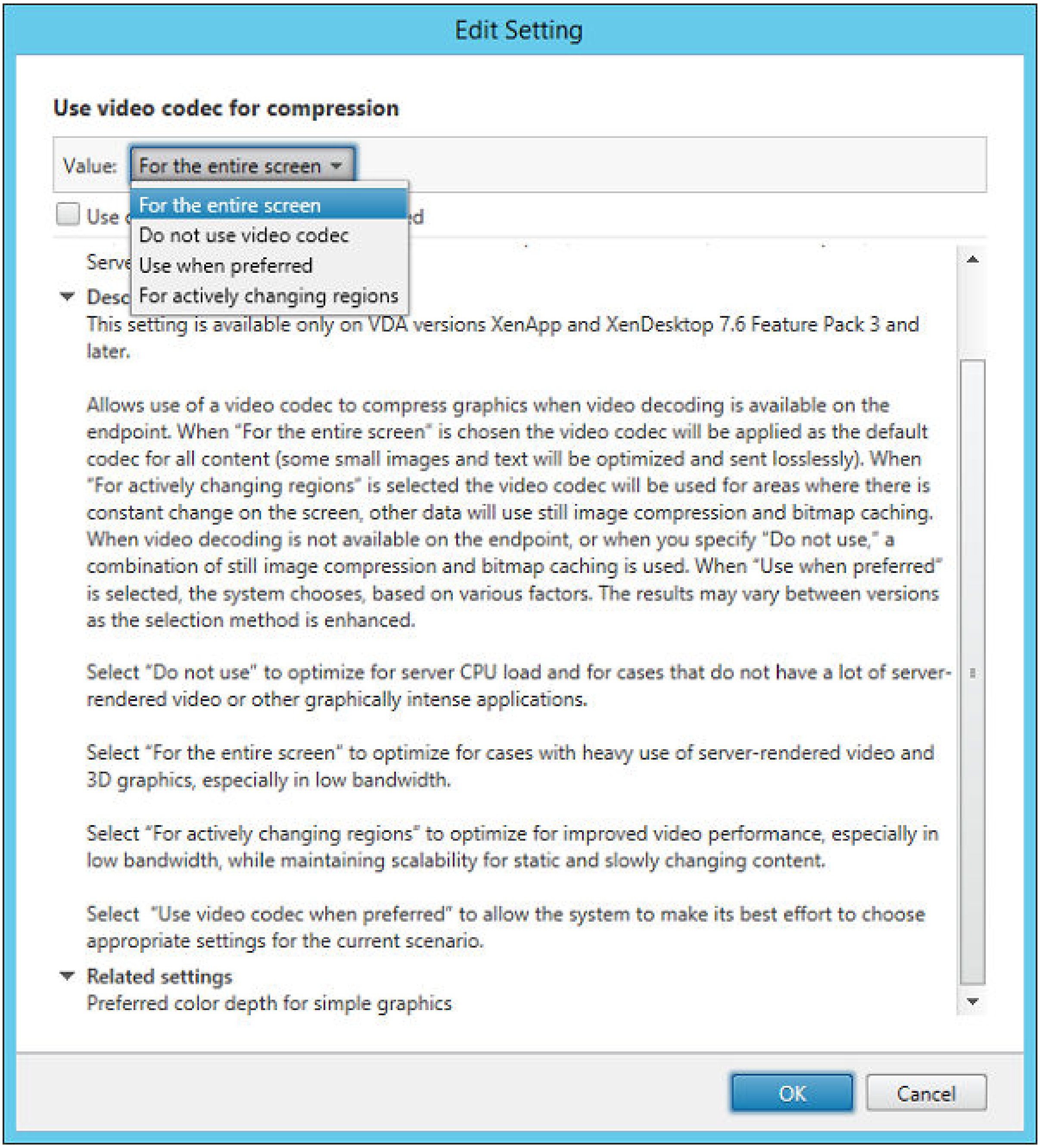
ICA SuperCodec is a H.264 decoder integrated on ThinOS ICA client side. Server encodes the session image into H.264 stream and sends it to client side. Client decodes the H.264 stream by SuperCodec and display the image on screen. This feature improves user experience especially for HDX 3D Pro desktops.

Supported Environment

XenDesktop/XenApp 7.5 or later versions

Prerequisities

In XenApp/XenDesktop version 7.9 and later, the default setting for **Use video codec for compression** is **Use when preferred**. For best performance on ThinOS device, Dell recommends that you set the **Use video codec for compression** policy to **For the entire screen**. Alternatively, you can also set the policy to **Do not use video codec**. This allows ThinOS to use **ThinWire Plus** that saves bandwidth and reduces CPU overhead.



Edit Setting

Use video codec for compression

Value: For the entire screen

This setting is available only on VDA versions XenApp and XenDesktop 7.6 Feature Pack 3 and later.

Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When "For the entire screen" is chosen the video codec will be applied as the default codec for all content (some small images and text will be optimized and sent losslessly). When "For actively changing regions" is selected the video codec will be used for areas where there is constant change on the screen, other data will use still image compression and bitmap caching. When video decoding is not available on the endpoint, or when you specify "Do not use," a combination of still image compression and bitmap caching is used. When "Use when preferred" is selected, the system chooses, based on various factors. The results may vary between versions as the selection method is enhanced.

Select "Do not use" to optimize for server CPU load and for cases that do not have a lot of server-rendered video or other graphically intense applications.

Select "For the entire screen" to optimize for cases with heavy use of server-rendered video and 3D graphics, especially in low bandwidth.

Select "For actively changing regions" to optimize for improved video performance, especially in low bandwidth, while maintaining scalability for static and slowly changing content.

Select "Use video codec when preferred" to allow the system to make its best effort to choose appropriate settings for the current scenario.

Related settings

Preferred color depth for simple graphics

Figure 9. Use video codec for compression setting

- **ThinWire Plus**—Equivalent to **Do not use video codec** option
- **Fullscreen H.264**—Equivalent to **For the entire screen** option
- **Selective H.264**—Equivalent to **For actively changing** regions

Verifying the working status of the ICA connections

- ICA SuperCodec is always enabled without any limitation.
- ThinOS event log displays ICA: SuperCodec enabled.

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

If you set the **Use video codec for compression** policy to **Do not use video codec**, ICA SuperCodec is disabled, and ThinOS does not print any log.

Anonymous logon

Anonymous logon feature enables the users to log into 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.

NOTE: Anonymous logon is not supported with legacy mode of StoreFront server.

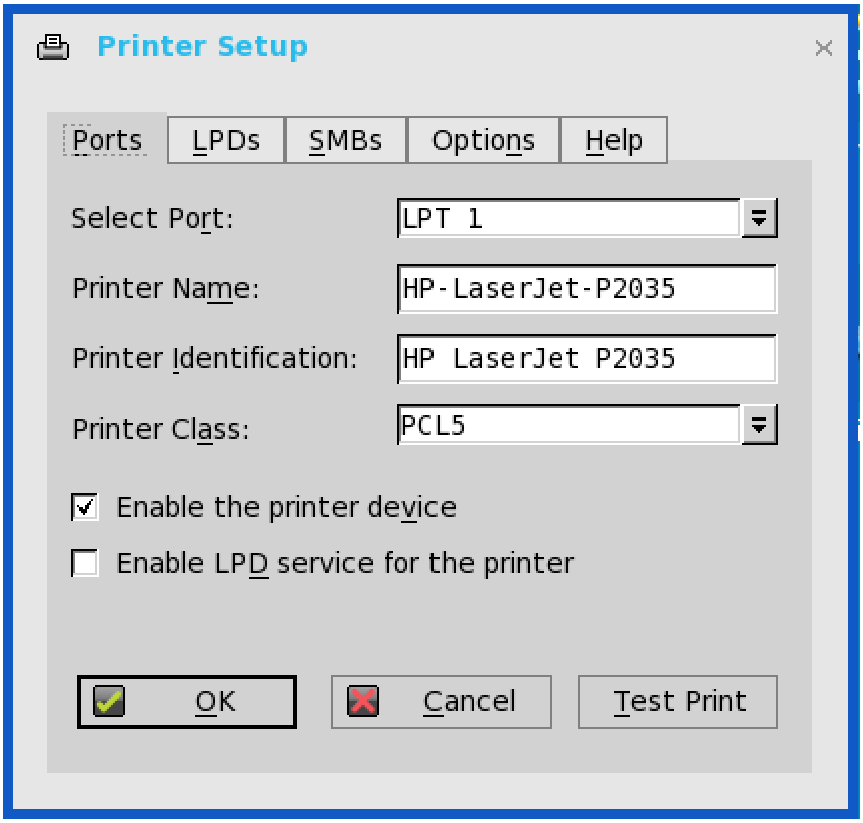
Configuring the Citrix UPD printer

Use of Citrix Universal Printer Driver (Citrix UPD) 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 UPD is the base of Citrix Universal Printer. It is an auto-created printer object that uses the Citrix UPD and is not tied to any specific printer defined on the client.
To configure the Citrix UPD usage on ThinOS:

1 Connect a printer to ThinOS client.

2 From the desktop menu, click **System Setup**, and then click **Printer**.

The **Printer Setup** dialog box is displayed.



Printer Setup

Select Port: LPT 1

Printer Name: HP-LaserJet-P2035

Printer Identification: HP LaserJet P2035

Printer Class: PCL5

☑ Enable the printer device

□ Enable LPD service for the printer

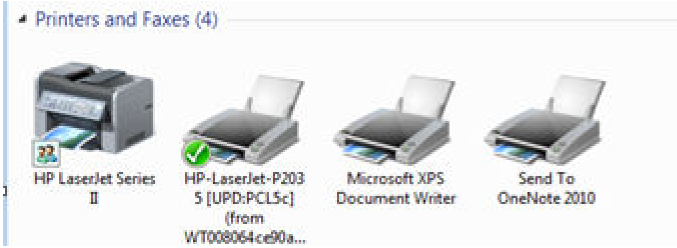
3 Enter the name of the printer in the **Printer Name** box.

4 Enter any string of the Printer identification in the **Printer Identification** box.

5 Select the type of the printer class from the drop-down list, select the check box to enable the **printer device** and then click **OK**.

6 Start a XenDesktop or XenApp application connection.

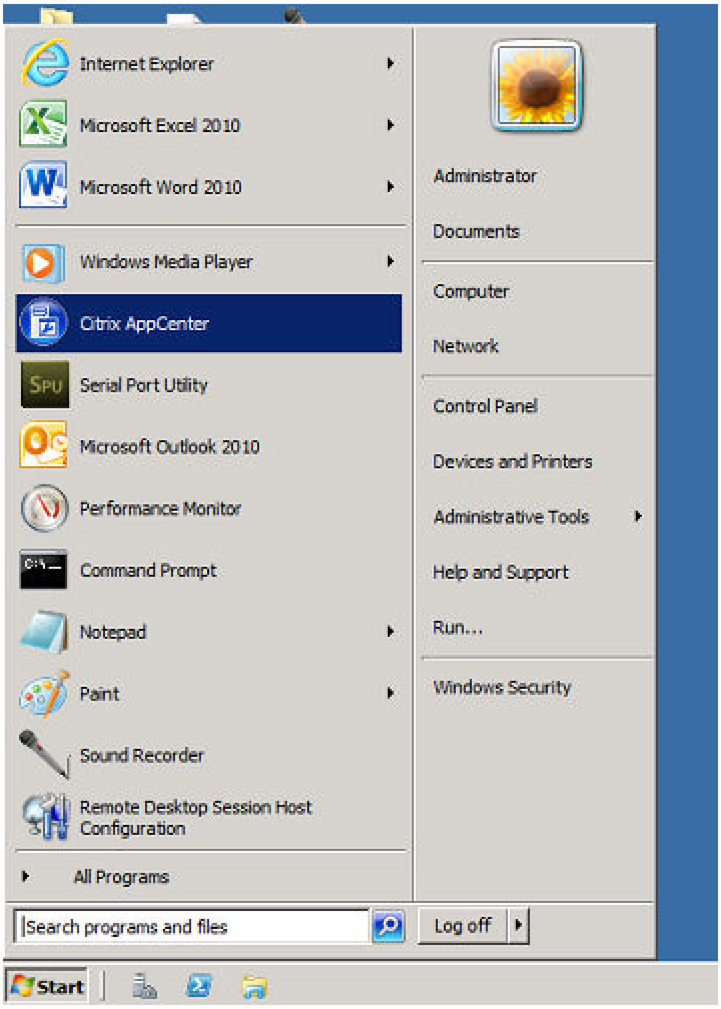
7 Open the Devices and Printers in the desktop or application, notice the printer is mapped as UPD printer by default. You can use the HP-LaserJet-P2035 [UPD:PCL5c] to perform the print job.


Printers and Faxes (4)
HP LaserJet Series II
HP-LaserJet-P2035 [UPD:PCL5c] (from WT008064ce90a...
Microsoft XPS Document Writer
Send To OneNote 2010

Citrix UPD configuration on server

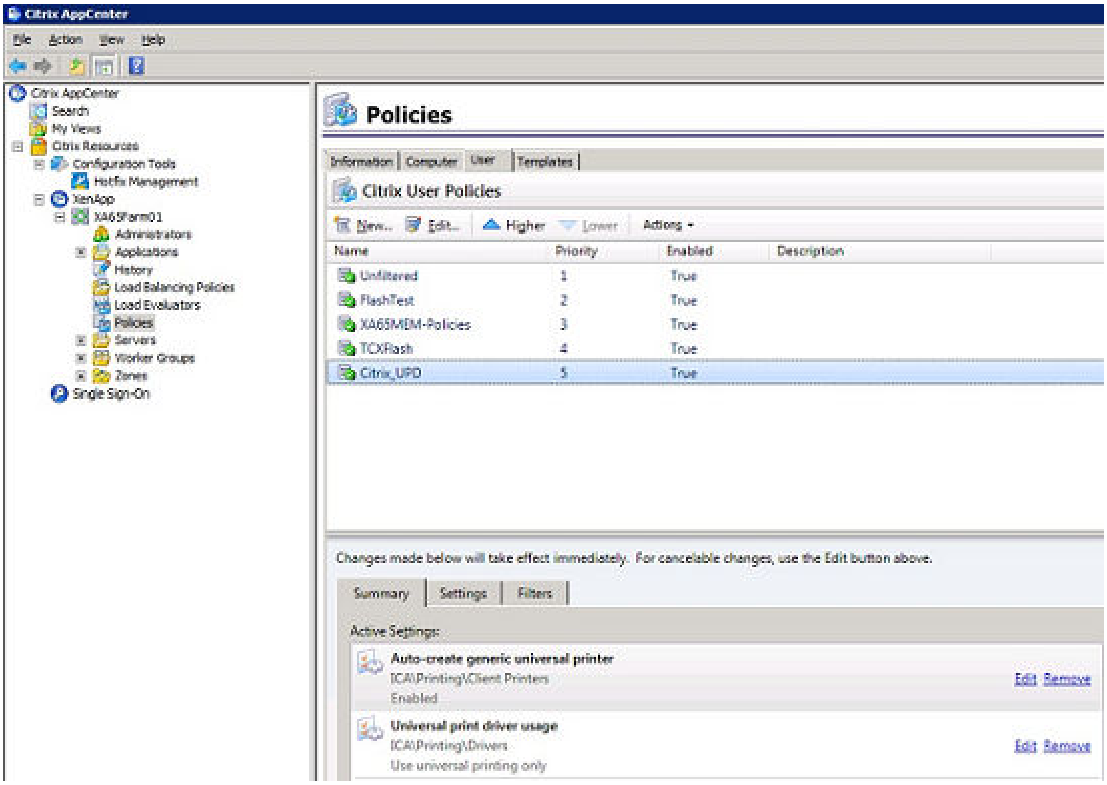
a To enable the printer policy, use the following guidelines:

1. To enable the printer policy in XenApp 6.5– Go to the DDC Server, click **Start** > **Citrix AppCenter** .



2. Click **Citrix Resources** > **XenApp** > **Policies** > **User** > **Settings** > **Printing** > **Client Printers** and enable the **Auto-create generic universal printer**.

3. Click **Printing** > **Drivers** and set the **Universal print driver usage** to **Use universal printing only** from the drop-down menu available.



Name	Priority	Enabled	Description
Unfiltered	1	True	
FlashTest	2	True	
XA65MDM-Policies	3	True	
TCXFlash	4	True	
Citrix_UPD	5	True	

Changes made below will take effect immediately. For cancelable changes, use the Edit button above.

Active Settings:

Auto-create generic universal printer
ICA\Printing\Client Printers
Enabled

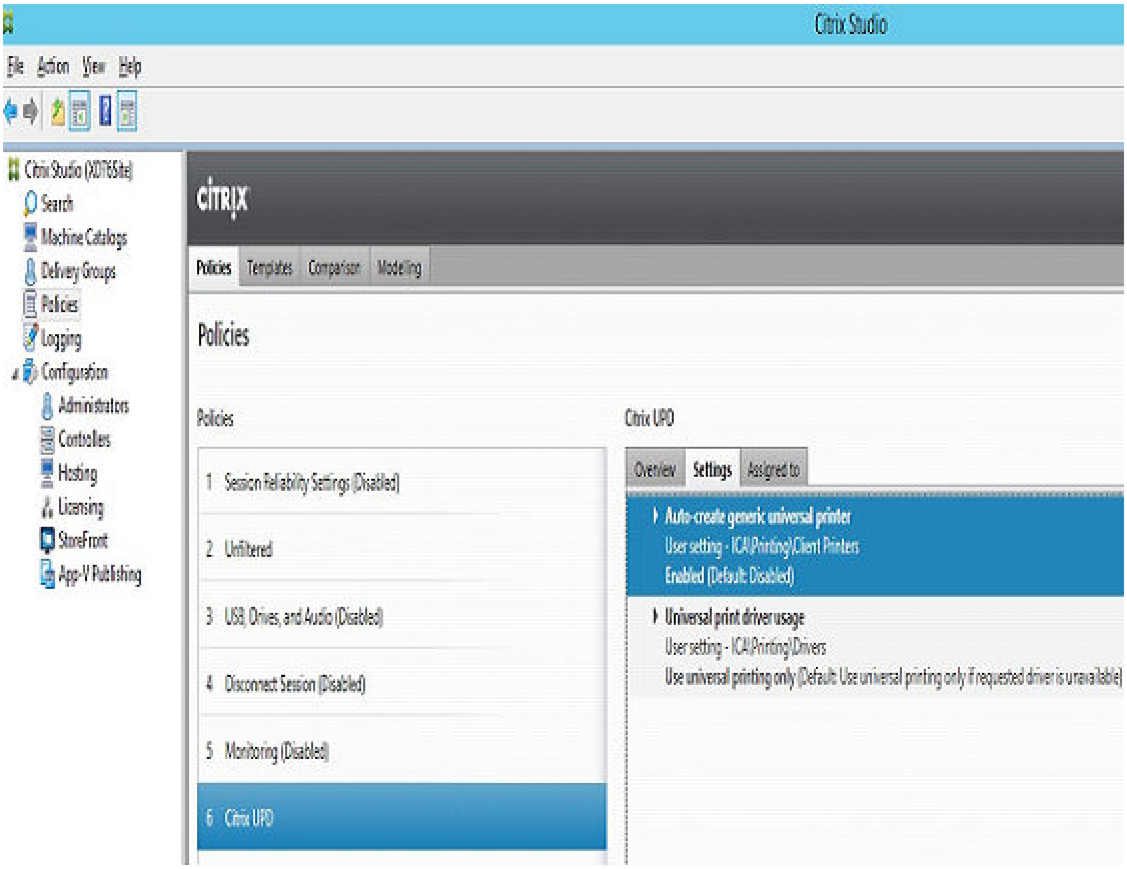
Universal print driver usage
ICA\Printing\Drivers
Use universal printing only

4 To enable the printer policy in XenApp/XenDesktop 7.5 and later versions, do the following:

a Go to the Citrix DDC Server,

1 Click **Citrix studio** > **policies** and add a policy. Enable the **Auto-create generic universal printer** option.

2 Set the **Universal print driver usage** to **Use universal printing only** from the drop-down menu.



1 Session Reliability Settings (Disabled)
2 Unfiltered
3 USB, Drives, and Audio (Disabled)
4 Disconnect Session (Disabled)
5 Monitoring (Disabled)
6 Citrix UPD

Auto-create generic universal printer
User setting - ICA\Printing\Client Printers
Enabled (Default: Disabled)

Universal print driver usage
User setting - ICA\Printing\Drivers
Use universal printing only (Default: Use universal printing only if requested driver is unavailable)

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 does not support EMF and XPS.

ⓘ **NOTE: The supported drivers in the following table are one of the supported drivers for Citrix UPD used in ThinOS. One of the recommended driver is provided here as an example.**

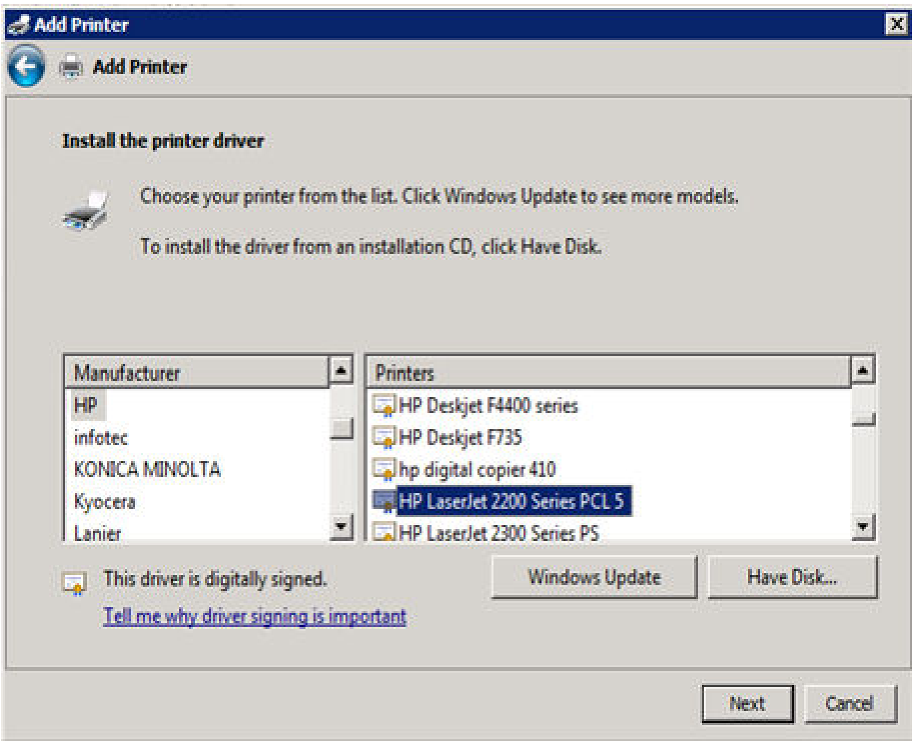
The supported drivers are listed in the following table:

Table 8. Supported drivers

Printer class	Printer driver
PS	HP Color LaserJet 2800 Series PS
PCL5	HP LaserJet 2200 Series PCL 5
PCL4	HP LaserJet Series II

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** > **Click Printer server properties** > **Driver tab** and then add **HP LaserJet 2200 Series PCL 5 driver**.



Add Printer

Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

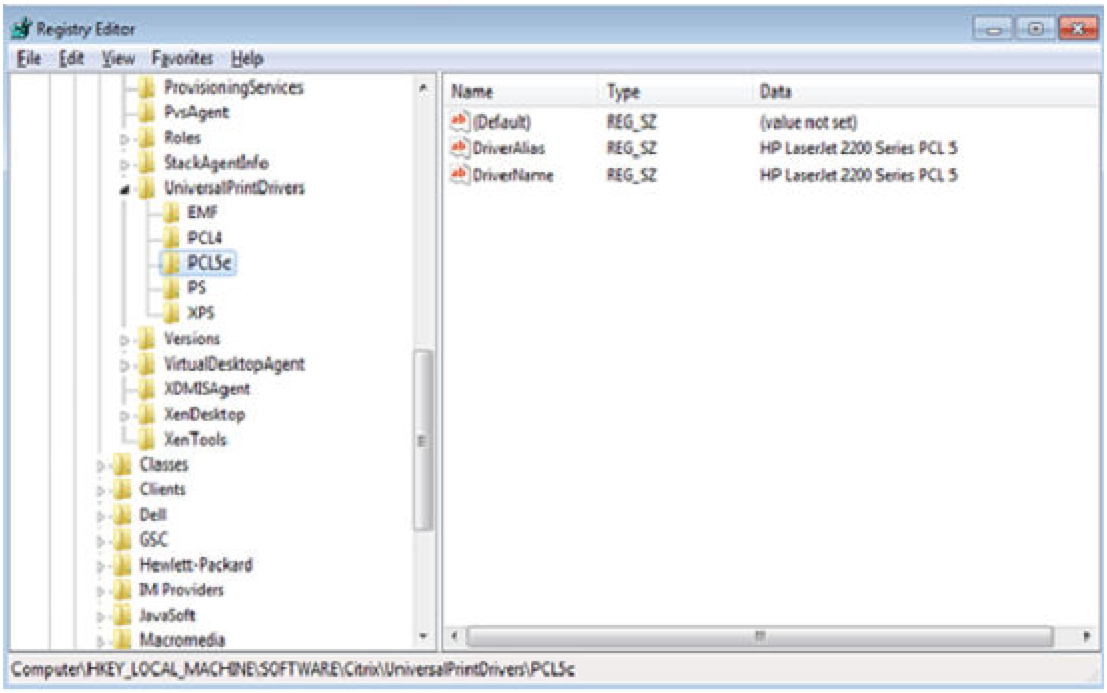
To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
HP	HP Deskjet F4400 series
infotec	HP Deskjet F735
KONICA MINOLTA	hp digital copier 410
Kyocera	HP LaserJet 2200 Series PCL 5
Lanier	HP LaserJet 2300 Series PS

This driver is digitally signed.

Tell me why driver signing is important

2 Under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\PCL5c\, change DriverAlias and DriverName **HP LaserJet 2200 Series PCL 5**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
DriverAlias	REG_SZ	HP LaserJet 2200 Series PCL 5
DriverName	REG_SZ	HP LaserJet 2200 Series PCL 5

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UniversalPrintDrivers\PCL5c

Flash Redirection

The Flash Redirection solution is to off-load flash content to the ThinOS client, and locally render and decode the flash playback. The off-loading 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.

Supported Environment— Supports only Citrix Connections with XenApp 6.5 and later versions and XenDesktop 7.0 and later versions.

Required packages

User must install the `FR.i386.pkg` package for the feature to work.

Installation of packages

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

   You can view the installed packages in the **Packages** tab in the **System Tools** dialog box.
4. **Server configuration for Flash redirection**
   a. To ignore the differences in flash player versions, user must add the `FlashPlayerVersionComparisonMask` and `ClientFlashPlayerVersionMinimum` registry key on the desktop.

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

      For more information, see docs.citrix.com/en-us/xenapp-and-xendesktop/7-9/hdx/flash-redirection.html.

      From XenDesktop 7.9, you must add more entries in registry for HDX FR to work. For information about these additional entries, refer to Citrix Technical documents.
5. **Client configuration for Flash redirection**

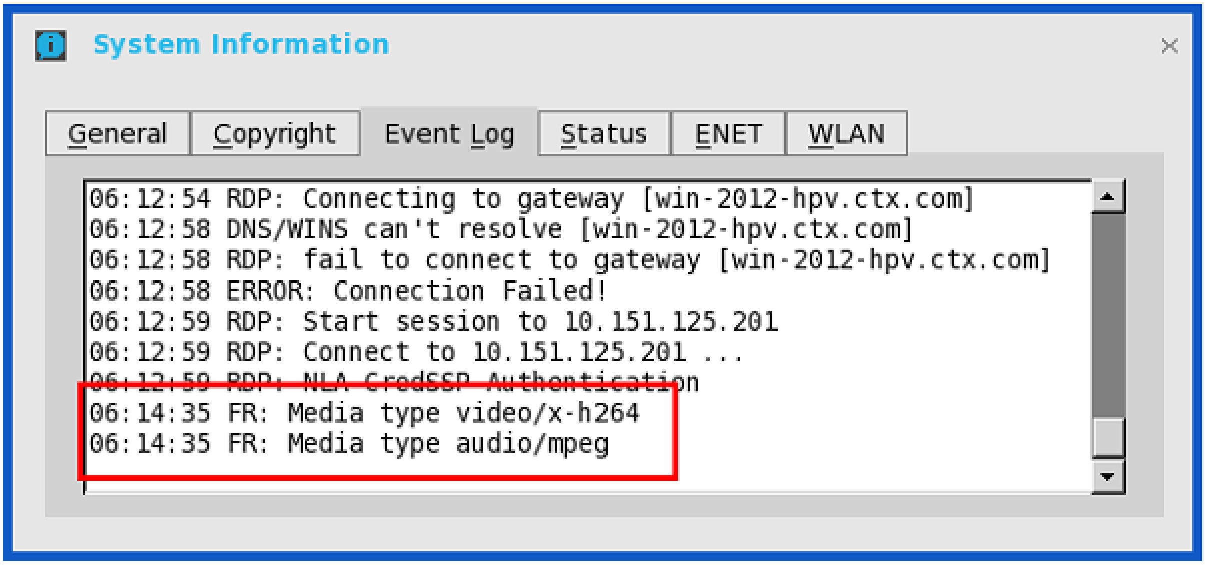
   By default, no client configuration is required. New INI parameters are added to support HDX FR Client configurations, for example, to fetch the server side content. The newly added INI parameters are:

```
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 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 event logs for HDX FR in the System Information dialog box.

   1. FR: Media type video/x-264
   2. FR: Media type audio/mpeg



```
06:12:54 RDP: Connecting to gateway [win-2012-hpv.ctx.com]
06:12:58 DNS/WINS can't resolve [win-2012-hpv.ctx.com]
06:12:58 RDP: fail to connect to gateway [win-2012-hpv.ctx.com]
06:12:58 ERROR: Connection Failed!
06:12:59 RDP: Start session to 10.151.125.201
06:12:59 RDP: Connect to 10.151.125.201 ...
06:12:59 RDP: NLA CredSSP Authentication
06:14:35 FR: Media type video/x-h264
06:14:35 FR: Media type audio/mpeg
```

For information about basic operations on Citrix HDX flash redirection and policies configurations, see Citrix documentation.

Known Issues

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

b After flash video is loaded it will stay in initial size; for example, resizing browser will not resize the video content.

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

d 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.

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

f 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.

Configuring VMware

VMware virtualization allows you to run multiple virtual machines on a single physical machine. VMware Horizon Client is a locally installed software application that communicates between View Connection Server and thin client operating system. It provides access to centrally hosted virtual desktops from your thin clients.

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

Configuring the VMware broker connection

To configure the VMware broker setup:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, from the drop-down list, select **VMware view**, and do the following:
   - **Broker Server**—Enter the IP address/Hostname/FQDN of the Broker Server.
   - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semicolon, and is case-sensitive.
   - **Security mode**—Select the preferred security mode from the following options:
     - **Warning**—Warn Security requires FQDN address with self-signed certificate, or without any certificate, but corresponding warning message is displayed for user to continue.
     - **Full**—Full Security requires FQDN address with domain certificate.
     - **Low**—Security allows FQDN/IP address with/without certificate.
     - **Default**—Follows global security mode settings.
   - **Connection Protocol**—From the drop-down list, select the type of protocol connection. By default, the option is set to **Server Default**.

     > NOTE: **The PCoIP only connection protocol is applicable only to PCoIP clients. If you do not install Horizon package, then the Blast only protocol option is not available for selection. PCoIP protocol is required for PCoIP session. Horizon package is required for Blast session.**

     The available options are:

     - **Server default**—Select this protocol connection to display the desktop with default protocol as configured in the VMware View Admin console, for each pool in the broker. If a desktop pool is configured with default protocol as **RDP** in the View Admin console, then only the RDP connection of the desktop is displayed in ThinOS after users sign in to the device.

  - **All Supported**—Select this protocol connection to display the desktop in all the available connections, when a desktop pool is configured to allow users to select protocol as **yes**. If a desktop is configured with default protocol as **PCoIP** and allow user to select protocol as **no**, then ThinOS only displays the desktop in the PCoIP connection.
  - **RDP only**—Select this protocol connection to display only the desktop in RDP connection. If a desktop pool is configured with default protocol as **PCoIP** in the View Admin console, and allow user to select protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.
  - **PCoIP only**—This option is available only for PCoIP enabled clients. Select this protocol connection to display only the desktop in the PCoIP connection, for each pool in the broker. If a desktop pool is configured with default protocol as **RDP** in the View Admin console, and allow user to select protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.
  - **Blast only**—VMware Blast display protocol can be used for remote applications and for remote desktops that use virtual machines or shared-session desktops on an RDS host. Select this protocol connection to display the desktop with the Blast protocol.
- **Log in anonymously using Unauthenticated Access**—Select this check box to anonymously log in to the VMware session with application remoting.

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

Using VMware Horizon View broker and desktop

VMware Horizon View Broker timeout—The VMware Horizon View Broker timeout does not force the user to sign out from the broker anymore when the secure tunnel is enabled.

In earlier version of ThinOS, when the broker times out, the user session is disconnected and the user is logged out from the broker. From ThinOS 8.2 release, ThinOS disconnects the user session from the broker, but does not force user logout. This is because the user has local connections other than the broker desktop, and these connections are active when the broker timeout is reached.

PCoIP session NUM/CAP keyboard status synchronizes with session instead of thin client—This is applicable for session startup only. The PCoIP session keyboard NUM/ CAP status synchronizes from remote session to client, whereas RDP/ ICA synchronizes status from local to remote session.

For example:

1. Set keyboard `NUM=off` in current PCoIP session.
2. Disconnect the session.
3. Set client keyboard `NUM=on`.
4. Reconnect to the PCoIP session.
5. The keyboard NUM status in both session and client is updated to `NUM=off`.

RDS desktop through PCoIP/Blast—You can view and connect to the Remote Desktop Service (RDS) desktop through the PCoIP/Blast protocol in the broker using PCoIP/Blast enabled the ThinOS clients. In VMware Horizon View 6.0 and later versions, the RDS desktop has RDP, PCoIP or Blast connections based on server configurations.

ⓘ NOTE: **The Horizon application is supported on both PCoIP and Blast. RDP is not supported.**

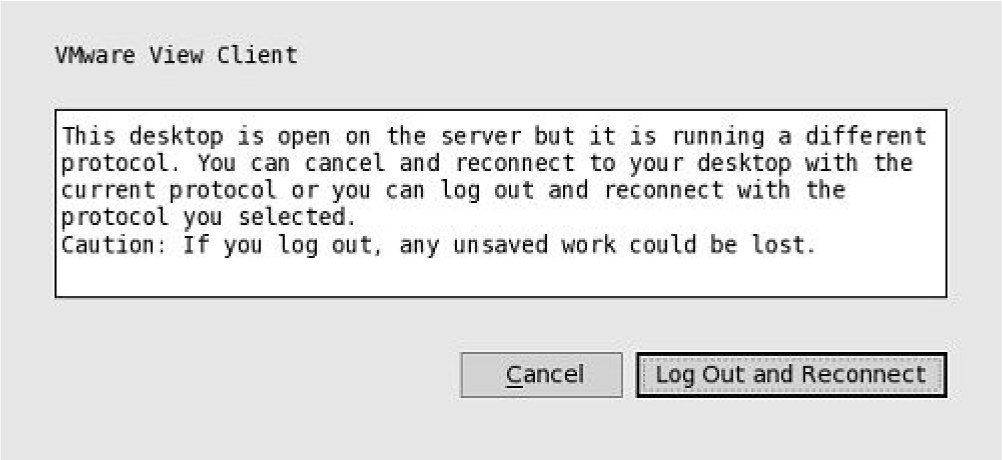
The **RDS desktop protocol switch message** dialog box is provided in this release. A typical user scenario is as follows:

1. Connect to the RDS desktop through protocol. For example, RDP.
2. Disconnect from the desktop.
3. Connect to the same RDS desktop through another protocol. For example, PCoIP.

   The message dialog box is displayed, allowing you with an option to continue.

   The options available are:

   - **Cancel**—You can end the PCoIP connection, and connect to the desktop in RDP again.
   - **Log Out and Reconnect**—You can connect to the desktop through PCoIP, and the earlier session in RDP is logged out.



VMware View Client

This desktop is open on the server but it is running a different protocol. You can cancel and reconnect to your desktop with the current protocol or you can log out and reconnect with the protocol you selected.
Caution: If you log out, any unsaved work could be lost.

USB redirection RDS desktop through PCoIP/Blast—This feature is supported.

Using unauthenticated access—You can anonymously log in to the VMware session with application remoting.

To use the unauthenticated option, do the following:

1 On your AD server, create two anonymous users, for example, anonymous1 and anonymous2.

2 Log in to your View Admin web portal.

3 Navigate to **Users and Groups** > **Unauthenticated Access**, and add the two new anonymous users to the View Connection Manager.

4 Navigate to **View Configurations** > **Select Servers** > **Connection Servers**, and select your connection server.

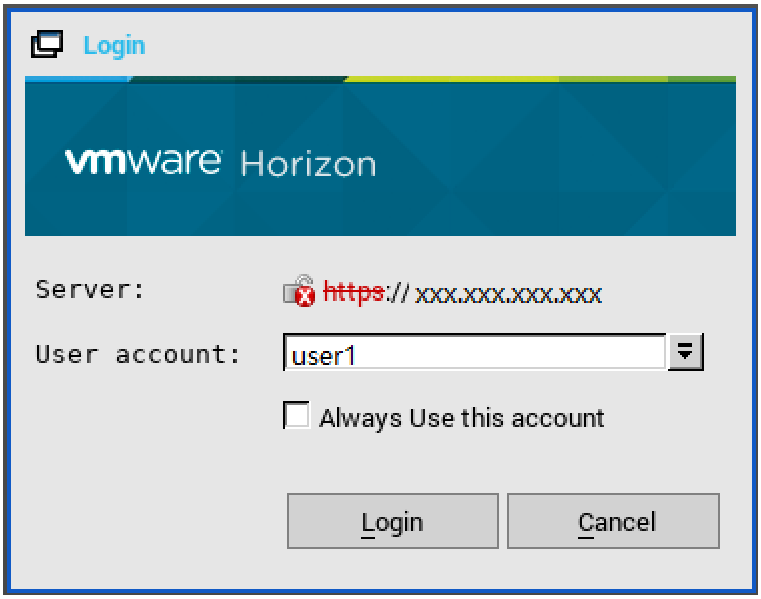
5 Click **Edit** > **Authentication** tab, and select the **Enabled for unauthenticated access** check box. Do not select any users for the default unauthenticated user.

6 Go to **Application Pools**, add a few applications that you have installed on the Virtual Machine, and entitle the applications to anonymous1 and anonymous2 user.

7 On the ThinOS broker setup dialog box for VMware View, select the **Log in anonymously using Unauthenticated Access** check box.

8 Restart your thin client.

The following dialog box is displayed:



Login

Server: ~~https~~:// xxx.xxx.xxx.xxx

User account: user1

□ Always Use this account

9 Select the **Always use this account** check box to use the login account that you have specified. You cannot change this login account for other users.

Hide Server URL—The server URL can be hidden in the Horizon View broker UI. You can configure this setting using any of the following methods:

- **Using View Connection Server web portal**
  a Log into your View Connection Server web portal.
  b Navigate to **View Configuration** > **Global Settings** > **Edit**, select the **Hide server information in client user interface** check box, and clear the **Hide domain list in client user interface** check box.
  c Click **OK**.
  d Log in to the VMware Horizon broker.
  The server URL is hidden, and the domain list is displayed.
- **Using INI parameter**
  Use the INI parameter, ConnectionBroker=vmware DisableShowServer=yes.

Hide Domain List—The domain list can be hidden in the Horizon View Broker logon UI. To configure this setting, do the following:

1. Log in to your View Connection Server web portal.
2. Navigate to **View Configuration** > **Global Settings** > **Edit**, select the **Hide domain list in client user interface** check box, and clear the **Hide server information in client user interface** check box.
3. Click **OK**.
4. Log in to the VMware Horizon broker.
   The domain list is hidden, and the server URL is displayed.

Supporting VMware Real Time Audio-Video

Use the Real-Time Audio-Video feature to run Skype and other online conference applications on the remote desktop. Using this feature, both audio and video devices that are connected to your thin client are available to use for VoIP in remote desktop.

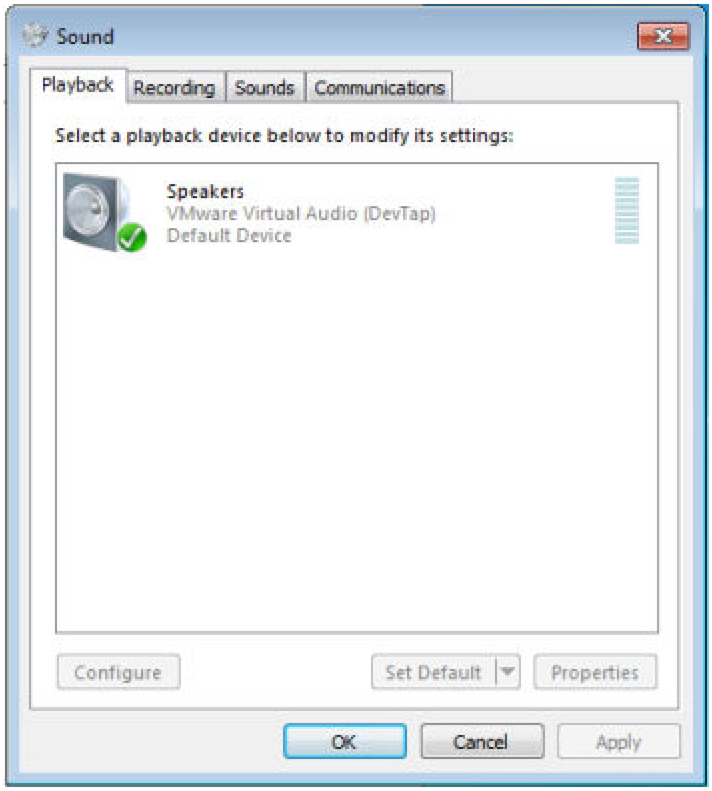
To know more about the VMware Real Time Audio-Video support, go to pubs.vmware.com/horizon-62-view/topic/com.vmware.horizon-view.desktops.doc/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html.

ⓘ NOTE: **There is no additional configuration for ThinOS. RTAV video requires RTME package to be installed on your device.**

To validate the VMware Real Time Audio-Video, do the following:

1. Connect to the VMware PCoIP or Blast desktop with the audio and video devices.

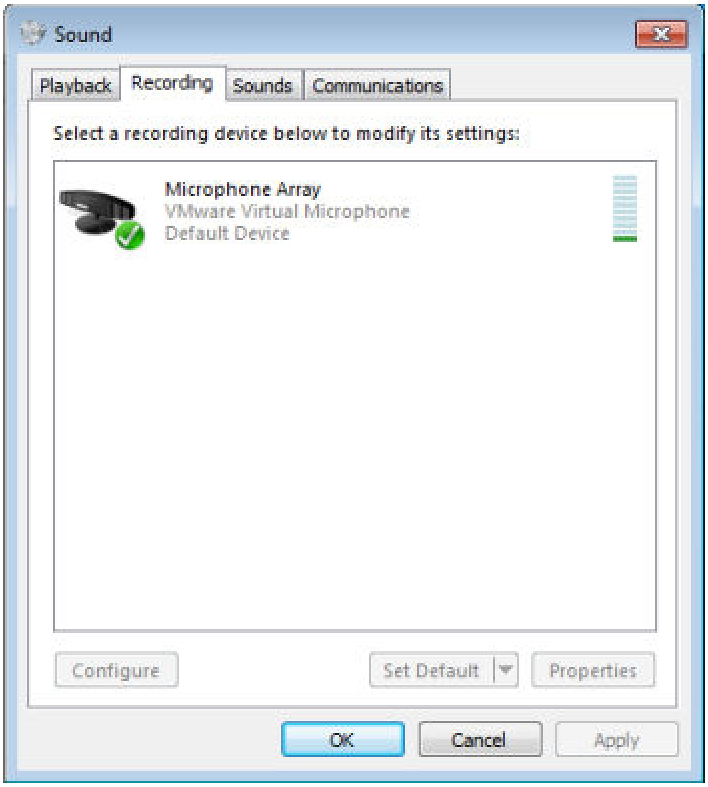
   ⓘ NOTE: **USB redirection must be disabled for the audio/video devices.**
2. Verify the audio playback of the system using the VMware virtual audio.



Select a playback device below to modify its settings:

Speakers
VMware Virtual Audio (DevTap)
Default Device

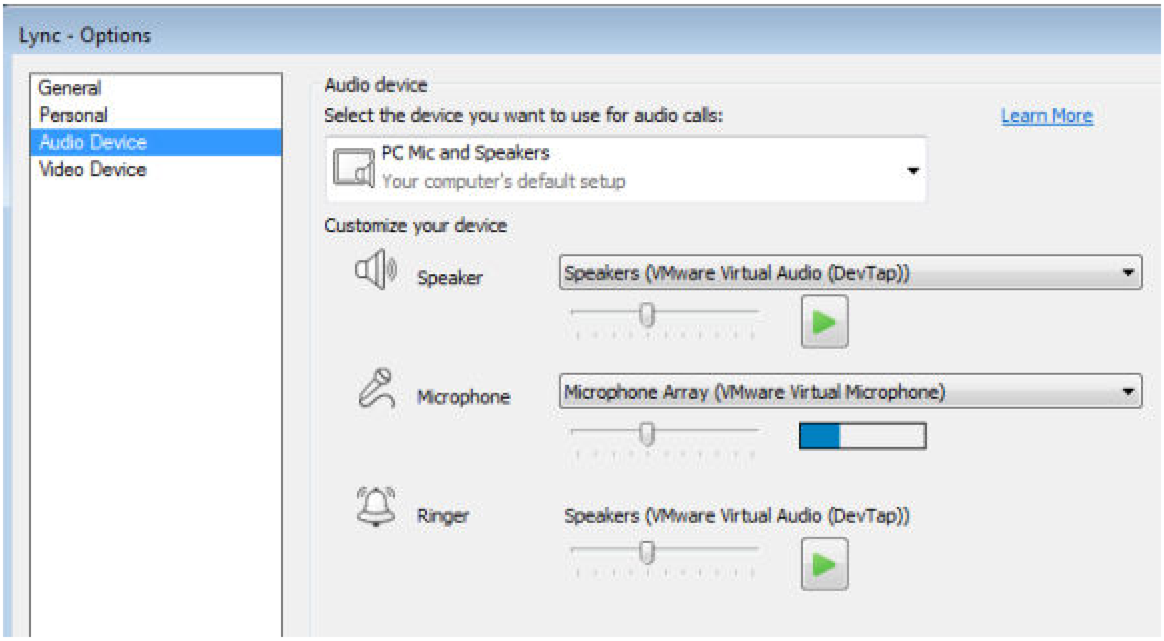
3 Verify the system audio recording using the VMware virtual microphone.



Select a recording device below to modify its settings:

Microphone Array
VMware Virtual Microphone
Default Device

4 Verify the audio settings in VoIP application.



Lync - Options

- General
- Personal
- Audio Device
- Video Device

Audio device

Select the device you want to use for audio calls: Learn More

PC Mic and Speakers
Your computer's default setup

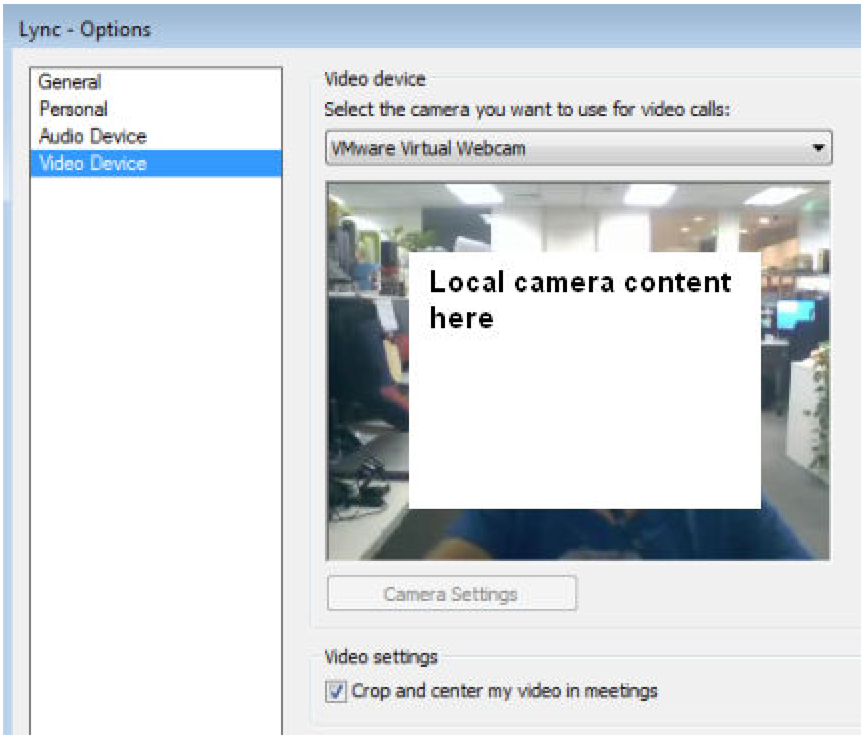
Customize your device

Speaker: Speakers (VMware Virtual Audio (DevTap))

Microphone: Microphone Array (VMware Virtual Microphone)

Ringer: Speakers (VMware Virtual Audio (DevTap))

5 Verify the video settings in VoIP application using the VMware virtual webcam.



Lync - Options

- General
- Personal
- Audio Device
- Video Device

Video device

Select the camera you want to use for video calls:

VMware Virtual Webcam

Camera Settings

Video settings

☑ Crop and center my video in meetings

6 Start the audio or video calls.

Dependencies and known issues

- Dependency: `RTME.i386.pkg` needs to be installed for RTAV video.
- The answer call button of the local audio device, supported by HDX RTME, is not supported by RTAV.
- RTAV does not support RDS desktop, for example, 2008 R2/ 2012 R2 according to VMware.
- Support for PCoIP and Blast protocol only. RDP protocol is not supported according to VMware.
- Webcam preferences are not supported. For example, the first webcam displayed in the Camera tab in local peripheral settings is used always.
- Camera/Video: High Definition video is not supported because of the RTAV limitation. The local camera setting does not affect RTAV video because of the application design. Dell recommend users not to interfere with the local camera settings.

Supporting VMware Blast

VMware Blast display protocol can be used for remote applications and for remote desktops that use virtual machines or shared-session desktops on an RDS host. Select this protocol connection to display the desktop with the Blast protocol.

NOTE: When you pause the pointer over the connection icons, the corresponding connection protocols are displayed in tooltip. This is designed for RDSH applications. From ThinOS 8.4 release, RDSH application is supported for both PCoIP and Blast protocol. These two protocols share the same application icon, and hence it is necessary for you to pause the pointer over the connection icons to identify its protocol.

Blast feature matrix on ThinOS

Table 9. Blast feature matrix

Blast features	Support on ThinOS	Comments/ Known issues
H.264 offload	Yes	NA
VDI desktops	Yes	NA
RDSH desktops	Yes	NA
RDSH applications	Yes	Application window does not support Seamless mode. For example, all applications open in single window because of the VMware limitation.
		RDSH application supports the PCoIP protocol with same limitation.
Unified communication	No	Third party plug-ins are not planned
MS VDI plug-in	No	NA
RTAV	Yes	NA
Windows media MMR	No	NA
Flash URL multicast	No	NA
Printer redirect	Yes	Supports printer redirection, and printer mapping with virtual print.
Smartcard redirect	Yes	NA
Scanner redirect	No	NA
Serial port redirect	No	NA
USB redirect—VDI/ RDSH	Yes	Enabled by default.
Client drive redirect	No	NA
Linux desktop	Yes	NA

Blast features	Support on ThinOS	Comments/ Known issues
Copy Paste text	Yes	See, VMware Horizon server and client configurations/documentation.
VPN connect	Yes	NA
AES 128/256	Yes	See, ThinOS AES design.
Multi-display/ 4K/ 32-bit	Yes	See, VMware Blast support information. For example, the pre-requisite is Virtual Machine video RAM.
ClearType fonts support	Yes	ThinOS supports the TrueType fonts
3D display	Yes	See, VMware Blast support information
Blast recovery from network interrupt	Yes	Requires Horizon View agent 7.0.1

For more information about VMware Horizon Blast, see VMware documentation.

For information about Blast Virtual Printing on ThinOS, see Blast Virtual Printing.

Support for multi-monitors in VMware Blast session

ThinOS supports multiple-monitor display to run virtual machines on each monitor.
Prerequisite: Update the VMware Blast package to the latest version. For more information, see the latest Dell Wyse ThinOS Release Notes.
User scenario:

1. Connect multiple monitors to the ThinOS device.
2. In the **Display Setup** dialog box, disable **Mirror Mode**, and configure the display layout.
3. Launch a full screen VMware Horizon Blast session.

- **Display numbers**—A virtual machine needs sufficient video memory to support multiple monitors. You can use up to four monitors with sufficient RAM.

Table 10. Display Layout matrix

Resolution	1920 x 1080					2560 x 1440				
No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
Horizontal	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA
Vertical	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA
Grid	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA

- **4K display**—With the VMware Blast display protocol a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

Table 11. 4K display support

Hardware version	Windows version	Number of 4K displays supported
10 (ESXi 5.5.x compatible)	7, 8, 8.x, and 10	1
11 (ESXi 6.0 compatible)	7—3D rendering feature and Windows Aero are disabled.	3
11	7—3D rendering feature is enabled.	1

Hardware version	Windows version	Number of 4K displays supported
11	8, 8.x, and 10	1

- **3D rendering**—You can configure 3D graphics rendering for connected desktops. To use the 3D rendering feature, use up to two monitors with a resolution of up to 1920 x 1200. For a resolution of 4K (3840 x 2160), only one monitor is supported.
- **Blast H.264**—The following table describes the performance of H.264 decoder in VMware Horizon sessions that use the VMware Blast display protocol:

Table 12. Blast H.264 decoding

Screen resolution within VMware Horizon Blast session	Blast H.264 decoding in VMware Horizon Blast session	Summary
Session display width is less than or equal to 1920 pixels.	Blast H.264 decoding is always enabled.	Horizon client uses Blast H.264 decoding even if the H.264 decoder setting is disabled using GUI or INI options.
Session display width is greater than 1920 pixels.	Blast H.264 decoding is disabled by default. You can enable Blast H.264 decoding either on the ThinOS GUI or by deploying the INI parameter.	By default, Horizon client does not use Blast H.264 decoding. If the Blast H.264 decoder setting is enabled on ThinOS, then the Horizon client uses H.264 decoding. Enabling H.264 may downgrade the session performance.

Support for multi-monitors in PCoIP session

ThinOS supports multiple-monitor display to run virtual machines on each monitor.
User scenario:

1. Connect multiple monitors to the ThinOS device.
2. In the **Display Setup** dialog box, disable **Mirror Mode**, and configure the display layout.
3. Launch a full screen PCoIP session.

- **Display numbers**—A virtual machine needs sufficient video memory to support three or four monitors. The default video memory on VMware vSphere supports only two monitors.
  - Supports one session up to four monitors in span mode with resolution up to 2560 x 1600.
  - Supports one session up to two monitors in span mode with resolution up to 3840 x 2160.

  The maximum number of monitors that can be stacked vertically is two. If you use more than two monitors, the monitors must be in the same mode and have the same screen resolution. For instance, if you use three monitors, all three monitors must be either in portrait mode or landscape mode, and must use the same screen resolution.
- **Display layout**—The display layout of the monitors must be aligned up and down, or left and right. Improper alignment results in unusual display.
- **3D rendering**—You can configure 3D graphics rendering for connected desktops. To use the 3D rendering feature, use up to two monitors with resolution up to 1920 x 1200.

Table 13. Matrix for multi screen support

PCoIP Multi-monitor support																
Wyse 5070 Extended thin client																
Display layout	Resolution	1920 x 1200					2560 x 1440					3840 x 2160				
	No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
	Horizontal	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA	Yes	NA	NA	NA	NA
	Vertical	Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA	NA	Yes	NA	NA	NA	NA
	Grid	NA	Yes	Yes	NA	NA	NA	Yes	Yes	NA	NA	NA	NA	NA	NA	NA

PCoIP Multi-monitor support																
Wyse 5070 thin client—Pentium																
Display layout	Resolution	1920 x 1200					2560 x 1440					3840 x 2160				
	No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
	Horizontal	Yes	Yes	NA	NA	NA	Yes	Yes	NA	NA	NA	Yes	NA	NA	NA	NA
	Vertical	Yes	Yes	NA	NA	NA	Yes	Yes	NA	NA	NA	Yes	NA	NA	NA	NA
Wyse 5070 thin client—Celeron																
Display layout	Resolution	1920 x 1200					2560 x 1440					3840 x 2160				
	No. of displays	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six	Two	Three	Four	Five	Six
	Horizontal	Yes	NA	NA	NA	NA	Yes	NA	NA	NA	NA	Yes	NA	NA	NA	NA
	Vertical	Yes	NA	NA	NA	NA	Yes	Na	NA	NA	NA	Yes	NA	NA	NA	NA

Blast Virtual Printing

Virtual printing with VMware Blast allows you to use local or network printers from the Blast desktop without the need of installing the additional print drivers on the remote desktop. For each printer configured locally on ThinOS, you must map the printer to the VMware Blast desktop. ThinOS Blast printer mapping is equivalent to VMware Blast virtual printing.

To map your printer, do the following:

ⓘ **NOTE: LPT printer is considered as an example to explain the printer mapping scenario. Printer mapping in ThinOS works similar to LPT for LPD and SMB printers.**

1 Power on the ThinOS client with the VMware View broker configured in the **Broker Setup** tab. Set the connection protocol as **All Supported** from the **Connection Protocol** drop-down list.

2 Go to **Global Connection Settings** > **Session**, and retain the **Exclude printer devices** check box selection. This option is selected by default.

3 Plug in a USB printer to the ThinOS client terminal.

4 Go to **System Setup** > **Printer**.

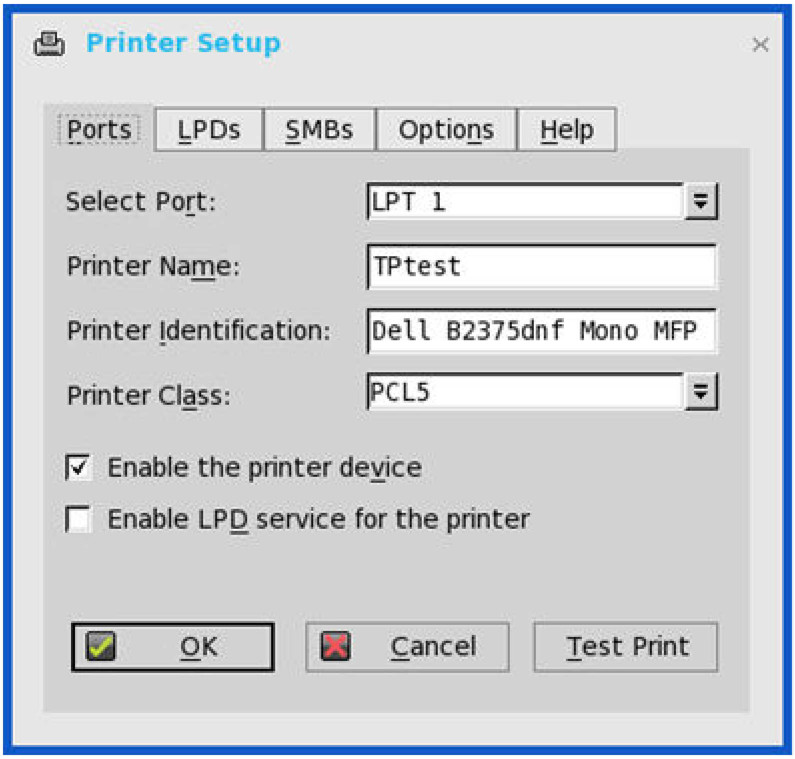
The **Printer Setup** dialog box is displayed.

5 In the **Printer Setup** dialog box, do the following:

a From the **Select Port** drop-down list, select **LPT 1**.

b Enter valid printer name and printer identification.

c Select the **Enable the printer device** check box.



Printer Setup

Select Port: LPT 1

Printer Name: TPtest

Printer Identification: Dell B2375dnf Mono MFP

Printer Class: PCL5

☑ Enable the printer device

☐ Enable LPD service for the printer

Figure 10. Printer Setup

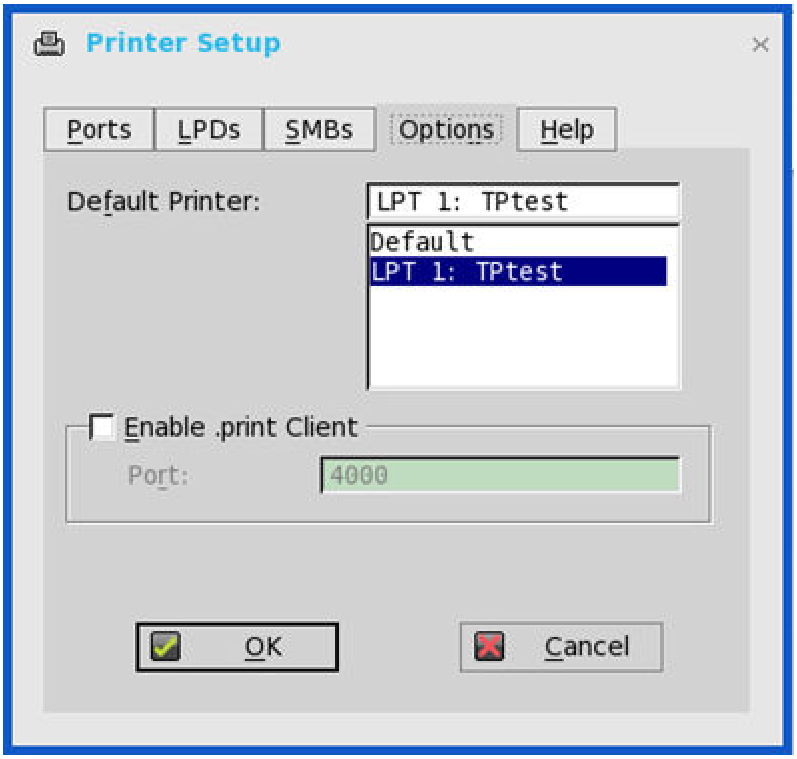
d Click **Ok** to save the configuration.

6 Click the **Options** tab, and do the following:

a Set **LPT1: <Printername>**as default printer.

NOTE: **Do not select the Enable .print Client check box.**

b Click **Ok** to save the configuration.



Default Printer: LPT 1: TPtest

Default
LPT 1: TPtest

☐ Enable .print Client

Port: 4000

Figure 11. Options

7 Connect to a VMware Blast session. Go to **Control Panel** > **Devices and Printers**. The printer that is configured locally in ThinOS is mapped to the session.

The mapped printer's driver is TP PS Driver and the port is TPVM port.

The virtual printer allows the ThinOS local printer to be mapped to the VMware Blast session without installing the printer driver in the session.

Supporting Teradici SDK

The PCoIP Client Software Development Kit (SDK) is a set of libraries and binaries that you can use to build or customize a PCoIP client.

ThinOS supports the Teradici SDK version 2.9.

User scenario:

- Behavior with earlier Teradici SDK versions: You were able to switch the USB disk redirection between sessions. For example, plug in the USB disk, and connect the desktop 1 and 2. The disk is redirected to desktop 1. If you disconnect from desktop 1, then the USB disk is redirected to desktop 2.
- Behavior with Teradici SDK version 2.9: When you disconnect from desktop 1, the USB disk is not redirected to desktop 2. You must remove the USB disk and plug in the USB disk again for redirection.

Configuring Microsoft Remote Desktop

Microsoft Remote Desktop application allows you to access and manage the data and resources of a remote device using an internet connection.

This section provides information about how to configure the Remote desktop broker connection on your ThinOS device, and other remote desktop features that you can configure on ThinOS.

Configuring the Microsoft Remote Desktop broker connection

To configure the Microsoft Remote Desktop broker setup:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, from the drop-down list, select **Microsoft**, and do the following:
   - **Broker Server**—Enter the IP address/Hostname/FQDN of the Broker Server.
   - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semi-colon, and is case-sensitive.
3. Click **OK** to save the settings.

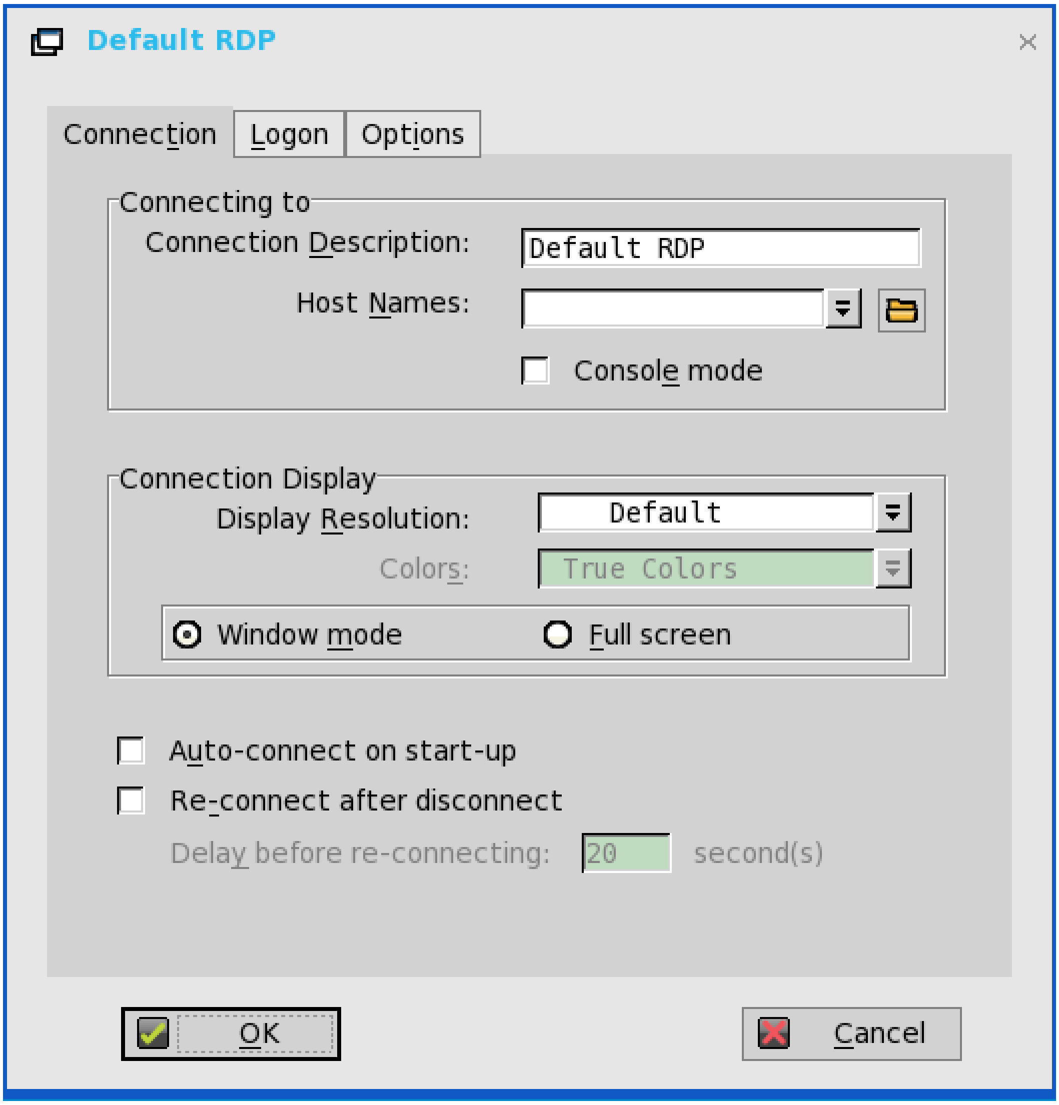
Configuring RDP connections

To configure the RDP connection option you selected in the Remote Connections:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, from the drop-down list, select the **Broker type** as **None**.
3. Click **RDP** connection protocol, and click **Configure**.

   The **Default RDP** dialog box is displayed.
4. Click the **Connection** tab, and use the following guidelines:



Default RDP

Connection | Logon | Options

Connecting to

Connection Description: Default RDP

Host Names:

□ Console mode

Connection Display

Display Resolution: Default

Colors: True Colors

● Window mode ○ Full screen

□ Auto-connect on start-up

□ Re-connect after disconnect

Delay before re-connecting: 20 second(s)

OK Cancel

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

b **Host Names**—Use the list to select the valid DNS server name or the IP address of the server to which the thin client connection is to be made you can also use **Browse** next to the box to make the selection you want. For example, a list of WTS servers on the local network from which you can select.

> NOTE: **The server name may be resolved using one of two mechanisms: DNS, and WINS. DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.**

c **Console mode**— Select to set the RDP connection with Windows Console mode.

d **Display Resolution**— Select the display resolution for this connection.

Colors—

Select the color depth of the RDP session. If High Colors (16 bits) or True **Colors** (32 bits) is selected and the RDP server does not support this color depth, the thin client renegotiates the color depth to the lower value for example, 256 Colors (8 bits). The highest is 32 bits, if hardware supports it.

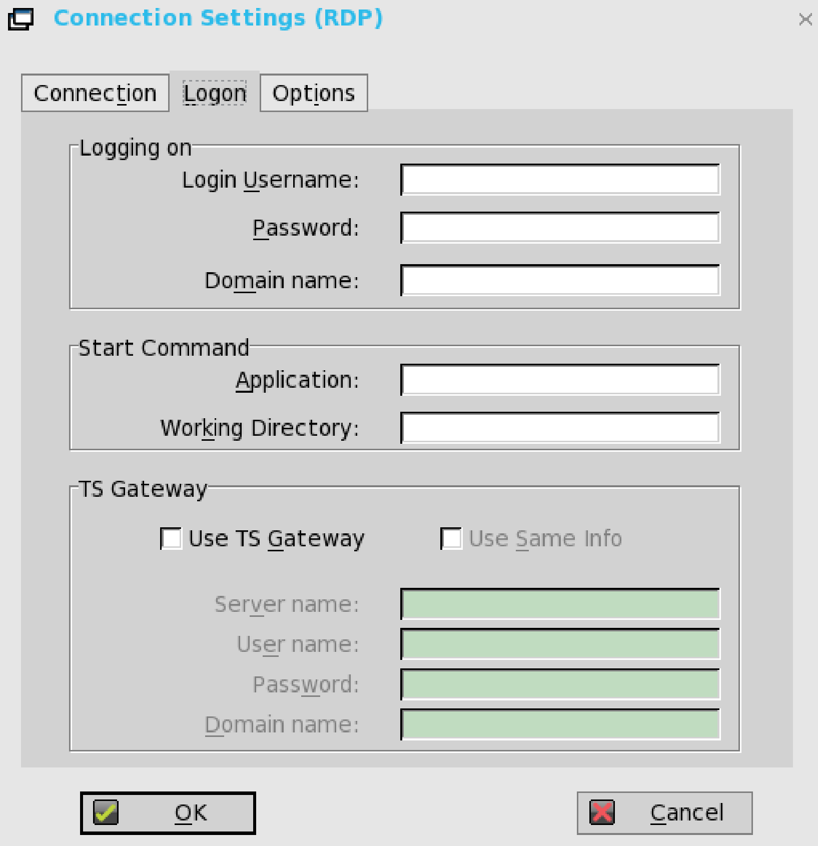
e **Window mode on 1 monitor** or **Full screen span all monitors**—Select the initial view of the session in window mode or full screen mode.

f **Auto-connect on start-up**—When selected, automatically connects the session on start-up.

g **Re-connect after disconnect**—When selected, causes the thin client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the **Delay before re-connecting** box (enter the number of seconds 1 to 3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds, if there is no INI file description of this connection, or is a Stand-alone user, or is simply omitted.

You can reset the options on the Connection tab of the Connection Settings (RDP) dialog box. To do so, click the **Reset VM** command button. This command button is located in the upper-right of the dialog box. It appears only with a VDM broker connection.

5 Click **Logon** tab, and use the following guidelines:



Connection Settings (RDP)

Connection | Logon | Options

Logging on

Login Username:

Password:

Domain name:

Start Command

Application:

Working Directory:

TS Gateway

□ Use TS Gateway □ Use Same Info

Server name:

User name:

Password:

Domain name:

OK | Cancel

a **Logging on** area —Enter login username, password, and domain name. If these boxes are not populated, you can enter the information manually in the RDP server login screen when the connection is made. Use the following guidelines:

- **Login Username** —Maximum of 31 characters is allowed.
- **Password**—Maximum of 19 characters is allowed.
- **Domain Name**—Maximum of 31 characters is allowed.

b **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.

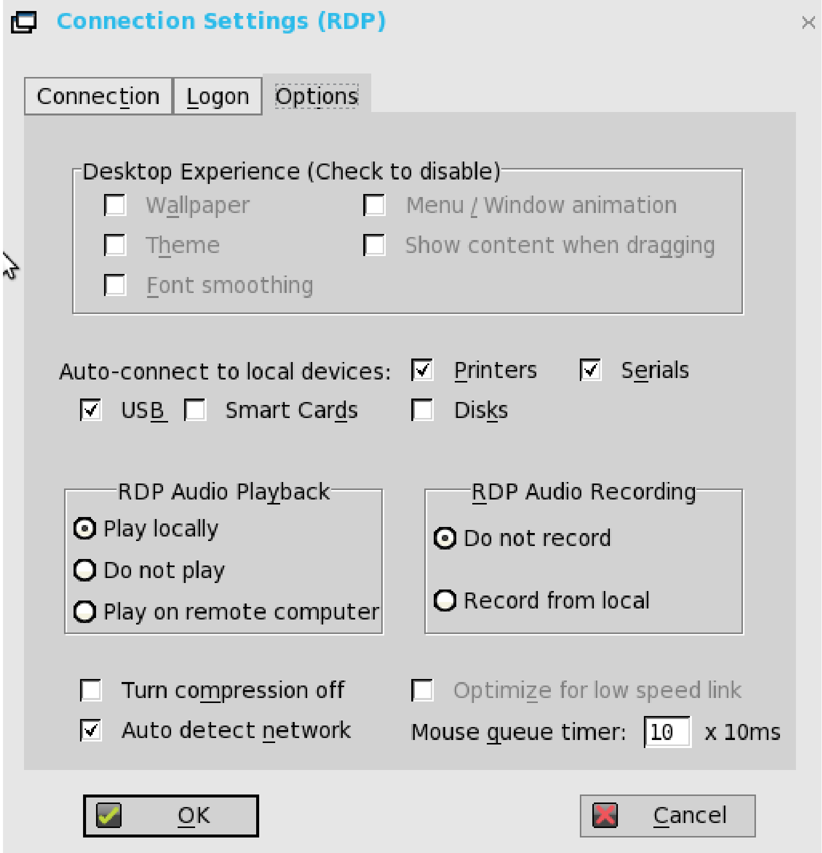
c **Use TS Gateway**—Enables the use of Terminal Services Gateway (TS Gateway) server when connecting. If required, then enter the IP address or URL of the TS Gateway server in the Server name box. You can also enable **Use Same Info** (if the server credentials are the same credentials as your Remote Desktop Credentials (Host remote computer credentials) in the Login Username, Password, and Domain name fields) or disable **Use Same Info** and enter the Server name, User name, Password, and Domain name of the TS Gateway server if required.

> **NOTE: A TS Gateway server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer with an Internet connection. A TS Gateway server enables Remote Desktop connections to a corporate network from the Internet without having to set up virtual private network (VPN) connections. Ask your network administrator whether you need to specify a TS Gateway server.**

- **User Name**—Enter a user name for the connection.
- **Password**—Enter the password.
- **Domain**—Enter the domain name.

NOTE: The user name, password, and domain name fields are optional. If you leave any of these fields blank, interactive login is required and users must enter the information at login time.

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



Connection Settings (RDP)

Connection | Logon | Options

Desktop Experience (Check to disable)

□ Wallpaper □ Menu / Window animation

□ Theme □ Show content when dragging

□ Font smoothing

Auto-connect to local devices: ☑ Printers ☑ Serials

☑ USB □ Smart Cards □ Disks

RDP Audio Playback

● Play locally

○ Do not play

○ Play on remote computer

RDP Audio Recording

● Do not record

○ Record from local

□ Turn compression off □ Optimize for low speed link

☑ Auto detect network Mouse queue timer: 10 x 10ms

OK Cancel

a **Wallpaper**—When selected, disables the desktop wallpaper.

b **Menu / Window animation**—When selected, disables the menu or window animation.

c **Theme**—When selected, disables the desktop themes.

d **Show content when dragging**—By default, when you grab a Window by the title bar and move it around, the contents of the window will move with it. Select this to disable this content view so that only the outline of the window moves when dragging it, until you drop the window. This option can be beneficial, as it uses less processing power.

e **Font smoothing**—Converts vector text to bitmap for better display.

f **Auto-connect to local devices**—Select any options (Printers, Serials, USB, Smart Cards, and Disks) to have the thin client automatically connect to the devices.

NOTE: USB—Redirects locally attached USB devices on the thin client to a Microsoft Windows terminal server. When the user connects to the terminal server, locally attached USB devices on the thin client are accessible.

g **RDP Audio Playback**—Select the audio playback options such as Play Locally, Do not play, and Play on remote computer.

h **RDP Audio Recording**—Select the audio recording options such as Do not record, and Record from local.

i **Turn compression off**—When selected, turns compression off (intended for high-speed connections).

j **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 dialup.

k **Auto detect network**—When selected, turns on the auto detect network feature. This feature is enabled by default. It also disables the Optimize for low speed link option and the Desktop Experience options by default.

l **Mouse queue timer**—Specifies the default queue timer of a mouse event in an ICA or RDP session (in 1/100 of a second). It can be used to adjust the bandwidth of a network.

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

Features of RDP protocol

Remote Desktop Protocol (RDP) is a network communications protocol developed by Microsoft that enables you to remotely access virtual desktops and applications. This section describes the functionality of ThinOS over RDP protocol.

Support for multi-monitors in RDP session

ThinOS supports multiple-monitor display to launch RDP desktops on each monitor.
User scenario:

1 Connect multiple monitors to ThinOS device.
2 In the **Display Setup** dialog box, disable **Mirror Mode**, and configure the display layout.
3 Launch an RDP desktop with full screen.

All data described in the following table is based on virtual machine without RemoteFX/vGPU enabled configuration.

Table 14. RDP display capability matrix

Destination endpoint	Maximum resolution per monitor [Enable Force Span]	Maximum display support [Span Monitors]
Windows 7 SP1	4096 (w) x 2048 (h)	4096 (w) x 2048 (h)
Windows 8.1	8192 x 8192	6 x 4K
Windows Server 2012 R2	8192 x 8192	6 x 4K
Windows 10	8192 x 8192	6 x 4K
Windows Server 2016	8192 x 8192	6 x 4K

RDP H.264

In ThinOS version 8.5.1, logs of H.264 and H.264-AVC444 are hidden and not displayed in the **Event Log** tab.

The following table describes the RDP H.264 functionality matrix.

Table 15. RDP H.264 functionality matrix

RDP session	Microsoft broker 2012 R2	Microsoft broker 2016	Resolution for H.264 Enabled
Windows 8.1/ 2012 R2	H.264 is used	H.264 is used	>= 576 x 576 and <= 2048 x 1280
Windows 10/ 2016	H.264 is not used	H.264-AVC444 is used	>= 576 x 576 and <= 3840 x 2160

The following table describes the RDP H.264 decoding matrix. All data described in the following table is based on virtual machine without RemoteFX/vGPU enabled configuration.

Table 16. RDP H.264 decoding matrix

Unit type	GPU	Session	Windows 10/Windows Server 2016		Windows 8.1/Windows Server 2012 R2	
		Display resolution	H.264-AVC444	Decoding	H.264	Decoding
Wyse 5070 Extended thin client	AMD	3840 x 2160	Enabled	Software	Disabled	
		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Hardware
		1920 x 1200	Enabled	Software	Enabled	Hardware
	Intel	3840 x 2160	Enabled	Software	Disabled	
		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Hardware
		1920 x 1200	Enabled	Software	Enabled	Hardware
Wyse 5070 thin client—Celeron processor Wyse 5070 thin client—Pentium processor	Intel	3840 x 2160	Enabled	Software	Disabled	
		2560 x 1440	Enabled	Software	Disabled	
		2048 x 1280	Enabled	Software	Enabled	Hardware
		1920 x 1200	Enabled	Software	Enabled	Hardware

NOTE:

- Windows 10/Window Server 2016 must be hosted in Microsoft RDS 2016 broker for enabling H.264-AVC444.
- H.264 logs and H.264-AVC444 logs are hidden and not displayed in the **Event Log** tab.

Known issues

- In Mirror mode with active session, when you change the resolution from 2048 x 1280 to greater than 2048 x 1280, the connected RDP session (Windows 8/ Windows 2012 R2) is closed forcibly and an error message—**RDP: The server-side graphics subsystem is in an error state and unable to continue graphics encoding** is displayed. This is because the session is not reconnected in Mirror mode after resolution is changed that resulted in H.264 codec exceeding its supported resolution.

  Workaround—You must manually reconnect the session after the resolution is changed.
- In an RDP session with VOR enabled by default (Windows 8.1 x86), you connect to a session with full screen, and span more than four 4K monitors. In this scenario, if you play a video, the session may be disconnected automatically with an error log **RDP: The server-side graphics subsystem is in an error state and unable to continue graphics encoding**. This is because VOR /x-264 requires more resources, such as RAM, than the server resources.

  Workaround—You can reduce the number of monitors or lower the resolutions or switch to other 64-bit operating system with more RAM.

Configuring H.264 AVC444 in RDP 10 session

Prerequisites:

- Thin client must run on ThinOS version 8.5 or later.
- Windows 10 or Windows Server 2016 must be created in Microsoft RDS 2016 broker or in the latest VMware View broker.

To configure the H.264 AVC444 in an RDP 10 session:

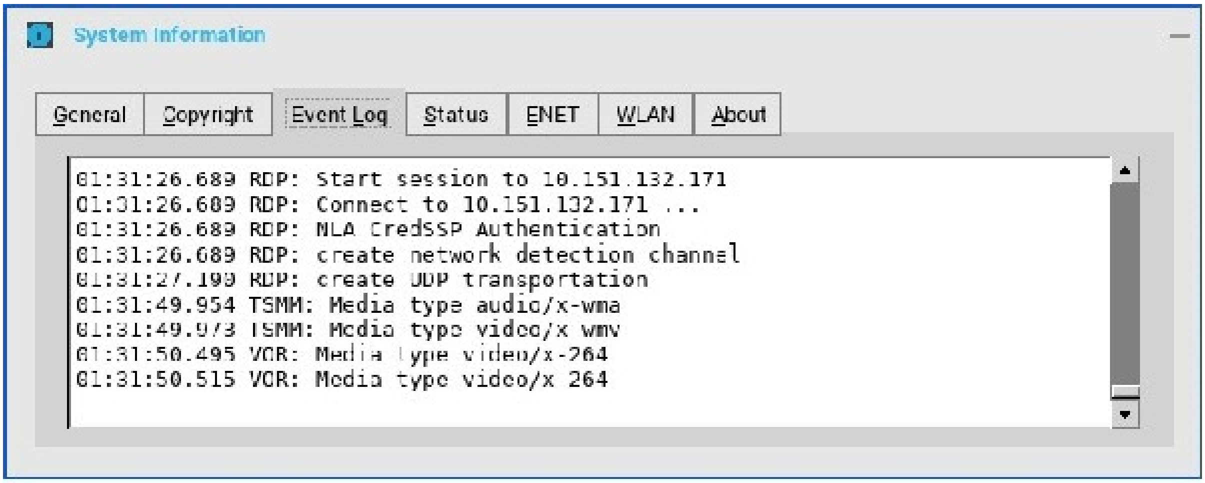
1. In the Windows session host, run gpedit.msc.
2. Open the Local Group Policy Editor.
3. Navigate to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Remote Session Environment**, and enable the following policies:

- Prioritize H.264/AVC 444 Graphics mode for Remote Desktop connections
- Configure H.264/AVC hardware encoding for Remote Desktop connections

4 Open **cmd.exe** and run **gpupdate /force**, or restart the server.

VOR codec in RDP session

When you are playing video in an RDP session—Windows 8.1, Windows 2012 R2, Windows 10 and Windows 2016—VOR codec is used. The following logs are displayed in the **Event Log** tab.



```
01:31:26.689 RDP: Start session to 10.151.132.171
01:31:26.689 RDP: Connect to 10.151.132.171 ...
01:31:26.689 RDP: NLA CredSSP Authentication
01:31:26.689 RDP: create network detection channel
01:31:27.199 RDP: create UDP transportation
01:31:49.954 TSMM: Media type audio/x-wma
01:31:49.973 TSMM: Media type video/x wmv
01:31:50.495 VOR: Media type video/x-264
01:31:50.515 VOR: Media type video/x 264
```

Figure 12. Event log tab

NOTE:

- Dependence 1—RDP GFX status, H.264 and VOR work only when GFX is enabled.
- Dependence 2—VOR is dynamic. So the enablement / disablement of VOR dynamically changes during the change in the video resolution (enlarge/shrink).
- Dependence 3—H.264 enablement is decided at the beginning of connection, depending on the maximum resolution available for the session.
- In Microsoft broker 2016, and Windows 10/2016 sessions, if H.264-AVC444 is enabled, then VOR is not used. If you disable H.264-AVC444, VOR is used.

In RDP session (RDP 8.1 and later), VOR, H.264 and H.264-AVC444 are enabled by default. To disable these parameter, use the following ini parameter: `SessionConfig-RDP EnalbeGFX=yes EnableVOR=no EnableRDPh264=no`.

TS Gateway in Microsoft Broker

User scenario:

1 Log in to Microsoft Broker with TS Gateway configured.

2 Launch a published collection.

TS Gateway connection is established.

The following table lists the TS Gateway versions supported by Windows Server.

Table 17. Supported TS Gateway versions

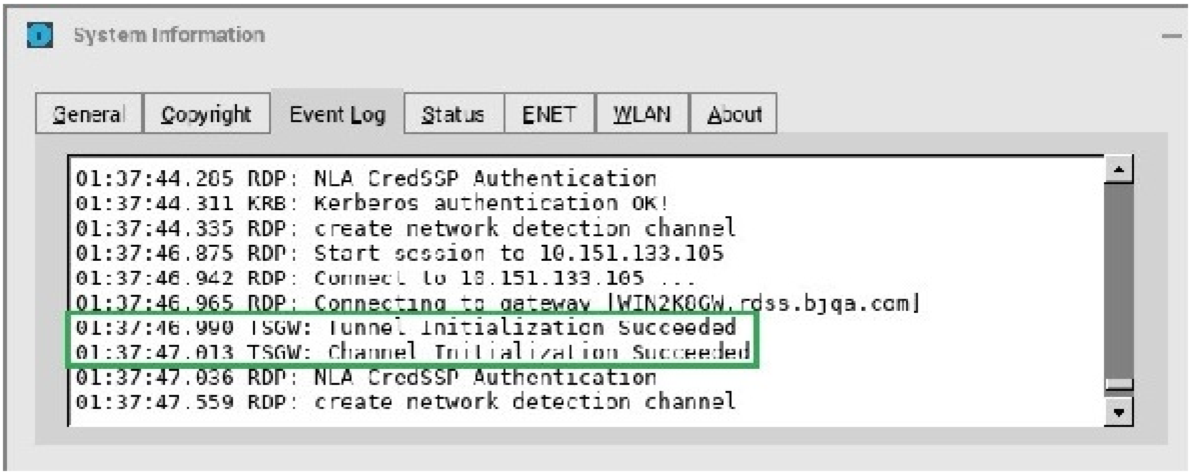
Server operating system	TS Gateway II	TS Gateway III	WebSocket
Windows 2008 R2	Support	Not support	Not Support
Windows 2012 R2	Support	Support	Not Support

Server operating system	TS Gateway II	TS Gateway III	WebSocket
Windows 2016	Support	Support	Support

ⓘ NOTE:

- In TS Gateway II or III connection, the setup uses a two half-duplex communication between Terminal Server (TS) Gateway server and thin client.
- In the WebSocket connection, the session connection setup uses a duplex communication between TS Gateway and thin client
- TS Gateway II and TS Gateway III are downward compatible with Windows Server 2016, that means, if the WebSocket connection fails or the TS Gateway server or thin client version does not support WebSocket, then TS Gateway II or TS Gateway III is used.

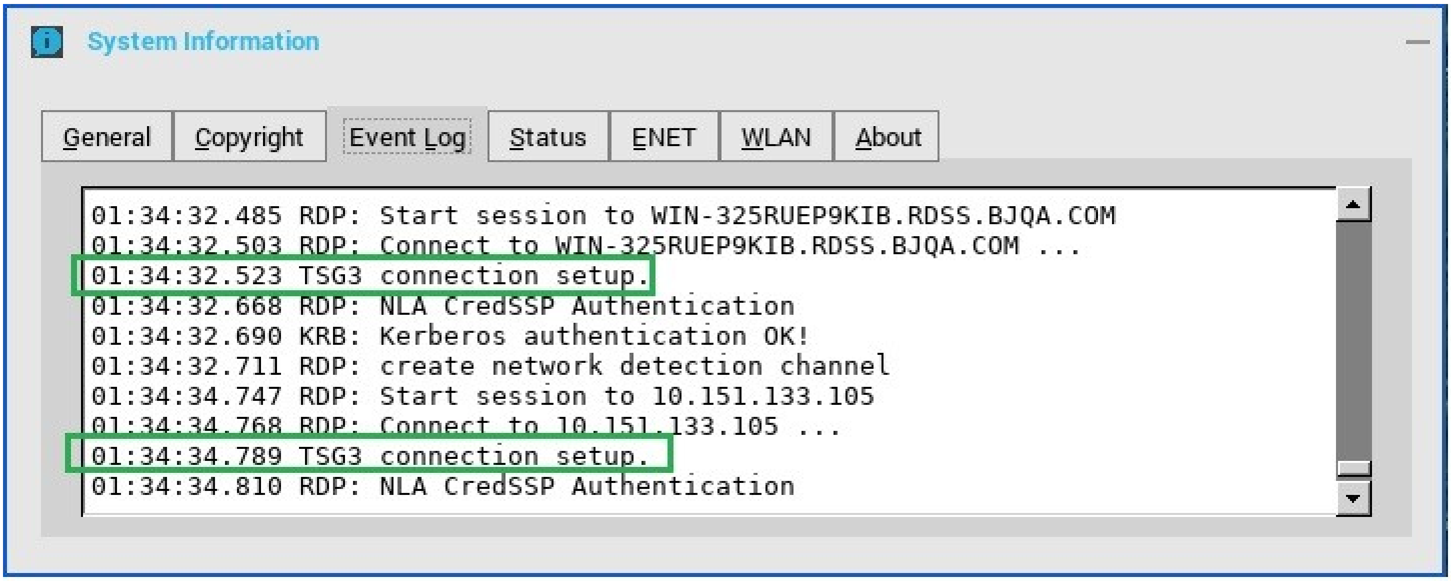
The following screenshot displays the TS Gateway II connection setup logs:



```
01:37:44.205 RDP: NLA CredSSP Authentication
01:37:44.311 KRB: Kerberos authentication OK!
01:37:44.335 RDP: create network detection channel
01:37:46.875 RDP: Start session to 10.151.133.105
01:37:46.942 RDP: Connect to 10.151.133.105 ...
01:37:46.965 RDP: Connecting to gateway [WIN2K0GW.rdss.bjqa.com]
01:37:46.990 TSGW: Tunnel Initialization Succeeded
01:37:47.013 TSGW: Channel Initialization Succeeded
01:37:47.036 RDP: NLA CredSSP Authentication
01:37:47.559 RDP: create network detection channel
```

Figure 13. Event log tab

The following screenshot displays the TS Gateway III connection setup logs:



```
01:34:32.485 RDP: Start session to WIN-325RUEP9KIB.RDSS.BJQA.COM
01:34:32.503 RDP: Connect to WIN-325RUEP9KIB.RDSS.BJQA.COM ...
01:34:32.523 TSG3 connection setup.
01:34:32.668 RDP: NLA CredSSP Authentication
01:34:32.690 KRB: Kerberos authentication OK!
01:34:32.711 RDP: create network detection channel
01:34:34.747 RDP: Start session to 10.151.133.105
01:34:34.768 RDP: Connect to 10.151.133.105 ...
01:34:34.789 TSG3 connection setup.
01:34:34.810 RDP: NLA CredSSP Authentication
```

Figure 14. Event log tab

ⓘ NOTE: **WebSocket connection log is hidden and not displayed in the Event Log tab.**

Configuring Dell vWorkspace

Workspace virtualization delivers a list of applications or desktops together as a single complete virtual workspace. It isolates and centralizes an entire computing workspace. vWorkspace provides flexible, location and platform independent access by delivering virtual workspace from multiple virtualization platforms.

This section provides information about how to configure a Dell vWorkspace broker connection on your ThinOS device.

Configuring the Dell vWorkspace broker connection

To configure the vWorkspace broker setup:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, from the drop-down list, select **Dell vWorkspace**, and do the following:
   - **Broker Server**—Enter the IP address/ Hostname/ FQDN of the Broker Server.
   - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be listed. Each desktop name is separated by a semi-colon, and is case-sensitive.
   - Select the check box to enable vWorkspace Gateway.
   - **vWorkspace Gateway**—Enter the IP Address of the vWorkspace Gateway.
3. Click **OK** to save the settings.

Configuring Amazon Web Services or WorkSpaces

Amazon WorkSpace is a cloud-based virtual desktop that allows you to access remote applications with ease.

Amazon WorkSpaces connection is applicable only for PCoIP clients running ThinOS 8.3, and later versions.

This section provides information about how to configure the Amazon WorkSpaces (AWS) connection on your ThinOS device, and other Amazon WorkSpace features that you can configure on ThinOS.

Configuring the Amazon WorkSpaces broker connection

Amazon WorkSpaces connection is applicable only for PCoIP clients. To configure the Amazon WorkSpaces (AWS) broker setup:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, from the drop-down list, select **Amazon WorksSpaces**, and do the following:
   - **Broker Server**—Enter the IP address/Hostname/FQDN of the Broker Server.
   - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be listed. Each desktop name is separated by a semi-colon, and is case-sensitive.
   - **Security mode**—Select the preferred Security mode from the following options:
     - **Warning** —Warn Security requires FQDN address for domain certificate installed in PCM. If certificate is not installed on the client, corresponding warning message is displayed for you to continue.
     - **Full**—Full Security requires FQDN address with domain certificate installed in PCM, and certificate installed on the client.
     - **Low**—Security allows FQDN/IP address with/without certificate.
     - **Default**— Follows global security mode settings.
   - **Connection Protocol**— The drop-down list is disabled for AWS broker. By default, the option is set to **PCoIP Only**.
3. Click **OK** to save the settings.

For information about deploying AWS WorkSpaces and AWS EC2 PCM for AWS WorkSpaces, go to www.teradici.com/web-help/Connecting_ZC_AWS_HTML5/TER1408002_Connecting_ZC_AWS.htm#03_DeployPCM.htm%3FTocPath%3D3.

For information about configuring the Broker Server address = “URI (https://<FQDN or IP address>) of the PCM”, go to www.teradici.com/web-help/Connecting_ZC_AWS_HTML5/TER1408002_Connecting_ZC_AWS.htm#05_Connect.htm%3FTocPath%3D5.

Known issues with Amazon Web Services or WorkSpaces

- Key combination **Ctrl + Alt** disconnects users from AWS session intermittently with old agent in AWS desktop. To fix this issue, update to latest agent by rebooting the desktop.
- Each user is assigned with one WorkSpaces desktop, and therefore logon with any username returns to the single desktop and then the session connects automatically. Disconnecting from the desktop returns user to logon screen.

6

Configuring local settings

You can configure available thin client settings on the thin 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 thin 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 thin clients in your environment, 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 peripherals 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.
- **Classic desktop**—Click User Name, and select **System Setup**.

ⓘ **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 preference
- Setting time and date
- Setting the custom information

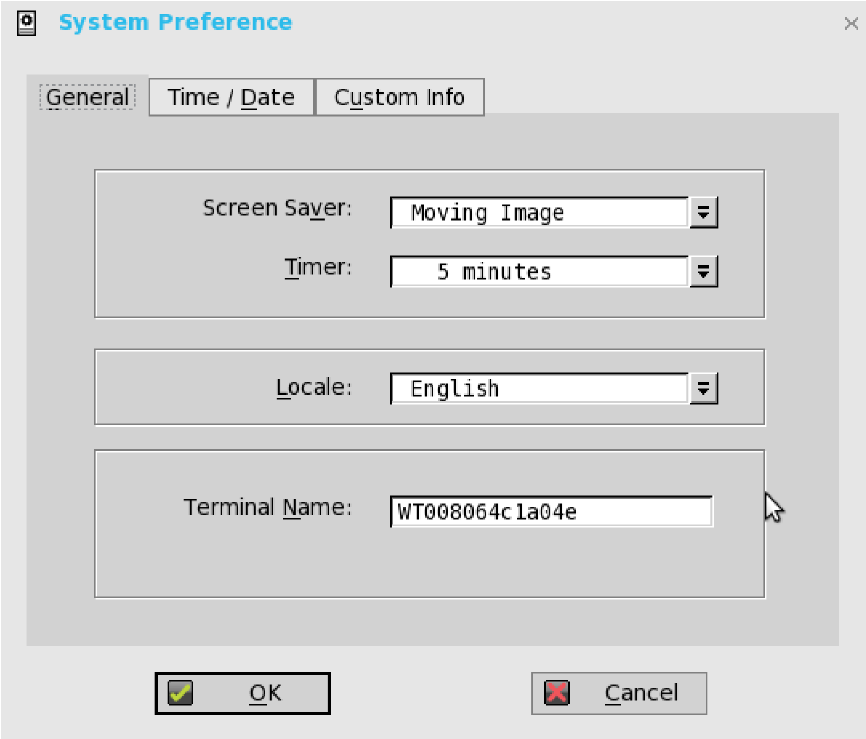
Setting the general system preference

To configure the general settings for system preference:

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

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

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



Screen Saver: Moving Image

Timer: 5 minutes

Locale: English

Terminal Name: WT008064c1a04e

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

Other available screen savers are **Flying Bubbles**, **Moving Image**, **Showing Pictures**, and **Playing Video**.

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 thin 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. 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 thin client. The default is a 14-character string composed of the letters WT followed by the thin 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.

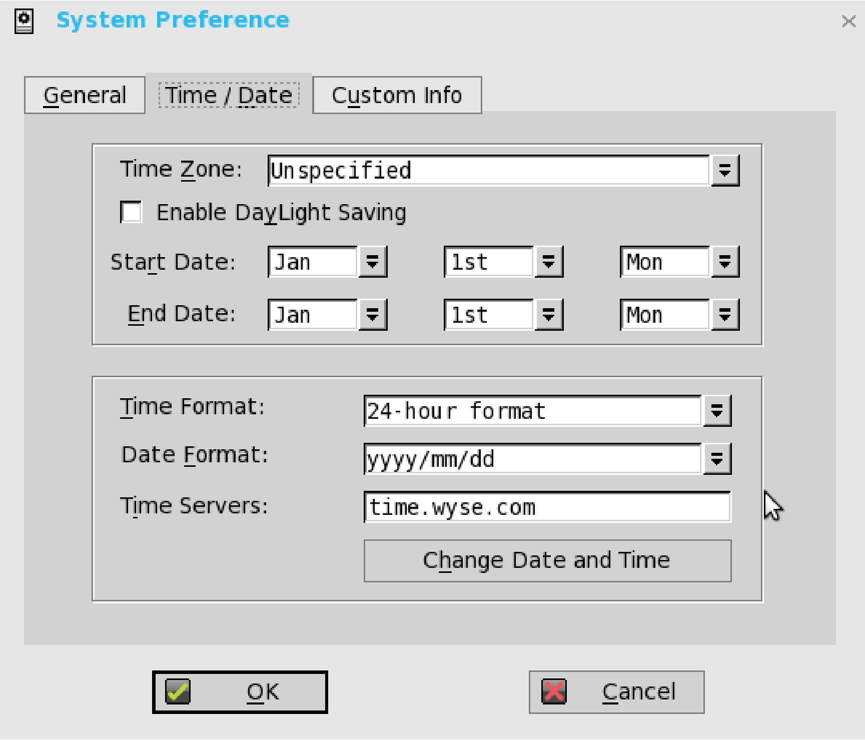
Setting the time and date

To configure the time and date settings:

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

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

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



Time Zone: Unspecified

□ Enable DayLight Saving

Start Date: Jan 1st Mon

End Date: Jan 1st Mon

Time Format: 24-hour format

Date Format: yyyy/mm/dd

Time Servers: time.wyse.com

   a **Time Zone**— Select a time zone where the thin client operates from the drop-down list. Default value 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 the 12 or 24-hour time format. **default is 24-hour format.**

   d **Date Format** — Allows you to select the 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 thin 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 thin client for SSL/ certification validation.

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

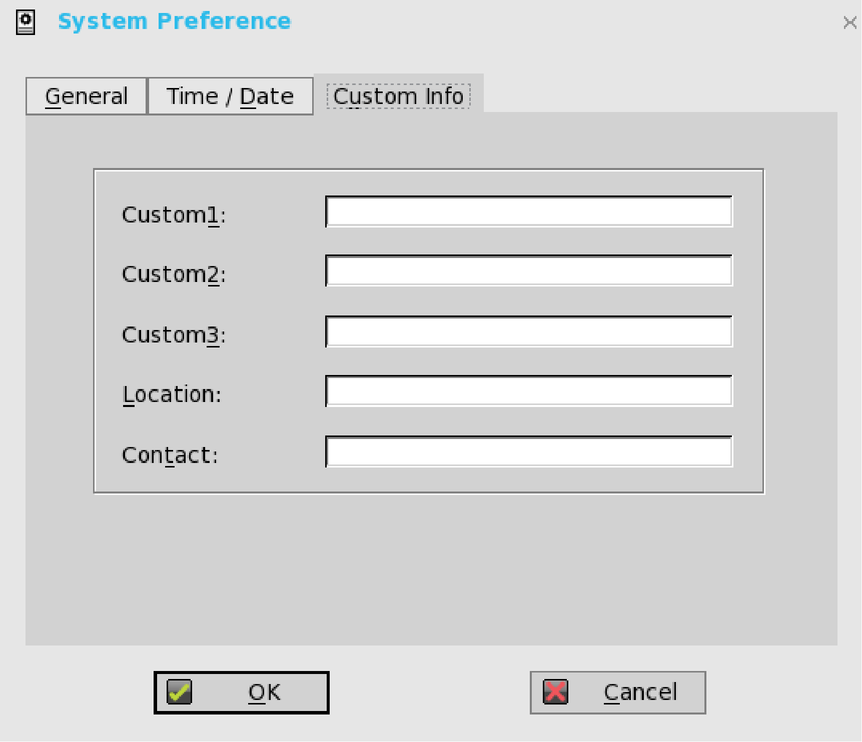
Setting the custom information

Use 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.
To set the custom information:

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

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

2 Click 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. 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 thin client software, see WDM documentation.



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

Configuring the display setup

The multi-display setup is a new feature introduced in ThinOS 8.5.1 release to support multiple monitors. Use the **Display Setup** dialog box to configure the display settings for the connected monitors.
To configure the display setup:

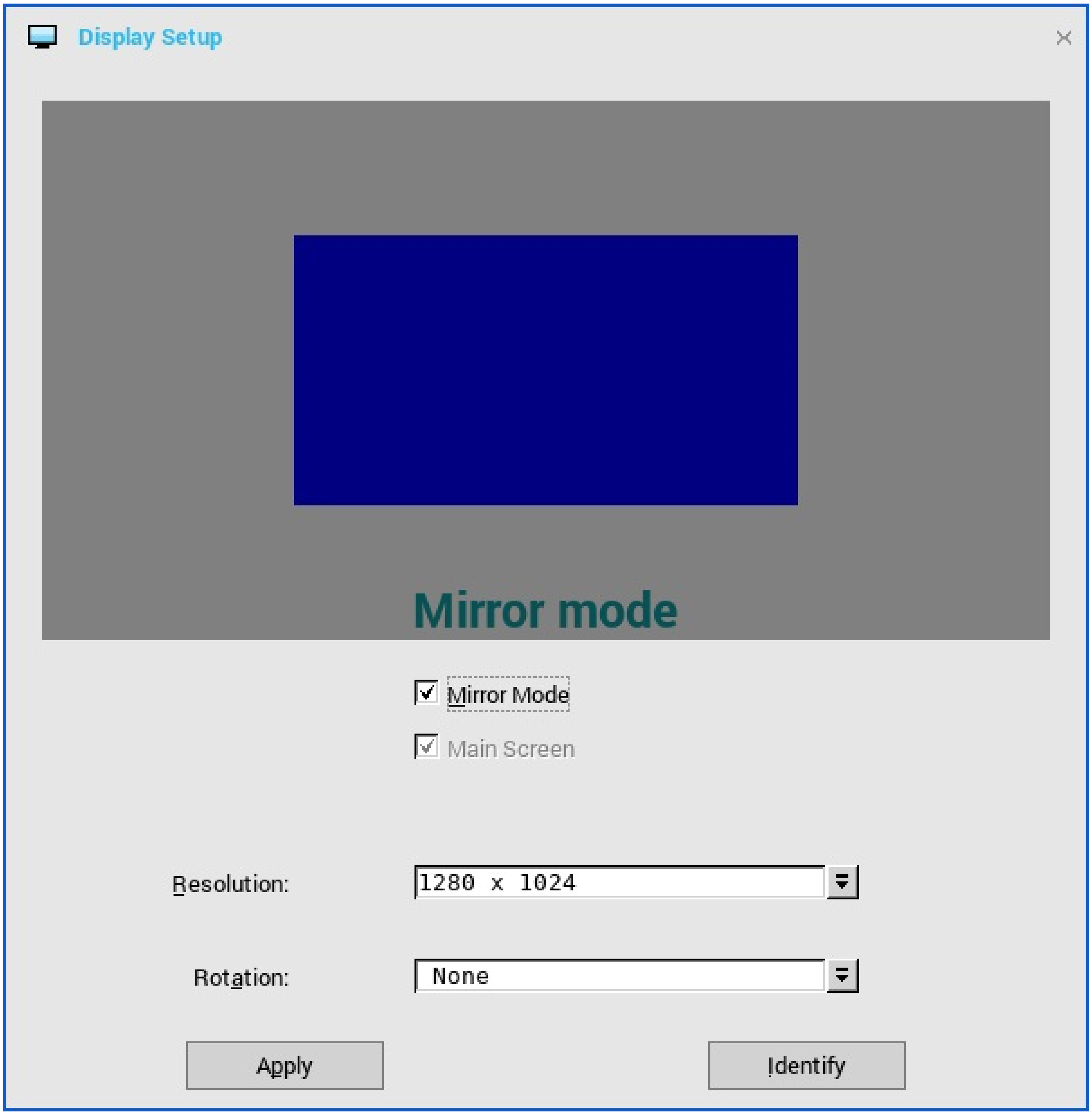
1 From the desktop menu, click **System Setup**, and then click **Display**.

The **Display Setup** dialog box is displayed.

2 In the **Display Setup** dialog box, configure the following options:

- **Mirror mode**—Select the **Mirror mode** check box to enable all connected monitors to use the same display settings configured on the primary monitor.

  The following screen represents the Mirror mode configuration.



Display Setup

Mirror mode

☑ Mirror Mode

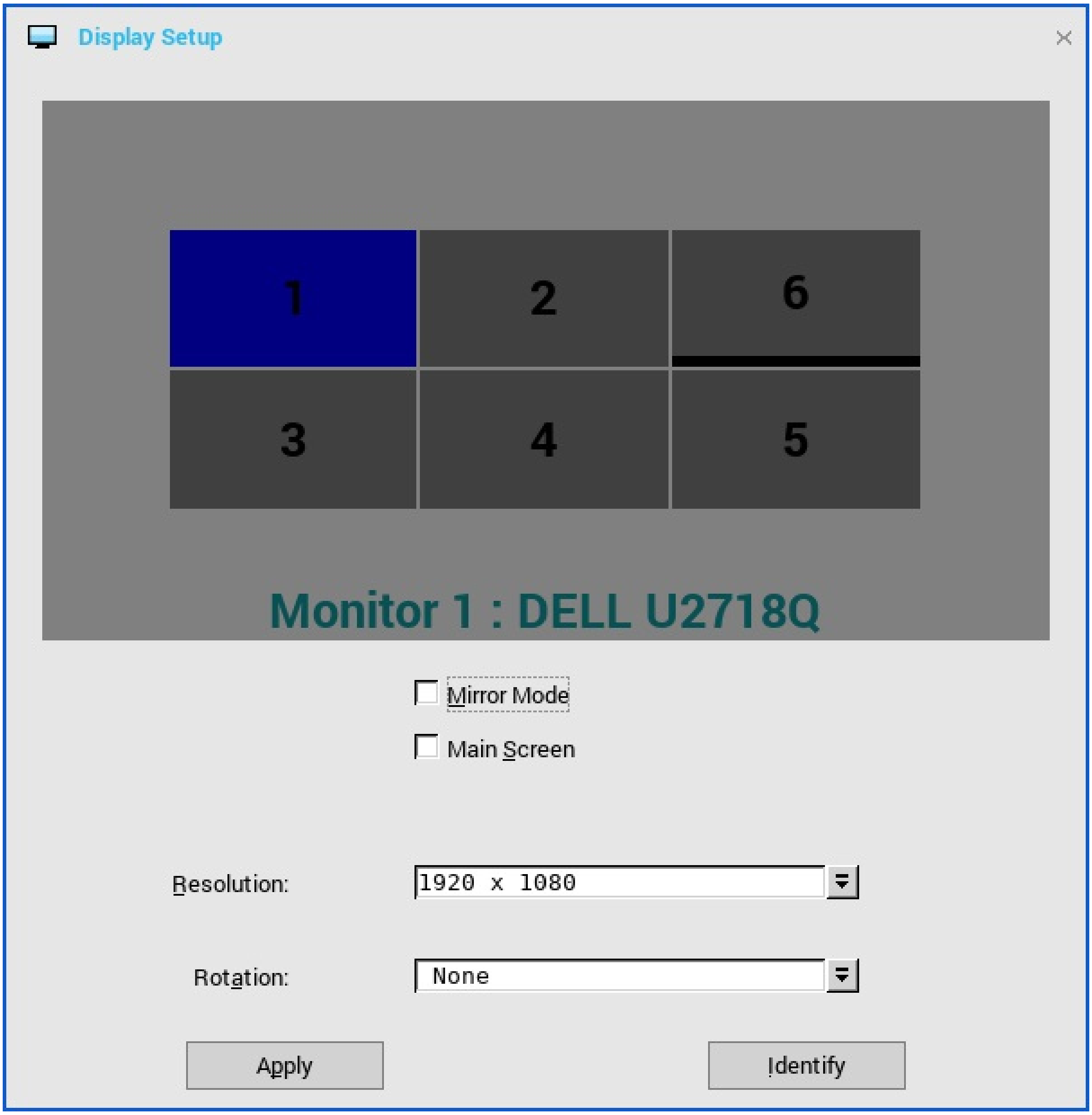
☑ Main Screen

Resolution: 1280 x 1024

Rotation: None

Figure 15. Display settings

If you clear the **Mirror mode** check box, the **Span Mode** is enabled. The following screen represents the span mode configuration.



Monitor 1 : DELL U2718Q

□ Mirror Mode

□ Main Screen

Resolution: 1920 x 1080

Rotation: None

Figure 16. Display settings

Blocks displayed on the screen represent the number of monitor screens connected to the thin client. Each block represents a single monitor screen.

Every monitor contains a unique display order number and display configuration. You can move the blocks horizontally or vertically and construct the multi-display layout in mixed directions. To construct a new display layout, move the blocks to your preferred position, and click **Apply**. A new display layout is created. However, the system sets the block to its default position if the block is moved to an incorrect position.

NOTE: Wyse 5070 Extended thin client supports up to six monitors.

- **Main screen**—Select the **Main screen** check box to set the monitor as primary monitor or main screen. To set a monitor as main screen, click the monitor block, and select the **Main screen** check box. After you set the monitor as main screen, the monitor block is highlighted with an underline, and the **Main screen** option is disabled for that monitor block. The **Main screen** option is available for other monitor blocks.

NOTE: Main screen option is effective only in Span Mode and always disabled in Mirror Mode.

- **Resolution**—From the **Resolution** drop-down list, select a display resolution supported by your monitor.

  In **Mirror Mode**, the resolution list is derived from the intersection of resolutions in all connected monitors.

  In **Span Mode**, select a monitor block and change its resolution from the **Resolution** drop-down list.
- **Rotation**—From the **Rotation** drop-down list, select an option to rotate the monitor screen in different directions—**Left turn 90 degrees** or **Right turn 90 degrees**. By default, the option is set to **None**.

3 Click **Apply**.

The new display settings are applied, and you can view the modified display.

4 Click **OK** to confirm the new settings.

ⓘ **NOTE: Use the Identify option, to know the display order number of the connected monitors.**

Hardware capability

This section describes the hardware capability for display.

Table 18. Port preferences

Model	Summary
Wyse 5070 thin client with Celeron processor	• On Wyse 5070 thin client without wireless module, the optional port can be used as second RJ-45, SFP, VGA, or second serial port. • On Wyse 5070 thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP. • When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive.
Wyse 5070 thin client with Pentium processor	• On Wyse 5070 thin client without wireless module, the optional port can be used as second RJ-45, SFP, VGA, or second serial port. • On Wyse 5070 thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP. • Back headset is disabled if front headphone is used. • When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive. • When VGA monitor is connected on VGA optional port, DisplayPort 3 becomes inactive.
Wyse 5070 Extended thin client	• On Wyse 5070 Extended thin client without wireless module, the optional port can be used as second RJ-45, SFP, or VGA. • On Wyse 5070 Extended thin client with wireless module, the optional port cannot be used as second RJ-45 or SFP. • Back headset is disabled if front headphone is used. • When monitor is connected on USB Type-C port, DisplayPort 2 becomes inactive. • When VGA monitor is connected on VGA optional port, DisplayPort 3 becomes inactive. • Power option is available on the first serial port. • PCIe slot is available.

Wyse 5070 thin client with Celeron processor

Table 19. Display matrix

Number of displays	Supported display resolution	
	4K resolution 3840 x 2160 @ 60 Hz	Non-4K resolution Up to 2560 x 1600 @ 60 Hz
One display	Yes	Yes

Number of displays	Supported display resolution	
Two displays	Yes	Yes
Three displays	No[1]	Yes[2]

[1] VGA port does not support 4K display. However, it supports a display with 1080p screen resolution.

[2] For non-4K displays, screen resolution up to 2560 x 1600 @ 60 Hz is supported on all ports except VGA. VGA port supports only 1080p resolution.

Table 20. Ports

Ports	DP1	DP2	VGA	USB Type-C
Monitor priority	1	2B[1]	3	2A[1]
4K display	Yes	Yes	No[2]	Yes
Non-4K display	Yes	Yes	Yes[2]	Yes

[1] DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

[2] VGA port supports only 1080p resolution.

NOTE: 4K resolution @ 60 Hz on USB-C type port is tested using the Type-C to HDMI and DP adapters. Dell monitor S2718D with USB type-C port supports up to 2560 x 1440 resolution.

Wyse 5070 thin client with Pentium processor

Table 21. Display matrix

Number of displays	Supported display resolution	
	4K resolution 3840 x 2160 @ 60 Hz	Non-4K resolution Up to 2560 x 1600 @ 60 Hz
One display	Yes	Yes
Two displays	Yes	Yes
Three displays[1]	Yes	Yes

[1] Dell recommends that you configure a maximum of two displays with 4K resolution and the third display with non-4K resolution on DisplayPort 3 for optimized stability and performance. However, based on the maximum technical capability of Wyse 5070 thin client with Pentium processor, ThinOS supports a maximum of three 4K displays.

Table 22. Ports

Ports	DP1	DP2	DP3	VGA	USB Type-C
Monitor priority	1	2B[1]	3B[2]	3A[2]	2A[1]
4K display	Yes	Yes	Yes	No[3]	Yes
Non-4K display	Yes	Yes	Yes	Yes[3]	Yes

[1] DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

[2] DP3 and VGA port are mutually exclusive with VGA port taking higher priority.

[3] VGA port supports only 1080p resolution.

ⓘ **NOTE: 4K resolution @ 60 Hz on USB-C type port is tested using the Type-C to HDMI and DP adapters. Dell monitor S2718D with USB type-C port supports up to 2560 x 1440 resolution.**

Wyse 5070 Extended thin client with AMD GPU

Table 23. Wyse 5070 Extended thin client with AMD GPU

Number of displays	Supported display resolution	
	4K resolution 3840 x 2160 @ 60 Hz	Non-4K resolution Up to 2560 x 1600 @ 60 Hz
One display	Yes	Yes
Two displays	Yes	Yes
Three displays[1]	Yes	Yes
Four displays[2]	Yes	Yes
Five displays[2]	Yes	Yes
Six displays[2]	Yes[2]	Yes

[1] For three displays, Dell recommends that you configure the first two 4K displays on the main board (DP1~DP3), and the third 4K display on AMD GPU card.

[2] Dell recommends that you configure a maximum of four displays with 4K resolution and the remaining displays with non-4K resolution on DisplayPort 3 and DisplayPort 6 for optimized stability and performance. However, based on the maximum technical capability of Wyse 5070 Extended thin client, ThinOS supports a maximum of six 4K displays.

ⓘ **NOTE: Best practice—To achieve maximum 4K display output, Dell recommends setting up 1080p on the DisplayPort 3, with rest of the monitors in 4K resolution to optimize performance.**

Table 24. Ports

Ports	DP1	DP2	DP3	VGA	USB Type-C	mDP4	mDP5	DP6
Monitor priority	1	2B[1]	3B[2]	3A[2]	2A[1]	4	5	6
4K display	Yes	Yes	Yes	No[3]	Yes	Yes	Yes	Yes
Non-4K display	Yes	Yes	Yes	Yes[3]	Yes	Yes	Yes	Yes

[1] DP2 and USB Type-C port are mutually exclusive with USB Type-C port taking higher priority.

[2] DP3 and VGA port are mutually exclusive with VGA port taking higher priority.

[3] VGA port supports only 1080p resolution.

ⓘ **NOTE: 4K resolution @ 60 Hz on USB-C type port is tested using the Type-C to HDMI and DP adapters. Dell monitor S2718D with USB Type-C port supports up to 2560 x 1440 resolution.**

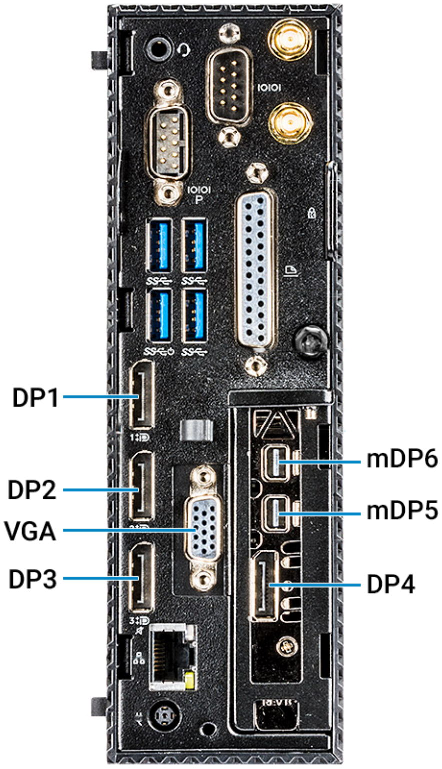


Figure 17. Ports on Wyse 5070 Extended thin client

Display priority—The following order defines the display priority set on ThinOS for Wyse 5070 Extended thin client:

- DP1 > DP2 > DP3 > DP4 > mDP5 > mDP6
- DP1 > USB Type-C > DP3 > DP4 > mDP5 > mDP6
- DP1 > DP2 > VGA > DP4 > mDP5 > mDP6
- DP1 > USB Type-C > VGA > DP4 > mDP5 > mDP6

NOTE: Display cable hot plug—Screen layout settings are changed based on supported display resolution and the port to which the monitor is plugged in.

NOTE: Earlier in ThinOS zero theme, the Display Setup window was aligned with left-hand setting panel. In current scenario, the Display Setup window is positioned to center of the screen regardless of Classic/Zero mode. This enhancement is made to easily configure the display setup along with the confirmation window.

Known issues

- Hot plugging a monitor may result in a black screen in the VDI connected session. To recover the session screen, you must power off the monitor, and then power on the monitor. This issue will be resolved in the next release.
- Hot plugging a monitor during VDI connection or display setup configuration may result in unexpected issues, such as terminal freeze or display layout change. This issue will be resolved in the next release.

Configuring the peripherals settings

The **Peripherals** dialog box enables you to configure the settings for the Keyboard, Mouse, Audio, Serial, Camera, Touch Screen, and Bluetooth.

- Configuring the keyboard settings
- Configuring the mouse settings
- Configuring the audio settings
- Configuring the serial settings
- Configuring the camera settings
- Configuring the touch screen settings
- Configuring the bluetooth settings

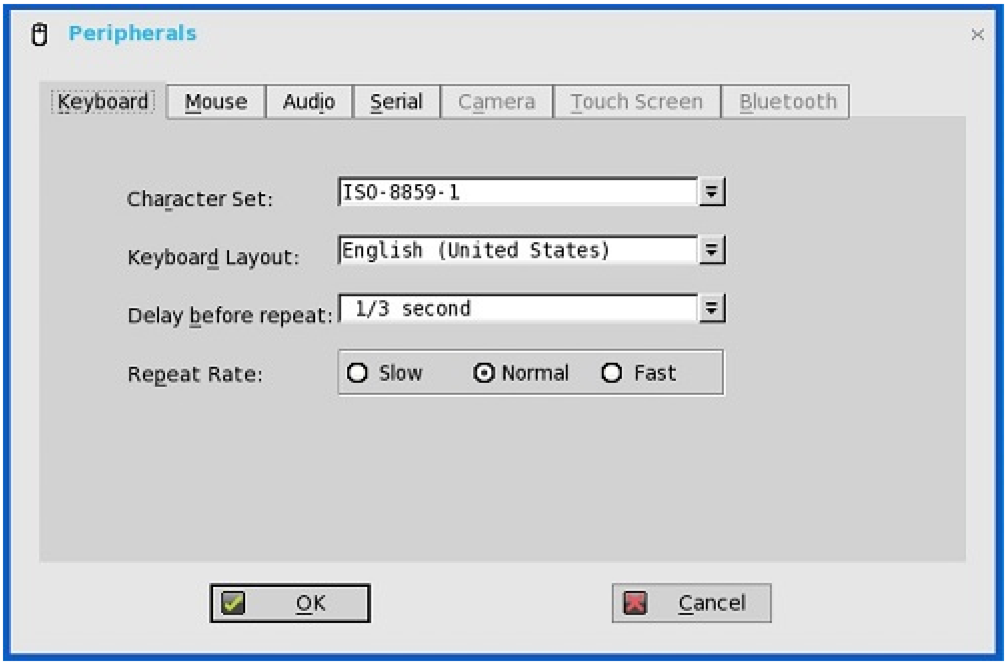
Configuring the keyboard settings

To configure the keyboard settings:

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

The **Peripherals** dialog box is displayed.

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



Character Set: ISO-8859-1

Keyboard Layout: English (United States)

Delay before repeat: 1/3 second

Repeat Rate: ○ Slow ● Normal ○ Fast

Table 25. Keyboard settings

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

Parameter	Description
	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.

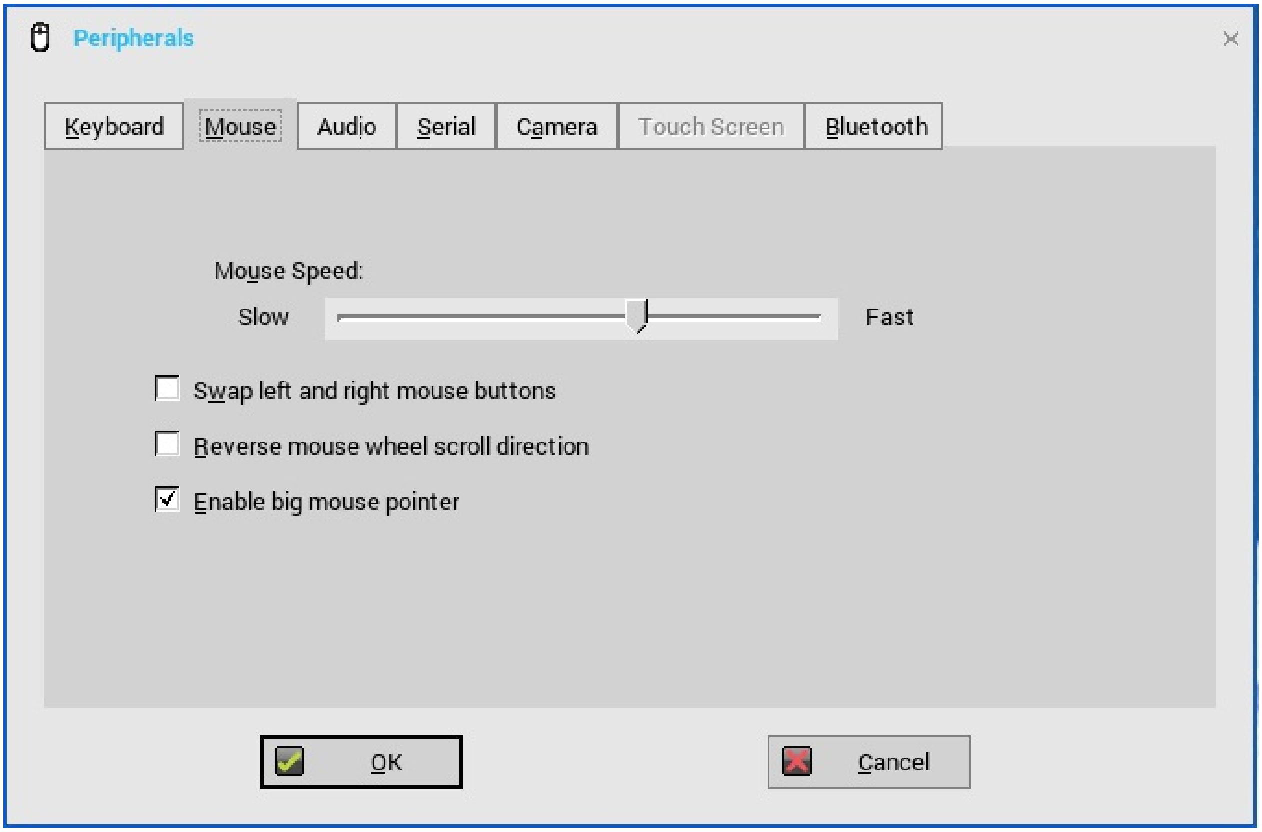
Configuring the mouse settings

To configure the mouse settings:

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

The **Peripherals** dialog box is displayed.

2 Click the **Mouse** tab to select the mouse speed and mouse orientation.



Peripherals

Keyboard | Mouse | Audio | Serial | Camera | Touch Screen | Bluetooth

Mouse Speed:

Slow Fast

☐ Swap left and right mouse buttons

☐ Reverse mouse wheel scroll direction

☑ Enable big mouse pointer

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 Select the **Enable big mouse pointer** check box to increase the size of the local mouse pointer by two times.

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

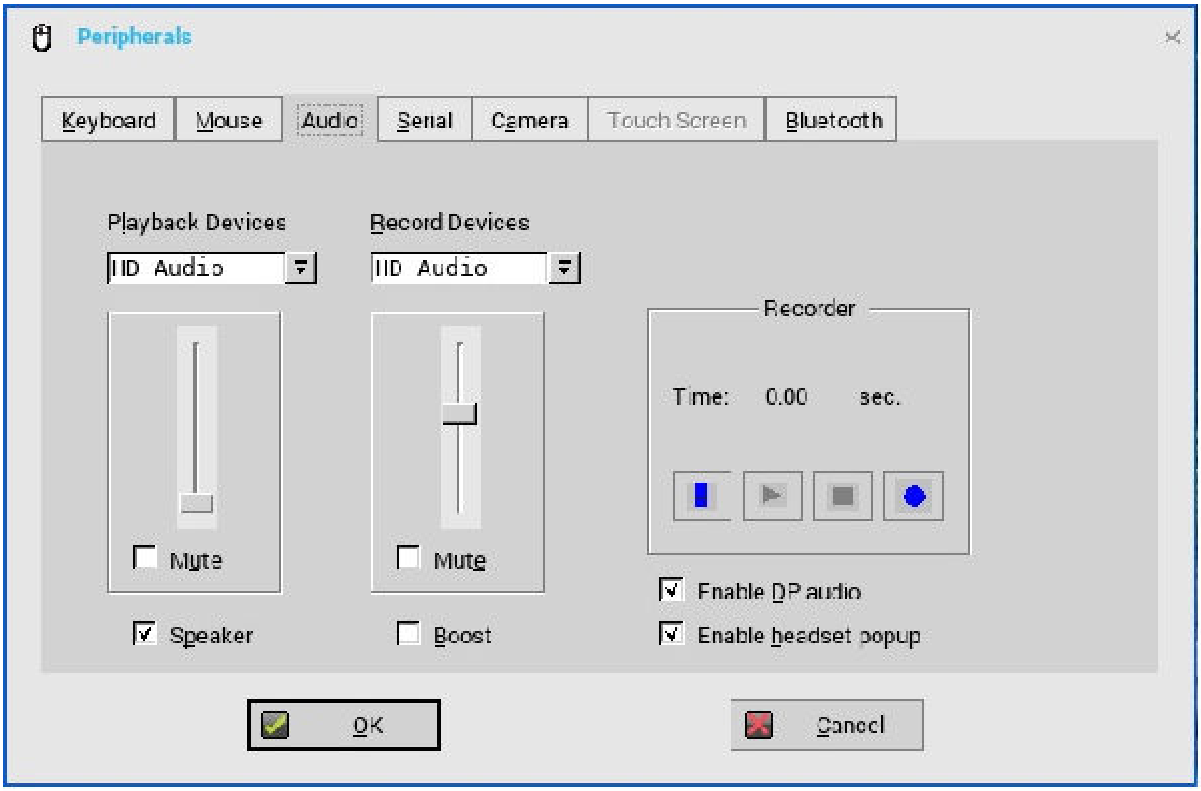
Configuring the audio settings

To configure the audio settings:

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

The **Peripherals** dialog box is displayed.

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



Playback Devices: HD Audio

Record Devices: HD Audio

□ Mute

□ Mute

Time: 0.00 sec.

☑ Speaker

□ Boost

☑ Enable DP audio

☑ Enable headset popup

Figure 18. Audio tab

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

- If the HD audio and DP audio options are available in playback devices, the thin client determines the priority between HD audio and DP audio when the DP cable is connected. In this scenario, select the playback device type that is based on your preference, and click **OK**. The playback device which you select takes the priority.
- 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 list.

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

c Click **Play** to play the audio.

d Use the **Recorder** tab and do the following:

- Collect information about the speaker and microphone being used.
- Examine the performance of the speaker and microphone being used.

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.

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

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

g Select the **Enable DP audio** check box to enable the DisplayPort audio function on your thin client.

h 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 ThinOS INI Reference Guide*.**

For information about the known issues, see the latest *Dell Wyse ThinOS Release Notes*.

Using DisplayPort audio

Use the DisplayPort (DP) interface to connect your thin clients to the display devices. The interface can include audio signals in the same cable as the video signals. To enable the DisplayPort audio, ensure that you set up the following components:

- A thin client that supports DisplayPort audio and/or dual mode with audio.
- A display device, such as monitor, that supports audio playback in ICA, RDP, Blast, or the PCoIP sessions.
- An analog audio device or a monitor built-in speaker.

On Wyse 5070 thin client, the DisplayPort audio is supported only on DisplayPort 1 and DisplayPort 2. To enable the DisplayPort audio on ThinOS:

1 Set up a monitor with DP audio support.

2 Connect the ThinOS client to monitor using the DP cable.

3 Plug the analog headset into the monitor DP audio interface.

4 On the ThinOS desktop, click **System Setup** > **Peripherals** > **Audio** > **Playback devices**, and select the **Enable DP audio** check box.

5 Start either an RDP, ICA, PCoIP, or Blast session.

6 Play a video, and check the audio output using the analog headset.

ⓘ **NOTE: ThinOS supports only the DisplayPort audio playback. Audio recording using DisplayPort is not supported.**

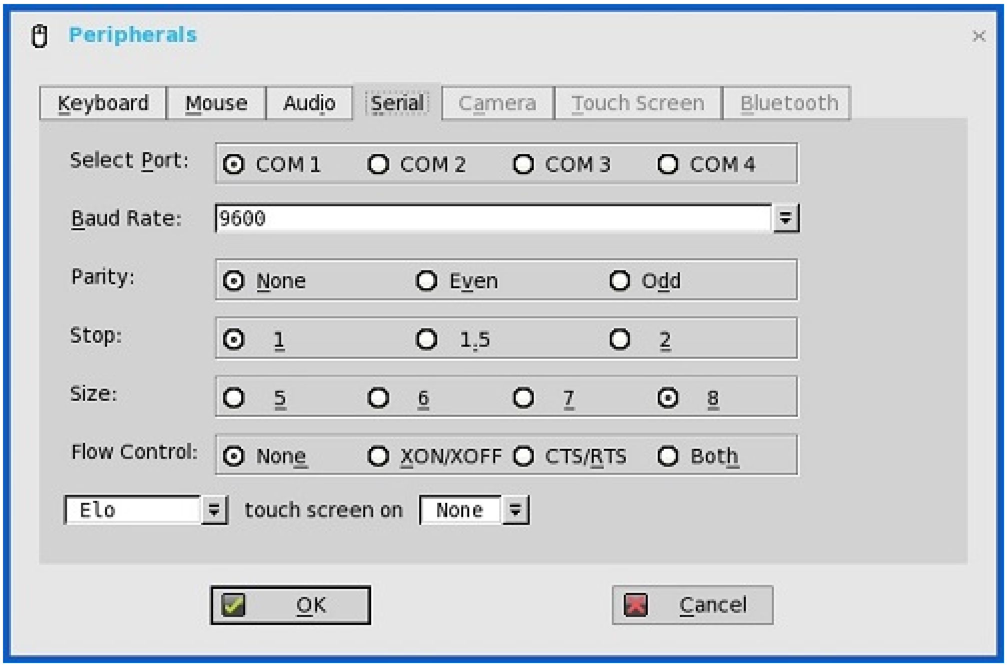
Configuring the serial settings

To configure the Serial settings:

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

The **Peripherals** dialog box is displayed.

2 Click the **Serial** tab and do the following:



Select Port: ● COM 1 ○ COM 2 ○ COM 3 ○ COM 4

Baud Rate: 9600

Parity: ● None ○ Even ○ Odd

Stop: ● 1 ○ 1.5 ○ 2

Size: ○ 5 ○ 6 ○ 7 ● 8

Flow Control: ● None ○ XON/XOFF ○ CTS/RTS ○ Both

Elo touch screen on None

a **Select Port**—Click the button to select the Port. Default is **COM 1**.

b **Baud Rate**—Select the Baud Rate from the drop-down list. Default is **9600**.

c **Parity**—Click the button to select the Parity.

d **Stop**—Click the button to select the stop bits **1, 1.5, 2**. Default value is **1**.

e **Size**—Click the button to select the Character size **5**, **6**, **7**, or **8** bits. **Default is 8.**

f **Flow Control**—Click the button to select Flow Control: Either **None**, **XON/XOFF**, **CTS/RTS**, or **Both** can be selected. Default is None.

g **Serial Touch Screen selections**—Select the required touch screen from the drop-down list. Available options are ELO, MicroTouch and FastPoint.

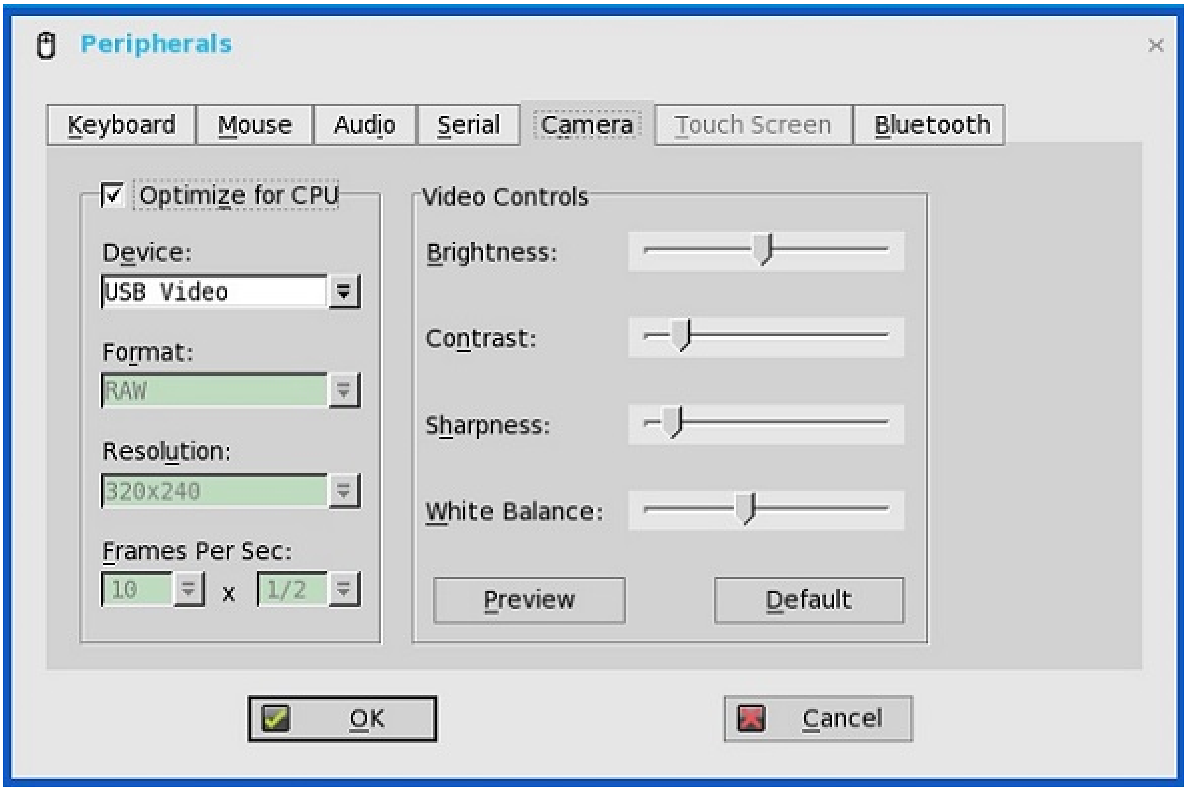
h **Touch Screen on**—Select the required serial port (COM port) or **None** from the drop-down list.

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

Configuring the camera settings

Use the **Camera** tab to interface with cameras that are locally connected to the thin client (USB) and supported by a UVC driver. When using the HDX RealTime webcam feature of XenDesktop/XenApp, 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.



☑ Optimize for CPU

Device: USB Video

Format: RAW

Resolution: 320x240

Frames Per Sec: 10 x 1/2

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 thin client (if the webcam supports Universal Video Driver).

Also, this feature is CPU intensive and is recommended for high performance products.

Configuring the touch screen settings

Use the **Touch Screen** tab to configure touch screens that are connected to the thin client. The tab is available (not grayed out) when the thin 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 version 8.5, the ELO touch screen does not work in certain scenarios. For more information, see the latest Dell Wyse ThinOS Release Notes.**

Configuring the Bluetooth settings

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

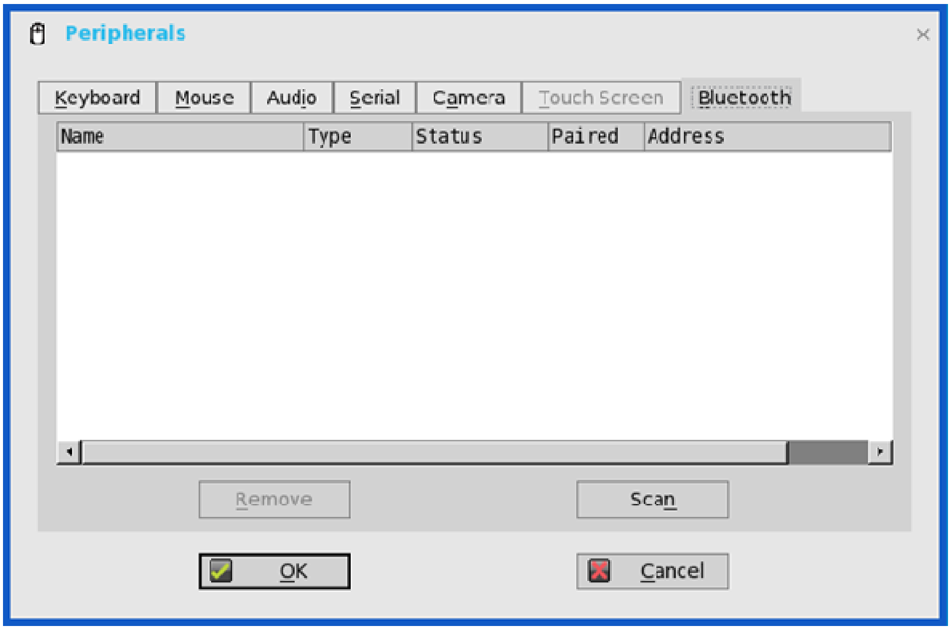
ThinOS supports Intel Dual Band Wireless AC 9560 chipset. For mouse, keyboard, and headset, ThinOS supports both Bluetooth 3.0 and 4.0.

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 desktop menu, click **System Setup**, and then click **Peripherals**.

The **Peripherals** dialog box is displayed.



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

Bluetooth enabled devices, such as headsets and mouses that are available in the thin client environment are listed in the **Bluetooth** page. The following attributes are displayed in the list:

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

  Both **Human Interface Devices (HID)** and **Headset** Bluetooth devices are supported.

  - **HID** type
    - HID includes mouse and keyboard.
    - The maximum number of HIDs that can be connected is seven.
  - **Headset** type
    - The 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 are still not supported.**

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

  Table 26. Bluetooth status

Attribute	Value	Summary
Status	Connected	The Bluetooth device is connected to the ThinOS device. It is ready to be used.
	Connecting	The Bluetooth device is connecting to the ThinOS device.
	Disconnected	The Bluetooth device is not connected to the ThinOS device.
Paired	Yes	The Bluetooth device is paired with the ThinOS device.
	No	The Bluetooth device is not paired with the ThinOS device.

- **Address**—Displays the address of the Bluetooth device connected to your thin client.

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

Table 27. User scenario

User scenario	Status
Device turned off	Disconnected | Paired
Device turned on	Connected | Paired
Device disconnected from ThinOS	Disconnected | Not Paired

- **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.
- **Connect**—Select a particular Bluetooth enabled device, and click **Connect** to connect the selected device to the thin client. If the Bluetooth device is connected successfully, the status is displayed as **Connected** in the **Bluetooth** window.
- **Remove**—Select a particular Bluetooth device, and click **Remove** to disconnect and remove the device from the list.
- **Auto Connect function**—The Auto Connect function is designed for HIDs.
  - ThinOS has no HIDs connected such as USB or Bluetooth HIDs.
  - The Bluetooth HIDs are configured as Page Scan mode.

  When you start the ThinOS client, the Bluetooth HIDs can connect to ThinOS automatically without scanning or pairing operations. The Bluetooth HIDs automatically reconnect after you restart the ThinOS client.
- **Reconnect function**—The Reconnect function is designed for HIDs and headsets.

  When you restart the system with the Bluetooth device (HID/headset) that is already paired and connected, the Bluetooth device automatically reconnects within a few seconds.

  For example, you can hover the Bluetooth mouse, and then click a few times for the Bluetooth mouse 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, see the latest Dell Wyse ThinOS release notes.

Known issues of the Bluetooth feature

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

   Workaround—Dell recommends using one mouse and one keyboard in ThinOS with Bluetooth connection.
2. The Bluetooth device name displays N/A sometimes.

   Workaround—Remove this device from the list and rescan.
3. Only supports volume button and mute button on Bluetooth headset.
4. The performance of Bluetooth feature is low during wireless connection.
5. A black or flickering screen is observed when you connect a 4K monitor to DP1 port on Wyse 5070 thin client with Intel Dual Band Wireless AC 9560 chipset. This is applicable to ThinOS 8.5_107 build.

   Workaround—Configure the display resolution to less than 4K resolution on monitor connected to DP1 port. This is specific to DP1 port and independent of the devices connected to other ports.
6. After reboot, you cannot reconnect the Bluetooth headsets, and you must reboot headsets to reconnect. This functionality works as designed by Intel.

   Workaround—Reopen the Bluetooth headset to reconnect.
7. After restoring the thin client to factory default settings, the Bluetooth connection may fail when you connect to a Bluetooth device the first time. However, the thin client connects to the Bluetooth device from second instance onwards.
8. When you initialize the Bluetooth, the screen flickers black only once before disconnecting the client from its power source and turning on the client again (power cycling).

   This is applicable to ThinOS 8.5_108 build. This issue will be fixed in next release.

USB support

USB port—USB 3.0 is compatible with USB 2.0. When USB 2.0 device is connected to 3.0 ports, the behavior of the device remains unaltered. For USB 3.0 device to connect to 3.0 ports, the device type should be of 5 Gbps. All types of USB devices work when connected to USB 3.0 port.

USB hard disk—Do not plug in the USB hard disk with 10 or more drives, or do not plug in more than 10 USB keys into ThinOS client. ThinOS does not detect the USB disk with 10 or more drives.

Known issue—Camera preview has some known issue.

Support for USB Type-C

Wyse 5070 thin client supports the USB Type-C port.

- The USB 3.1 Type-C connector can be used to perform the following activities:
  - Transfer data by using USB mass storage
  - Connect monitors

    ⓘ **NOTE: If you use USB Type-C, one monitor capability is reduced from rear panel, and DP2 is disabled.**
  - Charge smartphones
  - Connect USB 2.0, 3.0, and 3.1 compatible devices.
- The USB 3.1 Type-C cannot be used for the following:
  - Thunderbolt, HDMI, and MHL alt modes
  - Docking stations
  - Powering a thin client
- Limitation—In Wyse 5070 thin client, XHCI is used for all types of USB devices. The transmission speed gap between USB 3.0 and USB Type-C is not significant.

Configuring the printer settings

Use the **Printer Setup** dialog box to configure network printers and local printers that are connected to the thin client. Through its USB ports, a thin client can support multiple printers. If more than one printer is to be used and another port is not available on your thin 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
- Using the Help
- Configuring the Citrix UPD printer

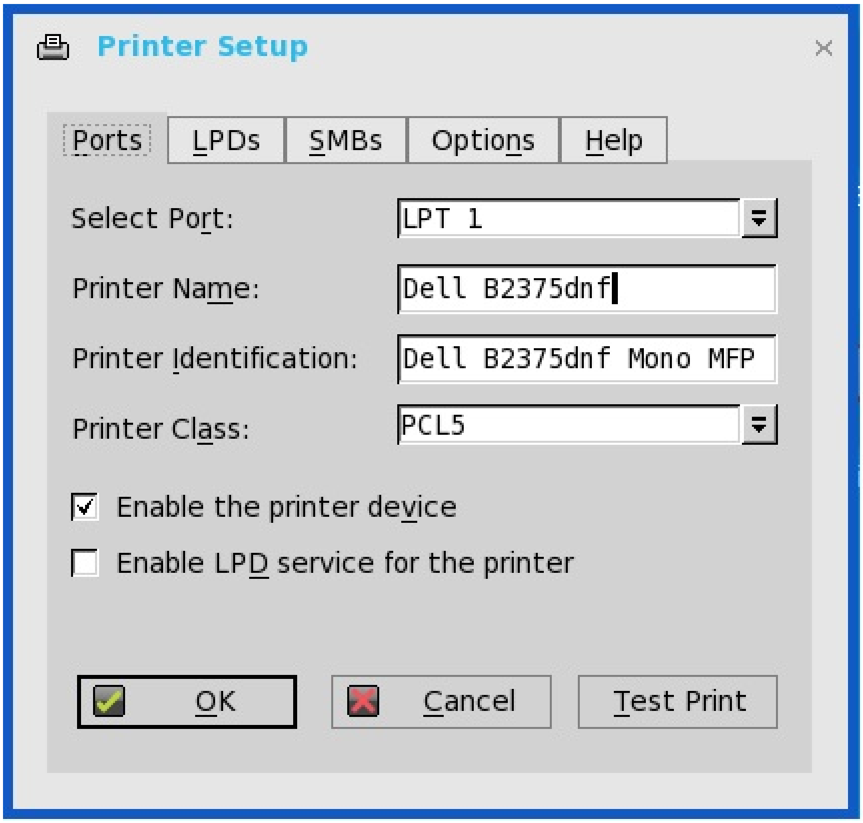
Configuring the ports settings

To configure the ports settings:

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

The **Printer Setup** dialog box is displayed.

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



Printer Setup

Ports | LPDs | SMBs | Options | Help

Select Port: LPT 1

Printer Name: Dell B2375dnf

Printer Identification: Dell B2375dnf Mono MFP

Printer Class: PCL5

☑ Enable the printer device

☐ Enable LPD service for the printer

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 allowed in the Printer Identification field is 31. If your printer driver string is more than 31 characters (including space), you can create a txt file (printer.txt) and upload to your file server. Edit the txt file and type the content, such as `"HP Color" = "HP Color LaserJet CM1312 MFP PCL6 Class Driver"`. Add the command line `printermap=printer.txt` to your wnos.ini file. Now, you can type `“HP Color”` in the Printer Identification field instead of the full driver string.**

d **Printer Class**— This is optional. Select the printer class from the list **PCL5**, **PS**, or **TXT** or **PCL4.**

e **Enable the printer device** — Select this option to enable the directly-connected printer. It enables the device to display on the remote host.

f **Enable LPD service for the printer** — Select this to make the thin client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network.

> NOTE:
>
> If the thin 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, see Configuring the Network Settings.

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

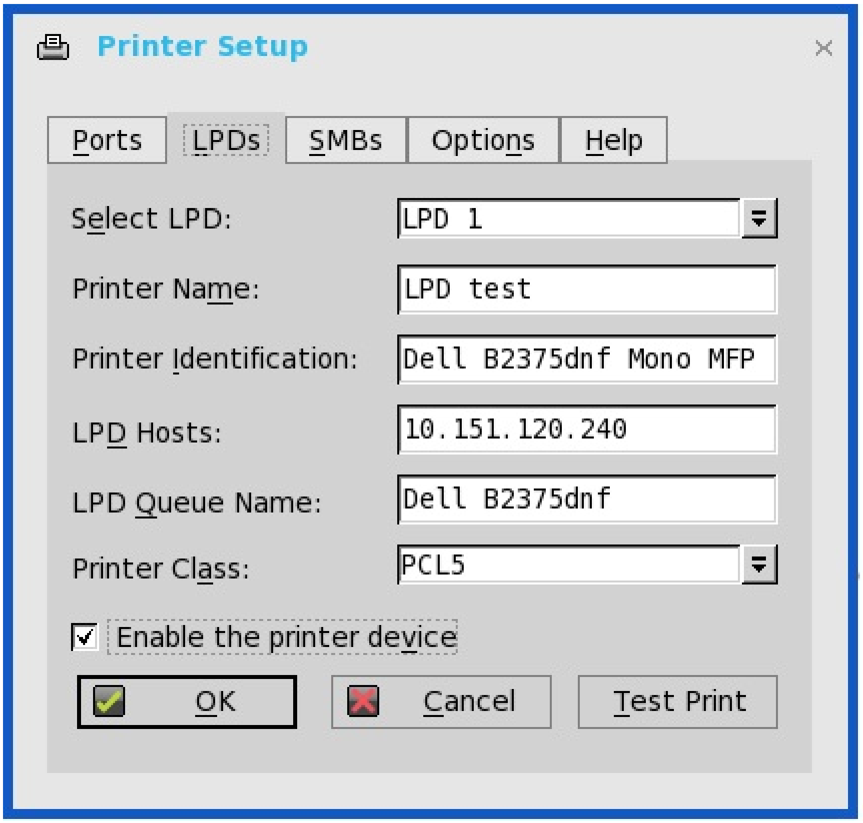
Configuring the LPDs settings

To configure the LPDs settings:

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

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:



Select LPD: LPD 1

Printer Name: LPD test

Printer Identification: Dell B2375dnf Mono MFP

LPD Hosts: 10.151.120.240

LPD Queue Name: Dell B2375dnf

Printer Class: PCL5

☑ Enable the printer device

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 thin client on your network, the entry in the LPD Hosts box is the name or address of that thin 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 thin client on your network, the LPD Queue Name must match the content of the Printer Name box on the thin 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 one session and you cannot access the LPD service host, then the TCP connection tries to connect to the LPD service host. The timeout period is 60 seconds. During this timeout period, if you try to close the session, the session waits until the LPD printer connection is established. The initialization failure logs are displayed.

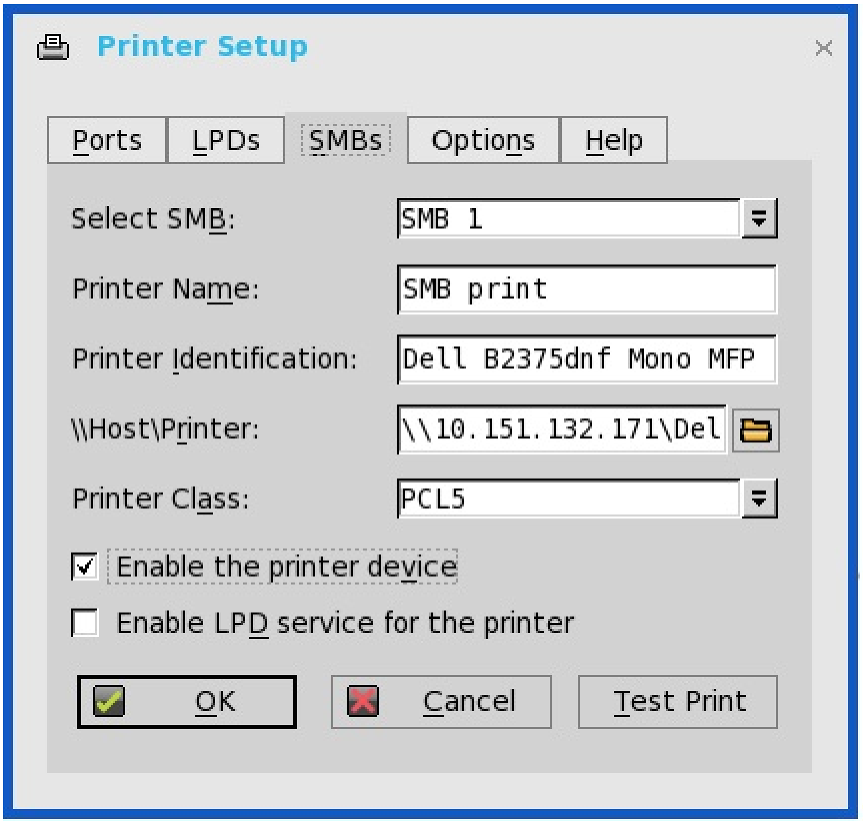
Configuring the SMBs settings

To configure the SMBs settings:

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

The **Printer Setup** dialog box is displayed.

2 Click **SMBs** tab, and use the following guidelines when printing to a Windows network printer.



Select SMB: SMB 1

Printer Name: SMB print

Printer Identification: Dell B2375dnf Mono MFP

\\Host\Printer: \\10.151.132.171\Del

Printer Class: PCL5

☑ Enable the printer device

☐ Enable LPD service for the printer

a **Select SMB**—Select the SMB you want from the list.

b **Printer Name**—(Required) Enter the name 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.

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 thin client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network, see Using Your Thin Client as a Print Server (LPD).

If the thin 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 thin client as described in Configuring the Network Settings.

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

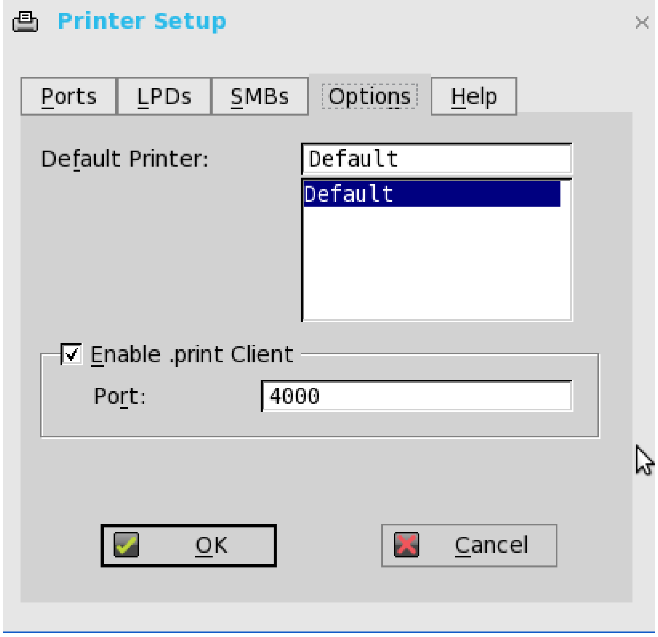
Using the printer setup options

To configure the printer setup options:

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

The **Printer Setup** dialog box is displayed.

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



Default Printer: Default

Default

☑ Enable .print Client

Port: 4000

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**.

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

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

Resetting to factory defaults using G-Key reset

High-privileged or stand-alone users can reset the thin client to factory default settings using the G-key reset feature.

To reset the thin client to factory default settings, restart the thin 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 Lock down mode.**

Resetting to factory defaults using shutdown reset

A high-privileged or stand-alone user can reset the thin client to factory default settings from the **Shutdown** dialog box.
To reset the thin client to factory defaults:

1. From the desktop menu, click **Shutdown**.

   The **Shutdown** dialog box is displayed.
2. After starting your thin client you will see a **Dell logo** for a short period of time.
3. Click **Restart the system** to restart your thin 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 lock down 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 thin client restarts. To correct this, power-on the thin client while continuously tapping the **V** key. This will restart the thin client with a default/automatic display resolution.

Performing diagnostics

Diagnostics include:

- System tools
- Using the troubleshooting options

System tools

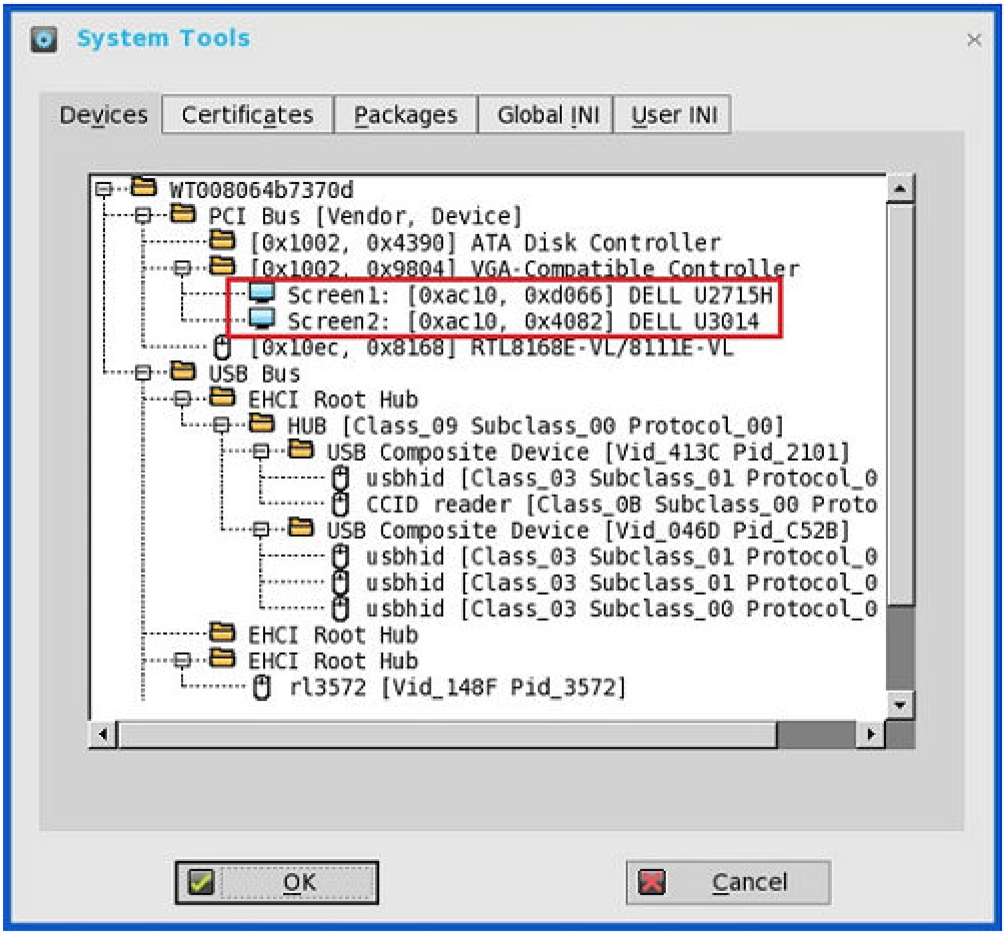
Use the **System Tools** dialog box to view device details, package details and Global INI/User INI information. You can also import certificates using the **Certificates** tab.

1 From the desktop 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 thin client are also displayed.

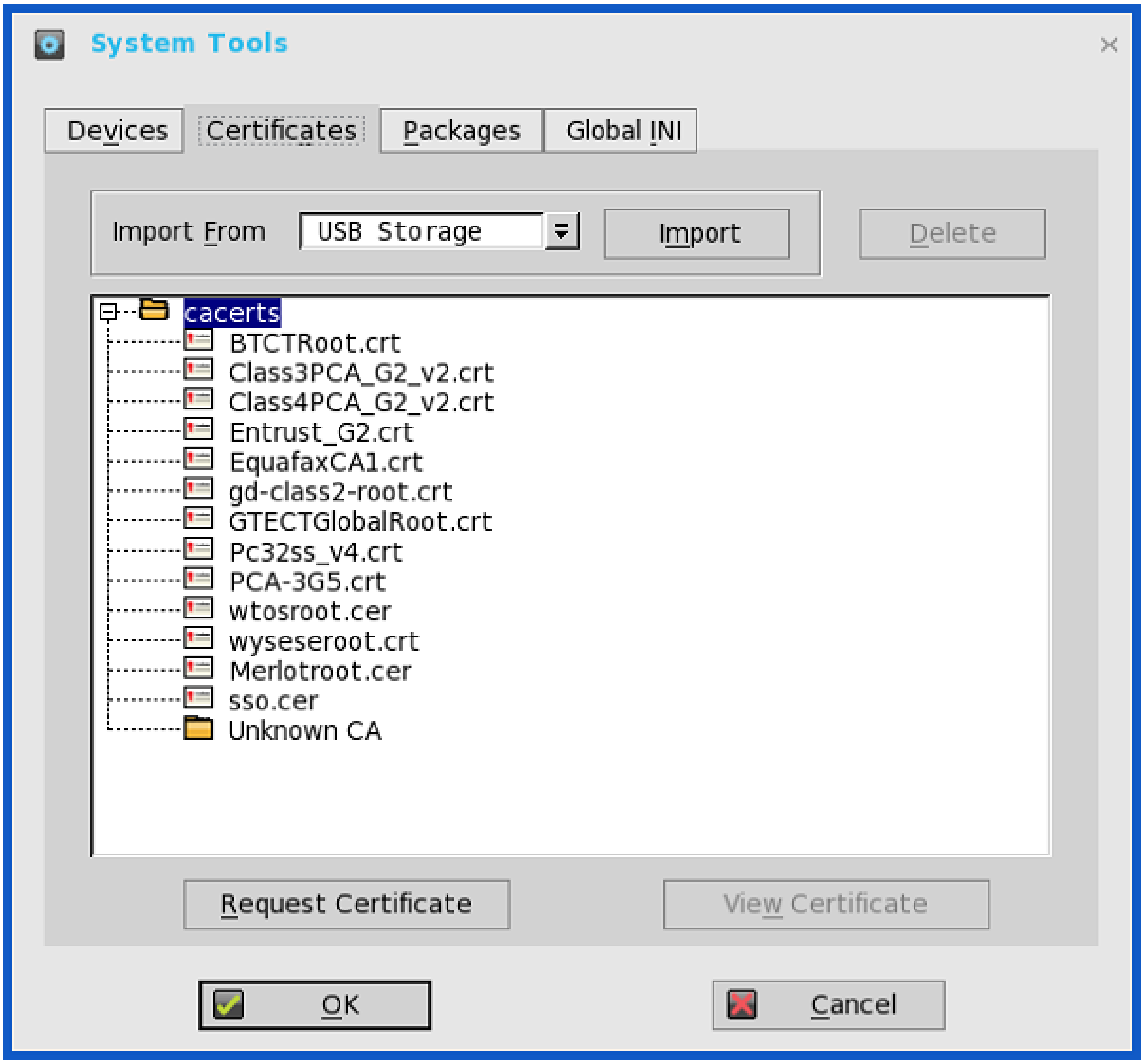
The Device Viewer button was previously available in the **Devices** tab of the **System Information** dialog box.



```
WT008064b7370d
    PCI Bus [Vendor, Device]
        [0x1002, 0x4390] ATA Disk Controller
        [0x1002, 0x9804] VGA-Compatible Controller
            Screen1: [0xac10, 0xd066] DELL U2715H
            Screen2: [0xac10, 0x4082] DELL U3014
        [0x10ec, 0x8168] RTL8168E-VL/8111E-VL
    USB Bus
        EHCI Root Hub
            HUB [Class_09 Subclass_00 Protocol_00]
                USB Composite Device [Vid_413C Pid_2101]
                    usbhid [Class_03 Subclass_01 Protocol_0
                    CCID reader [Class_0B Subclass_00 Proto
                USB Composite Device [Vid_046D Pid_C52B]
                    usbhid [Class_03 Subclass_01 Protocol_0
                    usbhid [Class_03 Subclass_01 Protocol_0
                    usbhid [Class_03 Subclass_00 Protocol_0
        EHCI Root Hub
        EHCI Root Hub
            rl3572 [Vid_148F Pid_3572]
```

ⓘ **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:



Import From: USB Storage

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 the default certificates, see About default certificates.

d Click **Request Certificate** to manually request certificate for your client. For more information about Simplified Certificate Enrollment Protocol, see Simplified Certificate Enrollment Protocol.

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

ThinOS packages that are installed on thin client are listed in the **Packages** tab.

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 displayed in the **Package** tab:

- `base.i386.pkg`
- `FR.i386.pkg`—This package is introduced to support Flash Redirection.
- `RTME.i386.pkg`—This package is introduced to support Citrix RTME.
- `Horizon.i386.pkg`—This package is introduced to support VMware Blast protocol. The package version number is updated to match the latest Horizon client.

To install this package, PKG installation INI file needs to be changed to `AddPkg=“horizon”`.

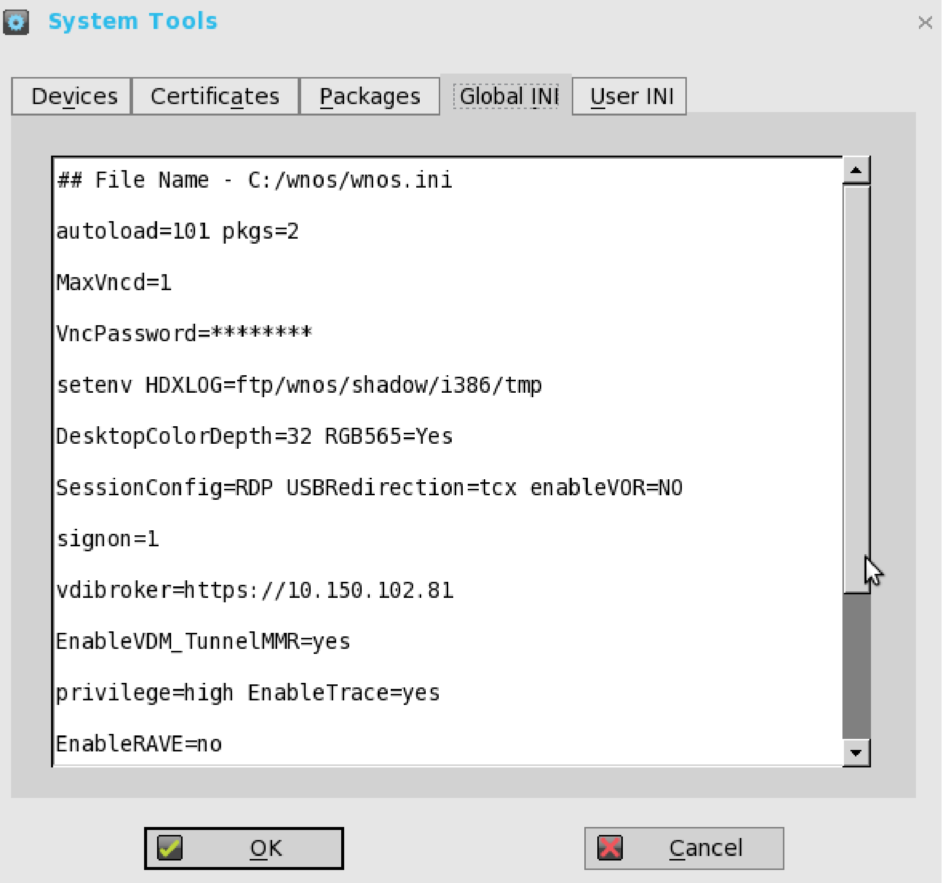
- `pcoip.i386.pkg`—This package is available only on PCoIP clients.
- `TCX.i386.pkg`—This package is introduced to support TCX.

You cannot delete the base package separately. If you click **Delete All**, all packages are deleted including the base package. When you click **Delete All**, a message is displayed prompting you to restart the device.

The `base.i386.pkg` is mandatory for all ThinOS clients. At present, PCoIP package is mandatory for the PCoIP enabled thin clients. Other packages are optional. Base package and PCoIP package are integrated into the ThinOS firmware image. Installing the latest ThinOS firmware image will automatically install the latest version of these packages on ThinOS client. You cannot manually install or upgrade these embedded packages. However, the package version details of respective packages are displayed in the **Packages** tab for engineering information purpose only.

> NOTE: **In every ThinOS release, the packages may be updated to the latest version. For information about the latest package version, see the latest Dell Wyse ThinOS release notes.**

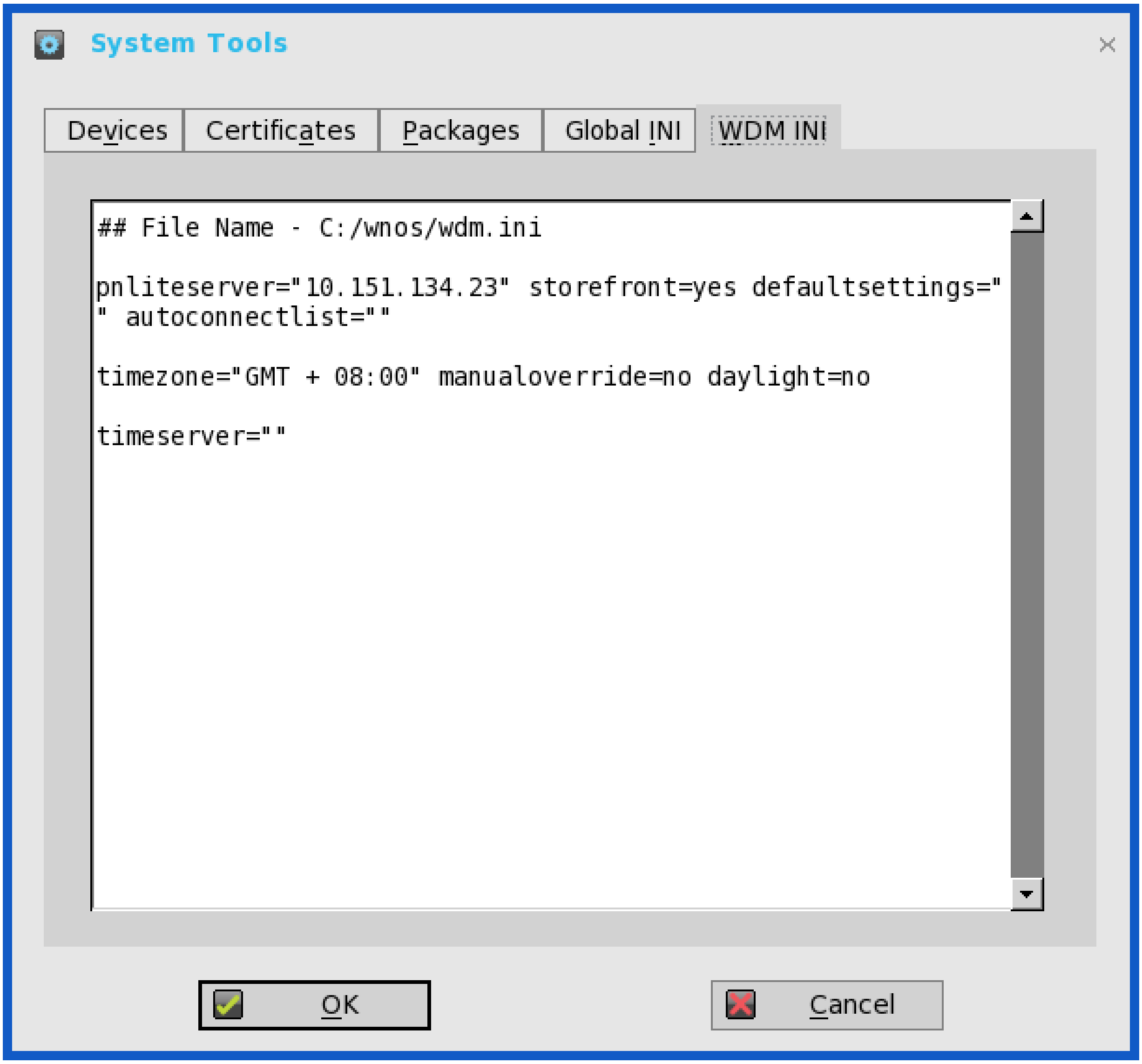
5 Click the **Global INI** tab to view wnos.ini information.



```
## File Name - C:/wnos/wnos.ini
autoload=101 pkgs=2
MaxVncd=1
VncPassword=********
setenv HDXLOG=ftp/wnos/shadow/i386/tmp
DesktopColorDepth=32 RGB565=Yes
SessionConfig=RDP USBRedirection=tcx enableVOR=NO
signon=1
vdibroker=https://10.150.102.81
EnableVDM_TunnelMMR=yes
privilege=high EnableTrace=yes
EnableRAVE=no
```

6 Click the **User INI** tab to view wnos.ini information.

7 Click the **WDM INI** to view the received WCM configurations.



```
## File Name - C:/wnos/wdm.ini

pnliteserver="10.151.134.23" storefront=yes defaultsettings="
" autoconnectlist=""

timezone="GMT + 08:00" manualoverride=no daylight=no

timeserver=""
```

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.

For more information about Wyse Device Manager (WDM) Package Manager and Profile Manager, see the *WDM Administrator's Guide*.

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

Simplified Certificate Enrollment Protocol

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).

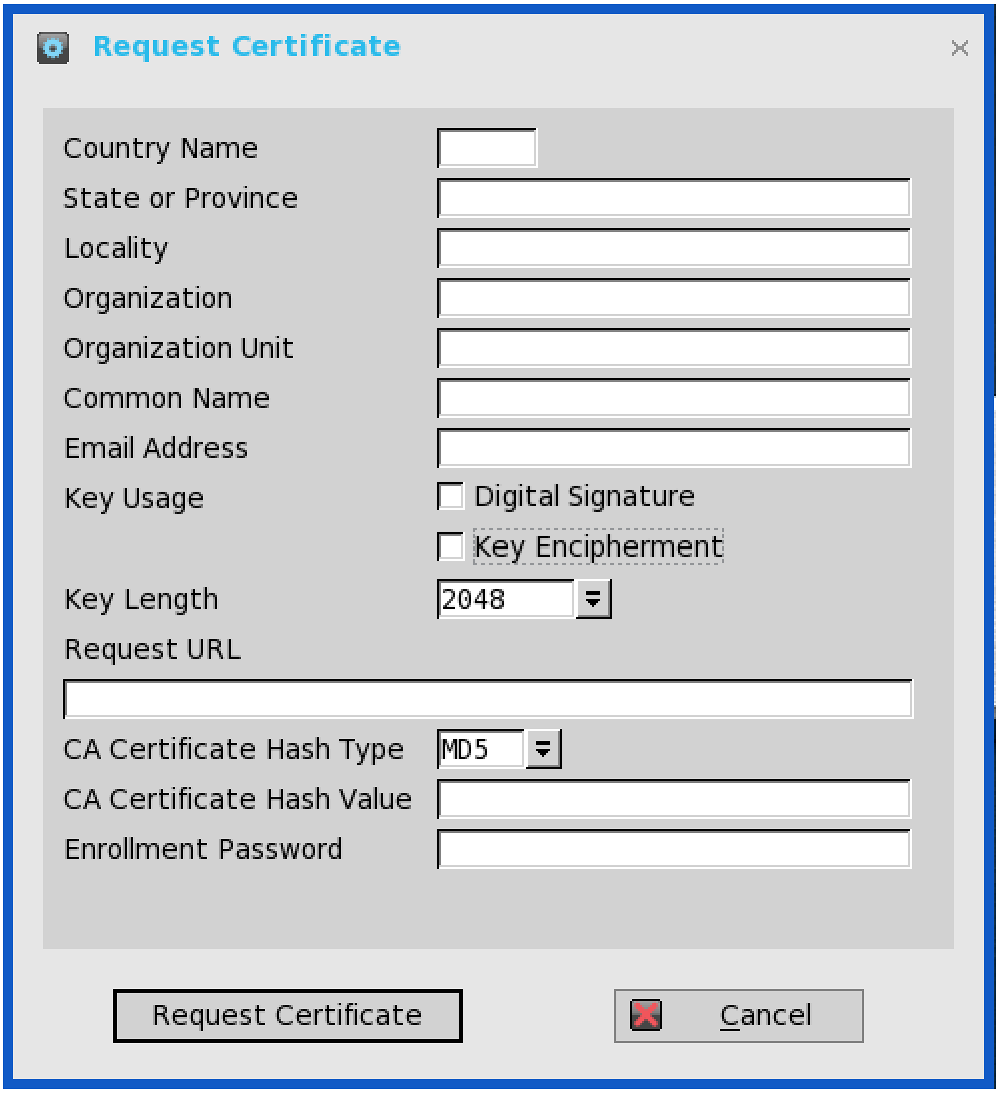
At the end of the transactions defined in this protocol, the network device has a private key and associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

ThinOS is treated as a network device. The functionality of ThinOS 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.



Request Certificate

Country Name

State or Province

Locality

Organization

Organization Unit

Common Name

Email Address

Key Usage □ Digital Signature
□ Key Encipherment

Key Length 2048

Request URL

CA Certificate Hash Type MD5

CA Certificate Hash Value

Enrollment Password

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:

- CA Certificate Hash type currently supports MD5, SHA1 and SHA256.
- Request server URL can be an HTTP or HTTPs link. You can add protocol prefix before 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, refer to the latest Dell Wyse ThinOS INI Reference guide.

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 28. 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
	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 29. 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

Certificate field	Default value/format
	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
	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 30. 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).

Certificate field	Default value/format
	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 31. 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 32. 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.
	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 33. 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

Certificate field	Default value/format
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.
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 34. 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 35. 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

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 36. 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

Certificate field	Default value/format

	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

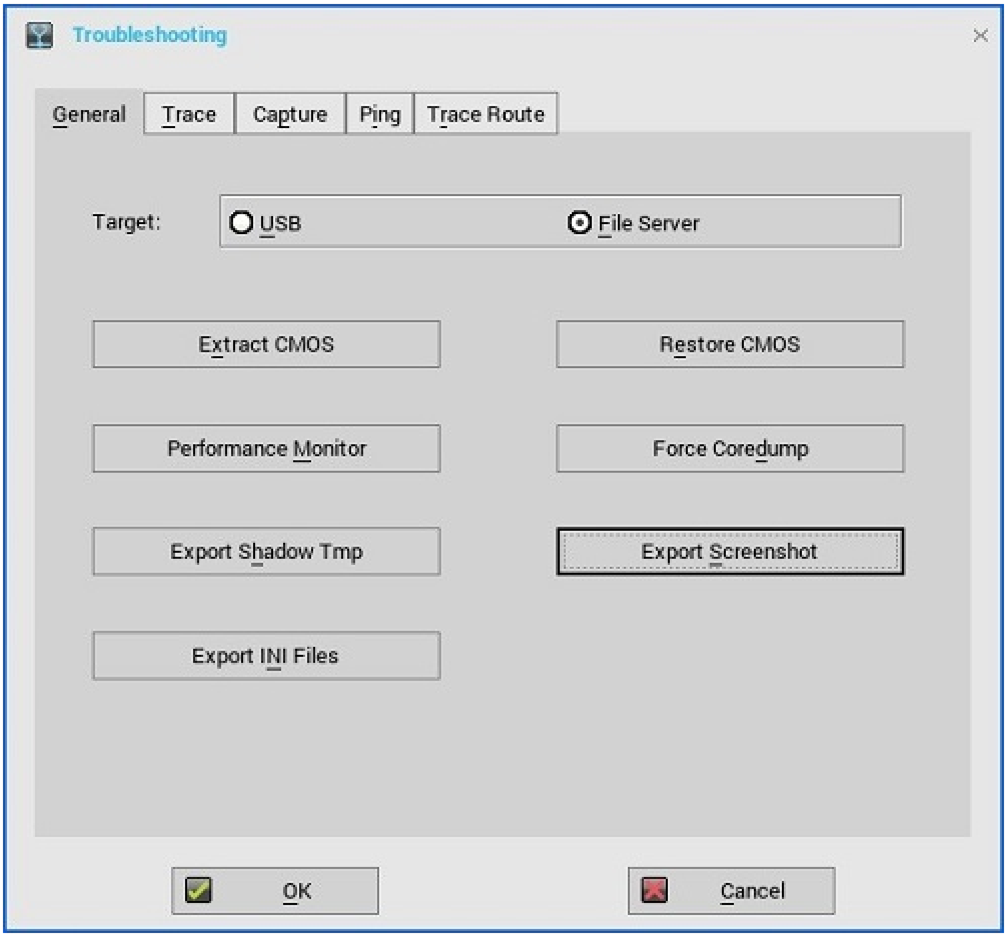
Public key	RSA (2048 bits). Key bits are displayed in the lower pane of the window.
Key usage	Certificate Sign, CRL Sign
Subject key ID	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Basic constraints	Subject Type=CA, Path Length Constraints=None
Thumbprint algorithm	sha1
Thumbprint	4e b6 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 CMOS management extract and restore cmos settings. It also allows you to view wnos.ini cached information for troubleshooting purposes.

To use the troubleshooting options:

1. From the desktop menu, click **Troubleshooting**.
   The **Troubleshooting** dialog box is displayed.

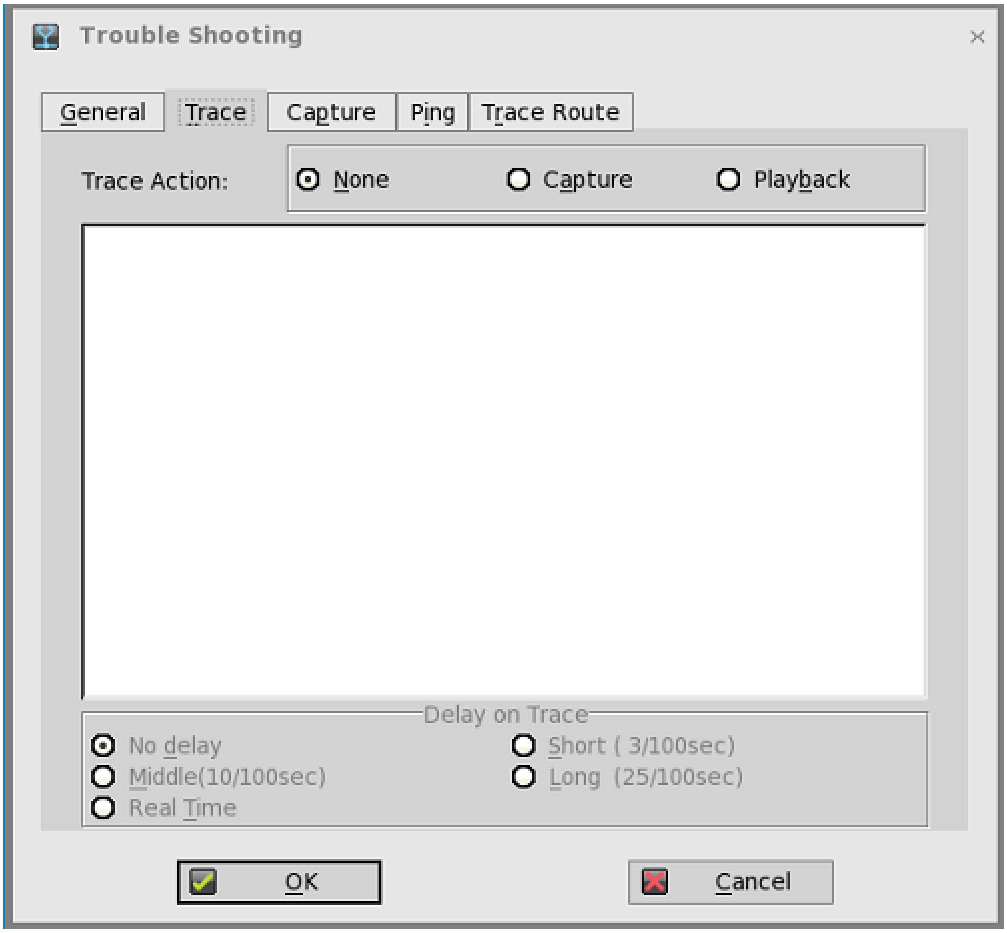


Target: ○ USB ● File Server

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

- Click either **USB** or **File Server** to select your target device you want to use for CMOS management.
- **Extract CMOS**—Click this option to extract the CMOS settings to the USB Key or file server based on your target device selection.
- **Restore CMOS**—Click this option to write the CMOS settings from the USB Key to the target thin client.
- **Performance Monitor**—Click this option to display your thin client CPU, Memory, and Networking information. The graphs display on top of all windows.
- **Force Coredump**—Use this option to forcibly generate the debug information for technical investigation when your system is not responding. Both the coredump file and the trap information image are saved to the local drive. After you restart the thin client, both the coredump file and trap issue screenshot file are uploaded to the */wnos/troubleshoot/* directory of the file server or a USB drive.
- **Export Shadow Tmp**—Use this option to export temporary logs for debugging purpose. The log files can be exported to a USB drive or file server depending on the target configuration.
- **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.
- **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.

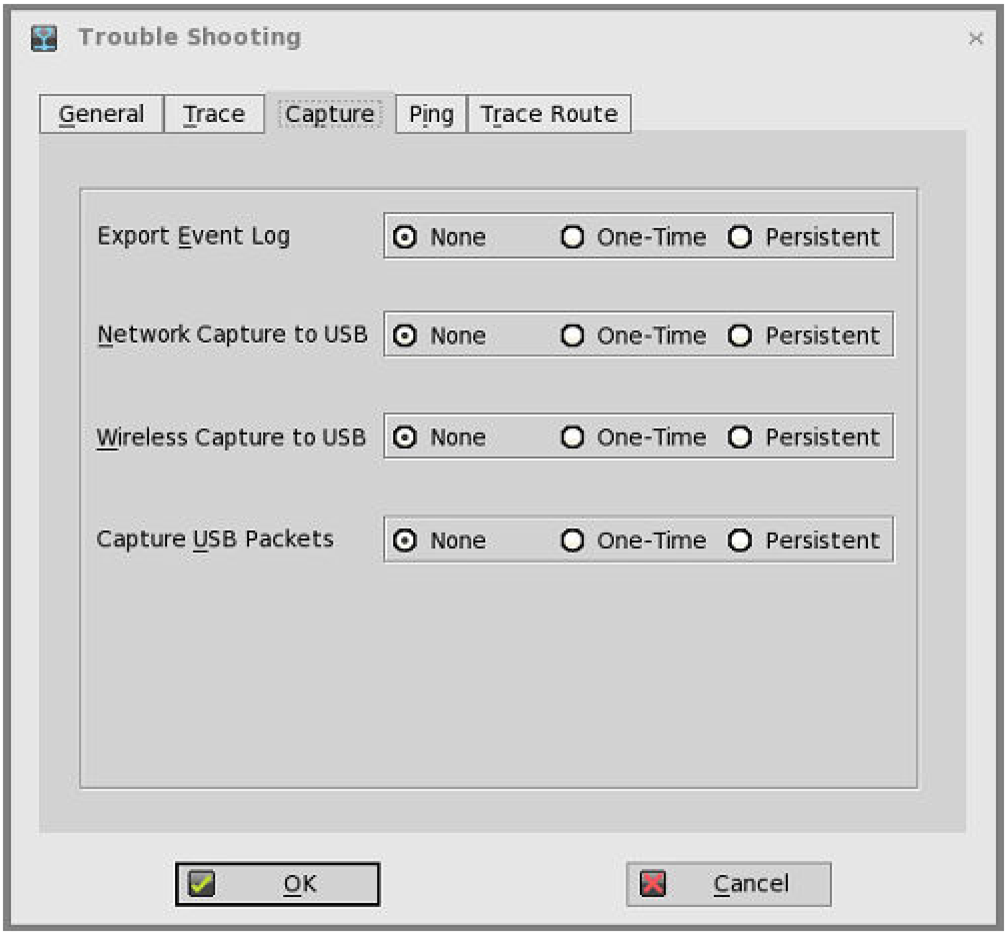
3 Click the **Trace** tab to configure the trace actions and delay on trace. The available options for trace action are None, Capture, and Playback.



Trace Action: ● None ○ Capture ○ Playback

Delay on Trace
● No delay ○ Short (3/100sec)
○ Middle(10/100sec) ○ Long (25/100sec)
○ Real Time

4 Click the **Capture** tab to configure the Export Event Log, Network Capture to USB, Wireless Capture to USB, and capture USB packets.



Export Event Log ● None ○ One-Time ○ Persistent

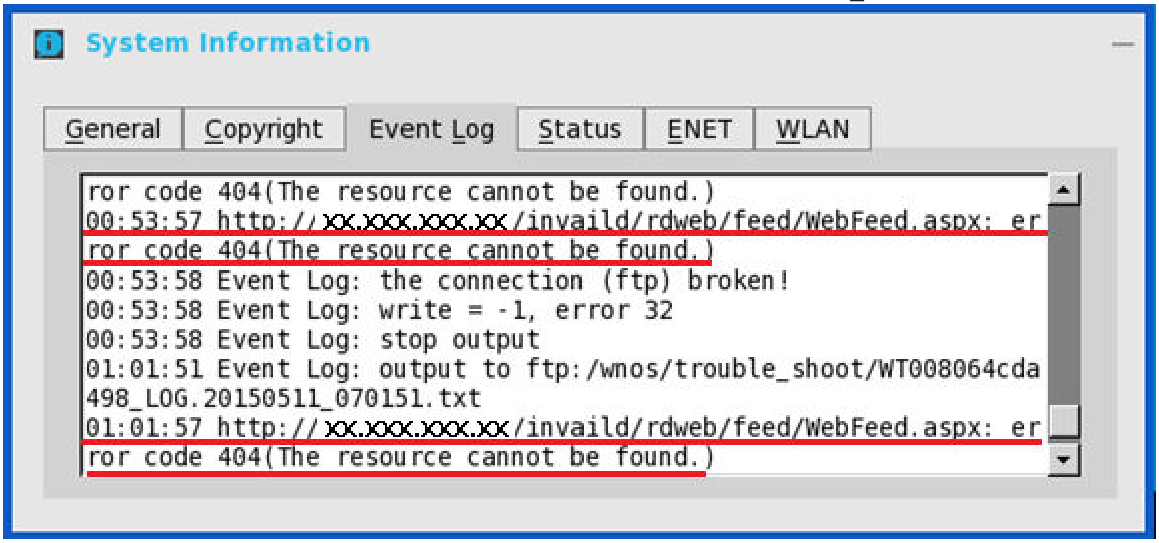
Network Capture to USB ● None ○ One-Time ○ Persistent

Wireless Capture to USB ● None ○ One-Time ○ Persistent

Capture USB Packets ● None ○ One-Time ○ Persistent

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.
- Turn off logging and then check the log file under the folder `ftp:/wnos/trouble_shoot`.



```
ror code 404(The resource cannot be found.)
00:53:57 http://xx.xxx.xxx.xx/invaild/rdweb/feed/WebFeed.aspx: er
ror code 404(The resource cannot be found.)
00:53:58 Event Log: the connection (ftp) broken!
00:53:58 Event Log: write = -1, error 32
00:53:58 Event Log: stop output
01:01:51 Event Log: output to ftp:/wnos/trouble_shoot/WT008064cda
498_LOG.20150511_070151.txt
01:01:57 http://xx.xxx.xxx.xx/invaild/rdweb/feed/WebFeed.aspx: er
ror code 404(The resource cannot be found.)
```

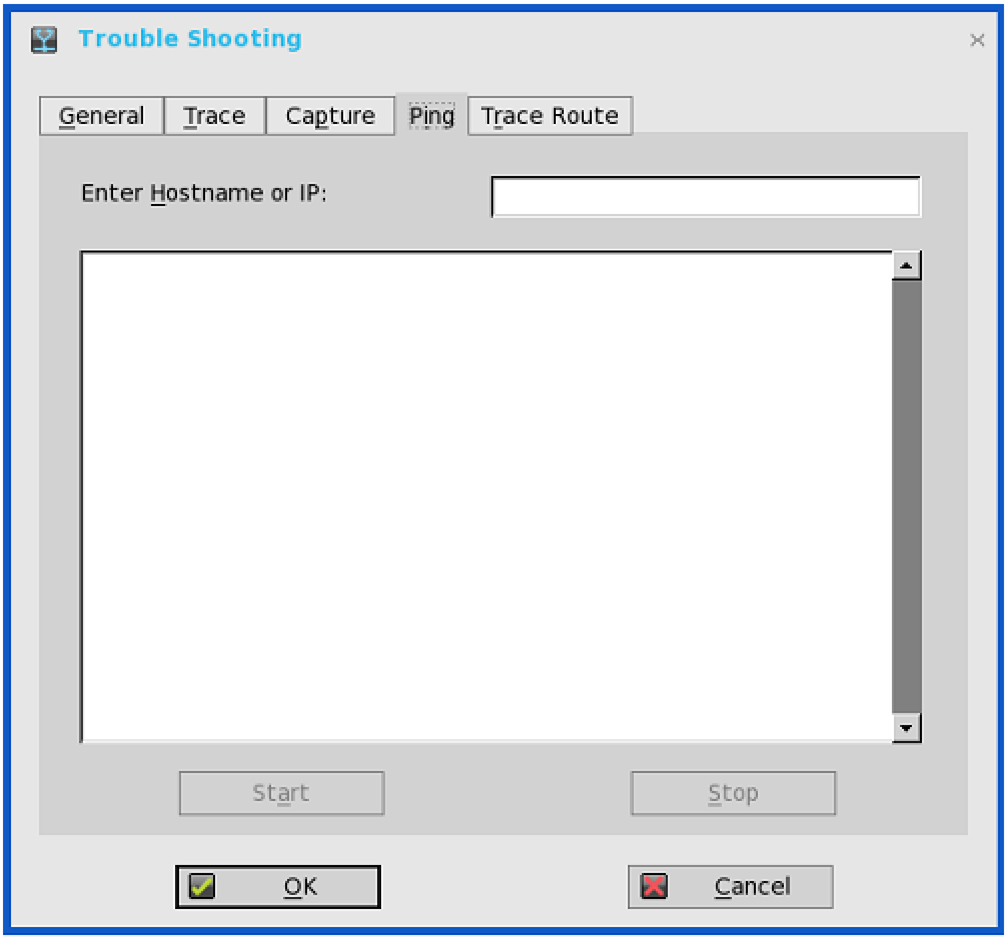
- Be sure to enable the Enable Trace option of the Privilege parameter in a wnos.ini file. For more information, see Dell Wyse ThinOS INI Guide.
- Use the **Network capture to USB** option to enable the capture of network information, that is, a network trace of all traffic coming in and out of the thin client to a USB drive that is inserted into the thin client.

After you log in 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 thin 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 thin 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:



- **Enter Hostname or IP**—Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be pinged.
- **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.
- **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**.
- **Stop**—Terminates the ping request and leaves the **Ping** dialog box open, so you can read the summary posted in the data area.

ⓘ NOTE:

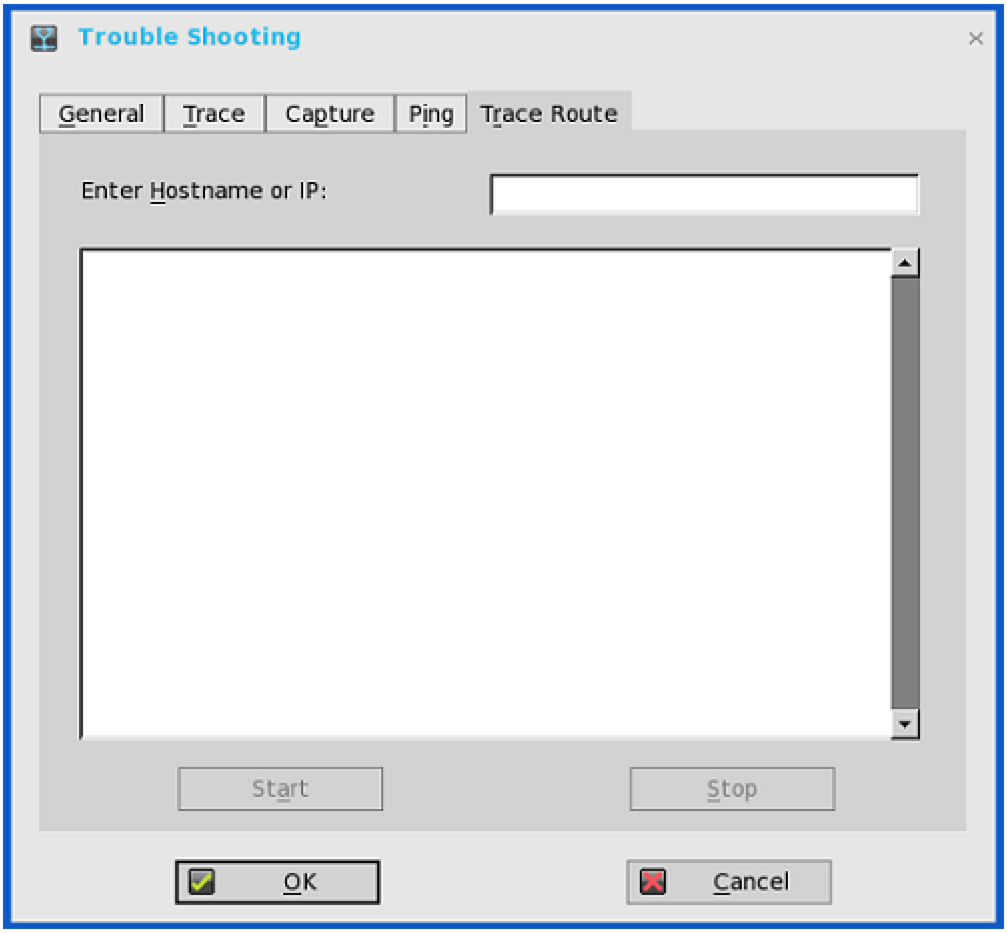
Ping sends an echo request to a network host. The host parameter is either a valid host name or an IP address. If the host is operational and on the network, it responds to the echo request. Ping sends one echo request per second and calculates round trip times and packet loss statistics. It displays 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:



- **Enter Hostname or IP** — Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be traced.
- **Data area**—Displays round-trip response time and identifying information for each device in the path.
- **Start**—Executes the tracert command.
- **Stop**—Terminates the tracert command and leaves the **Trace Route** dialog box open, so that you can read the information posted in the data area.

The tracert utility traces the path from your thin 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 **OK** to save the settings.

8

TCX Suite

Dell Wyse TCX Suite is a single software solution that provides the benefits of cloud client computing. The supported environments for Dell Wyse TCX Suite are Microsoft Remote Desktop Services, Citrix XenApp, Citrix XenDesktop, Teradici, and VMware Horizon View. The Collaborative Processing Architecture (CPA) used in Dell Wyse TCX divides the workload between the server and Plug-n-Play USB devices. TCX Suite uses the established software protocols to provide breakthrough multimedia and audio technology for cloud client computing environments. For more information about the TCX features, see the latest *Dell Wyse TCX Administrator's Guide*.

TCX Suite enables rich flash playback, multiple monitors awareness, rich multimedia playback, high-quality bidirectional audio capabilities, and seamless USB device access for cloud clients.

TCX Suite provides the following features:

- **TCX Flash Acceleration and TCX Flash Redirection**—Enhances the performance of the Flash video content in a remote computing environment.
- **TCX Multidisplay**—Provides productivity, enhancing advantages for cloud clients with multiple monitors by using virtual desktops.
- **TCX Multimedia**—Supports enhanced playback of MPEG, WAV, WMV, H.264, and other multimedia file formats. The software includes both the server and the client components that redirect multimedia processing tasks between the client and server for a rich user experience.
- **TCX Rich Sound**—Provides bidirectional audio capabilities for virtual desktops and applications and supports sound recording and playback applications. It supports zero-compromise deployment.
- **TCX USB Virtualizer**—Makes the USB devices attached to thin clients or endpoints visible to the virtual desktops and applications. It removes any dependencies on limited local device drivers for a broad range of USB-based printers, scanners, storage devices, Palmtop, BlackBerry, Pocket PC handhelds, HID devices, Webcams, headsets, iPhone, credit card machines, and smart cards.
- **TCX Monitor**—Helps you to efficiently identify the system state for proper functioning of USB and Flash Redirection modules.

TCX Flash Redirection

TCX Flash Redirection uses the client CPU to decode and render flash. TCX Flash Redirection uses the Adobe flash player plug-in that supports the NPAPI interface on the client. TCX Flash Redirection is supported over RDP and PCoIP protocols. TCX Flash Redirection uses less Server CPU cycles.

Prerequisites

- **TCX.i386.pkg** must be installed on client for the feature to work.
- **TFRSServerBHO Class** must be enabled in browser add-on.
- **Enable Protected Mode** is turned off in the Security options of Internet Explorer.
- **Enable third-party browser extensions** is enabled in the Advanced options of Internet Explorer.

Verifying the working status of TCX Flash Redirection

Verifying the status of TCX Flash Redirection is similar to HDX FR.

Use the following INI parameter to display the HW label:

```
MMRConfig=VIDEO flashingHW=1
```

Known Issues with TCX Flash Redirection

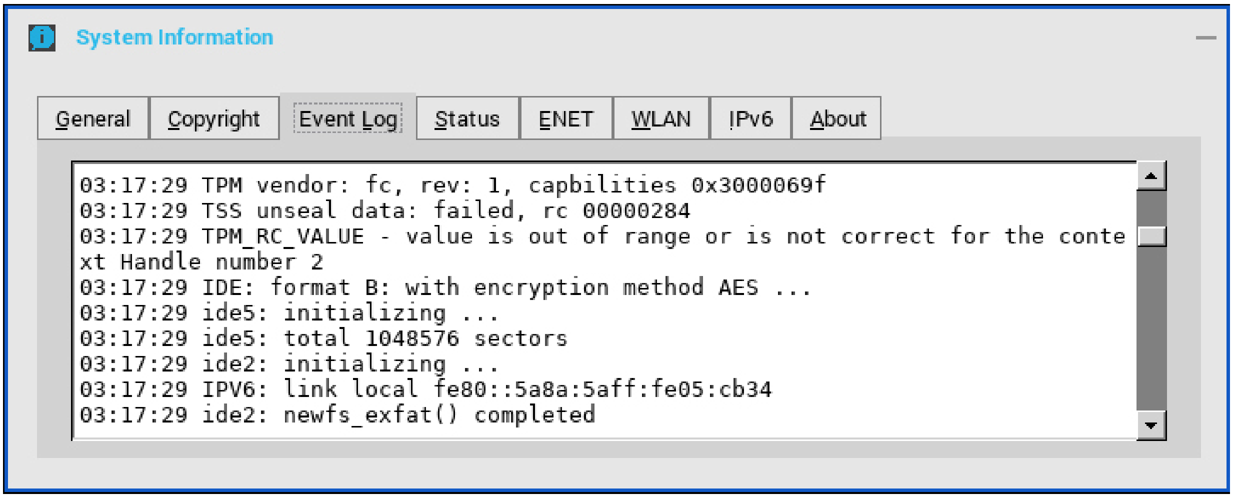
TCX FR on ThinOS is not working for certain flash video pages. However, the result is the same between FR over RDP, and FR over PCoIP. Dell recommends you to validate, and block the URL that does not work, before deploying TCX FR on all the systems.

9

Trusted Platform Module version 2.0

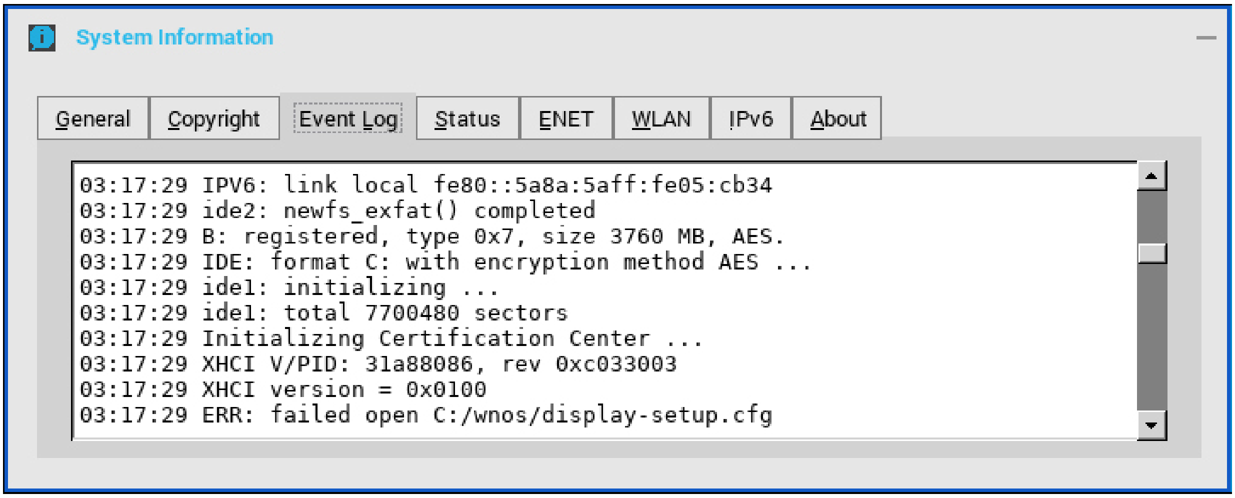
Wyse 5070 thin client supports disk encryption and decryption through Trusted Platform Module (TPM) version 2.0.

- Measured boot—SHA1 (Secure Hash Algorithm 1) is used to produce a hash value for ThinOS image, and extend the integrity measurement into Platform Configuration Registers (PCR) inside TPM—**TPM_PCR16**. This is used to generate disk encryption or decryption key.
- Disk encryption/decryption key
  - Disk C with user data and Disk B with system libraries are encrypted.
  - Prestored **KeyStub** and **TPM_PCR16** are used to generate disk encryption and decryption keys through TPM. The actual implementation is based on TPM-unseal operation.
  - If the key is modified, the key fails to verify the specific disk partition. The disk partition is formatted to make the partition valid. The following screenshot displays the event log:



```
03:17:29 TPM vendor: fc, rev: 1, capbilities 0x3000069f
03:17:29 TSS unseal data: failed, rc 00000284
03:17:29 TPM_RC_VALUE - value is out of range or is not correct for the conte
xt Handle number 2
03:17:29 IDE: format B: with encryption method AES ...
03:17:29 ide5: initializing ...
03:17:29 ide5: total 1048576 sectors
03:17:29 ide2: initializing ...
03:17:29 IPV6: link local fe80::5a8a:5aff:fe05:cb34
03:17:29 ide2: newfs_exfat() completed
```

Figure 19. Event log tab



```
03:17:29 IPV6: link local fe80::5a8a:5aff:fe05:cb34
03:17:29 ide2: newfs_exfat() completed
03:17:29 B: registered, type 0x7, size 3760 MB, AES.
03:17:29 IDE: format C: with encryption method AES ...
03:17:29 ide1: initializing ...
03:17:29 ide1: total 7700480 sectors
03:17:29 Initializing Certification Center ...
03:17:29 XHCI V/PID: 31a88086, rev 0xc033003
03:17:29 XHCI version = 0x0100
03:17:29 ERR: failed open C:/wnos/display-setup.cfg
```

Figure 20. Event log tab

- After the disk partition is formatted, some user configurations, such as display settings, user certificates, wireless settings—except the first SSID, as it is saved in NVRAM—cookie, and mirror file server data, are lost.

10

BIOS management on ThinOS

This appendix describes the BIOS management on the ThinOS devices with Dell Standard BIOS.

To make BIOS management consistent between Wyse and Dell BIOS, INI parameter Device=DellCmos is introduced for Dell Standard BIOS.

For BIOS configuration, if the password is configured, to update any settings, the password is required to be supplied. For example, the INI parameter to update settings must be followed with “CurrentPassword={}”. This is mandatory for Dell BIOS.

BIOS functionality matrix

Table 37. BIOS functionality matrix

Major requirement	INI parameter for BIOS management	Wyse 5070 thin client
Power on without beeps	N/A	Yes
Update BIOS from file server	N/A	Yes
Change BIOS password with INI	Device=DellCmos CurrentPassword={} NewPassword={} Device=Cmos CurrentPassword={} NewPassword={}	Yes
Change boot order with INI	Device=cmos BootOrder={PXE, HardDisk, USB}	Not applicable
Enable/Disable PXE imaging with INI	Device=DellCmos PXEBootSupport={yes, no}	Yes
Enable/Disable USB imaging with INI	Device=cmos BootFromUSB={yes, no} Device=DellCmos USBBootSupport={yes, no}	Yes
Manage AC recovery with INI	Device=cmos AutoPower={yes, no} Device=DellCmos ACRecovery={PowerOff, PowerOn, LastState}	Yes
Manage auto on time with INI	Device=DellCmos AutoPower={Disable, Daily, Workday} AutoPowerTime=hh:mm Device=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 AutoPowerDays=Sunday;Friday	Yes
CMOS Extract and Restore	Device=cmos Action={extract, restore} CurrentPassword={} Device=DellCmos Action={extract, restore} CurrentPassword={}	Yes
Audio management with INI	Device=cmos OnboardAudio={yes, no} Device=DellCmos Audio={yes, no}	Yes

Major requirement	INI parameter for BIOS management	Wyse 5070 thin client
USB Port management with INI	Device=cmos USBController={yes, no} Device=DellCmos USBRearPort={yes, no} USBFrontPort={yes, no} (Rear/Front for Dell BIOS only)	Yes
Admin lockup management with INI	Device=DellCmos AdminLock= {yes, no}	Yes
Wake on USB support	Device=DellCmos WakeOnUSB={yes, no}	Yes
Wake On LAN	Device=cmos WakeOnLan= {yes, no} Device=DellCmos WakeOnLan= {Disable, LAN, PXE}	Yes

Accessing BIOS settings

After starting your thin client, you will see a Dell logo for a short time. During this period, press and hold the F2 key.

When prompted, type the password **Fireport** to view the BIOS settings screen. 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.

Dell Standard BIOS management

This section describes how to configure and manage the ThinOS clients with Dell Standard BIOS.

The following Dell BIOS configurations are supported by using file server (INI parameters):

Table 38. BIOS configuration options

Parameters	Settings
System Configuration	Audio
Security	• Admin Setup Lockout • Admin Password – Enable/Disable Admin Password – Update Admin Password
USB Configuration	• Enable Front USB Ports • Enable Rear-Left Dual USB 2.0 Ports
Power Management	• Wake-On-LAN – Disabled – LAN Only – LAN with PXE Boot • AC Recovery – Power Off – Power On – Last Power State • Auto-On Time – Disabled

Parameters	Settings
	– Every Day – Weekdays – Select Days • Wake-On-USB
Device boot	• USB boot • PXE boot

For information about INI parameters and their usage, see the latest Dell Wyse ThinOS INI Reference Guide.

The following are examples of INI parameters:

- Device=DellCmos newpassword=1234567 or newpasswordenc=encrypted strings—Use this INI parameter to create the admin password when password is not set.
- Device=DellCmos currentpassword=1234567 newpassword="" or currentpasswordenc=encrypted strings—Use this INI parameter to clear the existing password.

Upgrading BIOS on Wyse 5070 thin client

This section describes the procedure to update BIOS on Wyse 5070 thin client with ThinOS, and Wyse 5070 thin client with PCoIP by using file server. The Dell Standard BIOS file is converted to BIN file format for signature and security purposes. The format of the BIN file is Wyse_5070_version.bin.

To upgrade BIOS using the file server:

1 Download the Dell BIOS file from the Dell support site.

  For example, Wyse_5070_1.0.3.bin. The BIOS version may be updated in each release. For the latest version of BIOS, see the latest Dell Wyse ThinOS Release Notes.

2 Rename the Dell BIOS file as X10_bios.bin.

3 Upload the renamed BIOS file to folder WNOS in the file server—ftp or https.

4 Ensure that the INI parameter autoload is enabled for firmware update in WNOS.INI.

5 Restart the thin client.

  The BIOS is updated automatically.

To verify whether the new BIOS is updated correctly, from the desktop menu, click the **System Information** option, or click the **System Information** icon in zero mode. In the **Event Log** tab, the BIOS version log is displayed.

For example, **System Version: 8.5_108—ROM 1.0.3**.

This log indicates that the BIOS version is updated to v1.0.3.

BIOS version can be viewed on the BIOS setup screen. To access the BIOS setup, do the following:

1 Restart the thin client, and during system boot, press the `F2` key.

2 Enter the BIOS password, if admin password is set.

3 Click **Settings** > **General** > **System Information**.

  The BIOS version is displayed on the screen.

BIOS can also be updated by using the Wyse Management Suite version 1.2 console. For more information about Wyse Management Suite, see *Dell Wyse Management Suite Administrator's Guide*.

Security

A new global security policy has been defined for ThinOS 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.

Table 39. INI parameter

INI parameter	Description

`SecurityPolicy={full | **warning** (default) | low}`
`SecuredNetworkProtocol={yes | no (default)}`
`TLSMinVersion={1 (default), 2, 3}`
`TLSMaxVesion={1, 2, 3 (default)}`
	Full—SSL connection need to verify server certificate. If it is untrusted, cancel the connection.
	Warning (default)—SSL connection need to verify server certificate. If it is untrusted, the user can continue or cancel the connection.
	Low: Server certificate is not verified– this is the value set for a few applications.
	After firmware is updated, the default value is set to warning for all applicable applications immediately.
	There is one exception for file server and WDM.
	The old ini SecurityLevel | SecureProtocol from Privilege segment is deleted.

All applications running on the default SSL security mode follow the global mode. In the global mode, the default value is Warning. The affected applications include VMware View, Amazon Workspaces (AWS), File Server, WDMService, Caradigm Server, and OneSign Server.

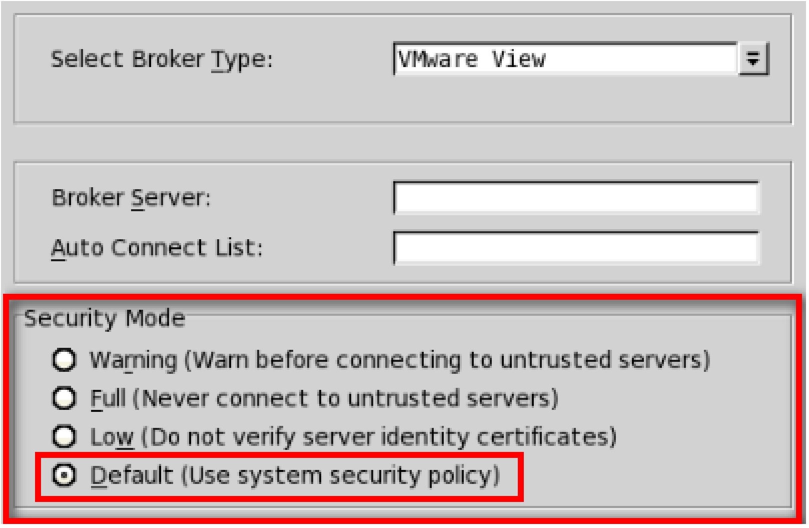
For more information about the security mode INI parameters, see Dell Wyse ThinOS INI Guide.

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.
- VMware View and AWS brokers include own security settings (GUI and INI).

  An additional option is added to follow the global mode as its new default value.



Select Broker Type: VMware View

Broker Server:

Auto Connect List:

Security Mode

- ○ Warning (Warn before connecting to untrusted servers)
- ○ Full (Never connect to untrusted servers)
- ○ Low (Do not verify server identity certificates)
- ● Default (Use system security policy)

- Wyse Management Suite, Microsoft RDS broker, Citrix broker, and SecureMatrix are always `Full`.

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://`.

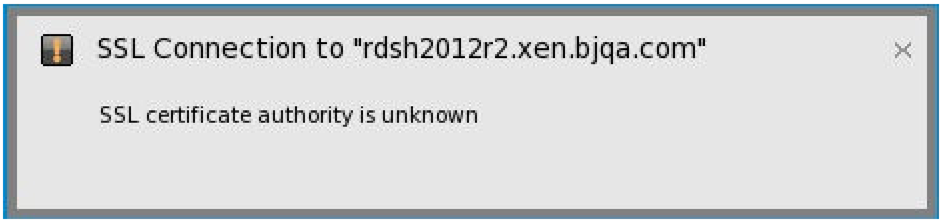
New firmware/client deploy information

- For `SecurityPolicy=Full`or `warning`, you are required to add certificates from the respective File, View, AWS, WDM, Wyse Management Suite, OneSign, and/or Caradigm server(s) to the ThinOS client before updating the firmware.
- The default protocol of File Server is still FTP and ftp prefix is added automatically, if the protocol is not provided.

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.

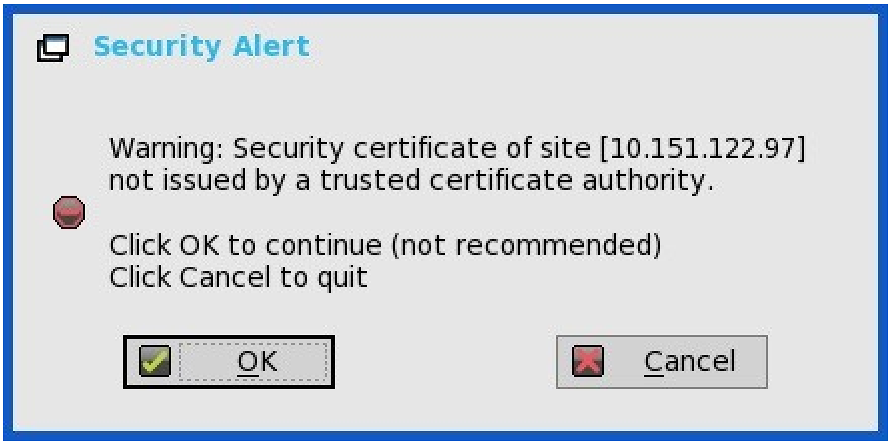
In full security mode, the following warning message is displayed:



SSL Connection to "rdsh2012r2.xen.bjqa.com"

SSL certificate authority is unknown

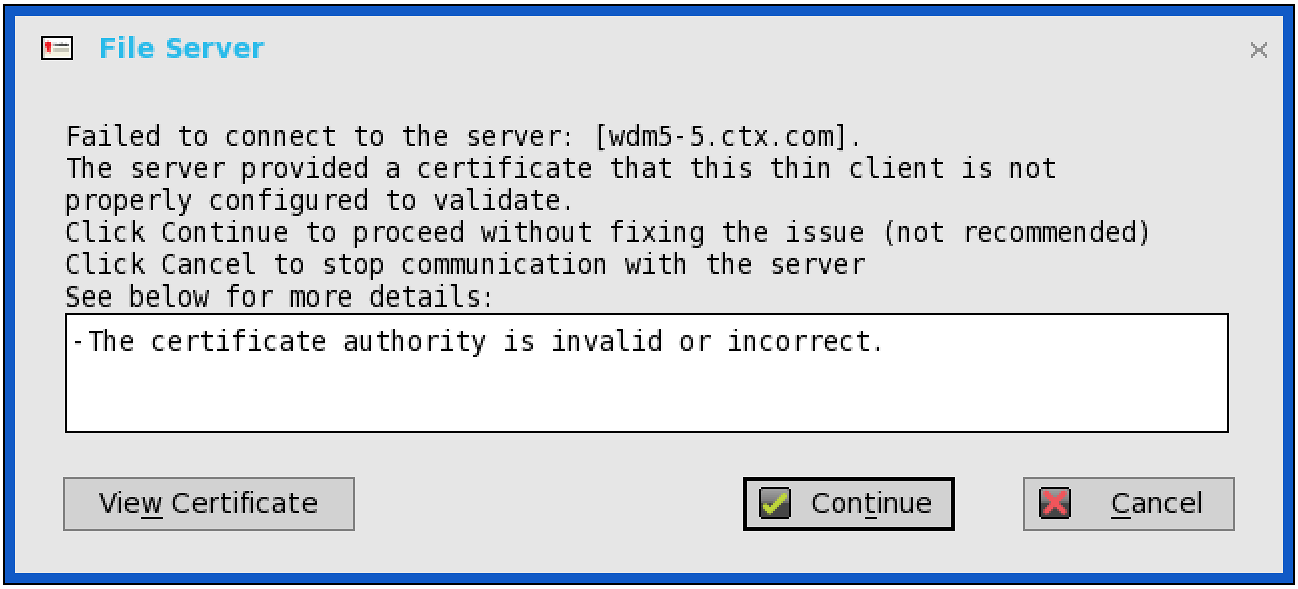
For warning security mode, the following warning messages are displayed:



Security Alert

Warning: Security certificate of site [10.151.122.97]
not issued by a trusted certificate authority.

Click OK to continue (not recommended)
Click Cancel to quit



File Server

```
Failed to connect to the server: [wdm5-5.ctx.com].
The server provided a certificate that this thin client is not
properly configured to validate.
Click Continue to proceed without fixing the issue (not recommended)
Click Cancel to stop communication with the server
See below for more details:
-The certificate authority is invalid or incorrect.
```

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.

Transport Layer Security

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 13.56MHZ card
  - Omnikey 5321 V2 Cl Sam (0x5341, 0x076b) reader supports 13.56 MHz card
  - Omnikey 5421 (0x5421, 0x076b), reader supports 13.56 MHz card
  - Omnikey 5321 CR (0x5320, 0x076b)
- **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 Dell Wyse ThinOS Release Notes.

A

Automating updates and settings using central configuration

This appendix describes how to set up your environment to provide your thin clients running ThinOS with automatic updates and configurations in three simple steps.

ⓘ **NOTE: Dell Wyse thin 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 thin clients. For information about configuring your thin clients to communicate with a WDM server or Wyse Management Suite, see the related INI parameters in Dell Wyse ThinOS INI Guide.**

How to set up automatic updates and configurations

For a thin client running ThinOS to successfully access INI files and update itself from a server, you must set up the server with the correct folder structure where the INI files and other update files are located, direct the thin client to the server, and then reboot or start the thin client

Once DHCP and servers are configured and available, the thin client checks (at each boot up) to see whether or not any updates are available on a predefined server DHCP Option **#161** specifies the server URL, DHCP Option **#162** specifies the root path to the server. If updates are available, the updates are automatically installed.

Using DHCP options

This table contains the DHCP options available for use.

Table 40. DHCP options

Option	Description	Notes
1	Subnet Mask	Required. However, it is not required unless the thin client must interact with servers on a different subnet. MS DHCP requires a subnet mask and is always send one.
2	Time Offset	Optional.
3	Router	Optional, but recommended. It is not required unless the thin client must interact with servers on a different subnet.
6	Domain Name Server (DNS)	Optional, but recommended.
15	Domain Name	Optional, but recommended. See Option 6.
28	Broadcast Address	Optional.
44	WINS servers IP Address	Optional.
51	Lease Time	Optional, but recommended.
52	Option Overload	Optional.
53	DHCP Message Type	Recommended.

Option	Description	Notes
54	DHCP Server IP Address	Recommended.
55	Parameter Request List	Sent by thin client.
57	Maximum DHCP Message Size	Optional (always sent by thin client).
58	T1 (renew) Time	Optional, but recommended.
59	T2 (rebind) Time	Optional, but recommended.
61	Client identifier	Always sent.
161	File server (ftp/http/https)	Optional string. Can be either the name or the IP address of the file server. If a name is given, the name must be resolvable by the DNS servers specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to also be the file server.
162	Root path to the file server (ftp/http/https)	Optional string. If the option provided by the server is blank and the server provides no value for the field, a null string is used. \wyse\wnos is automatically appended to the search path. For example, if you enter pub\serversoftware, the path searchedare pub\serversoftware\wyse\wnos. ⓘ **NOTE: You can have the \wyse automatic component of the search path omitted by appending a dollar sign ($) to the entered path. For example, if you enter `pub\serversoftware$`, the path searched will be `pub\serversoftware\wnos`.** ⓘ **NOTE: The usage or omission of a leading slash (\) on the path is critical on some servers. Some servers limit access to the root path of the user specified at login. For those servers, the usage of the leading slash is optional. Some *NIX servers can be configured to allow the file user access to the entire file system. For those servers, specifying a leading slash specifies that access is to start at the root file system. Proper matching of the file specification to the file server in use is critical to ensuring proper operation. A secured Windows server requires the slash to be specified in order to complete proper access.**
165	WMS Server	Optional string. Specifies the IP address of the Wyse Management Suite Server.

Option	Description	Notes
166	WMS MQTT Server	Optional string. Specifies the IP address of the MQTT Server.
167	WMS CA Validation	Optional string.
181	PNAgent/ PNLite server list	Optional string. The thin client uses the server to authenticate the Windows credentials of the user and to obtain a list of ICA published applications valid for the validated credentials. The user supplies those credentials when logging in to the thin client.
182	NT domain list for PNAgent/ PNLite	Optional string. The thin client creates a pull-down list of domains from the information supplied in option 182. This list is presented at thin client login in the order specified in the DHCP option (for example, the first domain specified becomes the default). The selected domain is the one which must authenticate the user ID and password. Only the selected domain is used in the authentication process. If the domain list is incomplete and the user credentials must be verified against a domain not in the list, assuming that the server in option 181 is capable of authenticating against a domain not in the list, the user has the option of not using any of the domains specified in option 182 and typing a different domain name at the time of login.
184	File server Username	Optional string. Username to use when authenticating to the server specified in Option 161.
185	File server Password	Optional string. Password to use when authenticating to the server specified in Option 161.
186	WDM server list	Optional binary IP addresses of WDM. This option can specify up to two WDM servers. If two are specified, at boot time the thin client attempts to check-in to the first server. If it cannot contact the first server, it tries to check-in to the second server.
187	WDM server port	Optional number. Byte, word, or two-bytes array. ⓘ **NOTE: The value of this option tag, when not embedded in Vendor Class Specific Information option, is interpreted in reverse order when it is sent as 2-bytes example, the value of 0x0050 was interpreted as 0x5000. This option tag was used by old ThinOS releases. New ThinOS releases still accept this option tag for backward compatibility.**
188	Virtual Desktop Broker server	Optional string.

Option	Description	Notes
190	WDM secure port	Optional number, word or two-bytes array. Specifies to use HTTPS to communicate with WDM instead of HTTP.
192	WDM server port	Optional number, word or two-bytes array. ⓘ NOTE: **The value of this option tag represents the same information as option tag 187. The difference is that ThinOS interprets the value of this option tag in correct order (for example, the value of 0x0050 is interpreted as0x0050). If the DHCP server provides both option tag 192 and 187, option tag 192 takes precedence.**
194	WDM FQDN	Optional Fully Qualified Domain Name for the WDM.
199	Wyse Management Suite Group Key	Optional string. Can provide a Wyse Management Suite Group Registration Key for the Wyse Management Suite agent. When Wyse Management Suite is disabled and the Group Key of Wyse Management Suite is null, this option takes effect. Wyse Management Suite uses the optional string as the Group Registration Key. If the Wyse Management Suite server or MQTT server is null, the Wyse Management Suite agent sets the values to the default server values.

B

Examples of common printing configurations

This appendix provides examples on using the **Printer Setup** dialog box and ThinOS INI parameters for common printing situations. Use these general guidelines in addition to the information provided in Configuring the Printer Setup.

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 network 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
  - Using INI parameters for Windows network printers
- Using your thin 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

Printing to local USB or parallel printers

You can print to locally attached printers through USB or parallel ports.

IMPORTANT: Microsoft Remote Desktop Session Host (RDSH), Microsoft Terminal Services, and Citrix XenApp each have their own printing policies that must be configured properly to allow client side printing. For details on configuring printing in these environments, see your vendor instructions.

Using the Printer Setup dialog box for local USB or parallel printers

In this example you have an HP LaserJet 4000 attached to a thin client USB port. When connecting USB printers, some printers fill out the Printer Name and Printer Identification fields for you.
To Configure the Printer to print locally attached printers through USB or Parallel ports.

1. From the desktop menu, click **System Setup** > **Printer**.

   The **Printer Setup** dialog box is displayed.
2. Click **Printer Setup**, and use the following guidelines for the Ports tab when printing to a local USB printer:
   a. **Select Port** — Select LPT1 or LPT2 port.
   b. **Printer Name** — Enter name you want displayed in your list of printers, most USB direct-connected printers report/fill in 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 report/fill in their printer identifications automatically. In our example case, enter HP LaserJet 4000 Series PCL.
   d. **Printer Class** — You can leave this as default.
   e. **Enable the printer device** — Must be selected to enable the directly connected printer enables the device so it displays on the remote host.

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

Using INI parameters for local USB or parallel printers

Configuring local printing using ThinOS INI parameters is simple and an easy way to configure a printer for all clients in your environment assuming every printer is the same.

Your INI parameters will look something like the following:

```
Printer=LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \
Enabled=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.**

Printing to non-Windows network printers

ThinOS can print to non-Windows network printers as long as the printers can accept LPR print requests. Most workgroup printers and large network printers have this capability be sure to check with your vendor that the printer can accept Line Printer Request print requests.

Once your thin client is configured to print to an LPR capable printer, the client will then redirect this printer through an RDP or 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

To configure the **Printer Setup** dialog box for Non-Windows Network Printers (LPD).

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

   The **Printer Setup** dialog box is displayed.

   In this example we have an HP LaserJet 4200n attached to a thin client through LPR.
2. Click the **LPDs** tab and use the following guidelines when printing to a non-Windows network printer:
   a. **Select LPD** — Select LPD1 or LPD2 port.
   b. **Printer Name** — 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.

      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 thin client on your network, the entry in the LPD Hosts box is the name or address of that thin 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 thin client on your network, the LPD Queue Name must match the content of the Printer Name box on the thin client with the printer attached.**

f **Printer Class** —You can leave this as default.

g **Enable the printer device** — Must be selected to enable the printer enables the device so it displays on the remote host.

Using INI parameters for non-Windows network printers

Configuring network printing using ThinOS INI parameters is simple and an easy way to configure a printer for all clients in your environment assuming every printer is the same.

Your INI parameters will look something like the following:

```
Printer=LPD1 \
LocalName="HP LaserJet 4200n" \
Host=10.10.10.1 \
Queue=auto \
PrinterID="HP LaserJet 4200 PCL6" \
Enabled=yes
```

ⓘ NOTE: **The PrinterID is the exact text of the Windows printer driver name, so if a printer driver is named HP LaserJet 4200n PCL6 in Windows, then it must be exactly the same in the PrinterID field in the INI parameters including capitalizations and spaces.**

Printing to Windows network printers

ThinOS can print to printers that are shared by Microsoft print servers. There are some configuration requirements that need to be considered when configuring SMB printing from ThinOS which may require changes to your thin client setup.

Since connecting to a Microsoft Windows Print Server requires domain credentials, you must provide the credentials to ThinOS 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 (Advanced)** in Using INI parameters for Windows network printers (SMB). This section will discuss both methods.

Using the Printer Setup dialog box for Windows network printers

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 Using INI parameters for Windows network printers.

Enter the context of your task here (optional). This is where introductory content goes.

1 From the desktop menu, click **System Setup** > **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 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

Configuring SMB printing using ThinOS 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 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. Defining an 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. Defining an 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 technicalhelp.de/

IMPORTANT: This is a non-supported tool that is linked solely for the purpose of this example.

3. Defining an SMB printer to use user credentials cached by ThinOS (advanced)

NOTE: This method requires that the user log in to ThinOS 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=RDP \
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 thin client as a print server

ThinOS thin client can be configured as a basic network print server, to share local printers with other thin clients.

Using the Printer Setup dialog box for configuring LPD services

From the Classic desktop mode only, a thin client can be configured to provide LPD (Line Printer Daemon) services making the thin client a printer server on the network. Set up the thin client that is to provide LPD print services as follows:
To configure LPD services using the Printer Setup dialog box.

1. From the desktop menu, click **System Setup** > **Network Setup** to open the **Network Setup** dialog box.
2. Enter a static IP address for the thin client.
3. From the desktop menu, click **System Setup** > **Printer** to open the **Printer Setup** dialog box and select any of the listed ports.
4. Select a 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 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 thin 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 thin 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 INI parameters is simple and an easy way to configure a ThinOS thin client to be a basic network print server, to share local printers with other thin 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 thin 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 thin 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, RDP or ICA) because ThinOS 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 thin client identifies with the thin client ID number 84 and thus is recognized as a thin 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 8.0_214, 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 device using either DameWare or VNC Viewer. Prior to 8.0_214, you could only use VNC Viewer.

D

Troubleshooting

This section describes some basic troubleshooting that you can implement when you experience any problem.

- Firmware/Package update: When the packages fail to update, or cannot function (cannot connect desktop) after update with new version firmware, or if there is further failure, the workaround is to remove all packages and reinstall the packages upon reboot.
- Blast connection: If there is a launch issue, check the remote desktop status and network status; reboot unit few times and the desktop connects successfully.

E

Frequently asked questions

Question: How to enable USB Redirection in RDP windows 10 session?

Solution—You must change the policy. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Service** > **Remote Desktop Session Host** > **Device and Resource Redirection** > **Do not allow supported Plug and Play device redirection** and disable this policy.

Firmware installation

Firmware installation is the process of installing the ThinOS firmware on your thin client. To install the ThinOS firmware, use any of the following methods:

- File Transfer Protocol (FTP) Windows server
- HTTP/HTTPS Windows server
- Dell Wyse Management Suite version 1.2
- Dell Wyse USB Imaging Tool version 3.1.0

Table 41. Firmware images

Platform	ThinOS	ThinOS with PCoIP
Wyse 5070 thin client—Celeron processor	X10_wnos	PX10_wnos
Wyse 5070 thin client—Pentium processor	X10_wnos	PX10_wnos
Wyse 5070 Extended thin client—Pentium processor	X10_wnos	PX10_wnos

Table 42. Package information

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

NOTE:

- – Before you install the firmware, or start the ThinOS client, Dell recommends that you connect the monitor, keyboard, mouse, and network to ensure that the thin client functions properly.
  – ThinOS checks for a network connection after boot up, before loading packages.

Firmware installation 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 wnos. The directory structure must read as C:\inetpub\ftproot\WYSE\wnos.

To upgrade the ThinOS firmware using FTP server:

1 Go to www.dell.com/support.
2 Download the latest ThinOS firmware and latest ThinOS 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\wnos folder, and the packages to C:\inetpub\ftproot\WYSE\wnos\pkg on your FTP server.
4 Create a wnos.ini text file (using a text editor) in the C:\inetpub\ftproot\WYSE\wnos folder with the following INI parameters:

```
Autoload=1 loadpkg=1 Addpkg=TCX,FR,horizon
```

The option `Autoload=1` enables the forced firmware installation/upgrade process. 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 and the PCoIP package are integrated into the ThinOS firmware image. Installing the latest ThinOS firmware image automatically installs the latest version of these packages on the ThinOS 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 8.3, 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 Dell Wyse ThinOS INI Reference Guide.

5 Save the wnos.ini file.
6 On the ThinOS client desktop, navigate to **System Setup** > **Central Configuration** > **General**.
7 In the **General** tab, enter the IP address of the FTP server or directory, username and password. The **Username** field must have the value `Anonymous` and the **Password** field is already pre-configured. If the FTP server supports Anonymous, then enter the username as **Anonymous** and use the pre-configured password, or just leave the **Username** and **Password** fields blank.

> **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 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 desktop, navigate to **System Information** > **General**, and check the System Version.

Firmware installation 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. 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 wnos. The directory structure must read as C:\inetpub\wwwroot\WYSE\wnos.

To upgrade the ThinOS firmware using HTTP or HTTPS server:

1. Go to www.dell.com/support.
2. Download the latest ThinOS firmware and latest ThinOS 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\wnos folder, and the packages to C:\inetpub\wwwroot\WYSE\wnos\pkg on your HTTP or HTTPS server.
4. Create a wnos.ini text file (using a text editor) in the C:\inetpub\wwwroot\WYSE\wnos folder with the following INI parameters:

   ```
   Autoload=1 loadpkg=1 Addpkg=TCX,FR,horizon
   ```

   The option `Autoload=1` enables the forced firmware installation/upgrade process. 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 and the PCoIP package are integrated into the ThinOS firmware image. Installing the latest ThinOS firmware image automatically installs the latest version of these packages on the ThinOS 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 8.3, 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 Dell Wyse ThinOS INI Reference Guide.
5. Save the wnos.ini file.
6. On the ThinOS 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 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 installation using Wyse Management Suite

Ensure that you have created a custom group and assigned the ThinOS devices to that group in Wyse Management Suite—see the latest Dell Wyse Management Suite Administrator's Guide.
Ensure that your ThinOS clients are registered to Wyse Management Suite.

To upgrade the ThinOS firmware using Wyse Management Suite:

1. Go to www.dell.com/support.
2. Download the latest ThinOS firmware and ThinOS 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 firmware file is uploaded, and the firmware file is listed on the **Apps & Data - ThinOS OS Image Repository** page.
8. Select the check box that corresponds to your ThinOS firmware file.
9. On the **Groups & Configs** page, select a custom group, and click **Edit Policies** > **ThinOS**.

   The **Select ThinOS 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.

Firmware installation using Dell Wyse USB Imaging Tool

Use the Dell Wyse USB Imaging Tool version 3.1.0 to install the ThinOS merlin image on your thin client. For information about installation instructions, see the *Dell Wyse USB Imaging Tool version 3.1.0 User's Guide* at downloads.dell.com/wyse/USBFT/3.1.0/.