Administrators Guide

Wyse® Thin Clients,
Based on Microsoft® Windows® XP Embedded

Products: R90LE, R90L, X90Le, X90L, X90e, X90, C90LE, V90LE, V90L, S90

Issue: 081309
PN: 883808-01 Rev. L

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

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

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

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

Caution

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

Regulatory Compliance for Thin Clients

Basic EMC and Safety Requirements

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

U.S.A. - FCC Part 15 (class B)

Canada - CAN/CSA-C22 No. 60950

Europe - EN 55022 (class B), EN 61000-3-2 (class A), EN 61000-3-3, EN 90650-1:2000+ALL

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 models with the wireless 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.

Device Power Supply

For use with external power supply included in the shipping carton.

Caution

Replace power adapter with the same or a certified equivalent model supplied by the manufacturer.

Model Cx0 Thin Client, Product C90LE

For use with External Power Supply Model PA-1031-0, or DA-30E12, or certified equivalent model supplied by the manufacturer, rated 12Vdc, 2.5A.

Model H12V Mobile Thin Client, Products X90, X90e

For use with External Power Supply Model 0335A2065 or certified equivalent model supplied by the manufacturer, rated 20Vdc, 3.25A.

Model Rx0L Thin Client, Product R90L

For use with External Power Supply Model 0335A1965 or certified equivalent model supplied by the manufacturer, output rated 19Vdc, 3.42A.

Model Rx0LE Thin Client, Product R90LE

For use with External Power Supply Model 0335A1965 or certified equivalent model supplied by the manufacturer, output rated 19Vdc, 3.42A.

Model SX0 Thin Client, Product S90

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

Model VX0 Thin Client, Products V90L, V90LE

For Use with External Power Supply Model LSE9802A1255, or certified equivalent model supplied by the manufacturer, output rated 12Vdc, 4.58A or minimum 4.0A.

Model Xn0L Mobile Thin Client, Products X90L, X90Le

For use with External Power Supply Model 0335A1965 or certified equivalent model supplied by the manufacturer, rated 19Vdc, 3.42A.

Battery Information

Models Cx0, H12V, Rx0L, Rx0LE, VX0, and Xn0L contain an internal button cell battery replaceable by Wyse or one of our Authorized Service Centers. For service, visit http://www.wyse.com/serviceandsupport/service/service.asp.

Warning

There is a risk of explosion if the battery is replaced by an incorrect type. Always dispose of used batteries according to the instructions accompanying the battery.

Warning

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

Models H12V and Xn0L mobile thin clients contain a user-replaceable battery pack. The battery is designed to work with your Wyse mobile thin client. Do not use a battery from other mobile thin clients or laptop computers with your mobile thin client. Replace the battery only with a compatible battery purchased from Wyse (refer to the Wyse Web site).

Caution

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

Contents

This page intentionally blank.

Summary of Revisions

Wyse Technology Inc. 883808-01 Rev. L

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

Reference	Description
Model Cx0, Product C90LE	New model and product information added to "Device Power Supply" and "Battery Information."

Wyse Technology Inc. 883808-01 Rev. K

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

Reference	Description
Wyse Technical Support and Services	New support and service information added to "Wyse Technical Support."
DHCP Options	New DHCP Options for FTP services added to Table 1 in "Using Dynamic Host Configuration Protocol (DHCP)."
"Using FTP File Servers"	Addition of new section to provide an overview on configuring FTP services.
VMware View Manager	Removal of *Configuring VMware Virtual Desktop Manager (VDM) Session Services*, as this information has been updated and moved to "Using VMware View Manger Services."
"Getting Started"	Addition of new chapter to provide an overview of the basic thin client functions and instructions on setting up the thin client.
Ericom *PowerTerm Session Manager* and *PowerTerm Emulation*	New *PowerTerm Session Manager* and *PowerTerm Emulation* information for Ericom PowerTerm Terminal Emulation added in "Managing Connections with Ericom PowerTerm Terminal Emulation."
VMware View Client	Addition of new VMware View Client connection information to "Using VMware View Client to Connect to a Virtual Desktop."
Configuring printers	Information on configuring printers updated and moved to "Configuring Printers."
"Controlling Sounds and Audio Devices"	Information on managing audio and audio devices updated and moved to "Controlling Sounds and Audio Devices."

Reference	Description
"Accessing Thin Client BIOS Settings"	Addition of new section to provide instructions on accessing the BIOS settings of a thin client.
Updated figures and workflow	All figures and workflow instructions have been updated to include and describe the new user interface.

1 Introduction

Wyse® thin clients running Microsoft® Windows® XP Embedded provide access to applications, files, and network resources made available on machines hosting Citrix™ ICA and Microsoft™ RDP session services. The thin clients contain a full featured Internet Explorer browser and thin client emulation software, Ericom – PowerTerm® TEC. Other locally installed software permits remote administration of the thin clients and provides local maintenance functions. Additional Addons are available that support a wide range of specialty peripherals and features for environments needing a secure Windows user interface with 32-bit Windows compatibility.

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 virtual private network (VPN) server.

About this Guide

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

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

XP Embedded 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 thin clients running Microsoft Windows XP Embedded. It also includes information to help you 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 Started," provides information to help you quickly get started using your thin client. It describes basic thin client functions and provides instructions on setting up the thin client for you and your users.

Chapter 4, "Getting to Know the Extended Features," contains information on the extended features of Wyse thin clients running Microsoft Windows XP Embedded that are not found in standard Windows XP.

Chapter 5, "Administrative Utilities and Settings," provides general information about the utilities and settings available for administrative use.

Chapter 6, "System Administration," contains local and remote system administration information to help you perform the routine tasks needed to maintain your Wyse thin client environment.

Finding the Information You Need in this Guide

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

Wyse Technical Support

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

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

Related Online Resources Available at Wyse

Wyse thin client features can be found in the datasheet for your specific thin client model. Datasheets are available on the Wyse Web site. Go to http://www.wyse.com/products, click the *Wyse Thin Clients* link, click the link for your thin client, and then click the *Download Datasheet* link.

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

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

Wyse Online Community

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

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 thin clients running Microsoft Windows XP Embedded. It also includes information to help you 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 can be used, including an 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 PPPoE is intended for devices which connect to the Internet directly from remote locations. The *New Connection Wizard* (available by clicking **Start | Control Panel**, double-clicking the **Network Connections** icon, and then clicking the **Create a new connection** link) can be used 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:
  - An enterprise dial-up server will directly connect to the enterprise intranet.
  - 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.

- **PPTP VPN** - 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* (available by clicking **Start | Control Panel**, double-clicking the **Network Connections** icon, and then clicking the **Create a new connection** link) can be used 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 How to Configure Your Network Services

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

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

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

Using Dynamic Host Configuration Protocol (DHCP)

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

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

Table 1 DHCP Options

Option	Description	Notes
1	Subnet Mask	Required.
3	Router	Optional but recommended. It is not required unless the thin client must interact with servers on a different subnet.
6	Domain Name Server (DNS)	Optional but recommended.
12	Hostname	Optional.
15	Domain Name	Optional but recommended.
43	Vendor Class Specific Information	Optional.
50	Requested IP	Required.
51	Lease Time	Required.
52	Option Overload	Optional.
53	DHCP Message Type	Required.
54	DHCP Server IP Address	Recommended.
55	Parameter Request List	Sent by thin client.
57	Maximum DHCP Message Size	Optional (always sent by thin client).
58	T1 (renew) Time	Required.
59	T2 (rebind) Time	Required.
61	Client identifier	Always sent.
155	Remote Server IP Address or name	Optional.
156	Logon User Name used for a connection	Optional.
157	Domain name used for a connection	Optional.
158	Logon Password used for a connection	Optional.
159	Command Line for a connection	Optional.
160	Working Directory for a connection	Optional.

Table 1 DHCP Options, Continued

Option	Description	Notes
161	FTP server list	Optional string. Can be either the name or the IP address of the FTP server where the updated thin client image is stored. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6.
162	Root path to the FTP files	Optional string.
163	SNMP Trap server IP Address list	Optional.
164	SNMP Set Community	Optional.
165	RDP startup published applications	Optional.
166	Ericom – PowerTerm® TEC Mode	Optional.
167	Ericom – PowerTerm® TEC ID	Optional.
168	Name of the server for the virtual port	Optional.

Using FTP File Servers

Windows XP Embedded WFR2 includes an FTP Upgrade utility that can be used to upgrade the XP Embedded thin client with Addons which are in Microsoft .msi form. This utility allows you to automatically or manually upgrade a thin client by downloading MSI packages from a specified FTP server. The MSI packages are stored on the FTP server in a directory in the FTP root path (this FTP file server name and root-path directory must be made available to the thin client). To select the upgrade options you want, use the **FTP Addon Installer** dialog box on the thin client as described in "Installing and Upgrading Addons Using the FTP Addon Installer."

Use the following guidelines to set up your servers:

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

Note

Use of DHCP is recommended. However, if a DHCP server is not available, fixed IP addresses (*FTP Path*) can be assigned using the **FTP Addon Installer** dialog box on the thin client.

Using DNS

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

Understanding Session Services

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

Note

Wyse thin clients running Windows XP Embedded also support virtual desktop solutions as described in "Using VMware View Manger Services."

- **General Guidelines** - The Thin-client session services are made available by servers hosting Citrix ICA and Microsoft RDP software products.
- **ICA Guidelines** - Independent Computing Architecture (ICA) is a three-tier, server-based computing technology that separates the logic of an application from its user interface. The ICA client software installed on the thin client allows the user to interact with the application GUI, while all of the application processes are executed on the server. For information on configuring ICA, refer to "Configuring 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.

- **RDP Guidelines** - Remote Desktop Protocol (RDP) is a network protocol that allows a thin client to communicate with the Terminal Service running on Windows 2000/2003/ Windows 2008 Server 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 6.x. For information on configuring RDP, refer to "Configuring RDP Session Services."

Configuring ICA Session Services

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

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

Configuring RDP Session Services

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

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

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

Note

If a Windows 2000, 2003, or 2008 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere accessible on the network. The server will grant a temporary (120-day) license on an individual device basis. Beyond the temporary (120-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).

Using VMware View Manger Services

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

Note

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

View Manager consists of the following major components:

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

Implementing View Client Support on Wyse Thin Clients

There are two ways to implement View Client support on Wyse thin clients running Windows XP Embedded:

- For the Windows XP Embedded WFR2 software release, View Client support is provided as part of the XP Embedded image by including the XP Embedded View Client component.
- For the Windows XP Embedded WFR1 software release, View Client support can be provided using a Wyse Device Manager (WDM) package to push the View Client to the Wyse thin clients.

Note

The View Client requires 9 MB of space in the flash memory of the thin client.

Note

You must install Microsoft Remote Desktop Connection (Terminal Services Client 6.0 or later) on the thin client before pushing the View Client WDM package to a thin client with an XP Embedded SP2 WFR 1 image.

This page intentionally blank.

3 Getting Started

This chapter provides information to help you quickly get started using your thin client. It describes basic thin client functions and provides instructions on setting up the thin client for you and your users.

What Happens When You Turn on Your Thin Client

What you see, initially, when you turn on or reboot a thin client, depends on the method of access to the enterprise intranet and how the network administrator has set up a user account. In addition, with WDM software, a thin client can also be turned on remotely using the Wake-On-LAN feature.

Logging On

After creating users (as described in "Managing Users and Groups with User Manager"), administrators can configure a user account to logon automatically or require manual logon with user credentials (User name, Password, and Domain) as described in "Enabling and Disabling Automatic Logon Using Winlog."

Note

Automatic logon to a User desktop is enabled on the thin client by default. To log on as an administrator, log off the User desktop while holding down the SHIFT key to display the **Log On to Windows** dialog box and use your administrator credentials to log on (default User name and Password are both *Administrator*).

Caution

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

Automatic Logon

Automatic logon to a User desktop is enabled on the thin client by default. If you want to log on as a different user while Auto Logon is enabled, log off the current desktop while holding down the SHIFT key to display the **Log On to Windows** dialog box and use your credentials to logon.

An administrator can log on and use *Winlog* (found in the administrator *Control Panel*) to enable or disable Auto Logon, and to change the default User name, Password, and Domain for a thin client. Only an administrator can change the Auto Logon properties of a thin client.

Note

To save any configurations you make on a thin client to persist after a thin client reboot (for example, Auto Logon properties), be sure to disable the File Based Write Filter *before* your configurations to the thin client, and then enable the File Based Write Filter *after* your configurations as described in "Configuring the Thin Client."

Manual Log-on

When automatic logon is not enabled, the **Log On to Windows** dialog box displays upon thin client startup.

Use the following guidelines:

- For a User account, the factory-default User name and Password are both *User*.
- For an Administrator account, the factory-default User name and Password are both *Administrator*.

Note

Passwords are case sensitive. User names are not case sensitive.

Configuring the Thin Client

While Users can make some configuration modifications to the thin client that are *not* lost when you simply log off and on again (as the same or different user), only administrators can modify thin client configurations to persist after a thin client reboot.

Use the following guidelines:

1. Log on as an administrator. If this is an initial logon to the thin client or you are logging on to the thin client of a User, you must log off the User desktop while holding down the SHIFT key to display the **Log On to Windows** dialog box and use your administrator credentials to logon (default User name and Password are both *Administrator*).

Note

Automatic logon to a User desktop is enabled on the thin client by default. An administrator can use *Winlog* (found in the administrator *Control Panel*) to enable or disable Auto Logon and change the default User name, Password, and Domain for the thin client. For example, as an administrator, you can use *Winlog* to configure *your* thin client to start with the **Log On to Windows** dialog box so that you can log on using your administrator credentials.

2. After logging on to the thin client, disable the File Based Write Filter by double-clicking the **FBWF Disable** icon on the desktop (this will disable the filter and reboot the system).
3. If automatic logon to a User desktop is enabled on the thin client, you must log off the User desktop and log on as an administrator (log off the User desktop while holding down the SHIFT key to display the **Log On to Windows** dialog box and use your administrator credentials to log on).
4. Configure the thin client as you want using the instructions in this guide. For example, you can configure the thin client to automatically upgrade Addons as described in "Installing and Upgrading Addons."
5. After you complete your configurations, you must enable the File Based Write Filter by double-clicking the **FBWF Enable** icon on the desktop (this will enable the filter and reboot the system). Your configurations on the thin client are now saved and they will persist after a thin client reboot.

For information about the File Based Write Filter, refer to "Using the File Based Write Filter (FBWF)."

About the Automatically Launched Utilities

The following utilities are automatically launched:

- **File Based Write Filter** - Upon system start, the File Based Write Filter utility is automatically launched. It provides a secure environment for thin client computing by protecting the thin client from undesired flash memory writes. The active or inactive status of the filter is indicated by the color of the File Based Write Filter status icon in the system tray of the taskbar. For more information about the File Based Write Filter, refer to "Using the File Based Write Filter (FBWF)."

Note

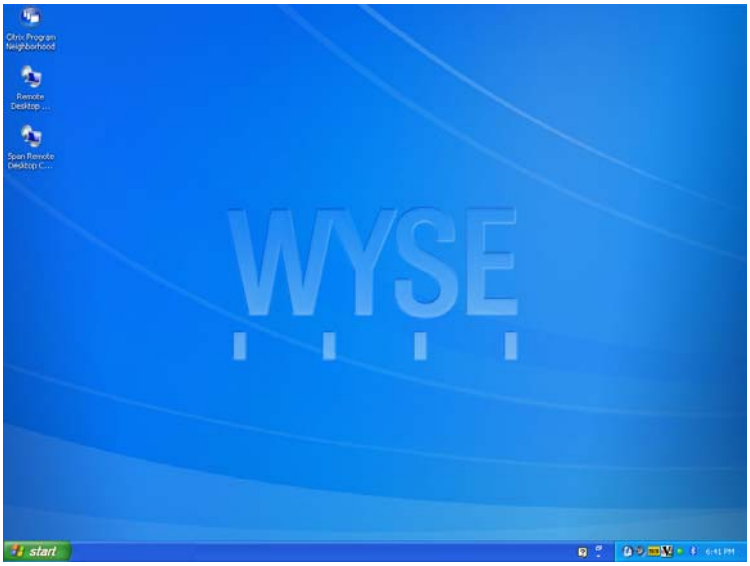
Changes made to the thin client configurations are lost when the thin client is restarted unless the files of the File Based Write Filter cache are flushed/ committed during the current system session. For procedures on flushing, refer to "Configuring the Thin Client," and "Using the File Based Write Filter (FBWF)."

- **NetXClean** - Upon system start, the NetXClean utility is automatically launched. NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. If you want to keep certain profile configurations (for example, printers), be sure to configure NetXClean to refrain from cleaning up any number of explicitly declared profiles. For more information about NetXClean, refer to "Understanding the NetXClean Utility."
- **VNC Server** - Upon successful thin client logon, 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 logon, 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

The default User desktop icons include Citrix Program Neighborhood, and Remote Desktop Connection (standard and Span). The *Start* menu includes Internet Explorer, Control Panel, and Printer and Faxes. The *All Programs* menu includes Citrix Program Neighborhood, Client Information, Internet Explorer, Remote Desktop Connection (standard and Span), Accessories, Startup, and Windows Media Player (if installed, the Ericom – PowerTerm® Terminal Emulation and VMware applications can also be accessed from the *All Programs* menu). The system tray of the taskbar includes Response Time, Volume, S3TrayPlus utility, TightVNC Service, File Based Write Filter status, Bluetooth Devices, and the System time.

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** | **Control Panel**) provides access to a limited set of resources for configuring user preference settings.
- Right-clicking the User desktop does not open a pop-up menu.
- You can copy and paste text between a remote session and the local machine 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 Microsoft documentation (go to http://support.microsoft.com and navigate to the Windows XP Support Center).

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

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

Understanding the Administrator Desktop

The default Administrator desktop icons include Citrix Program Neighborhood, Remote Desktop Connection (standard and Span), File Based Write Filter Disable, and File Based Write Filter Enable.The *Start* menu includes Internet Explorer, My Computer, My Network Places, Control Panel, Printer and Faxes, Search, and Run. The *All Programs* menu includes Citrix Program Neighborhood, Client Information, Internet Explorer, Remote Desktop Connection (standard and Span), Accessories, Startup, Windows Media Player, and WinVNC Current User Properties (if installed, the Ericom – PowerTerm® Terminal Emulation and VMware applications can also be accessed from the *All Programs* menu). The system tray of the taskbar includes Response Time, Volume, S3TrayPlus utility, TightVNC Service, File Based Write Filter status, Bluetooth Devices, and the System time.

Figure 2 Administrator desktop - example

Use the following guidelines:

- The Administrator *Control Panel* (available by clicking **Start** | **Control Panel**) provides access to an extended set of resources for configuring user preference settings and system administration.
- Right-clicking the Administrator desktop opens a pop-up menu.
- You can copy and paste text between a remote session and the local machine 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 Microsoft documentation (go to http://support.microsoft.com and navigate to the Windows XP Support Center).

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

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

Logging Off, Shutting Down, and Restarting

Use the *Shut Down* menu to log off, shut down, restart, or place the thin client in stand by (all 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** window (opened by using CTRL+ALT+DEL key combination).

Note

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

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

- **File Based Write Filter cache** - If you make changes to system configuration settings and want them to persist after a reboot, you must flush the files of the File Based Write Filter cache during the current system session. Otherwise, the new settings will be lost when the thin client is shut down or restarted. The File Based Write Filter cache contents are *not* lost when you simply log off and on again (as the same or different user); that is, you can flush the files of the File Based Write Filter cache after the new logon and still retain the changes. For instructions on flushing, refer to "Setting the File Based Write Filter Controls." For general information about the File Based Write Filter, refer to "Using the File Based Write Filter (FBWF)."

Note

A User cannot flush the files of the File Based Write Filter cache; this is a local or remote administrator function.

- **NetXClean Utility** - NetXClean is a clean-up utility that keeps extraneous information from being stored on the flash memory. Clean-up is triggered automatically on restart, shut-down, or user log-off. If you want to keep certain profile configurations (for example, printers), be sure to configure NetXClean to refrain from cleaning up any number of explicitly declared profiles. For details about NetXClean, 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 in **Start | 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*.

4 Getting to Know the Extended Features

This chapter contains information on the extended features of Wyse thin clients running Microsoft Windows XP Embedded that are not found in standard Windows XP.

Configuring and Using Peripherals

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

Note

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

Accessing the Extended Features of the All Programs Menu

This section provides an overview of the extended features found in the *All Programs* menu (options are available to use by clicking **Start** | **All Programs**).

This section includes information on:

- "Managing Connections with Citrix Program Neighborhood"
- "Viewing Client Information"
- "Browsing the Internet with Internet Explorer"
- "Establishing Remote Desktop Connections"
- "Using the Odyssey Client Manager"
- "Managing Connections with Ericom PowerTerm Terminal Emulation"
- "Synchronizing Thin Client Time with Neutron"
- "Using VMware View Client to Connect to a Virtual Desktop"

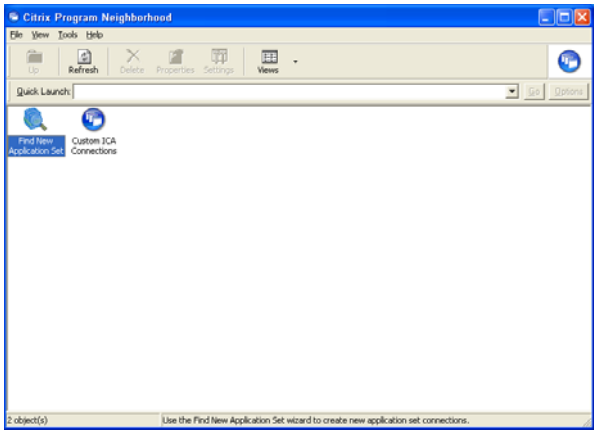
Note

For *WinVNC Current User Properties* information, refer to "Configuring WinVNC Current User Properties."

Managing Connections with Citrix Program Neighborhood

Cirtix Program Neighborhood is available to Users and Administrators. Use the Cirtix Program Neighborhood application (available by clicking **Citrix Program Neighborhood** in the *All Programs* menu or double-clicking the **Citrix Program Neighborhood** desktop icon) 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 3 Citrix Program Neighborhood



Viewing Client Information

Client Information is available to Users and Administrators. Use the **Client Information** dialog box (available by clicking **Client Information** in the *All Programs* menu) to view information about the thin client (the information shown in the dialog box 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, Ethernet MAC Address, Wireless MAC Address, Serial Number, Terminal H/W Rev, CPU Type, CPU Speed in MHz, Flash Configuration, RAM Configuration, and System Partition.

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

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

Browsing the Internet with Internet Explorer

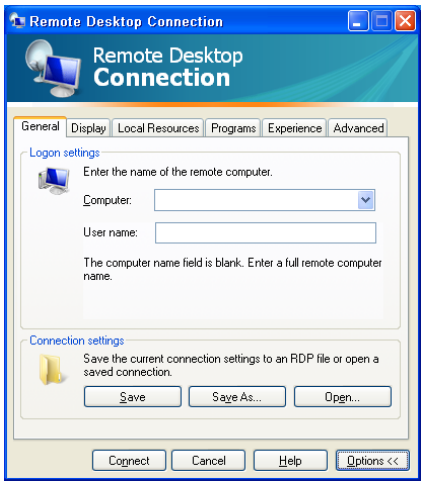
Microsoft Internet Explorer 7 is available to Users and Administrators. The browser (available by clicking **Internet Explorer** in the *All Programs* menu) has Internet option settings that have been preselected at the factory to limit writing to flash memory. These settings prevent exhaustion of the limited amount of flash memory available and should not be modified. If more browser resources are required, you can access another browser through an ICA or RDP session.

Figure 4 Internet Explorer

Establishing Remote Desktop Connections

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

Figure 5 Remote Desktop Connection - expanded view example



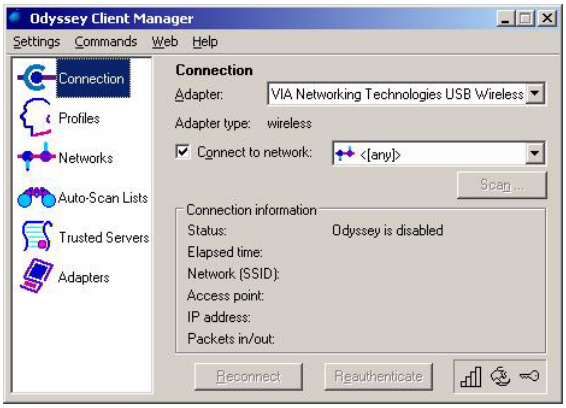
Using the Odyssey Client Manager

If purchased and installed, the Odyssey Client Manager is available to Users and Administrators. Clicking **Start | All Programs | Funk Software | Odyssey Client | Odyssey Client Manager** (or double-clicking the **Odyssey Client Manager** icon in the *Control Panel* or system tray of the Administrator taskbar) 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 6 Odyssey Client Manager

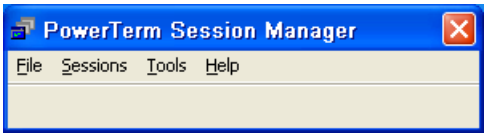


Managing Connections with Ericom PowerTerm Terminal Emulation

PowerTerm Session Manager and *PowerTerm Emulation* are available to Users and Administrators.

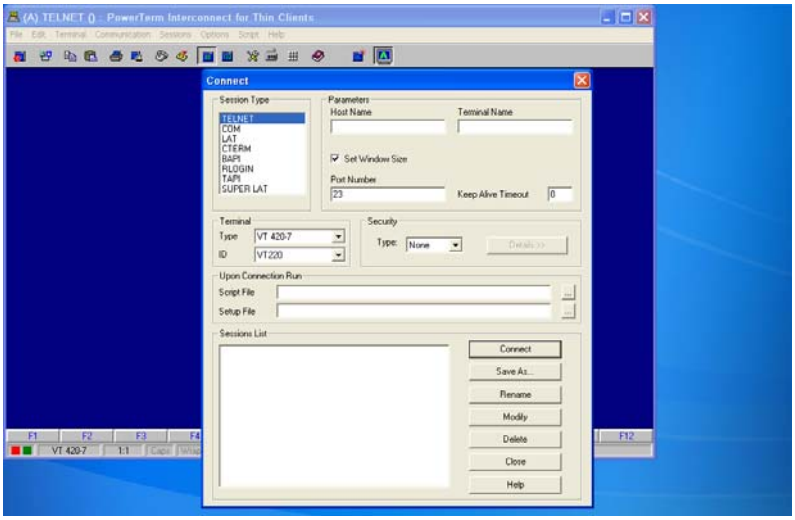
Use the **PowerTerm Session Manager** (available by clicking **Ericom-PowerTerm Terminal Emulation | PowerTerm Session Manager** in the *All Programs* menu) to manage your connections.

Figure 7 Ericom – PowerTerm® Session Manager



Use the **TEC** window and the Connect dialog box (available by clicking **Ericom-PowerTerm Terminal Emulation | PowerTerm Terminal Emulation** in the *All Programs* menu) to configure your connection information. For complete instructions on installing and using Ericom – PowerTerm® TEC, refer to the Ericom – PowerTerm® TEC documentation supplied separately.

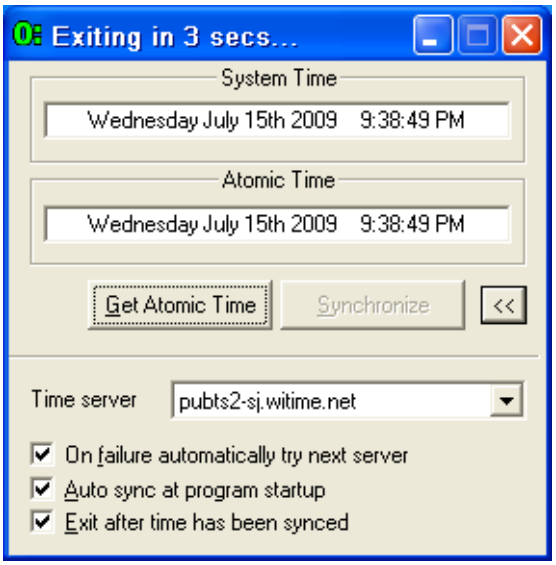
Figure 8 Ericom – PowerTerm® TEC and Connect



Synchronizing Thin Client Time with Neutron

Neutron time synchronization is available to Users and Administrators. Use the **Neutron** dialog box (available by clicking **Startup | Neutron** in the *All Programs* menu—click **>>** to open the extended menu of the dialog box) to view the current System Time and Atomic Time, to synchronize the System Time with the Atomic Time (click **Synchronize**), and to retrieve the current Atomic Time from a time server (click **Get Atomic Time**).

Figure 9 Neutron - extended view



Using VMware View Client to Connect to a Virtual Desktop

VMware View Client is available to Users and Administrators. Use the **VMware View Client** dialog box (available by clicking **VMware | VMware View Client** in the *All Programs* menu—click **>>** to open the extended menu of the dialog box) to connect to a virtual desktop.

Figure 10 VMware View Client - extended view

Use the following guidelines:

1. In the *Connection Server* drop-down menu, enter the host name or IP address of a View Connection Server and click **Connect**.
2. Enter the name and password for an entitled user, select the domain, and click **Login**.
3. Select a desktop from the list provided and click **Connect**. VMware View Client attempts to connect to the specified desktop. After you are connected, the client window appears.

Note

Information on using VMware View Client can be found on the VMware Web site at: http://www.vmware.com.

Accessing the Extended Features of the Administrator Control Panel

This section provides an overview of the extended features found in the Administrator *Control Panel* (options are available to use by clicking **Start** | **Control Panel**).

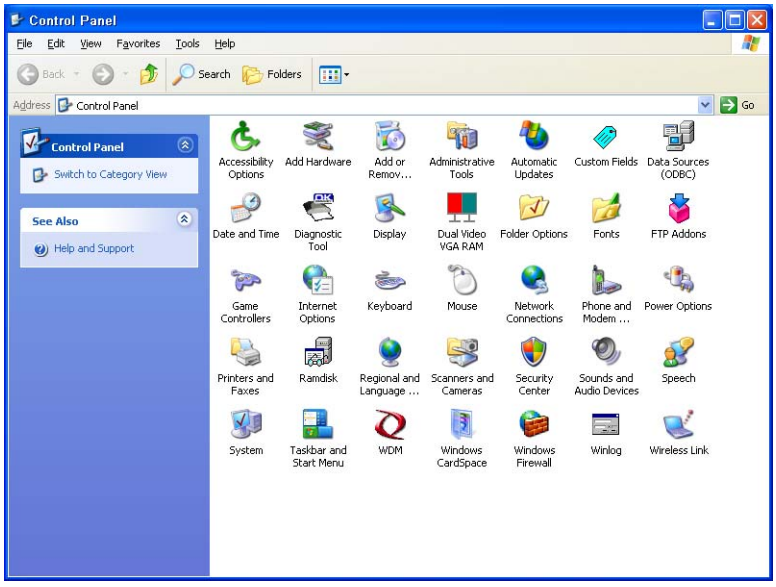
This section includes information on:

- "Accessing and Using the Administrative Tools"
- "Setting Configuration Strings with Custom Fields"
- "Configuring Dual Monitor Display"
- "Configuring Dual Video VGA RAM"
- "Configuring Touchscreens"
- "Configuring Printers"
- "Setting Ramdisk Size"
- "Selecting Regional and Language Options"
- "Controlling Sounds and Audio Devices"
- "Configuring WDM Properties"
- "Enabling and Disabling Automatic Logon Using Winlog."
- "Configuring Wireless Local Area Network (LAN) Settings"

Note

For *FTP Addon Installer* information, refer to "Installing and Upgrading Addons Using the FTP Addon Installer."

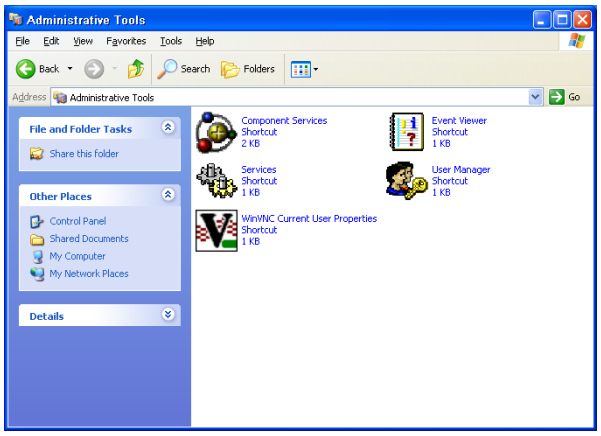
Figure 11 Administrator Control Panel



Accessing and Using the Administrative Tools

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

Figure 12 Administrative Tools



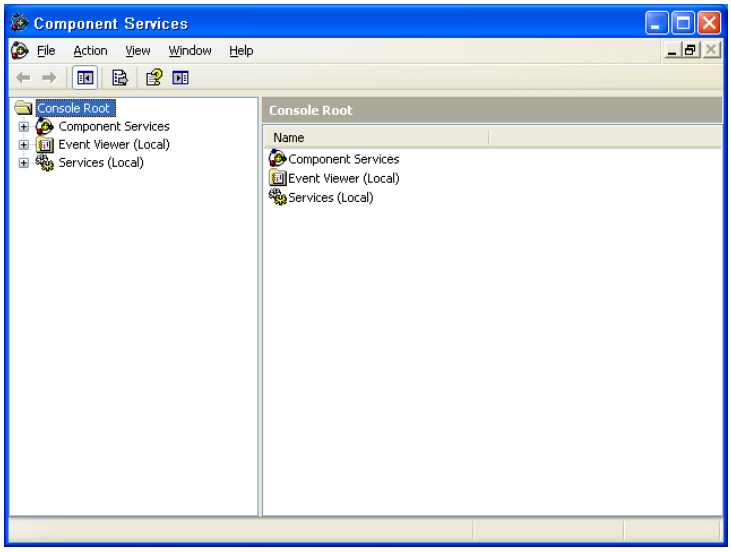
Administrative Tools are available for:

- "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.

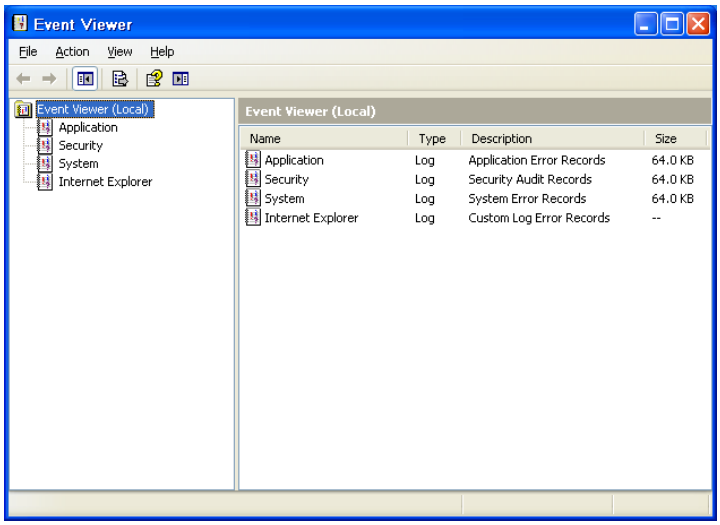
Figure 13 Component Services



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.

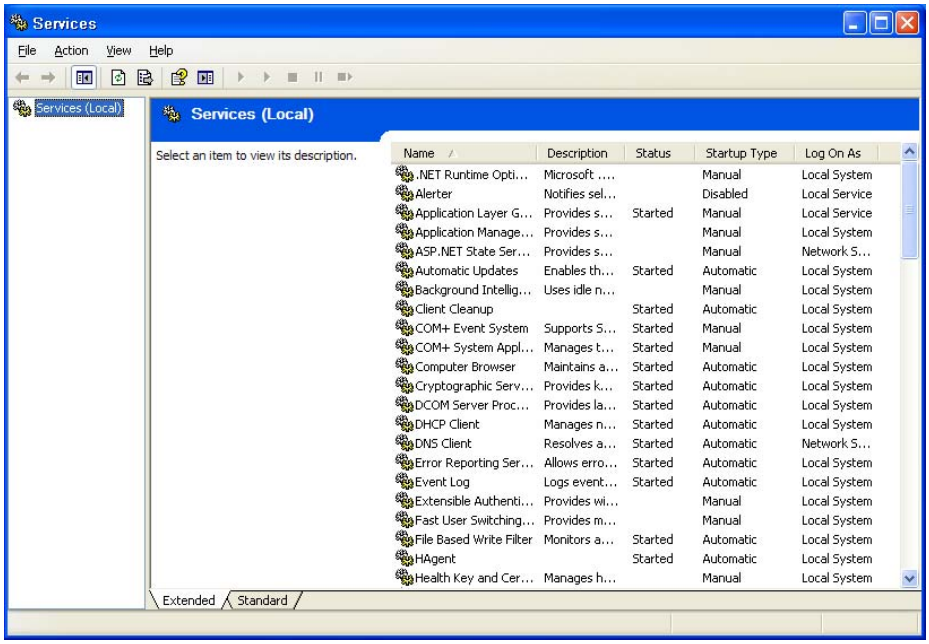
Figure 14 Event Viewer



Managing Services

Double-clicking the **Services** icon opens the **Services** window. This 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." VNC Server and Client Clean-up (NetXClean) can be stopped using the Task Manager.

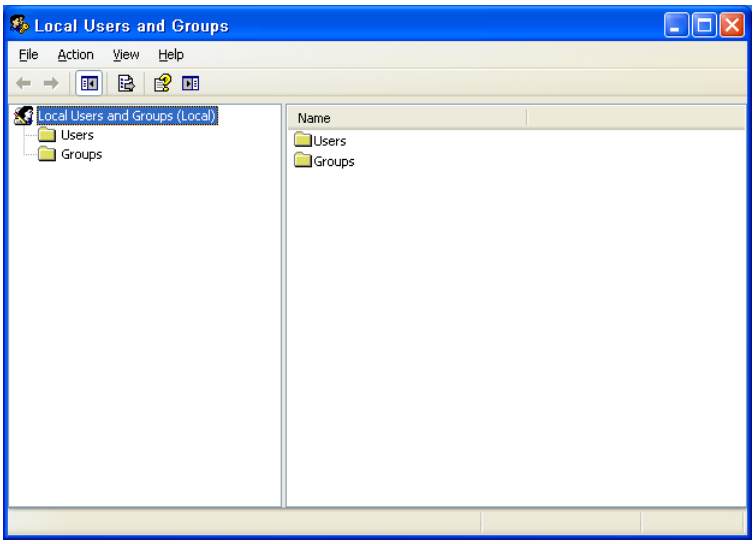
Figure 15 Services



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."

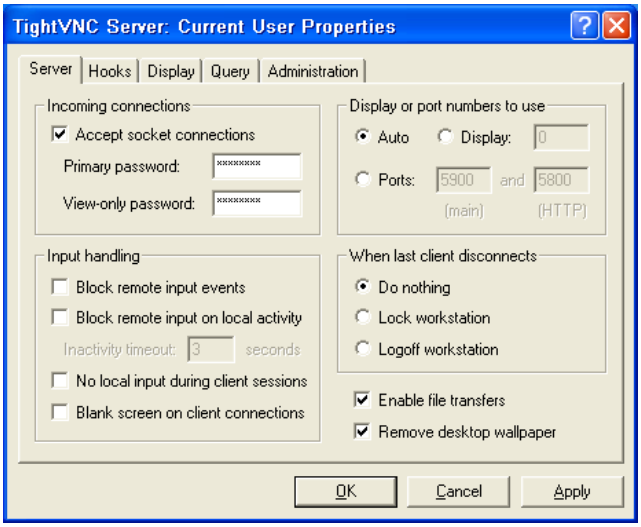
Figure 16 Local Users and Groups



Configuring WinVNC Current User Properties

Double-clicking the **WinVNC Current User Properties** icon (or clicking **WinVNC Current User Properties** in the *All Programs* menu or double-clicking the icon in the 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.

Figure 17 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

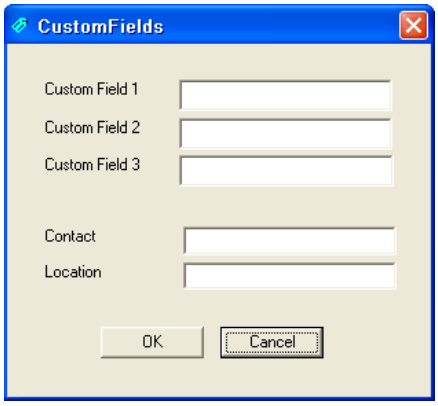
Double-clicking the **Custom Fields** icon in the *Control Panel* opens the **Custom Fields** dialog box. Use this dialog box to enter configuration strings for use by WDM software. The configuration strings can contain information about the location, user, administrator, and so on.

Clicking **OK** transfers the custom field information you enter in the dialog box to the Windows registry. The information is then available to the WDM Client Manager. To permanently save the information, flush the files of the File Based Write Filter cache during the system session in which the registry entries are made or changed (see "Configuring the Thin Client").

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

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

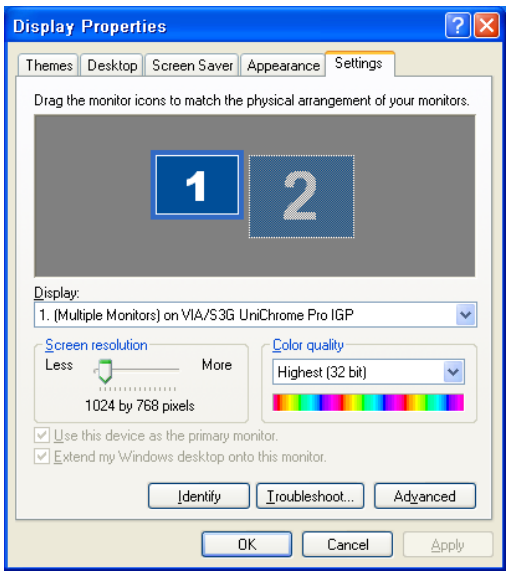
Figure 18 Custom Fields



Configuring Dual Monitor Display

(*For Dual-Monitor Capable Thin Clients Only*) You can use the *Settings* tab of the **Display Properties** dialog box (double-click the **Display** icon in the *Control Panel*, and then click the **Settings** tab) to configure the dual monitor settings as described in the Microsoft documentation at: http://www.microsoft.com. For Wyse Multi-Display Support and dual monitor support information, visit the Wyse Knowledge Base on the Wyse Web site.

Figure 19 Display Properties



Note

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

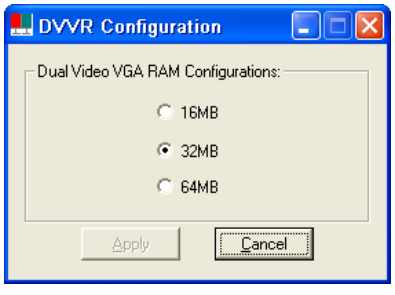
Configuring Dual Video VGA RAM

(*For Dual-Monitor Capable Thin Clients Only*) If the Dual Video VGA RAM option is installed on the thin client, double-clicking the **Dual Video VGA RAM** icon in the *Control Panel* opens the **DVVR Configuration** dialog box. Use this dialog box to configure the Dual Video VGA RAM size.

Note

It is recommended to reboot the thin client after configuring.

Figure 20 Dual Video VGA RAM



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.

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 files of the File Based Write Filter cache to save the installation. For procedures on flushing, refer to "Using the File Based Write Filter (FBWF)."

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, 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** | **Printers and Faxes** to open the **Printers and Faxes** dialog box.
3. Click **Add a printer** to open the *Add Printer Wizard*, and then click **Next**.
4. Select **Local printer attached to this computer**, *clear* the **Automatically detect and install my Plug and Play printer** check box, and then click **Next**.
5. Select **Use the following port**, select the port from the list, and then click **Next**.
6. Select the manufacturer and model of the printer and click **Next**.
7. Enter a name for the printer and click **Next**.
8. Select **Do not share this printer** and click **Next**.
9. Select whether or not to print a test page and click **Next**.
10. Click **Finish** (the installation will complete and a test page will print if this option was selected).

Setting Ramdisk Size

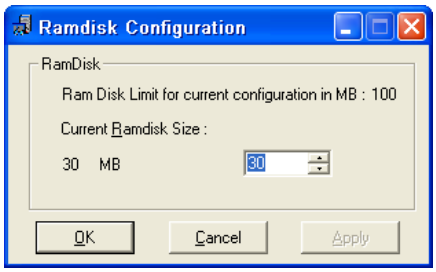
Ramdisk is volatile memory space used for temporary data storage. It is the Z drive shown in the **My Computer** window. It can also be used for temporary storage of other data according to administrator discretion (see "Saving Files and Using Local Drives").

The following items are stored on Ramdisk:

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

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 files of the File Based Write Filter cache have been flushed during the current system session *before* restarting the system (see "Configuring the Thin Client").

Figure 21 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).

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 | 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).

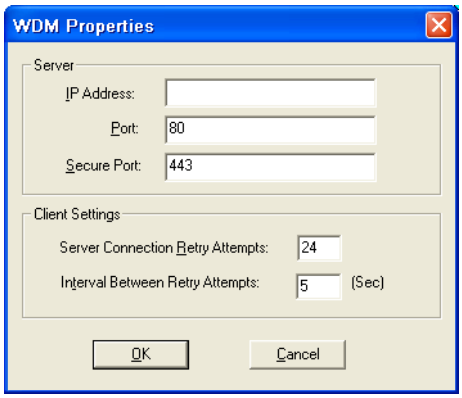
Controlling Sounds and Audio Devices

Double-clicking the **Sounds and Audio Devices** icon opens the **Sounds and Audio Devices** dialog box. Use this dialog box to manage your audio and audio devices. Volume can also be adjusted using the **Volume** icon in the system tray of the taskbar. Single-click the **Volume** icon to open the master volume control, or double-click the **Volume** icon to open the Volume Control application dialog box. Powered speakers are recommended.

Configuring WDM Properties

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

Figure 22 WDM Properties



Use the following guidelines:

1. Enter the IP address or hostname of the WDM Server.
2. Enter the port to use.
3. Click **OK**.

For information on WDM software, refer to "Using Wyse Device Manager Software for Remote Administration."

Enabling and Disabling Automatic Logon Using Winlog

Automatic logon to a User desktop is enabled on the thin client by default. Double-clicking the **Winlog** icon in the *Control Panel* opens the **Winlog** dialog box. Use this dialog box to enable or disable Auto Logon, and to change the default User name, Password, and Domain for a thin client.

Note

To save any configurations you make on a thin client to persist after a thin client reboot (for example, Auto Logon properties), be sure to disable the File Based Write Filter *before* your configurations to the thin client, and then enable the File Based Write Filter *after* your configurations as described in "Configuring the Thin Client." For information about the File Based Write Filter, refer to "Using the File Based Write Filter (FBWF)."

Figure 23 Winlog

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 *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 only available in the Administrator *Control Panel* and is used specifically for an 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 using the **Network Connections** dialog box (**Start | Control Panel | Network Connections**) or the *Device Manager* (**Start | Control Panel | System | Hardware | Device Manager**).

For information on configuring the optional Internal Wireless feature installed on some Wyse 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). Supported authentication modes are Open, Shared, WPA, and WPA2.

Using Wireless Zero Configuration (WZC)

Note

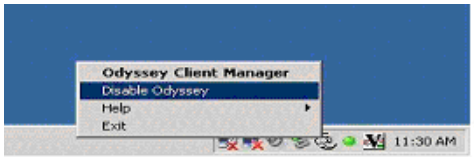
Before using these procedures, be sure you have imported any user certificates and computer certificates (of a server) you will need into the thin client.

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.".

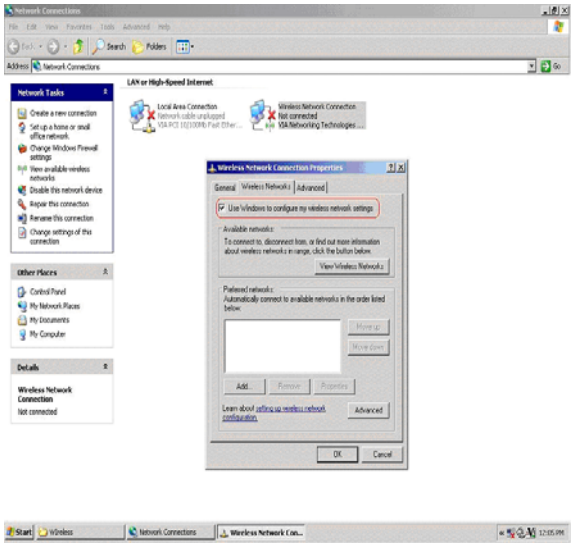
   To disable the Odyssey Client Manager, right-click on the Odyssey icon in the system tray of the Administrator taskbar and click **Disable Odyssey**.

Figure 24 Disable Odyssey



2. Open the **Network Connections** dialog box (**Start | Control Panel | 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 25 Wireless Network Connection Properties

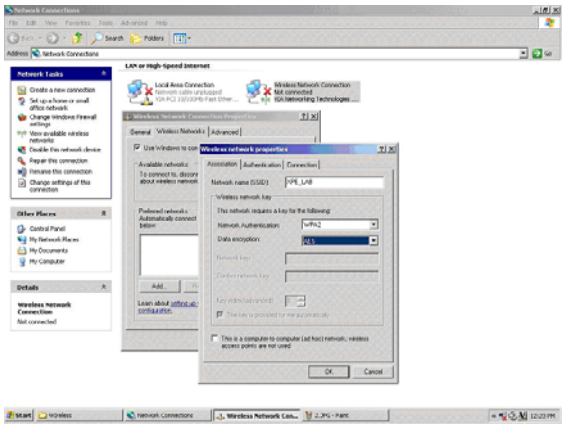


4. Select the **Wireless Network** tab and then select the **Use Windows to configure my wireless network settings** check box
5. Click **OK** and continue with "Configuring Wireless Thin Clients for EAP-TLS Authentication (Smart Card or other Certificate)" or "Configuring Wireless Thin Clients for PEAP-MS-CHAP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

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

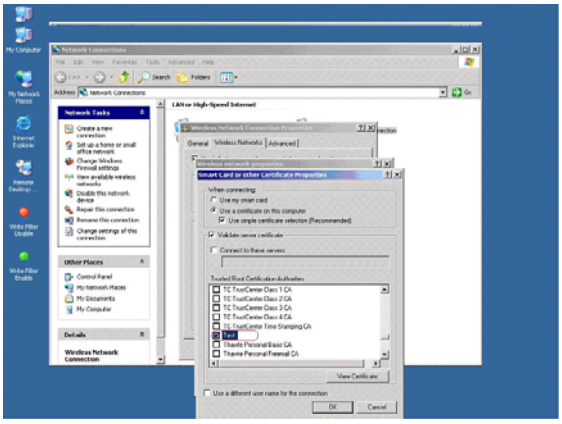
1. Right-click **Wireless Network Connection** and select **Properties** to open the **Wireless Network Connection Properties** dialog box.
2. Select the **Wireless Network** tab and then click **Add** to open the **Wireless Network Properties** dialog box.

Figure 26 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 27 Smart Card or other Certificate Properties - EAP-TLS

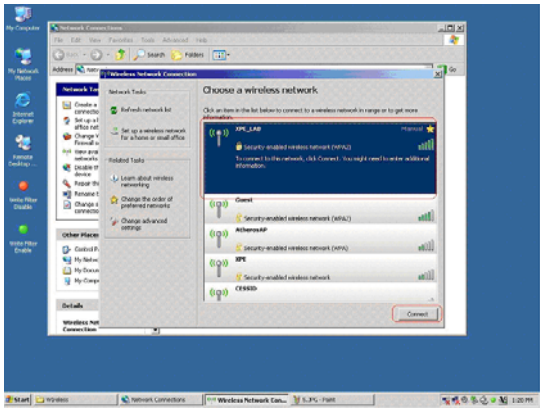


11. Select the **Use a certificate on this computer** option (to use a registry-based user certificate) and select the **Use simple certificate selection** check box.
12. Depending on whether or not you want to validate the computer certificate of the IAS server, select or clear the **Validate server 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, use the following guidelines:

1. Open the **Network Connections** dialog box (**Start | Control Panel | 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 28 Wireless Network Connection - EAP-TLS



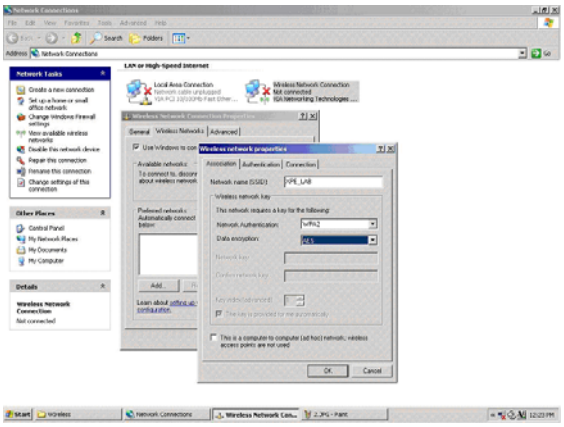
3. Select the connection you created in step 4 (the Network name (SSID)), and then click **Connect**.

A wireless connection should now be established.

Configuring Wireless Thin Clients for PEAP-MS-CHAP v2

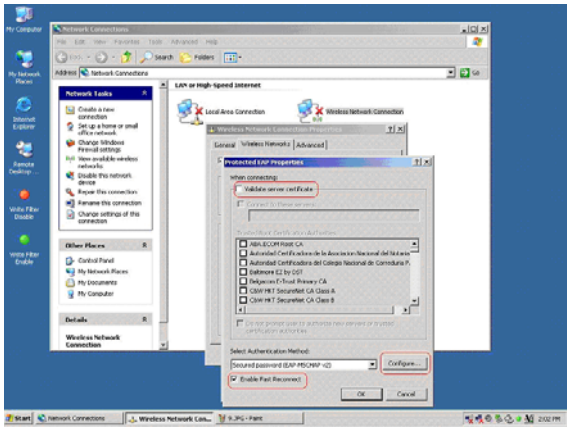
1. Right-click **Wireless Network Connection** and select **Properties** to open the **Wireless Network Connection Properties** dialog box.
2. Select the **Wireless Network** tab and then click **Add** to open the **Wireless Network Properties** dialog box.

Figure 29 Wireless Network Properties PEAP-MS-CHAP v2



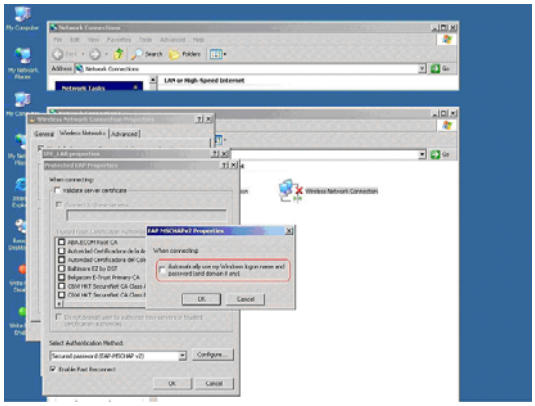
3. Click the **Association** tab.
4. Enter the Network name (SSID).
5. Select the **WPA2** option for Network Authentication.
6. Select the **AES** option for Data encryption.
7. Click the **Authentication** tab.
8. Select the **Enable IEEE 802.1x authentication for this network** check box.
9. Select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

Figure 30 Protected EAP Properties - PEAP-MS-CHAP v2



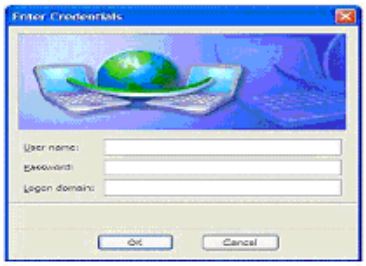
11. Clear the **Validate server certificate** check box.
12. Select the **Enable Fast Reconnect** check box.
13. Click **Configure** to open the **EAP MSCHAPv2 Properties** dialog box.

Figure 31 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.** You will be prompted to enter your credentials.
16. Click on the *Wireless Network Connection* pop-up message that appears on the system tray to open the **Enter Credentials** dialog box.
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 32 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.

Preserving Wireless Connections

Windows XP Embedded WFR2 includes a tool called *Regpersistence.exe* which is designed to configure wireless access in Write Filter Enable mode. When you configure wireless access with this utility, the authentication credentials persist across reboots, eliminating the need to re-authenticate each time the client systems are restarted. The utility preserves the service set identifier (SSID) for wireless connections across workgroup modes and domains. When Windows XP Embedded clients restart, they are automatically connected to the desired wireless access point.

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

- Open mode with WEP

Note

This authentication mode requires the network key to be entered while the client is connected to the wireless network. Windows XP Embedded clients are automatically connected to the wireless network after reboot.

- Shared mode with WEP
- WPA authentication with AES and TKIP
- WPA-PSK with AES and TKIP data encryption.
- WPA2 with AES and TKIP data encryption
- WPA2-PSK with AES and TKIP data encryption.
- PEAP authentication process

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

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

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

Note

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

Using PEAP Fast Reconnect

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

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

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

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

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

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

Using the Regpersistence Tool to Configure PEAP Wireless Connections

Use the following guidelines:

1. Image the Windows XP Embedded Client.
2. With the Write Filter enabled, configure a wireless connection.
3. When users log in, they are not prompted for wireless credentials.

Note

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

This page intentionally blank.

5 Administrative Utilities and Settings

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

It includes information on:

- “Using the File Based Write Filter (FBWF)”
- "Understanding the NetXClean Utility"
- "Saving Files and Using Local Drives"
- "Mapping Network Drives"
- "Participating in Domains"
- "Using the WinPing Diagnostic Utility"
- "Using the Net and Tracert Utilities"
- "Managing Users and Groups with User Manager"
- "Changing the Computer Name of a Thin Client"

Using the File Based Write Filter (FBWF)

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

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

Caution

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

Note

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

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

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

Changing Passwords with the File Based Write Filter

On Microsoft Windows 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 File Based Write Filter enabled, a thin client will successfully make this password change with the domain controller. However, since the File Based Write Filter is enabled, the next time the thin client is booted it will not retain the new password. In such cases, you can use the following options:

- Disable the machine account password change on the thin client by setting the `DisablePasswordChange` registry entry to a value of `1`.
- Disable the machine account password change 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. Wyse 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**, entering `regedit` in the **Open** text box, and then clicking **OK**.
2. Locate and click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
3. In the right pane, click the `DisablePasswordChange` entry.
4. On the *Edit* menu, click **Modify**.
5. In the **Value data** text box, enter a value of `1`, and then click **OK**.
6. Quit the Registry Editor.

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

Running File Based Write Filter Command Line Options

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

Caution

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

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

Note

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

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

Caution

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

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

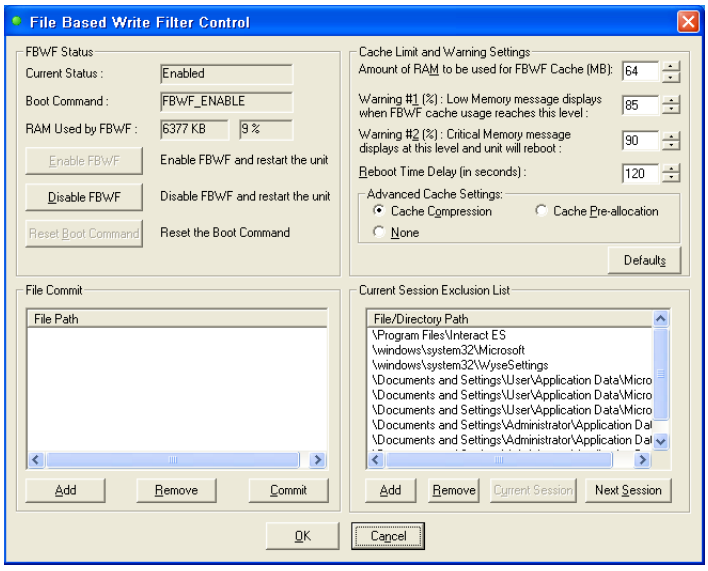
For convenience, the File Based Write Filter Enable and Disable icons are present on the Administrator desktop. Use these icons to enable or disable the File Based Write Filter.

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

Setting the File Based Write Filter Controls

The **File Based Write Filter Control** dialog box can be opened by double-clicking the FBWF icon in the system tray of the Administrator taskbar.

Figure 33 File Based Write Filter Control



Use the following guidelines:

- *FBWF Status* area includes:
  - **Current Status** - Shows the current status (Enabled or Disabled) of the File Based Write Filter.
  - **Boot Command** - Shows the current status of the Boot Command (FBWF_ENABLE means that the FBWF is enabled for the next session; and FBWF_DISABLE means that the FBWF is disabled for the next session).

  - **RAM used by FBWF** - Shows the amount of RAM used (in Kilobytes and Percentage) that is currently being used by the File Based Write Filter. If **Current Status** is Disabled, RAM Used by FBWF is always zero (0).
  - **Enable FBWF** - Allows you to enable the File Based Write Filter and prompts you to restart the thin client. If you do not restart the thin client, the changes made will not be saved until the thin client is restarted. After the system restarts to enable the File Based Write Filter, the File Based Write Filter status icon (in the desktop system tray) turns green.
  - **Disable FBWF** - Allows you to disable the File Based Write Filter and prompt you to restart the thin client. If you do not restart the thin client, the changes made will not be saved until the thin client is restarted. After disabling the File Based Write Filter, the File Based Write Filter status icon (in the desktop system tray) turns red and the File Based Write Filter remains disabled after the system restarts.
  - **Reset Boot Command** - Allows you to reset the current *Boot Command*. If there is no Boot Command pending, then **Reset Boot Command** is disabled.
- *Cache Limit and Warning Settings* area includes:
  - **Amount of RAM to be used for FBWF Cache** - Shows (in MB) the amount of RAM (in MB) that is to be used as File Based Write Filter cache. The value is calculated based on the following formula: Amount of RAM to be used for FBWF Cache = Total Available Physical RAM multiplied by the Percentage of RAM to be used.
  - **Warning #1 (%)** - Shows the FBWF cache percentage value at which a Low Memory warning message will be displayed to the user (Default value = 85, Minimum value = 50, Maximum value = 90).
  - **Warning #2 (%)** - Shows the FBWF cache percentage value at which a Critical Memory warning message will be displayed to the user, along with another message display counting down the number of seconds before automatic rebooting will occur (Default value = 95, Minimum value = 55, Maximum value = 95).
  - **Reboot Time Delay (in seconds)** - Shows the number of seconds that will lapse before system reboot in the **Warning #2 (%)** case of cache overflow.
- *Advanced Cache Settings* area includes options to allow you to improve the effectiveness of cache memory (**Cache Compression**, **Cache Pre-allocation**, or **None**)
- **Defaults** - Allows you to reset the *Cache Limit and Warning Settings* area and the *Advanced Cache Settings* area to their default values.
- *File Commit* area includes:
  - **File Path** - Allows you to add, remove, and commit files to the underlying media (delete a file path from the list if the file is not to be committed). The system will not restart the thin client. The changes are committed immediately.
- *Current Session Exclusion List* area includes:
  - **File/Directory Path** - Allows you to add and remove a file or directory to or from the exclusion list for the next session (retrieves the list of files or directories that are write through in the current session; the title of the pane is shown as *Current Session Exclusion List*) or the Next Session (retrieves the list of files or directories that are write through for the next session; the title of the pane is shown as *Next Session Exclusion List*). The system will not restart the thin client and the changes are not committed until an administrator restarts the thin client manually.

Understanding the NetXClean Utility

NetXClean keeps extraneous information from being stored in flash memory. NetXClean is a service that runs in the background. 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 some files in the File Based Write Filter cache puts junk in flash directories that must be kept clean). The NetXClean utility is particularly important when multiple users have log-on rights to a thin client, as memory space can be quickly used by locally stored profiles and temporary caching of information.

NetXClean TweakUI functions includes clearing:

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

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

Caution

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

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

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

NetXClean will not delete the following profiles:

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

Saving Files and Using Local Drives

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

Saving Files

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

Caution

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

Note

For File Based Write Filter information, refer to "Using the File Based Write Filter (FBWF)."

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

- Favorites
- Created connections
- Delete/edit connections

Mapping Network Drives

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

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

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 a Domain

As an administrator you can join a thin client to a domain through the **Computer Name Changes** dialog box (**Start | 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 File Based Write Filter should be disabled so that the domain information can be permanently stored on the thin client. The File Based Write Filter should remain disabled through the next boot as information is written to the thin client on the boot after joining the domain. This is especially important when joining an Active Directory domain. For instructions on disabling and enabling the File Based Write Filter, refer to "Using the File Based Write Filter (FBWF)."

To make the domain changes permanent, complete the following:

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

Note

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

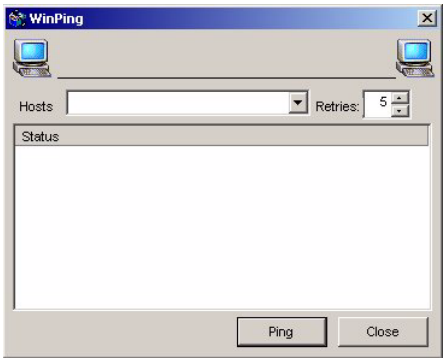
Note

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**, enter `WinPing` in the text box, and click **OK**.

Figure 34 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 example, to determine the route taken by packets across an IP network). For more information on these utilities, go to: http://www.microsoft.com.

Managing Users and Groups with User 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. As the Administrator, you 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 File Based Write Filter cache.

Creating New User Accounts

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

Caution

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

Use the following guidelines:

1. Log-in as an administrator and open the *User Manager* (**Start | Control Panel | Administrative Tools | User Manager**).
2. Click the **Users** folder, click **Action** in the menu bar, and then select **New User** to open the **New User** dialog box.
3. Enter the user information and credentials, select the attributes you want for the user, and then click **Create** (you can continue to create as many users as you want).
4. After creating the users you want, click **Close**. The users will appear in the list of users pane.

Configuring User Profiles

Only administrators can select the profile settings for a user.

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.*

Use the following guidelines (example of adding a user to the Administrator group):

Caution

Be sure to flush the files of the File Based Write Filter cache during the current system session in which an account is modified.

1. Log-in as an administrator and open the *User Manager* (**Start | Control Panel | Administrative Tools | User Manager**).
2. Click the **Users** folder, double-click on a user to open the **User Properties** dialog box, and then click the **Member of** tab.
3. Click **Add** to open the **Select Groups** dialog box.
4. Enter **Administrators** in the **Enter the object names to select** box to enable the **Check Names** command button.
5. Click **Check Names**, and then click **OK**. The user is now a member of both the Administrator and User groups.

Creating New Groups

Only administrators can create new 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 files of the File Based Write Filter cache during the current system session in which a new account is created.

Use the following guidelines:

1. Log-in as an administrator and open the *User Manager* (**Start | Control Panel | Administrative Tools | User Manager**).
2. Click the **Groups** folder, click **Action** in the menu bar, and then select **New Group** to open the **New Group** dialog box.
3. Enter the group name and description, and then click **Create** (you can continue to create as many groups as you want).
4. After creating the groups you want, click **Close**. The groups will appear in the list of groups pane.

Determining Group Membership

Use the following guidelines (example of adding a user to the Administrator group):

Caution

Be sure to flush the files of the File Based Write Filter cache during the current system session in which an account is modified.

1. Log-in as an administrator and open the *User Manager* (**Start | Control Panel | Administrative Tools | User Manager**).
2. Click the **Groups** folder, double-click on **Administrators** to open the **Administrators Properties** dialog box, and then click **Add** to open the **Select Users** dialog box.
3. Enter the user name in the **Enter the object names to select** box to enable the **Check Names** command button.
4. Click **Check Names**, and then click **OK**. The user is now a member of both the User and Administrator groups.

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 File Based Write Filter state (enabled or disabled). This maintains the specific computer identity information and facilitates the image management of the thin client.

Use the following guidelines:

1. Log-in as an administrator and open the **System Properties** dialog box (**Start | Control Panel | System**).
2. Click the **Computer Name** tab.
3. Click **Change**.
4. Enter the new computer name and click **OK**.

This page intentionally blank.

6 System Administration

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

It includes:

- "Using Wyse Device Manager Software for Remote Administration"
- "Accessing Thin Client BIOS Settings"
- "Installing and Upgrading Addons"
- "Using Windows Server Update Services (WSUS) on a Thin Client"
- "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 Software for Remote Administration

Wyse Device Manager™ (WDM) servers provide network management services to the thin client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot, rename, automatic device check-in support, Wake-On-LAN, change device properties, and so on).

Note

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

For information on setting WDM properties, refer to "Configuring WDM Properties."

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

Accessing Thin Client BIOS Settings

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

Installing and Upgrading Addons

To install or upgrade Addons, it is recommended that you use WDM (the thin client has a built-in WDM Agent for use as described in "Configuring WDM Properties").

Note

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

Installing and Upgrading Addons Using the FTP Addon Installer

While WDM is recommended for easy remote network management services to your thin client, you can use the **FTP Addon Installer** dialog box (only available to administrators) to install and upgrade Addons which are in Microsoft .msi form. The *FTP Addons* utility allows you to manually or automatically install/upgrade Addons on a thin client by downloading MSI packages from a specified FTP server.

Note

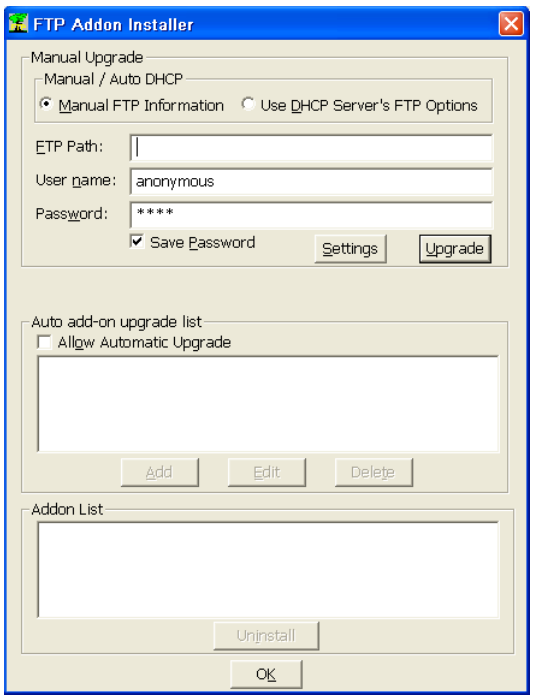
For information on configuring the Ramdisk size for temporary data storage, refer to "Setting Ramdisk Size."

Manually Installing and Upgrading Addons

Use the following guidelines:

1. Log-in as an administrator and open the **FTP Addon Installer** dialog box (**Start | Control Panel | FTP Addons**).

Figure 35 FTP Addon Installer dialog box - manual example



2. Depending on whether you select **Manual FTP Information** or **Use DHCP Server's FTP Options** complete one of the following:
   - If you selected **Manual FTP Information**, enter the IP address of the FTP server along with the path to the MSI package that installs the Addon (the MSI package on the FTP server must be accompanied by a Params.ini file in the same path or the installation will fail).
   - If you selected **Use DHCP Server's FTP Options**, the **FTP Path** box is disabled and displays the FTP server name and path derived from the DHCP server (DHCP Options 161 - FTP server list and 162 - Root path to the FTP files must be configured as described in "Using FTP File Servers").
3. Enter the credentials to connect to the FTP server (default User name is *anonymous* and the default Password is *Wyse*).
4. Select **Save Password** to allow FTP server login without entering credentials.
5. (Optional) Click **Settings** to open and use the **Network Configurable Settings** dialog box to set connection retry attempts and intervals between attempts.
6. Click the **Upgrade** button to download the Addon from the FTP server.

Note

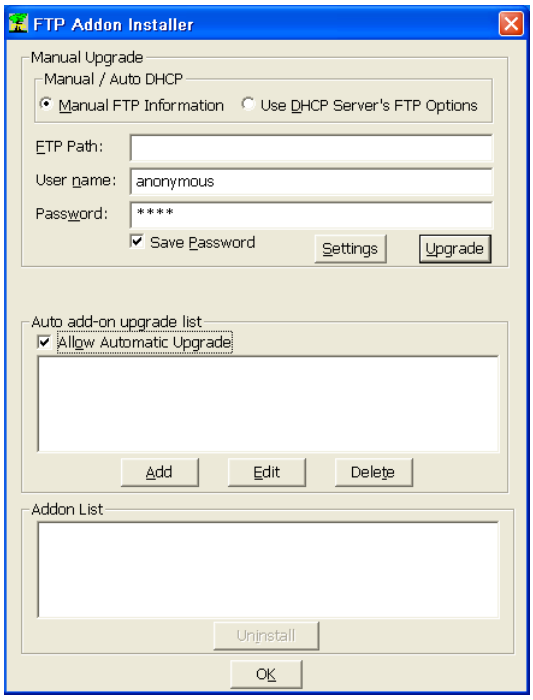
When you click the **Upgrade** button, the thin client reboots to disable the Write Filter. The reboot process takes approximately five seconds. Following the installation, the thin client reboots to enable the Write Filter.

Automatically Installing and Upgrading Addons

Use the following guidelines:

1. Log-in as an administrator and open the **FTP Addon Installer** dialog box (**Start | Control Panel | FTP Addons**).

Figure 36 FTP Addon Installer dialog box - automatic example



2. Depending on whether you select **Manual FTP Information** or **Use DHCP Server's FTP Options** complete one of the following:
   - If you selected **Manual FTP Information**, enter the IP address of the FTP server along with the path to the MSI package that installs the Addon (the MSI package on the FTP server must be accompanied by a Params.ini file in the same path or the installation will fail).
   - If you selected **Use DHCP Server's FTP Options**, the **FTP Path** box is disabled and displays the FTP server name and path derived from the DHCP server (DHCP Options 161 - FTP server list and 162 - Root path to the FTP files must be configured as described in "Using FTP File Servers").
3. Enter the credentials to connect to the FTP server (default User name is *anonymous* and the default Password is *Wyse*).
4. Select **Save Password** to allow FTP server login without entering credentials.
5. (Optional) Click **Settings** to open and use the **Network Configurable Settings** dialog box to set connection retry attempts and intervals between attempts.
6. Select the **Allow Automatic Upgrade** check box. The Addon pane displays a list of Addons, and Add, Edit, and Delete become active.
7. Click **Add** to open and use the **Add-on Upgrade FTP Info** dialog box (enter the **FTP Path** to the MSI package and enter the **User name** and **Password**, if necessary) to add a new Addon to the *Auto add-on upgrade list*.
8. (Optional) You can select an Addon in the *Auto add-on upgrade list* and click **Edit** to change information about the Addon.
9. (Optional) You can select an Addon in the *Auto add-on upgrade list* and click **Delete** to remove the Addon from the list.
10. After completing your configurations, click **OK**, and then reboot the thin client. The *FTP Addons* utility checks the *Auto add-on upgrade list*, and if an Addon in the list is not installed, or if a newer version is available for an Addon that is already installed, the thin client reboots to disable the Write Filter and performs the required installation or upgrade of an Addon. After the installation is complete, the thin client reboots to enable the Write Filter.

Note

The *FTP Addons* utility will automatically checks for newer versions of all Addons in the *Auto add-on upgrade list* each time the client restarts.

Uninstalling Addons Using the FTP Addon Installer

You can use the **FTP Addon Installer** dialog box to uninstall the thin client Addons that have been installed with the *FTP Addons* utility.

Use the following guidelines:

1. Log-in as an administrator and open the **FTP Addon Installer** dialog box (**Start | Control Panel | FTP Addons**).
2. Select the Addon to be uninstalled from the *Addon List*.
3. Click **Uninstall**. The thin client reboots to disable the Write Filter, the Addon is uninstalled, and then the thin client reboots to enable the Write Filter.

Note

If you uninstall an Addon that is included in the *Auto add-on upgrade list*, that Addon will be automatically removed from the list.

Caution

If you remove an Addon using the Windows *Add or Remove Programs* utility after disabling the Write Filter, the thin client must be rebooted once to update the *Addon List* in the **FTP Addon Installer** dialog box and enable the Write Filter.

Using Windows Server Update Services (WSUS) on a Thin Client

This section describes how to use WSUS to automatically deploy software updates on a Wyse thin client running Windows XP Embedded. Before using WSUS to deploy software updates, the server must be properly configured for WSUS.

Configuring the Thin Client for WSUS

The default Windows XP Embedded installation on a thin client does not allow users who are not administrators to receive update notifications. To check the update notification status on a thin client, do the following:

1. On the thin client, click **Start** | **Run**. In the **Run** box, enter **gpedit.msc**.
2. Navigate to **Computer Configuration**, then **Windows Components**, then **Windows Update**. If the “Allow non-administrators to receive update notifications” option or GPO does not appear, you need to modify the **wuau.adm** file on the thin client.

To modify the **wuau.adm** file to allow non-administrators to receive update notifications, follow these steps:

1. Disable the Write Filter on the thin client.
2. Copy the **wuau.adm** file from the Windows 2003 server or from the Windows XP operating system into the **c:\windows\inf** folder.
3. Enable the Write Filter on the client.

Note

The thin client must be part of a group or GPO configured on the server that distributes the updates.

Automatic Software Updates on Wyse Thin Clients Using WSUS

This section describes three ways to automatically deploy software updates on thin clients using WSUS:

- "Using WSUS on the Wyse Thin Client in Standalone Mode"
- "Configuring WSUS for Automatic Software Updates Using SMS"
- "Using WSUS with WDM"

Using WSUS on the Wyse Thin Client in Standalone Mode

You can configure WSUS on the Wyse thin client to automatically check for and install new software updates. By default, the client checks for updates every 22 hours, but you can configure a shorter interval (the frequency limit is one hour). When an update is available, the client downloads the update, using only available bandwidth, without user notification, since there is no impact to user activity (however, you can configure user notification, if desired).

Once the software is downloaded to the client, installation can occur according to the policy configured using *gpedit.msc*. When configuring policy, it is important to consider the impact of installations on the user. All client updates require reboot of the thin client.

Prerequisites

Before any software updates can be deployed via WSUS, you must:

- Install WSUS Server v. 2.0 or WSUS Server v.3.0 on the server.
- Configure communication between the thin client and the server.

To configure WSUS using the GUI:

1. Right-click the **My computer** icon and select **Properties** from the context menu.
2. Click the **services.msc** tab to display the Automatic Update Component and the corresponding service.
3. Configure the **Group Policy** to communicate with the WSUS intranet server.
4. When the Windows XP Embedded client contacts the WSUS server, notification of pending software updates appears on the taskbar.
5. To install the software updates, run the scripts to disable the Write Filter before the installation, and enable it after installation, as described in the "About VB Scripts" section.

Note

You must disable the Write Filter before you can install the required updates. When the Write Filter is enabled, the thin client can save the update files until the next client reboot. Upon reboot, the update files are deleted.

To configure WSUS using the command line interface:

1. From the **Start** menu, choose **Run** to display the command prompt.
2. At the command prompt, type **wuauclt.exe**.
3. Run the executable file and configure the **Group Policy** for the client to communicate with the WSUS intranet server.
4. To install the software updates, run a script to disable the Write Filter before the installation, and enable it after installation, as described in the "About VB Scripts" section.

Troubleshooting WSUS in Standalone Mode

WSUS provides a log for troubleshooting issues related to software updates. This log is located on the thin client, in the directory: **C:\windows\windowsupdate log**. This log displays all communications between the client and the server. You can use PERFMON to monitor memory allocation for the WSUS client web services component and WSUS server web services component of the update log.

Note

Alternatively, you can use a network monitoring or packet sniffing tool to monitor the traffic between the client and the server.

Table 2 shows the WSUS log format with some examples.

Table 2 WSUS Log Format

Date	Time	PID	TID	Component	Text
2005-06-01	18:30:03	992	810	Misc	= Logging initialized
2005-06-01	18:30:03	992	810	Misc	= Process
2005-06-01	18:30:03	992	810	Misc	= Module

Table 3 lists the components that can write to the WSUS log.

Table 3 WSUS Components

Component	Description
AGENT	Windows Update agent
AU	Automatic Updates is performing this task
AUCLNT	Interaction by AU with the logged on user
CDM	Device Manager
CMPRESS	Compression agent
COMAPI	Windows Update API
DRIVER	Device driver information
DTASTOR	Handles database transactions
DWNLDMGR	Creates and monitors download jobs
EEHNDLER	Expression handler used to evaluate update applicability
HANDLER	Manages the update installers
MISC	General service information
OFFLSNC	Detect available updates when not connected to the network
PARSER	Parses expression information
PT	Synchronizes updates information to the local datastore
REPORT	Collects reporting information
SERVICE	Startup/Shutdown of the Automatic Updates service
SETUP	Installs new versions of the Windows Update client when available
SHUTDWN	Install at shutdown feature
WUREDIR	Windows Update redirector files
WUWEB	Windows Update ActiveX control

Windows Update Log File Examples

The examples below illustrate the log files for selected activities.

Service Startup

```
2005-06-01 18:30:03 992 810 Service ************* 2005-06-01
18:30:03 992 810 Service ** START ** Service: Service startup
2005-06-01 18:30:03 992 810 Service *********
```

The Windows Update agent searches for available updates

```
2005-06-02 12:09:36 992 4e8 Agent ************* 2005-06-02
12:09:36 992 4e8 Agent ** START ** Agent: Finding updates [CallerId
= WindowsUpdate] 2005-06-02 12:09:36 992 4e8 Agent *********
2005-06-02 12:09:36 992 4e8 Agent * Added update
{AC94DB3B-E1A8-4E92-9FD0-E86F355E6A44}.100 to search result
2005-06-02 12:09:37 992 4e8 Agent * Found 6 updates and 10
categories in search
```

The user is offered one update and chooses to install it

```
2005-06-02 12:10:41 1660 d0c COMAPI ------------- 2005-06-02
12:10:41 1660 d0c COMAPI -- START -- COMAPI: Install [ClientId =
WindowsUpdate] 2005-06-02 12:10:41 1660 d0c COMAPI ---------
2005-06-02 12:10:41 1660 d0c COMAPI - Allow source prompts: Yes;
Forced: No; Force quiet: No 2005-06-02 12:10:41 1660 d0c COMAPI -
Updates in request: 1 2005-06-02 12:10:41 1660 d0c COMAPI -
ServiceID = {9482F4B4-E343-43B6-B170-9A65BC822C77} 2005-06-02
12:10:41 1660 d0c COMAPI - Updates to install = 1 2005-06-02
12:10:41 1660 d0c COMAPI <<-- SUBMITTED -- COMAPI: Install
[ClientId = WindowsUpdate]
```

The Windows Update agent starts the installation process

```
2005-06-02 12:10:41 992 58c Agent ************* 2005-06-02
12:10:41 992 58c Agent ** START ** Agent: Installing updates
[CallerId = WindowsUpdate] 2005-06-02 12:10:41 992 58c Agent
********* 2005-06-02 12:10:41 992 58c Agent * Updates to install =
1 2005-06-02 12:10:41 992 58c Agent * Title = <NULL> 2005-06-02
12:10:41 992 58c Agent * UpdateId =
{19813D2E-0144-43CA-AEBB-71263DFD81FD}.100 2005-06-02 12:10:41 992
58c Agent * Bundles 1 updates: 2005-06-02 12:10:41 992 58c Agent *
{08D9F87F-7EA2-4523-9F02-0931E291908E}.100
```

Configuring WSUS for Automatic Software Updates Using SMS

You can configure WSUS to use the SMS server to perform automatic software updates in either a Workgroup environment or using Active Directory.

Prerequisites

Before any software updates can be deployed via WSUS, you must:

- Install SMS 2003 or SMS 2007 on the server and the thin client.
- Install WSUS Server v. 2.0 or WSUS Server v.3.0 on the server.
- Configure the thin client for WSUS, following the procedure in the "Configuring the Thin Client for WSUS" section.

To use WSUS along with SMS to perform automatic software updates on a thin client:

Push the required script (pre-script) from the SMS server to the clients connected to the SMS server. The script must be configured to:

1. Disable the Write Filter.
2. Initiate the download and installation of the appropriate updates on the thin clients.
3. Enable the Write Filter.

About VB Scripts

Software distribution via SMS requires two Write Filter actions on the XP Embedded thin clients: one action disables the Write Filter before the application deployment, and the other action enables the Write Filter following the application deployment. There is one VB script to perform each action.

Note
The VB scripts run on the thin client without any prompt messages.

The **Disable_ewf_fbwf.vbs** script disables the EWF and FBWF Write Filters and restarts the thin client within 60 seconds. Following the restart, the Write Filter is disabled.

After this script is executed, you can deploy an application or patch to the thin client. Following the software deployment, run the Enable_ewf_fbwf.vbs script to enable the EWF and FBWF Write Filters and restart the thin client within 60 seconds. Following the restart, the Write Filter is enabled.

Note
If WSUS 3.0 is installed on the server, you can monitor the progress of the software updates on the thin clients and push the script to re-enable the Write Filter after the update is complete.

Troubleshooting WSUS Used with SMS

The tools described in the "Troubleshooting WSUS in Standalone Mode" section are available for use with SMS.

In addition, you can use the SMS server log to identify the package status and the WSUS client log to troubleshoot update status issues.

Using WSUS with WDM

You can use WDM to deploy the script that disables the Write Filter, and then configure the thin client to contact the WSUS server for software updates.

Prerequisites

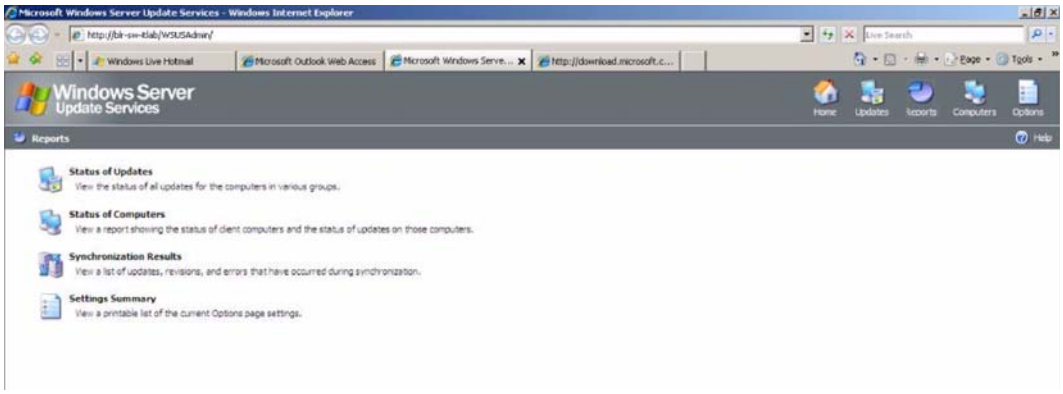
Before any software updates can be deployed via WSUS, you must:

- Install and configure WDM on the server
- Install WSUS Server v. 2.0 or WSUS Server v.3.0 on the server.
- Configure communication between the thin client and the server.

To configure automatic software updates:

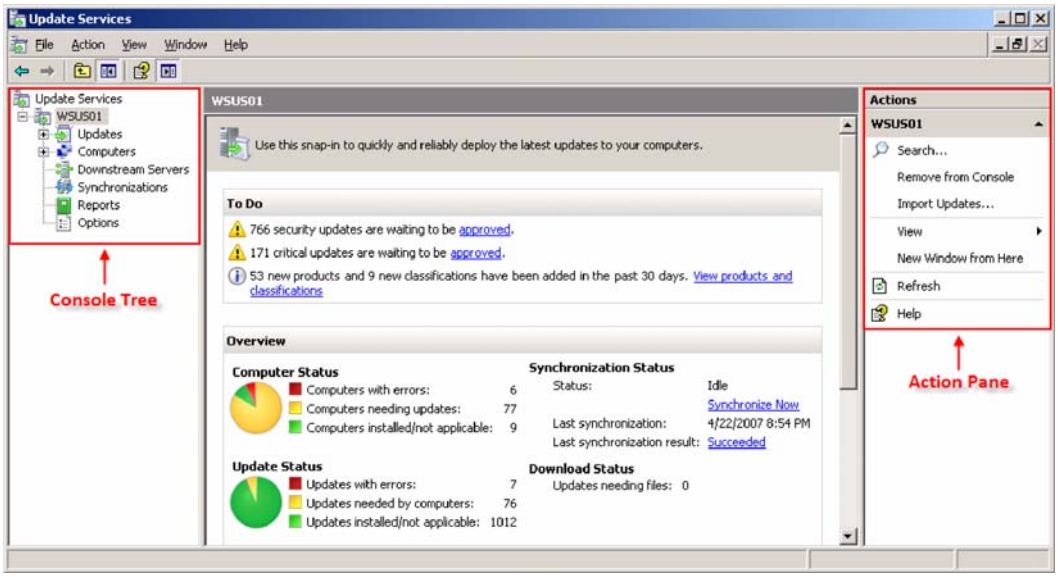
1. Use the WDM server to push the script that disables the Write Filter on the thin client.
2. Configure the thin client to contact the WSUS server for software updates, following the procedure in the "Configuring the Thin Client for WSUS" section.
3. Monitor the status of the software updates on the server.
   - In WSUS version 2.0, you can view the status of updates by navigating to: **WSUS Console** > **Reports** tab. (See Figure 37.)

Figure 37 WSUS 2.0 Reports Tab



- In WSUS version 3.0, a management console provides a more graphical view with multiple options for monitoring the download of updates. (See Figure 38.)

Figure 38 WSUS 3.0 Management Console



4. When the software updates are complete, use WDM to schedule the script that enables the Write Filter to run on the thin client.

Troubleshooting WSUS with WDM

You can use the steps described in the “Troubleshooting WSUS in Standalone Mode” section to troubleshoot the issues related to the software update on clients and on the WDM server by analyzing the relevant logs present on both the client and the server:

- **WindowsUpdate.log file**—provides statistics
- **PERFMON counters**—help administrators to check the utilization
- **Netmon or Ethereal trace**—shows data flow
- **Event logs**—display the events, including any failures

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

If you are running XP Embedded version 2.2 or earlier, you must follow these important instructions when imaging the Wyse thin clients with the standard XP Embedded 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 Wyse 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 39 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 | Control Panel | Administrative Tools | Services**).

Note

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

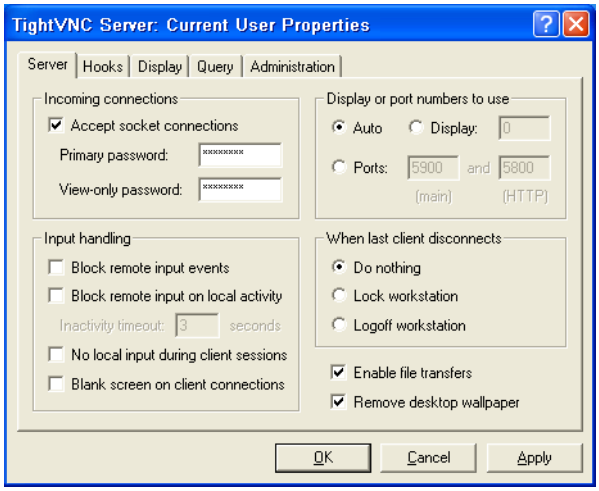
Setting VNC Server Properties

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 40 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 | Control Panel | 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

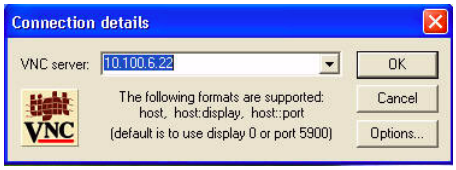
VNC Viewer software is included as a component of WDM software and must be installed on the remote (shadowing) machine. An administrator/user of the remote machine must know the IP address/name and the password of a the thin client that is to be operated/monitored.

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:

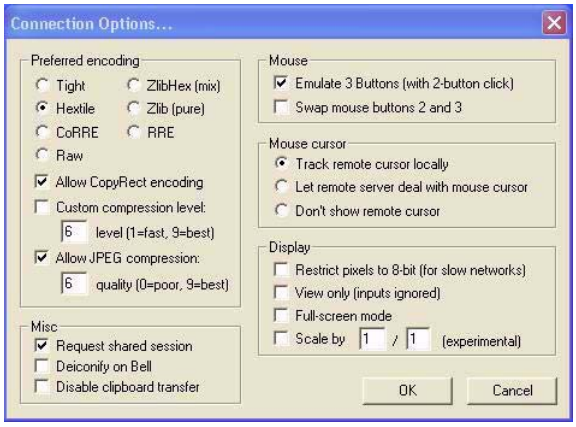
1. Double-click the **VNC Viewer** icon to open the Connection Details dialog box.

Figure 41 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 42 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:

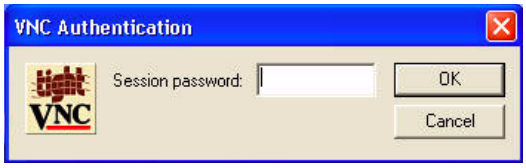
   ```
   snoopy:0
   ```

   or

   ```
   132.237.16.238:0
   ```

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

Figure 43 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® Thin Clients, Based on Microsoft® Windows® XP Embedded
Issue: 081309

Written and published by:
Wyse Technology Inc., August 2009

Created using FrameMaker® and Acrobat®