Administrators Guide

Wyse® Winterm™ 1 series, Based on Wyse Thin OS

Issue: 041707
PN: 883682-08 Rev. G

Copyright Notices

End User License Agreement (“License”)

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

Trademarks

Wyse and Winterm are registered trademarks, and the Wyse logo and Winterm logo are trademarks of Wyse Technology Inc. ICA is a registered trademark and MetaFrame is a trademark of Citrix Systems Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other products are trademarks and/or registered trademarks of their respective companies. Specifications subject to change without notice.

Patents

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

Restricted Rights Legend

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

Ordering Information

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

FCC Statement

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

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

Caution

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

EMC and Safety Requirements

Models 1125SE, SX0, and VX0 thin clients are compliant with the regulatory requirements in the regions listed below.

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

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.

Cable Notice

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

Noise Suppressor

A noise suppressor (ferrite bead) must be installed on the network cable of your thin client (except Models SX0 and VX0). This installation is necessary to maintain compliance with U.S. FCC B limits and European CISPR B EN55022 Class B limits. The noise suppressor is supplied by the manufacturer and is packed in your thin client shipping carton.

Device Power Supply

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

Model 1125SE Thin Client

For use with External Power Supply DVE Model DSA-0421S-12 330 or 324 or certified equivalent model supplied by the manufacturer, rated minimum 12V/2.5A or 12V/2A.

Model SX0 Thin Client

For use with External Power Supply DVE Model DSA-0151F-12A or certified equivalent model supplied by the manufacturer, rated minimum 12Vdc, 2.5A.

Model VX0 Thin Client

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

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

⚠ Warning

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

This page intentionally blank.

Contents

1 Introduction

Wyse® Winterm™ 1 series Thin Clients use the Wyse Thin OS. These highly optimized thin clients provide ultra-fast access to applications, files, and network resources made available on machines hosting Citrix™ ICA and Microsoft™ RDP session services. Locally installed software permits remote administration of the thin clients and provides local maintenance functions.

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

About this Guide

This guide is intended for administrators of the Wyse® Winterm™ 1 series Thin Client. It provides information and detailed system configurations to help administrators design and manage a Wyse® Winterm™ 1 series Thin Client environment. This guide assumes that you are familiar with TCP/IP, DHCP, and FTP protocols. The instructions in this guide assume that you are familiar with the *Users Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS*.

Although this guide discusses similar information to that contained in the *Users Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS*, refer to the *Users Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS* for information on configuring the thin client (locally) to manage the connections and applications available to users from a network server.

Organization of this Guide

This guide is organized as follows:

Chapter 2, "Establishing a Server Environment," contains information on the network architecture and enterprise server environment needed to provide network and session services for Wyse® Winterm™ 1 series Thin Clients. It also includes information to help you to address important considerations when configuring access to the server environment and when configuring the services to be provided by the server environment.

Chapter 3, "System Administration," provides system administration information, remote management information, and detailed system command and parameter configurations, to help you design and manage a Wyse® Winterm™ 1 series Thin Client environment.

Wyse Technical Support

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

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

Related Online Resources Available at Wyse

Wyse® Winterm™ 1 series Thin Client features can be found in the Datasheet for your specific thin client model. Datasheets are available on the Wyse Web site at: http://www.wyse.com/products.

Sample User Configuration Profile files (.ini files) are available from Wyse. These sample files are annotated to allow you to use them as a starter set on your FTP server and can be modified to suit your needs. The sample files are available on the Wyse Web site at: http://www.wyse.com/products/winterm/reference/1series.

The *Users Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS* is intended for users of the Wyse® Winterm™ 1 series Thin Client. It provides detailed instructions on using the thin client to manage the connections and applications available to users from a network server. It is available at: http://www.wyse.com/manuals.

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

2 Establishing a Server Environment

This chapter contains information on the network architecture and enterprise server environment needed to provide network and session services for Wyse® Winterm™ 1 series Thin Clients. It also includes information to help you to address important considerations when configuring access to the server environment and when configuring the services to be provided by the server environment.

Setting Up Access to Enterprise Servers

As discussed in the *Users Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS* 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 settings cannot be automated because the thin client has not yet accessed Global and User profiles. For certain privileges, 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 Direc**t - This is a connection from the thin client Ethernet port directly to the enterprise intranet. No additional hardware is required. In this configuration all network services may be used, including the enterprise DHCP server. A DHCP server on the network can provide not only the thin client IP address, but also the location of the file server containing the user profiles and software updates.
- **Wireless Direct** - An 802.11b USB Wireless Adapter can be used to access the enterprise intranet. The adapter connects to a USB port on the thin client and 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 802.11b USB Wireless Adapters and directly connected to the enterprise intranet. Contact Wyse for available wireless network devices.

  Service set identification (SSID), channel, and encryption keys must be entered in the Wireless Setup dialog box on the thin client and corresponding entries must be made in the access point dialog; except for this, thin client operation is the same as Ethernet direct access, including access to the enterprise DHCP server.

Note

The SSID and encryption keys can be set using the Device option in the .ini file. This allows you to configure units using a private .ini file prior to deployment and removes the need for manual entry.

- **PPPoE** - Thin client support for PPPoE is intended for devices which connect to the Internet directly from remote locations. PPPoE is used as an alternative to providing DHCP support or static IP addresses on all high speed lines. PPPoE is compatible with the use of PPTP, FTP, and/or PNAgent/PNLite.

The **No local LAN, invoke PPPoE only** option must first be selected in the Network Setup dialog box. After being selected, the PPPoE Manager can be used and is available from the desktop to configure and invoke PPPoE connection to WAN. Once connected, all packets are through a PPP connection over Ethernet to the DSL modem.

The PPPoE Manager dialog box is not accessible for users with sign-on privilege set to None. However, access to the PPPoE Manager dialog box is not necessary if the connection is to be established at startup. And unless the unit is locked down, establishing the PPPoE connection would take place before reading an ini file. Therefore any unit which is not locked down would have the default privilege (high) at this boot stage.

Open the PPPoE Manager dialog box by selecting it from the desktop menu. This dialog box also may be set to open automatically on system start-up.

The PPPoE Manager dialog box allows configuration for the following ISP login - properties:

- **Login Username** - (up to 43 characters)
- **Login Password** - (up to 15 characters)
- **Auto-Connect** - A check box to select if Auto-Connect on system startup is desired.
- **Use default gateway on remote (PPPoE) network** - A check box to select using the default gateway on system startup is desired.

- **Dial-up Modem** - A USB dial-up modem or a USB-to-Serial adapter connected to a serial modem can be used with the thin client to access a dial-up server.

  The dial-up server may provide either of two 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 must access an enterprise PPTP VPN server that connects to the enterprise intranet.

Note
The dial-up server must be a Microsoft Remote Access Server or another server that supports industry-standard protocols.

- **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. 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.

Note
For more information on these methods of access, refer to the *Users Guide: Wyse® Winterm™ 1 series, Based on Wyse Thin OS*.

About Configuring Network Services

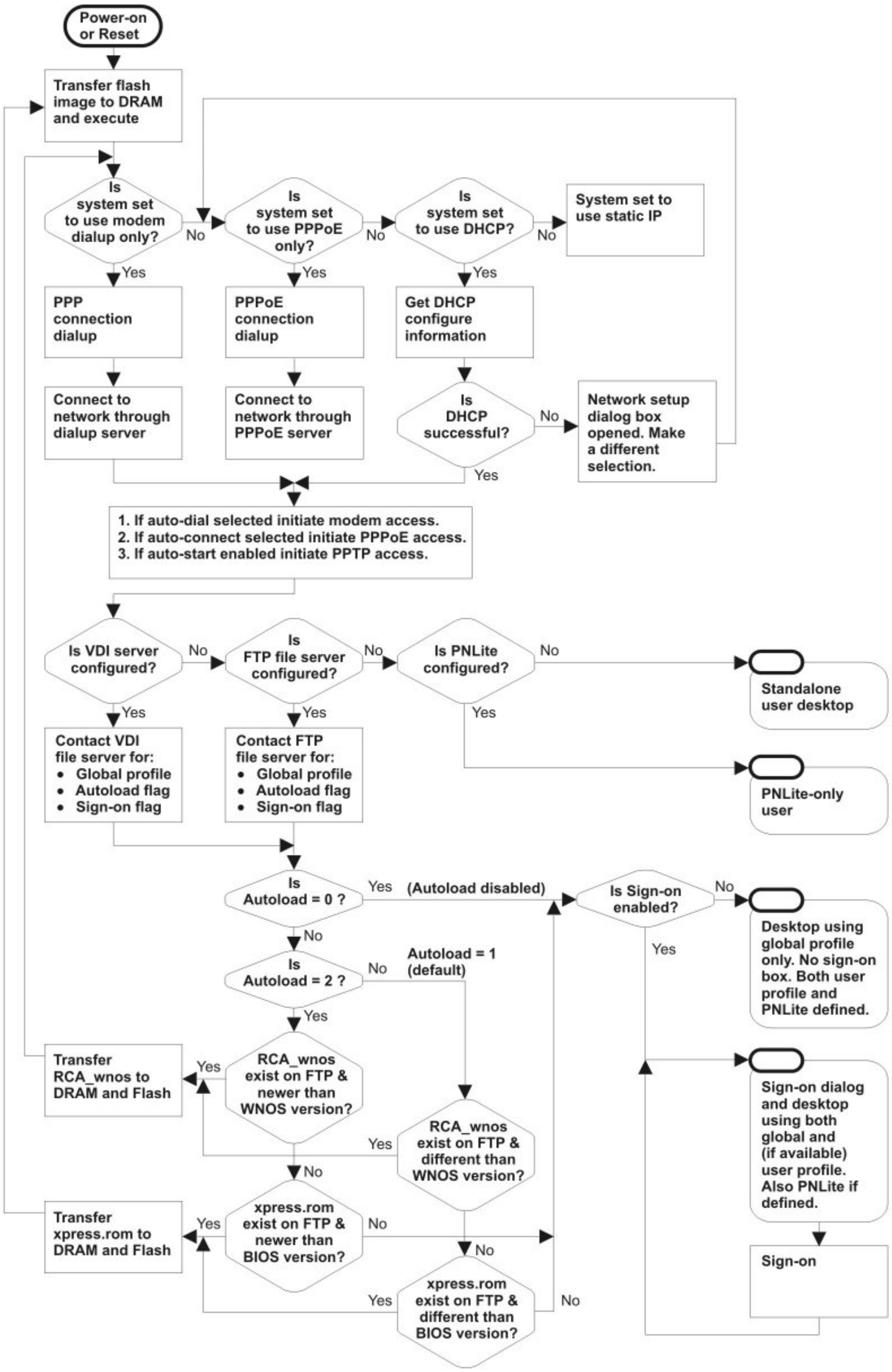
Network services used by the thin client include DHCP, FTP file services, Virtual Desktop file services, and DNS.

Note

Thin clients accept valid DNS names registered on a DNS server available to the enterprise intranet.

Figure 1 shows the thin client boot flow process.

Figure 1 Boot flow process


Power-on or Reset
Transfer flash image to DRAM and execute
Is system set to use modem dialup only?
No
Yes
Is system set to use PPPoE only?
No
Yes
Is system set to use DHCP?
No
Yes
System set to use static IP
PPP connection dialup
PPPoE connection dialup
Get DHCP configure information
Connect to network through dialup server
Connect to network through PPPoE server
Is DHCP successful?
No
Yes
Network setup dialog box opened. Make a different selection.
1. If auto-dial selected initiate modem access.
2. If auto-connect selected initiate PPPoE access.
3. If auto-start enabled initiate PPTP access.
Is VDI server configured?
No
Yes
Is FTP file server configured?
No
Yes
Is PNLite configured?
No
Yes
Standalone user desktop
PNLite-only user
Contact VDI file server for:
• Global profile
• Autoload flag
• Sign-on flag
Contact FTP file server for:
• Global profile
• Autoload flag
• Sign-on flag
Is Autoload = 0 ?
Yes
(Autoload disabled)
No
Is Sign-on enabled?
No
Yes
Desktop using global profile only. No sign-on box. Both user profile and PNLite defined.
Is Autoload = 2 ?
No
Autoload = 1 (default)
Yes
Transfer RCA_wnos to DRAM and Flash
Yes
RCA_wnos exist on FTP &amp; newer than WNOS version?
No
Yes
RCA_wnos exist on FTP &amp; different than WNOS version?
Sign-on dialog and desktop using both global and (if available) user profile. Also PNLite if defined.
Transfer xpress.rom to DRAM and Flash
Yes
xpress.rom exist on FTP &amp; newer than BIOS version?
No
No
Yes
xpress.rom exist on FTP &amp; different than BIOS version?
No
Sign-on

This section provides important overview information on the following service situations:

- "DHCP and FTP Servers Available"
- "FTP Server Available (DHCP Server Unavailable)"
- "DHCP and Virtual Desktop Servers Available"
- "Virtual Desktop Server Available (DHCP Server Unavailable)"
- "FTP and Virtual Desktop Servers Unavailable (Stand-alone User or PNAgent/ PNLite-only User)"

☒ **Caution**

If a thin client accesses the enterprise intranet through Dial-up, PPPoE, or PPTP VPN and the thin client is locked-down, a non-privileged or low-privileged user attempting to reboot to Stand-alone user mode will disable the Network Setup dialog box and System Reset capabilities. The user will not be able to re-access the enterprise intranet through this path. If this happens, the thin client must be moved to a location where it can access the enterprise intranet directly (Ethernet cable) and reboot so that you as an administrator can make any required changes to the thin client operating configurations (for example, set the profile to unlock the thin client) through the User profiles.

If the thin client is configured for Dial-up access, there must be an RAS server answering the configured telephone number. Otherwise, the thin client will require factory attention to recover it.

DHCP and FTP Servers Available

A thin client is initially (new-thin client or reset thin client to default configurations) configured to obtain its IP address and the location of the FTP server from a DHCP server. DHCP can only be used for the Ethernet Direct access and Wireless Direct access configurations.

As a network administrator, you must set up both DHCP and FTP network services and create Global and User profiles as described in this guide (see "Configuring Network Services" and "Understanding User Accounts and User Profile Ini Files." for details). If Wireless Direct access is used, the Wireless Setup dialog box must be configured locally.

If DHCP and FTP servers are available, simply connect the thin client to the network (either directly through a network cable or through a wireless network device), turn it on, and begin using the thin client. A sign-on name and password may be required for access to the profiles and session services. If applications published by Citrix PNAgent/PNLite services are available, a Domain name must be entered or selected from the list. One or more connection or application may start automatically if they are selected in the Global or individual User profiles.

✓ **Note**

If session connections or published applications are designated to open automatically on start-up, upon accessing the enterprise server environment you will see a session server log-in or server application window instead of the thin client desktop. Use CTRL+ALT+UPARROW to toggle between window display modes. Use CTRL+ALT+DOWNARROW to open a selection box for toggling between the desktop, the Connect Manager, and currently-active connections.

If the thin client accesses the enterprise server environment through Dial-up, PPPoE, and/ or PPTP VPN, the automation provided by a DHCP server is not available (see "FTP

Server Available (DHCP Server Unavailable)" and "FTP and Virtual Desktop Servers Unavailable (Stand-alone User or PNAgent/PNLite-only User)" for more information).

Note

This is true if these connections (Dial-up, PPPoE, and/or PPTP VPN) are manually initiated. If they are automatically started, FTP server services will be accessed through the Dial-up, PPPoE, or PPTP VPN connection.

FTP Server Available (DHCP Server Unavailable)

If a DHCP server is not available but an FTP server is available, the thin client user must locally enter (using the thin client Network Setup dialog box) network information that would otherwise be supplied by the DHCP server.

If the thin client is configured for DHCP (new-thin client or reset thin client to default configurations) but DHCP is not detected on the network, the Network Setup dialog box automatically opens when the thin client is started. You can also open the Network Setup dialog box manually by clicking on the desktop background, selecting **System Setup** from the desktop menu, and then clicking **Network**.

After opening the Network Setup dialog box, select the **Statically specified IP Address** option and configure the dialog box for the following information (any remaining information will be automatically populated from the User profiles when the FTP server is contacted):

- Static IP address of the thin client
- Subnet Mask
- Default Gateway
- DNS Domain Name (not necessary if DNS is not used)
- DNS Server Address (not necessary if DNS is not used)
- File Server IP address or DNS name of the FTP server on which the configuration files reside and the FTP path on the server to /wnos.
- PNAgent/PNLite Servers list (If PNAgent/PNLite is deployed on the network environment, enter the IP address or Host name with optional TCP port number of one or more PNAgent/PNLite servers that will provide published applications on the network)
- Ethernet Speed
- WINS Server Address (not necessary if DNS is not used)
- Username and Password for login to the FTP server
- Rapport Server Address (not necessary if DNS is not used)
- Time Server

After the network settings are configured, reboot the thin client before using it. As with the DHCP configuration, a sign-on name and password may be required (and if applications published by Citrix PNAgent/PNLite services are available, a Domain name must be entered or selected from the list). One or more connection or application may start automatically if selected in the Global or individual User profiles.

DHCP and Virtual Desktop Servers Available

A thin client is initially (new-thin client or reset thin client to default configurations) configured to obtain its IP address and the location of the Virtual Desktop server from a DHCP server. DHCP can only be used for the Ethernet Direct access and Wireless Direct access configurations.

As a network administrator, you must set up both DHCP and Virtual Desktop network services and create Global and User profiles in the Virtual Desktop Broker (see "Configuring Network Services" and "Understanding User Accounts and User Profile Ini Files." for more information). If Wireless Direct access is used, the Wireless Setup dialog box must be configured locally.

If DHCP and Virtual Desktop servers are available, simply connect the thin client to the network (either directly through a network cable or through a wireless network device), turn it on, and begin using the thin client. A sign-on name and password may be required for access to the profiles and session services. One or more connection or application may start automatically if they are selected in the Global or individual User profiles.

If the thin client accesses the enterprise server environment through Dial-up, PPPoE, and/or PPTP VPN, the automation provided by a DHCP server is not available (see "Virtual Desktop Server Available (DHCP Server Unavailable)" for more information).

☑ **Note**

This is true if these connections (Dial-up, PPPoE, and/or PPTP VPN) are manually initiated. If they are automatically started, Virtual Desktop server services will be accessed through the Dial-up, PPPoE, or PPTP VPN connection.

Virtual Desktop Server Available (DHCP Server Unavailable)

If a DHCP server is not available but a Virtual Desktop server is available, the thin client user must locally enter (using the thin client Network Setup dialog box) network information that would otherwise be supplied by the DHCP server.

If the thin client is configured for DHCP (new-thin client or reset thin client to default configurations) but DHCP is not detected on the network, the Network Setup dialog box automatically opens when the thin client is started. You can also open the Network Setup dialog box manually by clicking on the desktop background, selecting **System Setup** from the desktop menu, and then clicking **Network**.

After opening the Network Setup dialog box, select the **Statically specified IP Address** option and configure the dialog box for the following information (any remaining information will be automatically populated from the User profiles when the Virtual Desktop server is contacted):

- Static IP address of the thin client
- Subnet Mask
- Default Gateway
- DNS Domain Name (not necessary if DNS is not used)
- DNS Server Address (not necessary if DNS is not used)
- Ethernet Speed
- WINS Server Address (not necessary if DNS is not used)
- Username and Password for login to the FTP server
- Rapport Server Address (not necessary if DNS is not used)
- Time Server
- VDI Server

After the network settings are configured, reboot the thin client before using it. As with the DHCP configuration, a sign-on name and password may be required. One or more connection or application may start automatically if selected in the Global or individual User profiles.

FTP and Virtual Desktop Servers Unavailable (Stand-alone User or PNAgent/ PNLite-only User)

If FTP or Virtual Desktop Broker servers are not available (for example, Stand-alone User or PNAgent/PNLite-only User situations), configuration files are not available and network information must be entered locally at the thin client.

Stand-alone User - A Stand-alone user does not access user profiles or PNAgent/ PNLite-published applications. **New** and **Settings** command buttons appear on the Connect Manager dialog box (if this dialog box does not open automatically, open it from Desktop menu) that are not otherwise available to low-privileged and non-privileged sign-on users. Locally entered connection definitions are preserved when the thin client is turned off, but automatic software updates are not available when the power is turned on again.

PNAgent/PNLite-only User - This user does not access user profiles but applications published by Citrix PNAgent/PNLite services that are available (the IP address of a PNAgent/PNLite server and Domain are entered into the Network Setup dialog box or available through DHCP options 181 and 182). A log-on dialog box (similar to the standard log-on dialog box) opens for logging on to the PNAgent/PNLite server. Applications published by PNAgent/PNLite are listed in the Connect Manager (Published applications that add a shortcut to the client desktop will have an icon on the desktop which you can double-click to open). Locally-defined connections are not preserved when the thin client is restarted or turned off.

Configuring Network Services

Thin client network services reside on the enterprise intranet. When setting up thin client network services, remember that if thin clients are to access the enterprise intranet through Dial-up, PPPoE, or PPTP VPN, restrictions imposed by these access paths must be considered.

Note

Be sure you have read "About Configuring Network Services" before you begin configuring network services.

The FTP server or the Virtual Desktop server holds the user configuration profile files, while the FTP server holds the current and upgrade versions of the thin client software.

Note

For more information on the installation of software update images, refer to "Updating Software." For more information on user configuration files, refer to "Understanding User Accounts and User Profile Ini Files."

The thin client software is acquired from either local flash memory or the FTP server. During the boot process, the local image is transferred to RAM and executed far enough for the thin client to check the image and the profiles on the file servers. Under direction of the profile parameters and the version of the remote image, the image in RAM can be replaced with the remote image; and separately, the remote image can update the local flash-memory.

Note

New software images can be obtained from Wyse as they become available.

User configuration profile (.ini) files are created and maintained by you, the network administrator, and are stored on the file server. There is one Global .ini file for all users of a given file server and, if configured, unique User .ini file for each user. The thin client accesses the Global .ini files upon thin client initialization and accesses any individual User .ini file when the user logs on (if user log-on is required, the User .ini file must exist before that user can log on). The .ini files contain connection definitions and thin client settings. These text-based files must be created and maintained by using an ASCII text editor. If the .ini files are omitted or they cannot be accessed because a file server is not used, the thin client user must enter connection definitions locally (or for FTP servers, use what is published by PNAgent/PNLite servers residing on the network).

Note

You can also define connections in the ini files which are to be stored in local NV-RAM and used in cases where the file server fails.

To configure network services, use the information in the following sections:

- "About Configuring FTP Servers"
- "About Configuring Virtual Desktop Infrastructure Servers"
- "Configuring DHCP"
- "Configuring DNS"
- "Configuring WINS"
- "Configuring Wyse Device Manager Servers"

About Configuring FTP Servers

When the thin client boots, it accesses the software update images and user configuration profile files from the FTP server. The FTP server and path to the update files are available through DHCP vendor options 161 and 162 (see "Configuring DHCP"). If these are not specified, the default FTP server is the DHCP server from which the thin client receives its IP address and the default directory (`\wyse\wnos` for Windows FTP servers, or `/wyse/wnos` for Linux FTP servers). The FTP server and path to the update files can also be specified locally on the thin client. DHCP options 184 and 185 can be used to provide the User ID and Password for non-anonymous access to the FTP server in Wyse Thin OS version 4.3 and later. For Wyse Thin OS versions earlier than 4.3, the file server must have anonymous login capability and provide at least file read privilege for the anonymous user (it must also provide file write privilege if users are allowed to change their passwords).

✓ **Note**

Guidelines for Non-Anonymous Access: You must first create a local account (name the account so that you remember it is a non-anonymous account) on the FTP server defined between the DHCP vendor options 161 and 162 (DHCP Server). Then, add DHCP options 184 and 185 to provide the User ID and Password for non-anonymous access to the FTP server. Ensure that option 184 is the account User ID and that option 185 is the account Password, and that you keep consistency with FTP server DHCP vendor options (for example, ensure that the 184 and 185 options are string parameters). Then provide the non-anonymous account with read-only permissions through the entire FTP server path. Be sure to modify these guidelines according to your specific security environment and configuration.

Guidelines for Windows FTP Servers:

- You can use the tools available on the Windows server.
- For Wyse Thin OS versions earlier than 4.3, be sure the Windows server supports the anonymous log-in capability. For Wyse Thin OS version 4.3 and later, this support is not necessary because of the User Interface (UI)/DHCP feature to specify the login ID and password.

Guidelines for Linux FTP Servers:

- The FTP server must be configured to offer FTP services (by adding the following line or equivalent to its `/etc/inetd.conf` file, if it is not already present):
  ```
  ftp stream tcp nowait root /usr/sbin/tcpd in.proftpd
  ```
- The FTP server must be configured to support anonymous FTP. For most FTP servers, this requires establishment of an FTP login account by adding the following line or equivalent to the `/etc/password` file:
  ```
  ftp:x:17:1:Anonymous FTP directory:/home/ftp:/dev/null/
  ftp-shell
  ```

  The shell file `/dev/null/ftp-shell` need not exist, but some FTP servers require that it be listed in /etc/shells to allow FTP connections on this account.
- Depending on which Linux distribution you are using, additional modifications to a central configuration file for the FTP daemon may be necessary to enable anonymous FTP. You can try man protftp, man wuftpd, or man ftpd to access information applicable to your particular FTP daemon.
- A Linux server used for FTP must support passive FTP.

Configuring an FTP Server

To configure an FTP server, complete the following procedures:

1. Create the following directory structure on your FTP server:

```
<path from anonymous user FTP root>/wyse/wnos/
<path from anonymous user FTP root>/wyse/wnos/ini/
<path from anonymous user FTP root>/wyse/wnos/bitmap/
<path from anonymous user FTP root>/wyse/wnos/cacerts/
```

Note

There is a difference between a path obtained from the DHCP server and a path entered in the UI. If the path is obtained from DHCP, `/wyse/wnos` are appended. If the value is obtained from the UI, the `/wyse` portion is not appended; only `/wnos` is automatically inserted. As written in this first step, the configuration procedure will only work in conjunction with a DHCP server.

2. Depending on your thin client model, complete one of the following:
   Model 1125SE - Download the TWA_boot and TWA_wnos software images from the Wyse support FTP site and place them in the wnos subdirectory on your FTP server (TWA_boot loads in the 256K NOR image while TWA_wnos loads in the NAND flash image. Both of these files can be updated in the terminal through an FTP file server).
   Models SX0 and VX0 - Download the RCA_boot and RCA_wnos software images from the Wyse support FTP site and place it in the wnos subdirectory on your FTP server.

3. Download and unpack the Sample User Configuration Profile files (.ini files) from Wyse into a directory from which they can be examined and modified using an ASCII text editor. These sample files are annotated to allow you to use them as a starter set on your FTP server and can be modified to suit your needs. The sample files are available on the Wyse Web site at: http://www.wyse.com/products/winterm/reference/1series. Files include:
   - **wnos.kiosk** - Example wnos.ini file for a kiosk configuration
   - **wnos.login** - Example wnos.ini file to enable multiple user accounts
   - **user.ini** - Template for {username}.ini for individual user profiles

4. Determine whether all the thin clients served by this FTP server will be used as kiosks or will support individual user accounts. You must rename the downloaded files so that there will be one wnos.ini file available to all users globally; and for a multiple user account configuration there will be a unique {username}.ini file for each user. In addition:
   - **If the kiosk configuration is to be used** - change the name of `wnos.kiosk` to `wnos.ini`. Otherwise, for multiple user accounts, change the name of `wnos.login` to `wnos.ini`.
   - **If the individual user account configuration is to be used** - make a copy of `user.ini` for each user name as {username}.ini (where {username} is the name of the user) and place the files in the subdirectory ini of wnos. The files must have read permission enabled, and if users are to be allowed to change their passwords, the files also must have write permission enabled (so that the thin clients can write the encrypted user passwords to them). **For Linux servers**, use the `chmod` command to set the read/write permissions. **For Microsoft servers**, use the Properties dialog box to set read/write permissions.

5. If desired, you can customize the initialization files to match the local environment using the instructions in "Understanding User Accounts and User Profile Ini Files." If you modify the configuration .ini files to include icons and logos, place the images in the FTP subdirectory bitmap of wnos.

About Configuring Virtual Desktop Infrastructure Servers

When the thin client boots, it accesses the Global and User configuration profile files from a Virtual Desktop Infrastructure server. Virtual Desktop Infrastructure servers are available through DHCP vendor option 188 (see "Configuring DHCP").

The thin client communicates with Virtual Desktop Broker server by the sysinit, signon, signoff, and shutdown commands. When the thin client boots and successfully connects in a Virtual Desktop environment, it sends the sysinit command to the Virtual Desktop Broker, which then sends back the wnos.ini (Global profile) file (if a Broker connection cannot be made, the thin client will attempt to connect to FTP or PNLite servers). After the thin client successfully receives the wnos.ini from the Virtual Desktop Broker, a sign-on window displays, prompting the user for username and password credentials. The thin client then sends the signon command to the Virtual Desktop Broker with the username and password as its parameter. If the signon is successful, the Virtual Desktop Broker server will send back the user.ini (User profile) file (if the signon is unsuccessful, the user is prompted again for username and password credentials). The signoff command will be sent when a user disconnects from the connection; and the shutdown command will be sent when a user turns off the thin client power.

For Virtual Desktop Broker features and information (including configuration and server support), refer to: http://www.leostream.com.

Configuring DHCP

The DHCP service provides all thin clients on the network with their IP addresses and related network information when the thin clients boot. DHCP also supplies the IP address and directory path to the thin client software images and user profiles located on the file servers.

Use of DHCP is recommended. However, if a DHCP server is not available, fixed IP addresses can be assigned (this does, however, reduce the stateless functionality of the thin clients) and the fixed IP addresses must be entered locally for each device (as described in "FTP Server Available (DHCP Server Unavailable)" and "Virtual Desktop Server Available (DHCP Server Unavailable)").

Be aware of the following:

- If a particular thin client is to function as an LPD print server, it can be assigned a fixed IP address. However, you can also guarantee that an LPD server will get the same IP address every time by making a reservation for that thin client in the DHCP server. In that way, you can preserve the stateless nature of the thin client and still guarantee a fixed address for the server. In fact, you can assign a symbolic name to the reservation address so that other thin clients can reference the LPD server by name rather than by static IP address (the symbolic name must be registered with a DNS server before other thin clients will be able to locate this LPD server). The thin client does not dynamically register its name and the DNS registration must be manual.
- The thin client uses port 80 as the default to access a Wyse Device Manager (formerly known as Rapport) server. If a port other than 80 is used to access a Wyse Device Manager server, use option 187 in the list of DHCP options in Table 1 (option for Wyse Device Manager server is option 186 in the list of DHCP options). Wyse Device Manager options are the only options used by the thin client that are not in text form.
- The thin client uses port 80 as the default to access a PNAgent/PNLite server. If a port other than 80 is used to access a PNAgent/PNLite server, the port number must be specified explicitly with the server location in the form IP:port or name:port (option for PNAgent/PNLite server is option 181 in the list of DHCP options in Table 1).
- Many DHCP options correspond to places in the network configuration UI where the thin client user can enter information manually. Be aware that wherever there is information in the UI and the thin client receives information about the same function from one or more DHCP options, the information received from the DHCP server will

replace the information contained in the UI. However, if the thin client does not receive information from the DHCP server about a particular function, the information manually entered in the UI will remain and will be used.

Guidelines for Windows Servers:

- You can use the DHCP tools available on the Windows server.

Guidelines for Linux Servers:

- Enter DHCP options 161 and 162 (described in Table 1) in `/etc/dhcpd.conf` (refer to the manual page `man dhcpd.conf` for more information on DHCP and the syntax of this file). For example, if you want the computer to search `ftp://132.237.16.157/pub/serversoftware/wnos`, you would add the following line to `/etc/dhcpd.conf`:

  ```
  option option-161 132.237.16.157;option option-162 "pub/
  serversoftware$";
  ```

  As mentioned in Table 1, the `/wnos` suffix is automatically appended to the FTP path, so you should not specify it explicitly. In this case, the actual directory searched will be `pub/serversoftware/wnos`.

The DHCP options listed in Table 1 are accepted by the thin clients.

Table 1 DHCP Options

Option	Description	Notes
1	Subnet Mask	Required. However, it is not is not required unless the thin client must interact with servers on a different subnet (MS DHCP requires a subnet mask and will always send one).
2	Time Offset	Optional.
3	Router	Optional but recommended. It is not is not required unless the thin client must interact with servers on a different subnet.
6	Domain Name Server (DNS)	Optional but recommended.
15	Domain Name	Optional but recommended. See Option 6.
28	Broadcast Address	Optional.
44	WINS servers IP Address	Optional.
51	Lease Time	Optional but recommended.
52	Option Overload	Optional.
53	DHCP Message Type	Recommended.
54	DHCP Server IP Address	Recommended.
55	Parameter Request List	Sent by thin client.
57	Maximum DHCP Message Size	Optional (always sent by thin client).
58	T1 (renew) Time	Optional but recommended.
59	T2 (rebind) Time	Optional but recommended.

Table 1 DHCP Options, Continued

Option	Description	Notes
61	Client identifier	Always sent.
161	FTP server list	Optional string. Can be either the name or the IP address of the FTP server. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to also be the FTP server.
162	Root path to the FTP files	Optional string. If the option provided by the server is blank and the server provides no value for the field, a null string is used. `/wyse/wnos` is automatically appended to the search path. For example, if you enter `pub/serversoftware`, the path searched will be `pub/serversoftware/wyse/wnos`. **Note:** You may have the `/wyse` automatic component of the search path omitted by appending a dollar sign ($) to the entered path. For example, if you enter `pub/serversoftware$`, the path searched will be `pub/serversoftware/wnos`. **Note:** The usage or omission of a leading slash (/) on the path is critical on some servers. Some servers limit access to the root path of the user specified at login. For those servers, the usage of the leading slash is optional. Some *NIX servers can be configured to allow the FTP user access to the entire file system. For those servers, specifying a leading slash specifies that access is to start at the root file system. Proper matching of the file specification to the FTP server in use is critical to ensuring proper operation. A secured Windows server requires the slash be specified in order to complete proper access.
180	Authentication server list	Optional string for Wyse Thin OS version 4.2. Not used for Wyse Thin OS version 4.3.
181	PNAgent/PNLite server list	Optional string. The thin client uses the server to authenticate the Windows credentials of the user and to obtain a list of ICA published applications valid for the validated credentials. The user supplies those credentials when logging in to the thin client (see "Using the User Profile ini File Command Set").

Table 1 DHCP Options, Continued

Option	Description	Notes
182	NT domain list for PNAgent/PNLite	Optional string. The thin client creates a pull-down list of domains from the information supplied in option 182. This list is presented at thin client login in the order specified in the DHCP option (for example, the first domain specified becomes the default). The selected domain is the one which must authenticate the user ID and password. Only the selected domain is used in the authentication process. If the domain list is incomplete and the user credentials must be verified against a domain not in the list (assuming that the server in option 181 is capable of authenticating against a domain not in the list), the user has the option of not using any of the domains specified in option 182 and typing a different domain name at the time of login (see "Using the User Profile ini File Command Set").
184	FTP Username	Optional string. Wyse Thin OS version 4.3 and later only.
185	FTP Password	Optional string. Wyse Thin OS version 4.3 and later only.
186	Wyse Device Manager (formerly known as Rapport) server list	Optional binary IP addresses. This option can specify up to two Wyse Device Manager servers. If two are specified, at boot time then thin client will attempt to check-in to the first server. If it cannot contact the first server it will try to check-in to the second server. Wyse Thin OS version 4.3 and later only.
187	Wyse Device Manager (formerly known as Rapport) server port	Optional number. Wyse Thin OS version 4.3 and later only.
188	Virtual Desktop broker server port	Optional string.

✓ **Note**

The thin client conforms to both RFC-compliant DHCP servers (RFC numbers 2131 and 2132) and RFC-noncompliant Microsoft servers (which NULL terminate strings sent to the thin client). The thin client supports both infinite leases and leases that expire (per RFC 2131 and others).

Configuring DNS

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. There are also DDNS implementations available for *NIX environments. However, the thin client does not do dynamic registration and therefore, requires a static or non-variant IP address and manual DNS registration in order to provide LPD support by name (for example, in the case where the thin client is used as an LPD printer server or if DHCP is not available). For DHCP entry of DNS domain and server location information, refer to "Configuring DHCP."

Configuring WINS

The thin client does not do dynamic registration and therefore, requires a static or non-variant IP address and manual Windows Internet Naming Service (WINS) registration. Use the network address of an available WINS name server. WINS allows the thin client user to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than WINS will be used to make the connection. These entries are supplied through DHCP if DHCP is used.

☑ **Note**

You may use two WINS server addresses, separated by a semicolon, comma, or space. The first address is for the primary WINS server and the second is for a backup WINS server.

Configuring Wyse Device Manager Servers

Wyse Device Manager (formerly known as Rapport) servers provide network management services to the thin client. Use the IP addresses or host names with optional TCP port number for Wyse Device Manager servers. Each entry with optional port number is specified in the form IP:port or name:port, where :port is optional; if not specified, port 80 is used.

About Configuring Session Services

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

✓ **Note**
A browser must be available through one of the session services to access any on-line help documentation for users.

Be aware of the following connection information:

- There can be more connections than desktop space to display them.
- Connections can be defined in persistent memory (with a statement reading `enablelocal=yes` in the wnos.ini file). These connections can be displayed as Desktop icons only in Stand-alone mode with a Non-privileged user.
- Only the connections defined in an ini file and containing an icon= clause will be displayed on the desktop (only if there is enough desktop space).
- Connections can be displayed on the desktop without sign-on (when you define these connections in a wnos.ini file or when the wnos.ini file does not contain a signon=1 statement).

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. ICA connects to NT TSE, Windows 2003 server, or Windows 2000 hosts that have a Citrix MetaFrame server, Citrix Presentation server, or CDS installed. Load balancing is included. ICA browsing or DNS can be used to resolve the server name.

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.

Remote Desktop Protocol (RDP), like ICA, is a network protocol that allows a thin client to communicate with the Terminal Server or Windows 2000/2003 Server with Terminal Services over the network. This protocol is based on the T.120 protocol suite, an international standard multi-channel conferencing protocol. The thin client supports both RDP version 4.x and version 5.x.

For information on configuring RDP, refer to "Configuring RDP Session Services."

Configuring ICA Session Services

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

- Windows 2000 or 2003 Server with Terminal Services and one of the following installed:
  - Citrix MetaFrame XP
  - Citrix Presentation Server

Use the instructions accompanying these products to install them and make sessions and applications available to the thin clients sharing the server environment. If PNAgent/PNLite-published application services are to be made available to the thin clients, refer to "PNAgent/PNLite Installation Guidelines" when installing Citrix MetaFrame XP.

Be aware of the following:

- If a Windows 2000 or 2003 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere on the network. The server will grant a temporary (90-day) license on an individual device basis. Beyond the temporary (90-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).
- Any ICA connection which traverses a Dial-up or WAN connection, generally should have the **Optimize for low speed link** option selected in the user profile or the Connection Settings (ICA) dialog box.
- If an ICA connection is created using the Connect Manager and the Host Names or Application Name text box is left blank, a message appears prompting the user to enter the IP Address or Server Name of the ICA server to which to connect.
- An audio input port is available (Audio can be recorded).

PNAgent/PNLite Installation Guidelines

PNAgent/PNLite is a component of the Citrix XML publishing service. PNAgent/PNLite is an ICA connection mode that enables the thin client to connect to applications available (published) on an ICA server without having to configure connections for individual published applications.

Use the following guidelines during installation:

- **MetaFrame XP** - supports XML publishing services and during installation presents a series of prompts. During installation, you will be given an option to install the XML publishing service. Clicking **Yes** to this option allows you to change the default port (80) used by the service.
- **Citrix Presentation Server** - supports XML publishing services and during installation presents a series of prompts.

The port to be used for XML publishing services must be known for making the PNAgent/PNLite server location entries as appropriate to the operating mode requirements (for related information, refer to "Configuring DHCP," instruction on locally configuring the thin client Network Setup dialog box, and the "Using the User Profile ini File Command Set"). The thin client uses port 80 as the default, but if a port other than 80 is used, the port number must be specified explicitly with the PNAgent/PNLite server location in the form IP:port or name:port.

Configuring RDP Session Services

RDP session services can be made available on the network using any of the following services:

- Windows 2000 or 2003 Server with Terminal Services installed
- Windows NT 4.0 Terminal Services (WTS) Edition
- Windows XP

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

Be aware of the following:

- If a Windows 2000 or 2003 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere on the network. The server will grant a temporary (90-day) license on an individual device basis. Beyond the temporary (90-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).
- Any RDP connection which traverses a Dial-up or WAN connection, generally should have the **Optimize for low speed link** option selected in the user profile or the Connection Settings (RDP) dialog box.
- If an RDP connection is created using the Connect Manager and the Host Names or Application Name text box is left blank, a message appears prompting the user to enter the IP Address or Server Name of the RDP server to which to connect.
- Wyse Thin OS version 4.2 and later supports an RDP connection with no encryption (found in older versions of Microsoft NT4-TSE servers).
- Wyse Thin OS version 4.2 and later supports server browsing over Server Message Block (SMB) when defining an RDP connection. SMB browsing restrictions mean that the server desired may not be listed, in which case the user will need to know either the name or IP address of the target server and type that information into the text box (as it will not appear in the pull down list).

3 System Administration

This chapter provides system administration information, remote management information, and detailed system command and parameter configurations, to help you design and manage a Wyse® Winterm™ 1 series Thin Client environment.

✓ **Note**
The password for the BIOS is Fireport.

Updating Software

The software version is embedded in both the RAM and flash memory images. This version information is used to compare the images on the FTP server to the currently-loaded flash image on the thin client. A major revision number supersedes a minor revision number when making the comparison. In turn the minor version number takes precedence over the build number.

After obtaining software updates from Wyse, you must replace the existing software images in the wnos subdirectory on the FTP server to allow the thin clients to automatically detect and self-install the new software (upon thin client system start). The FTP server address and exact path to these files are specified in DHCP Options 161 and 162 (if DHCP is not used, the path is specified in the Network Setup dialog box).

Each time a thin client boots, it checks the software images on the FTP server, and if configured, automatically performs an update if a newer version is detected. Whether or not an update is performed depends on the AutoLoad setting in the Global profile (wnos.ini) as described in "Using the User Profile ini File Command Set." The image names and date-time stamps determine whether or not the update is newer than the version currently installed on the thin client.

There is a significant distinction between using DHCP and not using DHCP to access the various necessary files.

- If DHCP is used, the thin client software automatically inserts the path component `/wyse` following what it receives from the DHCP server (unless the path is terminated by a $); this is done only if a value is received from DHCP.
- If DHCP is not used and the configuration is done manually, the full path up to the wnos component must be inserted; there is no automatic `/wyse` insertion and no $ processing.
- For users familiar with the Wyse 3 series Thin Clients, the Wyse 3 series equipment does processing on both DHCP and manual input, as well as $ processing (as $ is a legal meta-character in manually entered strings). Wyse Thin OS software does not recognize a $ terminator as a legal meta-character in a locally entered string.

✓ **Note**
Citrix does not supply an ICA client for the Wyse thin client platforms. Citrix ICA auto-update does not function for the ICA client installed on the thin client; the ICA client is fully contained in the thin client system and can only be updated by changing that entire system. The RDP client is also not replaceable.

☒ **Caution**

Interrupting power during the update process can corrupt the FLASH on the thin client. Thin clients with corrupted FLASH must be shipped to Wyse for service.

Understanding the Software Update Processes

After a thin client has booted from the image stored locally in flash memory and has made its anonymous connection to your file server, the following processes occur for the default **AutoLoad value = 1**, cases where no wnos.ini file is found, and cases where a wnos.ini file is found which does not contain the keyword:

☑ **Note**

All thin client units using a particular file server are identically updated. There is no distinction between thin clients in this regard. If Autoload is enabled (value = 1 or 2), an update cannot be prevented from occurring. The software update process is governed by the AutoLoad value as follows.
AutoLoad value = zero - no update checking is done; the version (image/ software) is never updated.
AutoLoad value = 2 - the software update process identifies code which is newer than the one which is installed on the thin client. The code identifier is split into 4 parts, the major release identifier, the minor release identifier, the build number identifier, and the sub-build number identifier (if the sub-build number is 0, it will not be displayed). Each part is compared against the current code internal identifier in the same format. If the file identifier is greater, the update is performed. If the file identifier is less, the update is abandoned. If the file identifier is equal, the next term is examined until the build identifiers are found to be equal and the update is abandoned. This comparison process using the build number can be important in cases where you are using a beta release, or in cases where you need to reinstall a release with the same major and minor numbers but with an updated build.

Model 1125SE:

1. If called for, the thin client first looks for in the wnos directory for TWA_wnos. If this file exists and it has a different internally encoded version number than the image currently in flash memory, depending on the wnos.ini file AutoLoad setting (the default AutoLoad value is 1) the thin client will load this image into NAND flash and reboot.
2. The thin client will then (regardless of any circumstance in step 1) check for a file named TWA_boot. and, again, updates if appropriate. If an update is done the thin client will again reboot.

☑ **Note**

TWA_boot loads in the 256K NOR image while TWA_wnos loads the NAND flash image. Both of these files can be updated in the thin client through an FTP file server.

Models SX0 and VX0:

1. If called for, the thin client first searches in the wnos directory for RCA_wnos. If this file exists with a different internally encoded version number than the image currently in flash memory, and depending on the wnos.ini file AutoLoad setting (the default AutoLoad value is 1), the thin client will load this image into flash and reboot.
2. The thin client will then (regardless of any circumstance in step 1) check for a file named xperess.rom and again updates if appropriate. If an update is done, the thin client will again reboot.

Resetting to Factory Defaults Using G-Key Reset

High-privileged or Stand-alone users can reset the thin client to factory default settings using the **G**-key reset.

To reset the thin client to factory default settings, restart the thin client and continuously tap the **G** key during the restart process. G-key reset impacts all configuration items, including but not limited to both network configuration and connections defined in local NV-RAM.

✓ **Note**

G-key reset is disabled for Low-privileged and Non-privileged users in Lockdown mode.

Resetting to Factory Defaults Using Shutdown Reset

A High-privileged or Stand-alone user may reset the thin client from the Sign-off/Shutdown dialog box as follows:

1. Select either the **Shutdown and Restart the system** or the **Shutdown the system** option.
2. Select the **Reset the system setting to factory defaults** check box.
3. Click **OK**.

Shutdown reset impacts all configuration items, including but not limited to both network configuration and connections defined in local NV-RAM (Terminal name will not change). Shutdown reset is disabled if the current user is Non-privileged or Low-privileged, regardless of lockdown state.

Resetting Display Settings Using V-Key Reset

If the display settings are inappropriate for the particular monitor that is connected, it is possible that the display will not function properly when the thin client restarts. To correct this, power-on the thin client while continuously tapping the **V** key. This will restart the thin client with a display resolution of 640 x 480 pixels and a 60 Hz refresh rate.

Enabling a Disabled Network Setup Dialog Box

Although there are privileges and user modes associated with user access to thin client resources (see "Understanding User Accounts and User Profile Ini Files"), access to network setup (Network Setup dialog box) depends upon privilege level. A Stand-alone user either is by default a user with High privilege or has a thin client that is locked down. A Guest user has implicit privilege (of None) and all access is governed by that privilege. A PNAgent/PNLite only user has whatever privilege was set in the wnos.ini file at boot, whatever privilege was locked down at the last access of a wnos.ini file, or High privilege (by default).

If the .ini file Privilege command is set to Low or None, the thin client Network Setup dialog box will be disabled (the user cannot access it). There may be occasion to access the Network Setup dialog box (without changing the .ini file) when this condition exists. This situation could occur, for example, when you need to change to another FTP or Virtual

Desktop file server or add to the PNAgent/PNLite servers list. To access the Network Setup dialog box in such a case, disconnect the network cable and reboot the thin client to Stand-alone user mode. The Network Setup dialog box displays after the thin client initializes and you can then make the required entries (be sure to reconnect the network cable and reboot when finished).

Caution

If a thin client accesses the enterprise intranet through Dial-up, PPPoE, or PPTP VPN and the thin client is locked-down, a non-privileged or low-privileged user attempting to reboot to Stand-alone User mode will disable the Network Setup dialog box and System Reset capabilities. The user will not be able to re-access the enterprise intranet through this path. If this happens, the thin client must be moved to a location where it can access the enterprise intranet directly (Ethernet cable) and reboot so that you as an administrator can make any required changes to the thin client operating configurations (for example, set the profile to unlock the thin client) through the User profiles.

If the thin client is configured for Dial-up access, there must be an RAS server answering the configured telephone number. Otherwise, the thin client will require factory attention to recover it.

Rebooting Thin Clients Remotely

Wyse Device Manager (formerly known as Rapport) software can be used to remotely reboot thin clients. For information on Wyse Device Manager software, refer to "Using Wyse Device Manager Software For Remote Administration."

Understanding System Lockdown Operations

Lockdown status for a thin client is set or removed using the lockdown clause of the privilege statement. Lockdown establishes the default privilege level following thin client boot and before any privilege statement is read from an ini file. Access to many facilities is affected by the privilege level.

Non-Lockdown Operation

For normal operation, Low-privileged and Non-privileged users may access the Network Setup dialog box by temporarily disconnecting the Ethernet cable from the thin client and rebooting to Stand-alone user mode. The Network Setup dialog box can also be accessed by a G-key reset to factory default in addition to the system reset check box (available to any user with sufficient privilege to the Sign-off/shutdown dialog box).

Lockdown Operation

In most cases, access to the resources available when the system is not locked down is desirable; however, network environments requiring maximum security should not permit uncontrolled changes to thin client network access. Most facilities would include a privilege/lockdown statement in wnos.ini and might override the privilege in a user ini file without modifying the lockdown privilege. Thus, an administrator could log into any unit and have sufficient privilege to modify the configuration of that unit without altering the default privilege at the next reboot.

Caution

If the unit is configured for Dial-up access, there must be an RAS server answering the configured telephone number. Otherwise, the unit will require factory attention to recover it.

Using Wyse Device Manager Software For Remote Administration

Wyse Device Manager (formerly known as Rapport) software is a full-featured remote administration tool set available from Wyse Technology. The software accesses your thin client through the factory-installed Wyse Device Agent and Preboot Execution Environment (PXE) client utilities. PXE upgrade services and a Virtual Network Computing (VNC) Viewer are built into Wyse Device Manager software. Wyse Device Manager software allows the thin client administration functions (including firmware upgrades) to be performed without requiring an administrator to visit the individual thin client sites. For information on installing Wyse Device Manager software and configuring the server environment, refer to the Wyse Device Manager software documentation.

✓ **Note**

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

Wyse Device Manager software can be used to do the following operations:

- **Remote Reboot** - Wyse thin clients can be rebooted remotely using the Wyse Device Manager administration software.
- **Wake-On-LAN** - Your power-connected thin client can also be turned on by the Wake-On-LAN feature. Using this feature within a single Ethernet subnet, an administrator can turn on the thin client connection by using a LAN message that the thin client recognizes.

Understanding User Accounts and User Profile Ini Files

User profile .ini files are created and maintained by you the network administrator and are stored on the file server. There will be one wnos.ini file available to all users globally and there will be a unique {username}.ini file for each user under the subdirectory ini of wnos. The thin client accesses the Global wnos.ini file upon device initialization and accesses any applicable unique {username}.ini file when the user signs on. These files must be created and maintained using an ordinary ASCII text editor. Icons and logos specified in the configuration .ini files must be placed in the file server `/wnos/bitmap` subdirectory as described in "About Icons and Logos."

About Icons and Logos

Icons and logos specified in the configuration .ini files must be placed in the file server `/wnos/bitmap` subdirectory. Icons are specified in the icon clause of the connect statement and logos are specified in the FormURL statement. Supported image file types include .ico (icon), .bmp (bitmap), .jpg (JPEG), and .gif(GIF). Color depth for logos can be up to 256 colors. Color depth for icons can be 16 colors. It is recommended that .jpg format not be used for desktop icons.

Use the following guidelines:

- Typical desktop icons are 64 x 48 Pixels
- Typical sign-on logos are 100 x 61 Pixels, with transparent background
- Maximum-Size for sign-on logos are 352 x 80 Pixels (if smaller than this, it will be positioned at the top-left corner).

Using the User Profile ini File Command Set

The following sections provide information about the user profile `.ini` file command set.

- "About wnos.ini"
- "About {username}.ini"
- "Using the Sample .ini Files"
- "Knowing the General Rules of the ini Files"
- "Commands and Parameters - wnos.ini Only"
- "Commands and Parameters - wnos.ini and {username}.ini"
- "ICA and RDP Connect Parameter List"

Note

If you are using a Virtual Desktop file server, use the FTP commands and parameters shown as you normally would for an FTP server.

About wnos.ini

The `wnos.ini` file contains Global parameters for all thin clients accessing the file server. Commands in both Table 2 and Table 3 can be used in `wnos.ini`, but the commands in Table 2 are used only in `wnos.ini` and not in `{username}.ini`.

About {username}.ini

The `{username}.ini` file contains the connection profile for an individual user. Parameters in the User profile generally supersede the identically named Global parameters. However, Global parameters in Table 3 noted with * supersede the identically named User profile parameters. After user sign-off, User profile parameters in Table 3 noted with ** return to their original value set in wnos.ini.

Note

If both PNAgent/PNLite and a user profile are being used, the username must be defined in the Windows domain to be used, and the password must be the same for the domain and the profile.

Using the Sample .ini Files

Sample User Configuration Profile files (.ini files) are available from Wyse. These sample files are annotated to allow you to use them as a starter set on your file server and can be modified to suit your needs. The sample files are available on the Wyse Web site at: http://www.wyse.com/products/winterm/reference/1series.

Knowing the General Rules of the ini Files

General rules of the `.ini` files include the following:

- Commands and parameters can be entered for reference as necessary but are not mandatory unless changes from defaults are required. Certain parameters to the `Connect=` commands are mandatory and are noted in Tables 2 through 4.
- Commands and parameters must always be separated by spaces, regardless of the command.
- Blank lines can be used to enhance readability.
- Use \ as the last character at the end of a line (that is, `\<Enter>`) to indicate line continuation. There must be no white space between the \ and the `<Enter>` character. However, white space between parameter entries must be maintained. If the `\<Enter>` is not separated by at least one space from the last character of the line, the next line must start with a space or have the first set of characters concatenated with the last set from the continued line. For this reason, it is recommended that all continuation lines start with at least one space character. If all commands start at the left margin and all continuation lines have at least one leading blank, the indentation will enhance the readability of the `ini` file.
- The # character may appear anywhere on a line and all following characters (including those on continuation lines) are commented out until the end of the command is reached.
- String parameters containing white spaces must be placed within quotation marks (use common-practice nesting rules).
- For parameter list selections of type `{0, 1}`, `0` indicates false or no, and 1 indicates true or yes, as applicable. The older `{0, 1}` format is equivalent to and may be used instead of the {no, yes} format where indicated in Tables 2 through 4.
- For a URL parameter type, the parameter is assumed to point to a file under the thin client's home directory. The home directory is the `wnos` subdirectory for the log-in (you can specify username and password for file server access) of the file server that is specified by the File Server entry in the Network Setup dialog box. If a File Server directive is processed, the same user ID and password already configured on the thin client must be usable for accessing files on the new file server.
- Use semicolons or commas for list separators (such as for the list of ICA browsers).
- All `{username}.ini` files must be write-enabled to allow the thin client to place the encrypted user passwords in the files.
- The combined number of connection entries defined in a `{username}.ini` file and the `wnos.ini` file cannot exceed a defined total maximum number of connections. The maximum number of connections has a default limit of 216, but can be set from 100 to 1000 through wnos.ini.

Note

{username}.ini Only - The command which is valid in {username}.ini only is the password command. If it is present, it must be the first command in the file. It is created and updated by the thin client; it is not inserted by the administrator. When the Change Password check box is checked in the log-in dialog box, the user is prompted for a new password. The thin client checks to ensure that the two copies of the password are the same, encrypts the password, places it at the beginning of the user's ini file (replacing any previous password command), and writes the file back to the file server. If the user forgets the password, the administrator may edit the appropriate ini file, delete the password command and save the result. Then the next time the user attempts to log in, no value should be placed in the password field of the log-in dialog box. Because the password is encrypted using a one-way algorithm, the original password value can not be recovered from the ini file. A new password must be created.

Commands and Parameters - wnos.ini Only

Table 2 lists the Command/Parameter and Description set for `wnos.ini` only.

Table 2 wnos.ini Only

Command/Parameter	Description
AddCertificate=filename	Specifies a certificate file residing in the subfolder `cacerts` under the wnos folder to load on the nand flash device (on platforms with nand flash), or on the memory. This is required when configuring the Citrix Secure Gateway PNAgent Interface (PNAgent/Lite servers) in the Network Setup dialog box. Adding certificates are required if the user CSG environments use certificate agents that are not covered by the built-in certificates. The certificates are used to validate server identities by the thin client.
AutoLoad=[0, **1**, 2]	Selects firmware update mode. **Value and Action** 0 — Disable checking for image **1 — Enable firmware upgrade/downgrade (default)** 2 — Enable upgrade only
AutoPower={yes, **no**}	Controls how the system starts when the power is first applied to the thin client. If it is set to yes, the system starts itself without waiting for users to press the power button only in cases where the power was lost unexpectedly (if the unit was shut down properly before power was removed, when the power is restored, the unit will remain powered off). This setting is useful in a kiosk environment. The factory default is AutoPower=no. Once an AutoPower statement is processed, it alters the behavior of the thin client until a countermanding statement is processed. The effect of an AutoPower=`yes` statement continues even if the statement is removed from the ini file in which it was found. Use of the AutoPower option does not interfere with performing a user directed shutdown.
Community = community	Specifies the SNMP community name. A string of up to 31 characters. Once specified, it is saved in the non-volatile memory.
DefaultUser=username	Default sign-on user. Note that this user name is displayed in the Sign-on dialog box and may be either used or replaced.
DelCertificate={filename, all}	Removes the named file from the nand flash or from the memory. If DelCertificate=ALL, then all certificates will be deleted from the flash.

Table 2 wnos.ini Only, Continued

Command/Parameter	Description
DHCPOptionsRemap={yes, **no**} [FileServer={128-254}] [RootPath={128-254}] [FtpUserName={128-254}] [FtpPassWord={128-254}] [RapportServer={128-254}] [RapportPort={128-254}] [PnliteServer={128-254}] [DomainList={128 -254}] [VDIBroker={128 -254}]	If DHCPOptionsRemap=yes, the following parameters can be set (otherwise, they cannot). The options value must be between 128 and 254. Each value must be different. These options are used to configure DHCP server tags for thin client booting
DHCPVendorID = vendor	Specifies the vendor ID used for DHCP.
DisableButton={yes, no}	Disable power button.
DisableDomain={yes, no}	Disable the drop-down domain list in the PNAgent/PNLite Sign-on dialog box.
DomainList=List of NT domain names	A list of domain names that will appear in the thin client Sign-on dialog box as a selectable list to help users in selecting the domain to sign on to PNAgent/PNLite servers. Once specified, it is saved in the non-volatile memory. Enclose in quotation marks if spaces are included. For example: DomainList=”North_America, SQA, test-domain”
Dualhead={yes, no} [Mainscreen={1, 2}] [Orientation={hort, vert}]	(For supported dual monitor capable thin clients only) Set Dualhead to yes to support dual-monitor. The optional keyword Mainscreen sets which screen is used as the main screen. The optional keyword Orientation sets which style is used for display (hort means horizontal and vert means vertical).
EnableGKey={yes, no}	Enable or Disable G key reset. G key reset is supported for Privilege=High.
FileServer={IP address, DNS name}	This FTP server IP address or DNS name is entered into thin client local setup (non-volatile) and the thin client immediately uses this server to access files. Note that the target file server must support access using the same user ID as there is no way to change user ID and/or password in the ini files.
FormURL=URL to a file	URL to a sign-on window form or a bitmap filename displayed in the sign-on window under the thin client home directory. If auto dial-up is enabled, this statement is invalid. Default=Empty.

Table 2 wnos.ini Only, Continued

Command/Parameter	Description
Include=$mac	Load "/wnos/inc/mac-address.ini". **NOTE:** The file name does not include the symbol : in the mac address.
LongApplicationName={yes,no}	Set to yes to display all 38 characters in a desktop icon name. Otherwise, icons display up to 19 characters (the last three characters will be … if over 19 characters).
MaxVNCD={0 - 5}	This command is for Wyse Thin OS version 4.3 and later only. **Default = 1**. Set to 0 to disable shadowing, or a non-zero absolute count of the number of concurrent VNC sessions. The maximum count value allowed is 5.
Multifarm={yes, no}	wnos.ini supports Citrix multifarm functionality. When activated (multifarm=yes), PNAgent/PNLite users are able to authenticate to more than one Citrix farm.
MultiLogon={yes, no}	If set to yes, the PNAgent/PNLite sign-on authenticating window can input a different username, password, and domain while signing on to different PNAgent/PNLite server.
NoticeFile = filename	Specifies a legal notification file residing in the home folder as wnos.ini. The file is displayed in a dialog box, the user is prompted to accept before the sign-on process to continue.
PasswordServer=icaserver	Specify an ICA server that can be logged-on to modify a password when a user signs-on with a password timeout.
PrinterMap=a text file name (or possibly URL)	A text file to be included to define printer mappings. Each line in the file is of format Printer Identification=Printer Driver Name. For example: HL-1240 Series=HP LaserJet.
RapportDisable={yes, no}	Set to yes to disable the Rapport agent.
RapportServer=server_list	Specifies a list of IP address or DNS names (separated in comma) for the Wyse Device Manager (formerly known as Rapport) servers. Once specified, it is saved in the non-volatile memory.
RootPath=FTP root path	This FTP root path is entered into thin client local setup (non-volatile) and the thin client immediately uses this path to access files. The directory name \wnos will be appended to the FTP root path entry before use.

Table 2 wnos.ini Only, Continued

Command/Parameter	Description
SignOn={**yes**,no, NTLM} [MaxConnect=max] [ConnectionManager={maximize, **minimize**, hide}] [EnableOK={yes,no}] [DisableGuest={yes,no}] [DisablePassword={yes,no}] LastUserName={yes, no}	Yes/no choice to enable the sign-on process. Default=`yes` (enabled). If set to `NTLM`, user can be authenticated with NTLM protocol. The optional keyword `MaxConnect` sets the maximum number of connects allowed to be specified in the wnos.ini and username.ini together. The range allowed for the max is 100 to 1000. The default maximum is 216 entries. The optional parameter `ConnectionManager` sets the state of the Connect Manager during sign-on. The optional parameter `EnableOK` sets to show the OK and Cancel command buttons in the Sign-on dialog box. The optional parameter `DisableGuest` sets whether or not guest sign-on is disabled. The optional parameter `DisablePassword` sets whether or not to disable the password text box and password check box in the Sign-on dialog box. The optional keyword `LastUserName` sets to whether or not to display the last sign-on username after the user logs off.
Speedbrowser={**on**, off}	Enables ICA Speedscreen Browser Acceleration Function. Default=`on`.
SysName={client, DNS}	If set to DNS, a reverse DNS name from the DNS server is checked into the Wyse Device Manager (formerly known as Rapport) server (by default, the terminal name is checked in).
TcpTimeOut={**1**-255}	The Tcp Timeout option configures the timeout value of a TCP connection. The value must be between 1 and 255 (which means the connection timeout value is from 1x30 seconds to 255x30 seconds).
ThinPrintEnable={**yes**, no} [Port=port number]	Set to no to disable the thinprint client. The option Port sets the TCP port of thinprint. The default is 4000. The port number must be less than 65535.

Table 2 wnos.ini Only, Continued

Command/Parameter	Description
TimeZone=zone [ManualOverride={yes, no}] [daylight = {yes, no}] [start=mmwwdd end=mmwwdd] [TimeZoneName=timezonename] [DayLightName=daylightname]	This statement is valid if the zone is Unspecified on the thin client or with the ManualOverride option parameter. The allowable zones are referred to in the menu list in the System Preference dialog box such as: 'GMT – 12:00' to 'GMT + 13:00' at one hour increment, 'GMT + 03:30', 'GMT + 04:30', 'GMT + 05:30', 'GMT + 05:45', 'GMT + 06:30', 'GMT + 09:30', 'GMT – 3:30' and 'Greenwich Mean Time'. The option parameter ManualOverride overrides the terminal System Preference Menu setting with this TimeZone wnos.ini file setting. If EnableLocal=yes is set in wnos.ini, the TimeZone setting in wnos.ini will be saved into nvram. The option parameter Daylight is to enable/ disable the daylight saving. The mmwwd is a 6 digit number to specify the start and the end of daylight saving. Mm – 01 to 12 for the month of the year from Jan. to Dec. For example, 01 is January. Ww – 01 to 04 for the week of the month, 05 is the last week. For example, 01 is 1st week. Dd – 01 to 07 for the day in the week from Monday to Sunday. For example, 01 is Monday. The parameter daylight, start and end must be specified as their sequence. The option parameter TimeZoneName is the display name sent to the ICA/RDP session such as Eastern Standard Time. If the time zone enables the daylight saving, the option parameter DayLightName should be something like Eastern Daylight Time, otherwise it should be the same as TimeZoneName. **NOTE:** To configure daylight saving for an RDP session, you must enable the Allow Time Zone Redirection function. Use the following guidelines: Run *gpedit.msc* to open the Group Policy dialog box. Click **Computer Configuration** in the Local Computer Policy tree. Expand the Administrative Templates folder. Expand the Windows Components folder. Expand the Terminal Services folder. Click **Client/Server data redirection** to open the Setting list. Right-click **Allow Time Zone Redirection** and select **Properties** to open the Allow Time Zone Redirection Properties dialog box. Select the **Enabled** option, and then click **OK**. Close the Group Policy dialog box.
VncPassword = password	Specifies a string of up to 16 bytes as the password for shadowing.

Commands and Parameters - wnos.ini and {username}.ini

Table 3 lists the Command/Parameter and Description set for both `wnos.ini` and `{username}.ini`.

☑ **Note**

Global parameters in Table 3 noted with * supersede the identically named user profile parameters. After user sign-off, user profile parameters in Table 3 noted with ** return to their original value set in wnos.ini.

Table 3 wnos.ini and {username}.ini

Command/Parameter	Description
AltCacheDisable={yes, **no}	If set to `yes`, the new cache mechanism will be disabled allowing more memory to be available to a user (developed with Citrix Presentation Server 4.0 and Windows 2003 Server). Default=`no` (new cache mechanism is enabled).
**Alternate={yes, no}	Set to `yes` to use an alternate IP address returned from an ICA master browser to get through firewalls. Default = `no`. This setting in wios.ini will be saved into nvram if EnableLocal is set to `yes` in wnos.ini
**AutoSignoff={yes, no} [Shutdown = {yes, no}]	Set to `yes` to automatically sign-off a user when the last opened session is closed. Optionally, shutdown the thin client.
ClearLicense={yes, no}	Set to `yes` to clear the TSCAL license stored in the non-volatile memory. It can be replaced by FixLicense=clean.
Connect={ICA, RDP}	Connection protocol. Follow the selections from the ICA/RDP parameter list (refer to Table 4). Parameters marked with an asterisk * are mandatory. All connect parameters for each connection must be on the same logical line (\ may be used for line continuation - see rules as described in "Knowing the General Rules of the ini Files").
**DefaultPrinter={LPD1, LPD2, LPD3, LPD4, COM1, COM2, LPT1, LPT2, SMB1, SMB2, SMB3, SMB4}	Set default printer. Be sure the printer set as default is enabled or the setting will be invalid.
**DeskColor=rrr ggg bbb	Specifies the desktop background color in RGB string format (must be enclosed in quotes), where `rrr`, `ggg`, and `bbb` are decimal numbers in the rage of `0` to `255`. Default = “16 100 36” (green).

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
Desktop=*bitmap file* [Layout = {center**, tile}]	The `Desktop` command specifies a bitmap file to be used as wallpaper for the local desktop. This file could be a 4-bit, 8-bit, or 24-bit BMP file or a standard GIF file or a standard JPEG file. The file must be located in the FTP server `wnos\bitmap` directory. Default is no wallpaper. `Layout` is a parameter of the `Desktop` command. It specifies the arrangement on the desktop background of the bitmap file specified by the `Desktop` command. For the `tile` section, the image is replicated across the desktop. Default = `center`. If auto dial-up is set, it will be invalid.

Device=audio
volume={high, **middle**, low} or {0-25}
mute={**0**, 1, 2}
	Specifies the local audio volume.
	high is the maximum volume, middle is medium volume (default), and low is minimum volume. The values between 0-25 allows you to set the exact volume level.
	mute={0, 1, 2} sets the Mute check box in GUI (you can also select the volume Mute check box by using the GUI). If mute=2 is set it will disable audio and system beep.

*Device=Ethernet [Speed=speed] [MTU=mtu]	Speed is either Auto, 10M HD, 10M FD, 100M HD or 100M FD. This parameter is the same as EthernetSpeed. If it is set in wnos.ini, the statement in the [username].ini will be disabled. mtu is a value between 500 to 1500.
**Device=keyboard [numlockoff={yes, no}] [repeatrate={0-2}] [repeatdelay={0-7}]	Specifies the local keyboard. numlockoff=`yes` turns off the NumLock of the keyboard. repeatrate={0-2} sets the repeat rate to Slow (0), Medium (1) or Fast (2). Default = 1. repeatdelay={0-7} sets the repeat delay to 1/5 second (0), 1/4 second (1), 1/3 second (2), 1/2 second (3), 3/4 second (4), 1 second (5), 2 second (6), or No Repeat (7). Default = 2. This setting in wnos.ini will be saved into nvram if EnableLocal is set to `yes` in wnos.ini.
Device=Wireless [Mode={Infrastructure, AdHoc}] [SSID=ssid Channel={1-14}] [WepKey={None, 1-4}] [Key1=k1] [Key2=k2] [Key3=k3] [Key4=k4]	Defines wireless Ethernet device remotely. Not all parameters are needed. The values of k1 to k4 are any real value of 5 to 13 characters or 10 to 26 Hex digits. For example, you can define Key1 to have a key of `k1` and omit Key2, Key3, and Key4, in which case WepKey must equal 1.

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description

**DisableMouse={yes, no}
Or
MouseDisable={yes, no}
	Value and Disabled
	no — Mouse is enabled (default)
	yes — Mouse is disabled and no mouse pointer is shown on the screen. The pointer is enabled if any mouse activity occurs.

EnableLocal={yes, **no)	Set to yes to enable locally configured entries to show in the Connect Manager list (that is, activate local entries). Default = no. When connections defined in local NV-RAM are displayed in the Connect Manager, they are marked with an asterisk. Set to yes in wnos.ini will save the global information into nvram. The global information includes: SEAMLESS, ALTERNATE, Reconnect, IcaBrowsing, LowBand, NoReducer, Time settings, and Printer settings in wnos.ini.
*EthernetSpeed={Auto, 10M HD, 10M FD, 100M HD, or 100M FD}	Specify the Ethernet speed to either Auto, 10M HD, 10M FD, 100M HD, or 100M FD. Once specified, it is saved in the non-volatile memory. If changed, the system reboots. This statement can be replaced by Device=Ethernet Speed=speed.
FactoryDefault={**no**, yes}	Set to yes to reset the system setting to factory default (the option is only initialized once for each firmware change, however, you can set to no and then reboot so the option will be initialized again). Default is no.
FastDisconnet={yes, no}	If set to yes, pressing F12 will disconnect an ICA session.
FastDisconnetKey={F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12}	Set the disconnect key that will disconnect an ICA session.
FixLicence={Factory, clean, yes, no}	Set to replace the TSCAL license stored in the non-volatile memory.
HideIP={yes, no}	Set to yes to hide some information of the connection host or IP. Some examples of this include: When moving a mouse cursor over the connection icons on the desktop, a balloon help pop-up displays '…' instead of the host name. When a Reconnect to a connection message or an ICA error message window displays, the connection description displays instead of host name. When moving a mouse cursor over the PN icon, the connected PN servers do not display.

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
**ICABrowsing={udp, http}	Establishes the default browsing protocol. Default is udp. This setting can be overridden by the parameter HttpBrowsing={yes,no} in each connection property. The method of browsing selected must match the method provided by the server(s) being accessed. This setting in wmos.ini will be saved into nvram if EnableLocal is set to yes in wnos.ini.
**Inactive={10 to 480} (minutes)	**Default =0**. No Idle timeout=0, range = 10 minutes to 480 minutes.
*Include=path/filename	Include another .ini file at the position of this command. Only one level of including is allowed (no nesting) and only for username.ini.
**Language=code Charset={ISO-8859-1, ISO-8859-7}	Once specified in wnos.ini, it is saved in non-volatile memory. Set Charset={ISO-8859-7} to support Greek language on the desktop display. Default is ISO–8859-1. **Description and Code** Arabic (Saudi Arabia) — Ar_sau Arabic (Iraq) — Ar_ira Arabic (Egypt) — Ar_egy Arabic (Libya) — Ar_lib Arabic (Algeria) — Ar_alg Arabic (Morocco) — Ar_mor Arabic (Tunisia) — Ar_tun Arabic (Oman) — Ar_oma Arabic (Yemen) — Ar_yem Arabic (Syria) — Ar_syr Arabic (Jordan) — Ar_jor Arabic (Lebanon) — Ar_leb Arabic (Kuwait) — Ar_kuw Arabic (U.A.E.) — Ar_uae Arabic (Bahrain) — Ar_bah Arabic (Qatar) — Ar_qat Brazilian — br Canadian Multilingual — ca_ml Chinese (Simplified) — gb Chinese (Traditional) — b5 Croatian — croat Czech — cz Danish — dk Dutch — nl Dutch (Belgian) — nl_be English (Australian) — au English (3270 Australian) — au3270 English (New Zealand) — nz English (United Kingdom) — uk **English (United States) default — us**

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
(continued) **Language=code Charset={ISO-8859-1, ISO-8859-7}	Finnish — fi French (Belgian) — fr_be French (Canadian) — fr_ca French (France) — fr French (Swiss) — fr_sf German — de German (IBM) — de_ibm German (Swiss) — de_sg Greek — el Hungarian — hu Italian — it Italian (Swiss) — it142 Japanese — jp Korean — ko Norwegian — no Polish (214) — pl Polish Programmers — pl_prog Portuguese — pt Portuguese (Brazil) — pt2 Romanian — ro Slovakian — slovak Slovakian (Qwerty) — sk_q Slovenian — sloven Spanish — es Spanish (Mexican) — la Swedish — se Turkish — turk Turkish (QWERTY) — turk_q U.S. International — us_int
LowBand={no**, yes}	Establishes the default setting for all connections. yes or no choice to enable optimization for low speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Default = no (disabled). This setting in wnos.ini will be saved into nvram if EnableLocal is set to yes in wnos.ini.
LpdSpool={0 to 10}	Specifes the size of spool to buffer all data before sending it to the LPD printer. **Default = 5**. range = 0 MB to 10 MB.
MouseSpeed={0,1**, 2}	**Value and Mouse Speed** 0 — Slow **1 — Medium (default)** 2 — Fast
**MouseSwap={0, 1}	**Value and Mouse Swap** **0 — No (default)** 1 — Yes

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
NetworkPrinter=host/queue [PrinterID=Window driver name] [Enabled={**yes**, no}]	Specifies the configuration for the network (LPD) printer in the same way as described for the Printer Setup dialog box in the *Users Guide: Wyse® Winterm™ 1 series Based on Wyse Thin OS*. The host and queue parameters define the IP address and queue name of the printer; PrinterID defines the Windows printer driver name; The clause of Enabled={yes, no} is optional with the default set to yes.
**NoReducer={yes, no}	Establishes the default setting of compression off for all types of connections.
**Password=sign-on password	In wnos.ini - If set to the default password, the system will sign on automatically and not wait for username, password, and domain entries. In [username].ini - Be sure it is the encrypted password of the user or the system will fail to sign on. This can be changed by a user, if allowed, in the Sign-on dialog box.

PnliteServer=List of {IP address,DNS names} with optional port number for each entry
ReconnectAtLogon={**0**, 1, 2}
ReconnectFromButton={**0**, 1, 2}
	List of IP addresses or host names with optional TCP port number of PNAgent/PNLite servers. Default=Empty. Each entry with optional port is specified as Name-or-IP:port, where :port is optional; if not specified, port 80 is used as the default. If a port other than 80 is used, the port number must be specified explicitly with the server location in the form IP:port or name:port. Once specified, it is saved in the non-volatile memory.
	The statement PNAgentServer and Web interface for Citrix MetaFrame Server is equal to this statement.
	NOTE: This and the DomainList command can be used in {username}.ini, but generally are used only in wnos.ini.
	NOTE: The PNAgent/PNLite server list and associated domain list optionally may be entered in DHCP server options 181 and 182, respectively. If entered in both places, the wnos.ini and {username}.ini entries have precedence. However, {username}.ini will override wnos.ini if the identical commands (with different parameters) exist in {username}.ini.
	NOTE: When Multifarm=yes, use # to separate failover servers, and use , or ; to separate servers that belong to different farms.
	ReconnectAtLogon and **ReconnectFromButton**:
	0 = disable the option
	1 = reconnect to disconnected sessions only
	2 = reconnect to active and disconnected sessions

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
Printer={COM1, COM2, LPT1, LPT2} [Name=name] [PrinterID=window_driver] [Class=classname] [Enabled={**yes**, no}] [EnableLPD={yes, **no**}]	Configures local printers. The Name specifies the name of the printer and is required. If the PrinterID is not specified, the default `Generic/Text Only` is used. [Class=classname] is used in ThinPrint print for TPAutoconnect (the ThinPrint technology of mapping the printer from the client side). It can group printers to use the same template on the ThinPrint server side. The strings PCL5, PS, and TXT are pre-defined classes. The class can be a string with 7 characters. If Enabled is not specified, the default is to enable the printer. If EnableLPD is not specified, the LPD service will not be enabled. **NOTE:** The parameters must be specified in the order shown.
Printer={LPD1, LPD2, LPD3, LPD4} [Host= host] [Queue=queue] [PrinterID=window_driver] [Class=classname] [Enabled={**yes**, no}]	Defines an LPD printer. If the PrinterID is not specified, the default `Generic/Text Only` is used. [Class=classname] is used in ThinPrint print for TPAutoconnect (the ThinPrint technology of mapping the printer from the client side). It can group printers to use the same template on the ThinPrint server side. The strings PCL5, PS, and TXT are pre-defined classes. The class can be a string with 7 characters. If Enabled is not specified, the default is to enable the printer. Default = `yes`. This setting in wnos.ini will be saved into nvram if EnableLocal is set to `yes` in wnos.ini. **NOTE:** The parameters must be specified in the order shown. For backward compatibility, LPD is accepted as LPD1.
Printer={SMB1, SMB2, SMB3, SMB4} [Host=\[domain]\host] [Name=share_name] [PrinterID=window_driver] [Class=classname] [Enabled={yes, no}] [EnableLPD={yes, **no**}] [Username=username] [Password=password] [Domain=domain name]	Specifies printers on the shared Microsoft network. Name is the shared printer name. Host is specified as \domain\host if the host is configured within a Microsoft domain. Otherwise, host is specified as \\host. If the PrinterID is not specified, the default `Generic/Text Only` is used. [Class=classname] is used in ThinPrint print for TPAutoconnect (the ThinPrint technology of mapping the printer from the client side). It can group printers to use the same template on the ThinPrint server side. The strings PCL5, PS, and TXT are pre-defined classes. The class can be a string with 7 characters. If Enabled is not specified, the default is to enable the printer. If EnableLPD is not specified, the LPD service will not be enabled. Username specifies a user who can use the SMB printer. Password specifies the password of a user. Domain specifies the domain name of the SMB printer.

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
**PRIVILEGE=[None, Low, High] [LockDown= {yes, no}] [HideSysInfo = {yes, no}] [HidePPP = {yes, no}] [HidePN = {yes, no}] [HideConnectionManager = {yes, no}] [EnableNetworkTest = {yes, no}] [EnableTrace={yes, no}] [ShowDisplaySettings={yes, no}]	Privilege controls access to thin client resources. **Parameter and Operator Privileges** `None` — This level of access is typical for kiosk or other restricted-use deployment. The System Setup selection on the desktop menu is disabled (the Setup submenu cannot be displayed). The Connect Manager is available, however, the user cannot create a new connection or edit an existing connection. The user cannot reset the device to factory defaults. `Low` — This is the level assigned to a typical user and is the thin client default. The Network selection on the Setup submenu is disabled (the Network Setup dialog box cannot be opened). A user at this level cannot reset the device to factory defaults. `High` — (default) All thin client resources are available with no restrictions. This is an administrative level of log-on. A user at this level can reset the device to factory defaults. **NOTE:** If PRIVILEGE=None or Low is used, the Network Setup dialog box is disabled. If it is necessary to access this dialog box and the setting None or Low is not saved into nvram, remove the network connector and reboot to display the Network Setup dialog box. If the optional `LockDown=yes` is specified, the system saves the privilege level in the flash device. If the `LockDown=No` is specified, the system clears the privilege level from the flash device to the default unlocked state.If the device is set to LockDown without a High privilege level, the device will disable the G key reset on power-up. Optional Lockdown is used to set the default privilege of the thin client. For example, if `LockDown=Yes`, then the privilege is saved in permanent registry; if `LockDown=No`, then the privilege level is set to the default `high` in the permanent registry.The optional Lockdown parameter is thus used to set up the default privilege. That is, the system has a default `high` privilege level, which is stored in the permanent registry; if you do not specify a privilege in either the wnos.ini or user.ini files or the network is unavailable, the setting of the Lockdown parameter will take effect. It can be modified by a clause. For example, `privilege=<none|low|high> lockdown=yes` in wnos.ini or user.ini, which will set up the default privilege to the specified level. And a clause such as `privilege=<none|low|high> lockdown=no` will set up the default privilege back to `high` regardless of the specified level, and current effective privilege level specified. If the optional `HideSysInfo=yes` is set, then the System Information will be disabled. If the optional `HidePPP=yes` is set, then Dialup Manager, PPPoE Manager, and PPTP Manager will be disabled. If the optional `HidePN=yes` is set, then the PNAgent or PNLite icon will not be visible on the taskbar. If the optional `HideConnectionManager=yes` is set, then the Connect Manager window will not be visible. If the optional `EnableNetworkTest=yes` is set, the Network Test will be enabled (Privilege=None). If the optional `EnableTrace=yes` is set, two active items are added to the desktop right-click menu (Privilege=High). If the optional `ShowDisplaySettings=yes` is set, the Display feature in the popup menu will be enabled (Privilege=None).

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
Reconnect={yes, **no}	Establish the default setting of Reconnect for all types of connections. This setting in wnos.ini will be saved into nvram if EnableLocal is set to `yes` in wnos.ini.
RepeatDelay={0, 1, **2, 3, 4, 5, 6, 7}	**Value and Keyboard Delay Before Repeat (seconds)** 0 — 1/5 1 — 1/4 **2 — 1/3 (default)** 3 — 1/2 4 — 3/4 5 — 1 6 — 2 7 — No Repeat
RepeatRate={0, **1, 2}	**Value and Keyboard Repeat Rate** 0 — Slow **1 — Medium (default)** 2 — Fast
*Resolution=[DDC, 640x480, 800x600, 1024x768, 1280x1024, 1360x768, 1400x1050, 1440x900, 1600x1200, 1680x1050] [Refresh=60, 75, 85}	Set local display resolution and refresh rate. If set in wnos.ini, the statement in {username}.ini will be invalid.
ScreenSaver={0, 1, 5, 10, **20, 30, 60, 120, 180} [LockTerminal = {**0**, 1, 2}] [Type = {0,1,2}] [Image = imagefile	**Value and Delay Before Starting** 0 — Disabled 1 — 1 Minute 5 — 5 Minutes 10 — 10 Minutes **20 — 20 Minutes (default)** 30 — 30 Minutes 60 — 1 Hour 120 — 2 Hours 180 — 3 Hours The optional parameter LockTerminal specifies to put the thin client in a LOCK state when the screen saver is activated. The user will be prompted with a dialog box to enter the sign-on password to unlock the thin client. Default = `0`. When LockTerminal=2, the unlock window will not be moved and the desktop will black out. If EnableLocal=yes and it is set in wnos.ini, the state of LockTerminal will be saved into nvram. **NOTE:** The user must be signed on with a password for this action to take effect. The optional parameter Type specifies which type of screensaver to use. 0=Blank the Screen, 1=Flying Bubbles, 2=Moving Image. The optional parameter `imagefile` is to specify an imagefile residing in the subfolder bitmap under the home folder. **NOTE:** If type is set to 2 and no image file is specified then the default Wyse logo image is used.

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
Seamless={yes, **no} [HideTaskbar={**0**, 1, 2}]	If set to `yes`, then the default resolution for ICA published applications is set to Seamless. Default = `no`. This is a command for Wyse Thin OS v4.2 and later only. The keyword HideTaskbar sets the status of taskbar when maximizing the seamless window. If set to 1, the maximized size will be the full screen, the taskbar will be hidden when maximizing the seamless window. Moving the mouse over the lowest bottom of the screen (1/4 height of taskbar) will display the taskbar. This setting in wnos.ini will be saved into nvram if EnableLocal is set to `yes` in wnos.ini. When set Seamless=`yes` HideTaskbar=2, it removes the auto-hide taskbar function but it reports the full resolution to the ICA server in a similar way to HideTaskbar=1.
Serial={COM1, COM2, COM3, COM4} [Baud={1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200}] [Parity={None, Even, Odd}] [Stop={1, 1.5, 2}] [Size={5, 6, 7, 8}] [Flow={None, XON/XOFF, CTS/RTS, Both}] [Touch={yes, no}] [Touch_type={elo, microtouch, fastpoint}]	Configures local serial ports. Touch set to `yes` denotes that a serial touch screen is attached. Touch type set to elo to denote that an ELO touch screen is being used. Touch type set to microtouch to denote that a MicroTouch touch screen is being used. Touch type set to fastpoint to denote that a FastPoint touch screen is being used. **NOTE:** Parameters must be specified in the order shown.
**SessionConfig=ALL [unmapprinters={yes, no}] [unmapserials={yes, no}] [smartcards={yes, no}] [mapdisks={yes, no}] [disablesound={yes, no}]	`SessionConfig=ALL` establishes the default settings for all sessions. For each of the optional connection parameters set to yes, the default settings will be established accordingly.
**ShutdownCount={0 to 60} (seconds) OR **ShutdownCounter={0 to 60} (seconds)	Default = 10 seconds. Specifies the number of seconds to count down before the shutdown sequence starts upon using the thin client power button when there are active sessions (Maximum value =60). Set the value to 0 to commence shutdown immediately and prevent the display of the countdown pop-up dialog box.
TimeServer=server_list [TimeFormat = {24-hour format, 12-hour format}] [DateFromat = {yyyy/mm/dd, mm/dd/yyyy, dd/mm/yyyy}]	Specifies the SNTP time servers and optionally the display format. The time and date format setting in wnos.ini will be saved into nvram if EnableLocal=yes in wnos.ini.
**UniSession={yes, no}	If `unisession=yes` for a connection, the connection will launch only once at a time.

Table 3 wnos.ini and {username}.ini , Continued

Command/Parameter	Description
VDIBroker=vdi_broker_url	Specifies the VDI broker server (supports both http and https). If vdi_broker_url does not start with http nor https, the default protocol is http. For an https connection, only one URL is accepted.
VNCPrompt = {yes**, no} [{Accept, Reject} = {**10** to 600} (seconds)] [ViewOnly = {yes, no}]	VNCPrompt set to yes means the user will always be prompted before shadowing starts. The user will then choose to decline or accept VNC shadowing. no means the user will not be able to decline or accept shadowing. Default = yes. By default, the user will be prompted. Optional Accept, Reject specifies a permission prompt and expired time in seconds (**10** to 600) with an action to accept or reject (a user can accept or decline VNC shadowing on a prompt window before the client desktop is shadowed). Optional ViewOnly, specifies viewing only with no keyboard or mouse events to be allowed to interfere with the thin client under shadowing.

ICA and RDP Connect Parameter List

Table 4 lists the ICA and RDP Command/Parameter and Description set.

Table 4 ICA and RDP Connect Parameter List

Command/Parameter	Description
Alternate=[**no**, yes]	**ICA Only**.Yes/no choice to use an alternate IP address returned from an ICA master browser to get through firewalls. Default = no.
Autoconnect={**0**-99}	Set to 1 to start a connection automatically (after sign-on, if sign-on is enabled). Default = 0. The value of 0-99 is the delay in seconds before auto-starting the session.
Browserip=list of browsers	**ICA Only**. List of IP addresses or DNS registered names to specify ICA browsers. List items must be separated by semicolons or commas.
Colors={256, **32k**, 64k or high, 16m, true}	Session color mode. Default = 32k. For faster display performance, use 256 colors for the session. 64k = high. **NOTE:** Although the default is 32k colors, older ICA servers may not support the 32k mode. In this case, the thin client will negotiate with the server and run the session in the 256 color mode (high colors in ICA requires that the server be running MetaFrame 1.8 FR2 or higher). There is continued support for 64k colors. The thin client supports high colors for RDP as long as the server supports RDP version 5.x or higher.
Command=start command	A string of commands to be executed after logging on to the server. This entry is limited to 127 characters.
Console={**no**, yes}	**RDP Only**. Set to yes to login to a session in Console mode. **Note:** If Console=yes is set behind the RDP connection, the Time Zone redirection feature will be disabled.
Description=string description	Connection description. Enclose in quotation marks if there are embedded blanks or single quotes. For quotation marks, use common-practice nesting rules. Up to 19 characters are allowed for this entry.
Directory=working directory	A directory to be used as the working directory after logging on to the server. This entry is limited to 63 characters.
Disablesound={**no**, yes}	Specifies whether or not to disable remote sound upon connection start. **Default = no**.
Domainname={domain name,$DN}	Domain name in a Windows network. Up to 31 characters are allowed for this entry. $DN specifies that the thin client sign-on domain name is used.

Table 4 ICA and RDP Connect Parameter List, Continued

Command/Parameter	Description
Encryption={None, Basic, 40, 56, 128, Login-128}	Connection security level. The highest level is 128-bit security (Login-128 option is 128 bit encryption for login only, and is only available for ICA). The lowest is None. Default=`Basic`. **NOTE:** The server must support the specified level of encryption or the connection will fail.
Fullscreen={**no**, yes}	Yes/no choice to run the session full screen. Default = `no` (session runs in windowed screen).

Host=[name, IP, $UN]
OR
Application=published application
	A list of server hostnames or IP addresses. The thin client attempts to connect to the next server on the list if the previous one failed. List items must be separated by semicolons or commas. $UN specifies that the sign-on user name is used and it should be set in user.ini.
	NOTE: If Host=$UN is set in the wnos.ini, the hostname will display as Start (default). If Host=$UN is set in the user.ini, the hostname will display as the sign-on user name.
	ICA Only. Published application to launch. Required if no host is specified.

HttpBrowsing={no, yes}	**ICA Only**. Select browsing protocol. Set to no for udp, yes for http. Default = `no`. Note that this command is used to override the default method of browsing established in the ICABrowsing command.
Icon={default, bitmap file}	Specifies an icon to appear on the thin client desktop for this connection. Use default to display a system default icon for this connection. For another icon, enter the name (with extension) of the bitmap file, and ensure that the file is located in the FTP server wnos\bitmap directory. If not specified here and the icon is not specified by a PNAgent/PNLite server, no icon is displayed for this connection.
LocalCopy={**no**, yes}	Set to yes to save the connection to the local NVRAM. The description field is used as the index key into the local connection table. If a match is found, then the entry is updated. Otherwise, a new entry is created. Default=no. **Note:** there are a total of 16 local entries.
Logon_mode={**local-user**, smartcard, user-specified}	**ICA Only**. Specifies how users authenticate to the selected application set or ICA connection. Default = `local-user`.
Lowband={**no**, yes}	Yes/no choice to enable optimization for low speed connections, such as reducing audio quality and/or decreasing protocol-specific cache size. Default = `no` (disabled).

Table 4 ICA and RDP Connect Parameter List, Continued

Command/Parameter	**Description**
Mapdisks={**no**, yes}	Specifies whether or not to auto-connect and map connected USB sticks upon connection start. Default = no.
NoReducer={**no**, yes}	Set to yes to turn off compression. Default = no.
Password={password, $SN, $MAC, $IP, $UN, $TN, $PW, $DN}	Password to log-in to the application server. Either a conventional log-in password can be used or a variable can be used. Up to 19 characters are allowed for this entry. **Parameter and Value** password — Conventional log-on password $SN — Serial number used $MAC — MAC address used $IP — IP Address used $UN — Sign-on name used $TN — Terminal Name $PW — Sign-on password used $DN — Sign-on Domain Name used **CAUTION:** The application server password is not encrypted; it is strongly recommended not to specify it. The user will be prompted to enter the password when the connection is made. This application server password directive never starts a line, so it can be distinguished from the thin client user sign-on password (which does starts a line).
Password-enc= an encrypted password	Specifies an encrypted string as a password for a connection.
Rdp_No_Animation={**no**, yes}	**RDP Only**. If set to yes, then "Menu/Window animation" will be disabled. Default = no (enable the feature).
Rdp_No_Dragging={**no**, yes}	**RDP Only**. If set to yes, then "Show content when dragging a window" will be disabled. Default = no (enable the feature).
Rdp_No_Theme={**no**, yes}	**RDP Only**. If set to yes, then "Theme" will be disabled. Default = no (enable the feature).
Rdp_No_Wallpaper={**no**, yes}	**RDP Only**. If set to yes, then "Wallpaper" will be disabled. Default = no (enable the feature).
Reconnect={yes, **no**, 1 to 3600 (seconds)}	**Parameter Value and Action** yes — Restart the connection after 20 seconds when disconnected. Default delay time for reconnect is 20 seconds. no — (default) No re-connection after a disconnect. seconds — (integer) Interval to wait (in seconds) before automatically restarting the connection after disconnection. Valid range is 1 to 3600.

Table 4 ICA and RDP Connect Parameter List, Continued

Command/Parameter	Description
Resolution=[**default**, 640x480, 800x600, 1024x768, 1280x1024, 1360x768, 1400x1050, 1440x900, 1600x1200, 1680x1050]	Maximum connection resolution. Use this setting to restrict the highest resolution for connections. The thin client will operate at the lesser of this setting and resolution specified at the connection entry. The default setting **default** starts the connection using the current desktop display setting with no window frame and border. If the connection is to a published application, then the Seamless selection is available. For Seamless connections (applicable to ICA only), the Metaframe hosts select the connection window size that best fits the applications.
Smartcards={**no**, yes}	**ICA and RDP**. Specifies to use a smart card login server when the connection starts. The default is **no**.
UniSession={yes, no}	If `unisession=yes` for a connection, the connection will launch only once at a time.
UnmapPrinters={no, **yes**}	**ICA and RDP**. Specifies to auto-connect to local printers when the connection starts. The default is **yes**.
UnmapSerials={no, **yes**}	**ICA and RDP**. Specifies to auto-connect to local serials when the connection starts. The default is **yes**.
Username=[username, $SN, $MAC, $IP, $UN, $TN, $PW, $DN]	Name to log-in to the application server. Either a conventional log-in name can be used or a variable can be used. Up to 31 characters are allowed for this entry. The combination of all the variables such as $IP@$DN are also supported. **Parameter and Value** username — Conventional log-on name $SN — Serial number used $MAC — MAC address used $IP — IP Address used $UN — Sign-on name used $TN — Terminal Name $PW — Sign-on password used $DN — Sign-on Domain Name used
Username-enc= an encrypted username	Specifies an encrypted string as a username for a connection.

This page intentionally blank.

Figures

Tables

Administrators Guide

Wyse® Winterm™ 1 series, Based on Wyse Thin OS
Issue: 041707

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

Created using FrameMaker® and Acrobat®