Administrators Guide

Wyse® Enhanced
Microsoft® Windows® Embedded Standard 7 WFR2

Products: C90LE7, D90D7, R90L7, R90LE7, X90c7, X90m7, Z90D7, Z90DE7, Z90S7

Issue: 031813
PN: 883920-10 Rev. D

WYSE

Copyright Notices

End User License Agreement (“License”)

A copy of the Wyse Technology End User License Agreement is included in the software and provided for your reference only. The License at http://www.wyse.com/license as of the purchase date is the controlling licensing agreement. By copying, using, or installing the software or the product, you agree to be bound by those terms.

Trademarks

The Wyse logo and Wyse are trademarks of Wyse Technology Inc. Other product names mentioned herein are for identification purposes only and may be trademarks and/or registered trademarks of their respective companies. Specifications subject to change without notice.

Patents

This product and/or associated software are protected by copyright, international treaties, and various patents, including the following U.S. patents: 6,836,885 and 5,918,039.

Restricted Rights Legend

You acknowledge that the Software is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments. For additional information on exporting the Software, see http://www.microsoft.com/exporting.

Ordering Information

For availability, pricing, and ordering information in the United States and Canada, call 1-800-GET-WYSE (1-800-438-9973) or visit us at **wyse.com**. In all other countries, contact your sales representative.

FCC Statement

This equipment has been tested and found to comply with the limits for either Class A or Class B digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interconnect cables and shielded AC power cable must be employed with this equipment to insure compliance with the pertinent RF emission limits governing this device. Changes or modifications not expressly approved by the system's manufacturer could void the user's authority to operate the equipment.

CAUTION: Modifications made to the product, unless expressly approved by Wyse Technology, could void the user’s authority to operate the equipment.

Regulatory Compliance for Wyse Products

Basic EMC and Safety Requirements

Wyse appliances are compliant with the regulatory requirements in the regions listed below.

U.S.A.—FCC Part 15 (class B), cUL 60950

Canada—IC ICES-003, CAN/CSA-C22 No. 60950

Europe—EN 55022 (class B); EN 55024

Canadian DOC Notices

Class A - This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Class B - This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe B prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Wireless Usage and Requirements

Radio transmitting type devices (RF modules) are present in the models with the wireless option. These devices operate in the 2.4 GHz band (i.e. 802.11b/g WLAN and Bluetooth).

As a general guideline, a separation of 20 cm (8 inches) between the wireless device and the body, for use of a wireless device near the body (this does not include extremities) is typical. This device should be used more than 20 cm (8 inches) from the body when wireless devices are on and transmitting.

Some circumstances require restrictions on wireless devices. Examples of common restrictions include:

- When in environments where you are uncertain of the sanction to use wireless devices, ask the applicable authority for authorization prior to use or turning on the wireless device.
- Every country has different restrictions on the use of wireless devices. Since your system is equipped with a wireless device, when traveling between countries with your system, check with the local Radio Approval authorities prior to any move or trip for any restrictions on the use of a wireless device in the destination country.
- Wireless devices are not user-serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact the manufacturer for service.

Device Power Supply

Use only the external power supply that comes with your thin client. For power and voltage ratings, see the serial number label or regulatory label on your device. For power adapter replacement, contact your Wyse Service Representative. For proper replacement compare the labels on both mobile thin client and power adapter to ensure that their voltages match.

WARNING: Use of any other power adapter may damage your mobile thin client or the power adapter. The damage caused by an improper power adapter is not covered by warranty.

Battery Information

Models Cx0, Dx0D, Rx0L, Rx0LE, Xx0C, Xn0m, Zx0, and Zx0D contain an internal button cell battery replaceable by Wyse or one of our Authorized Service Centers. For service, visit http://www.wyse.com/serviceandsupport/service/service.asp.

WARNING: There is a risk of explosion if the battery is replaced by an incorrect type. Always dispose of used batteries according to the instructions accompanying the battery. Dispose of your battery properly when it no longer holds a charge or is damaged. Contact your local waste or environmental agency for instructions.

Perchlorate Materials - Special Handling May Be Required under California Code of Regulations, title 22. (Only required within the U.S.A.)

Models Xx0C and Xn0m mobile thin clients contain a user-replaceable battery pack. The battery is designed to work with your Wyse mobile thin client. Do not use a battery from other mobile thin clients or laptop computers with

your mobile thin client. Replace the battery only with a compatible battery purchased from Wyse's spare parts provider or one of our authorized service centers. For spare parts visit http://www.wyse.com/serviceandsupport/service/spares.asp.

WARNING: There is a risk of explosion if the battery pack is replaced by an incorrect type. Always dispose of used batteries according to local ordinance and/or regulation.

CAUTION: Misuse of the battery pack may increase the risk of fire of chemical burn. Do not puncture, incinerate, disassemble, or expose the battery to temperatures above 65°C (149°F). Keep the battery away from children. Handle damaged or leaking batteries with extreme care. Damaged batteries may leak and cause personal injury or equipment damage.

Contents

Summary of Revisions

Wyse Technology Inc. 883920-10 Rev. D

The following changes were made to this document since revision C:

Reference	Description
D90D7 and Z90DE7	D90D7 and Z90DE7 product support added to this guide.

Wyse Technology Inc. 883920-10 Rev. C

The following changes were made to this document since revision B:

Reference	Description
New X90m7 support	New X90m7 product support added to this guide.

Wyse Technology Inc. 883920-10 Rev. B

The following changes were made to this document since revision A:

Reference	Description
Updated figures and workflow	Figures and workflow instructions have been updated to include and describe the new user interface features.
New sections added to guide	"Connecting to a Printer" and "Connecting to a Monitor" quick reference sections added to "Getting Started: Quickly Learning the Basics."
"Using Realtek HD Audio Manager"	New Realtek HD Audio Manager feature added to "Notable Administrator Features."
"Using the WCM Client"	New Wyse Configuration Manager *WCM Client* feature added to "Notable Administrator Features."

This page intentionally blank.

1 Introduction

Wyse® thin clients running Wyse® Enhanced Microsoft® Windows® Embedded Standard 7 WFR2 provide access to applications, files, and network resources made available on machines hosting Citrix™ ICA and Microsoft™ RDP session services. The thin clients contain a full featured Internet Explorer browser and thin client emulation software, Ericom — PowerTerm® TEC. Other locally installed software permits remote administration of the thin clients and provides local maintenance functions. Additional add-ons are available that support a wide range of specialty peripherals and features for environments needing a secure Windows user interface with 32-bit Windows compatibility. Your thin client supports Microsoft Silverlight and Microsoft NET Framework 3.5 or later (for more information about Silverlight and Framework, see http://www.microsoft.com).

Session and networks services available on enterprise networks may be accessed on enterprise networks, a direct intranet connection, or from a remote location using a secure gateway from Citrix or VMware.

About this Guide

This guide is intended for administrators of Wyse thin clients running Wyse Enhanced Microsoft Windows Embedded Standard 7 WFR2. It provides information and detailed system configurations to help you design and manage a Wyse thin client environment. Depending on your hardware and software configurations, the figures you see may be different than the example figures shown in this guide.

This guide supplements the standard Microsoft Windows Embedded Standard 7 documentation supplied by Microsoft Corporation. It explains the differences, enhancements, and additional features provided by Wyse with the thin client. It does not attempt to describe the standard features found in Microsoft Windows Embedded Standard 7.

Windows Embedded Standard 7help can be accessed from the Microsoft Help and Support Web site at: http://support.microsoft.com/default.aspx.

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.

Wyse Technical Support

To access Wyse technical resources, visit http://www.wyse.com/support. If you still have questions, you can submit your questions using the Wyse Self-Service Center at http://support.wyse.com/selfservice.html or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

To access international support, visit http://www.wyse.com/global.

Related Documentation and Services

Fact Sheets containing the features of hardware products are available on the Wyse Web site. Go to http://www.wyse.com/products and use the *Cloud clients* tab to locate and download the Fact Sheet for your hardware product.

If you need to upgrade your Windows Embedded Standard 7 operating system, contact Wyse Customer Support at: http://www.wyse.com/support.

Wyse Cloud Software is available on the Wyse Web site at: http://www.wyse.com/products/software.

Wyse Online Community

Wyse maintains an online community where users of our products can seek and exchange information on user forums. Visit the Wyse Online Community forums at: http://community.wyse.com/forum.

2 Getting Started: Quickly Learning the Basics

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

- "Logging On"
- "Using Your Desktop"
- "Before Configuring Your Thin Clients"
- "Connecting to a Printer"
- "Connecting to a Monitor"
- "Logging Off"

TIP: While it can be used in environments without central configuration for basic connectivity needs, Wyse thin clients are designed to be centrally managed and configured using network and session services. In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all thin clients in your environment (see "Establishing a Server Environment").

CAUTION: To save any configurations you make on a thin client to persist after a thin client reboot, be sure to disable the File Based Write Filter *before* your configurations to the thin client, and then enable the File Based Write Filter *after* your configurations as described in "Before Configuring Your Thin Clients."

Logging On

What you see, initially, when you turn on or reboot a thin client, depends on the administrator configurations. After creating users (see "Managing Users and Groups with User Accounts"), administrators can configure a user account to logon automatically (see "Enabling and Disabling Automatic Logon Using Winlog") or require manual logon with user credentials.

CAUTION: It is recommended that all default passwords be changed on all thin clients (be sure to remember any new administrator password, as you will not be able to log on as an administrator without it). Only administrators can log on to a thin client and change passwords by using the CTRL+ALT+DEL key combination to open the *Windows Security* window, clicking **Change a Password**, and then using the **Change a Password** dialog box. Be sure to disable the File Based Write Filter *before* you change a password on the thin client, and then enable the File Based Write Filter *after* your change as described in "Working with the File Based Write Filter Utility."

Automatic Logon

For security, automatic logon to a *User* desktop is enabled on the thin client by default (and is a member of the *User* group; *not* a member of the *Administrator* group).

TIP: After automatic logon to a *User* desktop, *AutoPlay* for USB devices is disabled by default. To enable *AutoPlay* for a USB device, select the USB device you want in the **Devices and Printers** dialog box (**Start > Control Panel > Devices and Printers**) and click **AutoPlay**.

To log on as a different user or an administrator:

1. Use the *Log off* button (**Start > Log off**) to log off the current desktop while holding down the SHIFT key until the *Log On* window displays.
2. Log on as follows (passwords are case sensitive):
   - *Administrators* - default *Username* is **administrator** and default *Password* is **Wyse#123**.
   - *Users* - default *Username* is **user** and default *Password* is **Wyse#123**.

TIP: As an administrator, you can use *Winlog* to configure *your* thin client to start with the *Log On* window so that you can simply log on as an administrator (see "Enabling and Disabling Automatic Logon Using Winlog").

Manual Logon

If automatic logon is *not* enabled, the *Log On* window displays upon thin client startup.

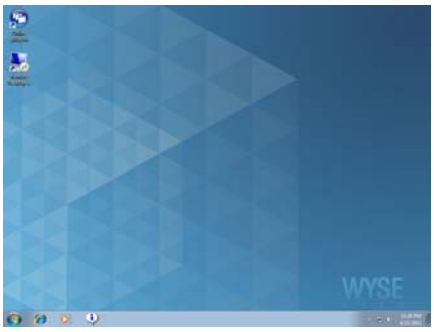
Log on as follows (passwords are case sensitive):

- *Administrators* - default *Username* is **administrator** and default *Password* is **Wyse#123**.
- *Users* - default *Username* is **user** and default *Password* is **Wyse#123**.

Using Your Desktop

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

TIP: For information about the functionality of the standard Windows Embedded Standard 7 desktop and *Start* menu items, see the Microsoft documentation (go to http://support.microsoft.com and navigate to the Windows 7 Support Center).



User Desktop - typically contains a full user taskbar, desktop with default connection icons, *Start Menu* (click the *Start* button to open the user menu), and the icons of the user system tray.

To connect to a connection (or switch between connections), simply click on the desktop connection icon you want or use the connection links in the *Start Menu*. See also "Notable User Features."

Administrator Desktop - contains a full administrator taskbar, desktop with default connection icons, File Based Write Filter icons, right-click desktop pop-up menu, *Start Menu* (click the *Start* button to open the administrator menu), and the icons of the administrator system tray.

In addition to the standard *Control Panel* icons, an extended set of resources for configuring user preference settings and system administration is included in the administrator *Control Panel* (**Start > Control Panel**). See also "Notable Administrator Features."

Before Configuring Your Thin Clients

Before you configure your thin clients, be aware that some utilities that are meant to protect thin clients will prevent your thin client configurations from persisting after log off and restart. That is, local settings and profile configurations you make are removed by utilities that prevent undesired flash memory writes and “clean-up” extraneous information from being stored on the local disk. While these utilities protect thin clients in important ways, there are instances where administrators want configurations to persist after logging off and restarting a thin client.

CAUTION: *Before* configuring your thin client, see "Working with the File Based Write Filter Utility" and "Working with the NetXClean Utility."

TIP: To help you to easily configure and manage multiple thin clients, use Wyse products such as the *Wyse USB Firmware Tool* and *Wyse Device Manager* (see http://www.wyse.com/products).

Working with the File Based Write Filter Utility

The File Based Write Filter provides a secure environment for thin client computing by protecting the thin client from undesired flash memory writes. Changes made to the thin client configurations are lost when the thin client is restarted unless the files of the File Based Write Filter cache are flushed/committed during the current system session. Only administrators can modify thin client configurations to persist after a thin client reboot.

1. Log on as an administrator (see "Logging On").
2. Disable the File Based Write Filter by double-clicking the **FBWF Disable** (red) icon on the desktop (this will disable the filter and reboot the system).
3. If automatic logon to a user desktop is enabled, you must log off the user desktop and log on as an administrator (as you did in step 1).
4. Configure the thin client as you want using the instructions in this guide.
5. After you complete your configurations, you must enable the File Based Write Filter by double-clicking the **FBWF Enable** (green) icon on the desktop (this will enable the filter and reboot the system). Your configurations on the thin client are now saved and they will persist after a thin client reboot.

For general information about the File Based Write Filter, see "Using the File Based Write Filter (FBWF)."

Working with the NetXClean Utility

NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. If you want to keep certain profile configurations (for example, printers and other peripherals), be sure to configure NetXClean to refrain from cleaning up any number of the explicitly declared profiles you want.

For general information about NetXClean, see "Understanding the NetXClean Utility."

For detailed instructions on using NetXClean, see Wyse Knowledge Base Solution #**10621** (go to the Wyse Knowledge Base at http://www.wyse.com/kb and search for **10621**).

Connecting to a Printer

To connect a parallel printer to your thin client through a USB port, you will need a USB-to-printer adapter cable (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 Devices and Printers."

Connecting to a Monitor

Depending on your thin client hardware, connections to monitors can be made using either a VGA (analog) monitor port or a DVI (digital) monitor port and the proper Wyse monitor cables/splitters. For information on configuring dual display settings, see "Configuring Dual Monitor Display."

TIP: For dual-monitor supported thin clients using a DVI to DVI/VGA splitter with VGA and DVI monitors at the same time, note that the VGA monitor will be the primary monitor.

Logging Off

Use the *Log off* menu (click **Start > Log Off arrow**) to select the option you want (log off, lock, restart, sleep, or shut down). You can also log off the thin client using the *Windows Security* window (opened by using CTRL+ALT+DEL key combination).

TIP: If automatic logon is enabled when you log off, the thin client immediately logs on to the default user desktop; use *Shut down* to turn the thin client off.

This page intentionally blank.

3 Notable User Features

This chapter includes an overview of the following notable Wyse-extended features for users found in the *All Programs* menu (**Start** > **All Programs**):

- "Browsing the Internet with Internet Explorer"
- "Viewing Wyse Client Information"
- "Managing Connections with the Citrix Online Plug-in"
- "Managing Connections with Ericom — PowerTerm® TEC"
- "Establishing Remote Desktop Connections"
- "Using VMware View Client to Connect to a Virtual Desktop"

TIP: For *ELO Touchscreen* information, see "Configuring Touchscreens."

Browsing the Internet with Internet Explorer

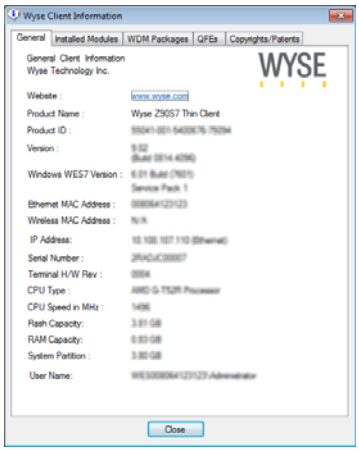
Use **Microsoft Internet Explorer 8** for your browser needs (**Start** > **All Programs > Internet Explorer**). The browser has Internet option settings that have been preselected at the factory to limit writing to flash memory. These settings prevent exhaustion of the limited amount of flash memory available and should not be modified. If more browser resources are required, you can access another browser through an ICA or RDP session.

TIP: The protected mode status of Internet Explorer is *Off*. This is because *User Access Control* (UAC) has been disabled in the build. The File Based Write Filter (FBWF) contained in the build will continue to protect your system (see "Using the File Based Write Filter (FBWF)").

Viewing Wyse Client Information

Use the **Wyse Client Information** dialog box (**Start** > **All Programs > Wyse Client Information**) to view information about the thin client (the information shown in the dialog box varies for different thin clients and software releases).

For example, the **General** tab displays thin client information such as the Website, Product Name, Product ID, Version, Windows WES7 Version, Ethernet MAC Address, Wireless MAC Address, IP Address, Serial Number, Terminal H/W Rev, CPU Type, CPU Speed in MHz, Flash Capacity, RAM Capacity, System Partition, and User Name.

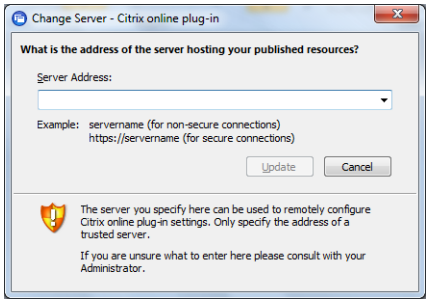


You can also click the following tabs to view additional thin client information:

- **Installed Modules** - Displays the list of applications that are installed on the thin client.
- **WDM Packages** - Displays the list of WDM Packages that have been applied to the thin client (see "Using Wyse Device Manager Software for Remote Administration").
- **QFEs** - Displays the list of Microsoft QFEs (formerly Hotfixes) applied to the thin client.
- **Copyrights/Patents** - Displays Wyse copyright and patent information.

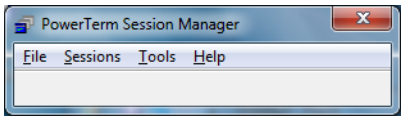
Managing Connections with the Citrix Online Plug-in

Use the **Citrix Online Plug-in** to access your hosted applications from your desktop or a Web interface (**Start > All Programs > Citrix Online Plug-in** or double-click the **Citrix Online Plug-in** desktop icon). Citrix documentation is available on the Citrix Web site at: http://www.citrix.com.

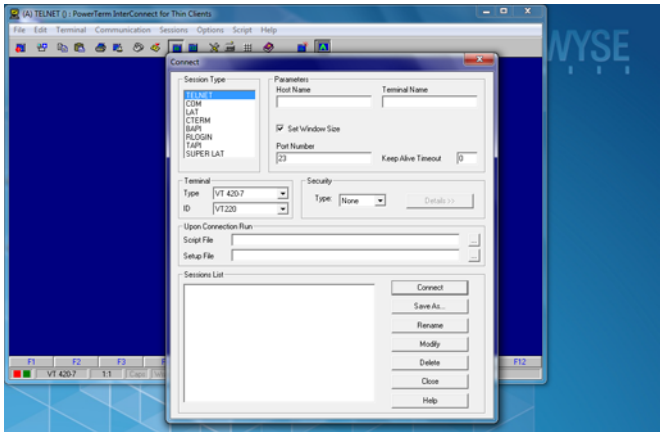


Managing Connections with Ericom — PowerTerm® TEC

Use the **PowerTerm Session Manager** (**Start** > **All Programs > Ericom-PowerTerm Terminal Emulation > PowerTerm Session Manager**) to manage your connections.

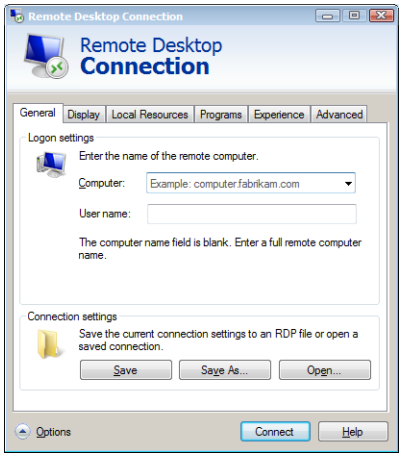


Use the **TELNET** window and the **Connect** dialog box (**Start** > **All Programs > Ericom-PowerTerm Terminal Emulation > PowerTerm Terminal Emulation**) to configure your connection information. Ericom — PowerTerm® TEC documentation is available at: http://www.wyse.com/manuals.



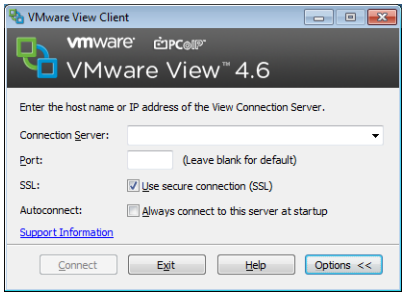
Establishing Remote Desktop Connections

Use the **Remote Desktop Connection** dialog box (**Start** > **All Programs > Remote Desktop Connection** or click the **Remote Desktop Connection** desktop icon) to establish and manage connections to remote applications. The standard version (default) is used for a single monitor display, while the *Span* version can be used when extending a single session to two monitors (for dual-monitor capable thin clients). If you find that the File Based Write Filter cache is becoming too full, you can disable Bitmap caching in the *Experience* tab (expanded view). Microsoft documentation is available on the Microsoft Web site at: http://www.microsoft.com.



Using VMware View Client to Connect to a Virtual Desktop

Use the **VMware View Client** dialog box (**Start** > **All Programs > VMware > VMware View Client**) to connect to a virtual desktop.

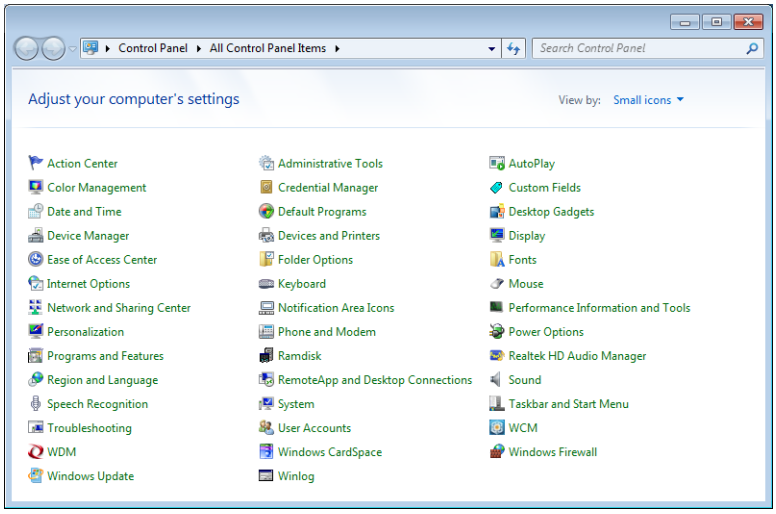


1. In the *Connection Server* drop-down menu, enter the host name or IP address of a *View Connection Server*, configure any *Options* you want, and then click **Connect**.
2. Enter the your credentials and click **Login**.
3. Select a desktop from the list provided and click **Connect**. *VMware View Client* connects to the selected desktop. After connection, the client window appears.

VMware View Client documentation is available on the VMware Web site at: http://www.vmware.com.

4 Notable Administrator Features

This chapter includes an overview of the following notable Wyse extended features for administrators found in the administrator *Control Panel* (**Start** > **Control Panel**):



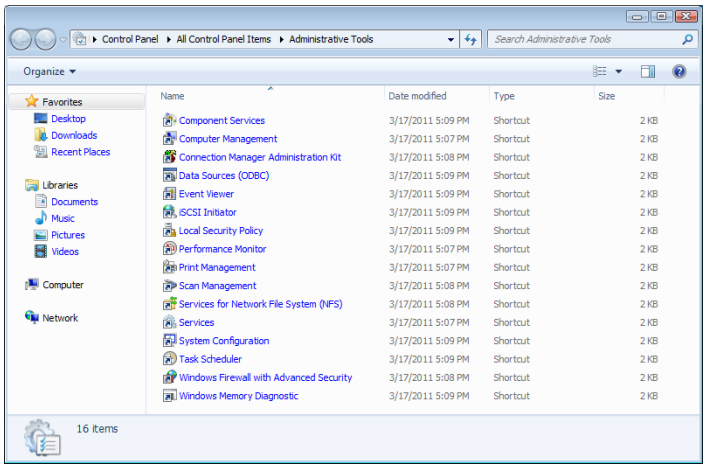
- "Accessing and Using the Administrative Tools"
- "Configuring Bluetooth Wireless Connections"
- "Setting Configuration Strings with Custom Fields"
- "Configuring Devices and Printers"
- "Configuring Dual Monitor Display"
- "Configuring Touchscreens"
- "Setting Ramdisk Size"
- "Using Realtek HD Audio Manager"
- "Selecting Region and Language"
- "Controlling Sounds and Audio Devices"
- "Managing User Accounts"
- "Using the WCM Client"
- "Configuring WDM Properties"
- "Enabling and Disabling Automatic Logon Using Winlog"
- "Configuring Wireless Local Area Network (LAN) Settings" (see also "Preserving Wireless Connections with the Regpersistence Tool")

TIP: Although users can be given permissions to configure some of the following features (for example, dual monitor display settings), only administrators can use the File Based Write Filter to modify thin client configurations to persist after a thin client reboot.

Accessing and Using the Administrative Tools

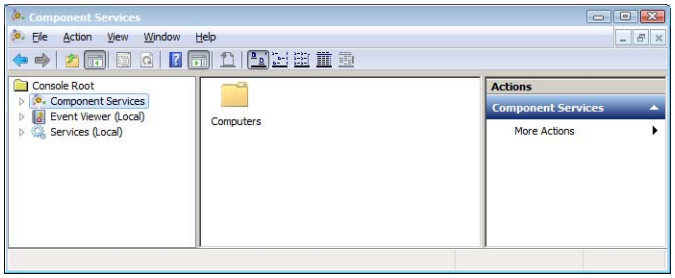
Use the **Administrative Tools** window (*Control Panel* **> Administrative Tools** icon) to access the following Wyse enhanced administrative tools:

- "Configuring Component Services"
- "Viewing Events"
- "Managing Services"



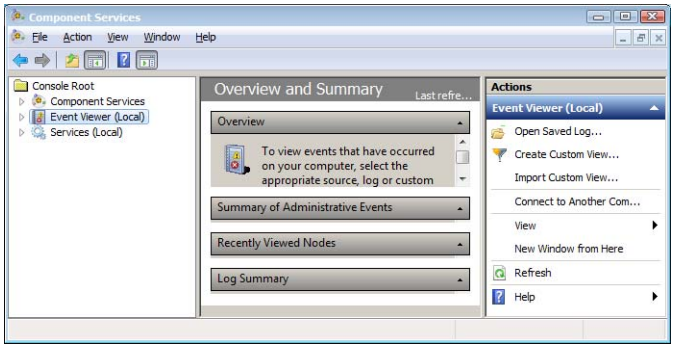
Configuring Component Services

Use the **Component Services** console (double-click the **Component Services** icon) to access and configure the *Component Services*, *Event Viewer*, and *Local Services*.



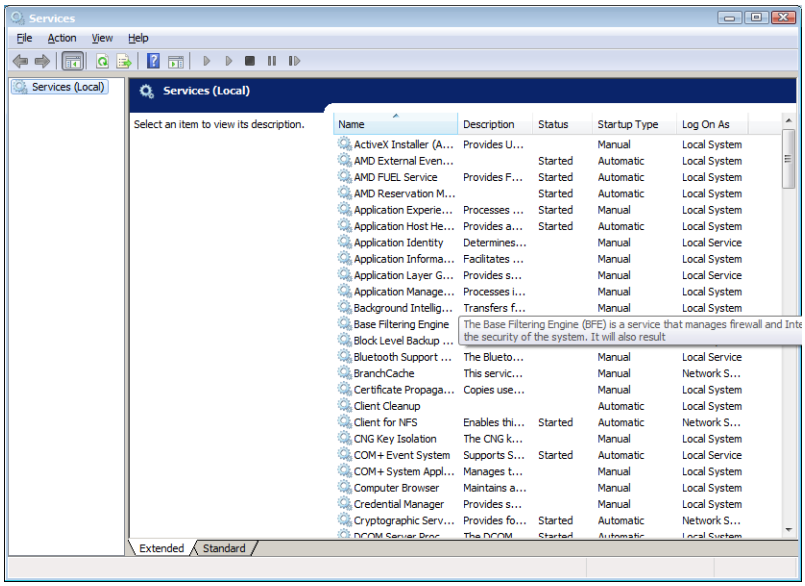
Viewing Events

Use the **Event Viewer** window (double-click the **Event Viewer** icon) to view monitoring and troubleshooting messages from Windows and other programs.



Managing Services

Use the **Services** window (double-click the **Services** icon) to view and manage the services installed on the thin client. *Client Clean-up* (NetXClean) and *VNC Server* are two services which may need to be stopped (using the *Task Manager*) or restarted by a thin client administrator and are discussed in "Understanding the NetXClean Utility" and "Configuring TightVNC Server Properties."

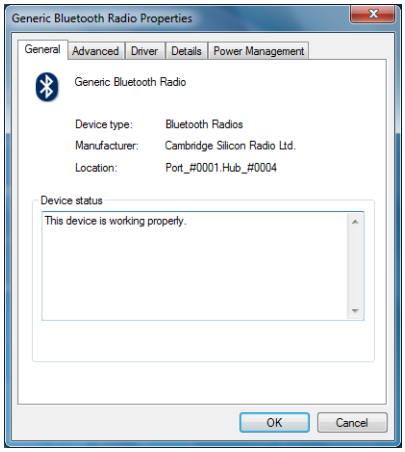


Configuring Bluetooth Wireless Connections

If the thin client has optional Wireless and Bluetooth capability, you can use your thin client with other Bluletooth-enabled devices.

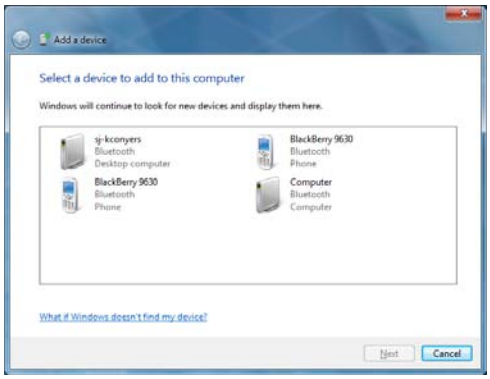
CAUTION: Be sure to flush the files of the File Based Write Filter cache to save the installation, and be sure to configure NetXClean to refrain from cleaning up your settings (see "Before Configuring Your Thin Clients").

Use the properties dialog box of an existing Bluetooth device (*Control Panel* **> Device Manager**, expand **Bluetooth Radios**, and then double-click the *Bluetooth* icon you want in the list; for example, *Generic Bluetooth Radio*) to manage an existing Bluetooth device. For example, you can update drivers using the *Driver* tab.



If you want to add another Bluletooth-enabled device to the thin client, you can use the *Add a Device* wizard.

1. Click the **Devices and Printers** icon in *Control Panel* to open the **Devices and Printers** window.
2. Click **Add a Device** to open and use the *Add a Device* wizard.
   TIP: Follow the instructions to turn on the Bluetooth-enabled device and ensure the device is discoverable (see the device documentation). When the Bluetooth-enabled device is discovered by the thin client, select the device, click **Next**, and then follow the wizard.



Setting Configuration Strings with Custom Fields

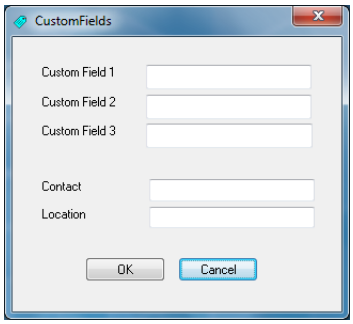
Use the **Custom Field** dialog box (*Control Panel* **> Custom Fields** icon) to enter configuration strings for use by Wyse Device Manager (WDM) software. The configuration strings can contain information about the location, user, administrator, and so on.

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*.

CAUTION: To permanently save the information, be sure to flush the files of the File Based Write Filter cache during the system session in which the registry entries are made or changed (see "Before Configuring Your Thin Clients").

For more information on using WDM for remote administration and upgrading thin client software, see "Using Wyse Device Manager Software for Remote Administration."

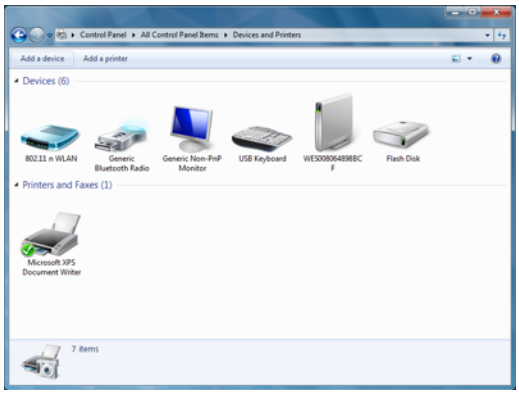
For details on using Custom Field information, see the WDM documentation.



Configuring Devices and Printers

Use the **Devices and Printers** window to add devices (see "Adding Devices") and printers (see "Adding Printers").

CAUTION: Be sure to flush the files of the File Based Write Filter cache to save the installation, and be sure to configure NetXClean to refrain from cleaning up your device or printer settings (see "Before Configuring Your Thin Clients").



Adding Devices

If you want to add a device to the thin client, you can use the *Add a Device* wizard.

1. Click the **Devices and Printers** icon in *Control Panel* to open the **Devices and Printers** window.
2. Click **Add a Device** to open and use the *Add a Device* wizard.

Adding Printers

If you want to add a printer to the thin client, you can use the *Add Printer* wizard.

1. Click the **Devices and Printers** icon in *Control Panel* to open the **Devices and Printers** window.
2. Click **Add a Printer** to open and use the *Add Printer* wizard.

A universal print driver is installed on the thin client to support text-only printing to a locally-connected printer. To print full text and graphics to a locally-connected printer, install the driver provided by the manufacturer according to the instructions.

Printing to network printers from ICA and RDP applications can be achieved through print drivers on the servers.

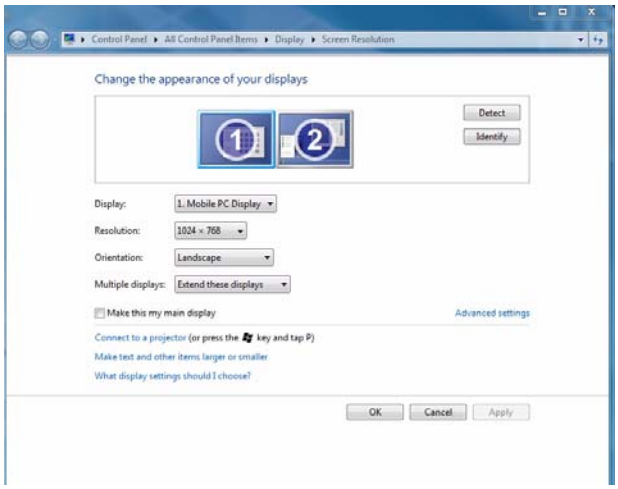
Printing to a locally-connected printer from an ICA or RDP session using the print drivers of the server produces full text and graphics functionality from the printer. To do this, install the print driver on the server and the text only driver on the thin client according to the following procedures:

1. Connect the printer to the thin client.
2. Click the **Devices and Printers** icon in *Control Panel* to open the **Devices and Printers** window.
3. Click **Add a printer** to open the *Add Printer* wizard, and then click **Next**.
4. Select **Add a local printer**.
5. Select **Use an existing port**, select the port from the list, and then click **Next**.
6. Select the manufacturer and model of the printer and click **Next**.
7. Enter a name for the printer and click **Next**.
8. Select **Do not share this printer** and click **Next**.
9. Select whether or not to print a test page and click **Next**.
10. Click **Finish** (the installation will complete and a test page will print if this option was selected).

Configuring Dual Monitor Display

(*For Dual-Monitor Capable Thin Clients Only*) Use the **Screen Resolution** window (*Control Panel* **>** **Display** icon **>** **Change Display Settings** link) to configure the dual monitor settings as described in the Microsoft documentation at: http://www.microsoft.com. For Wyse Multi-Display Support and dual monitor support information, visit the Wyse Knowledge Base at: http://www.wyse.com/kb.

CAUTION: When configuring dual monitor settings, be sure to set both monitors to the same screen resolution.



Configuring Touchscreens

If the *ELO Touchscreen* option is installed on the thin client, clicking the **ELO Touchscreen** icon in a user or administrator *Control Panel* allows you to calibrate and customize the settings for a touchscreen monitor that is connected to (or integrated with) a thin client. Re-calibration and adjustment of the monitor settings may be required after updating thin client software.

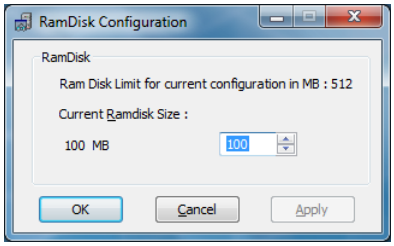
Setting Ramdisk Size

Ramdisk is volatile memory space used for temporary data storage. It is the Z drive shown in the **My Computer** window. It can also be used for temporary storage of other data according to administrator discretion (see "Saving Files and Using Local Drives").

The following items are stored on Ramdisk:

- Browser Web page cache
- Browser history
- Browser cookies
- Browser cache
- Temporary Internet files
- Print spooling
- User/system temporary files

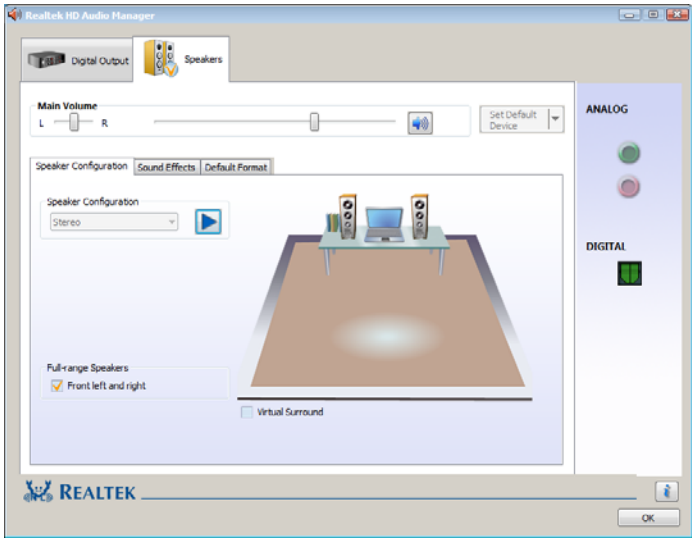
Use the **Ramdisk Configuration** dialog box (*Control Panel* **> Ramdisk** icon) to configure the Ramdisk size. If you change the size of the Ramdisk, you will be prompted to restart the system for the changes to take effect. However, to permanently save the changes be sure that the files of the File Based Write Filter cache have been flushed during the current system session *before* restarting the system (see "Before Configuring Your Thin Clients").



TIP: Depending on the thin client model and installed memory size, default Ramdisk size may vary. The minimum Ramdisk size that can be set is 2 MB; the maximum Ramdisk size that can be set is approximately 20% of actual RAM for a system with 512 MB or less of RAM, and approximately 10% of actual RAM for a system with more than 512 MB of RAM (note that for a system with 1 GB or more of RAM, the maximum Ramdisk size that can be set is limited to 100 MB).

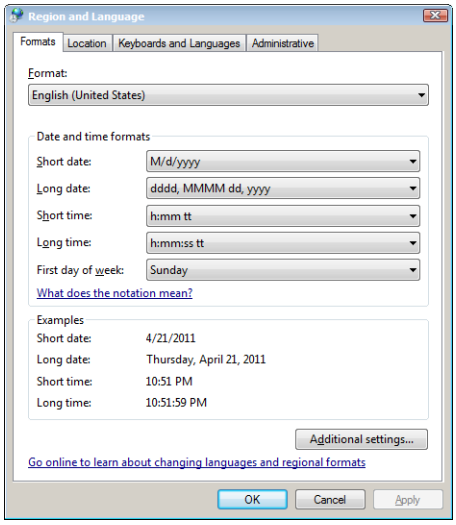
Using Realtek HD Audio Manager

Use the **Realtek HD Audio Manager** dialog box (*Control Panel* **> Realtek HD Audio Manager** icon) to manage your audio and audio devices. Volume can also be adjusted using the **Volume** icon in the system tray of the taskbar (click the **Volume** icon to open the master volume control). Powered speakers are recommended.



Selecting Region and Language

Use the **Region and Language** dialog box (*Control Panel* **> Region and Language** icon) to select your keyboard language.



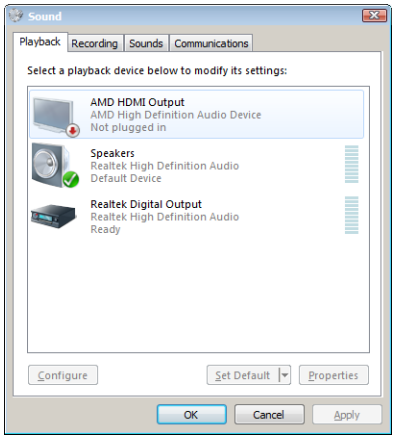
The following keyboard languages are supported (a language appropriate keyboard is required for any language other than English (US)):

Arabic	Finnish	Romanian
Belgian Dutch	French	Russian
Belgian French	German	Slovak
Brazilian (ABNT)+A34	Greek	Slovenian
Canadian Eng. (Multi)	Hebrew	Spanish
Canadian Fr (Multi)	Hungarian	Spanish Variation
Canadian French	Italian	Swedish
Czech	Italian (142)	Swiss French
Croatian	Latin American	Swiss German
Danish	Norwegian	Thailand
Dutch	Polish (214)	Turkish-F
English (UK)	Polish (Programmers)	Turkish-Q
English (US) (default)	Portuguese	US International

Third-party applications, Wyse applications, and Microsoft names remain in English after the interface is changed. If your thin client contains a multi-language build and you want to change to another language, be sure to restart the thin client after you select the language you want.

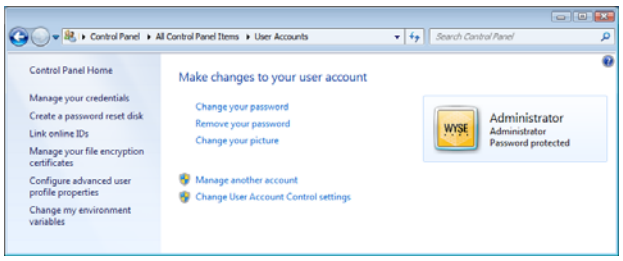
Controlling Sounds and Audio Devices

Use the **Sound** dialog box (*Control Panel* **> Sound** icon) to manage your audio and audio devices. Volume can also be adjusted using the **Volume** icon in the system tray of the taskbar (click the **Volume** icon to open the master volume control). Powered speakers are recommended.



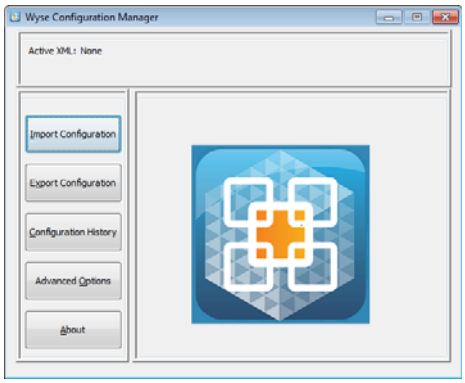
Managing User Accounts

Use the **User Accounts** window (*Control Panel* **> User Accounts** icon) to manage users and groups. For detailed information on the **User Accounts** window, see "Managing Users and Groups with User Accounts."



Using the WCM Client

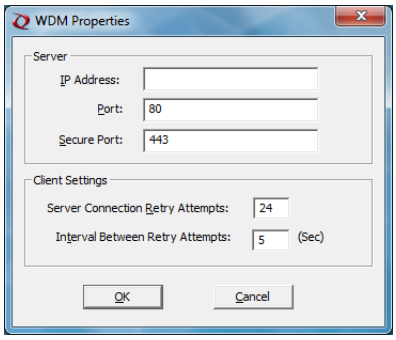
Use the **WCM Client** (*Control Panel* **> WCM** icon) to apply configuration files (created by the *WCM Application*) to the thin client.



Wyse Configuration Manager™ provides a simple solution to create and apply configuration files to Wyse thin clients. For information on obtaining and using Wyse Configuration Manager, see *Administrators Guide: Wyse Configuration Manager™*.

Configuring WDM Properties

Use the **WDM Properties** dialog box (*Control Panel* **>** **WDM** icon) to configure the Wyse Device Manager server location and thin client settings.



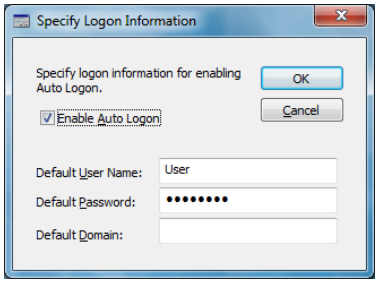
1. Configure *Server* settings:
   - Enter the *IP Address* or hostname of the WDM server.
   - Enter the *Port* to use (default is **80**).
   - (Optional) If you are using HTTPS, enter the *Secure Port* to use (default is **443**).
2. Configure *Client* settings:
   - Enter the *Server Connection Retry Attempts* (number of attempts to connect to the WDM server after a failed attempt).
   - Enter the *Interval Between Retry Attempts* (number of seconds between attempts to connect to the WDM server after a failed attempt).
3. Click **OK**.

For information on Wyse Device Manager software, see "Using Wyse Device Manager Software for Remote Administration."

Enabling and Disabling Automatic Logon Using Winlog

Automatic logon to a user desktop is enabled on the thin client by default. Use the **Winlog** dialog box (*Control Panel* **>** **Winlog** icon) to enable or disable Auto Logon, and to change the default User name, Password, and Domain for a thin client.

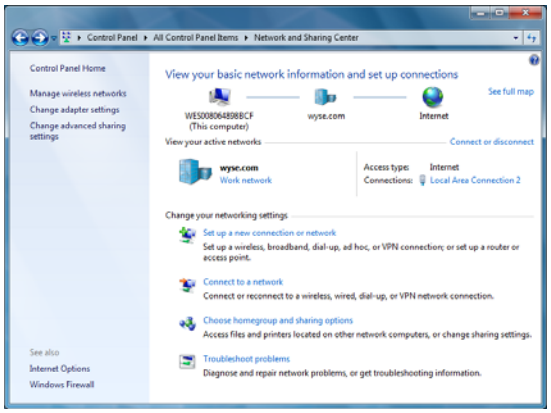
CAUTION: To save the settings so that they persist after a thin client reboot, be sure to flush the files of the File Based Write Filter cache (see "Before Configuring Your Thin Clients").



Configuring Wireless Local Area Network (LAN) Settings

If Wyse USB 802.11b hardware is installed on the thin client, clicking the **Network and Sharing Center** icon in the *Control Panel* allows you to:

- **Manage Wireless Networks** (click the **Manage Wireless Networks** link):
  - *Add* - Click **Add** to open and use the wizard to add a wireless network (to edit an existing wireless network, right-click it, and then select **Properties** to open and use the **Network Properties** dialog box).
  - *Adapter Properties* - Click **Adapter Properties** to open and use the properties dialog box for the wireless adapter.
  - *Profile Types* - Click **Profile Types** to open and use a dialog box to the enable or disable the ability to create Per User Profiles.
  - *Network and Sharing Center* - Click **Network Sharing Center** to return to the **Network and Sharing Center** dialog box (provides network settings, and gives access to network settings).
- **Change Adapter Settings** (click the **Change Adapter Settings** link):
  - Click **Organize** to open the list of options you can use to organize your network connections.
  - Select a connection to display the list of command buttons you can use to view the status, connect to, enable, disable, diagnose, rename, and change the settings of the connection.
- **Change Advanced Sharing Settings** (click the **Change Advanced Sharing Settings** link): Select the network profile settings you want for each of your networks.



For information on preserving your wireless connections with the Regpersistence Tool so that they persist across reboots, see"Preserving Wireless Connections with the Regpersistence Tool."

Preserving Wireless Connections with the Regpersistence Tool

The Regpersistence Tool is designed to configure wireless access in Write Filter Enable mode. When you configure wireless access with this utility, the authentication credentials persist across reboots, eliminating the need to re-authenticate each time the client systems are restarted. The utility preserves the service set identifier (SSID) for wireless connections across workgroup modes and domains. When thin clients restart, they are automatically connected to the desired wireless access point.

The Regpersistence Tool (.exe file) can be obtained from the Wyse *Support Downloads* Web site. Go to http://www.wyse.com/serviceandsupport/support/downloads.asp, select the Regpersistence Tool from the active product download list, and then download the file (the file is in .exe format and will need to be executed *before* use).

Windows Embedded Standard clients can connect to wireless networks using the following network authentication modes:

- Open mode with WEP (this authentication mode requires the network key to be entered while the client is connected to the wireless network; thin clients are automatically connected to the wireless network after reboot).
- Shared mode with WEP
- WPA authentication with AES and TKIP
- WPA-PSK with AES and TKIP data encryption.
- WPA2 with AES and TKIP data encryption
- WPA2-PSK with AES and TKIP data encryption.
- PEAP authentication process

The session keys that are generated during the PEAP authentication process provide keying material for the Wired Equivalent Privacy (WEP) encryption keys that encrypt the data that is sent between wireless clients and wireless access points.

You can use PEAP with any of the following authentication methods for wireless authentication (PEAP is *not* supported for use with EAP-MD5):

- EAP-TLS, which uses certificates for server authentication and either certificates or smart cards for user and client computer authentication.
- EAP-MS-CHAP v2, which uses certificates for server authentication and credentials for user authentication.
- Non-Microsoft EAP authentication methods.

TIP: PEAP is available as an authentication method for 802.11 wireless clients, but it is not supported for virtual private network (VPN) clients or other remote access clients. Therefore, you can configure PEAP as the authentication method for a remote access policy only when you are using Internet Authentication Service (IAS).

Using PEAP Fast Reconnect

When clients connect to an 802.11 wireless network, the authenticated session has an expiration interval configured by the network administrator to limit the duration of authenticated sessions. To avoid the requirement for authenticated clients to periodically re-authenticate and resume a session, you can enable the fast reconnect option.

PEAP supports fast reconnect, as long as each wireless access point is configured as a client of the same IAS (RADIUS) server. In addition, fast reconnect must be enabled on both the wireless client and the RADIUS server.

When PEAP fast reconnect is enabled, after the initial PEAP authentication succeeds, the client and the server cache TLS session keys. When users associate with a new wireless access point, the client and the server use the cached keys to re-authenticate each other until the cache has expired. Because the keys are cached, the RADIUS server can quickly determine that the client connection is a reconnect. This reduces the delay in time between an authentication request by a client and the response by the RADIUS server. It also reduces resource requirements for the client and the server.

If the RADIUS server that cached the session keys is not used, full authentication is required, and the user is again prompted for credentials or a PIN. This can occur in the following situations:

- The user associates with a new wireless access point that is configured as a client of a different RADIUS server.
- The user associates with the same wireless access point, but the wireless access point forwards the authentication request to a different RADIUS server.

In both situations, after the initial authentication with the new RADIUS server succeeds, the client caches the new TLS session keys. Clients can cache TLS session keys for multiple RADIUS servers.

Using the Regpersistence Tool to Configure PEAP Wireless Connections

1. Image the Windows Embedded Standard thin client.
2. Add the following user-specific folders to the File Based Write Filter Exclusion List:
   - Users\<username>\AppData\Roaming\Microsoft\Crypto
   - Users\<username>\AppData\Roaming\Microsoft\Protect
   - Users\<username>\AppData\Roaming\Microsoft\SystemCertificates
3. Add the username to the [Profile] section of the NetXClean.ini file.
4. Add the user to the *Administrators* group.
5. With the Write Filter enabled, configure a wireless connection. When users log in, they are not prompted for wireless credentials.

TIP: When you configure PEAP authentication with the Regpersistence Tool, the thin client must have a corresponding or relative user certificate and server certificate for authentication. With the Regpersistence Tool, the user name and domain name are saved across reboots; the PEAP authentication process prompts only for the password to prevent hackers from spoofing user credentials while users are connected across a WAN.

This page intentionally blank.

5 Additional Administrator Utility and Settings Information

This chapter provides additional information about utilities and settings available for administrators.

It discusses:

- "Automatically Launched Utilities"
- "Utilities Affected by Log Off, Restart, and Shut Down"
- “Using the File Based Write Filter (FBWF)”
- "Understanding the NetXClean Utility"
- "Saving Files and Using Local Drives"
- "Mapping Network Drives"
- "Participating in Domains"
- "Using the WinPing Diagnostic Utility"
- "Using the Net and Tracert Utilities"
- "Managing Users and Groups with User Accounts"
- "Changing the Computer Name of a Thin Client"

TIP: For *TightVNC* utility information, see "Using TightVNC to Shadow a Thin Client."

Automatically Launched Utilities

The following utilities are automatically launched:

- **File Based Write Filter** - Upon system start, the File Based Write Filter utility is automatically launched. It provides a secure environment for thin client computing by protecting the thin client from undesired flash memory writes. The active (green) or inactive (red) status of the filter is indicated by the color of the File Based Write Filter status icon in the system tray of the taskbar. See "Using the File Based Write Filter (FBWF)."
- **NetXClean** - Upon system start, the NetXClean utility is automatically launched. NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. If you want to keep certain profile configurations (for example, printers), be sure to configure NetXClean to refrain from cleaning up any number of explicitly declared profiles. See "Understanding the NetXClean Utility."
- **VNC Server** - Upon successful thin client logon, the Windows VNC Server utility is automatically launched. VNC allows a thin client desktop to be accessed remotely for administration and support. See "Using TightVNC to Shadow a Thin Client."

Utilities Affected by Log Off, Restart, and Shut Down

The following utilities are affected by logging off, restarting, and shutting down the thin client:

- **File Based Write Filter cache** - If you make changes to system configuration settings and want them to persist after a reboot, you must flush the files of the File Based Write Filter cache during the current system session. Otherwise, the new settings will be lost when the thin client is shut down or restarted. The File Based Write Filter cache contents are *not* lost when you simply log off and on again (as the same or different user); that is, you can flush the files of the File Based Write Filter cache after the new logon and still retain the changes. For instructions on flushing, see "Before Configuring Your Thin Clients." For detailed information about the File Based Write Filter, see "Using the File Based Write Filter (FBWF)."
  TIP: A user cannot flush the files of the File Based Write Filter cache; this is a local or remote administrator function.
- **NetXClean Utility** - NetXClean is a clean-up utility that keeps extraneous information from being stored on the flash memory. Clean-up is triggered automatically on restart, shut-down, or user log-off. If you want to keep certain profile configurations (for example, printers), be sure to configure NetXClean to refrain from cleaning up any number of explicitly declared profiles. For details about NetXClean, see "Before Configuring Your Thin Clients" and "Understanding the NetXClean Utility."
- **Power Management** - A Monitor Saver turns off the video signal to the monitor, allowing the monitor to enter a power-saving mode after a designated idle time. Power settings are available in **Start > Control Panel > Power Options**.
- **Wake-on-LAN** - This standard Windows Embedded Standard feature discovers all thin clients in your LAN, and enables you to wake them up by clicking a button. This feature allows Wyse Device Manager software, for example, to perform image updates and remote administration functions on devices that have been shut down or are on standby. To use this feature, the thin client power must remain on.
- **Thin Client Time** - After power off, clock time will not be lost as long as the power source remains on. Clock time will be lost if the power source is off *and* a battery is not installed. The local time utility can be set to synchronize the thin client clock to a time server automatically at a designated time, or manually.
  TIP: Correct time should be maintained as some applications require access to local thin client time. Use the **Date and Time** dialog box (**Start > Control Panel > Date and Time** or by clicking the time area in the taskbar and then clicking the *Change date and time settings* link) to edit the time and date as needed.

Using the File Based Write Filter (FBWF)

The File Based Write Filter provides a secure environment for thin-client computing by protecting the thin client from undesired flash memory writes (flash memory is where the operating system and functional software components reside). By preventing excessive flash write activity, the File Based Write Filter also extends the life of the thin client. It gives the appearance of read-write access to the flash by employing a cache to intercept all flash writes and returning success to the process that requested the I/O.

The intercepted flash writes stored in cache are available as long as the thin client remains active but are lost when the thin client is restarted or switched off. To preserve selected changes, the selected files of the cache can be transferred to the flash on demand by using WDM software or manually by using **Commit** in the **File Based Write Filter Control** dialog box; alternatively, if the files affected by the changes are not known, the changes can be made after disabling the File Based Write Filter using the **File Based Write Filter Control** dialog box, and then re-enabling the File Based Write Filter (see "Setting the File Based Write Filter Controls"). The File Based Write Filter can be controlled either through the command line (*fbwfmgr*) or by double-clicking the File Based Write Filter icon in the Administrator system tray. The File Based Write Filter can flush specified files to the flash from cache (only up to the point when the commit is performed; if more writes are performed on the files that have been flushed, then these files must be flushed/committed again if the additional changes also need to be preserved). The File Based Write Filter can also be enabled/disabled through the command line or through the File Based Write Filter Enable/Disable desktop icons. The status (enabled/disabled) of the File Based Write Filter is displayed by the File Based Write Filter status icon in the system tray (green indicates that the File Based Write Filter is enabled and red indicates that the File Based Write Filter is disabled).

CAUTION: Contents of the File Based Write Filter cache should never be flushed if it is eighty-percent or more full. The Administrator should periodically check the status of the cache and restart the thin client if the cache is more than eighty percent full.

TIP: A Terminal Services Client Access License (TSCAL) is always preserved regardless of File Based Write Filter state (enabled or disabled).
If you want to have other registry settings preserved regardless of File Based Write Filter state, contact Wyse support for help as described in "Wyse Technical Support."

This section provides the following information on using the File Based Write Filter:

- "Changing Passwords with the File Based Write Filter"
- "Running File Based Write Filter Command Line Options"
- "Enabling and Disabling the File Based Write Filter Using the Desktop Icons"
- "Setting the File Based Write Filter Controls"

Changing Passwords with the File Based Write Filter

On Microsoft Windows based machines, account passwords are regularly changed with the domain controller for security purposes. The same password process is applicable for a thin client if the thin client is a member of such a domain. With the File Based Write Filter enabled, a thin client will successfully make this password change with the domain controller. However, since the File Based Write Filter is enabled, the next time the thin client is booted it will not retain the new password. In such cases, you can use the following options:

- Disable the machine account password change on the thin client by setting the `DisablePasswordChange` registry entry to a value of `1`.
- Disable the machine account password change on the Windows based server by using the Microsoft documentation for the operating system. For example, on Windows 2003 Server, set the `RefusePasswordChange` registry entry to a value of `1` on all domain controllers in the domain (instead of on all workstations). Wyse thin clients will still attempt to change their passwords every 30 days, but the change will be rejected by the server.
  TIP: If you set the `RefusePasswordChange` registry entry in the Windows 2003 Domain Controller to a value of `1`, the replication traffic will stop, but not the thin client traffic. If you also set the `DisablePasswordChange` registry entry to a value of `1` in the thin client, both thin client and replication traffic will stop.

Disabling the machine account password change on the thin client

1. Start the Registry Editor by clicking **Start > Run**, entering `regedit` in the **Open** text box, and then clicking **OK**.
2. Locate and click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
3. In the right pane, click the `DisablePasswordChange` entry.
4. On the *Edit* menu, click **Modify**.
5. In the **Value data** text box, enter a value of `1`, and then click **OK**.
6. Quit the Registry Editor.

Disabling the machine account password change in Windows 2003

1. Start Registry Editor by clicking **Start > Run**, entering `regedit` in the **Open** text box, and then clicking **OK**.
2. Locate and click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
3. On the *Edit* menu, point to **New** and then click **DWORD Value**.
4. Enter `RefusePasswordChange` as the registry entry name, and then click **ENTER**.
5. On the Edit menu, click **Modify**.
6. In the Value data text box, enter a value of `1`, and then click **OK**.
7. Quit the Registry Editor.

Running File Based Write Filter Command Line Options

There are several command lines you can use to control the File Based Write Filter (command line arguments cannot be combined).

CAUTION: Administrators should use file security to prevent undesired usage of these commands.

Use the following guidelines for the command line option for the File Based Write Filter (you can also use the commands if you open an Command Prompt window by entering `command` in the **Run** box):

TIP: If you open a Command Prompt window and enter `fbwfmgr /`, all available commands are displayed. For information on a command, use `fbwfmgr /help <command>`. For example, for information on `/addvolume`, enter the following: `fbwfmgr /help /addvolume`.

- **fbwfmgr**
  With no arguments - Displays the File Based Write Filter configuration for the current and the next session.
- **fbwfmgr /enable**
  Enables the File Based Write Filter after the next system restart. The File Based Write Filter status icon is green when the File Based Write Filter is enabled.
- **fbwfmgr /disable**
  Disables the File Based Write Filter after the next system restart. The File Based Write Filter status icon remains red while disabled.
- **fbwfmgr /commit C: <file_path>**
  Commits the changes made to the file to the underlying media. Note that there is a single space between volume name and file_path. The file path must be an absolute path starting with `\`. For example, to commit a file `C:\Program Files\temp.txt` the command would be `fbwfmgr /commit C: \Program Files\temp.txt`.
- **fbwfmgr /restore C: <file_path>**
  Discards the changes made to the file, that is, it restores the file to its original contents from the underlying media. The file path must be an absolute path starting with `\`. If the file was deleted, it will be recovered.
- **fbwfmgr /addexclusion C: <file_or_dir_path>**
  Adds the file or the directory to the exclusion list of the volume. That is, the file or directory is removed from the protection of the File Based Write Filter. The exclusion will take effect after the next system reboot. The file or directory path must be an absolute path starting with `\`.
- **fbwfmgr /removeexclusion C: <file_or_dir_path>**
  Removes the file or the directory from the exclusion list of the volume. That is, the file or directory is included within the protection of the File Based Write Filter. The removal of the exclusion will take effect after the next system reboot. The file or directory path must be an absolute path starting with `\`.
- **fbwfmgr /overlaydetail**
  Displays the list of files and directories that are modified, along with the size of memory used by the File Based Write Filter to cache the modified data of the file or directory and the number of open handles to it.

CAUTION: Do not attempt to flush while a flush is currently being performed.

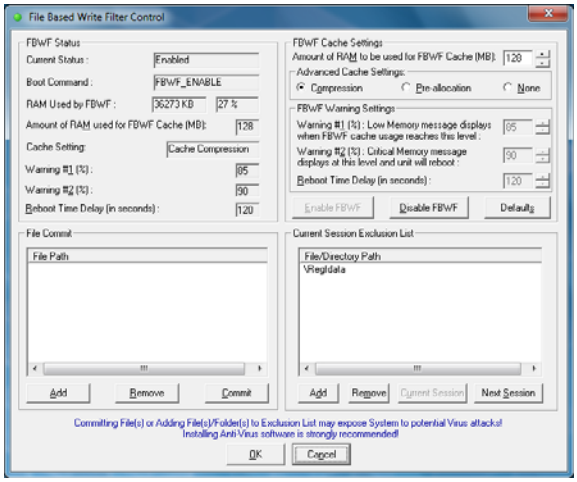
Enabling and Disabling the File Based Write Filter Using the Desktop Icons

For convenience, use the File Based Write Filter enable and disable icons present on the administrator desktop.

- **File Based Write Filter Enable Icon** - (Green) Double-clicking this icon enables the File Based Write Filter. This utility is similar to running the `fbwfmgr /enable` command line option as described in "Running File Based Write Filter Command Line Options." However, double-clicking this icon *immediately* restarts the system and enables the File Based Write Filter. The File Based Write Filter status icon in the system tray is green when the File Based Write Filter is enabled.
- **File Based Write Filter Disable Icon** - (Red) Double-clicking this icon allows you to disable the File Based Write Filter. This utility is similar to running the `fbwfmgr /disable` command line option as described in "Running File Based Write Filter Command Line Options." However, double-clicking this icon *immediately* restarts the system and disables the File Based Write Filter. The File Based Write Filter remains disabled and can only be enabled using the File Based Write Filter Enable icon or through the command line as described in "Running File Based Write Filter Command Line Options." The File Based Write Filter status icon in the system tray remains red while the File Based Write Filter is disabled.

Setting the File Based Write Filter Controls

Use the **File Based Write Filter Control** dialog box (double-click the FBWF icon in the system tray of the administrator taskbar) to view and manage your control settings.



Use the following guidelines:

- *FBWF Status* area includes:
  Current Status - Shows the current status (Enabled or Disabled) of the File Based Write Filter.
  Boot Command - Shows the current status of the Boot Command (FBWF_ENABLE means that the FBWF is enabled for the next session; and FBWF_DISABLE means that the FBWF is disabled for the next session).
  RAM used by FBWF - Shows the amount of RAM used (in Kilobytes and Percentage) that is currently being used by the File Based Write Filter. If **Current Status** is Disabled, RAM Used by FBWF is always zero (0).
  Amount of RAM used for FBWF Cache - Shows (in MB) the amount of RAM (in MB) that is used as File Based Write Filter cache for the current session.
  Cache Setting - Shows the cache setting for the current session.
  Warning #1 (%) - Shows the FBWF cache percentage value at which a Low Memory warning message will be displayed to the user for the current session.

Warning #2 (%) - Shows the FBWF cache percentage value at which a Critical Memory warning message will be displayed to the user, along with another message display counting down the number of seconds before automatic rebooting will occur for the current session.
Reboot Time Delay (in seconds) - Shows the number of seconds that will lapse before system reboot in the Warning #2 (%) case of cache overflow for the current session.

- *FBWF Cache Settings* area includes:
  Amount of RAM to be used for FBWF Cache - Shows (in MB) the amount of RAM (in MB) that is to be used as File Based Write Filter cache for the next session. This value should be in the range of 16 MB to 1024 MB. There is an additional check that this value should not exceed 35% of Total Available RAM.
- *Advanced Cache Settings* area includes options to allow you to improve the effectiveness of cache memory (**Cache Compression**, **Cache Pre-allocation**, or **None**).
- *FBWF Warning Settings* area includes:
  Warning #1 (%) - Shows the FBWF cache percentage value at which a Low Memory warning message will be displayed to the user (Default value = 85, Minimum value = 50, Maximum value = 90).
  Warning #2 (%) - Shows the FBWF cache percentage value at which a Critical Memory warning message will be displayed to the user, along with another message display counting down the number of seconds before automatic rebooting will occur (Default value = 95, Minimum value = 55, Maximum value = 95).
  Reboot Time Delay (in seconds) - Shows the number of seconds that will lapse before system reboot in the **Warning #2 (%)** case of cache overflow.
- **Enable FBWF** - Allows you to enable the File Based Write Filter and prompts you to restart the thin client. If you do not restart the thin client, the changes made will not be saved until the thin client is restarted. After the system restarts to enable the File Based Write Filter, the File Based Write Filter status icon (in the desktop system tray) turns green.
- **Disable FBWF** - Allows you to disable the File Based Write Filter and prompt you to restart the thin client. If you do not restart the thin client, the changes made will not be saved until the thin client is restarted. After disabling the File Based Write Filter, the File Based Write Filter status icon (in the desktop system tray) turns red and the File Based Write Filter remains disabled after the system restarts.
- **Defaults** - Allows you to reset the *FBWF Cache Settings* area, *Advanced Cache Settings* area, and the *FBWF Warning Settings* area to their default values.
- *File Commit* area includes:
  File Path - Allows you to add, remove, and commit files to the underlying media (delete a file path from the list if the file is not to be committed). The system will not restart the thin client. The changes are committed immediately.
- *Current Session Exclusion List* area includes:
  File/Directory Path - Allows you to add and remove a file or directory to or from the exclusion list for the next session (retrieves the list of files or directories that are write through in the current session; the title of the pane is shown as *Current Session Exclusion List*) or the Next Session (retrieves the list of files or directories that are write through for the next session; the title of the pane is shown as *Next Session Exclusion List*). The system will not restart the thin client and the changes are not committed until an administrator restarts the thin client manually.

Understanding the NetXClean Utility

NetXClean keeps extraneous information from being stored in flash memory. NetXClean clean-up is triggered by either a service startup or a user log-off. It runs in the background and performs the clean-up invisibly and no user input is necessary.

NetXClean prevents garbage files from building up and filling the free space in the flash (for example, if a flush of some files in the File Based Write Filter cache puts junk in flash directories that must be kept clean). The NetXClean utility is particularly important when multiple users have log-on rights to a thin client, as memory space can be quickly used by locally stored profiles and temporary caching of information.

NetXClean TweakUI functions includes clearing:

- Run history at log-on
- Document history at log-on
- Find Files history at log-on
- Find Computer history at log-on
- Internet Explorer history at log-on
- Last User at log-on
- Selected Items Now

NetXClean purges selected directories, files, and profiles. It uses a configuration file to determine which directories and files to purge (and what not to purge). To select different directories and files to purge, you must select them in the configuration file.

CAUTION: NetXClean purge selections are made by the manufacturer and should not be changed without manufacturer supervision.

Regardless of the configuration file selections, NetXClean does not clean any of the following directories or their parent directories:

- Windows directory
- Windows System subdirectory
- Current directory in which the service is installed

NetXClean will not delete the following profiles:

- Administrator
- All Users
- Default User
- The profile of the last user who logged on

Saving Files and Using Local Drives

Administrators need to know the following information about local drives and saving files.

Saving Files

Thin clients use an embedded operating system with a fixed amount of flash memory. It is recommended that you save files you want to keep on a server rather than on a thin client.

CAUTION: Be careful of application settings that write to the C drive, which resides in flash memory (in particular, those applications which by default write cache files to the C drive on the local system). If you *must* write to a local drive, change the application settings to use the Z drive. The default configuration settings mentioned in "Managing Users and Groups with User Accounts" minimize writing to the C drive for factory-installed applications.

Drive Z

Drive Z is the on-board volatile memory (`Ms-ramdrive`) of the thin client. It is recommended that you do not use this drive to save data that you want to retain.

For Ramdisk configuration information, see "Setting Ramdisk Size."

For information about using the Z drive with roaming profiles, see "Participating in Domains."

Drive C and Flash

Drive C is the on-board non-volatile flash memory. It is recommended that you avoid writing to drive C. Writing to drive C reduces the size of the flash. If the flash size is reduced to under 3 MB, the thin client will become unstable.

CAUTION: It is highly recommended that 3 MB of flash memory be left unused. If the free flash memory size is reduced to 2 MB, the thin client image will be irreparably damaged and it will be necessary for you to contact an authorized service center to repair the thin client.

The File Based Write Filter (if enabled) protects the flash from damage and presents an error message if the cache is overwritten. However, if this message occurs you will be unable to flush files of the File Based Write Filter cache and any thin client configuration changes still in cache will be lost. Items that are written to the File Based Write Filter cache (or directly to the flash if the File Based Write Filter is disabled) during normal operations include:

- Favorites
- Created connections
- Delete/edit connections

For information on the role of NetXClean in keeping the flash memory clean, see "Understanding the NetXClean Utility."

Mapping Network Drives

Users and administrators can map network drives. However, to retain the mappings after the thin client is restarted, you must complete the following:

- Select the **Reconnect at logon** check box.
- Flush the files of the File Based Write Filter cache during the current system session. Since a User log-on account cannot flush the files of the File Based Write Filter cache, the mappings can be retained by logging off the user account (*do not* shut down or restart the system), logging back on using an administrator account, and then flushing the files of the cache.

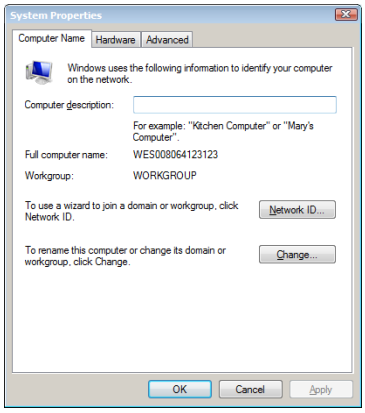
TIP: A remote home directory can also be assigned by using a user manager utility or by other means known to an administrator.

Participating in Domains

You can participate in domains by joining the thin client to a domain or by using roaming profiles.

Joining a Domain

As an administrator you can use the *Computer Name* tab on the **System Properties** dialog box (**Start > Control Panel** > **System > Change Settings**) to join a thin client to a domain (click **NetworkID** and then complete the wizard).



CAUTION: Exercise caution when joining the thin client to a domain as the profile downloaded at log-on could overflow the cache or flash memory.

When joining the thin client to a domain, the File Based Write Filter should be disabled so that the domain information can be permanently stored on the thin client. The File Based Write Filter should remain disabled through the next boot as information is written to the thin client on the boot after joining the domain. This is especially important when joining an Active Directory domain. For details on disabling and enabling the File Based Write Filter, see "Before Configuring Your Thin Clients."

To make the domain changes permanent, complete the following:

1. Disable the File Based Write Filter.
2. Join the domain.
3. Reboot the thin client.
4. Enable the File Based Write Filter.
5. Reboot the thin client.

TIP: If you use the FBWF Enable icon to enable the File Based Write Filter, the second reboot will happen automatically.
By default, the NetXClean utility will purge all but specifically selected profiles on the system when the thin client starts up or when the user logs off. For information on how to ensure a new profile is not purged by the NetXClean utility, see "Understanding the NetXClean Utility."

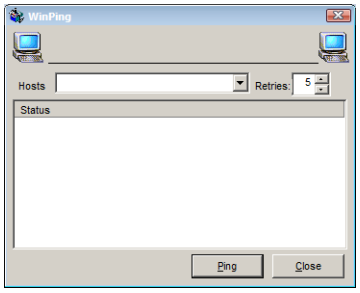
Using Roaming Profiles

You can participate in domains by writing roaming profiles to the C drive. The profiles must be limited in size and will not be retained when the thin client is restarted.

For successful downloading and proper functioning, there must be sufficient flash space available for roaming profiles. In some cases it may be necessary to remove software components to free space for roaming profiles.

Using the WinPing Diagnostic Utility

WinPing is used to launch the Windows PING (Packet InterNet Groper) diagnostic utility and view the results from pinging. To open the WinPing window, click **Start** > **Run**, enter `WinPing` in the box, and click **OK**.



WinPing is a diagnostic tool that 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. The default is to send 5 echo requests and then stop if no response is detected. WinPing sends one echo request per second, calculates round trip times and packet loss statistics, and displays a brief summary upon completion.

WinPing is used to:

- Determine the status of the network and various 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.

Using the Net and Tracert Utilities

Net and Tracert utilities are available for administrative use (for example, to determine the route taken by packets across an IP network). For more information on these utilities, go to: http://www.microsoft.com.

Managing Users and Groups with User Accounts

Use the **User Accounts** window (**Start > Control Panel** > **User Accounts**) to create and manage user accounts, create and manage groups, and configure advanced user profile properties. By default, a new user is only a member of the *Users* group and is not locked down. As the administrator, you can select the attributes and profile settings for users.

This section provides quick-start guidelines on:

- "Creating User Accounts"
- "Editing User Accounts"
- "Configuring User Profiles"

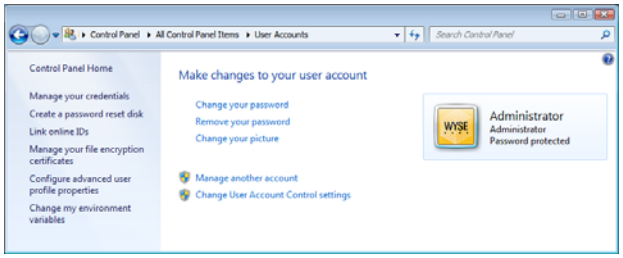
TIP: For detailed information on using the **User Accounts** window, click the *help* icon and *examples* links provided throughout the wizards. For example, you can use the **Windows Help and Support** window (click the *help* icon in the **User Accounts** window) to search for items such as *user profiles* and *user groups* and obtain links to detailed steps on creating and managing these items.

Creating User Accounts

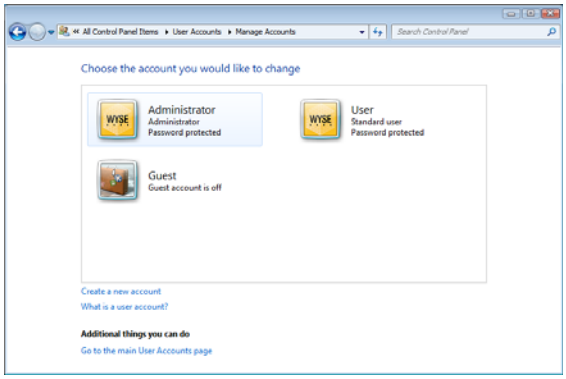
Only administrators can create new user accounts locally or remotely through VNC. However, due to local flash/disk space constraints, the number of additional users on the thin client should be kept to a minimum.

CAUTION: Be sure to flush the files of the File Based Write Filter cache during the current system session in which a new account is created (see "Before Configuring Your Thin Clients").

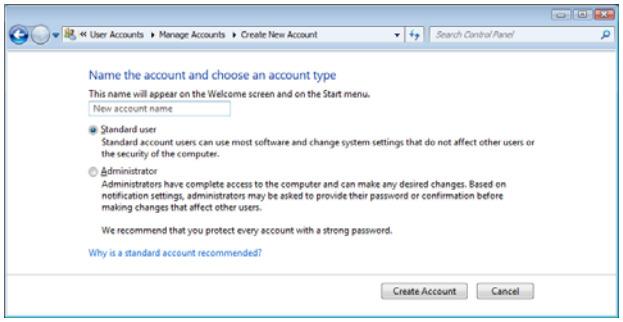
1. Log-in as an administrator and open the **User Accounts** window (**Start > Control Panel** > **User Accounts**).



2. Click the **Manage Another Account** link to open the **Manage Accounts** window.



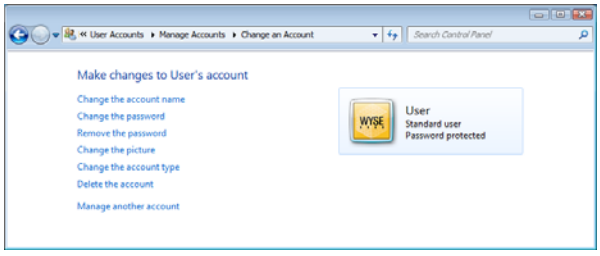
3. Click the **Create a New Account** link to open and use the wizard.



4. After creating the *Standard Users* and *Administrators* you want, the users will appear in the **Manage Accounts** window (**Start > Control Panel** > **User Accounts > Manage Another Account**).

Editing User Accounts

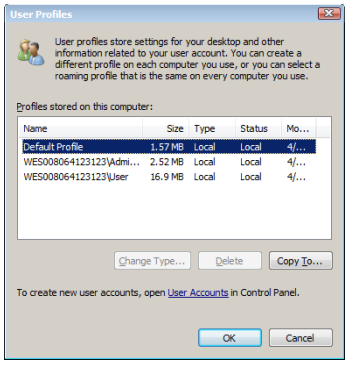
To edit the default settings of a *Standard User* or *Administrator* account, click on the account you want to modify in the **Manage Accounts** window (**Start > Control Panel** > **User Accounts > Manage Another Account**), and then make your changes.



Configuring User Profiles

To configure the *Default*, *Administrator*, and *User* profiles stored on the thin client, open the **User Profiles** window (**Start > Control Panel** > **User Accounts > Configure Advanced User Profile Properties**) and use the command buttons (**Change Type**, **Delete**, **Copy to**) according to Microsoft documentation provided throughout the wizards.

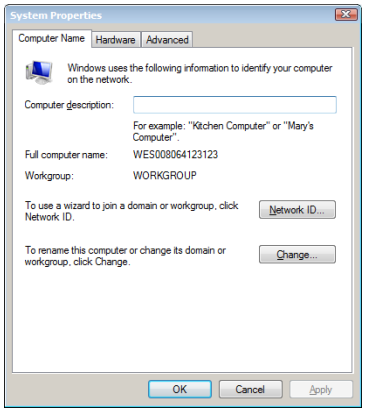
CAUTION: By default, all application settings are set to cache to C drive. It is highly recommended that you cache to the Ramdisk Z drive (as is pre-set in the account profiles) to avoid overflowing the File Based Write Filter cache.



CAUTION: Because of the limited size of the flash memory, it is strongly recommended that other applications available to new and existing users be configured to prevent writing to the local file system. For the same reason, it is also recommended that *extreme care be exercised when changing configuration settings of the factory-installed applications.*

Changing the Computer Name of a Thin Client

Administrators can use the *Computer Name* tab of the **System Properties** dialog box (**Start > Control Panel > System > Change Settings**) to change the computer name of a thin client. The computer name information and the Terminal Services Client Access License (TSCAL) are preserved regardless of the File Based Write Filter state (enabled or disabled). This maintains the specific computer identity information and facilitates the image management of the thin client.



6 System Administration

This chapter contains local and remote system administration information to help you perform the routine tasks needed to maintain your Wyse thin client environment.

It includes:

- "Restoring Default Settings"
- "Accessing Thin Client BIOS Settings"
- "Imaging Devices with the Wyse USB Firmware Tool"
- "Using Wyse Device Manager Software for Remote Administration"
- "Configuring and Using Peripherals"
- "Using TightVNC to Shadow a Thin Client"

Restoring Default Settings

Depending on the default settings you want to restore on the thin client, you can:

- Use the BIOS to restore default values for all the items in the BIOS setup utility (see "Accessing Thin Client BIOS Settings").
- Re-image the thin client to restore all factory default settings using the Wyse USB Firmware Tool or Wyse Device Manager (see "Imaging Devices with the Wyse USB Firmware Tool" and "Using Wyse Device Manager Software for Remote Administration").

Preparing to Re-image

The thin client (running WES) can only be returned to factory defaults by re-imaging the thin client (the same process used when upgrading the firmware). The re-imaging process requires:

- **A clean image** - Go to http://www.wyse.com/serviceandsupport/support/downloads.asp, select the active product download you need (images are device dependent; be sure to select the correct model you want to re-image), and then download the files. Note that these files are normally in a compressed (.zip) format and will need to be extracted (or executed, if in .exe format) *before* use.
- **Imaging software** - Wyse provides two imaging software products to re-image your thin client (running WES):
  - Wyse® USB Firmware Tool™ - recommended for smaller environments (see "Imaging Devices with the Wyse USB Firmware Tool").
  - Wyse Device Manager™- recommended for larger environments (see "Using Wyse Device Manager Software for Remote Administration").

Accessing Thin Client BIOS Settings

While starting a Wyse client you will see a Wyse logo for a short period of time. During this start-up you can press the **Del** key (**F2** key on mobile thin clients) to enter the BIOS of the thin client to make your modifications (when prompted, enter **Fireport** as the password).

Imaging Devices with the Wyse USB Firmware Tool

The Wyse® USB Firmware Tool™ provides a simple USB imaging solution to help IT and Customer Service staff quickly and easily image supported devices.

Using the tool's flexible windows utility, users can easily:

- Configure a USB key to *copy/pull* firmware from a source device (to later *push* to other target devices).
- Configure a USB key to *update/push* firmware (that you include on the USB key) to target devices (to upgrade firmware).
- Create *replicate/duplicate* USB keys (containing the original contents) for simultaneous usage on target devices (by users in several locations at the same time).

Using Wyse Device Manager Software for Remote Administration

Wyse Device Manager™ (WDM) servers provide network management services to the thin client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot, rename, automatic device check-in support, Wake-On-LAN, change device properties, and so on). With WDM you can manage all of your network devices from one simple-to-use console.

For information on setting WDM properties, see "Configuring WDM Properties."

For local custom fields that can be accessed by WDM, see "Setting Configuration Strings with Custom Fields."

Configuring and Using Peripherals

Depending on the ports available on the thin client, the thin client can provide services through a USB port, a serial port, an LPT port, or a PCMCIA card plugged into the back of the thin client (if the appropriate software is installed).

TIP: Addons for various services can be installed (Addons are available from Wyse for free or for a licensing fee). For information on Addons available, see the Wyse Web site at: http://www.wyse.com/products/software/firmware.

Wyse thin clients can be configured to use Bluetooth-enabled peripherals. See "Configuring Bluetooth Wireless Connections."

Using TightVNC to Shadow a Thin Client

TightVNC Server is installed locally on the thin client. It allows a thin client to be shadowed/operated/monitored from a remote machine on which *TightVNC Viewer* is installed (*TightVNC Viewer* is available from the TightVNC Web site; it is also included as a component of Wyse Device Manager software and must be installed on the remote/shadowing machine before use).

TightVNC (*Server* and *Viewer*) allows a remote administrator to configure or reset a thin client from a remote location rather than making a personal appearance at the thin client site (VNC is intended primarily for support and troubleshooting purposes). *TightVNC Server* starts automatically as a service at thin client startup. The service can also be stopped and started by using the *Services* window (opened by clicking **Start > Control Panel > Administrative Tools > Services**).

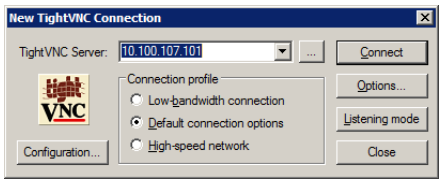
TIP: If you want to permanently save the state of the service, be sure to flush the files of the File Based Write Filter during the current system session.

Before an administrator on a remote machine (on which *TightVNC Viewer* is installed) can access a thin client (with *TightVNC Server*) the administrator must know the:

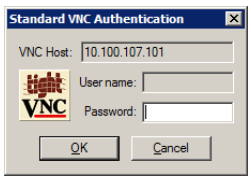
- *IP Address* (or valid DNS name) of the thin client that is to be shadowed/operated/monitored (see "Viewing Wyse Client Information"). To obtain the IP address of an administrator thin client, hover the mouse arrow over the VNC icon in the system tray of the Administrator taskbar.
- *Primary Password* of the thin client (default password is *Wyse*) that is to be shadowed/operated/monitored (see "Configuring TightVNC Server Properties").

To shadow a thin client from a remote machine:

1. Open the **New Tight VNC Connection** dialog box (for example, **Start > All Programs > TightVNC > TightVNC Viewer**).



2. Enter the IP address or valid DNS name of the thin client that is to be shadowed/operated/monitored (you can also set other options using the command buttons).
3. Click **OK** to open the **VNC Authentication** dialog box.

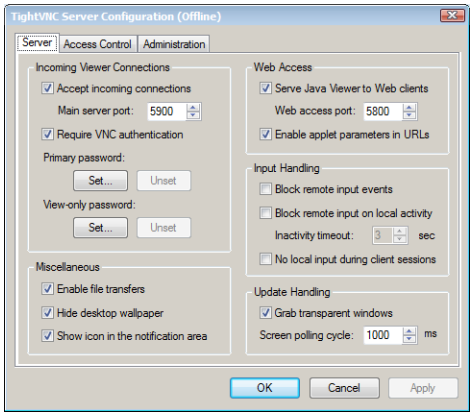


4. Enter the **Password** of the thin client that is to be shadowed (this is the *Primary Password* of the thin client that is to be shadowed - default password is *Wyse*) and click **OK**. The thin client that is to be shadowed/operated/monitored will be displayed for the administrator in a separate window on the remote machine. Use the mouse and keyboard on the remote machine to operate the thin client just as you would if you were operating it locally.

Configuring TightVNC Server Properties

Use the **TightVNC Server Configuration (Offline)** dialog box (**Start** > **All Programs > TightVNC > TightVNC Server (Application Mode) > TightVNC Server - Offline Configuration**) to select the parameters for the *TightVNC Server* utility installed on the thin client. For example, you can set the *Primary Password* (the password an administrator needs to use when shadowing the thin client) on the *Server* tab (default password is *Wyse*).

CAUTION: For security, it is highly recommended that the *Primary Password* be changed for administrator use only immediately upon receipt of the thin client.



A Establishing a Server Environment

This appendix contains information on the network architecture and enterprise server environment needed to provide network and session services for your Wyse thin clients.

It includes:

- "Understanding How to Configure Your Network Services"
- "Using Dynamic Host Configuration Protocol (DHCP)"
- "Using FTP File Servers"
- "Using Domain Name System (DNS)"
- "Understanding Session Services"
- "Configuring ICA Session Services"
- "Configuring RDP Session Services"
- "Using VMware View Manager Services"

Understanding How to Configure Your Network Services

Network services used by the thin client can include DHCP, FTP file services, and DNS. How you configure your network services depends on what you have available in your environment and how you want to design and manage it.

The following topics in this appendix provide important information to help you configure your network services:

- "Using Dynamic Host Configuration Protocol (DHCP)"
- "Using FTP File Servers"
- "Using Domain Name System (DNS)"

Using Dynamic Host Configuration Protocol (DHCP)

A thin client is initially configured to obtain its IP address and network configurations from a DHCP server (new thin client or a thin client reset to default configurations). A DHCP server can also provide the IP address or DNS name of the FTP server and the FTP root-path location of software (in Microsoft .msi form) for access through the DHCP upgrade process. Using DHCP to configure and upgrade thin clients is recommended and saves you the time and effort needed to complete these processes locally on multiple thin clients (if a DHCP server is not available, fixed IP addresses can be assigned and must be entered locally for each device). A DHCP server can also provide the IP address of the Wyse Device Manager (WDM) server (for information on WDM, see "Using Wyse Device Manager Software for Remote Administration").

The DHCP options listed in Table 1 are accepted by the thin clients. For more information on configuring a DHCP server see documentation on the Microsoft Web site at: http://www.microsoft.com.

Table 1 DHCP Options

Option	Description	Notes
1	Subnet Mask	Required.
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.
12	Hostname	Optional.
15	Domain Name	Optional but recommended.
43	Vendor Class Specific Information	Optional.
50	Requested IP	Required.
51	Lease Time	Required.
52	Option Overload	Optional.
53	DHCP Message Type	Required.
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	Required.
59	T2 (rebind) Time	Required.
61	Client identifier	Always sent.
155	Remote Server IP Address or name	Optional.
156	Logon User Name used for a connection	Optional.
157	Domain name used for a connection	Optional.
158	Logon Password used for a connection	Optional.
159	Command Line for a connection	Optional.
160	Working Directory for a connection	Optional.
161	FTP server list	Optional string. Can be either the name or the IP address of the FTP server where the updated thin client image is stored. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6.

Table 1 DHCP Options, Continued

Option	Description	Notes
162	Root path to the FTP files	Optional string.
163	SNMP Trap server IP Address list	Optional.
164	SNMP Set Community	Optional.
165	RDP startup published applications	Optional.
166	Ericom - PowerTerm® TEC Mode	Optional.
167	Ericom - PowerTerm® TEC ID	Optional.
168	Name of the server for the virtual port	Optional.

Using FTP File Servers

Windows Embedded Standard includes an FTP Upgrade utility that can be used to upgrade the Windows Embedded Standard thin client with software which are in Microsoft .msi form. This utility allows you to automatically upgrade a thin client by downloading MSI packages from a specified FTP server. The MSI packages are stored on the FTP server in a directory in the FTP root path (this FTP file server name and root-path directory must be made available to the thin client).

Use the following guidelines to set up your servers:

- **Automatic upgrades** - Params.ini and the MSI package must be present on your FTP server (in the same path) to upgrade the thin client.
- **DHCP upgrades** - If the DHCP server is supplying the location of the MSI package, be sure to configure the DHCP Options (in Table 1) that you need (defaults are 161 - FTP server list and 162 - Root path to the FTP files).
- **Anonymous log-on capability** - The FTP server must provide anonymous log-on capability.
- **User ID and Password** - The default FTP User name is *anonymous* and the default Password is *Wyse*.

Using Domain Name System (DNS)

Thin clients accept valid DNS names registered on a DNS server available to the enterprise intranet. The thin client will query a DNS server on the network for name to IP resolution. In most cases DNS is not required but may be used to allow hosts to be accessed by their registered DNS names rather than their IP addresses. Every Windows DNS server in Windows 2000 and later includes Dynamic DNS (DDNS) and every server registers dynamically with the DNS server. For DHCP entry of DNS domain and server location information, see "Using Dynamic Host Configuration Protocol (DHCP)."

Understanding Session Services

Before you use the information in this section to configure your ICA and RDP session services, be sure you understand and use the following guidelines:

TIP: Wyse thin clients running Windows Embedded Standard also support virtual desktop solutions as described in "Using VMware View Manager Services."

- **General Guidelines** - The Thin-client session services are made available by servers hosting Citrix ICA and Microsoft RDP software products.
- **ICA Guidelines** - Independent Computing Architecture (ICA) is a three-tier, server-based computing technology that separates the logic of an application from its user interface. The ICA client software installed on the thin client allows the user to interact with the application GUI, while all of the application processes are executed on the server. For information on configuring ICA, see "Configuring ICA Session Services."
  TIP: The ICA server must be licensed from Citrix Systems, Inc. You must purchase enough client licenses to support the total concurrent thin client load placed on the Citrix server farm. A failure to connect when all client seats are occupied does not represent a failure of Wyse equipment. The ICA client software is installed on the thin client.
- **RDP Guidelines** - Remote Desktop Protocol (RDP) is a network protocol that allows a thin client to communicate with the Terminal Service running on Windows 2003/2008 Server over the network. For information on configuring RDP, see "Configuring RDP Session Services."

Configuring ICA Session Services

Before you use the information in this section to configure your ICA session services, be sure you have read "Understanding Session Services."

ICA session services can be made available on the network using either Windows 2003/2008 Server with Terminal Services and one of the following installed:

- Citrix MetaFrame XP
- Citrix Presentation Server

Use the instructions accompanying these products to install them and make sessions and applications available to the thin clients sharing the server environment.

TIP: If a Windows 2003/2008 Server or Citrix XenApp 5.0 with Windows Server 2008 is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere accessible on the network. The server will grant a temporary (120-day) license on an individual device basis. Beyond the temporary (120-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).

Configuring RDP Session Services

Before you use the information in this section to configure your RDP session services, be sure you have read "Understanding Session Services."

RDP session services can be made available on the network to allow you to connect remotely to a desktop computer running Microsoft Windows NT®, Windows 2000, Windows 2003, Windows XP Professional, supported versions of Windows Vista, and supported versions of Windows 7 or a server running Microsoft® Windows NT® Server 4.0, Terminal Server Edition, Windows 2000 Server, Windows 2003 Server, and Windows 2008 Server. The Remote Desktop Protocol allows a thin client to execute Windows applications within a Windows GUI environment, even though they are actually being executed on the server.

Use the instructions accompanying these products to install them and make sessions and applications available to the thin clients sharing the server environment.

TIP: If a Windows 2003/2008 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere accessible on the network. The server will grant a temporary (120-day) license on an individual device basis. Beyond the temporary (120-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).

Using VMware View Manager Services

VMware® View Manager is a desktop management solution that enables system administrators to provision desktops and control user access. Client software securely connects users to centralized virtual desktops, back-end physical systems, or terminal servers.

TIP: Information on installing and configuring View Manager can be found on the VMware Web site at: http://www.vmware.com.

View Manager consists of the following major components:

- **View Connection Server** - a software service that acts as a broker for client connections by authenticating and then directing incoming remote desktop user requests to the appropriate virtual desktop, physical desktop, or terminal server.
- **View Agent** - a software service that is installed on all guest virtual machines, physical systems, or terminal servers in order to allow them to be managed by View Manager. The agent provides features such as RDP connection monitoring, virtual printing, remote USB support, and single sign on.
- **View Client** - a locally installed software application that communicates with View Connection Server in order to allow users to connect to their desktops using Microsoft Remote Desktop Protocol (RDP).
- **View Client with Offline Desktop (experimental)** - a version of View Client that is extended to support the Offline Desktop feature which allows users to download virtual machines and use them on their local systems.
- **View Portal** - a Web-based version of View Client supported by multiple operating systems and browsers.
- **View Administrator** - a Web application that allows View Manager administrators to configure View Connection Server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities.
- **View Composer** - a software service that is installed on the VirtualCenter server in order to allow View Manager to rapidly deploy multiple linked clone desktops from a single centralized base image.

Implementing View Client Support on Wyse Thin Clients

For the Windows Embedded Standard 7 software release, the latest VMware View Client support is provided as part of the Windows Embedded Standard image by including the View Client component.

TIP: For the previous release of Windows Embedded Standard software, the latest View Client support can be provided by using a Wyse Device Manager (WDM) package to push the View Client to your Wyse thin clients.

CAUTION: The View Client WDM package requires 9 MB of space in the flash memory of the thin client.

Tables

Administrators Guide

Wyse® Enhanced Microsoft® Windows® Embedded Standard 7 WFR2

Issue: 031813

Written and published by:
Wyse Technology Inc., March 2013

Created using FrameMaker® and Acrobat®