Dell Wyse ThinOS

Version 8.5.1 INI Reference Guide

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2018 - 09

Rev. A01

Contents

Summary of revisions

The following changes and enhancements have been made to this document since Dell Wyse ThinOS release 8.5.1.

Table 1. Newly added INI parameters

Reference	Description
• Device=Wireless [RoamScanChannelTime={1-15}] [RoamScanChannelProbes={1-4}] • OneSignServer=onesign_server [ConnectTimeout={0 ~ 65535}] • PnliteServer=<List of {IP address, DNS names, or URLs} > [CAGUserAsUPN=[yes, no]] [CAGExternal=[yes, no]] [DisableSFInit=[yes, no}] • WDAService=yes [enableReminder={yes, no}]	New parameters added in Connection settings for wnos.ini files, {username} INI and $MAC INI files.
• ConnectionBroker={default, VMware, Microsoft, Quest, AWS} [Host={broker_url}] [AutoConnectList={*|host1;host2;host3...}]	New parameters added in Connection settings for wnos.ini files only.

1

Introduction

Thin clients running Dell Wyse ThinOS firmware are designed solely for optimal thin client security and performance. These extremely efficient purpose-built thin clients are virus and malware-resistant and offer ultra-fast access to applications, files, and network resources within Citrix, Microsoft, VMware and Dell vWorkspace environments, and other leading infrastructures. ThinOS-based thin clients are self-managed, go from power-on to fully productive in seconds, and with no published API, locally accessible file system or browser, require no local antivirus software or firewall to protect against viruses or malware.

About this Guide

This guide is intended for administrators of Dell Wyse thin clients running ThinOS. It provides the detailed information you need to help you understand and use the ThinOS 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 your INI files with working examples.

Finding the Information You Need in this Guide

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

Supported platforms

Supported products

This table lists the supported Dell Wyse ThinOS products.

Table 2. Supported platforms

Platform	Processor
Wyse 5070 thin client	Celeron
Wyse 5070 thin client	Pentium
Wyse 5070 Extended thin client	Pentium

2

Getting Started: Learning INI File Basics

In this chapter you will learn how to construct and use the supported INI files.

It includes:

- Downloading and Using Sample INI Files
- Supported INI Files You can Construct
- Rules and Recommendations for Constructing the INI Files
- Placing the INI Files into the Folder Structure on the Server

After you become familiar with the INI file basics, you can refer to the parameter details you need in the other chapters and appendixes of this guide.

Downloading and using sample INI files

ThinOS Sample INI files can be downloaded and modified to suit the individual connection profile requirements. These sample files are annotated to allow you to use them as a starter set that you can modify to work on ThinOS.
To download and use the files:

1 Go to Dell support site.
2 Click **Product Support**, enter the Service Tag of your thin client, and then click **Submit**.

NOTE: If you do not have Service Tag, use the auto detect feature or manually browse for your thin client model.

3 Click **Drivers and Downloads**.
4 From the **Operating system** drop-down menu, select **ThinOS**.
5 Scroll down the page and download the sample INI file to the file server.
6 Open the text file by using an ASCII text editor, and modify the INI parameters as needed for your use.

Supported INI files you can construct

The INI files contain the parameters and its associated options and values necessary for the various functionality you want.

NOTE: For examples of parameters commonly used for basic deployments, see Examples: Basic Deployments.

You can construct the following INI files:

- wnos.ini file, see Working with wnos.ini Files.
- {username}.ini file, see Working with {username}.ini Files.
- $MAC.ini file, see Working with $MAC.ini Files.

IMPORTANT: The INI file processing hierarchy is as follows:

- **Scenario 1** — WNOS.ini exists. The WNOS.ini file is processed and if the Include=$MAC.ini (or Include={username}.ini) statement is included, then the relative MAC.ini (or {username}.ini) file is processed.
- **Scenario 2** — WNOS.ini exists and {username}.ini exists. The WNOS.ini file is processed and if the Include=$MAC.ini statement is included, then the MAC.ini file is processed. Once the credentials are provided, the {username}.ini file is processed.
- **Scenario 3** — WNOS.ini exists and MAC.ini exists. The WNOS.ini file is processed and if the Include={username}.ini statement is included, then the {username}.ini file is processed. Once the credentials are provided, the MAC.ini file is processed.

- **Scenario 4** — No ini files exist. Local configuration is applied.

Working with wnos.ini files

A wnos.ini file contains the global parameters you want that will affect all thin clients accessing the server. Parameters in both Connection Settings: wnos.ini files only, and Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files can be used in a wnos.ini file.

NOTE: Parameters in Connection Settings: wnos.ini files only can only be used in a wnos.ini file; they cannot be used in a {username}.ini file.

Working with $MAC.ini Files

A $MAC.ini file can be used for device-specific configurations. If the thin client locates a wnos.ini file, then the wnos.ini file is processed and if the Include=$MAC.ini statement is included, then the $MAC.ini file is processed. The $MAC.ini file is stored in the same directory as a wnos.ini file if you are not using a WNOS.INI file, otherwise the files should be stored in the INC directory.

NOTE: The placement of the include=$MAC.ini parameter within the wnos.ini file will dictate which value will take priority for a same specific parameter that is contained in both the wnos.ini file and the $MAC.ini file but is defined differently, that is different values for the same parameter.

For example, if the wnos.ini file has parameterA=valueRED, and the $MAC.ini file has the same parameterA=valueBLUE, then:

- If the include=$MAC.ini parameter is included in the wnos.ini file before the parameterA=valueBLUE statement, then the $MAC.ini parameterA=valueRED is discarded and parameterA=valueBLUE from the wnos.ini file is the final value used.
- If the include=$MAC.ini parameter is included in the wnos.ini file after the parameterA=valueBLUE statement, then the $MAC.ini parameterA=valueBLUE is discarded and parameterA=valueRED from the wnos.ini file is the final value used.

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 General Settings for wnos.ini Files, {username} INI, and $MAC INI Files.

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 descriptions in Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files can be used in a {username}.ini file.

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

Rules and recommendations for constructing the INI files

In general, ThinOS INI files follow currently accepted **standard** INI file formatting conventions. The INI files consist of Wyse parameters. If you are using an INI file, the only parameter you must use is the Connect parameter, see Connect in General Settings for wnos.ini Files, {username} INI, and $MAC INI Files. Any of the rest of the parameters can be used if you desire, but are not necessary unless you want changes from client and **other** defaults, for example, **other** can be the default resolution of your monitor.

Every parameter (and their options) 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 INI files have the same meaning that is, a parameter named WyseXYZ in a wnos.ini file and named WyseXYZ 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 the INI files:

1 **Global Connect Parameters First**

Global connect parameters should be listed before other connect parameters in a wnos.ini file.

2 **Connect is the Only Required Parameter**

As stated earlier, if you are using an INI file, the only parameter you must use is the Connect parameter. Any of the rest of the parameters can be used if you desire, but are not necessary unless you want changes from client and **other** defaults.

3 **Continue Lines by using a Space and Backslash**

Placing a space and 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; the requirement of white space between parameter entries is maintained by the use of the space before the backslash. In addition, starting all parameters at the left margin and placing at least one leading space or tab at the beginning of all (and only) continuation lines makes an INI file easier to read.

> **NOTE:**
> When you require string concatenation, you can use a backslash without a space before or after it to concatenate with the first set of characters from the previous line; for example the strings snow and ball may be concatenated to give snowball.

4 **Blank Lines Make Files Easy to Read**

Using blank lines is recommended for making code easier to read.

5 **Comment by using a # Sign**

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.

6 **Values with White Spaces Require Quotation Marks**

Values of parameters containing white spaces must be placed inside quotation marks. We recommend you use common-practice nesting rules.

7 **Separate Lists by using Semicolons or Commas**

Use semicolons or commas for list separators.

8 **{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.

9 **Use the wnos.ini File to Set the Maximum Number of Connection Entries Allowed**

The combined number of connection entries defined in a {username}.ini file and a wnos.ini 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.

10 **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 or {username}> parameter in the wnos.ini file. Although not required, We recommend that these parameters end with the parameter Exit=all.

> **NOTE:**
> No parameter should ever be executed twice. Some ThinOS 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.

IMPORTANT:

We recommend you place the include=<$mac.ini or {username}> statement on the last line of the wnos.ini file to verify that all parameters are processed properly for terminal-specific settings.

11 **Use of System Variables with Some Options of the Connect Parameter**

Some options of the Connect parameter can use the system variables shown in System Variables to map the string. All combinations of the variables are supported. For options that support use of system variables, see Connect Parameters Options.

System variables

The following table contains the system variables you can use with some options of the connect parameter:

Table 3. System variables

Option	Value
$SN	Serial number used.
$MAC	MAC address used.
$IP	IP Address used.
$IPOCT4	The fourth octet of IP Address, for example, if IP is 10.151.120.15, then the fourth octet is 15.
$TN	Terminal name.
$PF	Platform name—The first part of image name xxx_wnos, for example, R10L.
$UN	Sign-on name used.
$PW	Sign-on password used.
$DN	Sign-on domain name used.
$FIP	IP address used in fixed format with 3 digits between separators, for example, 010.020.030.040.ini. Using it in conjunction with the left/right modifier helps to define policy for subnet. For example, include=&Left($FIP,11).ini is specified to include file 010.020.030.ini for subnet 010.020.030.xxx.
$WPUN	PEAP/MSCHAPv2 username used (802.1x dependent).
$WPPW	PEAP/MSCHAPv2 password used (802.1x dependent).
$WPDN	PEAP/MSCHAPv2 domain used (802.1x dependent).
$DHCP (extra_dhcp_option)	Extra DHCP options for Windows CE unit, including 169, 140, 141, 166, 167. For example, set a string test169 for option tag 169 in DHCP server, and set TerminalName=$DHCP(169) in wnos.ini. Check terminal name in GUI, and the terminal name will be test169. 166 and 167 is default for CCM MQTT Server and CCM CA Validation in ThinOS. So you need to remap the options from GUI or INI if you want to use $DHCP(166) and/or $DHCP(167).
$SUBNET	Specifies Subnet notation. The format is {network_address}_{network_mask_bits}. For example, if the IP address is 10.151.120.15, and the network mask is 255.255.255.0, then 10.151.120.0_24 is used.

Option	Value
&Right($xx, i) or &Left($xx, i)	Specifies whether the variable is to be read from left or right. The $xx is any of the above parameters. The parameter i specifies left or right offset digits. The combinations of all the above variables, such as CTX&Right($IP,4)@&Left($UN,3) are supported. A replacement $SYS_VAR is used if the statements or parameters support.

Placing the INI files into the folder structure on the server

If you have set up your environment to provide your thin clients running ThinOS with automatic updates and configurations as described in *ThinOS Administrator's Guide*, you can use the following folder structure on your server under the **C:/inetpub/ftproot folder**, for FTP or **C:/inetpub/wwwroot folder**, for HTTP or HTTPS and place your INI files and other necessary files inside the structure as noted. This list describes the folder structure, starting with the root directory.

Table 4. Folder structure

Folder structure	Description
/wyse/	Required—The root directory. It stores the wnos folder.
/wyse/wnos	Required—The main INI configuration folder. It stores the wnos.ini file, {username}.ini file, $MAC.ini file, firmware, and the following optional folders: • bitmap folder • cacerts folder • font folder • inc folder • ini folder • locale folder • trouble_shoot folder
/wyse/wnos/bitmap	Optional—The folder where you can place custom images you plan to use.
/wyse/wnos/cacerts	Optional—The folder where you can place the CA certificates that can be imported to a thin client. **NOTE: Use the AddCertificate INI parameter in the wnos.ini file to import the certificates to thin clients.**
/wyse/wnos/font	Optional—The folder where you can place font files for languages such as Chinese Simplified, Chinese Traditional, Japanese, and Korean that requires the file.
/wyse/wnos/inc	Optional—The folder where you can place the mac.ini files. **NOTE: The use of parameter Include=$mac.ini will load / wnos/inc/mac-address.ini so that you can use inc in the folder structure and use $MAC.ini.**
/wyse/wnos/ini	Optional—The folder where you can place the {username}.ini files and {group} folder.
/wyse/wnos/trouble_shoot	Optional—The folder where you can place the trace files that you can capture and play back.

Folder structure	Description
	IMPORTANT: Be sure to enable the parameter, EnableTrace=yes.

3

Parameters for wnos INI files only

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

NOTE:

For information to help you construct and use the supported INI files, see Getting Started Learning INI File Basics.

Parameters in Connection Settings for wnos.ini Files Only can only be used in a wnos.ini file; they cannot be used in a {username}.ini file.

To increase usability such as relation to thin client dialog box equivalents, the supported parameters are separated into the following categories:

- General Settings for wnos.ini Files Only
- Peripheral Settings for wnos.ini Files Only
- Connection Settings for wnos.ini Files Only

IMPORTANT:

The underlined value for a parameter is the default value. Some parameters also have options shown within brackets [ ]. If an option has an underlined default value, that option and default value will automatically be used with the parameter; options without underlined values can also be used if you want to, but are not automatically used with the parameter.

In addition, when using parameters and options, you can leave the default value or change it to another value shown. For example, in the following case where:

ParameterX={**yes**, no}

[Option1={**0**, 1}]

[Option2={1, 2, 3, 4}]

If you use ParameterX, then Option1 and its default value 0 will automatically be used as Option1 has an underlined default value of 0. You can still use Option2 if you want to, however, Option2 is not automatically used with the parameter as Option2 does not have an underlined default value.

General Settings for wnos.INI Files Only

The following table contains the parameters used for configuring general settings. The underlined values are default values.

Table 5. General Settings: wnos.ini files only

Parameter	Description
AutoLoad={0, 1, 2, 101, 102, 201, 202} [LoadPkg={0, 1, 2}] [AddPkg={pkg1_name, pkg2_name, ...}] [DelPkg={pkg1_name, pkg2_name, ...}]	**AutoLoad**— Default is **1**. Specifies the firmware update mode. The following are the values and associated actions: 0 — Disables checking for image. 1— Enables forced firmware upgrade/downgrade process. This is the default value.

Parameter	Description
[VerifySignature={yes, no}]	2 — Enables comparison/non-forced upgrade process only. 101 — Enables firmware upgrade/downgrade process, but displays a window with **OK** or **Cancel** button before the process with a note of the version to downgrade or upgrade; displays a status complete window. 102 — Enables firmware upgrade, but displays a window with **OK** or **Cancel** button before the process with a note of the version to upgrade; displays a status complete window. 201 — Enables firmware upgrade or downgrade process, but displays a window with **OK** button before the process; displays a status complete window. 202 — Enables firmware upgrade only, but displays a window with **OK** button before the process; displays a status complete window. The option LoadPkg specifies how to update the external packages. If set to 0, this disables checking for packages. If set to 1 it enable packages upgrade/downgrade process, and if set to 2, it enables upgrade only. If LoadPkg is not in the statement, it will inherit the value of AutoLoad. For example, if the value is 0, and if AutoLoad=0, 1, and if AutoLoad=1, 101 or 201, and 2 if AutoLoad=2, 102 or 202. For example, if you set AutoLoad=1 LoadPkg=0, the firmware is checked, but the packages are not checked. From ThinOS 8.3, the external packages update mechanism is changed. Some packages are default, and loaded according to value of LoadPkg. For example RTME. Some packages need additional parameter AddPkg to add. For example, FR and TCX.The option AddPkg is for adding packages. It depends on the value of LoadPkg. The packages check comes after firmware check. The option DelPkg is for deleting packages. It does not depend on the value of LoadPkg. The packages specified in DelPkg are always deleted when loading the ini file. The value of AddPkg and DelPkg is one package name or a package name list. For example, AutoLoad=1 AddPkg="FR, TCX" DelPkg=RTME **NOTE: The AddPkg and DelPkg options depend on platforms that supports external packages. Only Wyse 3030 LT thin client with ThinOS, Wyse 3030 LT thin client with PCoIP, Wyse 3040 thin client with ThinOS, Wyse 3040 thin client with PCoIP, Wyse 5010 thin client with ThinOS, Wyse 5010 thin client with PCoIP, Wyse 5040 thin client with ThinOS, Wyse 5040 thin client with PCoIP, Wyse 5060 thin client with ThinOS, Wyse 5060 thin client with PCoIP, and Wyse 7010 thin client with ThinOS support it. The other legacy platforms does not support it.** **VerifySignature**—The option VerifySignature specifies whether or not the verification is required when updating the firmware and/or packages. It is introduced in ThinOS 8.4 release and later to enhance the security and integrity of the firmware and packages. If set to no, it will not check the signature so that the downgrade of

Parameter	Description
	the firmware and/or packages can happen, which do not support signature. The default is yes.
AutoPower={yes, no} or Device=cmos AutoPower=(yes, no)	Default is **no**. 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 and if the thin client was shut down properly before power was lost unexpectedly, when the power is restored, the thin client will be powered. This setting is useful in a kiosk environment. Once an AutoPower statement is processed, it alters the behavior of the thin client until a countermanding statement is processed. The effect of an AutoPower=yes statement continues even if the statement is removed from the INI file in which it was found. Use of the AutoPower option does not interfere with performing a user directed shutdown.
CCMEnable={yes, no} [CCMServer=server_address[:port] [GroupPrefix=<prefix>] [GroupKey=<hashkey>] [MQTTServer=<mqtt_address>[:<mqtt_port>]] [AdvancedConfig={no, yes}] [CCMDefault={no, yes}] [Override={no, yes}] [CAValidation=(yes, no)] [Discover=(yes, no)] [IgnoreMqtt=(yes, no)]	From ThinOS 8.4.1 release, these INI parameters are applicable to Wyse 3040 thin client. **CCMEnable** — Yes/no option to enable the Cloud Client Manager Agent. Default is **no** **CCMServer** — Specifies a IP address or URL address for the CCM server. Default protocol is HTTPS if "http://" or "https://" is not available. Default port is 443. Once specified, it is saved in the non-volatile memory. Example: CCMEnable=yes CCMServer=http://xxx:8080 **GroupPrefix and GroupKey** — The options GroupPrefix and GroupKey compose the Group Registration Key of the Cloud Client Manager server. Once specified, it is saved in the non-volatile memory. **NOTE:** The numbers before the dash on the Group Registration key is the GroupPrefix value and the characters to the right of the Group Registration Key is the GroupKey value. **NOTE: The length of GroupPrefix is fixed to four; the length range of GroupKey is from eight to 31 characters.** **MQTTServer** — Specifies a IP address or URL address for the MQTT server and MQTT port after the : (colon). Once specified, it is saved in the non-volatile memory. **AdvancedConfig** — Default is **no**. Yes/no option to enable the Cloud Client Manager server and MQTT server fields in the GUI. If AdvancedConfig=yes is specified, the Cloud Client Manager server and MQTT server fields in the Cloud Client Manager UI will be enabled. See also PRIVILEGE parameters in General Settings for wnos.ini Files, {username} INI, and $MAC INI Files. **CCMDefault** — Default is **no**. Yes/no option to enable the Configure Cloud management dialog will display during boot up. If CCMDefault=yes is specified and both the CCMServer and GroupKey are NULL, the Configure Cloud management dialog will display during boot up. Input group code to connect to the default Cloud Client Manager server and default MQTT server. The default

Parameter	Description
	CCM server is https://us1.cloudclientmanager.com/ccm-web/ and default MQTT server is us1-pns.cloudclientmanager.com. **Override** — Default is **no**. Yes/no option to allow a groupkey from the INI file to override the previous groupkey. If Override=yes is specified, the groupkey from the INI file will override the previous groupkey. The Groupkey can technically be applied in many places. You can configure the group key in order of priority, that is, if #1 is defined it will override #2. Groupkey priority policy is listed below: 1 Local GUI configuration or groupkey received from CCM in a Group Change command 2 Defined in INI file "ccmenable=yes groupkey=xxxx" 3 DHCP Option Tag #199 **NOTE:** The Groupkey assigned in DCHP option #199 and INI parameter are only used for first time deployment, that is, they only take effect if CCM is currently disabled or if CCM is enabled but group-key is NULL. If DCHP is defined and CCM is enabled or not NULL: The CCM Group key in the DHCP is ignored since it is configured manually in local UI or from CCM group change. If INI is defined and CCM is enabled or not NULL: The CCM Group key in the INI is ignored since it is configured manually in local UI or from CCM group change. **IMPORTANT:** There is an exception in the logic above when the 'override=yes' option is used in INI file. This will make #2 take priority over #1. For example, `CCMEnable=yes CCMServer=xxx:8080 GroupPrefix=wlab GroupKey=TC-TEST-ENG MQTTServer=xxx:1883 AdvancedConfig=yes Override=yes` **NOTE:** For detailed instructions on how to configure CCM in a wnos.ini file to enable the CCM Agent on supported ThinOS clients, refer to Knowledge Base Solution #**23875**, go to the Knowledge Base at www.dell.com/support and search for **23875**. **CAValidation**—If the option is set to yes, then the CCM agent will check the certificate when connected to https server. Default value is yes. **Discover**— If the option is set to yes, then the CCM agent will discover the CCM server, MQTT server and CA validation from DNS Record. Default value is yes. **IgnoreMqtt**—If IgnoreMqtt=yes is specified, CCM agent will not connect to MQTT server. Default value is no.
DefaultUser={username, $SYS_VAR} [Display={yes, no}]	Specifies the default sign-on user. See System Variables for a list of system variables for $SYS_VAR.

Parameter	Description
[disable={yes/no}]	**Display**—If the value is set to yes, the username field in sign-on window will be displayed. By default the value is set to no and the field will be obscured with asterisks (*). **disable**— If the value is set to yes, the user name field in sign-on window is disabled.
Password=<sign-on password> [disable={yes/no}] [encrypt={no, yes}]	**Password**— Specifies the password as the sign-on password. There is no minimum length. The maximum length is 64 characters. In wnos.ini this sets as the default password. The system will sign on automatically and not wait for username, password, and domain entries. **Disable**—If the value is set to yes, the password field in sign-on window is disabled. Default is no. **encrypt** - The default value is no. The options are used to enable or disable an encrypted string for a password in the INI file instead of clear text. If the value is set to yes, the password in the INI is an encrypt string instead of clear text.
DisableButton={no, yes} [DisableRestart={yes, no}]	Default is **no**. Yes/no option to disable the power button. If you set the option DisableRestart=yes, the radio button Restart the system in shutdown window is disabled. These settings are saved permanently and the default value is no.
EnableCacheIni	**IMPORTANT: Supported on Wyse 3010 thin client with ThinOS (T10) and Wyse 3020 thin client with ThinOS (T10D) only.** EnableCacheIni is no longer supported and cannot be used on platforms other than the Wyse 3010 thin client with ThinOS (T10). On platforms other than the Wyse 3010 thin client with ThinOS (T10), EnableCacheIni is replaced by the MirrorFileServer parameter, see MirrorFileServer parameter in General Settings for wnos.ini Files Only. Use EnableCacheIni on Wyse 3010 thin client with ThinOS platform (T10) only. This is because there is no local flash on Wyse 3010 thin client with ThinOS (T10) platform, and the MirrorFileServer parameter is not supported on it.
EnableGKey={yes, no}	Default is **yes**. Yes/no option to enable G key reset. G key reset is supported for Privilege=High in the NVRAM.
Exit={**yes**, no, all}	Default is **yes**. Specifies the INI file processing. **yes** — Processing returns to the prior INI file on the next line after $include. **no** — There is no operation. **all** — All INI file processing is exited.
Include=<$mac.ini file or {username}.ini file>	<$MAC.ini> Loads /wnos/inc/mac-address.ini.

Parameter	Description
	NOTE: The file name does not include the symbol **:** in the mac address. See also the Exit parameter for information on how to terminate Include. <{username}.ini> Loads /wnos/inc/{username}-address.ini. The file name does not include the symbol **:** in the {username} address. See also the Exit parameter for information on how to terminate Include.
MirrorFileServer={no, yes}	Default is **no**. Yes/no option to enable the cache all server files functionality. This enables the cache all server files such as INI files, wallpaper, bitmap, font, local messages and so on to the local flash when files are changed in the file server. ThinOS would use the cached files when files on the file server are unavailable. **IMPORTANT: S10 is not supported**
RootPath=<file server root path>	This file server 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 file server root path entry before use.
TerminalName=<name> [reboot={no, yes}]	**TerminalName** — Name of the client comprising a 15-character string. It can also be configured with system variables. Basically all the variables can be used except $TN (recursive), $UN, $PW, $DN. However, these are not yet available when parsing wnos.ini. Additionally combinations like xymac, sztnxyz etc are supported. **reboot** — Default is **no**. Yes/no option to reboot the thin client if the terminal name is changed.
TimeZone=<zone value> [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 zone values s are listed in the System Preference dialog box on the thin client and in TimeZone Parameter: Values. **NOTE:** The TimeZone parameter is dependent on the TimeServer=parameter. If a time server is not defined, the client CMOS/BIOS internal clock will be used as a reference. **ManualOverride** — Default is **no**. 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** — Default is **no**. Yes/no option to enable daylight saving time; MMWWDD is a 6 digit number to specify the start and the end of daylight saving time.

Parameter	Description
	IMPORTANT: The Start and End options are in the MMWWDD format, where: **MM** = Month of the year. Values are 01 to 12 for the months of the year from January to December. For example, 01 = January, 12 = December **WW** = Week of the Month. Values are 01 to 05 for the week of the month, 05 is the last week. For example, 01 = 1st week, 05 = the last week of the month. **DD** = Day of the week. Values are 01 to 07 for the day in the week from Monday to Sunday. For example, 01 = Monday, 07 = Sunday. **NOTE:** For the 2013 year, DST dates are Sunday, March 10, 2:00am and ends Sunday, November 3, 2:00am. **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: 1 Run **gpedit.msc** to open the **Group Policy** dialog box. 2 Click **Computer Configuration** in the Local Computer Policy tree, and expand the **Administrative Templates** folder. 3 Expand the **Windows Components** folder, and then expand the **Terminal Services** folder. 4 Click **Client/Server data redirection** to open the Setting list. 5 Right-click **Allow Time Zone Redirection** and select **Properties** to open the **Allow Time Zone Redirection Properties** dialog box. 6 Select the **Enabled** option, and then click **OK**. 7 Close the **Group Policy** dialog box. Overall example: `TimeZone="GMT - 08:00" ManualOverride=yes Daylight=Yes Start=030107 End=110107 TimeZoneName="Pacific Standard Time" DayLightName="Pacific Daylight Time"`

Peripheral settings for wnos.ini files only

The following table contains the parameters used for configuring peripheral settings such as keyboard, monitor, mouse, and printer. The defaults values are underlined.

Table 6. Peripheral Settings: wnos.ini files only

Parameter	Description
DEVICE_SECURITY=white_list/black_list vid_pid=[vvvv,pppp] class=name/[cc,ss,pp]	1 When DEVICE_SECURITY=white_list is set, the security is in high level, and you need to add all the devices (on board devices including Wyse 3020 thin client with ThinOS (T10D)'s netcard, and internal hub) to the list that you want to use, and all other devices are denied when the device is plugged-in. 2 When DEVICE_SECURITY=black_list is set, the security is mid-level, and customer can add the device which is not present in the list. 3 About key value: all the value are hex, and vid_pid = 0xvvvvpppp, class value is =0xccsspp; where, • vvvv=device vendor id • pppp=device product id • cc= device interface class • ss=device interface subclass • pp=device interface protocol 4 Class name is abbreviation for the defined class. Valid names are listed here:{Audio, CDC_control, HID, Pysical, Image, MASS_STORAGE, Hub, CDC_Data, Smart_Card, Content_Security, Video, Personal_Healthcare, AudioVideo, Billboard, Diagnostic_Device, Wireless, Miscellaneous, Application, VendorSpecific}. For detailed information, refer: www.usb.org/developers/defined_class. 5 The max number of devices/class table is 16. For Example: DEVICE_SECURITY=white_list class=HID class=Audio class=Video DEVICE_SECURITY=black_list vid_pid=0x0B0E2000 class=0x030101.
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.
ThinPrintEnable={no, yes} [Port=port number]	Default is **yes**. **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**.

Connection settings for wnos.ini files only

The following table contains the parameters used for configuring the connection settings. The default values are underlined.

Table 7. Connection Settings: wnos.ini files only

Parameter	Description
AddCertificate=filename	**AddCertificate** — Specifies a certificate file residing in the subfolder cacerts under the wnos folder to load on platforms with

Parameter	Description
password={plain text password} Password-enc={encrypted password}	nand flash, or on the memory. The length of the filename, including the trailing period and the file extension, is limited to 64 characters. AddCertificate must be used 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 specially used with PFX files.
CaradigmServer=vip list [EGPGroup=group name] [EnableLogOff={yes,no}] [SecurityMode={default, full, warning, low}] [DisableManualLogon=yes, no]	CaradigmServer=vip list contains a list of VIP addresses with optional TCP port number of Caradigm servers. EGPGroup defines the user group name. If EnableLogOff=yes is specified, the user is logged off from the session before system signs off. Otherwise the session is disconnected. The logged off user has a timeout value which can be set using SessionConfig parameter SessionLogOffTimeout. The default timeout value is 1, if no SessionLogOffTimeout is specified. SecurityMode specifies the SSL certification validation policy. If set to default, it applies the SecurityPolicy setting. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, drop the connection. If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, the default value of the setting is default. DisableManualLogon is set to yes to disable user to manually enter credentials to authenticate into the device. It only allows an already enrolled proximity badge and in active grace period to authenticate with a single badge tap. The default value is no
Community=community [Encrypt={yes, no}]	Specifies the SNMP community name. A string up to 31 characters are allowed. After the value is specified, it is saved in the non-volatile memory. If encrypt=yes, an encrypted string is used as a community name. The default value is set to no. **NOTE: Use our Windows Password_Gen tool or built-in tool to generate the encrypted string.**
ConnectionBroker={default, VMware, Microsoft, Quest, AWS} [IgnoreProfile={yes, no,}] [SecurityMode={Default,Low,Warning,Full}] [EnableVWGateway]={yes, no}	Default value is **default**. Specifies the type of VDI broker to use. Default is a 3rd party VDI broker. AWS is Amazon Workspace broker. It is only available with PCoIP build. **IgnoreProfile** — Default value is **no**.

Parameter	Description
[VWGateway]=url [ConnectionType]={Default, All, RDP, PCoIP, Blast} [EnableVDMCredSSP]={yes, no} [RDCollections={*collect1, collect2,...}] [DisableShowDisclaimer=[yes, no] [DisableShowServer=[yes,no] [EnableUnauthenticatedAccess]={yes,no} [Host={broker_url}] [AutoConnectList={*|host1;host2;host3...}]	Set IgnoreProfile=yes to disable parsing the global setting from the VDI broker. It is only valid in the case of ConnectionBroker=default. **SecurityMode** — SecurityMode specifies the security mode for the VMware broker and Amazon Workspace (AWS) broker. It is only valid in case of ConnectionBroker=VMware or ConnectionBroker=AWS. The details is as follows: • Set SecurityMode=Full to have the Client verify the server's certificate in highest security mode; if any relevant checks error, it will fail to connect to the server. • Set SecurityMode=Warning to have the Client allow connection continuation in the following two specific exceptions where full verification would fail: a Certificate is self-signed. b Certificate has an invalid time. • Set SecurityMode=Low to indicate that Client allows connection without any certificate verification. • Set SecurityMode=Default to indicate that Client follows the SecurityPolicy setting to verify the certificate. **NOTE:** For Dell vWorkspace broker, ConnectionBroker=Quest is recommended. EnableVWGateway and VWGateway are used to set the vWorkspace gateway. For VMware broker, ConnectionBroker=VMware is recommended. ConnectionBroker=VDM is still supported but deprecated. The option ConnectionType specifies the display protocol that you want to use when launching a session in VMware broker. If this parameter is set, then the desktops that meet the specified protocol are listed after broker sign on. This setting is only valid in case of PCoIP feature is supported. • Set ConnectionType=Default, only the desktops with the default protocol configured in broker server are listed (this is the default value for this setting). • If you set ConnectionType=All, both PCoIP and RDP desktops are listed. • If you set ConnectionType=RDP, only RDP desktops are listed. • If you set ConnectionType=PCoIP, only PCoIP desktops are listed. • If you set ConnectionType=Blast, only Blast desktops are listed. **EnableVDMCredSSP=yes**—The option is set to yes to enable RDP NLA mode connection when the VMware View broker session is launched. The default value is no. EnableVDMCredSSP=yes works only after you disable view security tunnel in server side. **RDCollections**—The option specifies the collections for Microsoft RD broker. Only the applications and desktops within the specified collections are displayed. The value can be a list separated by ',' or ';' and can use wildcard "*" to match the string. If the parameter is not set, all the applications and desktops are displayed. To get your RemoteApp or desktops collection name, do the following: 1 In RDS Server local, go to **C:\Users\administrator.RDSS \AppData\Roaming\Microsoft\Workspaces\{xxxx}\Resource**,

Parameter	Description
	and check that all your published collection (.rdp file) are listed. 2 Open the specify .rdp file which you want to define in .ini file with notepad and get the collection name from line `"loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.[collection name]"`. **DisableShowDisclaimer=yes**—The option is set to yes to disable popup/pre-logon message and automatically accept them without intervention when broker type is VMware View. The default value is no. **DisableShowServer=yes**—The option is set to yes to disable showing the view server URL in sign-on window and disclaimer window when broker type is VMware View. The default value is no. **EnableUnauthenticateAccess=yes**—The option **Yes** is set to enable the VMware View broker log. The default value is **No**. The option **Host** specifies the connection broker server IP address or FQDN. The option **AutoConnectList** can specify the VDI desktops or applications which are automatically launched when using VDI to sign on. If it is *****, all the VDI desktops or applications are automatically connected. The auto connect list is the connection description which can use wildcard to match the string.
DelCertificate={filename, all, builtin}	**filename** — Removes the named file from the nand flash or from the memory. **all** — Removes all certificates except built-in certificates included by default. **builtin** — Removes all certificates including the public certificates included by default.
DesktopColorDepth={16, 32} [RGB565={no, yes}]	**DesktopColorDepth** — Sets the desktop color to 16 or 32 bits. If DesktopColorDepth=16, the default color is 15 bits. **RGB565** — Default is**no**. Applies only if the desktop color is using 16 bits. **IMPORTANT:** If the RBG565 parameter value is changed to yes, the thin client will require a reboot.
DHCPExpire={reboot, shutdown}	Default is **reboot**. 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}]	Default is **no**. **DHCPOptionsRemap** — Specifies whether or not the following options can be set.

Parameter	Description
[RootPath={128 to 254}] [FtpUserName={128 to 254}] [FtpPassWord={128 to 254}] [RapportServer={128-254}] [RapportPort={128-254}] [WDMServer={128 to 254}] [WDMPort={128 to 254}] [PnliteServer={128 to 254}] [DomainList={128 to 254}] [VDIBroker-{248 to 254}] [RapportSecurePort={128-254}] [Discover={yes, no}] [WDMSecurePort={128 to 254}] [WDMFQDN={128-254}] [CCMGroupKey={128-254}] [CCMServer={128-254}] [CCMMQTTServer={128-254}] [CCMCAValidation={128-254}]	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. The option DisableOption12 sets if the option tag 12 in DHCP is accepted or not. As default, DHCP option 12 sets the hostname and domain name of the terminal. For example, the information of option 12 is terminal name.wyse.com, the terminal name will be set as terminalname and the domain name will be set as wyse.com. If you set different value for DisableOption12 from the value in NVRAM, the system will automatically reboot to make the value valid. (CIR36891) **RapportSecurePort**— Specifies the HTTPS port of WDM server. It is in 6.3 to support WDM4.7. **Discover**—If Discover=yes, the device fetches Wyse DHCP options from DHCP server, otherwise, it prevents the device from fetching those information. Default value is yes. If the device receives FileServer/WDMServer information through the DHCP server, then the associate User interface is protected. **NOTE:** WDMSecurePort is the specified HTTPS port of the WDM server. **WDMServer**—Value 186 specifies the IP address of WDM server. Value 192 specifies the HTTP port of WDM server. **WDMSecurePort**—Specifies the HTTPS port of WDM server. **WDMFQDN** — Specifies the Fully Qualified Domain Name (FQDN) of the WDM server. **NOTE: The CCMGroupKey, CCMServer, CCMMQTTServer and CCMCAValidation options are specified to remap the tags for CCM configuration.**
DHCPUserClassID=class_id [ParseVendorInfo={no, yes}]	**DHCPUserClassID** — Specifies the UserClassID used for DHCP. **ParseVendorInfo** — Default is **yes**. Yes/no option to specify whether or not ThinOS will interpret DHCP option 43. This is a vendor-specific information. 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 are allowed in a string.
DHCPVendorID=vendor [ParseVendorInfo={no, yes}]	**DHCPVendorID** — Specifies the VendorID used for DHCP. **ParseVendorInfo** — Default is **yes**. Yes/no option to specify whether or not ThinOS will interpret DHCP option 43. This is a vendor-specific information. 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 are allowed in a string.
DisableDomain={no, yes}	Default is **no**.

Parameter	Description
	Yes/no option to disable the drop-down domain list in the PNAgent/PNLite Sign-on dialog box.
DNSIPVersion={ipv4, ipv6} [DNSServer=server_list] [DNSDomain=dns_domain_url] [Combined={yes,no}]	Specifies the DNS server and domain. Default IP version is ipv4. The DNS Server is an IP list separated by **;** or **,**. The maximum size of this list is 16. For example: 10.200.5.53;192.168.100.1;192.168.200.8 **IMPORTANT: There is no space after the ;.** If Combined=yes, then the DNS server will combine the DNS server configured by DHCP and the static one. DNS domain will use the value configured by DHCP if static DNS domain is empty.
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 [disable={yes/no}]	A list of domain names that will appear in the thin client Sign-on dialog box as options to help users in selecting the domain to sign-on to PNAgent/PNLite servers. Once 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. **disable**— If the value is set to yes, the domain field in sign-on window is disabled.
Dualhead={no, yes} [ManualOverride={no, yes}] [Mainscreen={1, 2}] [Orientation={hort, vert}] [Align={Top|Left, Center, Bottom|Right}] [Taskbar={wholescreen, mainscreen}] [MonitorAutoDetect={yes,no}] [Swap={no, yes}] [EnsureDpIsOn ={yes, no}]	Default is **no**. **Dualhead** — Yes/no option to support a dual-monitor display. Default no sets monitors to mirror mode; yes sets monitors to span mode. **ManualOverride** — Default is **no**. Yes/no option to allow the local client to override display dualhead settings received from central configuration. If reset to factory defaults, it will once again take server settings for dualhead. This is helpful for scenarios where you have a mixture of dual head and single head deployments. For example: `Dualhead=yes ManualOverride=yes Mainscreen=1\Orientation=hort Taskbar=mainscreen` **NOTE:** If using, be sure the ManualOverride option is the first option used after the Dualhead parameter position in the statement. **Mainscreen** — Sets which screen is used as the main screen. When using a DVI to DVI and VGA cable, the DVI connected monitor will be the default mainscreen=1.

Parameter	Description

	Orientation — Default is **hort**. 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 — Default is **wholescreen**. 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. This is only when SysMode=Classic and has no effect on VDI mode.
	
	MonitorAutoDetect — Determines whether or not the system will detect how many monitors are connected. If only one monitor is connected, Span mode will be transferred to Mirror mode.
	
	Swap — Default is **no**. Yes/no option to use with older ThinOS 7.x builds to swap dual monitors when Mainscreen=2 is set. Swap=yes puts monitor 2 on the left or top of monitor 1 according to the orientation.
	
	For example, if you want a standard dual screen layout you would use:
	
	`DualHead=Yes \ Mainscreen=1 \ Orientation=Hort \ Taskbar=Mainscreen \ Align=Center`
	
	`Screen=1 Resolution=DDC Refresh=60 Rotate=None`
	`Screen=2 Resolution=DDC Refresh=60 Rotate=None`
	EnsureDpIsOn—The optional keyword is only used for Wyse 5010 thin client with ThinOS, Wyse 5010 thin client with PCoIP, Wyse 5060 thin client with ThinOS and Wyse 5060 thin client with PCoIP. When EnsureDpIsOn is set to yes, D-class will halt at boot time until DP monitor is plugged in.

EnableRAVE={yes, no}	Default is **yes**. Yes/no option to enable the client to use Citrix Multimedia Acceleration (RAVE) to play supported media files residing on an ICA server. This is a global parameter for all ICA connections. EnableRAVE=yes is default. **NOTE:** If EnableRAVE=no or this parameter is not present, the TCX Multimedia will be used for all media files. If EnableRAVE=yes, RAVE will be used only for media files it supports. EnableRAVE=yes is ignored unless a valid TCX Multimedia license is used.
FileServer=List of {IP address, DNS name} [Username=username] [Password=password] [SecurityMode={Low, Warning, Full, default}]	**FileServer** — Specifies the FTP or Web (http://) 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.

Parameter	Description
[Username-Enc={encrypted_password_string}] [Password-Enc={encrypted_password_string}]	**NOTE:** The target file server must support access using the same user credentials used in the INI files. The optional keyword Username and Password specify the username/password of the file server. When the client fetches the WNOS.INI file from a HTTPS server, ThinOS supports different security modes. The default follows SecurityPolicy and may be one of the three modes. The option SecurityMode specifies these security modes. **SecurityMode** — Specifies the security level for the file server during client verification of the server certificate. This option is only valid when connecting to an https file server. When configuring the https file server, the Username and Password options of the FileServer parameter can be omitted. Use the following guidelines: • Set SecurityMode=Full to have the client verify the server certificate in highest security mode; if any error occurs during verification, the client will not connect to the server and a pop-up message is displayed. • Set SecurityMode=Warning to have the client provide a warning when the client cannot verify the server certificate, but still allow the user to select to continue client connection to the server. • Set SecurityMode=Low to indicate that the client allows connection without any certificate verification. • Set SecurityMode=Default to indicate that the client follows SecurityPolicy settings to check certificate. • Default value of the setting is Default. If the settings are factory default or if you are upgrading to ThinOS 8.3 for the first time, the value is temporarily set to None. After loading any INI, it goes to default. • If the security mode value in WNOS.INI is not the same as the one saved in Client NVRAM, client shows a reboot dialog box. **NOTE: Security process includes:** 1 Verification that certificate has a valid date 2 Verification that Issuer is valid and correct 3 Certificate verification passes 4 CN and SAN on the certificate matches the DNS naming For Example: FileServer=https://10.151.122.66:444 SecurityMode=warning. **Username-Enc** specifies the AES encrypted username of the file server. **Password-Enc** specifies the AES encrypted password of the file server. Use Windows Password_Gen tool to generate the encrypted string.
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-on window, residing under the thin client home directory. The length of the path, including the

Parameter	Description
	home directory and the file, is limited to 128 characters. If auto dial-up is enabled, this statement is invalid.
HealthCastServer=vip list [LogLevel={0, 1, 2 ,3}] [SecurityMode={default, full, warning, low}] [ClientCertificate=certificate file name]	Specifies a list of VIP addresses with optional TCP port number of HealthCast servers. **LogLevel**—The option LogLevel is for debug purpose; 0 means no log. **SecurityMode** —Specifies the SSL certification validation policy. If set to default, it will apply SecurityPolicy setting. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, then drop the connection. If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, you may still continue or drop the connection. If set to low, the server certificate will not be checked. The value will be persistent, and the default value of the setting is default. **ClientCertificate** —The option specifies the client certificate file name during SSL connection between Healthcast server and client.
INACTIVE=minutes [NoSessionTimer=minutes] [LockTimer=seconds]	Default is 0. There is no Idle timeout. The range is 0 minutes to 480 minutes.If the value given is bigger than 480, 480 is set instead. If the value given is smaller than 0, 0 is set instead. When the system idle is time out in the configured minutes, the system will automatically sign off, reboot or shutdown which are based on the setting of AutoSignoff. **NoSessionTimer**— The parameter NoSessionTimer has the same range as INACTIVE and it is valid only if INACTIVE value is not 0. If there is a session use the value of Inactive, otherwise use the value of NoSessionTimer, if NoSessionTimer is configured. If AutoSignoff=yes Shutdown=yes is configured, then this statement can work before signon. If AutoSignoff=yes Reboot=yes is configured, this statement can work before signon. **LockTimer**—If the parameter LockTimer is set, the terminal is locked and the system idle is timeout in the configured seconds; System will automatically sign off, reboot or shutdown based on the setting of AutoSignoff.
LongApplicationName={no, yes}	Default is **no**. 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 "**...**".
MaxVNCD={0, 1} [VNCD_8bits={yes,no}] [VNCD_Zlib={yes, no}]	Default is **0**. Option to enable VNC shadowing. Default value is 0 means VNC shadowing is disabled. Set to 1 to enable shadowing. **NOTE:** Only one VNC client session is allowed and a password is required.

Parameter	Description
	See also VNCPrompt in Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files to enable a VNC shadowing prompt to a user. See also VncPassword in Connection Settings: wnos.ini files only to specify a string of up to 8 characters as the password used for shadowing. **VNCD_8bits** — Default is **yes**. Yes/no option to force the VNC server to send out images with 8-bits-per-pixel; if set to no, the VNC server will send out images with the current system color depth. **VNCD_Zlib** — Default is **no**. Yes/no option to allow the VNC server to send data with Zlib compression.
MMRConfig={VIDEO} [flashingHW={0, 1}]	This parameter specifies whether to show the “HW” label at the top left corner of video or not when HDX is hardware decoded. The default value is 0. Set flashingHW to 0, if you want to hide HW. Set flashingHW to 1, if you want to show HW.
Multifarm={no, yes}	Default is **no**. 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} [SequentialDomain={yes, **no**}]	Default is **no**. Yes/no option to support multiple log ons. If MultiLogon=yes, the PNAgent/PNLite sign-on authenticating window can input a different username, password, and domain while signing on to different PNAgent/PNLite servers. For backward compatibility, the following format is supported: MultiLogon=yes PNAgentServer=10.1.1.30;10.2.2.60 The SelectServerList statement is also supported: MultiLogon=yes SelectServerList=pna \ description=store host=http://proper-storefront-url.ctx.com description="Floor 3" host=10.1.1.30 \ description=""Floor 1" host=10.2.2.60 \ description="All Users" host=10.3.3.90 **NOTE:** The SelectServerList takes precedence over PNAgentServer. The PNA server description or name can be displayed on the signon window so that the user knows which and what server is logging on. See also SelectServerList={PNA, VDI} in Connection Settings for wnos.ini Files Only.

Parameter	Description
	If SequentialDomain=yes is specified, the domain configured in DomainList statement is selected in order. For example, set the following ini: DomainList="xen;wyse" multilogon=yes sequentialdomain=yes pnagentserver=10.151.134.23; https://csg-cn.wyse.com. When you logon to the first server 10.151.134.23, the domain xen is selected. Then logon to the second server https://csg-cn.wyse.com and the domain wyse is selected.
NoticeFile=filename [Resizable={no, yes}] [Timeout={0, 10 to 600}] [Title="notice_title"] [ButtonCaption="button_caption"]	**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-on process continues. **Resizable** — Default is **no**. Yes/no option to resize the dialog box to fit the text size. **Timeout** — Default is **0**. After the notice is accepted, if Timeout is specified in seconds, and if no mouse or keyboard is used, then the dialog box will display again after the seconds set. 0 means no timeout. **Title and ButtonCaption** — Specifies the notification window title and button that can be customized. For example, `NoticeFile=filename Title=Problem ButtonCaption=Ok`
OneSignServer=onesign_server [DisableBeep={yes,no}] [KioskMode=yes,no}] [TapToLock={0,1,2}] [EnableWindowAuthentication={yes,no}] [AutoAccess={VMW,XD,XA,LOCAL,RDSHD, RDSHA, RDSHPC}] [NetBIOSDomainName={yes,no}] [SuspendAction={0, 1}] [DisableHotKey={yes,no}] Loglevel=0/1/2/3 [DisablePromptToEnroll={yes,no}] [SecurityMode={default, full, warning, low}]	A list of host names or IP addresses with optional TCP port number or URLs of Imprivata OneSign servers. It should use https protocol. If OneSignServer="" is defined, then only imprivata virtual channel can work.If DisableBeep is set to yes, then Rfideas reader can be set to mute when a card is tapped. Default is no. If KioskMode is set to yes, then different OneSign user can unlock the client desktop. Default is no. Optional keyword TaptoLock is only active when KioskMode=yes. · If TapToLock=0, then tap a card to lock terminal is disabled. · If TapToLock=1(Tap to lock), then use the proximity card to lock the terminal. · If TapToLock=2(Tap over), then lock the terminal and log in as a different user. Default is 2. If EnableWindowAuthentication is set to yes and OneSign signon fails, then continue to sign-on with windows credential to pre-define broker. Default is yes. If AutoAccess is defined, then auto launch the corresponding type of broker. Otherwise, get the broker type from the Imprivata Server setting of computer and user policy. If none of them is defined, then launch the first available broker server from the Imprivata server. If AutoAccess=LOCAL is set, then launch the broker from the ThinClient setting; the broker getting from the Imprivata Server is ignored. **NOTE: AutoAccess can be set in [username].ini and wnos.ini. The wnos.ini has priority over [username].ini.**

Parameter	Description
	If NetBIOSDomainName is set to yes, then Imprivata domain list will show NetBIOS domain name and card user will authenticate to the broker server using NetBIOS domain name. Default is no. If SuspendAction is set to 0, then lock the terminal when you tap the card or press the hotkey. If set to 1, then signoff the terminal. If 'no' is defined, then lock the terminal in KioskMode and sign-off the terminal in none KioskMode. If DisableHotKey is set to yes, then no action when you press the hotkey defined in Imprivata Server. Only WebAPI 4 and later versions support the hotkey function. Loglevel—While configuring the Imprivata server, user can view the OneSign logs on ThinOS by enabling the Agent Logging feature. An ini configuration is needed correspondingly. Default value is 0. If set to 0, logs are not displayed. If DisablePromptToEnroll is set to yes, then ThinOS does not prompt you to enroll their security answers after OneSign sign-on. Default value is yes. SecurityMode specifies the SSL certification validation policy. If set to default, it applies SecurityPolicy setting. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, drop the connection. If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, and the default value of the setting is default. From ThinOS version 8.3_109, ThinOS supports OneSign 5.2 RDSH broker. Set AutoAccess=RDSHD or RDSHA to automatically launch Microsoft type broker. Set RDSHPC to automatically launch RDP session without broker.
PasswordServer=password_server [AccountSelfService={yes, no}] [connect={ica, rdp}] [encryption={Basic, 40, 56, 128, Login-128, None}]	Specify an ica/rdp server that can be used to log on to modify password when you sign-on with password timeout. The PasswordServer statement can specify the connection parameters as described in the Connect statement. If no parameter is specified, it connects with ICA protocol. AccountSelfService — Yes/no option to define the password server as an Account Self Service server. If AccountSelfService=yes follows PasswordServer, click the icon on the signon window to do account self-service. If Connect parameters do not follow AccountSelfService=yes, this password server will be the account self-service server of Citrix and clicking the icon will use Citrix protocol to unlock or change password for an account. If Connect parameters follow AccountSelfService=yes, clicking the icon launches a session to change password for an account.
PCoIP_Logging={yes, no} [Broker_Logging_Level={0,1,2,3,4}]	The option PCoIP_Logging can enable and disable the PCoIP client logs output in Trouble Shooting. If you set the value to yes, then it is same as selecting the Trouble Shooting Capture Export PCoIP Log radio button to persistent and no to none.

Parameter	Description
[Session_Logging_Level={0,1,2,3,4}]	The option Broker_Logging_level and Session_Logging_Level accord to PCoIP broker log level and PCoIP session log level. The default value is 0 which means critical log, 1 means log severity error, 2 means log severity info, 3 means log severity debug, and 4 means log severity unrestrained.
PlatformConfig=all [EncryptFS=yes]	Encrypts local flash, specifically cached INI files and credentials that are stored, if using signon=yes. **NOTE:** Event log will display new statements stating that FileSystem encryption has been enabled.
PlatformConfig="C/V/S/R/T Class" [Firmware={Firmware filename}] [BIOS={BIOS filename}] [ECFirmware={EC filename}]	If a specific platform is specified by the PlatformConfig parameter, then ThinOS 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, ThinOS will load the platform default Firmware and BIOS instead. For example: If you re-name the Wyse 3010 thin client with ThinOS (T10) firmware file from DOVE_boot to DOVE_boot_8.0_037., then you must use platformconfig-="T Class", then add Firmware=DOVE_boot_8.0_037. ThinOS will look on the file server for this exact firmware name. If that defined firmware name is not found, then ThinOS will fall back to the default logic and look for the DOVE_boot firmware. ECFirmware is only used for Wyse 3010 thin client with ThinOS (T10)/X10J/X10CJ to update EC firmware, it is not supported on other platforms. C: C10LE V: VL10 S: S10 R: R10L Wyse 3010 thin client with ThinOS (T10) If the ECFirmware file name is not specified, device will look for EC with default name: T10: T10_EC.bin
Proxy={yes, no} AppList={ccm;fr;rtme;wms} [Type={Global, http, https, socks5}] [Server=_host_port_] [User=_user_name] [Password=_password_] [Encrypt={yes, no}]	Specifies the proxy settings which are saved in non-volatile memory. If Proxy=no, all proxy settings are cleared and all the followed options are ignored. If Proxy=yes, the option AppList must be followed. It specifies which applications are applied to connect through proxy. WMS, CCM, FR, and RTME are supported. The application name is separated with semicolon. **NOTE: Wyse Management Suite is the successor to Cloud Client Manager (CCM).** The following options are used to configure one or several proxy server setting. The option Type specifies the proxy protocol including http, https and socks5. The option Server specifies the url of the proxy server. The option User and Password specify the credentials of this proxy server. The option Encrypt specifies if the password is encrypted or not.

Parameter	Description
	The option User and Password can support system variables. Because CCM runs before sign on, it is not appropriate to use $UN and $PW. If Type=Global, the proxy settings are saved into http proxy setting, and the https and socks5 proxy settings use the same setting as http proxy. And the followed proxy settings will be ignored. For example, Proxy=yes AppList=fr \ Type=http Server=server1:1234 user=$UN password=$PW (OR) Proxy=yes AppList=ccm \ Type=http Server=server1:1234 user=abc password=xyz \ Type=socks5 Server=server2:4321 user=abc password=1234 (OR) Proxy=yes AppList=ccm;fr;rtme \ Type=Global Server=server_global user=user_global password=password_global_encrypted Encrypt=yes
RapportDisable={yes, no} [DHCPinform={yes, no}] [DNSLookup={yes, no}] [QuickMode={yes, no}] [Discover={yes, no}] [SecurityMode={default, full, warning, low}]	Set to yes to disable the Rapport agent. If RapportDisable=no, the Rapport agent is enabled and you can discover the WDM server by the following ways: 1 The DHCP option tag values received from standard or WDM proxy DHCP service for vendor class RTIAgent 2 DNS service location record "_wdmserver._tcp" 3 DNS host name lookup "wdmserver" If RapportDisable=no, set DHCPinform=yes to perform the WDM server discovery as mentioned in number 1; set DNSLookup=yes to perform the WDM server discovery as mentiomned in number 2 and 3. If QuickMode=yes is specified, rapport agent will not block any other process during ThinOS boot up, and boot time of ThinOS will speed up. **NOTE: If file server is changed by WDM server, device will reboot automatically to make sure all settings from WDM server take effect. Default is yes.** **Discover**— If Discover=yes is specified, rapport discovers the WDM server information from DHCP option tag, DNS service location record and DNS host name. If the WDM server is discovered, the WDM server User Interface (UI) is protected on the device. The default value is yes. **SecurityMode** specifies the SSL certification validation policy. If set to default, SecurityPolicy setting is applied. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, drop the connection.

Parameter	Description
	If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, and the default value of the setting is default. If the settings are factory default or if you are upgrading to ThinOS 8.3 for the first time, the value is temporarily set to low. After loading any INI, it goes to Default value.
RapportServer=server_list [Retry=]	**IMPORTANT:** DISCONTINUED. DO NOT USE. Use **WDMServer** parameter, see WDMServer=<server_list> in Connection Settings for wnos.ini Files Only.
Reboot | shutdown={no, yes} Time=hh:mm [-hh:mm] [Wday={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}] [Idle=minutes]	**Reboot** — Yes/no option to enable automatic daily reboot of all ThinOS 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 ThinOS devices at 5:30 P.M. daily. If you set time as hh:mm-hh:mm, a random time during the configured time period is selected. **Wday**— The option Wday specifies the week day of scheduled reboot. **Idle**— The option Idle specifies the idle minutes. After the scheduled reboot time is reached, the unit reboots, if there is no session or the terminal is idle for specified idle minutes. If the session is still active, the reboot is delayed till the idle time is reached or log off the sessions. For example, If you set Reboot=yes time=20:30, the unit reboots on local time 20:30. If you set Reboot=yes time=20:30-4:30, the unit reboots on random time through 20:30 to 4:30. If you set Reboot=yes time=23:00 Wday=Friday,Monday, the unit reboots on local time 23:00 of Friday and Monday. If you set Reboot=yes time=1:00 Idle=10, the unit reboots on 1:00, if there are no sessions. If there is any active session, the reboot happens only if the unit is idle for 10 minutes or the system logs out from the session. Since 8.3_012 or later, scheduling a shutdown at a given time is supported. The options are same as schedule a reboot as above. For example, Set Shutdown=yes time=20:30, the unit shuts down at local time 20:30.
RegisterWINS=yes	Forces the thin client to register itself with a Microsoft WINS server.
ScepAutoEnroll={yes, no} AutoRenew={yes, no} InstallCACert={yes, no}	This option is to allow client automatically get certificates and renew certificates using SCEP protocol. **ScepAutoEnroll**—Set this keyword to yes to enable client's functionality to automatically obtain certificate.

Parameter	Description
[CountryName=country] [State=state] [Locality=locality] [Organization=organization_name] [OrganizationUnit=organization_unit] [CommonName=common_name] [Email=email_address] [KeyUsage=key_usage] [KeyLength={1024, 2048, 4096}] [subAltName=subject_alt_name_list] [RequestURL=scep_request_url] [CACertHashType={MD5, SHA1, SHA256}] [CACertHash=CA_HASH_VALUE] [EnrollPwd=enrollment_password] [EnrollPwdEnc=encrypted_enrollment_password] [ScepAdminUrl=scep_administrator_page_url] [ScepUser=scep_enrollment_user] [ScepUserDomain=scep_enrollment_user_domain] [ScepUserPwd=scep_enrollment_user_password] [ScepUserPwdEnc=encrypted_scep_enrollment_user_password]	Set **AutoRenew**—Set this keyword to yes to enable certificate auto renew. Client only tries to renew certificates requested either manually or automatically through SCEP from this client, and the renewal is performed only after a certificate's 1/2 valid period has passed. Set **InstallCACert**—Set this keyword to yes to install the root CA's certificate as trusted certificate after successfully getting a client certificate. **CountryName, State, Locality, Organization, OrganizationUnit, CommonName, Email**—These keywords together compose the subject identity of the requested client certificate. Country Name should be two letter in uppercase, other fields are printable strings with a length shorter than 64 bytes, and email_address should have a '@' in it. At least one of the above fields must be configured correctly to form the client certificate's subject identity. **KeyUsage** —This option is to specify key usage of the client certificate and should be set to a digitalSignature, keyEncipherment or both using a ';' concatenating these two as digitalSignature;keyEncipherment. **KeyLength**—This option is to specify the key length of the client certificate in bits, must one of the value in the list. **subAltName**—This option is to specify the client certificate's subject alternative names. It is a sequenced list of name elements, and every element is either a DNS name or an IP address. Use ';' as delimiter between them. **RequestURL**—The **RequestURL** option is to specify the SCEP server service URL. This field must be set correctly. The default protocol for SCEP services is HTTP, which also ensures data security. You can also add the prefix **https://** if SCEP service is deployed on HTTPS in your environment. **CACertHashType**—**CACertHashType** is used to verify the authenticity of the certificate authority. This option must be set to MD5, SHA1, or SHA256. **CACertHash**—This is the hash value used to verify certificate authority's certificate. Client will not issue a certificate request to a SCEP server and cannot pass certificate chain checking through a valid certificate authority. **EnrollPwd** or **EnrollPwdEnc**—These keywords are used to set the enrollment password from a SCEP administrator. **EnrollPwd** is the plain-text enrollment password and **EnrollPwdEnc** is the encrypted form of the same enrollment password. Use only one of these two fields to set the used enrollment password. As a substitute of using EnrollPwd or EnrollPwdEnc to directly specify an enrollment password, client allows using a SCEP administrator's credential to automatically get an enrollment password from a Windows SCEP server. In this case, the **ScepUser**, **ScepUserDomain**, **ScepUserPwd** (or ScepUserPwdEnc, in encrypted form instead of plan-text) are used to specify the SCEP administrator's credential, and ScepAdminUrl must be set correctly to specify the corresponding SCEP admin web page's URL. If neither EnrollPwd nor EnrollPwdEnc is set, client will try to use these set of settings to automatically get an enrollment password and then use that password to request a certificate. If communication security is necessary in your

Parameter	Description
	environment during this phase, please add https:// as the prefix for ScepAdminUrl to use HTTPS instead of the default HTTP protocol. Use ScepAutoEnroll=no AutoRenew=yes to only enable SCEP auto renew; all other parameters are not needed if ScepAutoEnroll is set to no. **NOTE: SCEP server's URL must be an HTTP or HTTPS link. Do not add protocol prefix to RequestURL and ScepAdminURL.**

SelectServerList={PNA, VDI}
 	
[Default=default_desc]
 	
list of servers {Server1; Server2; ...ServerN}
	Allows users to select one PNA or VDI server during logon. For server use the format:
	
	description = <server's description> host = <server's url> [<options>]
	
	NOTE: There must be "description" and "host" key words on each server.
	
	For PNA server options, use the options of the PnliteServer parameter in Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files.
	
	PNA example:
	
	`SelectServerList=PNA; Default=test3; description = test1; host = 192.168.0.10; autoconnectlist =*; reconnectfrombutton=0; description = test2; host = HostName2.wyse.com; TimeOut=200; descriprion = test3 host = https://server3.wyse.com`
	For a VDI server: If you want to use a VDI broker, specify ConnectionBroker in wnos.ini. Otherwise the VDI broker's type is default.
	
	VDI example:
	
	`ConnectionBroker=VDM SelectServerList=VDI; Default=test5 description = test4 host = 192.168.0.11; description = test5 host = host2.wyse.com`
	The Default option following "SelectServerList={PNA, VDI}" can specify the default server. The value is one of server description defined after that. After one selects another server and sign off, this default server is selected. If default option is not specified, the last selected server is selected in the next sign on.

Service={snmpd, thinprint, vncd, wdm, vda <port number>} disable={no, yes}	**Service** — Specifies the services you can enable or disable; there are different syntaxes for the different services. **disable** — **Default is no.** Yes/no option to disable the services. Disable must follow the Service parameter.
Service=snmpd disable={no, yes} [community=<snmp_community> [encrypt={yes, no}]] [communityReadOnly=<snmp_community_read_only> [encrypt={yes, no}]]	Default is **no**. **Service=snmpd disable** — Yes/no option to disable the snmpd service. **community** — The option community is same as the statement Community. encrypt option is same as that in the statement community.

Parameter	Description
[servers=server_list]	**communityReadOnly**— This option is to set community only has snmp get and get_next privileges. The following encrypt option is only for indicating, if value of communityReadOnly is encrypted. **Servers** —This option is set to limit the valid snmp management site to the IP addresses in the server_list parameter, which contains 1 to 4 IPv4 IP addresses currently. If not, all the set IP addresses seen as valid.
Service=thinprint disable={no, yes} [port=<port number>] [PkSize={0-64000}]	Default is **no**. **Service=thinprint disable** — Yes/no option to disable the thinprint service. **port** — Same as the statement ThinPrintEnable={no, yes} port=portnumber. **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. ThinOS 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} [servers=server_list] [HttpPort=_http_port_] [TcpPort=_tcp_port_]	**Service=vncd disable**—Yes/no option to disable the vncd service, same as MaxVncd={0, 1}. Default is **no**. **servers**—Use the servers option to limit the valid vncd client site to the IP addresses in the server_list parameter, which contains IPv4 IP or IP range addresses, such as 192.168.1.0/24; 192.168.2.48. If this option is not set, all IP addresses are displayed as valid. The service vncd supports both http and tcp connections. The option **HttpPort** enables you to set the http port for vncd service. The default port is 5800. The option **TcpPort** enables you to set the tcp port for vncd service. The default port is 5900.
Service=wdm disable={no, yes}	Default is **no**. Yes/no option to disable the WDM service, same as RapportDisable={no, yes}.
Service=<port number> disable={no, yes}	Default is **no**. Yes/no option to disable the service with this port number. The 80 port is an exception because the WDM is always started before loading the global profile (wnos.ini file).
SecurityPolicy={full, warning, low} [SecuredNetworkProtocol={yes, no}] [TLSMinVersion]={1,2,3}] [TLSMaxVesion={1,2,3}]	Specifies the global security mode for SSL connection. If application SecurityMode is default, application applies the setting. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, connection is dropped.If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it is up to you to continue or drop the connection. If set to low, the server certificate is not checked.

Parameter	Description
[DNSFileServerDiscover={yes, no}] [TLSCheckCN=[yes, no]]	The value is persistent, and the default value is **warning**. For those SSL connections with their own security policy, this does not impact. For example, File server, VMware View and AWS broker follows the global SecurityPolicy. Citrix broker, RDS broker and SECUREMATRIX are forced to high security mode. If the optional SecuredNetworkProtocol=yes is set, the unsecure protocols including ftp, http and tftp are disabled. The value is persistent, and the default value is no. TLSMinVersion and TLSMaxVersion allows you to configure the SSL connection. ThinOS supports SSLs from TLSMinVersion onwards. TLSMaxversion is the latest version of SSL supported by ThinOS. TLSMinVersion sets the minFallbackMinorVersion. Server uses the version equal to minFallbackMinorVersion or higher to communicate with the client. TLSMaxVersion sets the advertisedMinorVersion. Server uses this version equal or above to communicate with the client. If no value is set for TLSMinVersion then the default value is set to TLS1.0 and TLSMaxVersion is set to TLS1.2. The value 1, 2, 3 corresponds to TLS1.0, TLS1.1, TLS1.2 respectively. These parameters are used by engineers for internal tests. In classic mode, a DNS name wyseftpfbc4tc is resolved to discover the file server, if the global INI file in remote file server and local cache cannot be loaded. If the optional DNSFileServerDiscover=no is set, the function is disabled. The value is persistent, and the default value is yes. **TLSCheckCN**—This option enables you to check the server certificate common name for SSL connection in full security mode. This option does not impact SSL connections of VMware View, Amazon WorkSpaces and VPN. These connections continually check server certificate common name. The default value is changed to **Yes** from build version 8.5_106. **NOTE: Use NetBIOS or FQDN values to define a SSL—Https—connection when enabling TLSCheckCN option, as enabling TLSCheckCN results in SSL connection failure when an IP address is defined.**
SignOn={yes, no, NTLM} [MaxConnect=max] [ConnectionManager={maximize, minimize, hide}] [EnableOK={no, yes}] [DisableGuest={no, yes}] [DisablePassword={no, yes}] [LastUserName={no, yes}] [RequireSmartCard={yes or force, optional, no}] [SCRemovalBehavior= {none or -1, logoff or 0, lock or 1, killsessions or 2}]	**SignOn** — Default is **yes**. Yes/no/NTLM option to enable the sign-on 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-on user credentials must be available in the ftp://~/wnos/ini/ directory. **MaxConnect** — Default is **216**. Maximum number of connections allowed to be specified in the wnos.ini file and {username}.ini file added together. The range allowed for MaxConnect is 100 to 1000. The default maximum is 216 entries. **ConnectionManager** — Default is **minimize**. State of the Connect Manager during sign-on. **EnableOK** — Default is **no**. Yes/no option to show the OK and Cancel the command buttons in the Sign-on dialog box.

Parameter	Description
[SaveLastDomainUser={yes, no, user, domain}] [DefaultINI=filename] [IconGroupStyle={default, folder}] [IconGroupLayout={Vertical, Horizontal}] [PasswordVariables={yes, no} [LockTerminal={yes, no}] [ExpireTime={0, 1 - 480}] [UnlockRefresh={yes, no}] [SCShowCNName={yes,no}] [SCSecurePINEntry={no, yes}] [AutoConnectTimeout={10–300}] [DisableEditDomain={yes, no}] [AdGroupPrefix=adgrpnameprefix] [ClearUser={yes, no}] [DisableSignoff={yes, no}] [SFZeroButtons={yes, no}] [SignonStatusColor="rrr ggg bbb"]	**DisableGuest** — Default is **no**. Yes/no option to disable the guest sign-on. **DisablePassword** — Default is **no**. Yes/no option to disable the password text box and password check box in the Sign-on dialog box. **LastUserName** — Default is **no**. Yes/no option to display the last sign-on username after the user logs off. **RequireSmartCard** — Default is **optional**. If optional keyword is set to yes or force, only smartcard authentication is allowed. If set to no, smartcard authentication is disabled. If the value is set to optional, smartcard authentication is optional. **SCRemovalBehavior** — This parameter specifies the thin client behavior when a smart card is removed. The default value is **0**. · **none or -1** — If the smart card is removed then the client has no action. Whether the session can be used or not is dependent on the server policVNCD. · **logoff or 0** — System logs off. · **lock or 1** — System is locked and can be unlocked only when the same certificate is used with smart card. · **killsessions or 2** — This option can be used with the AutoSignoff parameter. **SaveLastDomainUser** — Yes/no option to save the username and domain into NVRAM once signon is successful. On next reboot, the username and domain saved in the NVRAM will be displayed in signon 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. **DefaultINI** — The optional DefaultINI configures a file name which is in the default folder of the username ini files. If the {username}.ini is not found, this file will be loaded as default. **IconGroupStyle** — The optional IconGroupStyle configures the icon group style on the desktop. PNAgent published applications can be configured with the client folder in the PNA server. If set IconGroupStyle=folder, the PNAgent published applications which are specified to display on the desktop will display with the folder. After clicking the folder icon, the subfolder or applications in this folder will display on the desktop. In this case, there is an Up to 1 Level icon on top. Clicking the icon will display the up one level folder contents. **IconGroupLayout** — Default is **vertical**. Configures the direction of the icongroup on the desktop. **PasswordVariables** — Default is **no**. Yes/no option to support variable mapping ($TN, $UN etc) for a password. **LockTerminal** — Default is **yes**. Yes/no option to lock the terminal. If set LockTerminal=no, the function of locking terminal is disabled. It disables the Lock Terminal from a Right Click on the desktop or from clicking the **Shutdown option** > **Lock Terminal**. It also disables lock terminal even if set ScreenSaver=minutes; LockTerminal=yes.

Parameter	Description
	ExpireTime — Specifies the signon expiration time. The range is 0 to 480 minutes. The default is **0** which means no expiration. If the value is larger than 480, then 480 is set instead. If the value is smaller than 0, then 0 is set instead. After system signon or starting a connection, the expiration time starts counting. Once the expiration time is reached, starting a connection by clicking the icon, menu or connection manager, will bring up a pop up message box to enter the password. Only if the password is same as the original signon password, the session starts. If the terminal is locked and unlocked with the password, the signon expiration time starts counting again. **UnlockRefresh** — Default is **yes**. Yes/no option to specifies the refresh action after unlocking the system in classic mode. Yes — While unlocking, the system will refresh the PNA list to verify the password. No — Disables refresh. **SCShowCNName** — Default is **yes**. Yes/no option to force the use of the CN name of the certificate as the user name when using smartcard signon. The default uses the UPN name as the user name. **SCSecurePINEntry** — Default is **no**. Yes/no option to enable Secure PIN entry function for pkcs15 smart card with Cherry keyboard. **AutoConnectTimeout**— Default is **30** seconds. This option sets the timeout for auto connect published application. The range is 10 seconds to 300 seconds. **DisableEditDomain**— The optional keyword DisableEditDomain, is set to yes to stop typing in the domain box manually. Typing the character @ or \ as in the format domain\user and user@domain in the username box are not allowed. **AdGroupPreFix**— The option AdGroupPreFix is only valid, when you configure SignOn=NTLM. If the option is configured, then the thin client verifies the names of all AD groups to which a sign-on user belongs, to get the first group name so that its prefix matches adgrpnameprefix, and load adgroup/"the_whole_ad_group_name".ini, if the configuration file exists, before loading the user specific INI. For example, if the sign on user is user_111 in a domain, and the user_111 belongs to group domain user and group tc_grp1_ad, the option is configured as AdGroupPrefix=tc_grp1. If the configuration file adgroup/tc_grp1_ad.ini is available, it will be loaded. **ClearUser**—The option keyword ClearUser, if set to yes, clears the username when login fails, and if set to no, retains username entered after login failure. The default value is no. **DisableSignoff**—The option keyword DisableSignoff, if set to yes, disables signoff button from shutdown and connection manager window. Also this parameter disables the logoff button on StoreFront desktop.

Parameter	Description
	SFZeroButtons—The option keyword SFZeroButtons. if set to yes, displays the buttons (shutdown, login and so on) at the bottom of signon window, such as Zero mode when set StoreFront style. **SignonStatusColor**—The option specifies the signon status text color in RGB string format (must be enclosed in quotes), where rrr, ggg, and bbb are decimal numbers in the range of 0 to 255. By default, the status text color is gray for ThinOS.
Speedbrowser={on, off}	Default is **on**. On/off option to enable the ICA Speedscreen Browser Acceleration Function.
SwitchApplication	**IMPORTANT: DISCONTINUED. DO NOT USE.**
SysMode={classic, vdi, VMware, Citrix} [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}] [ToolbarEnableOneSession={no, yes}] [ToolbarAutoQuit={yes, no}] [ToolbarStay={1~20}] [EnableLogonMainMenu={no, yes}}	**SysMode** — Specifies the 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 and for backward compatibility with WTOS 6.x. VDI mode (Zero interface) has a new launchpad-style interface optimized for full-screen sessions that is Desktops. Everything you need is accessed through an always available overlay interface. VMware mode looks similar to VDI mode but only allows VMware horizon broker. Login window and wallpaper is specific to horizon. Citrix mode makes the client turn to Xenith. Xen.ini is prefered in the next reboot. **NOTE: VMware mode and Citrix mode can only be used under wnos.ini. ZeroTheme is the alias for SysMode. You can also use ZeroTheme=xxx in wnos.ini.** The following options allow you to configure only when the Zero toolbar displays under VDI mode: **Toolbardisable** — Default is **no**. Yes/no option to disable the Zero toolbar from displaying; if set to yes, this option overrules other toolbar display options. **Toolbardisablemouse** — Default is **no**. Yes/no option to disable the Zero toolbar from automatically displaying once you pause the mouse pointer on the left side of the screen for a specified amount of time. **toolbarclick** — Default is **no**. 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 pausing the mouse pointer on 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** — Default is **no**. Yes/no option to hide the Home button.

Parameter	Description
	toolbar_no_minimizeall — Default is **no**. Yes/no option to hide the Home button thus affecting the ability to minimize displayed list of connections. **toolbardisablehotkey** — Default is **no**. Yes/no option to disable the CTR+ALT+UP ARROW keyboard shortcut that allows the toolbar to instantly display without a timer. **ToolbarEnableOneSession** — Default is **no**. Yes/no option to enable the toolbar when only one session is available. **ToolbarAutoQuit** — Default is **yes**. ToolbarAutoQuit=no prevents the sub-window from being closed. The toolbar will auto-hide after a certain amount of time after user pause the mouse pointer away from the toolbar. **ToolbarStay** — ToolbarStay={1~20} controls the auto-hide duration, 0.5s per value. Thus if ToolbarStay=1, the Toolbar will auto-hide after 0.5 second; If ToolbarStay=10, the Toolbar will auto-hide after 5 seconds. **EnableLogonMainMenu** — Default is **no**. Yes/no option to enable the main menu if you click the mouse button on the desktop prior to logon in Zero mode.
SysName	**IMPORTANT: DISCONTINUED. DO NOT USE.**
TcpTimeOut={1 , 2}	Default is **1**. Specifies the timeout value of a TCP connection. The number of 30 seconds for the timeout value of a TCP connection. The value must be **1** or **2** which means the connection timeout value is from 1x30= 30 seconds to 2x30= 60 seconds. Values of 3-255 are recognized only for backwards compatibility that is >2 = 60 seconds, however, these values should not be used and the value should be set to 2.
TCXLicense	**IMPORTANT: DISCONTINUED. DO NOT USE.**
VncPassword=<password> [encrypt={no, yes}]	**VncPassword** — Specifies a string of up to 8 characters as the password used for shadowing. **encrypt** — Default is **no**. Yes/no option to set according to whether or not the vncpassword you are using is encrypted.

Parameter	Description
	IMPORTANT: To use VNC Shadow, you must set MaxVNCD=1 and define a password; The MaxVNCD default is 0 and this disables VNC. If you are using an encrypted password, you must set encrypt to yes. For example: `VncPassword=<encoded password> encrypt=yes` If you are using a plain text password, you must set encrypt to no. For example: **`VncPassword=<plain text> encrypt=no`** See also MaxVNCD in Connection Settings: wnos.ini files only to enable VNC shadowing. See also VNCPrompt in Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files to enable a VNC shadowing prompt to a user.
WarnUnlinkDisabled={yes, no}	Default is **no**. Yes/no option to disable the pop-up warning message when a network has no link for an ICA/ RDP session.
WDAService=yes [Priority ={WDM, CCM, "WDM;CCM", "CCM;WDM"}] [disableNotice={yes, no}] [disableCancel={yes, no}] [noticeTime={0-255}] [interval = {0-65535}] [enableReminder={yes, no}]	WDA Service always runs in the background. **Priority**—If priority is available, WDA discovers the protocol according to it. There are only two protocols available now - WDM, and CCM. For example, if priority=WDM; CCM, WDA tries to discover WDM server and tries to check-in, and if it fails to check-in to WDM server, it tries to check-in the device to CCM server. **disableNotice**—If option is set to yes, count down prompt will not show when configuration from WDM is received. Default is no. **disableCancel**—If set to yes, there is no possibility to cancel count down prompt for WDM (device is going to reboot). Default is no. **noticeTime**—If this is set, then the time of countdown prompt is changed to seconds. Default is 20 seconds. Examples: WDAService=yes disableNotice=no disableCancel=yes noticeTime=0. In this scenario, count down prompt is displayed if WDM configuration is received, but you are not allowed to cancel system reboot, and amount time of count down prompt is set to default value (20 seconds). **interval**—If interval is available, WDA rediscovery is delayed after check-in fails (both CCM and WDM fails). This delay is changed to interval minutes. Default is 0. (WDA rediscovery delay is 24 hours). Example: WDAService=yes interval=30 WDA rediscovery delay is set as 30 minutes. **enableReminder**—If enableReminder is set to yes, the reboot warning window is displayed and the user has an option to postpone the reboot. The default value is No. Example: WDAService=yes enableReminder=yes

Parameter	Description
	Whenever a reboot is required from Wyse Management Suite agent, a warning dialog window is displayed. The user can postpone the reboot for as many times set by the admin.
WDMFlash=flash_size	The specified value will be saved into NVRAM, and then reports to the WDM server. This statement ensures that all the units would function with DDC regardless of flash size. This statement is valid for all platforms and replaces the previous S10 WDM Flash statement.
WDMService={yes, no} [DHCPinform={no, yes}] [DNSLookup={no, yes}] [QuickMode={yes, no}] [Discover={yes, no}] [SecurityMode={default, full, warning, low}]	Default is **yes**. **WDMService** — Yes/no option to disable the WDM agent. Discovering the WDM server is supported by the following: 1 DNS host name lookup **wdmserver** 2 DNS service location record **_wdmserver._tcp** 3 DHCP option tag values received from standard or WDM proxy DHCP service for vendor class **RTIAgent** **DHCPinform** — Default is **no**. Yes/no option to use DHCP information. **DNSLookup** — Default is **no**. Yes/no option to use DNSLookup. For Example: If WDMService=yes, setting DHCPinform=yes will do number 3, setting DNSLookup=yes will do numbers 1 and 2. If QuickMode=yes is specified, rapport agent will not block any other process during ThinOS boot up, and boot time of ThinOS will speed up. **NOTE: If file server is changed by WDM server, device will reboot automatically to make sure all settings from WDM server take effect. Default is yes.** **Discover**— If Discover=yes is specified, rapport discovers the WDM server information from the DHCP option tag, DNS service location record and DNS host name. If the WDM server is discovered, the WDM server User Interface (UI) is protected on device. The default value is yes. **SecurityMode** specifies the SSL certification validation policy. If set to default, it will apply SecurityPolicy setting. If set to full, the SSL connection needs to verify server certificate. If it is untrusted, then drop the connection. If set to warning, the SSL connection needs to verify server certificate. If it is untrusted, it's up to you to continue or drop the connection. If set to low, the server certificate is not checked. The value is persistent, and the default value of the setting is default. If the settings are factory default, or if you are upgrading to ThinOS 8.3 for the first time, the value is temporarily set to low. After loading any INI, it goes to default value.
WDMServer=<server_list>	**WDMServer** — Specifies a list of IP addresses or DNS names separated by using a comma for the WDM servers. Once specified, it is saved in non-volatile memory.

Parameter	Description
[Retry=<retry number value>]	**Retry** — Determines the number of attempts to retry a contact to WDM servers.
WINSServer=server_list	Specifies the WINS server address. The WINSserver is an IP list separated by "**;**" or "**,**", with a maximum list size of 2.
AutoSelectSingleCert={yes, **no**}	When HTTPS is configured to verify client certificate, one window pops up for user to select the client certificate. If only one client certificate is available, set **AutoSelectSingleCert=yes** does not prompt the window and automatically select the client certificate.

4

Parameters for wnos INI, {username} INI, and $MAC INI files

This chapter provides the supported parameters that you can use in a wnos.ini file, a {username}.ini file, and in a $MAC.ini file. For information to help you construct and use the supported INI files, see Getting Started: Learning INI File Basics

To increase usability such as relation to thin client dialog box equivalents, the supported parameters are separated into the following categories:

- General Settings for wnos.ini Files, {username} INI, and $MAC INI Files
- Peripheral Settings for wnos.ini Files, {username} INI, and $MAC INI Files
- Connection Settings for wnos.ini Files username INI and MAC INI Files

IMPORTANT:

The underlined value for a parameter is the default value. Some parameters also have options shown within brackets [ ]. If an option has an underlined value (default), that option and default value will automatically be used with the parameter. The options without underlined values can also be used if you want to, but are not automatically used with the parameter. In addition, when using parameters and options, you can leave the default value or change it to another value shown.

For example, in the following case where:

```
ParameterX={yes, no}
[Option1={0, 1}]
[Option2={1, 2, 3, 4}]
```

If you use ParameterX, then Option1 and its default value 0 will automatically be used as Option1 has an underlined value (default of 0). You can still use Option2 if you want to, however, Option2 is not automatically used with the parameter as Option2 does not have a default (underlined) value.

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 in this section noted with * do not allow this. Thus, if the parameters in this section 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 this section noted with ** that are used in a {username}.ini file or $MAC.ini file will return to the values set for those parameters in the wnos.ini file after a user sign-off.

For example, if your {username}.ini file contains the parameter MouseSwap=1—so that the mouse buttons are swapped for your left-hand use and you log off 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 log in can use their own user profile; assuming the administrator has not changed the default values in the wnos.ini file.

General settings for wnos.ini files, {username} INI, and $MAC INI files

The following table contains the parameters used for configuring general settings. The underlined values are defaults.

Table 8. General Settings: wnos.ini files, {username} INI, and $MAC INI Files

Parameter *** Global overrides identically-named user profile** **** After sign off, user profile returns to global value**	**Description**
AdminMode={no, yes} [admin-username=<encrypted_ username>] [admin-password=<encrypted_ password>] [Username=<username>] [Password=<password>] [Enc-username=encrypted_username] [Enc-password=encrypted_password] [ShowAESButton={yes, no}]	**AdminMode** —Default is **no**. Yes/no option to use the username and the password to obtain a high 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; no minimum length; maximum length is 30 characters—15 characters convert to 30 characters encrypted. **admin-password**—Specifies if admin-password=encrypted_password, then encrypted strings are used for admin-password; no minimum length; maximum length is 30 characters—15 characters convert to 30 characters encrypted. **Enc-username**—Specifies if the username is encrypted, and encrypted strings are used for the Enc-username. **Enc-password**—Specifies if the password is encrypted, and encrypted strings are used for the Enc-password. **NOTE:** The AdminMode items are on the right-click menu. **username**—Specifies the username; no minimum length; maximum length is 15 characters. **password**—Specifies the password; no minimum length; maximum length is 15 characters. **ShowAESButton**—If you set **ShowAESButton** to **Yes** and then enter the administrator mode, the **AES Encrypt** button populates in **System Admin**. To launch the encrypted generator to generate enc-password for INI settings, click **AES Encrypt**. Set **ShowAESButton=no**, to hide **AES Encrypt**. If Enc-Username and Enc-Password parameters are set, then the default value is **yes**. Otherwise, the default value is **no**.
BootOrder={PXE, HardDisk, USB}	**BootOrder** — Sets the boot order for the BIOS. The boot order must follow these rules: 1 The boot order is a list of these three options separated by a semi-colon (;) or a comma (,). 2 Every option must be used. 3 The options must be different. For example, the following settings are valid: `BootOrder=PXE;HardDisk;USB BootOrder=HardDisk;PXE;USB BootOrder=USB;PXE;HardDisk` However, the following settings are invalid:

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description

	`BootOrder=PXE;HardDisk BootOrder=PXE;PXE;USB`
	`BootOrder=PXE;HardDisk;USB;PXE`
	If the first boot order is not HardDisk, the system restart will boot from the BIOS setting.

BootpDisable={no, yes}	Default is **no**. **BootpDisable** — Yes/no option to disable BOOTP requests. ThinOS supports both DHCP and BOOTP to obtain the network configurations. In the first two attempts, only DHCP is requested. Then, both DHCP and BOOTP are requested. For some environments, BOOTP requests will delay obtaining the IP from the DHCP server. Set BootpDisable=yes will only perform a DHCP request. This setting is only valid after the next reboot.
CmosPassword=<password> [encrypt={no, yes}]	**CmosPassword** — Specifies the BIOS password on supported platforms; string up to 8 characters. **encrypt** — Default is **yes**. If encrypt=yes, an encrypted string is used as a password and the password is encoded by Dell Wyse encrypt tool.
CustomInfo={yes, no} [Custom1=custom1_str] [Custom2=custom2_str] [Custom3=custom3_str] [Location=location_str] [Contact=contact_str]	Yes/no option to configure or store custom information. If CustomInfo=yes, the custom information configured by the following options will be stored into NVRAM. If CustomInfo=no, the custom information in NVRAM will be cleared. For example: `CustomInfo=yes custom1=11 custom2=2 custom3=3 location=wyse contact=peter` **NOTE: Maximum length is 32 characters.**
**DeskColor="rrr ggg bbb"	Default is **"16 100 36"**; where DeskColor ="**16 100 36" (green)** is the default. Specifies the desktop background color in RGB string format that 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. **NOTE:** The MirrorFileServer parameter also supports the DeskColor parameter.
Desktop=bitmap file [Layout={tile, center, stretch}] [IconTextColor="rrr ggg bbb"]	**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 **Wyse wallpaper.** To disable the parameter, leave value blank (Desktop=wysedefault). When bitmap file is set in wnos.ini, at next restart, the thin client does not show Dell default wallpaper until INI wallpaper is loaded. To recover the Dell default wallpaper, set Desktop=DELLDEFAULT in wnos.ini or do a factory reset. When the parameter is set to Desktop=WYSEDEFAULT, the old Dell logo wallpapers that was used in versions earlier than ThinOS build 8.5.0 are loaded. When the parameter is set to **Desktop="'**, the wallpaper is disabled.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	Layout — This parameter specifies the arrangement on the desktop background of the bitmap file specified by the Desktop parameter. If auto dial-up is set, the Layout parameter becomes invalid. The default value is **stretch**. 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:** The MirrorFileServer parameter also supports the DeskColor parameter. **IconTextColor** — Specifies the icon text color in RGB string format that must be enclosed in quotes, where rrr, ggg and bbb are decimal numbers in the range of 0 to 255.
Device=DellCmos [CurrentPassword=password] [CurrentPasswordEnc=password encrypted] [NewPassword=password] [NewPasswordEnc=password encrypted] [Audio={yes, no}] [AdminLock={yes, no}] [AutoPower={Disable, Daily, Workday, Days}] [AutoPowerTime=hh:mm] [AutoPowerDays={Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}] [ACRecovery={PowerOff, PowerOn, LastState}] [USBRearPort={yes, no}] [USBFrontPort={yes, no}] [WakeOnLan={Disable, LAN, PXE}] [WakeOnUSB={yes, no}] [USBBootSupport={yes, no}] [PXEBootSupport={yes, no}] Action={extract, restore}	These INI parameters are applicable to thin clients with Dell standard BIOS. Supported platforms: · Wyse 3040 thin client with ThinOS · Wyse 3040 thin client with PCoIP **NOTE: All DellCmos settings, except CurrentPassword and CurrentPasswordEnc, take effect after power off restart.** **CurrentPassword**—This option provides the current BIOS password for changing BIOS settings when device's admin password is available. **CurrentPasswordEnc**—This option is used to provide encrypted current password. **NewPassword**—This option is used to change device's password. Current Password is not required if device's admin password is not available. **NewPasswordEnc**—This option is used to provide encrypted new password. **NOTE: Password encrypted is of higher priority. For example: If both CurrentPassword and CurrentPasswordEnc are configured, then CurrentPasswordEnc overwrites the CurrentPassword.** **Audio**— This option enables or disables the integrated audio controller. BIOS default value is **yes**. All Dell BIOS settings take effect after the power off restart. **AdminLock**—When enabled, this option prevents user from entering setup when an admin password is set. Default value is **no**. **AutoPower**—This option sets the time of day when you want the system to automatically turn on. No/Disable—The system does not automatically power up; Yes/Daily—The system power ups every day at the time specified in AutoPowerTime; Workday—The system power ups Monday through Friday at the time specified in AutoPowerTime ; Days—The system power ups on the days specified in AutoPowerDays; **AutoPowerTime**—This option specifies the auto power on time, value range of hh is 0 to 23, while mm is 0 to 59. **AutoPowerDays**— This option specifies the days to power up system automatically. For example,

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	Device=DellCmos AutoPower=Days AutoPowerTime=2:30 AutoPowerDays=Sunday; Friday; Saturday. **ACRecovery**— This option specifies how the system behaves when AC power is restored after an AC power outage. · PowerOff—System stays off after AC power is restored. · PowerOn—System powers on after AC power is restored. · LastState—System will keep the last power state as the last/previous state of the system was before AC power was removed. **USBRearPort**—If yes is specified, devices attached to the rear USB port are enabled, and available for Operating system. If no is specified, Operating System cannot detect any devices attached to the rear USB port. USB keyboard and mouse always work in the BIOS setup irrespective of this setting. **USBFrontPort**— If yes is specified, devices attached to the front USB port are enabled and available for Operating ystem. If no is specified, Operating System cannot detect any device attached to front USB port. USB keyboard and mouse always work in the BIOS setup irrespective of this setting. **WakeOnLAN**—This option allows the thin client to power up from the off state when triggered by special LAN signal.Wakeup from the standby state is unaffected by this setting and must be enabled in the operating system. This feature only works when the thin client is connected to AC power supply. · Disable— Do not allow the system to power on by special LAN signals when it receives a wak e up signal from the LAN or wireless LAN. · LAN—Allows the thin client to be powered on by special LAN signals. · PXE—A wake up packet sent to the system in either the S4 or S5 state causes the system to wa ke up, and immediately boot to PXE. · **WakeOnUSB**—WakeOnUSB allows the computer to power up from the off state when triggered by USB signal. Wakeup from the standby state is unaffected by this setting and must be enabled in the operating system. This feature only works when the computer is connected to AC. · If yes is specified, wake on USB is enabled. · If no is specified, wake on USB is disabled. **USBBootSupport**—If yes is specified, device allows operating system to boot from USB port. If no is specified, the operating system cannot boot device from USB port. **NOTE: USB, keyboard, and mouse always work regardless of being specified or not.** **PXEBootSupport**—If yes is specified, device allows operating system to boot from PXE. If no is specified, the operating system cannot boot device from PXE For extract action, CMOS content is saved to file $PF_cmos.$VER

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	$PF—name of Dell BIOS platform, including X10 and A10Q $VER—version of BIOS, like 1.2.2. With ThinOS log, CMOS, extract to **$PF_cmos.$VER** For restore action, CMOS content is updated from file **$PF_cmos.$VER** With a syslog, CMOS: restore from **$PF_cmos.$VER** The file is strongly checked and protected from corruption. The content is wrapped in a file header, including a field of magic number, checksum, timestamp, length and platform name. The content is first checksum and then AES encrypted during save operation. During restore operation, if the CMOS timestamp (stored in nvram) matches the timestamp on the file, the cmos content is not written every time to avoid wearing out the cmos chip. For usage of this feature, there should be a special INI user name like "cmos". The associated ini/cmos.ini should include one line as "Device=DellCmos Action=extract" (Pleaset note: "Device=DellCmos Action=extract" is not suggested to be written in global INI file, like wnos.ini, and it will take no effect if it has been written in global INI file). And "CurrentPassword" is must be required if device's BIOS password is existed regardless extract or restore action. e.g: Device=DellCmos CurrentPassword= xxxxx Action=restore After the administrator configured the CMOS on a template unit, the administrator should sign on to "cmos" account on WTOS to get the CMOS content saved to the cmos file on writable File Server wnos directory. Then, the wnos.ini should be configured with "Device=DellCmos action=restore", so all target units will get updated with the same CMOS setting as template unit after reboot. Once the restore action is finished, both the "Device=DellCmos Action=extract" and "Device=DellCmos action=restore" must be removed from the related INI files. The usage of other settings is self-explanatory. The only condition to use the setting is the BIOS GUI has such settings.
DEVICE=UsbTrace vid_pid={device vid/pin hex format} [max_len=500]	Specify the WTOS to trace USB device data to ftp or USB disk. For "vid_pid", device Vendor ID and Product ID hex value, and VID is high 16 bit while Product ID is low 16 bit. Allows to trace maximum of eight devices at one time. For "max_len", set a max len for capturing each USB transfer data. Default value is **128**. After you set this, you need to set option in Trouble shooting to start tracing the USB device data.
FactoryDefault={no, yes}	Default is **no**. Yes/no option to reset the system settings to factory default. This parameter, when set to yes, is only initialized once for each firmware change; however, you can set to no and then reboot so the option will be initialized again.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	NOTE: If the FactoryDefault parameter value is changed to yes, the thin client will reboot without notice to the user.
*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.
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}] [Win+L={no,yes}] [Alt+Tab={yes,no}]	**KeySequence** — Yes/no option to enable the following supported combined keys options. KeySequence=yes enables all of these options, each having a default of yes or no as noted that you can change individually to the setting desired. KeySequence=no disables all of these options regardless of the individual settings. **Ctrl+Alt+Del** — Default is **no**. Yes/no option to enable Ctrl+Alt+Del to lock the thin client if the user is logged in with a password. If the user is logged in without a password, this key sequence does not work. **Ctrl+Alt+Up** — Default is **yes**. Yes/no option to enable Ctrl+Alt+Up to toggle a session between fullscreen and window mode. **Ctrl+Alt+Down** — Default is **yes**. Yes/no option to enable Ctrl+Alt+Down to toggle between task selections. **Ctrl+Alt+Left** — Default is **yes**. Yes/no option to enable Ctrl+Alt+Left Arrow to lock the thin client if the user is logged in with a password. If the user is logged in without a password, this key sequence does not work. **Ctrl+Alt+Right** — Default is **yes**. Yes/no option to enable Ctrl+Alt+Right Arrow to lock the thin client if the user is logged in with a password. If the user is logged in without a password, this key sequence does not work. **Win+L** — Default is **no**. Yes/no option to enable use of Win+L key to lock the client. **Alt+Tab** — Default is **yes**. This option is used for task selection.
**Language=code [ManualOverride={yes,no}] [Charset={ISO-8859-1, ISO-8859-2, ISO-8859-5, ISO-8859-7}] [ImageSuffix={us, fr, de, gb, b5, jp, ko, la, default]	**Language** — Specifies the keyboard language to use. Once specified 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 below. **ManualOverride**— If you set ManualOverride=yes, all the parameters are only valid in factory default. It is helpful to configure keyboard setting manually in case of multiple nationalities within a company. This option must be following Language=code statement. **Charset** — Specifies which ISO option to use: ISO-8859-1— This is **Default**. 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.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	Keyboard Language List — Description and Code Arabic (Saudi Arabia) — Ar_sau Arabic (Iraq) — Ar_ira Arabic (Egypt) — Ar_egy Arabic (Libya) — Ar_lib Arabic (Algeria) — Ar_alg Arabic (Morocco) — Ar_mor Arabic (Tunisia) — Ar_tun Arabic (Oman) — Ar_oma Arabic (Yemen) — Ar_yem Arabic (Syria) — Ar_syr Arabic (Jordan) — Ar_jor Arabic (Lebanon) — Ar_leb Arabic (Kuwait) — Ar_kuw Arabic (U.A.E.) — Ar_uae Arabic (Bahrain) — Ar_bah Arabic (Qatar) — Ar_qat Brazilian — Br Canadian Multilingual — ca_ml Chinese (Simplified) — Gb Chinese (Traditional) — b5 Croatian — Croat Czech — Cz Czech (Qwerty) — Cz_q Danish — Dk Dutch — Nl Dutch (Belgian) — Nl_be Dutch (Belgian Comma) — Nl_be_c English (3270 Australian) — au3270 English (Australian) — Au English (New Zealand) — Nz

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	English (United Kingdom) — Uk **English (United States) (default) — Us** Estonian (Estonia) — Et_ee Finnish — Fi French (Belgian) — fr_be French (Belgian Comma) — fr_be_c 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 Icelandic — Is Italian — It Italian (Swiss) — it142 Latvian (Latvia) — lv_lv Latvian (Qwerty) — lv_lv_q Lithuanian (Standard) — lt_lt Lithuanian (IBM) — lt_lt_i Lithuanian (MS) — lt_lt_m Japanese — Jp Japanese_109a — Jp_109a Korean — Ko Korean (MS-IME2002) — ko_ime Norwegian — No Polish (214) — Pl Polish Programmers — pl_prog Portuguese — Pt Portuguese (Brazil) — Pt2

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	Romanian — Ro Russian — Ru Slovakian — Slovak Slovakian (Qwerty) — sk_q Slovenian — Sloven Spanish — Es Spanish (Mexican) English — La(us) Spanish (Mexican) Localized — La Swedish — Se Turkish — Turk Turkish (QWERTY) — turk_q U.S. International — us_int **NOTE:** Japanese refers to Japanese Input system (MS-IME2000), not JP. Russian keyboard is supported for server input; it is not supported to input locally. **ImageSuffix** — Localization builds have different suffixes according to the keyboard language as follows: jp (Japanese) gb (Simplified Chinese) b5 (Traditional Chinese) ko (Korean) la (Spanish Mexican) By default, with the above keyboard languages, the system will update the standard image according to the suffixes with the language code. With other keyboard languages, the system will update the standard image without the suffix specified. For example, if you set Language=jp, the system will update the image named C10_wnos.jp which is the Japanese localization build. If you set Language=us, the system will update the image named C10_wnos. The option ImageSuffix can specify the suffix of the image name when you do not want the default behavior.
Locale=<value> [load={yes | no}]	**Locale** — Specifies the system language. Locale changes the language for the user logon-experience screens only displayed during boot-up and logon and not the configuration or administrator screens. Values include: English, us, French, fr, German, de, Chinese Simplified, gb, Chinese Traditional, b5, Japanese, jp, Korean, ko, Latin, la. load=yes/no specifies whether or not to load the language file. The language file must end with the locale name and be placed under the folder wnos/locale in the file server.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	NOTE: For example, if you want to specify French and load the localized messages, you must place a file named French.msg under the folder wnos/locale in the file server, and then add Locale=French load=yes in the INI file. You can use Local=fr instead of Locale=French. **NOTE:** For Chinese Simplified, Chinese Traditional, Japanese, and Korean localization, a font file must also be placed under the folder wnos/font in the file server. For example, if you want to specify the system language to be Japanese, you must place a file named Japanese.msg under the folder wnos/locale in the file server, place a file named Japanese.fnt under the folder wnos/font in the file server, and then add Locale=Japanese load=yes in the INI file. If you are under a Wyse maintenance contract, you can download .fnt and .msg files from your My Downloads page in the Self-Service Center. If you are not under maintenance and wish to gain access to these files, you must complete a product registration.
LocaleList=<value>	**LocaleList** — Specifies a list of locale, so that a user can switch the system language as needed. Values include: English, us, French, fr, German, de, Chinese Simplified, gb, Chinese Traditional, b5, Japanese, jp, Korean, ko, Latin, la. All the values will be displayed in the GUI. To view the GUI, click **System Preference** > **General** > **Locale**. Be sure to place the necessary files, for example German.msg, Japanese.msg, Japanese.fnt, and so on under the correct folders as described in the Locale parameter description.
**Password=<sign-on password> [encrypt={no, yes}]	Specifies the password as the sign-on password; no minimum length; maximum length is 64 characters. **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-on dialog box. **encrypt** — Default is **no**. 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 ecrypted string instead of cleartext . For example: `Password=wyseatc@123` or `Password=NCAONIBINMANMLCOLKCNLL \ encrypt=yes`
** PRIVILEGE=[None, Low, High] [LockDown= {no, yes}] [HideSysInfo={no, yes}] [HidePPP={no, yes}]	Default is **high**. Privilege controls operator privileges and access to thin client resources. See also CCMEnable={yes, no}. None — This level of access is typical for kiosk or other restricted-use deployment. The System Setup selection on the desktop menu is disabled and the Setup submenu is not displayed. The Connect Manager is disabled by default.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
[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}] [EnablePrinterSettings={no, yes}] [CoreDump={ide, disabled] [EnableNetworkSetup={yes, no}] [DisableNetworkOptions={yes, no}] [EnableSystemPreferences={yes, no, TerminalNameOnly}] [DisableTerminalName={yes, no}] [DisableSerial={yes, no}] [DisableRotate={yes, no}] [DisableChangeDateTime={yes, no}] [EnableVPNManager={yes, no}] [TrapReboot={yes, no}] [EnableCancel={yes, no}] [EnablePeripherals={keyboard, mouse, audio, serial, camera, touchscreen, bluetooth}] [FastDHCP={yes,no}] TCPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF] UDPTosDscp=[Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF] [HideWlanScan={yes,**no**}]	The Connect Manager can be enabled 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 and 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** — Default is**no**. 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. **NOTE:** If the thin client is set to LockDown without a High privilege level, it will disable the G key reset on power-up. 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. **HideSysInfo** — Default is **no**. Yes/no option to hide the System Information from view. **HidePPP** — Default is **no**. Yes/no option to hide the Dialup Manager, PPPoE Manager, and PPTP Manager from view. **HidePN** — Default is **no**. Yes/no option to hide the PNAgent or PNLite icon from view on the taskbar. **HideConnectionManager** — Default is **no**. 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 by using HideConnectionManager=no; however, the user cannot create a new connection or edit an existing connection. **EnableNetworkTest** — Default is **no**. Yes/no option to enable the Network Test.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	EnableTrace — Default is **no**. Yes/no option to enable trace functionality. The active items are added to the desktop right-click menu in Privilege=Highlevel. **ShowDisplaySettings** — Default is **no**. 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** — Default is **no**. 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** — Default is **no**. Yes/no/auto option to hide the taskbar. If set to auto the taskbar will automatically hide/display the taskbar. 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. **EnablePrinterSettings** — Default is**no**. Yes/no option to enable printer configurations when a user Privilege=None. **CoreDump** — The option CoreDump=disabled will disable the core dump function. **EnableNetworkSetup** — This option is used to enable and disable the network setup. **DisableNetworkOptions** — This option is used to enable and disable the network options. **EnableSystemPreferences** —If the optional parameter, EnableSystemPreferences=TerminalNameOnly is set with Privilege=none, then the System Preferences menu is enabled, and only Terminal Name field can be accessed. **DisableTerminalName**— This option is used to enable and disable the terminal name. **DisableSerial** — This option is used to enable and disable the serial table in peripherals. **DisableRotate** — If the optional DisableRotate=yes is set, the rotate setting in the display setup will be disabled. This is only valid for C class clients because the rotation performance in C class may not be desirable. **NOTE:** If the optional EnableNetworkSetup=yes is set with Privilege={none, low}, the network setup will be enabled. If the optional DisableNetworkOptions=yes is set at the same time, the Options table will be disabled. If the optional EnableSystemPreferences=yes is set with Privilege={none, low}, the system preferences setup will be enabled. If the optional DisableTerminalName=yes is set at the same time, the terminal name field will be disabled. If the optional DisableSerial=yes is set with Privilege={none, low}, the serial table in peripherals setup will be enabled. **DisableChangeDateTime**— If the optional DisableChangeDateTime is set, the function of changing date and time locally will be disabled. For example, if you right-click the time label in taskbar, nothing is displayed. The **Change Date and Time** button in System Preference will be invisible.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	EnableVPNManager—If the optional EnableVPNManager=yes is set with Privilege={none, low}, the VPN Manager setup is enabled. **TrapReboot**— If the optional TrapReboot=yes is set, client reboots after the execution of the trap. **EnableCancel**— If the optional EnableCancel=yes is set with Privilege={none, low}, the counter down window for reboot or shutdown can be cancelled. The default value is no. For example, set the following ini, Inactive=1 AutoSignoff=yes Shutdown=yes ShutdownCounter=30 Privilege=none EnableCancel=yes. After no mouse and keyboard input in 1 minute, the system will pop up a counter down window to shut down in 30 seconds. You can cancel it. **EnablePeripherals**—If the optional EnablePeripherals is set with Privilege=none, the specified peripherals tab will be enabled. The value of the option can be a list of any valid value separated with "," or ";". For Camera, Touchscreen and Bluetooth, they can be enabled only, if the devices are available. For example, Privilege=none lockdown=yes EnablePeripherals=mouse,audio,camera,bluetooth, then mouse and audio tab will be enabled. If there are camera and/or bluetooth devices, the camera and/or bluetooth tab will be enabled too. The optional EnableKeyboardMouseSettings=yes can be replaced as: Privilege=none lockdown=yes EnablePeripherals=keyboard,mouse. **FastDHCP**— FastDHCP identifies the gateway first. If the gateway is same as the network before disconnection and the previous DHCP information is valid, the same information is used. The default value is yes. **TCPTosDscp**—Use this option to set the TOS field of all TCP packets when the fields are not pre-configured by other INI settings. **UDPTosDscp**—Use this option to set the TOS field of all UDP packets when the fields are not pre-configured by other INI settings.Added new sheet TOS_Priority_settings for TosDSCP INI, which is merged from TOS_Priority_settings.docx. **HideWlanScan**—Use this option to disable WIFI scan in lockdown mode. The default value is no.
ResourceURL={yes, no} [Type={Picture, Firmware, Package}] [URL=_url_path_] [User=_user_name] [Password=_password_] [Encrypt={yes, no}]	The resource files have their specified default path in file server, for example, the pictures for Showing Picture screen saver are from the folder **/wnos/picture** in file server (default), and the bitmap are from **/wnos/bitmap**. **ResourceURL**—If this option is set to yes, the subsequent options are use to configure one or more resource URL. The system fetches the resource files from the new URL. If this option is set to no, all the subsequent options are to be ignored. **Type**—This option specifies the resource type. Currently, only Picture is supported, which is for showing picture screen saver.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description

	Type=Picture—This option specifies the URL of pictures for **Showing Picture** screen saver.
	
	Type=Firmware—This option specifies the URL for ThinOS image, BIOS image, hosts, printermap and noticefile.
	
	Type=Package—This option specifies the URL for packages.
	
	Example:
	
	`ResourceUrl=yes \`
	
	`type=picture url=ftp://10.xxx.xxx.xx/pic1 user=pteng password=xxxxxx`
	
	`encrypt=no \`
	
	`type=firmware url=http://10.xxx.xxx.x/wnos1 user=administrator`
	
	`password=XXXXXX encrypt=yes \`
	
	`type=package url=https://10.xxx.xxx.xxx/wnos/pkg2 user=abc`
	
	`password=yyyy`
	URL—This option specifies a new URL of the resources.
	
	User and **Password**—These options specify the credentials of the new resource URL.
	
	Encrypt—This option specifies whether or not the password is encrypted. For example, ResourceUrl=yes type=picture url=ftp://10.xxx.xxx.xx/pic1 user=pteng password=xxxxxx encrypt=no

**ScreenSaver=value{0, 1, 3, 5, 10, 15, 30} [LockTerminal={0, 1, 2, 3}] [Type={0, 1, 2, 3, 4}] [VideoLink=httplink] [VideoSpan=no] [Unit=hour] [Image=imagefile] [PictureTimer={2-60}] [PictureOrder=random] [PictureCheck=always] [PictureLayout={stretch, tile, center}] [Sleep={0-180}]	**Screensaver**— Specifies to put the thin client in a screensaver state when the time limit for inactivity is reached, that is delay before starting is reached. Default value is **10**. Value and delay before starting the screensaver: 0 — Disabled 1 — 1 Minute 3- 3 Minutes 5 — 5 Minutes 10 — 10 Minutes 15 — 15 Minutes 30 — 30 Minutes The default screen saver value is 10 minutes and the maximum value is 180 minutes. If the value is not specified in the table, it is added to the drop down list in the GUI. **LockTerminal**— This is an optional parameter and specifies to put the thin client in LOCK state when the screen saver is activated. Default is **0**. **0** — Disabled.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	1 — Puts the thin client in a LOCK state when the screen saver is activated. The wallpaper is shown and the user is prompted with an unlock dialog box to enter the sign-on 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 wall paper cannot be viewed when the user is prompted with an unlock dialog box to enter the sign-on password to unlock the thin client. **3**— Puts the thin client in a LOCK state when the screen saver is activated, and the username and password are needed to unlock the terminal. The wallpaper is not shown and the Password field in the Unlocking window is invisible until you have entered the username. When you click **OK** or press the Return key, a message box pops up to input the username and password to unlock the terminal. **NOTE:** The user must be signed on with a password for a Lock action to take effect. If set in KeySequence, users can lock the thin client at any time by pressing Ctrl +Alt+Left arrow or Ctrl+Alt+Right arrow. **Unit** — This parameter converts the screen saver timer value from minutes to hours to set longer time. **Type** — Specifies which type of screensaver to use. 0 — Blank the Screen 1 — Flying Bubbles 2 — Moving Image 3 — Showing Pictures 4 — Playing Video If the value is set to **Type=None**, and the parameter **LockTerminal** is set to a non-zero value, the unlocking window is displayed when the screen saver times out. **VideoLink** — Specifies the video link address of the video file. Links with only http are supported. The mp4 video format is supported. **VideoSpan** — Specifies the video displayed mode in the screen. If the dual head is in span mode and VideoSpan=yes, it is spanned across all the screens. If VideoSpan=no, it is displayed in the main screen. **Imagefile** — This is an optional parameter and specifies an image file residing in the **bitmap** sub-folder under the home folder to be used as a **Moving Image** screensaver. If Type is set to 2 and no image file is present then the default Dell Wyse logo is used. If Type is set to 3, pictures residing in **picture** subfolder under the home folder are displayed. If **SelectGroup=yes**, then the pictures residing in the **picture** subfolder under the group folder are displayed. For example, `/wnos/ini/{group_dir}/picture` If group pictures do not exist, global pictures are used. Supported formats include JPG, GIF, PNG and BMP.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
	PictureTimer — Specifies the interval to wait in seconds to display another picture. Default value is **6 seconds**. **PictureOrder** — Specifies the order of picture files to display. **The default is to use the order of sort from A to Z**. If set to random, pictures are displayed randomly. **PictureCheck** — Specifies whether to check for picture files servers or not. **NOTE:** If set to always, the picture files in file servers are checked when the screen saver starts every time. By default, the system checks for picture files only when the screen saver starts for the first time to decrease network traffic. **PictureLayout**— The optional parameter is used to specify the arrangement on the desktop when pictures are displayed. For the tile selection, the image is replicated across the desktop. For the center selection, the image is placed at the center of the desktop without any image size change. For the stretch selection, the image is either expanded or shrinked to fill the desktop. The default value is stretch. **Sleep**—The optional parameter is used to specify the interval minutes to stop soft screen saver and turn off monitor. After the specified minutes, since software screen saver starts up, the software screen saver is stopped and turns off the monitor until screen saver is off. The value range is 0 to 180. The value 0 is default which disables this function.
**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. The default value is **10**, however, to commence shutdown immediately and prevent the display of the countdown dialog box, set the value to 0.
ShutdownInfo={no, yes}	Yes/no option to display various information such as System Version, Terminal Name, IP Address, and MAC Address in shutdown window.
S10WDMFlash=flash size	Specifies the flash size. This value will be saved into NVRAM and then eported to the WDM server. **NOTE:** This statement guarantees that all S10 thin clients function with DDC regardless of flash size.
TimeServer=server_list [TimeFormat={24-hour format, 12-hour format}] [DateFormat={yyyy/mm/dd, mm/dd/yyyy, dd/mm/yyyy}] [GetBiosDT={no, yes}]	**TimeServer** — Specifies the SNTP time servers to use for time retrieval. If a time server is not defined, the client CMOS/ BIOS internal clock will be used as a reference. **TimeFormat** — Default is **24-hour format**. Specifies the time format to use. **DateFormat** — Default is **yyyy/mm/dd**. 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** — Default is **no**. Yes/no option to obtain time from BIOS/CMOS when the timeserver is not available or cannot be contacted.

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description

	For Example:
	`TimeServer=time.nist.com\TimeFormat=24-hour formatDateFormat=mm/dd/yyyy`
	or
	`TimeServer=time.nist.gov\ TimeFormat=24-hour format\ DateFormat=mm/dd/yyyy`

WakeOnLAN={yes, no}	Default is **yes**. Wake-on-LAN allows a thin client to be turned on or woken up by a network message. If WakeOnLAN=yes, ThinOS will respond for the Wake-On-LAN packet for a remote wake up. If WakeOnLAN=no, ThinOS will not respond for the Wake-On-LAN packet. **NOTE:** To use the WakeOnLAN parameter with a C10LE, the C10LE must use BIOS version 1.0B_SPC001 or later.

Peripheral settings for wnos.ini files, {username} INI, and $MAC INI files

The following table contains the parameters used for configuring peripheral settings such as keyboard, monitor, mouse, printers and bluetooth devices. The underlined values are default values.

Table 9. Peripheral Settings for wnos.ini Files, {username} INI, and $MAC INI files

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	Description
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.**
Device=audio volume={low, middle, high} or {0 to 25} mute={0, 1, 2, 3} [mic_vol={high, middle, low} or {0-25}] [mic_mute={yes, no}] [mic_boost={yes, no, 1, 2, 3, 4}] [min_cache={1-50}] [EnableSpeaker={yes, no}][	Specifies the local thin client audio volume. **volume** — Default is **middle**. Specifies the volume level. high — maximum volume middle — medium volume low — minimum volume Values of 0-25 provide more exact volume level **mute** — Default is **0**. Option to enable/disable mute. 0 — no mute

[playback={device name string}] [record={device name string}] [mic_gain_device={device name string}] [mic_gain={1~8}] [DPaudio=yes,no] [local_button=yes, no] [jack_popup=[yes, no]	1 — mutes audio 2 — mutes audio and system beep 3 — mutes system beep **mic_vol** — Default is **medium**. Option to set volume levels to high, middle or low. high — maximum volume middle — medium volume low — minimum volume Values of 0-25 provide more exact volume level. **mic_mute** — Default is **no**. no — no mute yes — mutes audio **mic_ boost** — This option increases the mic decibels. **min_cache** — Default is **1**. This option is for configuring ThinOS audio playback minimum buffering amount in ten millisecond units. This can be used when network bandwidth is not large enough to play audio smoothly. In such cases, set min_cache higher, so that ThinOS will buffer more audio data before playing the audio. 1 – ThinOS will buffer at least 10 ms of audio data when playing audio. 50 – ThinOS will buffer at least 500 ms (0.5s) of audio data when playing audio. **EnableSpeaker** — Default is **yes**. Yes/no option to enable the internal loud speaker. **playback** — You can set a playback device name. **record** — You can set the record device name. **mic_gain_device**— Specify the device name on which you want the mic gain. **mic_gain**—Enhances the mic gain by number of times the specified value. The default value is 1. **DPaudio=[yes, no]**— The default option is DPaudio=yes. DP audio may impact display on A10Q with certain screen resolutions such as 1920x1200, 2048x1152, 2048x1280, 2560x1080, 2560x1440 (U2718Q, UP3216Q) however not limited. User needs to disable DP audio using INI or GUI. This setting only works for terminals with DP audio support (A10Q, D10Q, and U10). **local_button=[yes, no]** The default option is yes, if the value is no, the mute/volume up/volume down buttons are disabled in ThinOS local, but it works during session

	jack_popup— The default option of jack_popup is **yes**. If the jack_popup is set to **no**, jack selection message display is disabled when the jack headset is plugged in.
Device=bluetooth [Disable={yes, no}]	Set the parameter to disable bluetooth devices. The default value is no. The value is stored into NVRAM. If you set Disable=yes, the bluetooth devices are not initialized.
Device=MIC [Disable={yes, no}]	Device=MIC—This option enables or disables microphone devices. The default value is no and the value is stored in NVRAM. If the value is set to Disable=yes, the microphone devices are not registered to the system.
Device=camera [format=raw] [width={camera supported width}] [height={camera supported height}] [fps={camera supported fps}] [samplerate={0, 1, 2, 3, 4, 5}] [optimize={no, yes}] [Disable={yes, no}]	Specify the ThinOS local camera settings. **format** — Support only for raw video type; format=raw is fixed. **width** — The width of the resolution that the local camera supports. **height** — The height of the resolution that the local camera supports. **fps** — The frame per second (fps) of the resolution that the local camera supports. **samplerate** — The software level sample rate based on fps to optimize the performance, where the frame per second for the camera is actually equal to the fps value multiplied by the samplerate value. Samplerate values mean the following sample rates: 0 — 1/1 1 — 1/2 2 — 1/3 3 — 1/4 4 — 1/5 5 — 1/6 **optimize** — Default is **no**. Yes/ no option to optimize the width, height, and fps at 320 x 240 at 10 fps. That is, if optimize=yes, then 320 x 240 at 10 fps will be used for the local camera settings regardless of the individual settings in width, height, and fps; as long as the camera supports the 320 x 240 at 10 fps. If optimize=yes and the camera does not support the 320 x 240 at 10 fps settings, an error will be present in the Event Log of ThinOS. If optimize=no then the individual settings in width, height, and fps will be used as long as the camera supports them. **Disable**— When you specify Disable=yes, the device is disabled. For example, the **Camera** tab in peripherals setting is disabled, the **Exclude video devices** option in Global Connection Settings is disabled. The device cannot be accessed at local and remote sessions.
**Device=keyboard	**Device** — Specifies the local keyboard.

[numlockoff={no, yes}] [repeatrate={0, 1, 2}] [repeatdelay={0, 1, 2, 3, 4, 5, 6, 7}]	**numlockoff** — Default is **no**. Yes/no option to turn off the NumLock of the keyboard. **repeatrate** — Default is **1**. Specifies the keyboard repeat rate. 0 — Slow 1 — Medium 2 — Fast **repeatdelay** — Default is **2**. Specifies the keyboard delay in seconds, before repeat. 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 are saved into NVRAM if EnableLocal is set to yes in the wnos.ini file.
Device=mouse [Speed=[1-9]] [Swap={yes, no}] [FlipFlopWheel={yes, no}] [Big={yes, no}]	Speed is used to configure the speed of the moving mouse. 1 is the slowest, 9 is the fastest. The default value is 6. This parameter is the replacement of MouseSpeed. If the option Swap is set to yes, the right button is set as the primary button. The default value is no. If the option FlipFlopWheel is set to yes the mouse scroll wheel is inverted. The default value is no. If the option Big is set to yes, the mouse pointer size is increased by two times. The default value is no. This is designed for Wyse 5070 thin client only.
Device=Rfideas [DisableBeep={yes, no}] [DisableKeystroke={yes, no}] [SetCardType={yes, no} Configuration1={*} Configuration2={*}] [DisableInitialization={yes, no}] [DisableLed={yes, no}	**Device=Rfideas** — Specifies the local Rfideas readers. **DisableBeep** — Default is **yes**. Option disables the beep sound when the card is read. **DisableKeyStroke** — Default is **yes**. Option disables the keyboard movements and key strokes. **SetCardType** — Default is **no**. Used only for pcProx Plug readers. · If set to yes, then the Configuration #1 initializes to HID Prox 608x compatibility and Configuration #2 initializes to RDR-758x Equivalent. · If set to no, then the card type remains unchanged.

	DisableInitialization — Default is **no**. Option disables configurations to the card reader. **DisableLed**—If set to yes, then LED is turned off. If set to no, then LED is controlled by Reader. The default value is not set.
Device=UsbSerial [start=com{1~4}] [com{1~4}=com{5~8}]	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 with the INI file `Device=UsbSerial Start=COM3`. 1 Without any ini setting: The COM number registered is related with USB port number. Since USB port number is hardware property, it is always mounted in the same order, and there is no relation with the plug sequence. 2 If `Device=UsbSerial start=COMx` is set, then rule 1 does not work, the COM number is set by "x", and "x" range is 1-4, since ThinOS only supports maximum of four COM. 3 If `COMx=COMy` is set, the range for x is 1 - 4, and the real name in ThinOS is considered. The range for "y" is 5 - 8, since ICA running on ThinOS only supports maximum of eight COM. **NOTE: The INI `[com{1~4}=com{5~8}]` is applicable for ICA connections only.**
**DisableMouse={no, yes} or MouseDisable={no, yes}	**DisableMouse** — Default is **no**. 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** — Default is **no**. Yes/no option to disabled mouse pointer so that it is shown on the screen. The pointer is enabled if any mouse activity occurs.
LpdSpool={0-50}	Specifies the size of spool to buffer all the data before sending them to the LPD printer. The range of value is 0 to 10, that is, 0 MB to 10 MB. If the specified value is above the range, then the value is set to 5. The range of value is extended to 50. In build 8.2_001 or later builds, the LPD data is spooled to a file in a ram disk instead of a buffer. So the value of the parameter will not be related to the spool size as before. If LpdSpool=0, the function is disabled, otherwise the function is enabled.
LPTPortBind={yes, no}	**LPTPortBind** — Default is **Yes**. Specifies the LPT bind to the USB Port Policy. If set to Yes, then the registered port follows the following binding policy: LPT1 from USB ports 1/3/5/7 and LPT2 from USB posts 2/4/6. If set to No, then the LPT port plugged in first is LPT1 followed by LPT2, and so on.
MicBoost={no, yes}	Default is **no**.

	Yes/no option to enable on-board microphone boost.
**MouseNewSpeed={1-9}	Default is **6**. Value specifies the mouse speed within a range of 1 through 9, where 1 is slowest and 9 is fastest. This parameter is the replacement of MouseSpeed from build 7.0.1_07.
**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 Dell Wyse ThinOS Administrator's Guide. The host and queue parameters define the IP address and queue name of the printer. **PrinterID** — Specifies the Windows printer driver name. **Enabled** — Default is **yes**. Yes/no option to enable the network (LPD) printer.
Printer={COM1, COM2, LPT1, LPT2} [Name=<name>] [PrinterID=window_driver] [Class=classname] [Enabled={no, yes}] [EnableLPD={no, yes}]	Default is **COM1**. **Printer** — Specifies the local printer to configure. **Name** — Specifies the name of the printer. **This option must be used**. **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** — Default is **yes**. Yes/no option to enable the printer. **EnableLPD** — Default is **no**. Yes/no option to enable the LPD service. **NOTE: The parameters must be specified in the order shown.**
Printer={LPD1, LPD2, LPD3, LPD4, LPD5-LPD36} [LocalName=name] [Host= host] [Queue=queue] [PrinterID=window_driver] [Class=classname] [Enabled={no, yes}]	Default is **LPD1**. **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** — Default is **yes**. 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. For backward compatibility, LPD is accepted as LPD1. LPD2 – LPD4 are new in the 5.1. For WT1200 platform where Local flash is absent, locally configured LPD2-LPD4 and SMB1 to SMB4 disappear on power cycle.
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]	Default is **SMB1**. **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** — Default is **yes** . Yes/no option to enable the printer. **EnableLPD** — Default is **no**. 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.
**RepeatDelay={0, 1, 2, 3, 4, 5, 6, 7}	Default is **2**. 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}	Default is **1**. Specifies the keyboard repeat rate. 0 — Slow 1 — Medium 2 — Fast
*Resolution=[DDC, 640X480, 800X600, 1024X768, 1152X864, 1280X720, 1280X768, 1280X1024, 1360X768, 1366X768, 1368X768, 1400X1050, 1440X900, 1600X900, 1600X1200, 1680X1050, 1920X1080, 1920X1200] [Refresh=60, 75, 85} [rotate={right}]	Default is **DDC**. **Resolution** — Specifies the local display resolution. Option DDC can be specified to select default display resolution. **NOTE:** When using the Wyse Y Cable, DDC will properly work on both monitors by default. However, if connected to R10L/ R00x clients and you are using Dual DVI, then you must add the following DualHead INI parameter and DualHead option for DDC to properly work on both monitors: Parameter: DualHead=yes Option: ManualOverride=yes **Refresh** — Specifies the local display refresh rate. **NOTE:** If the Resolution or Refresh parameter values are changed, the thin client will reboot without notice to the user. **rotate** — Rotate allows you to rotate monitors for viewing in Portrait mode. For example: `screen=1 resolution=1280x1024 refresh=60 rotate=none` **NOTE:** Due to processing power requirements, rotate is not recommended and supported on the C class platforms at this time. **IMPORTANT:** The Screen parameter must be placed before the Resolution parameter. For example: `screen=1 resolution=1280x1024 refresh=60 rotate=none`
*Screen={1, 2}	Default is **1**. **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.

	NOTE: The Screen parameter must be placed before the Resolution parameter. For example: `screen=1 resolution=1280x1024 refresh=60 rotate=none`

Connection Settings for wnos.ini files, {username} INI, and $MAC INI files

The following table contains the parameters (and their options) used for configuring connection settings.

Table 10. Connection Settings: wnos.ini files, {username} INI, and $MAC INI files

Parameter * Global overrides identically-named user profile ** After sign off, user profile returns to global value	**Description**
**AltCacheDisable={no, yes}	Default is **no**. Yes/no option to disable the new cache mechanism allowing more memory to be available to a user. This is developed with Citrix Presentation Server 4.0 and Windows Server. If set to no, the new cache mechanism is enabled.
**Alternate={no, yes}	Default is **no**. 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.
AutoDetectNetwork={yes, no}	**RDP Only**. Default is **yes**. Yes/no option to enable RDP auto detect network feature. When this option is set to yes the **Optimize for low speed link** and the **Desktop Experience** options are disable by default.
**AutoSignoff={no, yes, 2-60} [Shutdown={no, yes}] [Reboot={no, yes}]	Default is **no**. **AutoSignoff** —This option can be used to automatically sign-off a user when the last opened session is closed. The default value is **no**. A value ranging from 2 to 60 can be configured. This value represents the number of seconds a session must be active prior to calling AutoSignOff. **Shutdown** — Default is **no**. Yes/no option to shut down the thin client. If shutdown is set to yes, the ShutdownCounter value is used to control the count-down before the system is turned off. **Reboot** — Default is **no**. 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}	Default is **no**.

	Yes/no option to clear the TSCAL license stored in the non-volatile memory. It can be replaced by FixLicense=clean.
Connect={ICA, RDP}	**Connect** — Connection protocol. Follow the ICA option list, see ICA Connect Options or RDP option list, see RDP Connect Options. Any options you use for your connection must be on the same logical line; ****can be used for line continuation, see Rules and Recommendations for Constructing the INI Files.
ConnectionBroker={default, Microsoft, Quest, VMware}	Default is **default**. Specifies the Connection Broker type. Select VMware to enable VDM XML support. If you enter VMware, the VMware logo appears on the login screen. For Dell vWorkspace broker, ConnectionBroker=Quest is recommended.
*Device=Ethernet [Speed={Auto, 10M HD, 10M FD, 100M HD, 100M FD, or 1000M} [MTU=mtu] [KeepAlive={1-600}] [Warning={no, yes}] [StaticIPWaitFileServer={0-255}] [WirelessWaitEnet={1-60}]	**Device** — Specifies to use an Ethernet. **Speed** — Default is **auto**. Specifies the ethernet speed to either Auto, 10 MHD, 10 M FD, 100 M HD, 100 M FD, or 1000 M. 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. **MTU** — A maximum transmission unit value between 500 to 1500. **KeepAlive** — Specifies a time value in seconds between 1 and 600 to keep an idle connection alive. **Warning** — Default is **no**. 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` **StaticIPWaitFileServer** — Default is **0**. Specifies the timeout threshold in seconds for cases of static IP. **NOTE: The default 0 turns off this parameter and allows the system to wait the system default 120 seconds.** If the Speed parameter value is changed, the thin client requires a reboot. **WirelessWaitEnet**—This option specifies the wait period before the wireless initializes in case of Enet Up. The default value is 5.
Device=mtouch [mult_touch={yes, no}] [mult_jitter={5-50}]	This parameter specifies the ThinOS multi-touch Monitor setting. For **mult-touch**, if the value is set as yes, multi-touch is supported. If the values is set as no, multi touch is not supported. The default value is yes. For **mult-jitter**, choose larger value if you prefer single click. Choose smaller value to have better user experience. The default value is 30.
Device=vusb	**Device** — Specifies the ID of a local USB device that is not redirected by default.

[ForceRedirect=DeviceID, fast]
 	
[ForceLocal=DeviceID]
 	
[Type={TCX, HDX}]
 	
[InterfaceRedirect={no, yes}]
 	
[TCXDVCdefault={yes, no}]
	ForceRedirect — Specifies a forced redirect of the local USB device to the server. This parameter has priority over ForceLocal. `Device=vusb ForceRedirect=0x07B4,0x0254,0x01,0x01,0x00,fast` .
	
	When the **ForceRedirect** option is used with **fast**, the **Reset device** command is not executed before the command **Redirect device to server**.
	
	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 TCX USB: Local Device (0x04f2,0x0112,0x03,0x01,0x01), set the parameter as:
	`Device=vusb ForceRedirect=0x04f2,0x0112,0x03,0x01,0x01`
	
	Type —**For Citrix Environments Only**. This option allows you to force the usage of HDX for USB virtualization. For example:
	`Device=vusb Type=HDX`
	
	NOTE: To use the TCX option, TCX Suite must be install on the target server.
	
	InterfaceRedirect — Default is **no**. Yes/no option to enable part of a composite device to run locally and part of the device to run on a remote session.
	
	TCXDVCdefault—Default is **no**. If the value is set to yes, the view RDP makes the first connection faster when the USB device is redirected.

Device=Wireless [Mode={Infrastructure, AdHoc}] [SSID=ssid Channel={1-14}] [WepKey={None, 1-4}] [Key1=k1] [Key2=k2] [Key3=k3] [Key4=k4] [Key1Enc=key1 encrypted] [Key2Enc=key2 encrypted] [Key3Enc=key3 encrypted] [Key4Enc=key4 encrypted] [RoamSensitive={high, medium, low}] [Algorithm={Open, SharedKey}] [DisableBand={None, 2.4G, 5G}] [PreferBand={None, 2.4G, 5G}]	**Device** — Defines the wireless Ethernet device remotely and saves to the local NVRAM. Not all options are needed. For example, you can define Key 1 to have a key of k1 and leave out Key 2 through Key 4. **NOTE: See also IEEE8021X={yes, no}.** **General example**: `device=wireless SSID=THINOS RoamSensitive=low` k1 to k4 are any real values of 5 to 13 characters or 10 to 26 Hex digits. Encrypted keys will overwrite unencrypted keys. Thus, if both Key1 and Key1 Encare are configured, then Key1Enc will overwrite Key1. **RoamSensitive** — Defines the sensitivity level of wireless roaming with respect to launching the Roaming daemon: high - signal lower than -60 dBm medium - signal lower than -70 dBm low - signal lower than -80dBm The RoamSensitive parameter is also used to enable wireless roaming. If it is not configured in the INI file, roaming will never be launched even if the signal is lower than -80dbm, unless it totally loses a wireless signal. **Algorithm** — Specifies the authentication method of WEP between ThinOS and the access point. If set to Open, open

[Priority=ssid_list] [DisableN={no, yes}] [DisableWlan={yes, no, EnetUp}] [RoamScanChannelTime={1-15}] [RoamScanChannelProbes={1-4}]	authentication will be selected. If set to ShareKey, shared key authentication will be selected. **DisableBand** — Default is **None**. Use to disable 2.4G or 5G 802.11 band. **PreferBand** —This parameter is used to set the priority of wireless connection band, and select the 2.4G or 5G access point to connect. Default is None. **Priority** — sets the priority of wireless profiles. The ssid list is separated by a semicolon or comma and the priority is from high to low. **DisableN** — Default is **no**. Yes/no option to disable 802.11n Wi-Fi wireless networking. **DisableWlan**— Used to disable the wireless connection. If DisableWlan=EnetUp, and the Ethernet is on while booting, the wireless connection is disabled. `Device=Wireless Mode=Infrastructure SSID=ThinIsIn IEEE8021X=yes network=wireless profile=ThinIsIn access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 Device=Wireless Mode=Infrastructure SSID=wtos_95 roamsensitive=high IEEE8021X=yes network=wireless profile=wtos_95 access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 Device=Wireless Mode=Infrastructure SSID=wtos_11n IEEE8021X=yes network=wireless profile=wtos_11n access=WPA2-PSK wpa2pskpwd=2wsx3edc Device=Wireless Priority="wtos_11n,wtos_95,ThinIsIn"` **RoamScanChannelTime** allows you to set the time the thinclient stays on one channel for scanning the surrounding aps. The default value is 2. The RoamScanChannelTime sets the time 10 times the provided value. The time ranges from 10ms to 150ms. For example, if you set RoamScanChannelTime=10, the thin client stays on one channel for 100ms. If you do not set the value or if the value is out of range, the thin client reverts to the default value 2. **RoamScanChannelProbes** allows you to set the number of probes the thin client sends out on a channel. The default value is 4. This value ranges from 1 to 4. If you do not set the value or if the value is out of range, the number of probe is reverted to the default value 4.
DISABLETSGW	**IMPORTANT: DISCONTINUED. DO NOT USE. See TSGWENABLE**
**EnableLocal={no, yes} [HideDefault={no, yes}]	Default is **no**.

	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. **NOTE: The global information includes: SEAMLESS, ALTERNATE, Reconnect, icaBrowsing, LowBand, NoReducer, Time settings, and Printer settings in a wnos.ini file.** **HideDefault** — Default is **no**. Yes/no option to hide the default ICA and RDP connections that are present on the devices.
ENABLETSGWSAMEINFO	**IMPORTANT: DISCONTINUED. DO NOT USE.**
*EthernetSpeed={Auto, 10M HD, 10M FD, 100M HD, 100M FD, 1000M}	Default is **auto**. **EthernetSpeed** — Specifies the Ethernet Speed to either Auto, 10M HD, 10M FD, 100M HD, or 100M FD. Once specified, it is saved in the non-volatile memory. This parameter can be replaced by the Device and Speed parameters. **NOTE:** If the EthernetSpeed parameter value is changed, the thin client will require a reboot.
Fastconnect={yes, no} [Key={F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Pause/Break}] [Ctrl={yes, no}] [Alt={yes, no}] [Connect={ICA, RDP, PCoIP}] [List={*|app1|server1;app2}] [Title={*_seamless_window_title*]	If you set the parameter to yes, press the special key to launch specified desktop or published application. If the desktop or published application is available, pressing the key brings it to the foreground. If you set to no, the followed options are ignored and disables fast connect functions. The followed options need to be configured to one or several fast connect setting. The option Key specifies the fast connect key. The option Ctrl specifies whether the Control key is combined or not, for fast connect key. The option Alt specifies whether the Alt key is combined or not, for fast connect. The option Connect specifies the protocol of fast connecting session. The option List specifies the connecting list of the desktop or published application. It supports wildcards * to match the session host/application or description. Also it supports a list separated by ; or ,. The option Title specifies the seamless window name. It supports wildcards * to match the window name. For a seamless window, it is needed because seamless windows share session. It uses List option to match session and uses the option Title to match the seamless window. For example, fastconnect=yes \ key=F1 ctrl=no alt=no connect=ica list="Excel 2013" title="*Excel*" \

	key=F2 ctrl=yes alt=no connect=ica list="XA76-2008R2*". When you press F1, the application Excel 2013 is launched. If there is a seamless window which matches the title *Excel* in this session, the seamless window is brought to the foreground, else it is launched. When you press Ctrl+F2, the desktop XA76-2008R2* is launched. If the desktop is available, it is brought to the foreground.
FastDisconnect={yes, **no**, Signoff} [CtrlKey={yes, **no**}] [AltKey={yes, **no**}] [PowerButton=signoff]	Default value is **no**. If the value is set to yes, pressing the **F12** (default) key or the key defined in FastDiconnectKey= statement will close the active window of the session. If the active window is a seamless window, the action will only close the window. If the window is not a seamless window, then the session will be disconnected. If the option Ctrl Key and/or Alt Key is set to yes, then the function key should be combined with **Ctrl** key and/or **Alt** key. For PCoIP session, press **Ctrl+Alt+F12** key combination to disconnect the session unless FastDisconnect=no is configured. This combined disconnect key is compatible with other platforms such as P25 and Linux. If the value is set to Signoff, pressing the **F12** (default) or the key defined in FastDisconnectKey= statement will disconnect all sessions and return to the signon window. If PowerButton is set to signoff, pressing the power button of the unit after you sign on will disconnect all sessions and return to the logon window. Otherwise, the unit will shutdown normally.
FastDisconnectKey={F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Pause\Break}	Specifies the disconnect key that will close the active window from the session.
FixLicense={Factory, clean, yes, no, OldFormat}	Default is **no**. 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.
HideIP={no, yes}	Default is **no**. 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.

Hosts=<hosts file name>	Specifies the file name of the hosts. This file is a simple text file that associates IP addresses with hostnames, one line per IP address. The length of the file name is limited to 63 characters. The file must be placed in file server and can be cached if set MirrorFileServer=yes in the wnos.ini. When resolving a host name, the system will initially look in the file and if not found, will search DNS, WINS, and so on. The following is an example of format in the hosts file: 10.151.122.1 gateway.ctx.com 10.151.122.123 myvm.ctx.com
icaBrowsing={udp, **http}	Default is **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 server(s) being accessed. This setting in a wnos.ini file will be saved into NVRAM, if EnableLocal=yes is set in the wnos.ini file.
IEEE8021X={yes, no} network={wired, wireless} [Profile=ssid] [access={WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT}] [eap={yes, no}] [servervalidate={yes, no}] [servercheck={yes, no}] [servername={"servername for EAP-TLS, EAP-PEAP, EAP-FAST"}] [eaptype={None, EAP-LEAP, EAP-TLS, EAP-PEAP, EAP-FAST}] [leapun={username for EAP-LEAP}] [leappwd={password for EAP-LEAP}] [leappwdEnc={password encrypted for EAP-LEAP}] [tlsauthtype={user, machine}] [tlsclntcert={client certificate filename for EAP-TLS}] [tlsclntprikey={filename of certificate with private key for EAP-TLS}] [tlsclntprikeypwd={password for private key}] [tlsclntprikeypwdEnc={password encrypted for private key}] [peapeap={EAP-MSCHAPV2, EAP-GTC}] [peapidentity={identity/username for PEAP}] [peapmschapun={username for EAP-PEAP/ EAP-MSCHAPV2}]	1 If IEEE8021X is set to no, then all parameters following it is ignored. 2 If network is not configured, the configuration is ignored. 3 The key left of equal is case sensitive, and the value right of equal case is not case sensitive except for credential information; for example username, password or certificate filename. 4 If two entries exist in an INI file, one each for wired and wireless, both will take effect; for example IEEE8021X=yes network=wired EAP=yes ... IEEE8021X=yes network=wireless access=WPA-ENT ... 5 All EAP credential information is stored whatever the eaptype setting. 6 The default values are underlined. 7 All passwords here should be encrypted. 8 The wildcard server include three entries in INI file. If both the servervalidate entry and servercheck entry are set to yes, the servername entry is valid. 9 Server certificate validation is mandatory in EAP-TLS authentication. If the eaptype entry is set to EAP-TLS, the servercheck entry must be set to yes. 10 Server list must be included in double quotation marks. For example IEEE8021X=yes Network=wireless access=WPA2-ENT eap=yes servervalidate=yes servercheck=yes servername=";test.com;wireless98; test.com" eaptype=eap-peap peapeap=eap-mschapv2 peapmschapun=administrator peapmschappwd=password . 11 Additional option timeoutretry specifies the retry times when 8021x authentication times out, which means that it is only validated when the optional network type is wired. For example, timeoutretry=3 allows you to retry thrice after 8021x authentication times out.

[peapmschappwd={password for EAP-PEAP/EAP-MSCHAPV2}] [peapmschappwdEnc={password encrypted for EAP-PEAP/EAP-MSCHAPV2}] [peapmschapdm={domain for EAP-PEAP/ EAP-MSCHAPV2}] [peapmschaphidedm={yes,no}] [peapsinglesignon={yes, no}] [peapgtcun={username for EAP-PEAP/ EAP-GTC}] [peapgtcpwd={password for EAP-PEAP/ EAP-GTC}] [peapgtcpwdEnc={password for encrypted for EAP-PEAP/EAP-GTC}] [wpapskpwd={passphrase for WPA-PSK}] [wpapskpwdEnc={passphrase encrypted for WPA-PSK}] [wpa2pskpwd={passphrase for WPA2-PSK}] [wpa2pskpwdEnc={passphrase encrypted for WPA2-PSK}] [encryption={TKIP|CCMP}] [fasteap={EAP-MSCHAPV2, EAP-GTC}] [fastidentity={Identity for EAP_FAST}] [fastmschapun={username for EAP-FAST/EAP-MSCHAPV2}] [fastpmschappwd={password for EAP-FAST/EAP-MSCHAPV2}] [fastmschappwdEnc={password encrypted for EAP-FAST/EAP-MSCHAPV2}] [fastmschapdm={domain for EAP-FAST/EAP-MSCHAPV2}] [fastmschaphidedm={yes,no}] [fastsinglesignon={yes, no}] [fastgtcun={username for EAP-FAST/EAP-GTC}] [fastgtcpwd={password for EAP-FAST/EAP-GTC}] [fastgtcpwdEnc={password for encrypted for EAP-FAST/EAP-GTC}] [wiredreset={yes, no}]	12 Additional option Profile specifies the type of ssid authentication to be configured. When we support multiple ssid wireless settings, the statement ieee8021x must be after the statement device=wireless, and one additional profile parameter is needed to identify the type of ssid authentication which is configured. For example, #ThinIsIn Device=Wireless Mode=Infrastructure SSID=ThinIsIn|IEEE8021X=yes network=wireless profile=ThinIsIn access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 peapmschapdm=wyse #wtos_95 Device=Wireless Mode=Infrastructure SSID=wtos_95|IEEE8021X=yes network=wireless profile=wtos_95 access=WPA2-ENT eap=yes eaptype=EAP-PEAP peapeap=EAP-MSCHAPV2 Example: IEEE8021X=yes network=wireless access=wpa-ent eap=yes eaptype=eap-tls tlsclntcert=user.cer tlsclntprikey=user.pfx tlsclntprikeypwd=12345678 OR IEEE8021X=yes network=wireless access=wpa-ent eap=yes eaptype=eap-tls tlsclntcert=user.cer tlsclntprikey=user.pfx tlsclntprikeypwd=12345678 leapun=user1 password=1234 peapmschapun=user1 peapmschappwd=12345 peapmschapdm=wyse.com IEEE8021X=yes network=wired eap=yes eaptype=eap-tls tlsclntcert=user.cer tlsclntprikey=user.pfx tlsclntprikeypwd=12345678 By default, peapidentity is same as peapmschapun.If peapmschaphidedm is set to yes, the domain will use saved peap MSCHAP domain name and the prompts dialog will not include the domain field when you perform ieee8021x authentication. The following example describes wildcard server validation: IEEE8021X=yes network=WIRED access=WPA2-ENT servervalidate=yes eap=yes eaptype=EAP-PEAP servercheck=yes servername=w2k8-ACS-64.sqawirelsess.com peapmschapdm=EAP-MSCHAPV2 peapgtcun=sqawirless2 peapmschappwd=123!@#qwe The username of ieee8021x (fastmschapun, peapmschapun, peapgtcun, leapun) can be configured as system variables like $mac, $sn etc. By default, fastidentity is same as fastmschapun. If fastmschaphidedm is set to yes, the domain uses saved EAP_FAST MSCHAP domain name, and the prompts dialog does not include the domain field when you perform ieee8021x authentication. The following example describes wildcard server validation:IEEE8021X=yes network=WIRED access=WPA2-ENT servervalidate=yes eap=yes eaptype=EAP-FAST servercheck=yes servername=w2k8-

	ACS-64.sqawirelsess.com fastmschapdm=EAP-MSCHAPV2 fastgtcun=sqawirless2 fastmschappwd=123!@#qwe **wiredreset** is used to reset MII when **authenticate cancel** occurs. This option is only for wired-network and is disabled by default.
**Inactive={0, to 480} (minutes) [NoSessionTimer=0-480]	Default is **0**. Specifies that if there is no keyboard or mouse use in the configured time in minutes, it will sign off or shutdown or reboot depending on AutoSignoff= ... If NoSessionTimer is set, then when there is an active sessions, use this timer to replace the Inactive value. The following controls whether to reboot or shutdown or sign off. `AutoSignoff=yes [Shutdown=yes] [Reboot=yes]`
IPProto=ICMP [DisableTStamp={yes, no}] [DisableEcho={yes, no}]	Configures the ICMP protocol. **DisableTStamp** — If DisableTStamp=yes, the system will not reflect the ICMP timestamp (13) request. **DisableEcho** — If DisableEcho=yes, the system will not reflect the ICMP echo (8) request. In this case, the unit cannot be pinged.
**LowBand={no, yes}	Default is **no**. Yes/no option to enable optimization for low speed connections, such as reducing audio quality or decreasing protocol-specific cache size or both. This setting in a wnos.ini file will be saved into NVRAM, if EnableLocal=yes is set in the wnos.ini file.
MMRCodecConfig=AUDIO [disableac3={no, yes}] [disablempeg={no, yes}] [disablewma1={no, yes}] [disablewma2={no, yes}] [disablewma3={no, yes}] [disablemp3={no, yes}] [disablepcm={no, yes}]	**MMRCodecConfig** — **Only for platforms with TCX Multimedia**. Specifies the audio to allow the disabling of the various codec options when playing audio. **disableac3** — Default is **no**. Yes/no option to disable the ac3 codec when playing audio. **disablempeg** — Default is **no**. Yes/no option to disable the mpeg codec when playing audio. **disablewma1** — Default is **no**. Yes/no option to disable the wma1 codec when playing audio. **disablewma2** — Default is **no**. Yes/no option to disable the wma2 codec when playing audio. **disablewma3** — Default is **no**. Yes/no option to disable the wma3 codec when playing audio. **disablemp3** — Default is **no**. Yes/no option to disable the mp3 codec when playing audio. **disablepcm** — Default is **no**. Yes/no option to disable the pcm codec when playing audio.
MMRCodecConfig=VIDEO [disablempeg1={no, yes}]	**MMRCodecConfig** — **Only for platforms with TCX Multimedia**. Specifies the video to allow the disabling of the various codec options when playing video.

[disablempeg2={no, yes}] [disablejpeg={no, yes}] [disablewmv1={no, yes}] [disablewmv2={no, yes}] [disablewmv3={no, yes}]	**disablempeg1** — Default is **no**. Yes/no option to disable the mpeg1 codec when playing video. **disablempeg2** — Default is **yes**. Yes/no option to disable the mpeg2 codec when playing video. **disablejpeg** — Default is **no**. Yes/no option to disable the jpeg codec when playing video. **disablewmv1** — Default is **no**. Yes/no option to disable the wmv1 codec when playing video. **disablewmv2** — Default is **no**. Yes/no option to disable the wmv2 codec when playing video. **disablewmv3** — Default is **no**. Yes/no option to disable the wmv3 codec when playing video.
**NoReducer={no, yes}	Default is **no** — Enables compression. Yes/no option to turn off 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 percent for text-based applications such as Microsoft Word and 40 percent less for graphics applications than the uncompressed data streams.
OneSignServer=onesign_server [DisableBeep={no, yes} [KioskMode={no, yes}] [EnableFUS={no, yes}] [TapToLock={0, 1, 2}] [EnableWindowAuthentication={yes,no}] [AutoAccess={VMW,XD,XA}] [NetBIOSDomainName={no, yes}] [ConnectTimeout={0 ~ 65535}]	Specifies a list of host names or IP addresses with optional TCP port number or URLs of Imprivata OneSign servers. **IMPORTANT: An https protocol must be used.** OneSign virtual desktop access offers a seamless authentication experience and can be combined with single sign-on for no click access to desktops and applications in a virtual desktop environment. The following inputs are acceptable values: https://ip or https://FQDN **DisableBeep** — Default is **no**. Yes/no option to set the Rfideas reader to mute when a card is tapped. **KisokMode** — Default is **no**. Yes/no option to allow the OneSign user to share the client desktop. **EnableFUS** — Default is **no**. Yes/no option to set the Citrix client to remain running when switch users. **TaptoLock** — Default is **2**. Only active when KioskMode=yes. Specifies tap to lock.

	If TapToLock=0, then tap a card to lock terminal is disabled. If TapToLock=1 (Tap to lock), then use the proximity card to lock the terminal. If TapToLock=2 (Tap over), then lock the terminal and log in a different user. **EnableWindowAuthentication** — Default is **yes**. Yes/no option to sign-on with the user's Windows credentials to pre-defined broker if the OneSign sign-on fails. **AutoAccess** — Specifies the corresponding type of broker to automatically start. If not defined, the broker type is obtained from the Imprivata Server setting of the computer and user policy. If none of them is defined, then the first available broker server from the Imprivata server is started. **NOTE:** AutoAccess can be set in [username].ini and wnos.ini, however, the wnos.ini, has priority over [username].ini. **NetBIOSDomainName** — Default is **no**. Yes/no option to enable the authentication to the broker server using the NetBIOS domain name. If set to yes, the Imprivata domain list will show NetBIOS domain name and the card user will authenticate to the broker server using the NetBIOS domain.
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={LDAP, RSA}] [CAGAuthMethod={LDAP, RSA, LDAP+RSA, RSA+LDAP}] [RequestIconDataCount={0-65535}] [DefaultSettings={XenApp, XenDesktop}] [SmartcardPassthrough={yes, no}] [StoreFront={no, yes}] [HttpUserAgent={UserAgent}] [CAGSendDomain= {yes, no}] [SFIconSortMode={0, 1, 2, 3}] [IgnoreDefaultGateway={yes, no}] [CAGUserAsUPN={yes, no}] [CAGExternal={yes, no}] [DisableSFInit={yes, no}]	**PnliteServer** — Specifies the list of IP addresses or host names with optional TCP port number or URLs of PNAgent/PNLite servers. The list is empty by default. Each entry with optional port is specified as Name-or-IP:port, where port is optional; if not specified, port 80 is used as the default. If a port other than 80 is used, the port number must be specified explicitly with the server location in the form IP:port or name:port. Once specified, it is saved in the non-volatile memory. The statement PNAgentServer and Web interface for Citrix MetaFrame Server is equal to this statement. **NOTE:** PnliteServer and the DomainList parameters can be used in a {username}.ini file, but generally are used only in a wnos.ini file. 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 the Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files 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 log in.

Default is **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.

Default is **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 started when using PNA to sign on. If AutoConnectList=*, then all the PNA applications will be automatically connected.

The autoconnectlist is the connection description of application or host name which can use the wildcard * to match the string.

IMPORTANT: Appname values are case sensitive.

Timeout — Specifies the time in seconds where a client will try to establish a connection before reporting that it is unreachable.

CAGRSAAuthMethod or **CAGAuthMethod** — CAGAuthMethod option is used for CAG authentication configuration.

NOTE: This option replaces CAGRSAAuthMethod. If CAGAuthMethod=RSA which is same as the prior CAGRSAAuthMethod=RSASecurid, an extra passcode field needs to be input except username/password/domain. If CAGAuthMethod=LDAP, no passcode field is needed.

- CAGAuthMethod={LDAP+RSA, RSA+LDAP} — Used for CAG authentication configuration.
- If CAGAuthMethod = LDAP+RSA, an extra passcode field needs to be input except username/password/domain. If the CAG server is configured for a double authentication policy, this ini corresponds to the first auth LDAP and second auth RSA.
- If CAGAuthMethod = RSA+LDAP, it has the same result with CAGAuthMethod = RSA, compared to LDAP+RSA. If CAG server configure double authentication policy, this ini correspond to First auth RSA and Second auth LDAP.

RequestIconDataCount — RequestIconDataCount is used for requesting 32-bit color icons. It is a counter which means that only the count of the icons will be requested. The default number is **10**.

For example, if set RequestIconDataCount=0, no icon data will be requested. If set RequestIconDataCount=5, only 5 icons are requested.

DefaultSettings — Specifies the default settings for XenApp or XenDesktop.

Xen App Default Settings:

1 SignOn=Yes

2 PnliteServer= RequestIconDataCount=20

3 desktopcolordepth=32

4 LongApplicationName=yes

5 sessionconfig=ica progressivedisplay=yes ondesktop=yes

6 device=audio volume=high

7 Seamless=yes FullscreenReserved=yes

8 sessionconfig=all mapdisks=yes

9 Enabled by default: Disks, Serials, Sound

10 Disabled by default: USB, Printers, Smart Cards

Xen Desktop Default Settings:

1 SignOn=Yes

2 sysmode=vdi toolbarclick=yes toolbardelay=3

3 sessionconfig=ica progressivedisplay=yes

4 PnliteServer=

5 AutoSignoff=yes

6 Enable by default: Printers, Serials, USB, Sound

7 Disabled by default: Disk, Smart Cards

SmartcardPassthrough — Default is **yes**. Yes/no option to enable/disable the smartcard pass through mode.

StoreFront — Default is **no**. Yes/no option to support Citrix StoreFront Authentication. The value will be saved into NVRAM.

HttpUserAgent—The option will replace the default "CitrixReceiver WTOS/1.0" during Netscaler login. If you are using "WTOS/1.0" as Netscaler Session Policy, set this INI parameter to retain your Netscaler policy configuration.

CAGSendDomain—This option sends domain as domain\user to external network Netscaler to support Netscaler and DUO passcode authentication. The default value is no.

SFIconSortMode sorts storefront dekstop icon. The default value is 0.

0— sorts by the position value from server side.

1—sorts in alphabetic order.

2—sorts in alphabetic order with desktop first.

3—sorts in alphabetic with application first.

IgnoreDefaultGateway—When the value is **Yes**, the default gateway of the selected store during Netscaler login is ignored. Always use pnliteserver to continue. When the value is set to **no**, the Netscaler server is used as default gateway to reset the login again. The default value is **no**.

CAGUserAsUPN—This value allows the client to send username to server in the format username@fqdn, similar to an email address. Third party authentication for Netscaler uses this format. Example: Okta authentication.

CAGExternal—This value allows CAG login with external network mode directly without check beacons and reduces login time.

DisableSFInit—This value disables storefront initialization process when you turn on the thin client. This is because, the storefront

	initialization process takes time to start which is not required during logon.
RTPTosDscp={Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF}	Sets RTP/UDP audio channel in the TOS fields.
SaveSysinfo={usb, _proto_, _full_url_} [ScardLog=0xF] [Username=_username_] [Password=_password_] [Size=_file_length_limit] [Append={yes, no}]	Configure the target clients to save the event logs. **full_url**—If set as a specified full url name, it is saved into the specified url. Otherwise, it is saved as a file name, such as **/wnos/troubleshoot/{TERMNAME}_LOG_{DATE}_{TIME}.txt**. **usb**—If set to usb, it is saved into the last mounted USB disk. **proto**—If set to a protocol, for example, ftp, http or https, it is saved into the file server with this protocol. **Scardlog**—The Smart card Log option is a bit mask to control the following logs: • 0x1 Context log • 0x2 Handle log • 0x4 Status log • 0x8 Transfer log **Username** and **Password**—The options specify the account of the file server or url. If not set, the default account of file server is used. **Size**—This option specifies the file size limitation. When the file is greater than the specified size, the file will be cleared. **Append**—This option appends the event log to the same file name instead of creating a new file. It is only valid for full url with ftp. The protocol http or https is also supported from 8.4.1 release. For example, `savesysinfo=http://10.151.121.3/wnos/yyy.txt username=administrator password=wyseatc append=yes Size=4000`. The event log file yyy.txt is appended in every boot-up. If the file size is up to 4000 bytes, then the file is cleared and continues to save the log.
**Seamless={no, yes} [HideTaskbar={0, 1, 2, 3}] [FullscreenReserved={no, yes}]	**Seamless** — Default is **no**. Yes/no option to set the default resolution for ICA published applications to Seamless for ICA connection parameters. **HideTaskbar** — Default is **0**. 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 excluding the FullscreenReserved parameter in a wnos.ini file will be saved into NVRAM if EnableLocal=yes is set in the wnos.ini file.

	NOTE: • 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.
SecureMatrixServer=<SecureMatrix Server Host name or IP address/FQDN or URL> [EnableSelectTable]	Specifies the Host name or IP address/FQDN or URL of the Secure Matrix server. Http or https protocol usage is decided by the server configuration. If SecureMatrixServer is defined, the user must pass authentication with the Secure Matrix server first, and then there is a seamless log in to the brokers if the server can provide the correct broker credentials, if not, the user must enter broker credentials to log in. For Example: SecureMatrixServer=https://gsb01.bjqa.com **NOTE:** Before using this parameter, use the Secure Matrix documentation to set up the Matrix Server. Also, be sure you import the relevant GSB Server Certificate file when using https. EnableSelectTable enables you to select the table type (3 or 4 tabs) when you change the password (SMXBridge server 3.9 start supports this feature). Default value is No.

SelectGroup={no, yes}
 	
[Default=default_desc]
 	
description=group1
 	
[groupname=name1]
 	
[description=group2]
 	
[groupname=name2]
	Default is **no**.
	
	SelectGroup — Yes/no option to allow a user to select from a group list on the Log on dialog box during a log in. If yes, the description will display in the group list box.
	
	groupname — The group name is used to identify the group including the directory and file name. If not defined, the description will become the group name.
	
	The Default option following "SelectGroup=yes" can specify the default group. The value is one of group description defined after that. After you select another group and sign off, this default group will be selected.
	
	If default option is not specified, the last selected group will be selected in the next sign on.
	
	For example:
	
	`SelectGroup=yes \`
	`default="Sus team" \`
	`description="Dev team" groupname=dev \`
	`description="Sus team" \`
	`description="SQA team" groupname=sqa \`
	`description="guest"`
	
	Group 1: Description="Dev team" groupname=dev

	The file \wnos\ini\dev\dev.ini must be created in the file server. In the dev.ini, the broker, domain list, or connections can be defined for the dev team. Group 2: .Description="Sus team" The file \wnos\ini\Sus team\Sus team.ini must be created in the file server. In the Sus team.ini, the broker, broker list, or connections can be defined for the Sus team. Group3...4...n...and so on. After a user selects a group, the system will load the group ini file first, and then load the \wnos\ini\{group_name}\username.ini. If the username.ini in the group directory is not found, it will attempt to load \wnos\ini\username.ini as before. Because the group list may define different brokers, the SelectServerList statement will be invalid if set SelectGroup=yes.
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** — Default is **COM1**. 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** — Default is **no**. Yes/no option to denote that a serial touch screen is attached. **Touch_XYReverse** — Default is **no**. Yes/no option to denote a reversal of the X and Y coordinates which are needed for some touch screens. **Touch_type** — Default is **elo**. Specifies the type of touchscreen being used. **NOTE: Options must be specified in the order shown. 9035366678**
SessionConfig=ALL [unmapprinters={no, yes}] [unmapserials={no, yes}] [smartcards={no, yes}] [mapdisks={no, yes}] [disablesound={no, yes, 2}] [unmapusb={no, yes}] [DisksReadOnly={no, yes}] [MouseQueueTimer={0–99}] [WyseVDA={no, yes}]	**SessionConfig** — Specifies the default settings of the optional connection parameters for all sessions. **unmapprinters** — Default is **no**. Yes/no option to un-map printers. **unmapserials** — Default is **no**. Yes/no option to un-map serials. **smartcards** — Default is **no**. Yes/no option to use smartcards. **mapdisks** — Default is **no**. Yes/no option to map disks. **disablesound** — Default is **no**. Yes/no option to disable sound. If value is set to 2, the sound at remote computer is disabled. **unmapusb** — Default is **no**. Yes/no option to un-map USBs. **DisksReadOnly** — Default is **no**. Yes/no option to mount mass storage disks as read-only.

[WyseVDA_PortRange=startPort, endPort] [UnmapClipboard={no, yes}] [DefaultColor={0,1,2}] [VUSB_DISKS={yes, no}] [VUSB_AUDIO={yes, no}] [VUSB_VIDEO={yes, no}] [VUSB_PRINTER={yes, no}] [FullScreen={no, yes}] [Resolution={default, vga_resolution}] [DisableResetVM={no, yes}] [WyseVDAServerPort=serverPort] [FontSmoothing={yes, no}] [AutoConnect={yes, no}] [MultiMonitor={yes, no}] [EnableImprivataVC={yes,no}] [Locale=LocaleID] [SessionLogoffTimeout=seconds] [GroupSession={yes,**no**}]	**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. **WyseVDA** — Default is **no**. Yes/no option to enable Virtual Desktop Accelerator for all ICA and RDP sessions. **WyseVDA_PortRange** — Sets the ThinOS VDA client port range. The port range must follow these rules: 1 The port range is a list of start port and end port separated by a semicolon (;) or a comma (,). 2 Both ports must be between 1 and 65535. 3 The end port must be greater than start port. For example, WyseVDA_PortRange=3000,3010, the start port is 3000, the end port is 3010. **UnmapClipboard** — Default is **no**. 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 parameter is set to yes in wnos.ini. **DefaultColor** — Specifies the default color depth to use for the session 0=256, 1=High color, 2=True Color. **VUSB_DISKS** — Default value is yes. **VUSB_AUDIO, VUSB_VIDEO, and VUSB_PRINTER** — The default value is **no**. The options specifies if these USB devices are redirected to the server using TCX Virtual USB or ICA or RDP USB redirection. In addition, by default, these devices are set as local devices. **NOTE: For example, if you want to use USB disks as a network disk, you can set SessionConfig=all mapdisks=yes VUSB_DISKS=no.** If you want to use USB disks as server side device, you can set SessionConfig=all mapdisks=no VUSB_DISKS=yes. The devices are displayed in device manager of the session. **FullScreen** — Default is **no**. Specifies the default screen mode. When using FullScreen in a Dual Screen mode, the session will be displayed in Span mode **Resolution** — Default is **default**. Specifies the session resolution. For example, 640 x 480 and other supported resolutions. Default will set the resolution to the native resolution of the monitor. Setting the resolution to a value smaller than the native resolution of the monitor, will allow the session in Windowed mode. The resolution value cannot be higher than the native resolution. **DisableResetVM** — Default is **no**. Set DisableResetVM=yes to disable Reset VM function. As default, this function is controlled by the server side is enabled including VMware View or Citrix PNA. **WyseVDAServerPort** — Sets Wyse VDA Server Port for a ThinOS VDA client. The default port is 3471. The port range must be from 1029 to 40000. For example, WyseVDAServerPort=3000, sets VDA server port to 3000 and the client will connect to the VDA server using this port. **FontSmoothing** — Default is **yes**. Set no to disable font smoothing.

	AutoConnect — Default is **yes**. Set no to disable auto connect function. **MultiMonitor** — Default is **yes**. Sets a multiple monitor layout. Set MultiMonitor=no to disable multiple monitor layout function. The session has the same desktop width and height with local virtual desktop size, spanning across multiple monitors, if necessary. **EnableImprivataVC**— Default is **yes**. If set to no, the Imprivata Virtual Channel is disabled. The user can use vusb redirect instead of Imprivata Virtual Channel mode to use the Rfideas or finger print device in session as server side remote device. **[Locale=LocaleID]**— Set Locale=LocaleID to set Locale in session for localization configuration to work. For information about LocaleID, refer to link msdn.microsoft.com/en-us/library/windows/desktop/dd318693(v=vs.85).aspx. **SessionLogoffTimeout**—Setting SessionLogoffTimeout value forces all sessions to logoff when user signs off from the broker. The default value is 0 which retains the same behavior as before, and also disconnects the sessions. If you set a value, for example 30 seconds, broker sign-off waits for 30 seconds for all sessions to finish logoff, then, automatically session logs off. Broker sign-off will continue. During the waiting process, one notice prompts for user to check whether the session stops working if something is not saved. This feature currently supports Citrix Xen broker sessions and View Broker sessions only. **GroupSession=yes**—Set to enable the function of grouping sessions and the menu item of Group Sessions is checked when you right click on the desktop. The default value is no and the original state of Group Sessions is unchecked.
SessionConfig=ICA [desktopmode={fullscreen, window}] [mapdisksunderz]: DISCONTINUED. DO NOT USE. [TosIpPrecedence={0–5}] [TosDscp={Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/EF}] [DiskMapTo=a character sequence] [SysMenu={remote, local}] [SessionReliability={no, yes}] [WarnPopup={yes, no}] [ondesktop={no, yes, all, none, desktops, applications, ondesktop_list}] [AudioQuality={default, high, medium, low}] [USBRedirection={TCX, ICA|HDX}] [ZLKeyboardMode={0, 1, 2}] [ZLMouseMode={0, 1, 2}] [SucConnTimeout=seconds]	**SessionConfig** — Specifies the ICA default settings of the optional connection parameters for all ICA sessions. **desktopmode** — Default is **fullscreen**. Specifies the display mode of an ICA published desktop when using an ICA PNAgent logon; the default is **fullscreen mode for a PNA desktop application**. **mapdisksunderz** — DISCONTINUED. DO NOT USE. **TosIpPrecedence** — Allows you to set IP Precedence in the TOS fields. **TosDscp** — Sets IP DSCP in the TOS fields. **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 ThinOS, it will be D:/), T is mapped to the second disk (in ThinOS, 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.

[HDXFlashUseFlashRemoting={Never,Always}] [HDXFlashEnableServerSideContentFetching={Disabled,Enabled}] [EnableRTME={Yes, No}] [FlipByTimer={0, 1}] [RefreshTimeOut={dd:hh:mm}] [Timeout={Yes, No}] [PasswordExpireNotify={yes, no}] [RefreshPopupNotice={yes, no}] [DisableReceiverLogo={Yes, No}] [MMRClientFetchDisabled={Yes, No}] [ClientName=_client_name_] [DisableMMRSeek ={yes, no}]	**SysMenu** — Default is **local**. 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** — Default is **no**. Yes/no option to enable session reliability. **WarnPopup**— If WarnPopup=no, the option can disable the warning message when session reliability happens in order to decrease the administrative support calls. **ondesktop**— This option specifies the connections that are displayed on the desktop. It enhances ondesktop options for SessionConfig=ICA so that the VDI brokers can work with ondesktop options too. • If AutoConnectList is set in the VDIServer statement, all connections configured in AutoConnectList parameter are displayed. • The connections show on desktop as default. • The connections can be controlled by using the values available. • The connection is added to the connection manage list even if the connection is not displayed on the desktop. all - show all, same as default none - don't show any desktops - only show desktops applications - only show applications The others will be handled as a ondesktop_list. For example, if set ondesktop="word; excel", only show the applications "word" and "excel". all—display all connections. none—no connections are displayed. desktops—display only the desktop connections. applications — display only applications, the connections are handled as an ondesktop_list. For example, if you set ondesktop=word; excel, then only the applications word and excel are displayed. The ondesktop_list also supports wildcard when the star * is used, similar to the AutoConnectList parameter in VDIServer. For example, if the value is set as **ondesktop=*IE***, any application which includes the string IE is displayed. **AudioQuality** — Default is **default**. Specifies the audio quality of ICA sessions. **NOTE: Medium quality is recommended for Speech scenarios. For example: SessionConfig=ICA AudioQuality=high** **USBRedirection** — Default is **ICA|HDX**. Option to select the channel of usb devices redirection. This option is recommended to replace the older setting device=vusb type={TCX, HDX}. **ZLKeyboardMode** — Specifies to accelerate the display of the input text on the client device over a high latency connection. 0=off, 1=on, 2=auto **ZLMouseMode** — Specifies to accelerate the visual feedback for mouse-clicks on the client device over a high latency connection. 0=off, 1=on, 2=auto **SucConnTimeout**— This option will enhance the seamless session share. During the first session logon, immediately start second or

	later sessions, which will wait for the time set with SucConnTimeout (or the logon success) to make sure new applications share with the first logon session. **HDXFlashUseFlashRemoting**— Default is **Always**, which means the HDX is enabled always. The value Never is to disable HDX. **HDXFlashEnableServerSideContentFetching**— Default is **Disabled**, which means the server side fetching content is not enabled. The value enabled is to enable this function. **EnableRTME**— This option controls the launch of RTME service. The default value is enabled. **FlipByTimer**— This option selects the screen refresh method. For some old server, there is no EndOfFrame transferred to the client. Then we can use this option to fix such issues. **RefreshTimeOut**—RefreshTimeOut triggers auto-refresh which updates ICA applications automatically. The value format dd:hh:mm, indicate days&&hours&&minutes as the auto-refresh interval. The default value is 0, that disables auto-refresh. **Timeout**– This option controls the credential prompt after ICA broker logon was timeout. Session ticket is invalid now. If yes, users have to enter their credential to re-login to launch session, if no, ThinOS will use the default credential to do login in background. The default is yes. **NOTE: Other Citrix INI parameters are not listed here. However, these Citrix INI parameters are supported on ICA connection by using INI `SessionConfig=ICA`.** **PasswordExpireNotify** —This option enables the password expire notification, which should configure in storefront server side, Authentication, password change set as At any time. Then before the password expires, logon prompts a message displaying the number of days after which the password will expire and let you change the password. The option WarnPopup=no can disable the warning message when session reliability happens to decrease the administrative support calls. **RefreshPopupNotice** — This option enables or disables the popup notice during refresh in progress. The default value is yes. **DisableReceiverLogo**—Hides the CitrixReceiver logo in left top corner in storefront style. The default value is No. **MMRClientFetchDisabled** — This option disables RAVE client content fetching. The default value is No. **ClientName** can specify the client name for ICA session, the default is terminal name. It can use system variable. For example, SessionConfig=ICA ClientName=$mac **NOTE: The mac address includes a special character ':'. This may cause the following issue. Etoken Java(aladdin) and Etoken CardOS SmartCard fail to logon XenDesktop 7.15 desktop.** The option **DisableMMRSeek** can be used to disable client side MMR seek capability. Default value is **No**. This setting causes issues with some specific servers. For example, Windows10.
SessionConfig=PCoIP	**SessionConfig** — Specifies the PCoIP default settings of the optional connection parameters for all PCoIP sessions.

[USBRedirection={PCoIP, TCX}] [ShowDisconnectMessage={yes, no}] [ShowReconnectMessageTime=seconds] [ResumeTimeout=seconds] [DisableRTAV={yes, no}]	**USBRedirection** — Default is **PCoIP**. Specifies the channel of USB devices redirection. **ShowDisconnectMessage** — Default is **yes**. Yes/no option to display a disconnect message when a session is disconnected. If set to yes, the message is displayed; if set to no, the message will only show in the Event Log. **ShowReconnectMessaageTime**— This option specifies the number of seconds to show the session reconnect message box after the session detects the network congest. The default value is 50 seconds. **ResumeTimeout**—The option ResumeTimeout specifies the number of seconds to wait after the reconnection dialog box prompts, and before the session successfully reconnects. If timeout value is reached then the session is closed. The default value is 1200 seconds. **DisableRTAV**—The RTAV virtual channel may impact the performance of audio or video related applications. For the parameter **DisableRTAV**, when the value is set to **Yes** the RTAV virtual channel in the session is disabled. The default value is **no**.
SessionConfig=RDP [MaxBmpCache={128 to 1024}] [EnableNLA]={no, yes}] [ForceSpan={no, yes}] [EnableTSMM={yes, no}] [EnableGFX]={yes, no}] [EnableVOR={yes, no}] [EnableRdpH264]={yes, no}] [EnableRecord={yes, no}] [EnableRFX={yes, no}] [USBRedirection={TCX, RDP}] [RDPScreenAlign4={yes,no}] [WallPaper={yes, no}] [Dragging={yes, no}] [Animation={yes, no}] [Theme={yes, no}] [TosIpPrecedence={0-5}] [TosDscp={Default/CS1/CS2/CS3/CS4/ CS5/CS6/CS7/AF11/AF12/AF13/AF22/AF23/ AF31/AF32/AF33/AF42/AF43/EF}] [AutoDetectNetwork={yes, no}]	**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. **EnableNLA** — Default is **yes**. Yes/no option to utilize the Network Level Authentication feature in RDP 7. **ForceSpan** — Default is **no**. Yes/no option to disable RDP Multi Monitor feature. **EnableTSMM** — Default is **yes** . Yes/no option to enable RDP7 Multi-media redirect. **EnableGFX** —The option when set to yes, enables RDP8 Pipelined Graphics feature. Default is **yes** for all platforms other than Wyse 3010 thin client with ThinOS (T10). If this option is configured as no, the option EnableVOR and option EnableRdpH264 will be internally set to no despite of the settings in INI. **EnableVOR** — Default is **yes**. H.264. Yes/no option to enable RDP8 Video Optimized Redirect. **NOTE: The EnableVOR parameter is not supported on C or V class.** **EnableRdpH264**— Default is **yes**. This option enables RDP8.1 h. 264 graphics feature. This option is internally set to no if the option EnableGFX is set to no manually or by default. **EnableRecord** — Default is **yes** . Yes/no option to enable RDP feature of recording from local. **EnableRFX** — Default is **yes**. Yes/no option to enable Bitmap Codec RemoteFX. **USBRedirection** — Default is **TCX** . Option to select the channel of USB devices redirection. **RDPScreenAlign4** — Default is **no**. RDPScreenAlign4=yes can force RDP session width to 4 pixels aligned.

[TSGWEnable={yes, no}] [GracefulReconnTimeout={10 - 100}] [ForceUpdatedNLA={yes, no}] [TsgwWebsock={yes, no}]	For example: `SessionConfig=RDP MaxBmpCache=1024 DefaultColor=1 EnableNLA=yes ForceSpan=yes EnableTSMM=no EnableRecord=yes EnableRFX=no RDPScreenAlign4=no` The options Wallpaper, Dragging, Animation and Theme can set the RDP experience. Default is **yes**. **TosIpPrecedence** — Allows you to set IP Precedance in the TOS fields. **TosDscp** — Sets IP DSCP in the TOS fields. **AutoDetectNetwork** —Default is **yes**. Yes/no option to enable an RDP session to adapt its data transfer to band width of network. **TSGWEnable**—Default is **yes**. Yes/no option to obtain/enable TS gateway for the applications and desktops from Microsoft RDS broker server. The default value is yes which means that the TS Gateway setting is automatically obtained or enabled from the Microsoft RDS broker server. **GracefulReconnTimeout**—This value is to set a timeout for RDP to reconnect the session if no response is received from server side during this time limit. It avoids the case of RDP session freezing for a long time and not reconnecting due to poor network quality or short time network disconnection. There is no default value for this option. The feature is disabled if it is not set. Valid value is 10 to 100, in seconds. Limitation: Certain sessions in Windows10 servers disconnect and reconnect when the session is idle with this parameter enabled. The issue occurs when H.264-AVC444 is enabled without RemoteFX/ vGPU support on server side. You can avoid the issue by not configuring H.264-AVC444 policy in the server. **ForceUpdatedNLA** allows the client side force server to use updated CredSSP, which addresses the vulnerability issue CVE-2018-0886. If the value is set to **yes**, the client disconnects the session during session login when the server uses unpatched CredSSP. The default value is **no**. **TsgwWebsock** is set when you are using WebSocket connection between the client and Windows 2016 Terminal Service Gateway. The default value is no.
SessionConfig=Blast [EnableH264={**yes**,no}] [NetworkCondition={ Excellent,**Typical**, Poor }]	**[EnableH264={yes,no}]** —This parameter controls the Blast H264 feature on the supported platforms. The default value is yes. The value yes enables H264 and the value no disables H264. This works on Blast H.264 supported platforms only. **NetworkCondition**—This parameter controls the Blast network condition. The default value is **Typical**. The following are the values and associated actions: Excellent—Network is very good. Typical—Network is normal. Poor—Network is bad.

	This parameter impacts the Blast to select UDP or TCP. When the network is **Excellent** and **Typical**, the Blast selects TCP. When it is **Poor**, the Blast selects UDP.
TcpMaxRetransmission={2~12}	Configures the retransmission of a TCP connection. The default value of this option is **5**.
TerminalName=name [reboot={yes, no}] [Capital={yes, **no**}]	User can set a string up to 15 characters as terminal name. It can be configured as system variable like $MAC, $SN or $IP etc. If reboot is set to yes and the terminal name is changed, the terminal will reboot.If "TerminalName=$DNS" is set, the system will do reverse DNS lookup to configure the terminal name. For example, if the DNS server configures the terminal IP as reverse dns name p12345.wysespt.com, the terminal name will be configured as p12345. If you set Capital=yes, the terminal name is capitalized.
**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. **NOTE:** 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 or VDM host which will be automatically started when using VDI or VDM sign-on. If the value is *, all of the VDI or VDM hosts will automatically be connected. The autoconnectlist is the connection description which can use the wildcard * to match the string.
VirtualCenter=virtual_center_url	Specifies the Virtual Center Server that supports both http and https. If the virtual_center_url does not start with http or https, the default protocol used is http. **NOTE:** 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. Only this setting can enable the Virtual Center functions.
**VNCPrompt={no, yes} [{Accept, Reject}={10 to 600} (seconds)] [ViewOnly={no, yes}] [ActiveVisible={no, yes}]	Default is **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. See also MaxVNCD in Connection Settings for wnos.ini files only to enable VNC shadowing.

	See also VncPassword in Connection Settings for wnos.ini Files Only to specify a string of up to 8 characters as the password used for shadowing. **Accept, Reject** — Default is **10**. 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** — Default is **no**. 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** — Default is **no**. Yes/no option to display a VNC session-end notice after the VNC session ends.
VPN=openconnect [Description=string_description] [Server=server_ip_or_name] [Username=username_string] [Password=password_string] [Autoconnect={yes, no}] [Username-enc=encrypted_username_string] [Password-enc=encrypted_password_string] Folder=[folder]	The INI parameter **openconnect** enables you to connect to Cisco AnyConnect VPN servers, that use standard TLS protocols for data transport. **Description**— Specifies the session name. The length of the string is limited to 21 characters. **Server**— Specifies the VPN server IP or the VPN server name. The length of the string is limited to 63 characters. **Username**— Specifies the login username. The length of the string is limited to 31 characters. **Password**— Specifies the login password. The length of the string is limited to 31 characters. **Autoconnect**— Specifies the option to enable or disable auto-connect on system startup. **Username-enc**— Specifies AES encrypted Login Username **Password-enc**— Specifies AES encrypted Login Password **Folder**— Specifies the grouping of connections. Displays the folder on ThinOS desktop only if the mode is classic mode and the paraneter signon is set as signon=yes icongroupstyle=folder. The folder can include sub folders, for example, connect=rdp host=10.151.122.71 icon=default folder=rdp\test1

TOS priority settings for TosDSCP INI

Routers treat network packets differently based on priority of the TOS tag in the IP header.

IP header has a 1-byte field called TOS—Type of Service.

IP precedence is older than DSCP. DSCP is compatible with IP Precedence.

Table 11. TOS priority settings

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
IP precedence	IP precedence							
DSCP	DSCP							

	Class Selector	Drop Precedence		

CS1 Dscp (001 000) match packets with precedence 1 (Low)

CS2 Dscp (010 000) match packets with precedence 2

CS3 Dscp (011 000) match packets with precedence 3

CS4 Dscp (100 000) match packets with precedence 4

CS5 Dscp (101 000) match packets with precedence 5

CS6 Dscp (110 000) match packets with precedence 6

CS7 Dscp (111 000) match packets with precedence 7 (High)

Table 12. TOS priority settings

IP precedence(3 bits)			DSCP (6 bits)				
Name	Value	bits	Per-Hop behavior	ClassSelector	DropPrecedence	Code point Name	DSCP Bits(decimal)
Routine	0	0	Default	NA	NA	Default	000 000 (0)
Priority	1	1	AF	1	1.Low	AF11	001 010 (10)
					2.Medium	AF12	001 100 (12)
					3.High	AF13	001 110 (14)
Immediate	2	10	AF	2	1.Low	AF21	010 010 (18)
					2.Medium	AF22	010 100 (20)
					3.High	AF23	010 110 (22)
Flash	3	11	AF	3	1.Low	AF31	011 010 (26)
					2.Medium	AF32	011 100 (28)
					3.High	AF33	011 110 (30)
Flash Override	4	100	AF	4	1.Low	AF41	100 010 (34)
					2.Medium	AF42	100 100 (36)
					3.High	AF43	100 110 (38)
Critical	5	101	EF	NA	NA	EF	101 110 (46)
Internetwork Control	6	110	NA	NA	NA	NA	(48-55)
Network Control	7	111	NA	NA	NA	NA	(56-63)

Table 13. TOS priority settings

IP precedence (3 bits)		DSCP (6 bits)	
Name	**Useful**	**Name**	**Useful**
Routine	Try as usual	NA	NA
Priority	For data traffic	AF11	Big block data
Immediate		NA	NA
Flash	For Voice control data	NA	NA
Flash Override	Video streaming	NA	NA
Critical	Voice Data	EF	Interactive Voice
Internetwork Control	Reserved	NA	NA
NetworkControl		NA	NA
		NA	NA

NOTE: The information in this section is leveraged based on the research on web. Specific priority designs must be arranged by network architect.

A

Connect Parameter: Options

This appendix provides the supported options for the Connect parameter in the following supported connections:

- ICA Connect Options
- RDP Connect Options

ICA connect options

Table shown here contains the supported options used for ICA connections (after you use the **Connect=ICA** parameter/selection).

IMPORTANT:

If an option has an underlined value (default), that option and default value will automatically be used with Connect=ICA; options without underlined values can also be used if you want to, but are not automatically used with Connect=ICA. In addition, when using options, you can leave the default value or change it to another value shown.

For example, in the following case where:

Connect=ICA

[Option1={0, 1}]

[Option2={1, 2, 3, 4}]

Since you are using Connect=ICA, then Option 1 and its default value 0 will automatically be used as Option 1 has an underlined value (default of 0). You can still use Option 2 if you want to, however, Option 2 is not automatically used with the parameter as Option 2 does not have a default value.

NOTE:

Any option in ICA Connect Options 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-off. 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 off 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.

ICA connect: options

Table 14. ICA connect: options

Option	Description
Alternate=[no, yes]	**Default is no**. Yes/no option to use an alternate IP address returned from an ICA master browser to get through firewalls.
AudioQualityMode={0, 1, 2, 3}	**Default is 0**. Specifies the audio quality of a session.

	0 – Default 1 – High Quality 2 – Medium Quality 3 – Low Quality
Autoconnect={0 to 99}	**Default is 0**. Use for automatically starting a session after you sign in, if sign-on 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.
Browserip=list of browsers	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}	**Default is high**. Session color mode. For faster display performance, use 256 colors for the session. • 256 is 8-bits • 32k is 15-bits • 64k or high is 16-bits • 16m is 24-bits • true is 32-bits **NOTE:** • 64k is the same value as high. • 16m — 24-bits over ICA is only supported by Windows XP and Windows 2003 server. It is not supported by Windows Server 2008 or newer. • true — 32-bit remote connections are not supported by Windows XP or Windows 2003 server. It requires Windows Vista, Windows Server 2008, or newer with ICA.
Command=start command	A string of commands to be executed after logging on to the server. This entry is limited to 127 characters.
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 logging on to the server. Maximum of 63 characters are allowed.
Disablesound={no, yes, 2} or {**0**, 1, 2}	**Default is no**. Specifies whether or not to disable remote sound upon connection start.

Domainname={domain name,$DN}	Domain name to use in a Windows network. $DN specifies that the thin client sign-on domain name is used. Maximum of 19 characters are allowed.
Encryption={None, Basic, 40, 56, 128, Login-128}	**Default is Basic**. Connection security encryption level. The highest level is 128-bit security (Login-128 option is 128 bit encryption for login only).The lowest is None. **NOTE:** The server must support the specified level of encryption or the connection will fail.
Fullscreen={no, yes}	**Default is no**. 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:** $UN (see System Variables) specifies that the sign-on user name is used and should be set in a {username}.ini file. If set to Host=$UN in a {username}.ini file, the hostname will display as the sign-on user name. If set to Host=$UN in a wnos.ini file, the hostname will display as the default start. **Application** — Defines the published application to launch. Application is required if no host is specified.
HttpBrowsing={no, yes}	**Default is no**. 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. For information, see Connection Settings: wnos.ini files, {username} INI, and $MAC INI Files.
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 after the session is inactive. During this period, one dummy packet will be sent to the server if network traffic is lost. Default is **10**.
LocalCopy={no, yes}	**Default is no**.

	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}	**Default is local-user**. Specifies how users authenticate to the selected application set or ICA connection.
Lowband={no, yes}	**Default is no**. 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}	**Default is no**. Yes/no option to auto-connect and map any connected USB flash drive upon connection start.
Mapdisksunderz	**IMPORTANT: : DISCONTINUED. DO NOT USE** .
[NO_FontSmoothing={no, yes}]	**Default is no**—font smoothing is enabled by default. Yes/no option to disable font smoothing. If set to yes, the font smoothing is disabled.
NoReducer={no, yes}	**Default is no**. Yes/no option to turn off compression. Default is no, which enables compression. To turn off compression, enter yes. Used here is an option of the Connect statement. It sets the value of NoReducer only for this specified connection. **NOTE:** By default the ICA protocol compresses the data to minimize the amount of data that needs to traverse the network. This compression can be as much as 50 percent for text-based applications such as Microsoft Word and 40 percent less for graphics applications than the data streams that are not compressed.
Password={password, $SYS_VAR}	Password to log-in to the application server. Either a conventional login password or a variable can be used. Maximum of 19 characters are allowed. The value of password is a conventional login password. The value of $SYS_VAR is a system variable found in Table: System variables.

	IMPORTANT: The application server password is not encrypted; it is strongly recommended not to specify it. The user will be prompted to enter the password when the connection is made. This application server password directive never starts a line, so it can be distinguished from the thin client user sign-on password which does starts a line. **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-on password with encryption to determine whether sign-on is successful.
Password-enc=an encrypted password	Specifies an encrypted string as a password for a connection.
Reconnect={no, yes, 1 to 3600 (seconds)}	**Default is no**. 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.
Resolution=[default, Seamless, <monitor resolution>]	**Default is default**. Specifies the connection display resolution. default — Starts the connection using the current desktop display setting with no window frame and border. Seamless — 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. <monitor resolution> — Resolution values you can use in the form X x Y depending on your client. Example for monitor resolution: 1024 x 768. See the Release Notes of your client.
SessionReliability={no, yes}	**Default is no**. Yes/no option to enable session reliability. **NOTE:** ThinOS 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.
UniSession={no, yes}	**Default is no**. Yes/no option to use a unisession. The connection will launch only once at a time.

UnmapClipboard={no, yes}	**Default is no**. Yes/no option to disable clipboard redirection for an ICA session if redirecting the clipboard.
UnmapPrinters={no, yes}	**Default is no**. Yes/no option to not auto-connect to local printers when the connection starts.
UnmapSerials={no, yes}	**Default is no**. Yes/no option to not auto-connect to local serials when the connection starts.
UnmapUSB={no, yes}	**Default is no**. Yes/no option to not auto-connect to local USB devices (Virtual USB) when the connection starts.
Username=[username, $SYS_VAR]	Username to log-in to the application server. Either a conventional login username or a variable can be used. Maximum of 31 characters are allowed. The value of username is a conventional login username. The value of $SYS_VAR is a system variable found in System variables. **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.
[WyseVDA={no, yes}]	**Default is no**. Yes/no option to enable Wyse Virtual Desktop Accelerator for all ICA sessions.

RDP connect options

Table shown here contains the supported options used for RDP connections after you use the **Connect=RDP** parameter/selection.

IMPORTANT:

If an option has an underlined value (default), that option and default value will automatically be used with Connect=RDP; options without underlined values can also be used if you want to, but are not automatically used with Connect=RDP. In addition, when using options, you can leave the default value or change it to another value shown.

For example, in the following case where:

Connect=RDP

[Option1={0, 1}]

[Option2={1, 2, 3, 4}]

Since you are using Connect=RDP, then Option 1 and its default value 0 will automatically be used as Option1 has an underlined value (default of 0). You can still use Option 2 if you want to, however, Option 2 is not automatically used with the parameter as Option 2 does not have a default (underlined) value.

NOTE:

Any option in RDP Connect Options 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-off.

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 off 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.

RDP connect options

Table 15. RDP connect options

Option	Description
Autoconnect={0 to 99}	**Default is 0**. Use for automatically starting a session after sign-on, if sign-on is enabled. The value of 0-99 is the delay in seconds before auto-starting the session.
Colors={256, 32k, 64k or high, 16m, true}	**Default is high**. Session color mode. For faster display performance, use 256 colors for the session. · 256 is 8-bits · 32k is 15-bits · 64k or high is 16-bits · 16m is 24-bits · true is 32-bits **NOTE:** · 64k is the same value as high. · 16m — 24-bits over RDP is only supported by Windows XP and Windows 2003 server. It is not supported by Windows Server 2008 or newer. · true — 32-bit remote connections are not supported by Windows XP or Windows 2003 server. It requires Windows Vista, Windows Server 2008, or newer with RDP.
Command=start command	A string of commands to be executed after logging on to the server. This entry is limited to 127 characters.
Console={no, yes}	**Default is no**. Yes/no option to login 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 logging on to the server. Maximum of 63 characters are allowed.
Disablesound={no, yes, 2} or {0, 1, 2}	**Default is no** or **Default is 0**. 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-on domain name is used. Maximum of 19 characters are allowed.
Fullscreen={no, yes}	**Default is no**. Yes/no option to run the session in full screen. If Fullscreen=no then the session runs in a windowed screen. **NOTE:** Fullscreen=Yes and DualHead=Yes will result in Span Mode when connecting to a Windows server 2003 or a Windows XP Pro Client. Fullscreen=Yes and DualHead=Yes will result in Extended mode when connecting to a Windows Server 2008 (any version) and to a Windows 8 or above desktop.
Host=[name, IP, $SYS VAR]	Host — A list of server host names 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:** $UN specifies that the sign-on user name is used and should be set in a {username}.ini file. , see System Variables. If set to Host=$UN in a {username}.ini file, the hostname will display as the sign-on user name. If set to Host=$UN in a wnos.ini file, the hostname will display as the default Start.
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}	**Default is 10**.

	Specifies the number of minutes to keep a session connected after the session is inactive. During this period, one dummy packet will be sent to the server if network traffic is lost.
LocalCopy={no, yes}	**Default is no**. 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=prompt	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}	**Default is no**. 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}	**Default is no**. Yes/no option to auto-connect and map any connected USB flash drive upon connection start.
NoReducer={no, yes}	**Default is no** — Enables compression. Yes/no option to turn off compression. To turn off compression, enter yes. Used here is an option of the Connect statement. It sets the value of NoReducer only for this specified connection. **NOTE:** By default the RDP protocol compresses the data to minimize the amount of data that needs to traverse the network. This compression can be as much as 50 percent for text-based applications such as Microsoft Word and 40 percent less for graphics applications than the uncompressed data streams.
Password={password, $SYS_VAR}	Password to log-in to the application server. Either a conventional login password or a variable can be used. Maximum of 19 characters are allowed. The value of password is a conventional login password. The value of $SYS_VAR is a system variable found in System Variables. **IMPORTANT:** The application server password is not encrypted; we strongly recommend not to specify it. The user will be prompted to enter the password when the connection is made. This application server password directive never starts a line, so it can be distinguished from the thin client user sign-on password which does starts a line.

	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 password into the {username}.ini file with encryption. This password is then checked against the sign-on password with encryption to determine whether sign-on is successful.
Password-enc=an encrypted password	Specifies an encrypted string as a password for a connection.
RDPAudioQualityMode	**NOTE: DISCONTINUED. DO NOT USE.**
RDPAudioRecord={no, yes}	**Default is no**. Yes/no option to specify whether users can record audio to the server. This requires a Windows 7 Server.
Rdp_No_Animation={no, yes}	**Default is no**. Yes/no option to disable the Menu and Window animation feature; use yes to disable the feature.
Rdp_No_Dragging={no, yes}	**Default is no**. Yes/no option to disable the Show content when dragging a window feature; use yes to disable the feature.
Rdp_No_Fontsmoothing={no, yes}	**Default is no**. Yes/no option to disable the Font smoothing feature; use yes to disable the feature.
Rdp_No_Theme={no, yes}	**Default is no**. Yes/no option to disable the Theme feature; use yes to disable the feature.
Rdp_No_Wallpaper={no, yes}	**Default is no**. Yes/no option to disable the Wallpaper feature; use yes to disable the feature.
Reconnect={no, yes, 1 to 3600 (seconds)}	**Default is no**. 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.
Resolution=[default, <monitor resolution>]	**Default is default**. Specifies the connection display resolution.

	default — Starts the connection using the current desktop display setting with no window frame and border. <monitor resolution> — Resolution values you can use in the form XxY. For example: 1024 x 768 depend on your client. See the Release Notes for your client. **NOTE:** If Using DualHead=Yes and setting this resolution value to Default will start the RDP session in Span Mode. If you want to use only the fullscreen of one monitor use Resolution=DDC. This option is ignored if Fullscreen=Yes
Smartcards={no, yes}	**Default is no**. Yes/no option to use a smart card login server when the connection starts.
TSGWDomainName=[domain]	Specifies the TS Gateway Domain for RDP session.
TSGWENABLE={no, yes}	**Default is no**. Yes/no option to enable TS gateway.
TSGWNAME=[hostname]	Specifies the TS Gateway host address.
TSGWPassword=[password]	Specifies the TS Gateway Password for the RDP session.
TSGWPassword-enc=[encrypted-password]	Specifies the encrypted TS Gateway Password for RDP session.
TSGWSERVER=[hostname]	Specifies the TS Gateway host address.
TSGWUsername=[username]	Specifies the TS Gateway Username for RDP session.
TSGWUsername-enc=[encrypted-username]	Specifies the encrypted TS Gateway Username for RDP session.
TSGWUSESAMEINFO={no, yes}	**Default is no**. Yes/no option to apply RDP connection credential to Gateway credential.
UniSession={no, yes}	**Default is no**. Yes/no option to use a unisession—a connection will launch only once at a time.
UnmapClipboard={no, yes}	**Default is no**. Yes/no option to disable clipboard redirection for an RDP session if redirecting the clipboard.
UnmapPrinters={no, yes}	**Default is no.** Yes/no option to not auto-connect to local printers when the connection.
UnmapSerials={no, yes}	**Default is no**. Yes/no option to not auto-connect to local serials when the connection.
UnmapUSB={no, yes}	**Default is no**.

	Yes/no option to not auto-connect to local USB devices (Virtual USB) when the connection starts.
Username=[username, $SYS_VAR]	Username to log-in to the application server. Either a conventional login username or a variable can be used. Maximum of 31 characters are allowed. The value of username is a conventional log-on username. The value of $SYS_VAR is a system variable found in Table: System variables. **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.
[WyseVDA={no, yes}]	**Default is no**. Yes/no option to enable Wyse Virtual Desktop Accelerator for all RDP sessions.

B

TimeZone Parameter: Values

Using the TimeZone parameter, Table “TimeZone Parameter: Values” contains the zone value options that can be used.

For Example:

```
TimeZone="GMT - 08:00" ManualOverride=Yes Daylight=Yes \
Start=030207 End=110107 TimeZoneName=Pacific \
DaylightName=Pacific
```

Remember to use quotation marks (" ") since the option includes spaces. The example above uses the " \" to break a single continuous line into multiple likes for easier reading with no" \" on the last line of the parameter.

NOTE:
The Start and End options are in the MMWWDD format, where:

MM = Month of the year. Values are 01 to 12 for the months of the year from January to December.

For example, 01 = January, 12 = December

WW = Week of the Month. Values are 01 to 05 for the week of the month, 05 is the last week.

For example, 01 = 1st week, 05 = the last week of the month.

DD = Day of the week. Values are 01 to 07 for the day in the week from Monday to Sunday.

For example, 01 = Monday, 07 = Sunday

U.S. Only:

For the 2013 year, DST dates are Sunday, March 10, 2:00 am and ends Sunday, November 3, 2:00 am.

Start=030207 End=110107

For the 2014 year, DST dates are Sunday, March 9, 2:00 am and ends Sunday, November 2, 2:00 am.

Start=030207 End=110107

TimeZone Parameter: Values

Table 16. TimeZone Parameter: Values

Geographic Time Zones	Time Zones Name
(GMT-12:00) International Date Line West	Dateline
(GMT-11:00) Coordinated Universal Time-11	UTC-11
(GMT-10:00) Hawaii	Hawaiian
(GMT-09:00) Alaska	Alaskan

Geographic Time Zones	Time Zones Name
(GMT-08:00) Pacific Time (US & Canada)	Pacific
(GMT-07:00) Arizona"	US Mountain
(GMT-07:00) Chihuahua, La Paz, Mazatlan	Mountain (Mexico)
(GMT-07:00) Mountain Time (US & Canada)	Mountain
(GMT-06:00) Central America"	Central America
(GMT-06:00) Central Time (US & Canada)	Central
(GMT-06:00) Guadalajara, Mexico City, Monterrey	Central (Mexico)
Geographic time zones	Time zones name
(GMT-06:00) Saskatchewan	Canada Central
(GMT-05:00) Bogota, Lima, Quito, Rio Branco	SA Pacific
(GMT-05:00) Chetumal	Eastern (Mexico)
(GMT-05:00) Eastern Time (US & Canada)	Eastern
(GMT-05:00) Indiana (East)	US Eastern
(GMT-04:30) Caracas	Venezuela
(GMT-04:00) Asuncion	Paraguay
(GMT-04:00) Atlantic Time (Canada)	Atlantic
(GMT-04:00) Cuiaba	Central Brazilian
(GMT-04:00) Georgetown, La Paz, Manaus, San Juan	SA Western
(GMT-03:30) Newfoundland	Newfoundland
(GMT-03:00) Brasilia	E. South America
(GMT-03:00) Cayenne, Fortaleza	SA Eastern
(GMT-03:00) City of Buenos Aires	Argentina
(GMT-03:00) Greenland	Greenland
(GMT-03:00) Montevideo	Montevideo
(GMT-03:00) Salvador	Bahia
(GMT-03:00) Santiago	Pacific SA
(GMT-02:00) Coordinated Universal Time-02	UTC-02

Geographic Time Zones	Time Zones Name
(GMT-01:00) Azores	Azores
(GMT-01:00) Cape Verde Is.	Cape Verde
(GMT) Casablanca	Morocco
(GMT) Coordinated Universal T+A35:A98ime	UTC
Geographic time zones	Time zones name
(GMT) Dublin, Edinburgh, Lisbon, London	GMT
(GMT) Monrovia, Reykjavik	Greenwich
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	W. Europe
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	Central Europe
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	Romance
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb	Central European
(GMT+01:00) West Central Africa	W. Central Africa
(GMT+01:00) Windhoek	Namibia
(GMT+02:00) Amman	Jordan
(GMT+02:00) Athens, Bucharest	GTB
(GMT+02:00) Beirut	Middle East
(GMT+02:00) Cairo	Egypt
(GMT+02:00) Damascus	Syria
(GMT+02:00) E. Europe	E. Europe
(GMT+02:00) Harare, Pretoria	South Africa
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	FLE
(GMT+02:00) Istanbul	Turkey
(GMT+02:00) Jerusalem	Israel
(GMT+02:00) Kaliningrad (RTZ 1)	Russia TZ 1
(GMT+02:00) Tripoli	Libya
(GMT+03:00) Baghdad	Arabic
(GMT+03:00) Kuwait, Riyadh	Arab

Geographic Time Zones	Time Zones Name
(GMT+03:00) Minsk	Belarus
(GMT+03:00) Moscow, St. Petersburg, Volgograd (RTZ 2)	Russia TZ 2
(GMT+03:00) Nairobi	E. Africa
(GMT+03:30) Tehran	Iran
(GMT+04:00) Abu Dhabi, Muscat	Arabian
(GMT+04:00) Baku	Azerbaijian
(GMT+04:00) Izhevsk, Samara (RTZ 3)	Russia TZ 3
(GMT+04:00) Port Louis	Mauritius
(GMT+04:00) Tbilisi	Georgian
(GMT+04:00) Yerevan	Caucasus
(GMT+04:30) Kabul	Afghanistan
(GMT+05:00) Ashgabat, Tashkent	West Asia
(GMT+05:00) Ekaterinburg (RTZ 4)	Russia TZ 4
(GMT+05:00) Islamabad Karachi	Pakistan
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	India
(GMT+05:30) Sri Jayawardenepura	Sri Lanka
(GMT+05:45) Kathmandu	Nepal
(GMT+06:00) Astana	Central Asia
(GMT+06:00) Dhaka	Bangladesh
(GMT+06:00) Novosibirsk (RTZ 5)	Russia TZ 5
(GMT+06:30) Yangon Rangoon	Myanmar
(GMT+07:00) Bangkok, Hanoi, Jakarta	SE Asia
(GMT+07:00) Krasnoyarsk (RTZ 6)	Russia TZ 6
(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi	China
(GMT+08:00) Irkutsk (RTZ 7)	Russia TZ 7
(GMT+08:00) Kuala Lumpur, Singapore	Singapore
(GMT+08:00) Perth	W. Australia

Geographic Time Zones	Time Zones Name
(GMT+08:00) Taipei	Taipei
(GMT+08:00) Ulaanbaatar	Ulaanbaatar
(GMT+08:30) Pyongyang	North Korea
(GMT+09:00) Osaka, Sapporo, Tokyo	Tokyo
(GMT+09:00) Seoul	Korea
(GMT+09:00) Yakutsk (RTZ 8)	Russia TZ 8
(GMT+09:30) Adelaide	Cen. Australia
(GMT+09:30) Darwin	AUS Central
(GMT+10:00) Brisbane	E. Australia
(GMT+10:00) Canberra, Melbourne, Sydney	AUS Eastern
(GMT+10:00) Guam, Port Moresby	West Pacific
(GMT+10:00) Hobart	Tasmania
(GMT+10:00) Magadan	Magadan
(GMT+10:00) Vladivostok, Magadan (RTZ 9)	Russia TZ 9
(GMT+11:00) Chokurdakh (RTZ 10)	Russia TZ 10
(GMT+11:00) Solomon Is., New Caledonia	Central Pacific
(GMT+12:00) Anadyr, Petropavlovsk-Kamchatsky (RTZ 11)	Russia TZ 11
(GMT+12:00) Auckland, Wellington	New Zealand
(GMT+12:00) Coordinated Universal Time+12	UTC+12
(GMT+12:00) Fiji	Fiji
(GMT+13:00) Nuku'alofa	Tonga
(GMT+13:00) Samoa	Samoa
(GMT+14:00) Kiritimati Island	Line Islands

Best Practices: Troubleshooting and Deployment Examples

This appendix contains the following best practices information:

- Troubleshooting INI Files
- Examples: Basic Deployments

Troubleshooting INI Files

General recommendations when encountering INI parameter usage problems and errors include:

- Check for spelling and format mistakes.
- Use the following process:

  a Restart the thin client.

  b Check thin client system information: for example, the Event log.

  c Search the Event log to see if there is an invalid statement.

Examples: Basic deployments

To help you get started, the following sections provide examples of parameters commonly used for basic deployments.

Citrix XenDesktop Broker Deployment

```
Autoload=1
Privilege=High
Timeserver=NTPserver.whatever.com timeformat="12-hour format" Dateformat=mm/dd/yyyy
TimeZone='GMT - 05:00' ManualOverride=no Daylight=yes Start=030207 End=110107
TimeZoneName=Eastern DayLightName=Eastern
SignOn=Yes
PNliteServer=https://XenDesktopDDC
Domainlist=yourdomain
Sysmode=VDI
```

Citrix Presentation Server/XenApp Deployment (with Optional Published Application)

```
Autoload=1
Signon=no
Seamless=yes
Connect=ICA \
BrowserIP=IPaddress \
Application="application" \
Description="name" \
Icon=default \
Domainname=Domain \
LocalCopy=no
```

Microsoft Broker Deployment

```
Autoload=1
Signon=yes
ConnectionBroker=Microsoft Host=ipadress
```

```
Domainlist=
Privilege=
```

VMware View Broker Deployment

```
Autoload=1
ConnectionBroker=VMware
VDIBroker=https://ViewServerAddress
TimeServer=IPAddress TimeFormat="12-hour format" DateFormat=mm/dd/yyyy
TimeZone='GMT - 05:00' ManualOverride=No Daylight=Yes Start=030207 End=110107
TimeZoneName=Eastern DaylightName=Eastern
```

Microsoft Terminal Services/Remote Desktop Service Deployment

```
Autoload=1
Signon=no
Seamless=yes
Connect=RDP \
Host=IP or Name of MS RDS server \
Description="Description" \
Username=Username \
Domainname=Domain \
Password=Password \
LocalCopy=no
```

Quest

```
ConnectionBroker=Quest
Signon=no
Domainlist=
```