Cisco Virtual Experience Client 2112/2212 INI Files Reference Guide for WTOS 7.0_214

July 3, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25153-01

Cisco Virtual Experience Client 2112/2212 INI Files Reference Guide for WTOS 7.0_214

CONTENTS

Preface

Overview

The Cisco Virtualization Experience Client (VXC) 2112 and 2212 are workstation-class virtualization clients that run WTOS firmware for use with the Independent Computing Architecture (ICA) and the Remote Desktop Protocol (RDP). The ICA and RDP protocols are designed to deliver a user desktop from a centralized host server across standard IP networks, enabling you to use applications and desktop peripherals as if you were using them locally.

The Cisco VXC 2112 and Cisco VXC 2212 are highly optimized thin clients that provide ultra-fast access to applications, files, and network resources available on machines hosted by Citrix infrastructures. WTOS uses the Cisco VXC engine to provide a secure, near-zero management core that requires no local antivirus software or firewall to protect against viruses or malware.

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

WTOS Initialization (INI) files are plain-text files that you can construct to contain the configuration information you want for your thin clients running WTOS (both on a global level and on an individual user level). For example, these INI files can be used by applications to save information about a user's preferences and operating environment.

Caution Information and procedures presented in this guide are intended for use by system administrators and should not be used by untrained persons.

Audience

This guide is intended for administrators of Cisco VXC clients running WTOS. It provides the detailed information you need to help you understand and use the WTOS INI files. It contains information on the different INI files you can use and the rules for constructing the files. It also provides the parameter details you need (with working examples) to get the most out of your INI files. In addition, this guide also includes an appendix that contains all of the supported connect options you can use for ICA and RDP connections.

Organization

The manual is organized as follows.

Chapter	Description
Chapter 1, "Understanding WTOS INI Files"	Contains the basic information you need to help you understand and use the WTOS INI files. It contains information on the different INI files you can use and the rules and recommendations for constructing the files. In addition, this chapter contains information on the Sample User INI files that you can download and modify to quickly get your file server up and running for your thin client environment.
Chapter 2, "WNOS INI Only Parameters"	Provides the supported parameters that you can use in a wnos.ini file.
Chapter 3, "WNOS INI and {username} INI Parameters"	Provides the supported parameters that you can use in a wnos.ini file and in a {username}.ini file.
Appendix A, "ICA and RDP Connection Options"	Provides the supported options that you can use for ICA and RDP connections.
Appendix B, "Sample INI Files"	Provides sample INI files for centralized Cisco VXC client configuration.

Related Documentation

For more information, see the documents available at the following URLs:

Cisco Virtualization Experience Client 2000 Series

http://www.cisco.com/en/US/products/ps11499/tsd_products_support_series_home.html

Cisco Virtualization Experience Client Manager

http://www.cisco.com/en/US/products/ps11582/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

CHAPTER 1

Understanding WTOS INI Files

This chapter contains the basic information you need to help you understand and use the WTOS INI files. It contains information on the different INI files you can use and the rules and recommendations for constructing the files. In addition, this chapter contains information on the Sample User INI files that you can download and modify to quickly get your file server up and running for your thin client environment.

After you become familiar with the INI files, you can refer to the parameter details you need in the following sections of this guide:

- WNOS INI Only Parameters
- WNOS INI and {username} INI Parameters
- ICA and RDP Connection Options

About WTOS INI Files

WTOS INI files contain the parameters and associated values necessary for the various functionality you want.

You can construct the following INI files:

- wnos.ini file (see Working with wnos.ini Files, page 1-1)
- {username}.ini file (see Working with {username}.ini Files, page 1-2)

Working with wnos.ini Files

A wnos.ini file contains the “global” parameters you want that will affect all thin clients accessing the file server. Parameters in both Table 2-1 on page 2-1 and Table 3-1 on page 3-2 can be used in a wnos.ini file.

Note Parameters in Table 2-1 on page 2-1 can only be used in a wnos.ini file; they cannot be used in a {username}.ini file.

Working with {username}.ini Files

A {username}.ini file contains the user-specific or "user profile" parameters you want that will comprise the connection profile for an individual user. These parameters will affect only the user you specify. Parameters in Table 3-1 on page 3-2 can be used in a {username}.ini file.

Note "User profile" parameters (found in the {username}.ini file) generally override the identically named "global" parameters (found in the wnos.ini file), however, some "global" parameters do not allow this (for hierarchical precedence of one variable over another, refer to the parameter notations in Table 3-1 on page 3-2.

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

Rules and Recommendations for Constructing WTOS INI Files

In general, WTOS INI files follow currently accepted "standard" INI file formatting conventions. WTOS INI files consist of WTOS parameters. These parameters can be entered as necessary for reference, but are not mandatory unless changes from defaults are required or the parameter is noted as required in the tables. Every parameter has a name and a value with the name appearing to the left of the equals sign (name=value). All parameters with the same name in the various WTOS INI files have the same meaning (that is, a parameter named XYZ in a wnos.ini file and named XYZ in a {username}.ini file will have the same meaning). Number signs (#) indicate the start of a comment. Comments can begin anywhere on a line. Everything between the # and the End of Line is ignored.

Along with these general formatting conventions, use the following guidelines when constructing WTOS INI files:

- **Order of Parameters**—Global connect parameters should be listed before other connect parameters in a wnos.ini file.
- **Mandatory Parameters**—As stated earlier, parameters can be entered as necessary for reference, but are not mandatory unless changes from defaults are required or the parameter is noted as required in the tables. For example, the Connect= parameter is mandatory.
- **Use of Backslashes and White Spaces**—Placing a backslash (\) at the end of a line indicates line continuation; that is, the backslash means that the line and the following line are, for the purposes of reading code, the same line. No white space can appear after the backslash; however, white space between parameter entries must be maintained. Therefore, the line after a backslash must either start with a space (not a tab) or concatenate with the first set of characters from the previous line. To avoid confusion, starting each line with at least one white space character is recommended. Starting all parameters at the left margin and placing at least one leading space at the beginning of all continuation lines makes an INI file easier to read.
- **Use of Blank Lines**—Using blank lines is recommended for making code easier to read.
- **Use of Number Signs**—As stated earlier, number signs (#) indicate the start of a comment. Comments can begin anywhere on a line. Everything between the # and the End of Line is ignored.
- **Use of Quotation Marks**—String parameters containing white spaces must be placed inside quotation marks (use common-practice nesting rules).

- **Use of List Separators**—Use semicolons or commas for list separators.
- **Use of Equivalent Parameter Values**—For parameter values of type {0, 1}, zero (0) indicates false or no, and one (1) indicates true or yes, as applicable. The format {0, 1} is equivalent to, and can be used instead of, the format {no, yes} for the parameters using these formats in the tables.
- **Use of the Home Directory**—The home directory is the wnos subdirectory for the sign-in. For example, C:\Inetpub\ftproot\cisco\wnos).

  You can specify the username and password for file server access in the Central Configuration dialog box (see *Cisco Virtualization Experience Client 2112/2212 ICA Administration Guide for WTOS*). If a file server directive is processed, the same username and password already configured on the thin client is usable for accessing files on the new file server.
- **{username}.ini Files must be Write-Enabled**—All {username}.ini files must be write-enabled to allow the thin client to place the encrypted user passwords in the files.
- **Number of Connection Entries Allowed**—The combined number of connection entries defined in a {username}.ini file and a 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 using the wnos.ini file.
- **Use of the {username}.ini and {mac}.ini Parameters**—The {username}.ini and {mac}.ini parameters can appear in the wnos.ini file. However, these parameters must be below the include=$un.ini parameter or the include=$mac.ini parameter in the wnos.ini file. Although not required, it is recommended that these parameters end with an Exit=all parameter.

Warning **No parameter should ever be executed twice. Some WTOS hardware configuration parameters require a reboot to become active, and if the same parameters are defined more than once, the thin client may then go into an infinite reboot cycle.**

  Placing the include=$mac.ini statement on last line of the wnos.ini file to verify that all parameters are processed properly for terminal-specific settings is recommended.
- **Use of System Variables**—Some parameters can use the system variables shown in Table 1-1 to map the string. All combinations of the variables, such as CTX&Right($IP,4)@&Left($UN,3) are supported. A replacement $SYS_VAR will be used if the statements or parameters support it.

Table 1-1 System Variables

Parameter	Value
$SN	Serial number used
$MAC	MAC address used.
$IP	IP Address used.
$UN	Sign-in name used.
$PW	Sign-in password used.
$TN	Terminal name.
$DN	Sign-in domain name used.
$WPUN	PEAP/MSCHAPv2 username used (802.1x dependent).

Table 1-1 System Variables (continued)

Parameter	Value
$WPPW	PEAP/MSCHAPv2 password used (802.1x dependent).
&Right($xx, i) or &Left($xx, i)	Specifies whether the variable is to be read from left or right. The $xx is any of the above parameters. The parameter i specifies left or right offset digits.

CHAPTER 2

WNOS INI Only Parameters

This chapter provides the supported parameters that you can use in a wnos.ini file.

Parameters for wnos.ini Files Only

Table 2-1 contains the supported parameters you can use in wnos.ini files. Parameters with bold values (defaults) are required parameters for a wnos.ini file (those parameters without bold values are optional). Parameters in Table 2-1 can only be used in a wnos.ini file; they cannot be used in a {username}.ini file.

Table 2-1 Parameters for wnos.ini Files Only

Parameter	Description
AddCertificate=filename password={plain text password} Password-enc={encrypted password}	AddCertificate—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. The length of the filename, including the trailing period and the file extension, is limited to 64 characters. This parameter 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. Supported files include .crt file on ICA CSG; .cer and .pfx in 802.1x. Password and Password-Enc are for special use with PFX files.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
AutoLoad=[0, **1**, 2, 101, 102, 201, 202] [PXE= {imaging}]	AutoLoad—Specifies the firmware update mode. • 0—Disable checking for image. • 1—Enable a forced firmware upgrade/downgrade process. Default is 1. • 2—Enable a comparison/non-forced upgrade only process. • 101—Enable firmware upgrade/downgrade process, but have a popup message with OK and Cancel buttons appearing before the process; completion message appears after process. • 102—Enable upgrade only, but have a popup message box with OK and Cancel buttons appearing before the process; completion message appears after process. • 201—Enable a forced firmware upgrade/downgrade process, but have a popup message with OK button appearing before process although process will begin in 20 seconds in any case; completion message appears after process. • 202—Enable a comparison/non-forced upgrade only process, but have a popup message with OK and Cancel buttons appearing before the process; completion message appears after process. PXE—Specifies for WTOS clients that boot from PXE to flash the image from an FTP server to the unit, otherwise the system runs in a normal mode. **Note** PXE is not applicable to Cisco VXC clients.
AutoPower={**no**, yes}	Yes/no option on how the system starts when the power is first applied to the thin client. If set to yes, then the system starts itself without waiting for users to press the power button (in cases where power was lost unexpectedly; even if the thin client was shut down properly before power was lost unexpectedly, when the power is restored, the thin client will be powered on). This setting is useful in a kiosk environment. After 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. Maximum of 31 characters is allowed in a string. After being specified, it is saved in the non-volatile memory.
ConnectionBroker={**default**, VDM}	Specifies the type of VDI broker to use.
DefaultUser={username, $SYS_VAR}	Specifies the default sign-in user. See Table 1-1 on page 1-3 for a list of system variables for $SYS_VAR.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
DelCertificate={filename, all}	Removes the named file from the nand flash or from the memory. If DelCertificate=ALL, then all certificates (except built-in certificates) will be deleted from the flash.
DesktopColorDepth={16, 32}	DesktopColorDepth—Sets the desktop color to 16 or 32 bits. If DesktopColorDepth=16, the default color is 15 bits.
DHCPExpire={**reboot**, shutdown}	When a DHCP lease expires, a message notifies the user as follows: "DHCP Expired, you must reboot." • reboot—After 5 seconds, the system reboots. • shutdown—After 5 seconds, the system shuts down.
DHCPOptionsRemap={**no**, yes} [DisableOption12={**no**, yes}] [FileServer={128 to 254}] [RootPath={128 to 254}] [FtpUserName={128 to 254}] [FtpPassWord={128 to 254}] [RapportServer={128 to 254}] [RapportPort={128 to 254}] [PnliteServer={128 to 254}] [DomainList={128 to 254}] [VDIBroker-{248 to 254}] [RapportSecurePort={128 to 254}]	DHCPOptionsRemap—Specifies whether or not the following options can be set. (the options are for use when default DHCP options discussed in the *Cisco Virtualization Experience Client 2112/2212 ICA Administration Guide for WTOS* must be remapped). The value for each option must be from 128 to 254. Values for the options must be different for each option. These options are used to configure DHCP server tags for thin client booting. **Note** The DisableOption12 option sets whether or not the Option12 tag is accepted. By default, DHCP option 12 sets the hostname and domain name of the terminal. For example, if the option 12 information is terminalname.cisco.com, the terminal name will be set as terminalname and the domain name will set as cisco.com. If the DisableOption 12 setting is different than the value in NVRAM, the system will automatically reboot to make the value valid. **Note** RapportSecurePort is the specified HTTPS port of the Cisco VXC Manager server.
[DHCPUserClassID=class_id {ParseVendorInfo={no, **yes**]	DHCPUserClassID—Specifies the UserClassID used for DHCP. ParseVendorInfo—Yes/no option to specify whether or not WTOS will interpret DHCP option 43 (vendor-specific information). Default is yes. If ParseVendorInfo is set to no and the DHCPVendorID is also used with this parameter, you must set ParseVendorInfo=yes and then reboot the thin client twice. Maximum of 26 characters is allowed in a string.
DHCPVendorID=vendor [ParseVendorInfo={no, **yes**}]	DHCPVendorID—Specifies the VendorID used for DHCP. ParseVendorInfo—Yes/no option to specify whether or not WTOS will interpret DHCP option 43 (vendor-specific information). Default is yes. If ParseVendorInfo is set to no and the DHCPVendorID is also used with this parameter, you must set ParseVendorInfo=yes and then reboot the thin client twice. Maximum of 26 characters is allowed in a string.
DisableButton={**no**, yes}	Yes/no option to disable the power button.
DisableDomain={**no**, yes}	Yes/no option to disable the drop-down domain list in the PNAgent/PNLite sign-in dialog box.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
DNSTTL={0-3600}	Specifies the Time to Live (TTL) of DNS name caching; the default is from DNS server settings. **Note** If DNSTTL=0, the DNS hostname in a connection always queries the DNS server to get the IP.
DomainList=List of NT domain names	A list of domain names that will appear in the thin client sign-in dialog box as options to help users in selecting the domain to sign-in to PNAgent/ PNLite servers. After being specified, it is saved in non-volatile memory. **Note** Be sure to enclose in quotation marks if spaces are included. For example: DomainList= “North_America, SQA, test-domain”
Dualhead={**no**, yes} [ManualOverride={**no**, yes}] [Mainscreen={1, 2}] [Orientation={**hort**, vert}] [Align={Top|Left, Center, Bottom|Right}] [Taskbar={**wholescreen**, mainscreen}]	(For supported dual-monitor capable thin clients only) Dualhead—Yes/no option to support a dual-monitor display. ManualOverride—Yes/no option to allow the local client to override display dualhead settings received from central configuration (a factory default reset will again take server settings for dualhead). This is helpful for scenarios where you have a mixture of dualhead and single head deployments. For example: Dualhead=yes ManualOverride=yes Mainscreen=1 \ Orientation=hort Taskbar=mainscreen Mainscreen—Sets which screen is used as the main screen. Orientation—Sets which style is used for display (hort means horizontal and vert means vertical). Align—Sets how screens are aligned: Top means screens are top aligned in “hort” orientation. Left means screens are left aligned in “vert” orientation. Center means screens are center aligned. Bottom means screens are bottom aligned in “hort” orientation. Right means screen are right aligned in “vert” orientation. Taskbar—Sets which style is used for the taskbar: “wholescreen” places the taskbar at the bottom of the entire screen; “mainscreen” places it at the bottom of the main screen. ⚠ **Caution** If Dualhead is changed from no to yes, the thin client requires a reboot to change the monitor display.
EnableCacheIni={**no**, yes}	Yes/no option to enable the WNOS INI cache functionality (cache WNOS INI file to local flash when WNOS INI is changed in file server), WTOS would use cached WNOS INI when WNOS INI on the file server is unavailable. Default set to no to disable WNOS INI cache functionality.
EnableGKey={no, **yes**}	Yes/no option to enable G key reset. G key reset is supported for Privilege=High in the NVRAM.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
Exit={**yes**, no, all}	Specifies the INI file processing. • yes—Processing returns to the prior INI file on the next line after $include. • no—There is no operation. • all—All INI file processing is exited.
FileServer=List of {IP address, DNS name} [Username=username] [Password=password]	FileServer—Specifies the FTP server IP address or DNS name that is entered into thin client local setup (non-volatile memory); the thin client immediately uses this server to access files. Username—Specifies the username of the file server. Password—Specifies the password of the file server. **Note** The target file server must support access using the same user credentials used in the INI files
FormURL=URL to a file	Specifies the URL to the name of a bitmap file (.ico, .bmp, .jpg, or .gif), to be displayed in the sign-in window, residing under the thin client home directory. The length of the path, including the home directory and the file, is limited to 128 characters. If auto dial-up is enabled, this statement is invalid.
Include=$mac.ini	Loads "/wnos/inc/mac-address.ini". **Note** The file name does not include the symbols ":" in the mac address. See also the Exit parameter for information on how to terminate Include.
LongApplicationName={**no**, yes} DisplayWidth={400–7000}	Yes/no option to display all 38 characters in a desktop icon name. If LongApplicationName=no then icons will display up to 19 characters (any over 19 characters and the last three characters will be "…"). The DisplayWidth specifies the pixels of session list width in "Zero LaunchPad" mode. The default is 400.
MaxVNCD={0, **1**}	Option to enable VNC shadowing. Default value is 1 which means VNC shadowing is enabled. Note that only one VNC client session is allowed. Set to 0 to disable shadowing.
Multifarm={**no**, yes}	Yes/no option to support Citrix multifarm functionality for the wnos.ini files. If Multifarm=yes, PNAgent/PNLite users are able to authenticate to more than one Citrix farm.
MultiLogon={**no**, yes}	Yes/no option to support multiple sign-ins. If MultiLogon=yes, the PNAgent/PNLite sign-in authenticating window can input a different username, password, and domain while signing in to different PNAgent/PNLite servers.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
NoticeFile=filename [Resizable={**no**, yes}] [Timeout={**0**, 10 to 600}]	NoticeFile—Specifies a legal notification file residing in the home directory folder. The file is displayed in a dialog box and the user is prompted to accept it before the sign-in process continues. Resizable—Yes/no option to resize the dialog box to fit the text size. Timeout—After the notice is accepted, if Timeout (seconds) is specified, and if no mouse or keyboard is used, then the dialog box will display again after the seconds set. (0 means no timeout).
PasswordServer=password_server [connect={ica, rdp}] [encryption={Basic, 40, 56, 128, Login-128, None}]	Specifies an ICA server where you can sign-in and modify a user password when a user sign-in fails (both URL and server list are supported). Specifies an ICA/RDP server where you can sign-in and modify the password when a user sign-in fails. The PasswordServer statement can specify the connection parameters as described in the Connect statement. If no parameter is specified, it will connect with an ICA protocol. For example: PasswordServer=10.151.120.189 connect=rdp \ encryption=Basic
PlatformConfig=S Class or VClass [Firmware={Firmware filename}] [BIOS={BIOS filename}]	If a specific platform is specified by the PlatformConfig parameter, then WTOS will attempt to load the Firmware and BIOS whose filenames are specified by the Firmware and BIOS parameters. If the written Firmware and BIOS are valid on file server, they will be loaded by default, if the written Firmware and BIOS are invalid on file server, WTOS will load the platform default Firmware and BIOS instead.
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={**no**, yes}	Yes/no option to disable the Cisco VXC Manager agent.
RapportServer=server_list [Retry=retry number]	RapportServer—Specifies a list of IP addresses or DNS names (separated by using a comma) for the Cisco VXC Managerservers. After being specified, it is saved in non-volatile memory. Retry—Determines the number of attempts to retry a contact to Cisco VXC Manager servers.
Reboot={no, yes} Time=hh:mm	Reboot—Yes/no option to enable automatic daily reboot of all WTOS devices. Time—Specifies the time to reboot and must be in a 24-hour format. For example: Reboot=Yes Time=17:30 will reboot all WTOS devices at 5:30 p.m. daily.
RegisterWINS=yes	Forces the thin client to register itself with a Microsoft WINS server.
RootPath=FTP root path	This FTP root path is entered into thin client local setup (non-volatile memory). 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 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
SelectServerList={PNA, VDI}; list of servers {Server1; Server2; ServerN}	Allows users to select one PNA or VDI server during sign-in. For a PNA server, use the format: <description> - <host> [- <options>] For a VDI server, use the format: <description> - <host> **Note** Be sure to use a comma (,) or a semicolon (;) to separate different servers and to use a dash (-) to separate the server description, host, and other options. **For PNA server options**: Use the options of the PnliteServer parameter in Table 3-1 on page 3-2. PNA example: SelectServerList=PNA ; ServerDescription1 - 192.168.0.10 - autoconnectlist=* reconnectfrombutton=0; ServerDescription2 - HostName2.cisco.com - TimeOut=200; ServerDescription3 - https://server3.cisco.com; **For a VDI server:** If you want to use a VDM VDI broker, specify ConnectionBroker=VDM in wnos.ini. Otherwise the VDI broker type is default. VDI example: ConnectionBroker=VDM SelectServerList=VDI ; description1 – 192.168.0.11; description2 – host2.cisco.com
Service={snmpd, thinprint, vncd} disable={**no**, yes}	Service—Specifies the services you can enable or disable (there are different syntaxes for the different services). disable—Yes/no option to disable the services. disable must follow the Service parameter.
Service=snmpd disable={**no**, yes} {community=<snmp community>}	Service=snmpd disable—Yes/no option to disable the snmpd service. community—Same as the statement “Community.”
Service=thinprint disable={**no**, yes} [port=<port number>] [PkSize={0-64000}]	Service=thinprint disable—Yes/no option to disable the thinprint service. port—Same as the statement “ThinPrintEnable={no, yes} port=port number.” PkSize—Specifies the default packet size that will be sent to the server when negotiating with the thinprint server. The value 0 will rely on the server default setting, 64000 in ThinPrint 7.6 and 32000 in previous ThinPrint versions. WTOS only allocates a buffer of 64K, so if the default packet size of the server is above 64000, this setting must be set or printing will fail.
Service=vncd disable={**no**, yes}	Yes/no option to disable the vncd service (same as “MaxVncd={0, 1}”).
Service=<port number> disable={**no**, yes}	Yes/no option to disable the service with this port number. The 80 port is an exception because the Cisco VXC Manager is always started before loading the global profile (wnos.ini file).

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
SignOn={**yes**,no, NTLM} [MaxConnect=max] [ConnectionManager={maximize, **minimize**, hide}] [EnableOK={**no**, yes}] [DisableGuest={**no**, yes}] [DisablePassword={**no**, yes}] [LastUserName={**no**, yes}] [RequireSmartCard={**no**, yes}] [SCRemovalBehavior= {-1, **0**, 1}] [SaveLastDomainUser={yes, no}]	SignOn—Yes/no/NTLM option to enable the sign-in process. If set to NTLM, a user can be authenticated with an NTLM protocol. The user must be a domain user and the same sign-in user credentials must be available in the ftp://~/wnos/ini/ directory. The NTLM protocol also requires a WINS server. MaxConnect—Maximum number of connections allowed to be specified in the wnos.ini file and {username}.ini file totalled together. The range allowed for MaxConnect is 100 to 1000. The default maximum is 216 entries. ConnectionManager—State of the Connect Manager during sign-in. EnableOK—Yes/no option to show the OK and Cancel command buttons in the sign-in dialog box. DisableGuest—Yes/no option to disable the guest sign-in. DisablePassword—Yes/no option to disable the password text box and password check box in the sign-in dialog box. LastUserName—Yes/no option to display the last sign-in username after the user signs off. RequireSmartCard—Yes/no option to force sign-in with smartcard. SCRemovalBehavior—Specifies what happens after a smart card is removed. -1—System keeps working, but cannot communicate further with the server, and the lock terminal option is grayed out. 0—System will sign out 1—System will be locked and can be unlocked only when the same certificate is used with the smart card SaveLastDomainUser—Yes/no option to save the username and domain into NVRAM after sign-in is successful. On next reboot, the username and domain saved in the NVRAM will be displayed in sign-in server as the default username and domain if no DefaultUser is set in the wnos.ini file. The size of username/domain is limited to 32 characters, and if larger than 32, it will first be truncated and then saved into NVRAM.
Speedbrowser={**on**, off}	On/off option to enable the ICA Speedscreen Browser Acceleration Function.
SwitchApplication={**yes**, no}	Yes/no option to allow switching between open applications using the Alt+Tab key combination.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
SysMode={classic, vdi} [toolbardisable={**no**, yes}] [toolbardisablemouse={**no**, yes}] [toolbarclick={**no**, yes}] [toolbardelay={0-4}] [toolbar_no_conmgr={**no**, yes}] [toolbar_no_minimizeall={**no**, yes}] [toolbardisablehotkey={**no**, yes}]	SysMode—Specifies the Cisco VXC Zero interface (optimized for VDI) or the Classic interface. This value will be remembered across reboots until changed. If not defined and an INI is present, Classic mode is the default. If no INI is present, VDI mode is the default. Classic mode has full taskbar, desktop and connection manager and is recommended for a terminal server environment. VDI mode (Cisco VXC Zero interface) has a launchpad-style interface optimized for full-screen sessions (i.e. Desktops). Everything you need is accessed through an always available overlay interface. The following options allow you to configure if and when the Cisco VXC toolbar will display under VDI mode. Toolbardisable—Yes/no option to disable the Cisco VXC toolbar from displaying (it set to yes, this option overrules other toolbar display options). Toolbardisablemouse—Yes/no option to disable the Cisco VXC toolbar from automatically displaying after the mouse pointer hovers on the left side of the screen for a specified amount of time. toolbarclick—Yes/no option to pop up the toolbar only if clicking on the left-most side of the screen. toolbardelay—Specifies the seconds to delay before displaying the toolbar after hovering the mouse pointer over the left-most side of the screen. The value 0 will have no delay. The other values 1, 2, 3,4 will delay 0.5, 1, 1.5 and 2 seconds respectively. toolbar_no_conmgr—Yes/no option to hide the Home button. toolbar_no_minimizeall—Yes/no option to hide the Home button (thus affecting the ability to minimize displayed list of connections). toolbardisablehotkey—Yes/no option to disable the CTR+ALT+UPARROW hotkey that allows the toolbar to instantly display (without a timer).
SysName={**client**, DNS}	Specifies system name. If set to DNS, a reverse DNS name from the DNS server is checked into the Cisco VXC Manager server (by default, the terminal name is checked in).
TcpTimeOut={**1** to 255}	Specifies 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).
TerminalName=name [reboot={no, yes}]	TerminalName—Name of the thin client comprising a 15-character string. reboot—Yes/no option to reboot the thin client if the terminal name is changed.
ThinPrintEnable={no, **yes**} [Port=port number]	ThinPrintEnable—Yes/no option to enable the thinprint client. port—The TCP port of the thinprint client. The default port number value is 4000. The port number value must be less than 65535.

Table 2-1 Parameters for wnos.ini Files Only (continued)

Parameter	Description
TimeZone=zone [ManualOverride={**no**, yes}] [daylight={**no**, yes}] [start=mmwwdd end=mmwwdd] [TimeZoneName=timezonename] [DayLightName=daylightname]	TimeZone—Specifies the time zone if the zone is unspecified on the thin client or is used with ManualOverride. Supported zones are listed in the System Preference dialog box (for example: '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'). ManualOverride—Yes/no option to override the thin client System Preference Menu setting with this TimeZone setting. TimeZone settings in the wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file. Daylight—Yes/no option to enable daylight saving time; mmwwd is a 6-digit number to specify the start and the end of daylight saving time using the following: • mm —01 to 12 for the month of the year from January to December. For example, 01 is January. • ww—01 to 05 for the week of the month. For example, 01 is the first week. • dd—01 to 07 for the day in the week from Monday to Sunday. For example, 01 is Monday. TimeZoneName—Display name sent to the ICA/RDP session (such as Eastern Standard Time). DayLightName—Display name for daylight saving time. If daylight saving time is enabled, DayLightName should be named something similar to Eastern Daylight Time, otherwise it should be the same as TimeZoneName. **Note** To configure daylight saving time 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 [encrypt={**no**, yes}]	VncPassword=password—Specifies a string of up to 16 bytes as the password used for shadowing. encrypt—Yes/no option to encrypt the password; an encrypted string is used as a password (ensures US HIPPA and Congress Acts compliance).

CHAPTER 3

WNOS INI and {username} INI Parameters

This chapter provides the supported parameters that you can use in a wnos.ini file and in a {username}.ini file.

Parameters for wnos.ini Files and {username}.ini Files

Table 3-1 contains the supported parameters you can use in wnos.ini files and {username}.ini files. Parameters with bold values (defaults) are required parameters for a wnos.ini file or a {username}.ini file (those parameters without bold values are optional).

Caution As stated previously, "user profile" parameters (found in the {username}.ini file) generally override the identically named "global" parameters (found in the wnos.ini file). However, some "global" parameters do not allow this—specifically, parameters in Table 3-1 noted with an asterisk (*) do not allow this "user profile" override. Thus, if the parameters in Table 3-1 that are noted with * are used in both a {username}.ini file and in a wnos.ini file, the noted parameters in the wnos.ini file will override the same noted parameters in the {username}.ini file.

For example, if the parameter Resolution=1024x768 is used in the {username}.ini file and the same parameter Resolution=1280x1024 is used in the wnos.ini file, the Resolution=1280x1024 in the wnos.ini file will override the Resolution parameter in the {username}.ini file. Therefore, if you want the parameter Resolution=1024x768 in the {username}.ini file to be used, you must not use the Resolution parameter in the wnos.ini file.

Note Parameters in Table 3-1 noted with two asterisks (**) that are used in a {username}.ini file will return to the values set for those parameters in the wnos.ini file after a user sign-out.

For example, if your {username}.ini file contains the parameter MouseSwap=1 (so that the mouse buttons are swapped for your left-handed use) and you sign out of the thin client, then the MouseSwap value will return to the original default value of 0 (MouseSwap=0) contained in the wnos.ini file—so that others who sign in can use their own "user profile" (assuming the administrator has not changed the default values in the wnos.ini file).

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
AdminMode={**no**, yes} [admin-username=encrypted_username] [admin-password=encrypted_password] [Username=username] [Password-password]	AdminMode—Yes/no option to use the username and the password to obtain a high privilege thin client configuration when the Privilege parameter level is set to high (Privilege=high). admin-username—Specifies if admin-username=encrypted_username, then encrypted strings are used for admin-username. admin-password—Specifies if admin-password=encrypted_password, then encrypted strings are used for admin-password. **Note** Right-click on AdminMode to access the shortcut menu items
AltCacheDisable={no**, yes}	Yes/no option to disable the new cache mechanism allowing more memory to be available to a user (developed with Citrix Presentation Server 4.0 and Windows Server). If set to no, the new cache mechanism is enabled.
Alternate={no**, yes}	Yes/no option to use an alternate IP address returned from an ICA master browser to get through firewalls. This setting in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file.
AutoSignoff={no**, yes} [Shutdown={**no**, yes}] [Reboot={**no**, yes}]	AutoSignoff—Yes/no option to automatically sign-out a user when the last opened session is closed. Shutdown—Yes/no option to shut down the thin client. If shutdown is set to yes, the ShutdownCounter value is used to control the countdown before the system is shut off. Reboot—Yes/no option to reboot the thin client. If Reboot is set to yes, the ShutdownCounter value is used to control the count down before the system is rebooted.
ClearLicense={**no**, yes}	Yes/no option to clear the TSCAL license stored in the non-volatile memory. It can be replaced by FixLicense=clean.
Connect={ICA, RDP} [NO_FontSmoothing={**no**, yes}]	Connection protocol. Follow the selections from the ICA/RDP option list (refer to Table A-1 on page A-1). Some options are required. All options for each connection must be on the same logical line (\ can be used for line continuation—see Rules and Recommendations for Constructing WTOS INI Files, page 1-2). NO_FontSmoothing—**ICA Only** Yes/no option to disable font smoothing. Default is no (font smoohing is enabled by default). Set to yes to disable font smoothing.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
ConnectionBroker={**default**, VDM}	Specifies the Connection Broker type. Choose VDM to enable VDM 2.1 XML support. If you enter VDM, the VMware logo appears on the sign-in screen. 
**DefaultPrinter={LPD1, LPD2, LPD3, LPD4, COM1, COM2, LPT1, LPT2, SMB1, SMB2, SMB3, SMB4}	Specifies the default printer. Be sure the printer set as default is enabled or the setting will be invalid.
DeskColor="rrr ggg bbb" where DeskColor ="16 100 36" (green)** is the default	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. When using this parameter in a wnos.ini file, it will be saved to NVRAM if EnableLocal is set to yes in the wnos.ini file.
Desktop=bitmap file [Layout={center, tile, **stretch}]	Desktop—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 Cisco wallpaper. To disable the parameter, leave value blank (Desktop=). Layout—Specifies the arrangement on the desktop background of the bitmap file specified by the Desktop parameter (if auto dial-up is set, Layout is invalid). For center, the image is placed in the center of the desktop without image size change. For tile, the image is replicated across the desktop. For stretch, the image is modified to fill the desktop. **Note** In dual-monitor mode, the wallpaper is replicated and specified separately for each monitor (instead of being shared by the two monitors).
Device=audio volume={low, **middle**, high} or {0 to 25} mute={**0**, 1, 2}	Device—Specifies the local audio volume. volume—low is minimum volume, middle is medium volume, and high is the maximum volume. The values between 0 and 25 allows you to set the exact volume level. mute—Selects the volume Mute check box in the 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.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter * Global overrides identically named user profile ** After sign-out, user profile returns to global value	Description
*Device=Ethernet [Speed={**Auto**, 10M HD, 10M FD, 100M HD, or 100M FD} [MTU=mtu] [KeepAlive={5-600}] [Warning={**no**, yes}]	Device—Specifies to use an ethernet. Speed—Specifies the ethernet speed to either Auto, 10M HD, 10M FD, 100M HD or 100M FD. If Speed is set in a wnos.ini file, the Speed statement in the {username}.ini file will be disabled. **Note** Device and Speed parameters can be replaced by the EthernetSpeed parameter. KeepAlive—Specifies a time value (in seconds between 5 and 600) to keep an idle connection alive. Warning—Yes/no option to warn about an idle connection. In the seconds of the specified KeepAlive, if the tcp connection is idle and Warning=yes, one log will be printed for the session. For example: device=ethernet keepalive=20 warning=yes MTU—A maximum transmission unit value between 500 and 1500. **Caution** If the Speed parameter value is changed, the thin client will require a reboot.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
Device=keyboard [numlockoff={no**, yes}] [repeatrate={0, **1**, 2}] [repeatdelay={0, 1, **2**, 3, 4, 5, 6, 7}]	Device—Specifies the local keyboard. numlockoff—Yes/no option to turn off the NumLock of the keyboard. repeatrate—Specifies the keyboard repeat rate. • 0—Slow • 1—Medium • 2—Fast repeatdelay—Specifies the keyboard delay before repeat (in seconds). • 0—1/5 • 1—1/4 • 2—1/3 • 3—1/2 • 4—3/4 • 5—1 • 6—2 • 7—No Repeat **Note** These settings in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file.
Device=UsbSerial Start=COMx	Specifies the first COM port number that can be used by USB-serial port. For example, the first USB-Serial port on a VL10 thin client is COM2 by default, but it can be changed to COM3 (Device=UsbSerial Start=COM3) with the INI file.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter * Global overrides identically named user profile ** After sign-out, user profile returns to global value	Description
Device=vusb [ForceRedirect=DeviceID] [ForceLocal=DeviceID] [Type={HDX}]	Device—Specifies the ID of a local USB device that is not redirected by default. ForceRedirect—Specifies a forced redirect of the local USB device to the server. This parameter has priority over ForceLocal. ForceLocal—Specifies that the local USB device should not be redirected to the server. The DeviceID can be found in the event log. For example, if you find "HDX USB: Local Device(0x04f2,0x0112,0x03,0x01,0x01)", set the parameter as: Device=vusb ForceRedirect=0x04f2,0x0112,0x03,0x01,0x01 Type—**ICA Only**. In ICA environments, allows you to force the usage of HDX for USB virtualization. For example: Device=vusb Type=HDX
DisableMouse={no**, yes} or MouseDisable={**no**, yes}	DisableMouse—Yes/no option to disabled mouse pointer so that it is shown on the screen. The pointer is enabled if any mouse activity occurs. or MouseDisable—Yes/no option to disabled mouse pointer so that it is shown on the screen. The pointer is enabled if any mouse activity occurs.
EnableLocal={no**, yes} [HideDefault={**no**, yes}]	Yes/no option to enable locally configured entries to show in the Connect Manager list. When connections defined in local NV-RAM are displayed in the Connect Manager, they are marked with an asterisk. If EnableLocal=yes is in a wnos.ini file, then the global information will be saved into NVRAM. The global information includes: SEAMLESS, ALTERNATE, Reconnect, IcaBrowsing, LowBand, NoReducer, Time settings, and Printer settings in a wnos.ini file. HideDefault—Yes/no option to hide the default ICA and RDP connections that are present on the devices.
*EthernetSpeed={**Auto**, 10M HD, 10M FD, 100M HD, or 100M FD}	EthernetSpeed—Specifies the EthernetSpeed to either Auto, 10M HD, 10M FD, 100M HD, or 100M FD. After being specified, it is saved in the non-volatile memory. This parameter can be replaced by the Device and Speed parameters. ⚠ **Caution** If the EthernetSpeed parameter value is changed, the thin client will require a reboot.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
FactoryDefault={**no**, yes}	Yes/no option to reset the system settings 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). ⚠ **Caution** If the FactoryDefault parameter value is changed to yes, the thin client will reboot without notice to the user.
FastDisconnet={**no**, yes}	Yes/no option to use F12 key press to disconnect an ICA session.
FastDisconnectKey={F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Pause\Break}	Specifies the disconnect key that will disconnect an ICA session.
FixLicense={Factory, clean, yes, **no**, OldFormat}	Specifies the option to replace the TSCAL license stored in the non-volatile memory. **Note** The OldFormat value specifies to keep the same license format as version 5.2.x of the TSCAL license.
HideIP={**no**, yes}	Yes/no option to hide the information of the connection host or IP. Some examples 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.
icaBrowsing={udp**, http}	Establishes the default browsing protocol. This setting can be overridden by the parameter HttpBrowsing in each connection property. The method of browsing selected must match the method provided by the servers being accessed. This setting in a wmos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file.
Inactive={0**, 10 to 480} (minutes)	Specifies the inactive time before timeout. No Idle timeout=0. Inactive range can be set from 10 minutes to 480 minutes.
*Include=path/filename	**For {username}.ini file only**. Specifies to include another INI file at the position of this parameter. Only one level of including is allowed (no nesting) and only for a {username}.ini file

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
KeySequence={no, yes} [Ctrl+Alt+Del={**no**, yes}] [Ctrl+Alt+Up={no, **yes**}] [Ctrl+Alt+Down={no, **yes**}] [Ctrl+Alt+Left={no, **yes**}] [Ctrl+Alt+Right={no, **yes**}]	KeySequence—Yes/no option to enable the combined keys options. Ctrl+Alt+Del—Yes/no option to enable Ctrl+Alt+Del to lock the thin client if the user is signed in with a password (if the user is signed in without a password, this key sequence does not work). Ctrl+Alt+Up—Yes/no option to enable Ctrl+Alt+Up to toggle a session between fullscreen and window mode. Ctrl+Alt+Down—Yes/no option to enable Ctrl+Alt+Down to toggle between task selections. Ctrl+Alt+Left—Yes/no option to enable Ctrl+Alt+Left Arrow to lock the thin client if the user is signed in with a password (if the user is signed in without a password, this key sequence does not work). Ctrl+Alt+Right—Yes/no option to enable Ctrl+Alt+Right Arrow to lock the thin client if the user is signed in with a password (if the user is signed in without a password, this key sequence does not work).
Language=code [Charset={ISO-8859-1**, ISO-8859-2, ISO-8859-5, ISO-8859-7}]	Language—Specifies the language to use on the desktop display. After beingspecified in a wnos.ini file, it is saved in non-volatile memory. The code used must be exactly the same as the character string shown in the keyboard language list in Keyboard Language Codes, page 3-25. Charset—Specifies which ISO option to use: • ISO-8859-1—Supports part 1 of the standard character encoding of the Latin alphabet. • ISO-8859-2—Supports the Czech, Hungarian, Polish, Romanian, and Slovenian languages on the desktop display. • ISO-8859-5—Supports Cyrillic characters on the desktop display. • ISO-8859-7—Supports the Greek language on the desktop display. For the list of codes supported, see Keyboard Language Codes, page 3-25.
LowBand={no**, yes}	Yes/no option to enable optimization for low speed connections (on all connections), such as reducing audio quality or decreasing protocol-specific cache size. This setting in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file.
LpdSpool={0, 1, 2, 3, 4, **5**, 6, 7, 8, 9, 10}	Specifies the size of spool to buffer all data before sending it to the LPD printer.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
**MouseSpeed=value	Values specifies the mouse speed. **Note** "ini=(null)" means 0 (for number) or "NULL" for strings. • 0—Slow • (null)—Slow • **1**—Normal (default) • 2—Fast
**MouseSwap={0, 1}	0/1 option to swap the mouse buttons (for example, for left-handed use). • 0—No • 1—Yes
NetworkPrinter=host/queue [PrinterID=Window driver name] [Enabled={no, **yes**}]	NetworkPrinter—Specifies the configuration for the network (LPD) printer in the same way as described for the Printer Setup dialog box in the *Cisco Virtualization Experience Client 2112/2212 ICA Administration Guide for WTOS*. The host and queue parameters define the IP address and queue name of the printer. PrinterID—Specifies the Windows printer driver name. Enabled—Yes/no option to enable the network (LPD) printer.
NoReducer={no**, yes}	Yes/no option to turn off compression. Default is no, which enables compression. To turn off compression, enter yes. Used here this parameter is a global statement for all connections. It sets the default value of NoReducer. **Note** By default both the ICA and RDP protocols compress their data to minimize the amount of data that needs to traverse the network. This compression can be as much as 50% for text-based applications (for example, Microsoft Word) and 40% less for graphics applications than the uncompressed data streams.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
Password=sign-on password [encrypt={no**, yes}]	Specifies the password as the sign-on password. In a wnos.ini file—If set to the default password, the system will sign on automatically and not wait for username, password, and domain entries In a [username].ini file—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-in dialog box. encrypt—Yes/no option to use an encrypted string for a password in the INI file instead of clear text. If encrypt=yes, the password in the INI is an encrypted string instead of cleartext. For example: Password=ciscoatc@123 or Password=NCAONIBINMANMLCOLKCNLL \ encrypt=yes

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
PnliteServer=List of {IP address, DNS names, or URLs} [ReconnectAtLogon={**0**, 1, 2}] [ReconnectFromButton={**0**, 1, 2}] [AutoConnectList={*/ appname1;appname2; appname3...}] [timeout=5…300] [CAGRSAAuthMethod=RSASecurid]	PnliteServer—Specifies the list of IP addresses or host names with optional TCP port number or URLs of PNAgent/PNLite servers (by default the list is 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. After being 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** PnliteServer and the DomainList parameters can be used in a {username}.ini file, but generally are used only in a wnos.ini file. **Note** The PNAgent/PNLite server list and associated domain list optionally can be entered in DHCP server options 181 and 182, respectively. If entered in both places, the entries from this table will take precedence. However, the {username}.ini file will override the wnos.ini file if the identical parameters with different values exist in the {username}.ini file. **Note** When Multifarm=yes, use # to separate failover servers, and use a comma (,) or a semicolon (;) to separate servers that belong to different farms. ReconnectAtLogon—Specifies the reconnection function at sign-in. • 0—disables the option • 1—reconnects to disconnected sessions only • 2—reconnects to active and disconnected sessions ReconnectFromButton—Specifies the reconnection function from the reconnect command button. • 0—disables the option • 1—reconnects to disconnected sessions only • 2—reconnects to active and disconnected sessions AutoConnectList—Specifies the PNA applications that will be automatically launched when using PNA to sign-in. If AutoConnectList=*, then all the PNA applications will be automatically connected.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
(continued) PnliteServer=List of {IP address, DNS names, or URLs} [ReconnectAtLogon={0, 1, 2}] [ReconnectFromButton={0, 1, 2}] [AutoConnectList={*/ appname1;appname2; appname3...}] [timeout=5…300] [CAGRSAAuthMethod=RSASecurid]	Timeout—Specifies the time (in seconds) a client will try to establish a connection before reporting that it is unreachable. CAGRSAAuthMethod=RSASecurid—Specifies CAGRSAAuthMethod to enable the Dual Authentication feature where RSA + Domain credentials will be used when authenticating with a Nestscaler/CAG platform. For example: pnliteserver = https://cag2.qaxen.com \ CAGRSAAuthMethod = RSASecurid
Printer={**COM1**, COM2, LPT1, LPT2} [Name=name] [PrinterID=window_driver] [Class=classname] [Enabled={no, **yes**}] [EnableLPD={**no**, yes}]	Printer—Specifies the local printer to configure. Name—Specifies the name of the printer and is required. PrinterID—If not specified, the default Generic/Text Only is used. Class—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. Class can be a string with 7 characters. Enabled—Yes/no option to enable the printer. EnableLPD—Yes/no option to enable the LPD service. **Note** The parameters must be specified in the order shown.
Printer={**LPD1**, LPD2, LPD3, LPD4} [LocalName=name] [Host= host] [Queue=queue] [PrinterID=window_driver] [Class=classname] [Enabled={no, **yes**}]	Printer—Specifies the LPD printer to configure. LocalName—Specifies the name of the printer. If LocalName is not specified, the Queue name is used. Host—Specifies the host name of the printer. Queue—Specifies the queue name of the printer. PrinterID—Specifies the windows driver to use for the printer. If not specified, the default Generic/Text Only is used. Class—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. Class can be a string with 7 characters. Enabled—Yes/no option to enable the printer. These settings in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file. **Note** The parameters must be specified in the order shown. LPD is accepted as LPD1.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
Printer={**SMB1**, SMB2, SMB3, SMB4} [LocalName=name] [Host=\[domain]\host] [Name=share_name] [PrinterID=window_driver] [Class=classname] [Enabled={no, **yes**}] [EnableLPD={**no**, yes}] [Username=username] [Password=password] [Domain=domain name]	Printer—Specifies the shared Microsoft network printer to configure. LocalName—Specifies the name of the shared printer. Host—Specifies the host name of the shared printer specified as \domain\host when the host is configured within a Microsoft domain (otherwise, host can be specified as \\host). Name—Specifies the shared name of the shared printer. PrinterID—Specifies the windows driver to use for the printer. If not specified, the default Generic/Text Only is used. Class—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. Class can be a string with 7 characters. Enabled—Yes/no option to enable the printer. EnableLPD—Yes/no option to enable the LPD printer. Username—Specifies the username of a user who can use the SMB printer. Password—Specifies the password of a user who can use the SMB printer. Domain—Specifies the domain name of the SMB printer.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter * Global overrides identically named user profile ** After sign-out, user profile returns to global value	Description
PRIVILEGE=[None, Low, **High] [LockDown= {**no**, yes}] [HideSysInfo={**no**, yes}] [HidePPP={**no**, yes}] [HidePN={**no**, yes}] [HideConnectionManager={**no**, yes}] [EnableNetworkTest={**no**, yes}] [EnableTrace={**no**, yes}] [ShowDisplaySettings={**no**, yes}] [EnableKeyboardMouseSettings={no, yes}] [KeepDHCPRequestIP={**no**, yes}] [SuppressTaskBar={**no**, yes, auto}]	Privilege controls operator privileges and access to thin client resources. 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 disabled by default (the Connect Manager can be enabled (visible) by using the HideConnectionManager=no option, however, the user cannot create a new connection or edit an existing connection). The user cannot reset the thin client to factory defaults. Low—This access level is assigned to a typical user. The Network selection on the Setup submenu is disabled (the Network Setup dialog box cannot be opened). The user cannot reset the thin client to factory defaults. High—Administrator access level allows all thin client resources to be available with no restrictions. A user can reset to factory defaults. **Note** If 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. LockDown—Yes/no option to allow lockdown of the thin client. If yes is specified, the system saves the privilege level in flash. If no is specified, the system clears the privilege level from flash to the default unlocked state. ⚠ **Caution** If the thin client is set to LockDown without a High privilege level, it will disable the G key reset on power-up. **Note** LockDown can be 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. 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 file or the {username}.ini file or the network is unavailable, the setting of LockDown will take effect. It can be modified by a clause. For example, privilege=<none|low|high> lockdown=yes in a wnos.ini file or a {username}.ini file sets the default privilege to the specified level.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
(continued) **PRIVILEGE=[None, Low, **High**] [LockDown= {**no**, yes}] [HideSysInfo={**no**, yes}] [HidePPP={**no**, yes}] [HidePN={**no**, yes}] [HideConnectionManager={**no**, yes}] [EnableNetworkTest={**no**, yes}] [EnableTrace={**no**, yes}] [ShowDisplaySettings={**no**, yes}] [EnableKeyboardMouseSettings={no, yes}] [KeepDHCPRequestIP={**no**, yes}] [SuppressTaskBar={**no**, yes, auto}]	HideSysInfo—Yes/no option to hide the System Information from view. HidePPP—Yes/no option to hide the Dialup Manager, PPPoE Manager, and PPTP Manager from view. HidePN—Yes/no option to hide the PNAgent or PNLite icon from view on the taskbar. HideConnectionManager—Yes/no option to hide the Connect Manager window from view. **Note** As stated earlier, although the Connect Manager is disabled by default if Privilege=none, the Connect Manager can be enabled (visible) by using HideConnectionManager=no (however, the user cannot create a new connection or edit an existing connection). EnableNetworkTest—Yes/no option to enable the Network Test. EnableTrace—Yes/no option to enable trace functionality (active items are added to the desktop right-click menu in Privilege=High level). ShowDisplaySettings—Yes/no option to enable the Display Settings in a popup menu. EnableKeyboardMouseSettings—Yes/no option to enable the keyboard and mouse configuration preferences. KeepDHCPREquest—Yes/no option to keep the same IP address that is requested from the DHCP server after a request fails and does not invoke the Network Setup dialog box. SuppressTaskBar—Yes/no/auto option to hide the taskbar (auto will automatically hide/display the taskbar as used). When using this parameter in a wnos.ini file, it will be saved to NVRAM if EnableLocal is set to yes in the wnos.ini file.
Reconnect={no**, yes}	Yes/no option to enable automatic reconnection to an application after a server disconnection. This setting in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter * Global overrides identically named user profile ** After sign-out, user profile returns to global value	Description
RepeatDelay={0, 1, **2, 3, 4, 5, 6, 7}	Specifies the keyboard delay before repeat (in seconds). • 0—1/5 • 1—1/4 • 2—1/3 • 3—1/2 • 4—3/4 • 5—1 • 6—2 • 7—No Repeat
RepeatRate={0, **1, 2}	Specifies the keyboard repeat rate. • 0—Slow • 1—Medium • 2—Fast
[Screen={**1**, 2}]*Resolution=[**DDC**, 640x480, 800x600, 1024x768, 1280x1024, 1360x768, 1400x1050, 1440x900, 1600x1200, 1680x1050] [Refresh=60, **75**, 85} [rotate={left,none,right}]	Screen—Specifies the monitor for the Resolution parameter. You can configure each monitor with its own resolution; the specific monitor is set with the Screen= option (default value is 1). Resolution—Specifies the local display resolution. Option DDC can be specified to select default display resolution. Refresh—Specifies the local display refresh rate. ⚠ **Caution** If the Resolution or Refresh parameter values are changed, the thin client will reboot without notice to the user. rotate—Rotate is an experimental feature allowing you to rotate monitors for viewing in Portrait mode. For example: screen=1 resolution=1280x1024 refresh=60 rotate=none
SaveSysinfo={usb}	Specifies that the WTOS event logs will be saved into the last mounted USB disk. The file used for saving Event log information is named WTOS_log.txt and is located at the root path of the USB disk.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
ScardLog=0xF	A bitmask controlling the following logs: • 0x1—Context log • 0x2—Handle log • 0x4—Status log • 0x8—Transfer log

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter * Global overrides identically named user profile ** After sign-out, user profile returns to global value	Description
ScreenSaver={0, 1, 5, 10, **15, 30, 60, 120, 180} [LockTerminal={**0**, 1, 2}] [Type={0,1, 2}] [Image=imagefile]	Screensaver—Specifies to put the thin client in a screensaver state when the inactivity (delay before starting) time limit is reached. Value and delay before starting the screensaver: • 0—Disabled • 1—1 Minute • 5—5 Minutes • 10—10 Minutes • 15—15 Minutes • 30—30 Minutes • 60—1 Hour • 120—2 Hours • 180—3 Hours LockTerminal—Specifies the thin client LOCK state function when the screen saver is activated. • 0—Disabled • 1—Puts the thin client in a LOCK state when the screen saver is activated. The user is prompted with an unlock dialog box to enter the sign-in password to unlock the thin client. LockTerminal settings are saved into NVRAM if LockTerminal=1 and EnableLocal=yes is set in the wnos.ini file. • 2—Puts the thin client in a LOCK state when the screen saver is activated, however, the unlock dialog box cannot be viewed and the desktop will use Blank the Screen as the screensaver. **Note** The user must be signed in with a password for a Lock action to take effect. **Note** If set in KeySequence, users can lock the thin client at any time by pressing Ctrl+Alt+Left Arrow or Ctrl+Alt+Right Arrow. Type—Specifies which type of screensaver to use. • 0—Blank the Screen • 1—Flying Bubbles • 2—Moving Image Image—Specifies an image file residing in the subfolder bitmap (under the home folder) to use as a screensaver Moving Image. **Note** If Type=2 and no image file is specified, then the default Cisco logo image is used.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
Seamless={no**, yes} [HideTaskbar={**0**, 1, 2, 3}] [FullscreenReserved={**no**, yes}]	Seamless—Yes/no option to set the default resolution for ICA published applications to Seamless for ICA connection parameters. HideTaskbar—Specifies the status of the taskbar when maximizing the seamless window. 0—Do not hide the taskbar 1—Taskbar will be hidden when maximizing the seamless window to full screen. Moving the mouse over the lowest bottom of the screen will display the taskbar. This setting (not including the FullscreenReserved parameter) in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file. 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. When set Seamless=yes HideTaskbar=3, the maximized size does not cover the taskbar, but the session size on the server side is reported as the full-screen size. When set Seamless=yes FullscreenReserved and the applications are configured for fullscreen mode, they will be launched in fullscreen mode, not seamless mode.
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={**no**, yes}] [Touch_XYReverse={**no**, yes}] [Touch_type={**elo**, microtouch, fastpoint}]	Serial—Specifies the local serial ports configuration. Baud—Specifies the local serial port baud rate. Parity—Specifies the local serial port parity. Stop—Specifies the local serial port stop. Size—Specifies the local serial port size. Flow—Specifies the local serial port flow. Touch—Yes/no option to denote that a serial touch screen is attached. Touch_XYReverse—Yes/no option to denote a reversal of the X and Y coordinates (needed for some touch screens). Touch_type—Specifies the type of touchscreen being used. **Note** Parameters must be specified in the order shown.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
SessionConfig=ALL [unmapprinters={no**, yes}] [unmapserials={**no**, yes}] [smartcards={**no**, yes}] [mapdisks={**no**, yes}] [disablesound={**no**, yes}] [unmapusb={**no**, yes}] [DisksReadOnly={**no**, yes}] [MouseQueueTimer={0-99}] [OffScreen={**no**, yes}] [UnmapClipboard={**no**, yes}] [DefaultColor={0,1,2}]	SessionConfig—Specifies the default settings of the optional connection parameters for all sessions. unmapprinters—Yes/no option to un-map printers. unmapserials—Yes/no option to un-map serials. smartcards—Yes/no option to use smartcards. mapdisks—Yes/no option to map disks. disablesound—Yes/no option to disable sound. unmapusb—Yes/no option to un-map USBs. DisksReadOnly—Yes/no option to mount mass storage disks as read-only. MouseQueueTimer—Specifies the default queue timer of a mouse event in an ICA or RDP session (in 1/100 of a second). It can be used to adjust the bandwidth of a network. USB for all ICA and RDP sessions. OffScreen—(**ICA Only**) Yes/no option to enable offscreen support for all sessions. When using this parameter in a wnos.ini file, it will be saved to NVRAM if EnableLocal is set to yes in the wnos.ini file. UnmapClipboard—Yes/no option to disable clipboard redirection for all sessions. For ICA and RDP, specifies if redirecting the clipboard. This setting in wnos.ini will be saved into nvram if EnableLocal is set to yes in wnos.ini. The option keyword DefaultColor specifies the default color depth session would use.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
SessionConfig=ICA [desktopmode={fullscreen**, window}] [mapdisksunderz={**no**, yes}] [DiskMapTo=a character sequence] [OutBufCount=count] [SysMenu={remote, **local**}] [SessionReliability={**no**, yes}] [ondesktop={**no**, yes, all, none, desktops, applications}] [ProgressiveDisplay={**no**, yes}] [BranchRepeater={**no**, yes}] [DisableIcaPing={**no**,yes}] [AudioQuality={**default**, high, medium, low}]	SessionConfig—Specifies the ICA default settings of the optional connection parameters for all ICA sessions. desktopmode—Specifies the display mode of an ICA published desktop when using an ICA PNAgent sign-in (the default is fullscreen mode for a PNA desktop application). mapdisksunderz—Yes/no option to map disks under the Z drive. **Note** mapdisksunderz=yes takes effect only if mapdisks=yes. DiskMapTo—Specifies to map disks to a character sequence. **Note** A sequence of characters can be used by DiskMapTo, with each letter mapped to one disk in order. For example, if RTNM is the sequence, R is mapped to the first disk (in WTOS, it will be D:/), T is mapped to the second disk (in WTOS, it will be E:/), and so on. Only the letters “a” through “y” and “A” through “Y” are accepted (all lowercase letters are changed to uppercase; other characters will be skipped; and duplicate characters will be omitted). For example, #GGefZzedAF1JaE will be mapped to GEFDAJ. The number of disks mapped to the session depends on the number of valid letters provided. If no letter is provided, all disks will be mapped to the session using default driver letters. OutBufCount—Specifies the output buffer count of the ICA server and client (the default value is 0x2c). SysMenu—Specifies the system menu mode when right-clicking the taskbar button of a seamless window. If it is remote, the system menu will come from the remote server; otherwise, it will be the local menu. SessionReliability—Yes/no option to enable session reliability. ondesktop—Specifies options for displaying connection icons on the desktop: • If AutoConnectList is set in the PNLiteServer statement, all connections configured in AutoConnectList parameter will display on the desktop. • Default is no and means that the property of ondesktop will be controlled by the server. However, the connections are still always added to the Connect Manager list and PNA menu list

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
(continued) **SessionConfig=ICA [desktopmode={**fullscreen**, window}] [mapdisksunderz={**no**, yes}] [DiskMapTo=a character sequence] [OutBufCount=count] [SysMenu={remote, **local**}] [SessionReliability={**no**, yes}] [ondesktop={**no**, yes, all, none, desktops, applications}] [ProgressiveDisplay={**no**, yes}] [BranchRepeater={**no**, yes}] [DisableIcaPing={**no**,yes}] [AudioQuality={**default**, high, medium, low}]	• In cases other than no, the connection is controlled by the local thin client. If set so that the connection icon does not display on the desktop, the connection icon will also not be added to the Connect Manager list nor the PNA menu list. all—same as yes, display all connections on desktop none—do not display any connections desktops—only display connections on desktop applications—only display applications, the connections will be handled as an ondesktop_list. For example, if you set ondesktop="word; excel", then only the applications “word” and “excel” will be displayed. **Note** The ondesktop_list also supports wildcard “*” like AutoConnectList parameter in PNLiteServer. For example, if set ondesktop= “*IE*”, any application which name includes the string “IE” (“farm1:IE”, “farm2:IExplore”, and so on) will be shown. ProgressiveDisplay—Yes/no option to enable Progressive Display support in ICA. BranchRepeater—Yes/no option to enable a branch repeater function including Reducer V3 and High Throughput. DisableIcaPing—Yes/no option to disable ping. Default is no. AudioQuality—Specifies the audio quality of ICA sessions. **Note** Medium quality is recommended for Speech scenarios. For example: SessionConfig=ICA AudioQuality=high

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
SessionConfig=RDP [MaxBmpCache={128 to 1024}] [DefaultColor={0,1,2}] [EnableNLA]={no,yes**}] [EnableTSMM[7.1_006]={yes,no}] [ForceSpan[7.1_006]={no,yes}]	SessionConfig—Specifies the RDP default settings of the optional connection parameters for all RDP sessions. MaxBmpCache—Specifies the maximum bitmap cache number (this impacts the memory usage of an RDP session). DefaultColor—Specifies auto (0), 16-bit (1), and 32-bit (2) options. EnableNLA—Yes/no option to enable the Network Level Authentication feature in RDP 7 (default is yes). The option EnableTSMM=yes can enable RDP7 Multimedia redirect. Default is yes. For example: SessionConfig=RDP MaxBmpCache=1024 \ DefaultColor=1 EnableNLA=no The option ForceSpan=yes can disable RDP Multi Monitor feature. Default is no.
SessionConfig=RDP [MaxBmpCache={128 - 1024}] [DefaultColor={0,1,2}] [EnableNLA[7.0.0_23]={yes,no}] [ForceSpan[7.1_009]={yes,no}] [EnableTSMM[7.1_009]={yes,no}] [EnableRecord[7.1_009]={yes,no}]	Set “RDP” to establish the default setting for RDP sessions. The option keyword MaxBmpCache specifies the maximized bitmap cache number. It will impact the memory usage of an RDP session. The option keyword DefaultColor specifies the default color depth session would use The option EnableNLA=yes can enable RDP NLA authentication login. Default is yes. The option ForceSpan=yes can disable RDP Multi Monitor feature. Default is no. The option EnableTSMM=yes can enable RDP7 Multi-media redirect. Default is yes. The option EnableRecord=yes can enable RDP feature of recording from local. Default is no. For example: SessionConfig=RDP MaxBmpCache=1024 DefaultColor=1 EnableNLA=yes ForceSpan=yes EnableTSMM=no EnableRecord=yes
**ShutdownCount={0 to 60} (seconds) or **ShutdownCounter={0 to 60} (seconds)	ShutdownCount or ShutdownCounter—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 (default is 10, however, to commence shutdown immediately and prevent the display of the countdown pop-up dialog box, set the value to 0).

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
ShutdownInfo={no, yes}	Yes/no option to display various information (such as System Version, Terminal Name, IP Address, and MAC Address) in shutdown window.
TimeServer=server_list [TimeFormat={"**24-hour format**", "12-hour format"}] [DateFormat={**yyyy/mm/dd**, mm/dd/yyyy, dd/mm/yyyy}] [GetBiosDT={**no**, yes, 0, 1}]	TimeServer—Specifies the SNTP time servers to use for time retrieval. TimeFormat—Specifies the time format to use. DateFormat—Specifies the date format to use. **Note** The TimeFormat and DateFormat settings in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file. GetBiosDT—Yes/no option to obtain time from BIOS/CMOS when the timeserver is not available or cannot be contacted.
**UniSession={no, yes}	Yes/no option to launch the connection only once at a time.
VDIBroker=vdi_broker_url [AutoConnectList={*|host1;host2;host3…}]	VDIBroker—Specifies the VDI broker server (supports both http and https). If the vdi_broker_url does not start with http or https, the default protocol used is http. For an https connection, only one URL is accepted. **Caution** If the VDIBroker parameter value is changed, the thin client will reboot without notice to the user so it can reconnect to the new server. AutoConnectList—Specifies the VDI/VDM host which will be automatically launched when using VDI/VDM sign-in. If the value is *, all of the VDI/VDM hosts will automatically be connected.

Table 3-1 Parameters for wnos.ini Files and {username}.ini Files (continued)

Parameter *** Global overrides identically named user profile** **** After sign-out, user profile returns to global value**	**Description**
VirtualCenter=virtual_center_url	Specifies the Virtual Center server (supports both http and https). If the virtual_center_url does not start with http or https, the default protocol used is http. **Caution** If a VirtualCenter in an INI file is different from the original URL, the thin client will reboot for the new URL to take effect. **Note** Only this setting can enable the Virtual Center functions.
VNCPrompt={no, **yes} [{Accept, Reject}={**10** to 600} (seconds)] [ViewOnly={**no**, yes}] [ActiveVisible={**no**, yes}]	VNCPrompt—Yes/no option to enable a VNC shadowing prompt to a user (VNCPrompt set to yes means the user will always be prompted before shadowing starts and the user will then decline or accept VNC shadowing; VNCPrompt set to no means the user will not be able to decline or accept shadowing). Accept, Reject—Specifies the amount of time (in seconds) a user has to accept or reject the VNC shadowing prompt before the client desktop is shadowed. ViewOnly—Yes/no option to specify that the desktop being shadowed can only be viewed by the person who is shadowing (no keyboard or mouse events are allowed to interfere with the thin client being shadowed). ActiveVisible—Yes/no option to display a VNC session-end notice after the VNC session ends.

Keyboard Language Codes

Table 3-2 contains the description and codes for keyboard languages

Table 3-2 Keyboard Language List—Description and Code

Arabic (Algeria)—Ar_alg	Arabic (Bahrain)—Ar_bah
Arabic (Egypt)—Ar_egy	Arabic (Iraq)—Ar_ira
Arabic (Jordan)—Ar_jor	Arabic (Kuwait)—Ar_kuw
Arabic (Lebanon)—Ar_leb	Arabic (Libya)—Ar_lib
Arabic (Morocco)—Ar_mor	Arabic (Oman)—Ar_oma
Arabic (Qatar)—Ar_qat	Arabic (Saudi Arabia)—Ar_sau
Arabic (Syria)—Ar_syr	Arabic (Tunisia)—Ar_tun
Arabic (U.A.E.)—Ar_uae	Arabic (Yemen)—Ar_yem
Brazilian—Br	Canadian Multilingual—ca_ml

Table 3-2 Keyboard Language List—Description and Code (continued)

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**
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 (see Note)	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	

Note In the preceding table, Japanese refers to Japanese Input system (MS-IME2000), not JP.

Note The Russian keyboard is only supported for server input; it is not supported for local input.

APPENDIX A

ICA and RDP Connection Options

This appendix provides the supported options that you can use for ICA and RDP connections.

Options for ICA and RDP Connections

Table A-1 contains the supported options you can use for ICA and RDP connections (after Connect=ICA or Connect=RDP). Options with bold values (defaults) are required options for an ICA or an RDP connection (those options without bold values are optional).

Note Any option in Table A-1 that is used in a {username}.ini file will return to the default value set for that option in the wnos.ini file after a user sign-out. For example, if your {username}.ini file contains the option Reconnect=yes (so that a lost connection will restart 20 seconds after disconnection) and you sign out of the thin client, then the Reconnect value will return to the original default value of no (Reconnect=no) contained in the wnos.ini file—so that others who sign in can use their own "user profile" (assuming the administrator has not changed the default values in the wnos.ini file).

Table A-1 Options for ICA and RDP Connections

Option	Description
Alternate=[**no**, yes]	**ICA Only**. Yes/no option to use an alternate IP address returned from an ICA master browser to get through firewalls.
AudioQualityMode={**0**, 1, 2, 3}	**ICA Only**. Specifies the audio quality of a session. Default = 0. • 0 Default • 1 High Quality • 2 Medium Quality • 3 Low Quality
Autoconnect={**0** to 99}	Use for automatically starting a session (after sign-in, if sign-in is enabled). The value of 0–99 is the delay in seconds before auto-starting the session.
AppendUsername=1	This enhancement allows user names to display in the title bar of an ICA session at the client side.
BranchRepeater ={**no**, yes}	**ICA Only**. Yes/no option to enable a branch repeater function including Reducer V3 and High Throughput.

Table A-1 Options for ICA and RDP Connections (continued)

Option	Description
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. For faster display performance, use 256 colors for the session. **Note** 64k is the same value as high. 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 signing in to the server. This entry is limited to 127 characters.
Console={**no**, yes}	**RDP Only**. Yes/no option to sign-in to a session in Console mode. **Note** If Console=yes is set behind the RDP connection, the TimeZone redirection feature will be disabled.
Description=string description	Connection description. Enclose the string description in quotation marks if there are embedded blanks or single quotes. For quotation marks, use common-practice nesting rules. Maximum of 38 characters are allowed.
Directory=working directory	A directory to be used as the working directory after signing in to the server. Maximum of 63 characters is allowed.
Disablesound={**no**, yes, 2} or {**0**, 1, 2}	Specifies whether or not to disable remote sound upon connection start. **Note** Disablesound=2 only works in RDP sessions and indicates that the remote computer sound should be disabled at the remote computer.
Domainname={domain name,$DN}	Domain name to use in a Windows network. $DN specifies that the thin client sign-in domain name is used. Maximum of 19 characters is allowed.
Encryption={None, **Basic**, 40, 56, 128, Login-128}	**ICA Only**. Connection security encryption level. The highest level is 128-bit security (Login-128 option is 128 bit encryption for sign-in only). The lowest is None. **Note** The server must support the specified level of encryption or the connection will fail.
Fullscreen={**no**, yes}	Yes/no option to run the session in full screen. If Fullscreen=no then the session runs in a windowed screen.
Host=[name, IP, $SYS VAR] or Application=published application	Host—A list of server hostnames or IP addresses to which the thin client will attempt to connect (the next server on the list is attempted if the previous one failed). List items must be separated by semicolons or commas. **Note** $UN (see Table 1-1 on page 1-3) specifies that the sign-in user name is used and should be set in a {username}.ini file. If set to Host=$UN in a {username}.ini file, the hostname will display as the sign-in user name. If set to Host=$UN in a wnos.ini file, the hostname will display as the default Start. Application—For **ICA Only** and defines the published application to launch. Application is required if no host is specified.

Table A-1 Options for ICA and RDP Connections (continued)

Option	Description
HttpBrowsing={**no**, yes}	**ICA Only**. Yes/no option to select an http browsing protocol. Use HttpBrowsing=no for User Datagram Protocol (UDP). **Note** This option is used to override the default method of browsing established in the ICABrowsing parameter (see Table 3-1).
Icon={default, bitmap file}	Specifies an icon to appear on the thin client desktop for a connection. Use Icon=default to display a system default icon for a connection. To use an icon other than the default icon, enter the name (with extension) of the bitmap file (ensure that the file is located in the FTP server wnos\bitmap directory). If Icon= is not specified and the icon is not specified by a PNAgent/PNLite server, no icon is displayed for a connection.
KeepAlive={0 to 127}	Specifies the number of minutes to keep a session connected (alive) after the session is inactive. During this period, one dummy packet will be sent to the server if network traffic is lost. Default=10.
LocalCopy={**no**, yes}	Yes/no option to save the connection to the local NVRAM. The connection description of the Description option 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. Maximum total of local entries is 16.
Logon_mode={**local-user**, smartcard, user-specified}	**ICA Only**. Specifies how users authenticate to the selected application set or ICA connection.
Logon_mode=prompt RDP Only.	Specifies one dialog box will pop up to allow a user to enter username, password, and domain before connecting to the RDP session. This can prevent the need to input credentials twice in some cases of server redirection (load balancing).
Lowband={**no**, yes}	Yes/no option to enable optimization for low speed connections (such as reducing audio quality and/or decreasing protocol-specific cache size).
Mapdisks={**no**, yes}	Yes/no option to auto-connect and map any connected USB flash drive upon connection start.
Mapdisksunderz={**no**, yes}	**ICA Only**. Yes/no option to map disks under a Z volume label. **Note** Mapdisksunderz=yes takes effect only if Mapdisks=yes.
NoReducer={**no**, yes}	Yes/no option to turn off compression. Default is no, which enables compression. To turn off compression, enter yes. Used here this option is an option of the “Connect” statement. It sets the value of NoReducer only for this specified connection. **Note** By default both the ICA and RDP protocols compress their data to minimize the amount of data that needs to traverse the network. This compression can be as much as 50% for text-based applications (for example, Microsoft Word) and 40% less for graphics applications than the uncompressed data streams.
OffScreen={**no**, yes}	**ICA Only**. Yes/no option to enable offscreen support for a session. When using this option in a wnos.ini file, it will be saved to NVRAM if EnableLocal is set to yes in the wnos.ini file.

Table A-1 Options for ICA and RDP Connections (continued)

Option	Description
Password={password, $SYS_VAR}	Password to sign-in to the application server. Either a conventional sign-in password or a variable can be used. Maximum of 19 characters is allowed. The value of password is a conventional sign-in password. The value of $SYS_VAR is a system variable found in Table 1-1 on page 1-3. **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-in password (which does starts a line). **Note** The Password option is not written into a {username}.ini file by a user. When the New Password check box is selected, the system writes the new, changed password into the {username}.ini file with encryption. This password is then checked against the sign-in password with encryption to determine whether sign-in is successful.
Password-enc= an encrypted password	Specifies an encrypted string as a password for a connection. Reconnect={no, yes, 1 to 3600 (seconds)}
RDPAudioQualityMode={**0**, 1, 2}	**RDP Only**. Specifies the audio playback quality of an RDP session. 0—Dynamic; 1—Medium; 2—High; Default = 0.
RDPAudioRecord={**no**, yes}	**RDP Only**. Yes/no option to specify whether users can record audio to the server (requires Windows 7 Server). Default is no.
Rdp_No_Animation={**no**, yes}	**RDP Only**. Yes/no option to disable the Menu and Window animation feature (use yes to disable the feature).
Rdp_No_Dragging={**no**, yes}	**RDP Only**. Yes/no option to disable the Show content when dragging a window feature (use yes to disable the feature).
Rdp_No_Fontsmoothing={**no**, yes}	**RDP Only**. Yes/no option to disable the Font smoothing feature (use yes to disable the feature).
Rdp_No_Theme={**no**, yes}	**RDP Only**. Yes/no option to disable the Theme feature (use yes to disable the feature).
Rdp_No_Wallpaper={**no**, yes}	**RDP Only**. Yes/no option to disable the Wallpaper feature (use yes to disable the feature).
Reconnect={**no**, yes, 1 to 3600 (seconds)}	Controls automatic reconnection to an application after a server disconnection. yes—Use to restart the connection (the default delay time for yes reconnect is 20 seconds). no—Use to prevent reconnection after a disconnect. 1 to 3600—Use an integer value of 1 to 3600 seconds to restart the connection after the delay you want (for example, use 50 and the automatic reconnection to an application will occur after 50 seconds).

Table A-1 Options for ICA and RDP Connections (continued)

Option	Description
Resolution=[**default**, Seamless, VGA_resolution]	Specifies the connection display resolution. default—Starts the connection using the current desktop display setting with no window frame and border. Seamless—(**ICA Only**) Available for use if the connection is to a published application. For Seamless connections, the MetaFrame hosts select the best-fit connection window for applications. VGA_resolution—The VGA resolutions you can use are as follows: • 640X480, 800X600, 1024X768, 1152X864, 1280X720, 1280X768, 1280X1024, 1360X768, 1366X768, 1368X768, 1400X1050, 1440X900, 1600X900, 1600X1200, 1680x1050, 1920X1080, 1920X1200
SessionReliability={**no**, yes}	**ICA Only**. Yes/no option to enable session reliability. **Note** WTOS thin clients do not support UDP browsing to obtain a new configuration about session reliability on the server. The thin client always connects to the default port.
Smartcards={**no**, yes}	**RDP Only**. Yes/no option to use a smart card sign-in server when the connection starts.
UniSession={**no**, yes}	Yes/no option to use a unisession (a connection will launch only once at a time).
UnmapClipboard={**no**, yes}	Yes/no option to disable clipboard redirection for ICA and RDP sessions if redirecting the clipboard.
UnmapPrinters={**no**, yes}	Yes/no option to auto-connect to local printers when the connection starts.
UnmapSerials={**no**, yes}	Yes/no option to auto-connect to local serials when the connection starts.
UnmapUSB={**no**, yes}	Yes/no option to auto-connect to local USB devices (Virtual USB) when the connection starts.
Username=[username, $SYS_VAR]	Username to sign-in to the application server. Either a conventional sign-in username or a variable can be used. Maximum of 31 characters is allowed. The value of username is a conventional sign-in username. The value of $SYS_VAR is a system variable found in Table 1-1 on page 1-3. **Note** The combination of all the variables such as $IP@$DN are also supported.
Username-enc= an encrypted username	Specifies an encrypted string as a username for a connection.

APPENDIX B

Sample INI Files

The following sections provide sample INI files that you can reuse and modify to configure your WTOS environment:

Sample User INI File

```
#
# This is an example of a file that specifies an environment for a
# particular user.  If the sign-on name is user1, this file would
# be named user1.ini and must be located in the ini subdirectory
# of the wnos directory.  This file completes the environment
# description started by wnos.ini, in that it contains additional
# connection definitions, specification of a display resolution to
# be used for this user, and (possibly) designation of this user
# as one who has additional privileges.
#
# CAUTION:  The user PASSWORD string is included here for reference
# only.  It must not be created manually or modified by the network
# administrator. It is an encrypted string generated and entered
# by the Cisco VXC unit; it can be changed only by the user via
# the Cisco VXC Change Password dialog box (see Cisco VXC
# ICA Appliance Users Guide). Initially a new user account does
# not require a password, but as soon as one is entered (or
# subsequently changed) the Cisco VXC device encrypts it and places
# the encryption string on the first line of this file. If the user
# forgets the password for this account, the network administrator
# can delete the entire PASSWORD line to allow the user to create a
# new password. The format is:
#
#    PASSWORD = [Encrypted user password string created by
#                the Cisco VXC]
#
# The following password entry was automatically encrypted and
# entered by a Cisco VXC as a result of typing "user" as the
# password.
#
PASSWORD = lFmaRU6KufIAU
#
# The following directive establishes this user as one who has the
```

```
# ability to view and alter the network configuration on any
# Cisco VXC on which this user is logged in.  It also grants the
# ability to temporarily define new connections and view and/or
# temporarily alter existing connection definitions using the
# Connection Settings dialog box.  If the argument to this
# directive is set to zero or if the directive is omitted from
# the user1.ini file, the individual(s) using this sign-on do not
# have this privilege.
#
privilege=1
#
# The following directive establishes the maximum display
# resolution available to this user.  If the attached display
# device is capable of communicating with the Cisco VXC using the
# DDC II protocol and the monitor has a lesser display capability
# than contained in the directive, the lower resolution will be
# used.  Even if the monitor is capable of higher resolutions than
# defined in this directive, they will not be used while this user
# is logged on.  The statement can be used to adapt the device to
# the visual abilities of a user.  The example limits the display
# to an image 800 pixels wide by 600 pixels high.
#
resolution=800x600
#
# The following directive establishes the maximum time a connection
# can be idle before the Cisco VXC will disconnect from the host.
# The default value used if the directive is omitted is zero,which
# means that the client will never disconnect.  Otherwise, the
# units are minutes and the range of acceptable values is from 10
# to 480 (8 hours).  The server may also have a configured idle
# time that is independent of this setting.
#
inactive=150
#
# The following directive describes the ICA connection to a
# published application (WordPad for this example).  The connection
# is started as soon as the user signs on.  When it terminates, the
# user remains signed on and a standard desktop is displayed.  The
# connection can be reactivated by signing off and on again or by
# selecting either the corresponding icon or the entry in the
# Connect Manager dialog box.  Note that the directive is continued
# onto multiple lines.  Continuation is accomplished by putting the
# following characters at the end of each line to be continued:
#
# \<Enter>.
#
# This only works if there is no space between the \ and the
# <Enter> character (the line will not be continued otherwise).
# There must also be a space between each argument on the
# reassembled line.  The continuation sequence does not constitute
# a space; instead, each argument has a trailing blank space.
# Leading <TAB> characters on the continuation line serve the same
# function and also contribute to the overall readability.  The
# function of each of the arguments is:
#
#     connect=ica      Specifies that this is a connect statement
#                      and that the type of connection is ICA,
#                      (currently, ICA is the only supported
#                      connection type). This must be the first
#                      item specified on the line.
#     description="x"  Text to appear either under the icon on the
#                      Cisco VXC desktop or in the Connect Manager
#                      The text must be surrounded by double
#                      quotation marks if it contains space or
```

```
#                       punctuation characters.
#     icon=default      The bitmap to be used for the Cisco VXC
#                       desktop display.  The argument is either
#                       default or a file name.  If a file name is
#                       specified, it must be located in the bitmap
#                       directory under the wnos directory on the
#                       FTP server.
#     username=me       The username on the server which runs the
#                       published application.  The username
#                       determines the privileges and default
#                       directory used on the server.
#     password="x@y"    The password for the specified username.
#                       The password must be surrounded by double
#                       quotation marks if it contains spaces or
#                       punctuation characters.  This is the actual
#                       unencrypted password for the account.
#     domainname=mine   The Windows domain which defines the
#                       specified username.
#     browserip=a,b,c   The IP address(es) or DNS name(s) of
#                       machines that might be the ICA master
#                       browser.  When the master browser is
#                       contacted, it is used to resolve the
#                       application name to a specific server that
#                       can provide the requested service. In this
#                       example, a list of possible master browsers
#                       is provided.  The servers on the list are
#                       accessed in order until one is found that is
#                       operational. That server is consulted for a
#                       resolution of the published application
#                       name.  To establish a connection
#                       successfully, the first operational server
#                       contacted must be capable of resolving the
#                       application name.
#     application=Notepad     The name of an application published
#                       using MetaFrame administrative tools.  This
#                       application will be run when a server has
#                       been selected and the login to the server
#                       is successful.
#     autoconnect=1     The connection will be attempted as soon as
#                       this file has been processed and any
#                       software updates have been completed.
#
# The username, password and domainname fields may be omitted if
# the ICA anonymous user provides sufficient access and privilege
# to accomplish the intended task.
#
connect=ica \
        description="Word processing" \
        icon=default \
        username=me password="x z" domainname=sqa \
        browserip=nil,132.237.176.7 \
        application=wordpad \
        autoconnect=1
#
# The following directive describes the ICA connection to a fixed
# server.  When the connection is activated, it will stop when the
# login dialog box for the ICA server is displayed.  The user must
# log in manually and run applications using a normal desktop
# display.  No master browsers are named, so the host name must be
# either resolvable by the locally contactable ICA master browser
# or by the DNS server in use.  The name will be resolved by
# appending the DNS domain name to the host name and querying the
# DNS servers.  Both pieces of information might be obtained from
# a properly configured DHCP server or might come from the local
```

```
# network configuration.
#
connect=ica \
        host=seven \
        description="Lab machine" \
        icon=lab.bmp

# Note: it is recommended to start each statement at the beginning
#       of a new line, and all continuation options are indented with a Tab
#       character or multiple spaces for readability.
```

Sample Sign-in INI File

```
#
# This file provides an example of an environment where all users
# will log on following processing of this file.  Each user will
# have (potentially) a different desktop display of available
# connections.  Each user may have a different password for
# authentication.
#
# The user desktop displayed following sign-on will be a combination
# of connections specified here (global) and connection specified
# in their individual environment specifications.  Cisco VXC
# is capable of accepting up to 16 connection definitions, total.
# Those defined globally will be displayed first, followed by those
# specified for the individual. If the sum of the number of
# connections in the two files exceeds sixteen only the first
# sixteen will be processed.
#
# The following directive enables the use of the sign-on dialog box.
#
signon=1
#
# The following directive allows the Cisco VXC to attempt to
# locate code files on the FTP server and to update the current
# code on the device if the version on the server is different.
#
autoload=1
#
# The following URL specifies a bitmap file which overlays the top
# left part of the sign-on dialog box.  It can be used to present a
# company logo, special instructions for the day (of limited length)
# or any other desired customization. The Cisco VXC will attempt to
# locate the file in the directory named bitmap, directly under the
# directory named wnos, which contains this file.
#
formurl=blazer.bmp
#
# The following directive causes the Cisco VXC to use a different
# FTP server. This overrides and replaces the fileserver in the
# local network setup and/or the one obtained from DHCP option 161.
# It will be used from the time this directive is processed until
# the value in the local user interface is manually edited, until a
# new value is obtained from a DHCP server on reboot, or until
# another fileserver directive is processed.  Until reset using one
# of the named methods, the new value will persist across reboots
# and power cycle events.  The argument may be either an IP address
# or a DNS name.
#
FileServer=filesrv.cisco.com
#
```

```
# The following directive causes the Cisco VXC to access a different
# path on the FTP server.  This overrides and replaces the path in
# the local network setup and/or the one obtained from DHCP option
# 162.  Its characteristics are the same as the fileserver
# directive.  When this is actually used, the directory name wnos
# will be appended to the rootpath before use.  For instance,
# (assuming that the DHCP server does not supply values for options
# 161 and 162) immediately after the reboot following the processing
# of these two directives the Cisco VXC will start an FTP session
# with fileserv.cisco.com and attempt to retrieve
# /blazer/cisco/wnos/wnos.ini
#
RootPath=blazer/cisco
#
# The following directives specify the global connections that
# will be present on all user desktops or in all user Connect Lists
# following sign-on.
#
# The following directive will, when activated, establish a
# connection to a specific ICA server.  Note that the directive is
# continued onto multiple lines.  Continuation is accomplished by
# putting the following characters at the end of lines to be
# continued:
#
# \<Enter>
#
# This only works if there is no space between the \ and the
# <Enter> character; the line will not be continued otherwise.  The
# function of each of the arguments is:
#
#     connect=ica      Specifies that this is a connect statement
#                      and that the type of connection is ICA,
#                      (currently, ICA is the only supported
#                      connection type). This must be the first
#                      item specified on the line.
#     description="x"  Text to appear either under the icon on the
#                      Cisco VXC desktop or in the Connect List.
#                      The text must be surrounded by double
#                      quotation marks if it contains spaces or
#                      punctuation.
#     icon=default     The bitmap to be used for the Cisco VXC
#                      desktop display.  The argument is either
#                      default or a file name.  If a file name is
#                      specified, it must be located in the bitmap
#                      directory under the wnos directory on the
#                      FTP server.
#     host=IP          The IP address or DNS name of the ICA server
#                      to be contacted when this connection is
#                      established.
#     username=me      The username on the server that runs the
#                      published application.  The username
#                      determines the privileges and default
#                      directory used on the server.
#
# Since the following connection omits the password and domainname
# fields, the client will attempt to perform a login using no
# password and the default domain (whatever was last used on that
# system).  This will probably fail and present the user with
# a login dialog box.  This is more secure than putting passwords
# into a file on an FTP server, which can be downloaded by anyone.
#
connect=ica \
        description= "Global1" \
        icon=noname.ico \
```

```
        host=132.237.20.80 \
        username=test1 password="test password"

# Note: it is recommended to start each statement at the begining
#       of a new line, and all continuation options are indented with a Tab
#       character or multiple spaces for readability.
```

Sample Kiosk INI File

```
#
# This file provides an example of an environment where all users
# will use the same ICA connection to perform their work.  The
# connection will start as soon as the unit is turned on.  In this
# example the connection is to a published application (which could
# be a Windows desktop, but is not in this example).
#
# The following directive disables display of the sign-on dialog
# box.
#
signon=0
#
# The following directive allows the Cisco VXC to attempt to
# locate code files on the FTP server and to update the current
# code on the unit if the version on the server is different.
#
autoload=1
#
# The following directive describes the ICA connection to a
# published application (NotePad in this example).  The description
# field provides text that identifies the connection, either under
# the icon on the Cisco VXC desktop (if an icon is specified) or in
# the Connect List dialog box.  Note that the directive is continued
# onto multiple lines.  Continuation is accomplished by putting the
# following characters at the end of the line to be continued:
#
# \<Enter>
#
# This only works if there is no white space between the \ and the
# <Enter> character (the line will not be continued otherwise).
# There must also be white space between each argument on the
# reassembled line.  The continuation sequence does not constitute
# white space; instead, each argument has a trailing blank.  The
# leading <TAB> characters on the continuation line serve the same
# function and also contribute to the overall readability.  The
# function of each of the arguments is:
#
#     connect=ica      Specifies that this is a connect statement
#                      and that the type of connection is ICA
#                      (currently, ICA is the only supported
#                      connection type). This must be the first
#                      item specified on the line.
#     description="x"  Text to appear under the icon on the Cisco VXC
#                      desktop and in the Connect List dialog box.
#                      The text must be surrounded by double
#                      quotation marks if it contains white space
#                      or punctuation.
#     icon=default     The bitmap to be used for the Cisco VXC
#                      desktop display.  The argument is either
```

```
#                       "default" or a file name.  If a file name is
#                       specified, it must be located in the bitmap
#                       directory under the wnos directory on the
#                       FTP server.
#     username=me       The username on the server that runs the
#                       published application. The username
#                       determines the privileges and default
#                       directory used on the server.
#     password="x@y"    The password for the specified username.
#                       The password must be surrounded by double
#                       quotation marks if it contains punctuation
#                       or spaces.  This is the unencrypted password
#                       for the account.
#     domainname=mine   The Windows domain that defines the specified
#                       username.
#     browserip=a,b,c   The IP address(es) or DNS name(s) of machines
#                       that might be the ICA master browser.  When
#                       the master browser is contacted, it resolves
#                       the application name to a specific server
#                       that can provide the requested service.  In
#                       this case, a list of possible master browsers
#                       is provided.  The servers on the list are
#                       accessed in order until one is found that is
#                       operational.  That server is consulted for a
#                       resolution of the published application name.
#                       To establish a connection successfully, the
#                       first operational server contacted must be
#                       capable of resolving the application name.
#     application=notepad    The name of an application published
#                       using MetaFrame administrative tools.  This
#                       application will be run as soon as  a server
#                       has been selected and the login to the server
#                       is successful.
#     autoconnect=1     The connection will be attempted as soon as
#                       this file has been processed and any software
#                       updates have been completed.
#
# The username, password and domainname fields may be omitted if the
# ICA anonymous user provides sufficient access and privilege to
# accomplish the intended task.
#
connect=ica \
        description="Text capture" \
        icon=default \
        username=me password="x z" domainname=sqa \
        browserip=nil,132.237.176.7 \
        application=notepad \
        autoconnect=1

# Note: it is recommended to start each statement at the begining
#       of a new line, and all continuation options are indented with a Tab
#       character or multiple spaces for readability.
```