Administrators Guide

Wyse® Winterm™ 9 series,
Based on Microsoft® Windows® XP Embedded

Issue: 030107
PN: 883808-01 Rev. F

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

Wyse and Winterm are registered trademarks, and the Wyse logo and Winterm logo are trademarks of Wyse Technology Inc. ICA is a registered trademark and MetaFrame is a trademark of Citrix Systems Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other products are 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 http://www.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 (refer to “Thin Client Requirements Compliance”), 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.

Caution

Changes or modifications not covered in this manual must be approved in writing by the manufacturer’s Regulatory Engineering department. Changes or modifications made without written approval may void the user’s authority to operate the equipment.

Regulatory Compliance for Thin Clients

EMC and Safety Requirements

Models x150SE, SX0, VX0, and Model J400, Products 941GXL and G90 thin clients are compliant with the regulatory requirements in the regions listed below (Model J400, Products 941GXL and G90 are not currently certified for China or Korea).

U.S.A. - FCC Part 15 (class B), UL60950
Canada - ICES-003, CAN/CSA-C22 No. 60950
Europe - EN 55022 (class B), EN 61000-3-2 (class A), EN 61000-3-3, EN 55024, EN 90650-1:2000+ALL
Australia / New Zealand - AS/NZS CISPR 22
Japan - VCCI CISPR 22 (class B)
China - CCC GB9254-1998, GB17625.1-2003, GB 4943-2001
Korea - MIC

RF & EMC Requirements

Model VX0 thin clients with internal wireless option are compliant with the regulatory standards in the regions listed below.

U.S.A. - FCC Part 15 C, 15.401-15.407, FCC 1.1310 (RF exposure)
Canada - RSS-210
Europe - EN 55022 (class B), EN300.328, EN301.489-1, EN301.489-17
Australia / New Zealand - AS/NZS 4771
Japan - Telec (Equipment Radio Regulation, 2006)
China - SRRC (CMII)
Korea - MIC (RRL)

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 module) are present in the Model VX0 as an option. These devices operate in the 2.4 GHz band (i.e. 802.11b/g WLAN & 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.

Cable Notice

The use of shielded I/O cables is required when connecting this equipment to any and all optional peripheral or host devices. Failure to do so may cause interference and violate FCC and international regulations for electromagnetic interference.

Noise Suppressor for Models x150SE and J400, Products 941GXL Thin Clients

A noise suppressor (ferrite bead) must be installed on the network cable of your thin client. This installation is necessary to maintain compliance with U.S. FCC B limits and European CISPR B EN55022 Class B limits. The noise suppressor is supplied by the manufacturer and is packed in your thin client shipping carton.

Device Power Supply

For use with external power supply included in the shipping carton, or a certified equivalent model supplied by the manufacturer.

Model J400, Product 941GXL Thin Client

For use with External Power Supply Li Shin Model LSE9802A1255 or certified equivalent model supplied by the manufacturer, rated +12Vdc, 4.58A.

Model x150SE Thin Client

For use with External Power Supply DVE Model DSA-0421S-12 3 30, or certified equivalent model supplied by the manufacturer, rated 12Vdc, 2.5A.

Model SX0 Thin Client

For use with External Power Supply DVE Model DSA-0421S-12 3 30, or certified equivalent model supplied by the manufacturer, rated 12Vdc, 2.5A.

Model VX0 Thin Client

For Use with External Power Supply Model LSE9802A1255, or UL Listed Power Unit marked “Class 2” or “LPS” and rated for minimum 12 Vdc, 4.0A.

Battery Information: The VX0 Thin Client contains a battery replaceable by qualified service personnel only.

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.

Contents

1 Introduction

Wyse® Winterm™ 9 series Thin Clients use Windows™ XP embedded (XPe) operating system. These thin clients provide a full featured Internet Explorer browser and access to applications, files, and network resources made available on machines hosting Citrix™ ICA and Microsoft™ RDP session services. Thin client emulation software is installed locally by default. 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 the latest 32-bit Windows compatibility.

Session and network services available on enterprise networks may be accessed through a direct Intranet connection, a dial-up server, or an ISP which provides access to the Internet and thus permits the thin client to connect to an enterprise VPN (virtual private network) server.

Note

The latest firmware version release for Wyse® Winterm™ 9 series Thin Clients is based on the Microsoft XPe SP2 release.

About this Guide

This guide is intended for administrators of the Wyse® Winterm™ 9 series Thin Client. It provides information and detailed system configurations to help administrators design and manage a Wyse® Winterm™ 9 series Thin Client environment.

This guide supplements the standard Windows XP and Windows XPe 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 Windows XP and Windows XPe.

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

Organization of this Guide

This guide is organized as follows:

Chapter 2, "Establishing a Server Environment," contains information on the network architecture and enterprise server environment needed to provide network and session services for Wyse® Winterm™ 9 series Thin Clients. It also includes information to help you to address important considerations when configuring access to the server environment and when configuring the services to be provided by the server environment.

Chapter 3, "Getting to Know the Extended XPe Features," provides information on the extended features of the Winterm™ 9 series Thin Client operating system that are not found in standard Windows XP.

Chapter 4, "Administrative Utilities and Settings," contains general information about the utilities and settings available for administrative use.

Chapter 5, "System Administration," contains information and detailed instructions to help you manage your thin client environment.

Wyse Technical Support

To access Wyse technical resources, visit http://www.wyse.com/serviceandsupport. If you still have questions, you can submit your questions using the Wyse Support Help Form, or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 5:00 am to 5:00 pm PST, Monday through Friday.

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

Related Online Resources Available at Wyse

Wyse® Winterm™ 9 series Thin Client features can found in the Datasheet for your specific thin client model. Datasheets are available on the Wyse Web site at: http://http://www.wyse.com/products.

If you need to upgrade your XPe operating system, contact Wyse Customer Support at: http://www.wyse.com/serviceandsupport.

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

2 Establishing a Server Environment

This chapter contains information on the network architecture and enterprise server environment needed to provide network and session services for Wyse® Winterm™ 9 series Thin Clients. It also includes information to help you to address important considerations when configuring access to the server environment and when configuring the services to be provided by the server environment.

Setting-Up Access to the Enterprise Servers

There are five basic methods of access to the enterprise server environment available to the thin client. Except for Ethernet Direct, all of the access methods require that some local settings be made on the thin client. These local settings are retained and are available for the next thin client system start. Activating these local settings and the defined connections can also be automated at thin client system start.

Methods of access include:

- **Ethernet Direct** - This is a connection from the thin client Ethernet port directly to the enterprise intranet. No additional hardware is required. In this configuration all network services may be used, including the enterprise DHCP server. A DHCP server on the network can provide not only the thin client IP address, but also the location of the file server containing the software updates. For more information on DHCP, refer to "Using Dynamic Host Configuration Protocol (DHCP)."
- **Wireless Direct** - A supported wireless adapter (or the optional internal wireless feature) can be used to access the enterprise intranet. A wireless adapter uses short-range wide-band radio to communicate with a wireless access point. Typically, wireless access points are located at several locations in the enterprise within range of the wireless adapters and directly connected to the enterprise intranet. For more information on configuring wireless network devices or the optional thin client internal wireless feature, refer to "Configuring Wireless Local Area Network (LAN) Settings" and "Configuring the Internal Wireless Feature."
- **PPPoE** - Thin client support for Point-to-Point Protocol over Ethernet (PPPoE) is intended for devices which connect to the Internet directly from remote locations. The New Connection Wizard can be used (available from Network Connections in the Control Panel) to configure and invoke a PPPoE connection. Once connected, all packets are through a PPP connection over Ethernet to the DSL modem. For more information on the New Connection Wizard, refer to documentation on the Microsoft Web site at: http://www.microsoft.com.
- **Dial-up Modem** - A dial-up modem can be used with the thin client to access a dial-up server. The dial-up server must be a Microsoft Remote Access Server or another server that supports industry-standard protocols. The dial-up server can provide either of the following methods of access to the enterprise intranet:
  - Direct access - An enterprise dial-up server directly connects to the enterprise intranet.
  - Indirect access - An Internet Service Provider (ISP) dial-up server simply provides access to the Internet, from which the thin client accesses an enterprise PPTP VPN server that connects to the enterprise intranet.

- **VPN (PPTP)** - PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data between a remote client (in this case the thin client) and an enterprise server environment by creating a virtual private network (VPN) across TCP/IP-based data networks such as the Internet. It provides a password-protected path through the enterprise firewall to the enterprise server environment in which the network and session services required by thin clients reside. The New Connection Wizard can be used (available from Network Connections in the Control Panel) to configure and invoke a VPN connection.

  An Internet Service Provider (ISP) must be available to provide access to the Internet. Any of the standard means of connecting to the ISP may be used, such as a dial-up modem, cable modem, and DSL modem. The connection to the ISP must be established first, before contacting the enterprise PPTP VPN server. This includes dial-up access as well as direct access through the cable modem and DSL modem paths. For more information on the New Connection Wizard, refer to documentation on the Microsoft Web site at: http://www.microsoft.com.

Understanding the Network Services Used and Provided by the Thin Client

Setting-up network services allows users to initiate connections to the enterprise servers providing ICA, RDP, and other services. Network services used by the thin client include DHCP, DNS, and LPD.

Note

The thin client can act as an LPR client and use the LPD services provided by other nodes on the network. In addition, the thin client can act as an LPD server and provide print services to other nodes on the network.

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). Using DHCP to configure thin clients saves you the time and effort needed to complete these processes locally on multiple thin clients. A DHCP server can also provide the IP address of the Wyse Device Manager server (for information on Wyse Device Manager, refer to "Using Wyse Device Manager (WDM) for Remote Administration and Upgrades").

Note

If a particular thin client is to function as an LPD print server, it should be assigned a fixed IP address. However, you can also guarantee that an LPD server will get the same IP address every time by making a reservation for that thin client in the DHCP server. In that way, you can preserve the stateless nature of the thin client and still guarantee a fixed address for the server. In fact, you can assign a symbolic name to the reservation address so that other thin clients can reference the LPD server by name rather than by static IP address (the symbolic name must be registered with a DNS server before other thin clients will be able to locate this LPD server). The thin client does not dynamically register its name and the DNS registration must be manual.

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

Note

Use of DHCP is recommended. If a DHCP server is not available, fixed IP addresses can be assigned (this does, however, reduce the stateless functionality of the thin clients) and must be entered locally for each device.

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.

Table 1 DHCP Options, Continued

Option	Description	Notes
159	Command Line for a connection	Optional.
160	Working Directory for a connection	Optional.
163	SNMP Trap server IP Address list	Optional.
164	SNMP Set Community	Optional.
165	RDP startup published applications	Optional.
166	Terminal Emulation Mode	Optional.
167	Terminal Emulation ID	Optional.
168	Name of the server for the virtual port	Optional.

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. However, the thin client does not do dynamic registration and therefore, requires a static or non-variant IP address and manual DNS registration in order to provide LPD support by name (for example, in the case where the thin client is used as an LPD printer server). For DHCP entry of DNS domain and server location information, refer to "Using Dynamic Host Configuration Protocol (DHCP)."

Configuring and Providing Line Printer Daemon (LPD) Services

A thin client can be configured to provide Line Printer Daemon (LPD) services (making the thin client a printer server receiving print jobs from one or more clients and spooling these jobs to a designated physical port). The LPD server receives print jobs sent to a named line printer queue from the LPR client and prints them on the designated printer.

For more information on LPD configuration, refer to documentation on the Microsoft Web site at: http://www.microsoft.com.

A thin client can also be configured as an LPR client. LPR is a component of the Line Printer Daemon Protocol. LPR is a client sending a print job to a server. LPR works in conjunction with the Line Printer Daemon (LPD) server by assigning a print job to a named line printer queue managed by the LPD server. The LPD is a server receiving print tasks from one or more clients and spooling these jobs to a physical port.

For more information on LPR configuration, refer to documentation on the Microsoft Web site at: http://www.microsoft.com.

Understanding Session Services

Thin-client session services are made available by servers hosting Citrix ICA and Microsoft RDP software products.

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, refer to the "Configuring Independent Computing Architecture (ICA) Session Services."

Note

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.

Remote Desktop Protocol (RDP) is a network protocol that allows a thin client to communicate with the Terminal Server or Windows 2000/2003 Server with Terminal Services over the network. This protocol is based on the T.120 protocol suite, an international standard multi-channel conferencing protocol. The thin client supports RDP version 5.x. For information on configuring RDP, refer to "Configuring Remote Desktop Protocol (RDP) Session Services."

Configuring Independent Computing Architecture (ICA) Session Services

ICA session services can be made available on the network using either of the following services:

- Windows 2000 or 2003 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.

Note

If a Windows 2000 or 2003 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere on the network. The server will grant a temporary (90-day) license on an individual device basis. Beyond the temporary (90-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 Remote Desktop Protocol (RDP) 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, and Windows XP Professional, or a server running Microsoft® Windows NT® Server 4.0, Terminal Server Edition. The Remote Desktop Protocol allows a thin client to execute Windows applications within a Windows graphical user interface (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.

Note

If a Windows 2000 or 2003 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere on the network. The server will grant a temporary (90-day) license on an individual device basis. Beyond the temporary (90-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).

3 Getting to Know the Extended XPe Features

This chapter provides information on the extended features of the Winterm™ 9 series Thin Client operating system that are not found in standard Windows XP.

Controls for most of these extended XPe features are available only through an Administrator logon account—exceptions include the Citrix Program Neighborhood, the Microsoft™ Terminal Server Client (Remote Desktop Connection), and if installed, a special-order terminal emulation application.

Logging On to the Thin Client

Users can log-on automatically or manually.

Note
The password for the BIOS is Fireport.

Automatic Log-on

Automatic log-on is enabled on the thin client by default. An administrator can use the Winlog applet in the Control Panel to enable/disable auto logon and change the auto logon user name, password, and domain. Only an Administrator logon account can change auto logon properties.

Note
To save the changes, be sure to flush the Enhanced Write Filter cache at any time during the current system session. For information about the Enhanced Write Filter and procedures for flushing the cache, refer to "Using the Enhanced Write Filter (EWF)."

The Log-on to Windows dialog box is automatically by-passed if automatic log-on is enabled. However, if you want to log-on as a different user while auto logon is enabled, log off while holding down the SHIFT key to display the Log-on to Windows dialog box. You can then manually enter log-on information.

Manual Log-on

When automatic log-on is not enabled, the Log-on to Windows dialog box displays upon thin client startup.

Enter the log-on information using the following guidelines:

- For a User log-on account, the factory-default user name and password are both `User`.
- For an Administrator log-on account, the factory-default user name and password are both `Administrator`.

Note
Passwords are case sensitive but user names are not case sensitive.

Caution

For security purposes it is recommended that all passwords be changed from the defaults. An administrator can change passwords by using the CTRL+ALT+DEL key combination to open the Windows Security dialog box and then clicking **Change Password.** The password cannot be changed when logged-on as a user.

Note

An administrator can create additional user accounts by using the User Manager utility (available by double-clicking the **Administrator Tools** icon in the Control Panel). However, due to local memory constraints, the number of additional users should be kept to a minimum. For administrator information on User accounts, refer to "Managing Users and Groups with User Manager."

About the Automatically Launched Utilities

The following utilities are automatically launched:

- **Enhanced Write Filter** - Upon system start, the Enhanced Write Filter utility is automatically launched. The Enhanced Write Filter provides security and protects the flash memory from excessive write activity. The active/inactive status of the Enhanced Write Filter is indicated by the color of the Enhanced Write Filter status icon in the system tray of the desktop taskbar. For more information about the Enhanced Write Filter, refer to "Using the Enhanced Write Filter (EWF)."

Note

Changes made to the thin client configurations are lost when the thin client is restarted unless the Enhanced Write Filter cache is flushed during the current system session. For procedures on flushing the cache, refer to "Using the Enhanced Write Filter (EWF)."

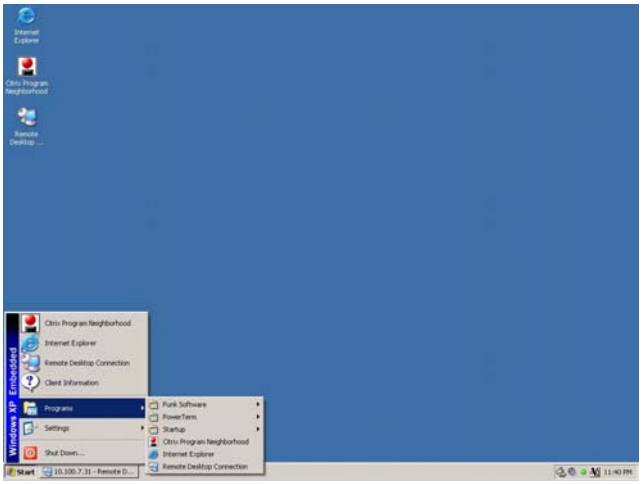
- **NetXClean** - Upon system start, the NetXClean utility is automatically launched. NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. For more information about NetXClean, refer to "Understanding the NetXClean Utility."
- **VNC Server** - Upon successful thin client log-on, the Windows VNC Server utility is automatically launched. VNC allows the thin client desktop to be accessed remotely for administration and support. For more information about VNC, refer to "Using WinVNC to Shadow a Thin Client."
- **Time Synchronization Utility** - Upon successful thin client log-on, the time synchronization utility dialog box displays. This feature can be disabled by an administrator (locally or remotely) if desired. For more information about time synchronization, refer to "Synchronizing Thin Client Time with Neutron."

Understanding the User Desktop

Desktop icons present on a default user desktop include Citrix Program Neighborhood, Remote Desktop Connection, and Internet Explorer. These items are also available from

the Start menu (if installed, the terminal emulation application can also be accessed from the Start menu). The audio volume icon, VNC Server icon, Enhanced Write Filter status icon, and the System time are located in the system tray of the taskbar.

Figure 1 User desktop - example



Note

Links to ICA-published applications may also be listed in the Start menu and/or appear as desktop icons.

Use the following guidelines:

- The user Control Panel (available by clicking **Start** | **Settings** | **Control Panel**) provides access to a limited set of resources for configuring Windows XP user preference settings. You must be logged on as an administrator to access the extended set of system resources.
- Right-clicking the users desktop does not open a pop-up menu.
- You can copy and paste text between a remote session and the local computer by using standard Windows copy and paste methods.

For information about the functionality of the standard Windows XP desktop and Start menu items, refer to the applicable Microsoft documentation (search and navigate to the Windows XP Support Center) at: http://support.microsoft.com/default.aspx.

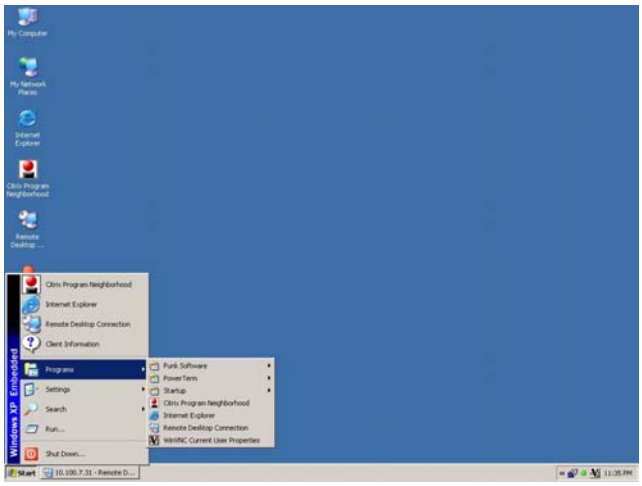
For more information about Citrix Program Neighborhood, refer to "Managing Connections with Citrix Program Neighborhood."

For more information about Remote Desktop Connection, refer to "Establishing Remote Desktop Connections."

Understanding the Administrator Desktop

Desktop icons present on the default Administrator desktop include My Computer, My Network Places, Citrix Program Neighborhood, Remote Desktop Connection, Internet Explorer, Enhanced Write Filter Enable, and Enhanced Write Filter Disable. Citrix Program Neighborhood, Internet Explorer, and Remote Desktop Connection are also available from the Start menu (if installed, the terminal emulation application can also be accessed from the Start menu). The audio volume icon, Enhanced Write Filter status icon, VNC Server icon, and the System time are located in the system tray of the taskbar. Extended resources (see "Accessing the Programs Extended Menu") available to administrators, can also be accessed from the Start menu. In addition, right-clicking the Administrator desktop opens a pop-up menu.

Figure 2 Administrator desktop - example



For information about the functionality of the standard Windows XP desktop and Start menu items, refer to the applicable Microsoft documentation (search and navigate to the Windows XP Support Center) at: http://support.microsoft.com/default.aspx.

Viewing Thin Client Information

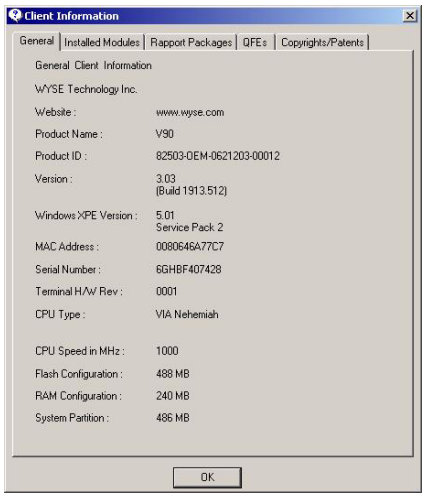
Use the Client Information dialog box (available by clicking **Start | Client Information**) to view various information about the thin client.

Note

The information shown varies for different thin clients and software releases.

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

Figure 3 Client Information



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.
- **Rapport Packages** - Displays the list of Rapport Packages (Rapport is now called Wyse Device Manager) that have been applied to the thin client.
- **QFEs** - Displays the list of Microsoft QFEs (formerly Hotfixes) applied to the thin client.
- **Copyrights/Patents** - Displays Wyse copyright and patent information.

Logging Off, Restarting, and Shutting Down the Thin Client

Use the Start menu on the taskbar to log off, restart, or shut down the thin client (options are available to use by clicking **Start | Shut Down**).

You can also log off or shut down the thin client using the Windows Security dialog box (which can be opened by using CTRL+ALT+DEL).

Note

If automatic log-on is enabled, when you log off (without shutting down) the thin client immediately logs on the default user. For instructions on logging on as a different user, refer to "Logging On to the Thin Client."

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

- **Enhanced Write Filter cache** - If you make changes to system configuration settings and want them to persist, you must flush the Enhanced 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 Enhanced 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 Enhanced Write Filter cache after the new log-on and still retain the changes. For instructions on flushing the Enhanced Write Filter cache, refer to "Setting the Enhanced Write Filter Controls." For general information about the Enhanced Write Filter, refer to "Using the Enhanced Write Filter (EWF)."

Note

A User log-on account does not have cache flush privileges; 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. For details about NetXClean, refer to "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. Settings are available by clicking **Start | Settings | Control Panel | Display | Screen Saver | Power**.
- **Wake-on-LAN** - This standard Windows XP feature allows Wyse Device Manager software 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.

Note

Correct time should be maintained as some applications require access to local thin client time. The Date and Time Properties dialog box can be opened by double-clicking the System time area in the taskbar or by double-clicking the **Date and Time** icon in the Control Panel.

Accessing the Programs Extended Menu

This section provides an overview of the Programs extended menu (options available to use by clicking **Start** | **Programs**) including:

- "Using the Odyssey Client Manager"
- "Managing Connections with PTSManager and ptw32"
- "Synchronizing Thin Client Time with Neutron"
- "Managing Connections with Citrix Program Neighborhood"
- "Browsing the Internet with Internet Explorer"
- "Establishing Remote Desktop Connections"
- "Setting WinVNC Current User Properties"

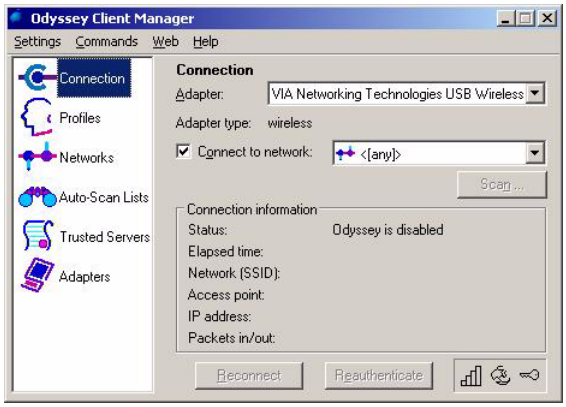
Using the Odyssey Client Manager

If purchased and installed, the Odyssey Client Manager is available to users and administrators. Clicking **Start | Programs | Funk Software | Odyssey Client | Odyssey Client Manager** (or double-clicking the icon in the Control Panel or Administrator system tray) opens the Odyssey Client Manager dialog box. Use this dialog box to establish a secure connection to an enterprise wireless or wired 802.1X network.

For information on using the Odyssey Client Manager, refer to http://www.juniper.net/products/aaa/odyssey/oac.html).

For information on configuring the optional Internal Wireless feature by using the Windows Wireless Zero Configuration utility, refer to "Using Wireless Zero Configuration (WZC)."

Figure 4 Odyssey Client Manager



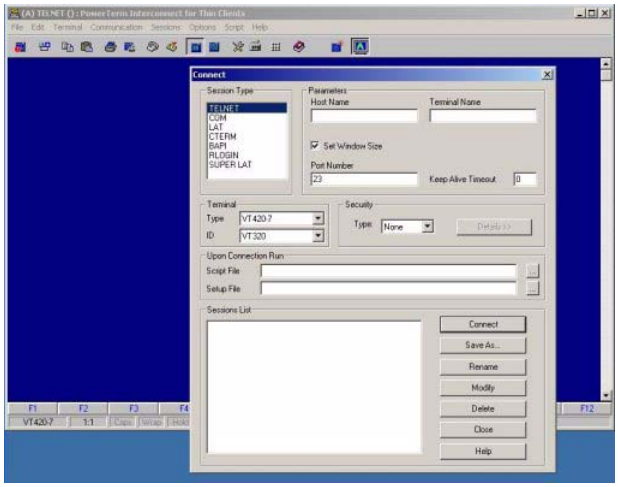
Managing Connections with PTSManager and ptw32

PTS Manager and ptw32 are available to users and administrators. Clicking **Start | Programs | PowerTerm | PTSManager** (by default, a desktop icon is not installed) opens the Power Term Session Manager. Use the Power Term Session Manager to manage your connections.

Figure 5 Power Term Session Manager

Clicking **Start | Programs | PowerTerm | ptw32** (by default, a desktop icon is not installed) opens the terminal emulation window and Connect dialog box.

Figure 6 Terminal emulation and Connect



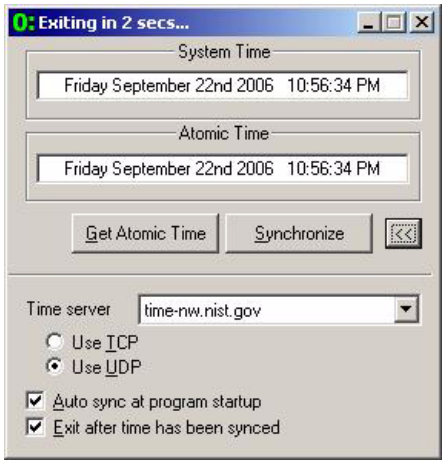
The ptw32 application allows you to configure your connection information. For complete instructions on installing and using terminal emulation, refer to the terminal emulation documentation supplied separately.

Synchronizing Thin Client Time with Neutron

Neutron time synchronization is available to users and administrators. Clicking **Start | Programs | Startup | Neutron** opens the Neutron dialog box. The Neutron dialog box contains the current System Time and Atomic Time. To Synchronize the System Time with the Atomic Time, click **Synchronize** in the Neutron dialog box. To retrieve the current Atomic time from a time server, click **Get Atomic Time**.

To configure the Time server IP address, click **>>** in the Neutron dialog box to open the extended menu and select an IP address from the Time server list. You can also select (using the options and check boxes) whether to use TCP or UDP, whether or not you want Auto synchronization to occur at system startup, and whether or not to exit the Time server after the time has been synchronized. To close the extended menu, click **<<**.

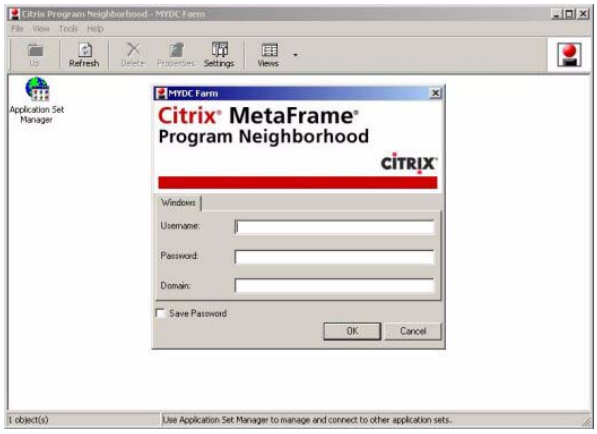
Figure 7 Neutron - extended view



Managing Connections with Citrix Program Neighborhood

Cirtix Program Neighborhood is available to users and administrators. Clicking **Start | Programs | Citrix Program Neighborhood** or **Start | Citrix Program Neighborhood** (or double-clicking the desktop icon) opens the Citrix Program Neighborhood window. Use this program to manage connections to remote applications running on ICA servers. Documentation for the ICA client application is available on the Citrix Web site at: http://download2.citrix.com/files/en/products/client/ica/current/docs/ica_win32_guide.pdf

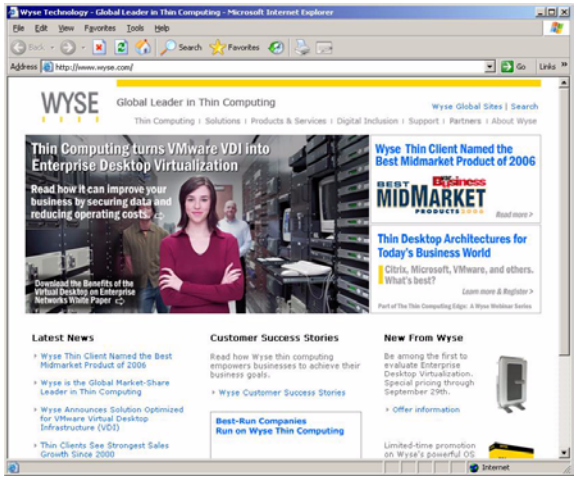
Figure 8 Citrix Program Neighborhood



Browsing the Internet with Internet Explorer

Microsoft Internet Explorer (MSIE) browser is installed locally on the thin client, and is available to users and administrators. Clicking **Start | Programs | Internet Explorer** or **Start | Internet Explorer** (or double-clicking the desktop icon) opens IE. The Internet options settings for the browser 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. A user can access another browser through an ICA or RDP account if more browser resources are required.

Figure 9 Internet Explorer



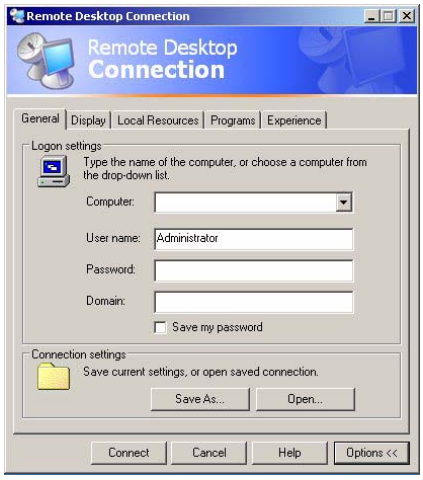
Establishing Remote Desktop Connections

Remote Desktop Connection is available to users and administrators. Clicking **Start | Programs | Remote Desktop Connection** or **Start | Remote Desktop Connection** (or double-clicking the desktop icon) opens the Remote Desktop Connection dialog box (you can expanded the view by clicking **Options**). Use this program to establish and manage connections to remote applications. For information on using the Remote Desktop Connection, refer to the Microsoft documentation at: http://www.microsoft.com

Note

If you find that the Enhanced Write Filter cache is becoming too full, you can disable Bitmap caching in the Experience tab.

Figure 10 Remote Desktop Connection - expanded view



Setting WinVNC Current User Properties

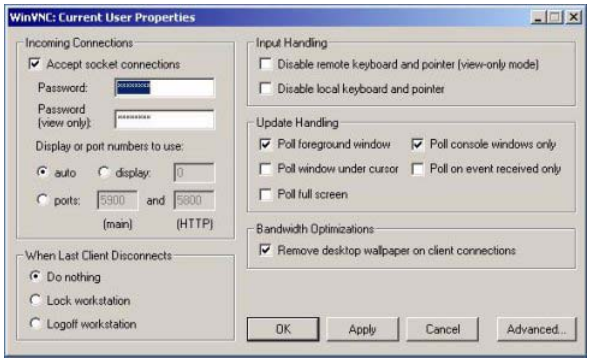
WinVNC Current User Properties is available to Administrators only. Clicking **Start | Programs | WinVNC Current User Properties** (or double-clicking the icon in the Administrator system tray) opens the WinVNC: Current User Properties dialog box. Use this dialog box to enter the VNC log-on password (the default password is `Wyse`), and to select the parameters for the VNC server utility installed on a thin client.

VNC Server allows a thin client to be operated/monitored (shadowed) from a remote machine on which VNC Viewer is installed. VNC is intended primarily for support and troubleshooting purposes. For information on VNC user settings, refer to "Using WinVNC to Shadow a Thin Client."

Note

Hovering the mouse pointer over the VNC icon on the taskbar shows the current IP address of the thin client.

Figure 11 WinVNC: Current User Properties

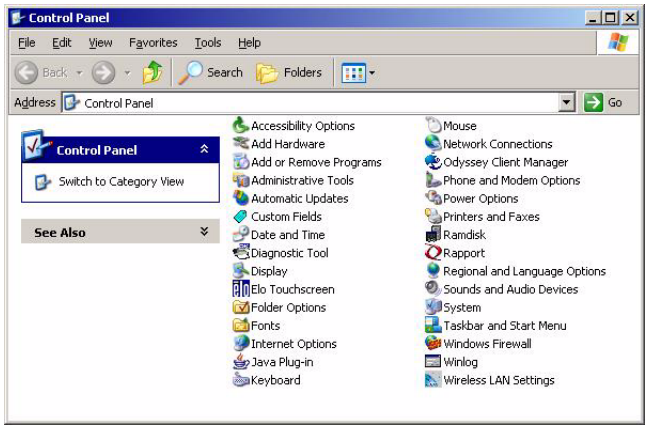


Accessing the Administrator Control Panel Extended Options

This section provides an overview of the Administrator Control Panel extended options (options available to use by clicking **Start** | **Settings | Control Panel**), including:

- "Accessing and Using the Administrative Tools"
- "Setting Configuration Strings with Custom Fields"
- "Configuring Touchscreens"
- "Using Sun Java Runtime Environment"
- "Setting Ramdisk Size"
- "Configuring Rapport Properties"
- "Selecting Regional and Language Options"
- "Configuring Winlog for Automatic Logon."
- "Configuring Wireless Local Area Network (LAN) Settings"

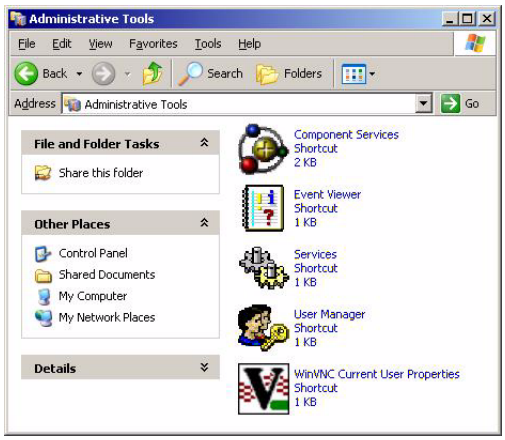
Figure 12 Administrator Control Panel - Classic View/List



Accessing and Using the Administrative Tools

Double-clicking the **Administrative Tools** icon in the Control Panel opens the Administrative Tools window.

Figure 13 Administrative Tools



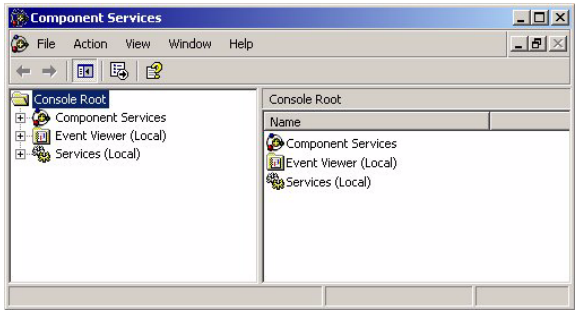
Administrative Tools are available for:

- "Configuring Component Services"
- "Viewing Events"
- "Managing Services"
- "Managing Users"
- "Configuring WinVNC Current User Properties"

Configuring Component Services

Double-clicking the **Component Services** icon opens the Component Services window. The console allows access to configure the Component Services, Event Viewer, and Local Services.

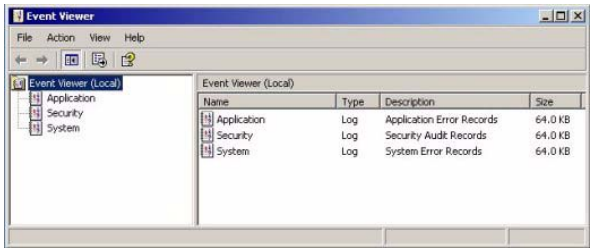
Figure 14 Component Services



Viewing Events

Double-clicking the **Event Viewer** icon opens the Event Viewer window. This tool displays monitoring and troubleshooting messages from Windows and other programs.

Figure 15 Event Viewer



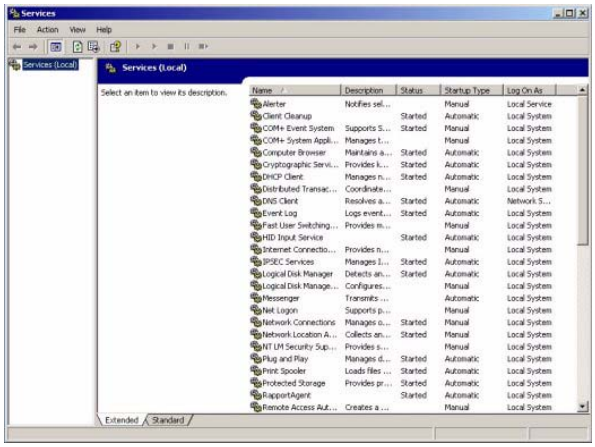
Managing Services

Double-clicking the **Services** icon opens the Services window. The **Services** window lists the services installed on the thin client. VNC Server and Client Clean-up (NetXClean) are two services which may need to be stopped or restarted by a thin client administrator and are discussed in "Administrative Utilities and Settings."

Note

VNC Server and Client Clean-up (NetXClean) can be stopped using the Task Manager.

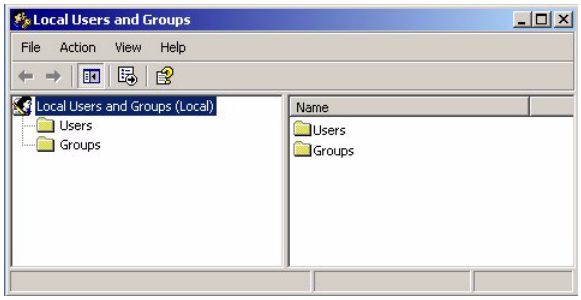
Figure 16 Services



Managing Users

Double-clicking the **User Manager** icon opens the Local Users and Groups window. This tool allows administrators to manage users and groups. For detailed information on the User Manager, refer to "Managing Users and Groups with User Manager."

Figure 17 Local Users and Groups



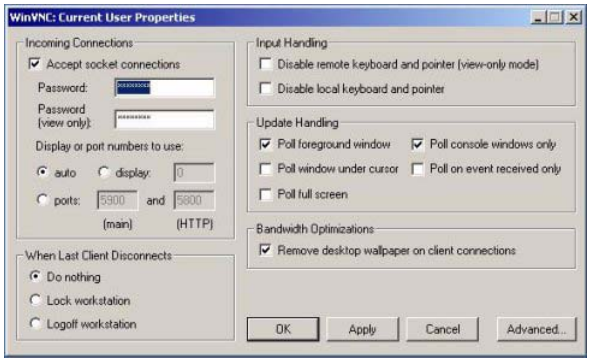
Configuring WinVNC Current User Properties

Double-clicking the **WinVNC Current User Properties** icon opens the WinVNC: Current User Properties dialog box. Use this dialog box to enter the VNC log-on password (the default password is `Wyse`), and to select the parameters for the VNC server utility installed on a thin client.

Note

This dialog box can also be opened from the Administrator **Start** | **Programs** menu (or by double-clicking the icon in the Administrator system tray).

Figure 18 WinVNC: Current User Properties



VNC server allows a thin client to be operated/monitored (shadowed) from a remote machine on which VNC Viewer is installed. VNC is intended primarily for support and troubleshooting purposes. For information on VNC user settings, refer to "Using WinVNC to Shadow a Thin Client."

Note

Hovering the mouse pointer over the VNC icon on the taskbar shows the current IP address of the thin client.

Setting Configuration Strings with Custom Fields

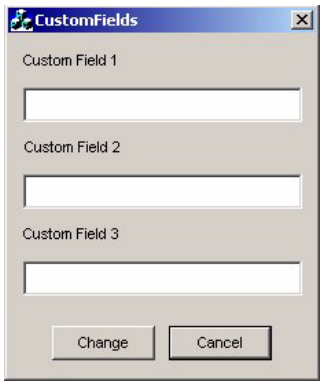
Double-clicking the **Custom Fields** icon in the Control Panel opens the Custom Fields dialog box. Use this dialog box to enter configuration strings for use by Wyse Device Manager (formerly Rapport) software. The configuration strings can contain information about the location, user, administrator, and so on.

Clicking **Change** in the dialog box transfers the custom field information to the Windows registry. The information is then available to the Wyse Device Manager Client Manager. To permanently save the information, flush the Enhanced Write Filter cache during the system session in which the registry entries are made or changed.

For more information on using Wyse Device Manager for remote administration and upgrading thin client software, refer to "System Administration."

For details on using custom field information, refer to the Wyse Device Manager documentation.

Figure 19 Custom Fields



Configuring Touchscreens

If the ELO Touchscreen option is installed on the thin client, double-clicking the **ELO Touchscreen** icon in the 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.

Note

Re-calibration and adjustment of the monitor settings may be required after updating thin client software.

Using Sun Java Runtime Environment

Sun Java Runtime Environment (JRE) is available, but does not include the Microsoft Virtual Machine. Information about this application can be found online at: http://java.sun.com.

Setting Ramdisk Size

Ramdisk is volatile memory space set aside for temporary data storage. It is the Z drive shown in the My Computer window.

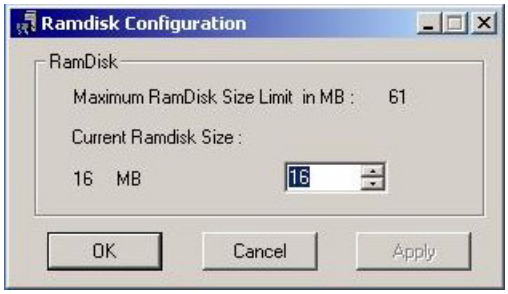
The following items are stored on Ramdisk:

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

The Ramdisk can also be used for temporary storage of other data according to administrator discretion (see "Saving Files and Using Local Drives").

Double-clicking the **Ramdisk** icon in the Control Panel opens the Ramdisk Configuration dialog box. Use this dialog box 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 Enhanced Write Filter cache has been flushed during the current system session *before* restarting the system.

Figure 20 Ramdisk Configuration



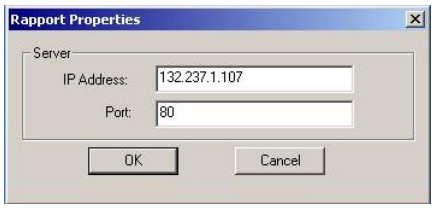
Note

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).

Configuring Rapport Properties

Double-clicking the **Rapport** icon in the Control Panel opens the Rapport Properties dialog box. Use this dialog box to configure the Rapport settings.

Figure 21 Rapport Properties



To configure:

1. Enter the Wyse Device Manager Server hostname or IP address in the IP Address text box.
2. Enter the port to use in the Port text box.
3. Click **OK**.

For information on Wyse Device Manager (formerly known as Rapport) software, refer to "Using Wyse Device Manager (WDM) for Remote Administration and Upgrades."

Selecting Regional and Language Options

Double-clicking the **Regional and Language Options** icon in the Control Panel opens the Regional and Language Options dialog box. Use this dialog box to select your keyboard language. The following keyboard languages are supported:

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

Note

A language appropriate keyboard is required for any language other than English (US). Keyboards are different for each of the languages listed.

The default language for the user interface is English (US). 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, complete the following procedures:

1. Click **Start | Settings | Control Panel**.
2. Double-click the **Regional and Language Option** icon to open the Regional and Language Options dialog box.

3. Click the **Languages** tab.
4. Select a language from the Language used in menus and dialogs list, and click **Apply** (a message informs you that changes will not take effect until you logoff and logon again).
5. Click **OK**.
6. In the Regional and Language Options dialog box, click **OK** and then close the Control Panel.
7. Log off the current user.
8. Log on to the thin client (the GUI will be in the selected language).

Configuring Winlog for Automatic Logon

Automatic log-on is enabled on the thin client by default. Double-clicking the **Winlog** icon in the Administrator Control Panel opens the Winlog dialog box. Use this dialog box to enable or disable auto logon, and to change the auto logon user name, password, and domain. Only an Administrator logon account can change auto-logon properties.

Note

To save the changes, be sure to flush the Enhanced Write Filter cache at any time during the current system session. For information about the Enhanced Write Filter and procedures for flushing the cache, refer to "Using the Enhanced Write Filter (EWF)."

Configuring Wireless Local Area Network (LAN) Settings

If Wyse USB 802.11b hardware is installed on the thin client, double-clicking the **Wireless LAN Settings** icon in the Administrator Control Panel allows you to configure wireless LAN settings (such as the wireless network ID, and so on).

Note

The Wireless LAN Settings icon is available only in the Administrator Control Panel and is for the specific Actiontec USB wireless device only.
The wireless LAN settings made using this icon are not applied to any other wireless cards (such as Cisco 350 and Orinoco Silver).
Any non-Actiontec adapters must be configured through **Start | Control Panel | Network Connections** or through the Device Manager.

For information on configuring the optional Internal Wireless feature installed on some Wyse® Winterm™ 9 series Thin Clients, refer to "Configuring the Internal Wireless Feature."

Configuring the Internal Wireless Feature

You can configure the optional Internal Wireless feature by using either the Windows Wireless Zero Configuration utility (see "Using Wireless Zero Configuration (WZC)") or the Odyssey Client Manager (for documentation on using the Odyssey Client, refer to http://www.juniper.net/products/aaa/odyssey/oac.html).

Using Wireless Zero Configuration (WZC)

Note

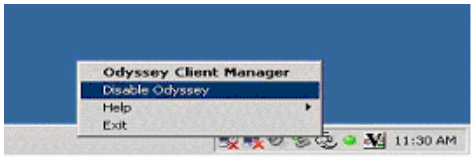
Before using these procedures, be sure you have imported any user certificates and computer certificates (of a server) you will need into the thin client.

To configure the optional Internal Wireless feature by using WZC:

1. If the Odyssey Client Manager is installed, you must disable it as described in this section. If it is not installed, then continue with "Configuring Wireless Thin Clients for EAP-TLS Authentication (Smart Card or other Certificate)" or "Configuring Wireless Thin Clients for PEAP-MS-CHAP v2.".

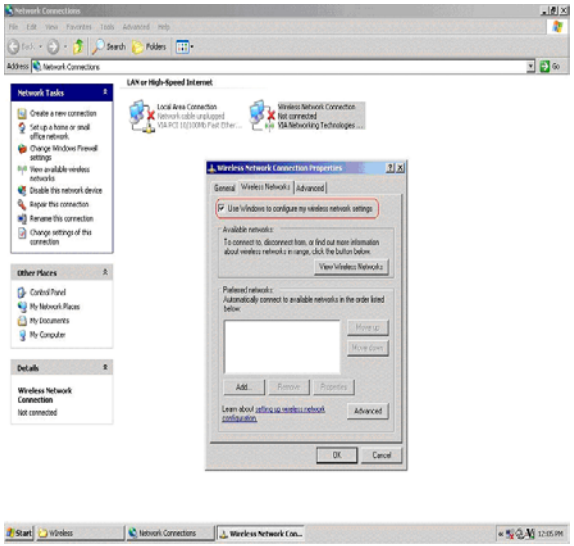
   To disable the Odyssey Client Manager, right-click on the Odyssey icon in the system tray and click **Disable Odyssey**.

Figure 22 Disable Odyssey



2. Click **Start | Settings | Network Connections** to view the available network connections.
3. Right-click **Wireless Network Connection** and select **Properties** to open the Wireless Network Connection Properties dialog box.

Figure 23 Wireless Network Connection Properties

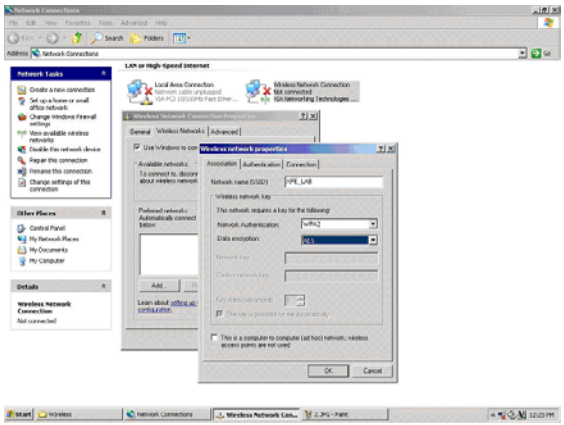


4. Select the **Wireless Network** tab and then select the **Use Windows to configure my wireless network settings** check box
5. Click **OK** and continue with "Configuring Wireless Thin Clients for EAP-TLS Authentication (Smart Card or other Certificate)" or "Configuring Wireless Thin Clients for PEAP-MS-CHAP v2."

Configuring Wireless Thin Clients for EAP-TLS Authentication (Smart Card or other Certificate)

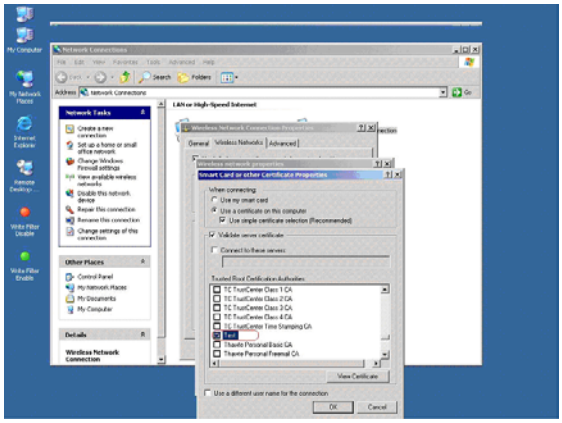
1. Right-click **Wireless Network Connection** and select **Properties** to open the Wireless Network Connection Properties dialog box.
2. Select the **Wireless Network** tab and then click **Add** to open the Wireless Network Properties dialog box.

Figure 24 Wireless Network Properties - EAP-TLS



3. Click the **Association** tab.
4. Enter the Network name (SSID).
5. Select the **WPA2** option for Network Authentication.
6. Select the **AES** option for Data encryption.
7. Click the **Authentication** tab.
8. Select the **Enable IEEE 802.1x authentication for this network** check box.
9. Select the **Smart Card or other Certificate** option for EAP type.
10. Click **Properties** to open the Smart Card or other Certificate Properties dialog box.

Figure 25 Smart Card or other Certificate Properties - EAP-TLS

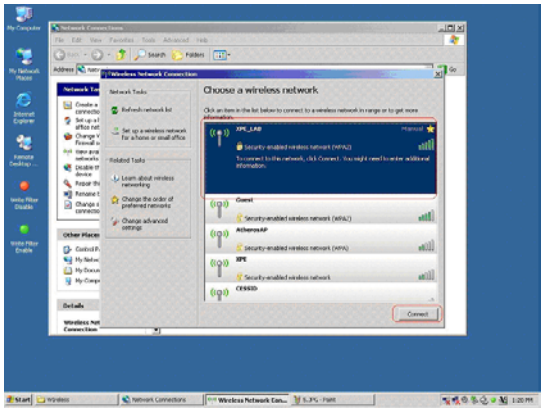


11. Select the **Use a certificate on this computer** option (to use a registry-based user certificate) and select the **Use simple certificate selection** check box.
12. Depending on whether or not you want to validate the computer certificate of the IAS server, select or clear the **Validate server certificate** check box. If you select the check box, select the certificate you want (which you have already imported into the thin client) in the *Trusted Root Certification Authorities* list, and then click **OK**.
13. Click **OK** until all changes have been saved and all dialog boxes have been closed.

A wireless connection should now be established; if a wireless connection is not established:

1. Click **Start | Settings | Network Connections** to view the available network connections.
2. Right-click **Wireless Network Connection** and select **View Available Wireless Networks** to open the Wireless Network Connection dialog box.

Figure 26 Wireless Network Connection - EAP-TLS



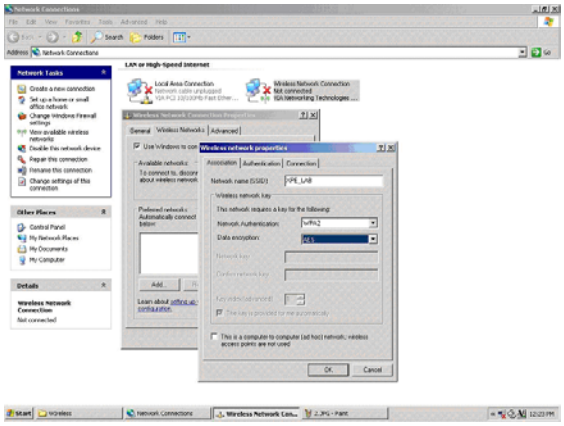
3. Select the connection you created in step 4 (the Network name (SSID)), and then click **Connect**.

A wireless connection should now be established.

Configuring Wireless Thin Clients for PEAP-MS-CHAP v2

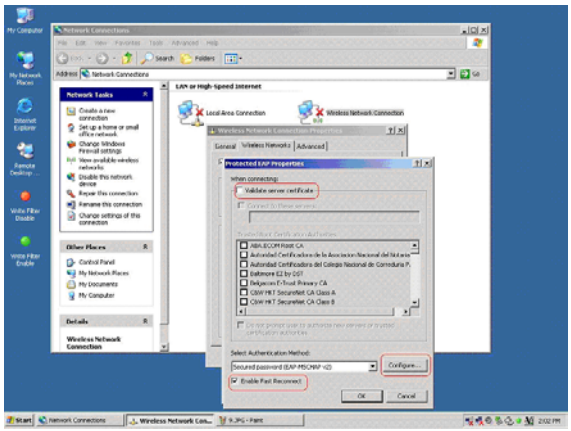
1. Right-click **Wireless Network Connection** and select **Properties** to open the Wireless Network Connection Properties dialog box.
2. Select the **Wireless Network** tab and then click **Add** to open the Wireless Network Properties dialog box.

Figure 27 Wireless Network Properties PEAP-MS-CHAP v2



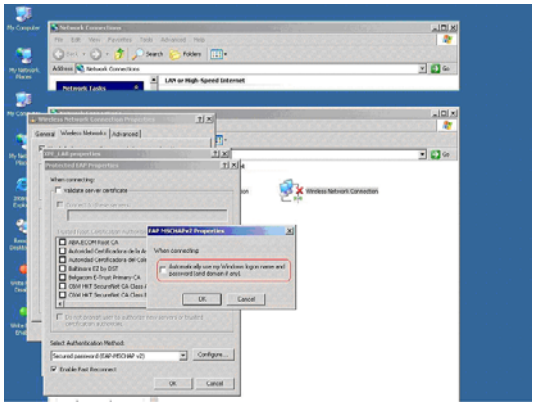
3. Click the **Association** tab.
4. Enter the Network name (SSID).
5. Select the **WPA2** option for Network Authentication.
6. Select the **AES** option for Data encryption.
7. Click the **Authentication** tab.
8. Select the **Enable IEEE 802.1x authentication for this network** check box.
9. Select the **Protected EAP (PEAP)** option for EAP type.
10. Click **Properties** to open the Protected EAP Properties dialog box.

Figure 28 Protected EAP Properties - PEAP-MS-CHAP v2



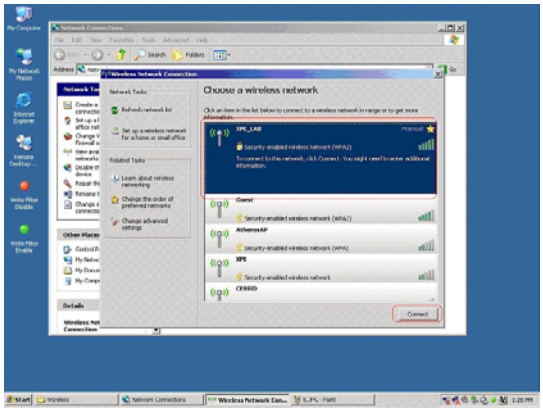
11. Clear the **Validate server certificate** check box.
12. Select the **Enable Fast Reconnect** check box.
13. Click **Configure** to open the EAP MSCHAPv2 Properties dialog box.

Figure 29 EAP MSCHAPv2 Properties - PEAP-MS-CHAP v2



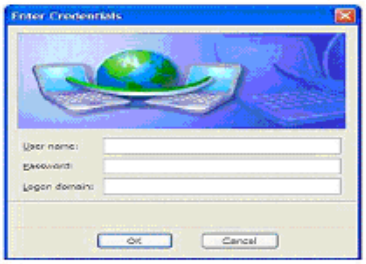
14. Clear the **Automatically use my windows logon name and password (and domain if any)** check box and click **OK**.
15. Click **OK** until all changes have been saved and all dialog boxes have been closed.
16. Right-click **Wireless Network Connection** and select **View Available Wireless Networks** to open the Wireless Network Connection dialog box.

Figure 30 Wireless Network Connection - PEAP-MS-CHAP v2



17. Select connection you created in step 4 (the Network name (SSID)), and then click **Connect**.
18. Click on the *Wireless Network Connection* pop-up message that appears on the system tray to open the Enter Credentials dialog box.

Figure 31 Enter Credentials - PEAP-MS-CHAP v2



19. Enter the User name, Password and Domain name, and then click **OK**.

A wireless connection should now be established.

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-in to the back of the thin client (if the appropriate software is installed).

Note

Add-ons for other services can be installed (Add-ons are available from Wyse for free or for a licensing fee). For information on Wyse Add-ons available, refer to the Wyse Web site at: http://www.wyse.com/products/software/firmware/.

Configuring Printers

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. Be sure to flush the Enhanced Write Filter cache to save the installation. For procedures on flushing the cache, refer to "Using the Enhanced Write Filter (EWF)."

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

Note

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, you must install the print driver on the server and the text only driver on the thin client according to the procedures in "Adding Printers."

Adding Printers

To install the print driver on the server and the text only driver on the thin client:

1. Connect the printer to the thin client.
2. Click **Start** | **Settings | Printers and Faxes**.
3. Double-click **Add a printer** to open the Add Printer Wizard.
4. Click **Next** in the first window of the wizard.
5. Select the **Local printer attached to this computer** option.
6. Ensure that the **Automatically detect and install my Plug and Play printer** check box is *not* selected.
7. Click **Next**.
8. Select the **Use the following port** option.
9. Select the appropriate port from the list and click **Next**.
10. Select the **Manufacturer** and **Model** of the printer and click **Next**.

11. Enter a name for the printer and click **Next**.
12. Select the **Do not share this printer** option and click **Next**.
13. Select whether or not to print a test page and click **Next**.
14. Click **Finish** (the installation will complete and a test page will print if this option was selected).

Controlling Thin Client Audio

Audio can be redirected from applications to the audio jacks on the thin client. The level can be controlled externally (for example, by using a 600-ohm potentiometer control). The volume can also be adjusted using the sound icon in the taskbar system tray. You can single-click the sound icon to open the master volume control, or double-click the sound icon to open the volume control application dialog box. Powered speakers are recommended.

This page intentionally blank.

4 Administrative Utilities and Settings

This chapter contains general information about the utilities and settings available for administrative use.

It discusses:

- “Using the Enhanced Write Filter (EWF)”
- "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 Manager"
- "Changing the Computer Name of a Thin Client"

Using the Enhanced Write Filter (EWF)

The Enhanced 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 Enhanced 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 the results of writes to the registry, favorites, cookies, and so on, the contents of the cache can be transferred (flushed) to the flash on demand by using Wyse Device Manager software or manually by using the Enhanced Write Filter Control dialog box (see "Setting the Enhanced Write Filter Controls"). It can be opened either through the **Start | Run** command line (`ewfmgr.exe C:`) or by double-clicking the Enhanced Write Filter (EWF) icon in the Administrator system tray. After the Enhanced Write Filter has flushed the cache, all future writes during the current system session are written to the flash, with no further caching until a thin client system restart occurs. The Enhanced Write Filter can also be enabled/disabled through the command line or through the Enhanced Write Filter Enable/Disable desktop icons. The status (enabled/disabled) of the Enhanced Write Filter is displayed by the Enhanced Write Filter status icon on the taskbar system tray (green indicates that the Enhanced Write Filter is enabled, yellow indicates that the Enhanced Write Filter is in transition and will change on the next system start, and red indicates that the Enhanced Write Filter is disabled).

Use these general guidelines when configuring the thin client for permanent changes:

- To avoid flash corruption, it is strongly recommended to flush the Enhanced Write Filter cache immediately following a fresh restart before making permanent modifications to the system.
- Do not flush the cache if the thin client has been used in the current system session.

Caution

The Enhanced 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.

Note

A Terminal Services Client Access License (TSCAL) is always preserved regardless of Enhanced Write Filter state (enabled or disabled).
If you want to have other registry settings preserved regardless of Enhanced Write Filter state, contact Wyse support for help at: http://www.wyse.com.

For more detailed information on using the Enhanced Write Filter, refer to:

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

Changing Passwords with the Enhanced Write Filter

On Microsoft Windows NT-based computers and on Microsoft Windows 2000 or 2003-based computers, machine account passwords are regularly changed with the domain controller for security purposes. By default, on Windows NT-based computers, the machine account password automatically changes every seven days. On Windows 2000 or 2003-based computers, the machine account password automatically changes every 30 days.

The same password process is applicable for a thin client if the thin client is a member of such a domain. With the Enhanced Write Filter enabled, a thin client will successfully make this password change with the domain controller. However, since the Enhanced 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 in Windows NT 4.0 or in Windows 2000 or 2003, by setting the `RefusePasswordChange` registry entry to a value of `1` on all domain controllers in the domain instead of on all workstations. Winterm™ 9 series Thin Clients will still attempt to change their passwords every 30 days, but the change will be rejected by the server.

Note

On Windows NT 4.0 domain controllers, you must change the `RefusePasswordChange` registry entry to a value of `1` on all Backup Domain Controllers (BDCs) in the domain *before* you make the change on the Primary Domain Controller (PDC). Failure to follow this order will cause event ID 5722 to be logged in the event log of the PDC.
If you set the `RefusePasswordChange` registry entry in the Windows 2000 or 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

To disable the machine account password change on the thin client:

1. Start the Registry Editor by clicking **Start | Run**, typing `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, type a value of `1`, and then click **OK**.
6. Quit the Registry Editor.

Disabling the machine account password change in Windows NT 4.0 or in Windows 2000 or 2003

To disable the machine account password change in Windows NT 4.0 or in Windows 2000 or 2003:

1. Start Registry Editor by clicking **Start | Run**, typing `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. Type `RefusePasswordChange` as the registry entry name, and then click **ENTER**.
5. On the Edit menu, click **Modify**.
6. In the Value data text box, type a value of `1`, and then click **OK**.
7. Quit the Registry Editor.

Running Enhanced Write Filter Command Line Options

There are several **Start** | **Run** command lines you can use to control the Enhanced Write Filter.

Note
Command line arguments cannot be combined.

Caution
Administrators should use NT file security to prevent undesired usage of these commands.

Use the following guidelines for the **Start** | **Run** command line option for the Enhanced Write Filter:

- **ewfmgr.exe C:**
  With no arguments - Opens the Enhanced Write Filter Control dialog box. For a description of the dialog box, refer to "Setting the Enhanced Write Filter Controls."
- **ewfmgr.exe C: -commit**
  Commits changes and disables the Enhanced Write Filter until the next system start. The Enhanced Write Filter status icon is yellow until the next system start.
- **ewfmgr.exe C: -disable**
  Flushes the cache and disables the Enhanced Write Filter; the Enhanced Write Filter remains disabled after the system start and must be enabled manually either through the Enhanced Write Filter Control dialog box or through the command line. The Enhanced Write Filter status icon remains red while disabled.
- **ewfmgr.exe C: -enable**
  Enhanced Write Filter enabled after the next system start. After enabling the Enhanced Write Filter you must restart. You do not need to flush the cache first since the Enhanced Write Filter is currently disabled. The Enhanced Write Filter status icon is green when the Enhanced Write Filter is enabled.

Note
The Enhanced Write Filter status icon on the taskbar system tray turns red immediately when the cache flush operation is started, although the flush action can take up to several minutes to complete.

Caution
Do not attempt to flush the cache while the cache is currently being flushed.

If you open an MS-DOS Prompt window (by entering `command` in the Run text box), append "`.exe`" to the `ewfmgr` command:
`ewfmgr.exe C:`, `ewfmgr.exe C: -commit`, `ewfmgr.exe C: -disable`, and `ewfmgr.exe C: -enable`.

Enabling and Disabling the Enhanced Write Filter Using the Desktop Icons

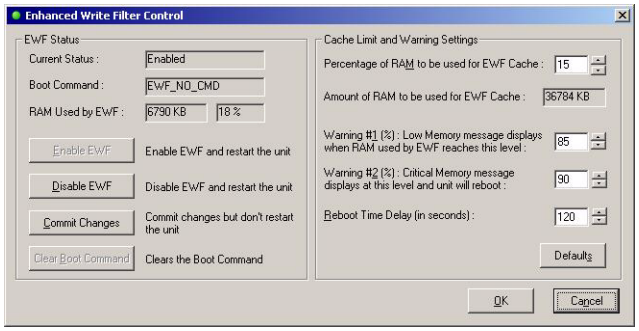
For convenience, the Enhanced Write Filter Enable and Disable icons are present on the Administrator desktop. Use these icons to enable or disable the Enhanced Write Filter.

- **Enhanced Write Filter Enable Icon -** Double-clicking this icon allows you to enable the Enhanced Write Filter using the Enhanced Write Filter Control dialog box. This utility is the equivalent of running the `ewfmgr.exe C: -enable` command line option as described in "Running Enhanced Write Filter Command Line Options." The Enhanced Write Filter is enabled and the system will automatically restart. You do not need to flush the cache first as the Enhanced Write Filter is currently disabled. The Enhanced Write Filter status icon in the taskbar system tray is green when the Enhanced Write Filter is enabled.
- **Enhanced Write Filter Disable Icon -** Double-clicking this icon allows you to disable the Enhanced Write Filter using the Enhanced Write Filter Control dialog box. This utility is the equivalent of running the `ewfmgr.exe C: -disable` command line option as described in "Running Enhanced Write Filter Command Line Options." This flushes the cache and disables the Enhanced Write Filter. The Enhanced Write Filter remains disabled after the system start and can only be enabled using the Enhanced Write Filter Enable icon or through the command line as described in "Running Enhanced Write Filter Command Line Options." The Enhanced Write Filter status icon in the taskbar system tray remains red while the Enhanced Write Filter is disabled.

Setting the Enhanced Write Filter Controls

The Enhanced Write Filter Control dialog box can be opened by double-clicking the EWF icon in the Administrator system tray.

Figure 32 Enhanced Write Filter Control



Use the following guidelines:

- EWF Status area includes:
  - **Current Status** - Shows the current status (Enabled or Disabled) of the Enhanced Write Filter.
  - **Boot Command** - Shows the current status (EWF_ENABLE, EWF_DISABLE, EWF_NO_CMD, or EWF_COMMIT) of the Boot Command.
  - **RAM used by EWF** - Shows the amount of RAM used (in Kilobytes and Percentage) that is currently being used by the Enhanced Write Filter. If **Current Status** is Disabled, RAM Used by EWF is always zero (0).
  - **Enable EWF** - Allows you to commit changes, enable the Enhanced Write Filter and prompt you to restart the thin client (the **Enable EWF** command button is disabled and the **Commit Changes** command button is enabled when the

Enhanced Write Filter is currently enabled). If you do not restart the thin client, the changes made will not be saved until the thin client is restarted.

Note

After the system restarts to enable the Enhanced Write Filter, the Enhanced Write Filter status icon (in the desktop system tray) turns green.

- **Disable EWF** - Allows you to flush the cache, disable the Enhanced Write Filter, and prompt you to restart the thin client (the **Disable EWF** command button and the **Commit Changes** command button are disabled when the Enhanced Write Filter is currently disabled). If you do not restart the thin client, the changes made will not be saved until the thin client is restarted.

Note

After flushing the cache and disabling the Enhanced Write Filter, the Enhanced Write Filter status icon (in the desktop system tray) turns red and the Enhanced Write Filter remains disabled after the system restarts.

- **Commit Changes** - Allows you to run the EWF_COMMIT Boot Command. The system will not restart the thin client and the changes are not committed until an administrator restarts the thin client manually.
- **Clear Boot Command** - Allows you to clear the current Boot command. If there is no Boot Command pending (that is, the Boot Command status is EWF_NO_CMD), then **Clear Boot Command** is disabled.

- Cache Limit and Warning Settings area includes:
  - **Percentage of RAM to be used for EWF Cache** - Shows the percentage of RAM that is to be used as Enhanced Write Filter cache (Default value = 15; Minimum value = 10; Maximum value = 35).
  - **Amount of RAM to be used for EWF Cache** - Shows (in KB) the amount of RAM (in KB) that is to be used as Enhanced Write Filter cache. The value is calculated based on the following formula: Amount of RAM to be used for EWF Cache = Total Available Physical RAM multiplied by the Percentage of RAM to be used.
  - **Warning #1 (%)** - Shows the EWF 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 EWF 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.
  - **Defaults** - Allows you to reset the four Cache Limit and Warning Settings area setting fields to their default values.
  - **OK** - Allows you to close the Enhanced Write Filter Control dialog box and store (in the registry) any changes made to the settings.
  - **Cancel** - Allows you to close the Enhanced Write Filter Control dialog box without storing any changes made to the settings.

Understanding the NetXClean Utility

NetXClean keeps extraneous information from being stored in flash memory. NetXClean is a service that runs in the background and operates only on the flash memory.

NetXClean clean-up is triggered by either a service startup or a user log-off. It 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 the Enhanced Write Filter cache puts junk in flash directories that must be kept clean or allows junk to continue being written to flash after the Enhanced Write Filter cache is flushed (until a restart occurs). 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 Manager" minimize writing to the C drive for factory-installed applications.

Note

For Enhanced Write Filter information (and flushing the cache to permanently save configuration data), refer to "Using the Enhanced Write Filter (EWF)."

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, refer to "Setting Ramdisk Size."

For information about using the Z drive with roaming profiles, refer to "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 Enhanced 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 the Enhanced Write Filter cache and any thin client configuration changes still in cache will be lost.

Note

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

Items that are written to the Enhanced Write Filter cache (or directly to the flash if the Enhanced Write Filter has been flushed) during normal operations include:

- Favorites
- Created connections
- Delete/edit connections

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 Enhanced Write Filter cache during the current system session.
  Since a User log-on account cannot flush the Enhanced 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 cache.

Note

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 the thin client to a Domain

As an administrator you can join a thin client to a domain through the Computer Name Changes dialog box (opened by clicking **Control Panel** | **System** | **Computer Name** | **Change**).

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 Enhanced Write Filter should be disabled so that the domain information can be permanently stored on the thin client. The Enhanced 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 instructions on disabling and enabling the Enhanced Write Filter, refer to "Using the Enhanced Write Filter (EWF)."

To make the domain changes permanent, complete the following:

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

Note

If you use the Enable Desktop Icon to enable the Enhanced 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, refer to "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.

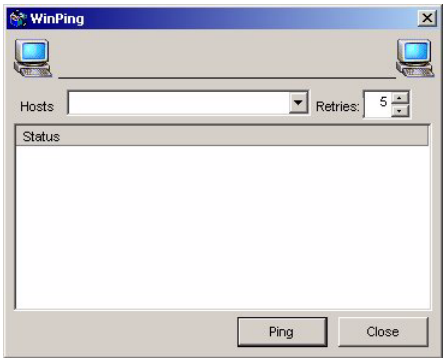
Note

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**, type `WinPing` in the text field, and click **OK**.

Figure 33 WinPing



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 more information on these utilities, go to: http://www.microsoft.com.

Managing Users and Groups with User Manager

The User Manager allows administrators to create new user accounts and configure user profiles. It also allows administrators to create new groups and determine group membership.

By default, a new user is only a member of the Users group and is not locked down. You, as the Administrator, must select the attributes and profile settings for a new user.

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 User and Administrator accounts) to avoid overflowing the Enhanced Write Filter cache.

Creating New User Accounts

New User accounts can be created by using the User Manager. You must be logged-on as an administrator to create new user accounts. You can create user accounts locally or remotely through VNC. However, due to local flash/disk space constraints, the number of additional users should be kept to a minimum.

Caution

Be sure to flush the Enhanced Write Filter cache during the current system session in which a new account is created.

To create a new user:

1. Log-in as an administrator.
2. Click **Start | Settings | Control Panel | Administrative Tools**, and then double-click the **User Manager** icon to open the Local Users and Groups window.
3. Click the **Users** folder to view the contents in the right pane.
4. Click **Action** in the menu bar, and then click **New User** to open the New User dialog box.
5. Enter a user name and password, and then select the attributes you want for the user.
6. Click **Create**.
7. Click **Close**.

Configuring User Profiles

Only an administrator can select the profile settings for a user. For example, new users cannot put themselves into the Administrators group, only an administrator can add a user to the Administrators group.

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.*

To configure a user profile (example of adding a user to the Administrators group):

1. Log-in as an administrator.
2. Click **Start | Settings | Control Panel | Administrative Tools**, and then double-click the **User Manager** icon to open the Local Users and Groups window.
3. In the Local Users and Groups window, select (highlight) the **Users** folder in the left pane.
4. In the right pane of the Local Users and Groups window, double-click the name of the user to open the [user name] Properties dialog box.
5. Click the **Member Of** tab.
6. Click **Add** to open the Select Groups dialog box.
7. Type `Administrators` in the Enter the object names to select field to enable the **Check Names** command button.
8. Click **Check Names**, and then click **OK**.

   The user is now a member of both the Administrators and Users groups.
9. Flush the cache to retain this change.

Creating New Groups

New groups can be created by using the User Manager. You must be logged-on as an administrator to create new groups. You can create groups locally or remotely through VNC. However, due to local flash/disk space constraints, the number of additional groups should be kept to a minimum.

Caution
Be sure to flush the Enhanced Write Filter cache during the current system session in which a new group is created.

To create a new group:

1. Log-in as an administrator.
2. Click **Start | Settings | Control Panel | Administrative Tools**, and then double-click the **User Manager** icon to open the Local Users and Groups window.
3. Click the **Groups** folder to view the contents in the right pane.
4. Click **Action** in the menu bar, and then click **New Group** to open the New Group dialog box.
5. Enter the group name and description.
6. Click **Create**.
7. Click **Close**.

Determining Group Membership

Only an administrator can determine group membership. For example, new users cannot put themselves into the Administrators group, only an administrator can add a user to the Administrators group.

To add a user to the Administrators group:

1. Log-in as an administrator.
2. Click **Start | Settings | Control Panel | Administrative Tools**, and then double-click the **User Manager** icon to open the Local Users and Groups window.
3. In the Local Users and Groups window, select (highlight) the **Groups** folder in the left pane.
4. In the right pane of the Local Users and Groups window, double-click the Administrators group to open the [group name] Properties dialog box.
5. Click **Add** to open the Select Users dialog box.
6. Type the name of the user you want to add in the Enter the object names to select field to enable the **Check Names** command button.
7. Click **Check Names**, and then click **OK**.

   The user is now a member of the Administrators group.
8. Flush the cache to retain this change.

Changing the Computer Name of a Thin Client

Only an administrator can change the computer name of a thin client.

Note

The computer name information and the Terminal Services Client Access License (TSCAL) are preserved regardless of the Enhanced Write Filter state (enabled or disabled). This maintains the specific computer identity information and facilitates the image management of the thin client.

To change the computer name of a thin client:

1. Log-in as an administrator.
2. Click **Start | Settings | Control Panel | System** to open the System Properties window.
3. Click the **Computer Name** tab.
4. Click **Change**.
5. Enter the new computer name in the text field provided.
6. Click **OK**.

This page intentionally blank.

5 System Administration

This chapter contains information and detailed instructions to help you manage your thin client environment.

It discusses:

- "Using Wyse Device Manager (WDM) for Remote Administration and Upgrades"
- "Installing Add-ons"
- "User Instructions on the First Boot Process After Loading a Standard Image (v2.2 or Earlier Only)"
- "Using WinVNC to Shadow a Thin Client"

Using Wyse Device Manager (WDM) for Remote Administration and Upgrades

Wyse Device Manager (formerly known as Rapport) software is a full-featured remote administration tool set available from Wyse Technology. The software accesses your thin client through the factory-installed WDM Agent and Preboot Execution Environment (PXE) client utilities. PXE upgrade services and a Virtual Network Computing (VNC) Viewer are built into Wyse Device Manager software. Wyse Device Manager software allows the thin client administration functions (for example, Shutdown, Reboot, Wake-On-LAN, and firmware upgrades) to be performed without requiring an administrator to visit the individual thin client sites.

For information on installing Wyse Device Manager software and configuring the server environment, refer to the Wyse Device Manager software documentation.

For local custom fields that can be accessed by Wyse Device Manager, refer to "Setting Configuration Strings with Custom Fields."

Note

Ordering information for Wyse Device Manager software is available on the Wyse Web site at: http://www.wyse.com/products/software/rapport/.

Installing Add-ons

To install an add-on, an administrator must use the built-in Wyse Device Manager (WDM) Agent, PXE, and VNC server utilities of the thin client. Disable the Enhanced Write Filter and enable the Enhanced Write Filter as needed to save the changes.

Note

For more information on Wyse Device Manager software refer to the Wyse Web site at: http://www.wyse.com/products/software/rapport/.
Add-ons are available from Wyse for free or for a licensing fee. For information on Wyse Add-ons available, refer to the Wyse Web site at: http://www.wyse.com/products/software/firmware/.

User Instructions on the First Boot Process After Loading a Standard Image (v2.2 or Earlier Only)

If you are running XPe version 2.2 or earlier, you must follow these important instructions when imaging the Winterm™ 9 series Thin Clients with the standard XPe image downloaded from the Wyse Web site.

Note

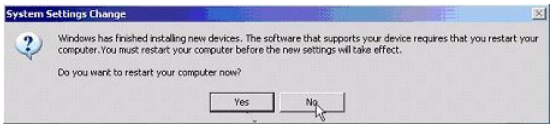
When performing a mass distribution of a custom device image that has been created with Rapport, certain devices will require unique preparation prior to image creation and distribution. Please contact the device manufacturer for more detailed information.

The Winterm™ 9 series Thin Clients automatically run through the configuration steps on first boot after imaging. Failure to follow these instructions may result in system corruption. You must not close the DOS window that is present during the process; the DOS window will close automatically.

Event: The System Settings Change message may appear shortly after the first boot, depending on the specific hardware configuration of the thin client.

- The New Hardware Found message displays in the system tray (lower right hand corner of the screen).
- The System Settings Change message prompts for a system restart.

Figure 34 System Settings Change message



Action: If this System Settings Change message appears, click **No**. Do not interrupt the thin client while it is automatically running through configuration and reboot.

Using WinVNC to Shadow a Thin Client

Administrators Only - WinVNC Server is installed locally on the thin client. It allows a thin client to be operated/monitored (shadowed) from a remote machine on which VNC Viewer is installed. This 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.

VNC 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 | Settings | Control Panel | Administrative Tools | Services**).

Note

If you want to permanently save the state of the service, be sure to flush the Enhanced Write Filter during the current system session.

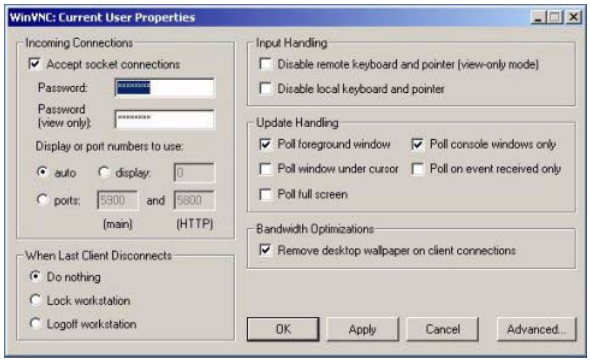
Setting VNC Server Properties

To open the WinVNC: Current User Properties dialog box, click **Start | Programs | WinVNC Current User Properties**, or double-click the **WinVNC** icon in the system tray of the Administrator taskbar. For information on configuring VNC, refer to the VNC documentation at: http://www.realvnc.com.

Caution

The default password in this dialog box is `Wyse`. For security, it is highly recommended that the password be changed (to one known only by the Administrator) immediately upon receipt of the thin client.

Figure 35 WinVNC: Current User Properties



Before a remote machine (on which VNC Viewer is installed) can access a thin client:

- The IP address (or valid DNS name) of the thin client that is to be operated/monitored must be known by the remote administrator/user. This IP address can be obtained from the Details area (Local Area Connection) of the Network Connections dialog box (accessed by clicking **Start** | **Settings** | **Network Connections**, clicking the **Local Area Connection** icon and scrolling down to the Details area in the left pane).

Note

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.

- A password for an administrator to use must be entered into the WinVNC: Current User Properties dialog box.

Setting VNC Viewer Options

VNC Viewer software is included as a component of Wyse Device Manager software and must be installed on the remote (shadowing) machine. An administrator/user of the remote machine must know the IP address/name and the password of a the thin client that is to be operated/monitored.

If a UNIX, Linux, Solaris, or HP-UX machine is to be used to remotely access your thin client, the appropriate VNC Viewer software must be obtained and installed on the remote machine. For information on VNC software, refer to the VNC Web site at: http://www.realvnc.com.

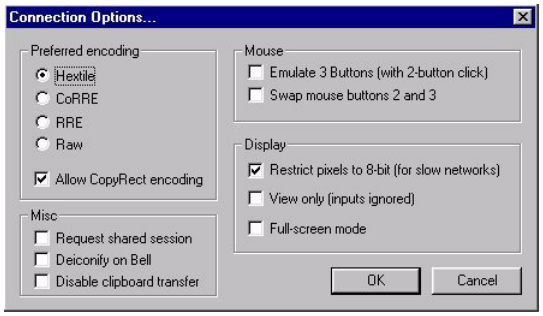
An administrator/user of the remote (shadowing) machine can log-on to a thin client by completing the following:

1. Double-click the **VNC Viewer** icon to open the Connection Details dialog box.

Figure 36 VNC Connection Details

2. (Optional) You can configure advanced VNC connection options using the Connection Options dialog box. For example, if the network is slow, click **Options** to open the Connection Options dialog box, select the **Restrict Pixels to 8-bit** check box in the Display area (reduces color depth for better transmission speed), and then click **OK** to return to the Connection Details dialog box.

Figure 37 VNC Connection Options



Note

The VNC Connection Options dialog box varies for different VNC software releases.

Configure using the following general guidelines:

- **Preferred encoding** options - Normally the VNC Viewer requests CopyRect, Hextile, CoRRE and RRE in that order. The selection alters this behavior by specifying the encoding method to be used before any of the others are tried.
- **Allow CopyRect encoding** - When selected, VNC Viewer informs the VNC Server it can cope with CopyRect encoding.
- **Request shared session** - When you make a connection to a VNC Server, all other existing connections are normally closed. This option requests that they be left open, allowing you to share the desktop with someone already using it.

- **Deiconify on Bell** - Often a beep will sound because you are being notified of something such as e-mail arriving or a compilation finishing. This selection causes a minimized VNC Viewer to be restored when the bell character (escape sequence) is received.
- **Disable clipboard transfer** - Clipboard changes caused by cutting or copying at either the VNC Viewer or the VNC Server are normally transferred to the other end. This option disables clipboard transfers.
- **Emulate 3 Buttons (with 2-button click)** - When selected, users with a two-button mouse can emulate a middle button by clicking both buttons at once.
- **Swap mouse buttons 2 and 3** - Generally selected by left-handed persons.
- **Restrict pixels to 8-bit (for slow networks)** - When selected, reduces color depth for better transmission speed.
- **View only (inputs ignored)** - Select this option if you only want to monitor the desktop of the remote thin client but do not want to operate it using the keyboard and mouse.
- **Full-screen mode** - Causes the connection to start in full-screen mode.

3. In the VNC Server box of the Connection Details dialog box, enter the IP address or valid DNS name of the thin client that is to be operated/monitored followed by a colon and 0. For example:

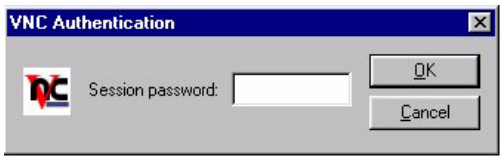
   ```
   snoopy:0
   ```

   or

   ```
   132.237.16.238:0
   ```

4. Click **OK** to open the VNC Authentication dialog box.

Figure 38 VNC Authentication



5. Enter the Session password of the thin client that is to be operated/monitored (this is the password used in the WinVNC: Current User Properties dialog box of the thin client) and click **OK**.

   The thin client that is to be operated/monitored will be displayed in a separate window on the remote machine (on which VNC Viewer is installed). Use the mouse and keyboard on the remote machine (on which VNC Viewer is installed) to operate the thin client that is to be operated/monitored, just as you would if you were operating it locally.

This page intentionally blank.

Figures

Tables

Administrators Guide

Wyse® Winterm™ 9 series, Based on Microsoft® Windows® XP Embedded
Issue: 030107

Written and published by:
Wyse Technology Inc., March 2007

Created using FrameMaker® and Acrobat®