2016 - 12

Dell Wyse ThinOS 8.3.1 / ThinOS Lite 2.3.1 Hot Fix Release Notes

Dell Wyse ThinOS software is designed to run on a broad array of Dell Wyse hardware platforms. New releases are created to support new hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on current, actively shipping hardware platforms, and those hardware platforms that are within their first year after their official End of Life date. Beyond the one year time period, new software releases are no longer certified for use with the older hardware, even though it is possible that they may still work. This allows us to advance our product with features and functions that might not have been supported by the previous hardware, with previous generation CPUs and supporting components.

Current Version: ThinOS 8.3, Build 109/ ThinOS Lite 2.3, Build 109
Release Date: 2016-12-23
Previous Version: ThinOS 8.3, Build 014/ ThinOS Lite 2.3, Build 014(Build 105 for Wyse 5060 thin client)

Contents

Client software licensing and maintenance options

Dell Wyse thin client software maintenance is required to receive new versions of thin client software and subsequent releases of corresponding documentation and tools. Use of this software on more than one device requires you to first purchase the additional copies of, or licenses to, the software from Dell Wyse.

Support matrix

The following platforms and images are supported in this release:

Table 1. Platforms and images

Platform	Images
C10LE	C10_wnos
R10L	R10_wnos

Platform	Images
Wyse 3010 thin client with ThinOS (T10)	DOVE_boot
Wyse 3020 thin client with ThinOS (T10D)	T10D_wnos
Wyse 3030 LT thin client with ThinOS	U10_wnos
Wyse 3030 LT thin client with PCoIP	PU10_wnos
Wyse 5010 thin client with ThinOS (D10D)	ZD10_wnos
Wyse 7010 thin client with ThinOS (Z10D)	
Wyse 5040 AIO thin client with ThinOS (5212)	
Wyse 5010 thin client with PCoIP (D10DP)	PD10_wnos
Wyse 5040 AIO thin client with PCoIP (5213)	
Wyse 5060 thin client with ThinOS	D10Q_wnos
Wyse 5060 thin client with PCoIP	D10QP_wnos
C00X	C00_xen
R00LX	R00_xen
Wyse 3010 zero client for Citrix (T00X)	T00_xen.bin
Wyse 3020 zero client for Citrix (T00DX)	T00D_xen
Wyse 5010 zero client for Citrix (D00DX)	ZD00_xen

The following packages are updated to newer version:

Table 2. Packages

Packages	Version
RTME	1.19.40087
TCX	1.10.39982
FR	1.16.39982

New features

HealthCast Single Sign-On solution

The HealthCast SSO solution is designed to improve user convenience, streamline workflow, and strengthen security compliance in demanding environments. The same proximity cards used for physical access are used to tap-in and tap-out of unique user sessions and to tap-over any sessions inadvertently left open on the ThinOS devices. Typically, you must enter your password once every day, and use your proximity cards to streamline workflow and save time as they move between shared computers securely. Additionally, proximity cards can be secured with a PIN, if configured by the organization. The HealthCast SSO solution also supports user self-service password reset so that you can reset your own passwords without the need to call the help desk.

NOTE: The HealthCast SSO Solution on ThinOS is a client-server solution. ThinOS provides the client-side functionality, but you must also install and configure the HealthCast Server components on a server system in order for the solution to work properly. Please contact HealthCast (www.gohealthcast.com) for one or more server installation executables, server requirements, and configuration information.

Configuration of HealthCast SSO solution on ThinOS

HealthCast Web API Server is integrated with ThinOS 8.3.1 hot fix release to implement the HealthCast SSO solution. To use the HealthCast SSO solution, ThinOS must be configured to use the HealthCast Web API Server. You can do this using the INI file (wnos.ini), or using the ThinOS UI. Dell recommends you to use the INI file for large deployments.

INI configuration

To configure the ThinOS to use the HealthCast Web API Server, add these parameters to your wnos.ini file:

- HealthCastServer— The server address and options needed for the client to connect to the HealthCast Web API Server.
  HealthCastServer=<https address> SecurityMode=<default, full, warning, low> ClientCertificate=<cert-pfx-file-name>
  For example: HealthCastServer=https://server1.example.com SecurityMode=full ClientCertificate=client-cert.pfx.

  For more information on INI parameters, see INI parameters.

ThinOS UI configuration

- To configure ThinOS to use the HealthCast Web API using the ThinOS UI on the client , go to **System Setup** > **Remote Connections** > **Authentication** UI.

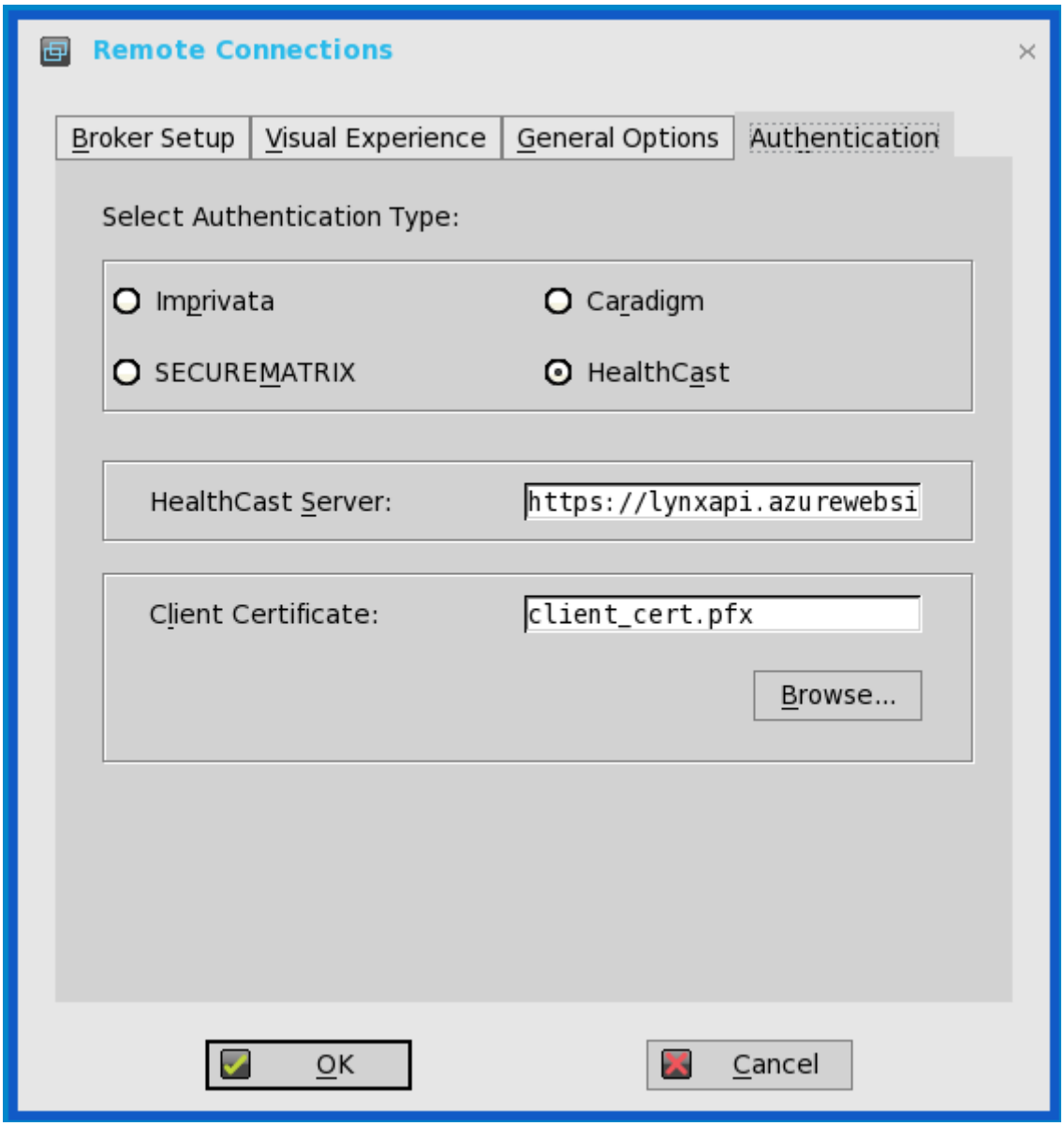

Figure 1. Authentication

HealthCast SSO features and functionality on ThinOS

The following are the HealthCast SSO features and functionality on ThinOS:

- **Proximity card enrollment**
  - HealthCast supports user self-enrollment. Therefore, there is no need to bring the proximity card to a special registration station, or for IT staff to be involved. Instead, you must only tap the disenrolled proximity card at a terminal and you can follow the easy registration process. This is a one-time event after which you can use the card wherever HealthCast is installed.

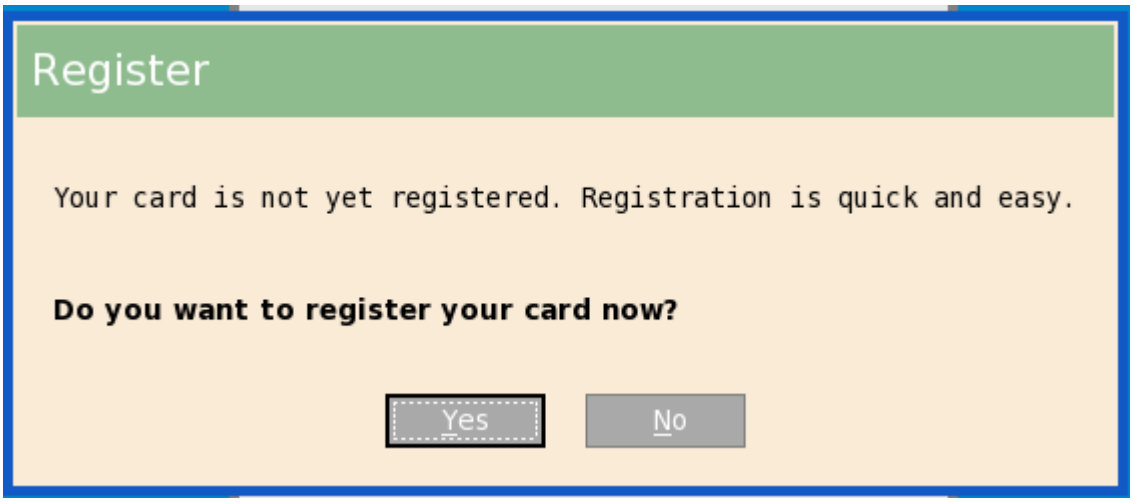

Figure 2. Proximity card enrollment

- **Manual login and lock/unlock terminal**
  - If you do not have a card, or choose not to use your card, then you can manually log in using your user name and password. Administrators can disable manual login, if they wish, so that users can sign on with their proximity cards. You can also lock or unlock the terminal, if you have signed on with a manual login.

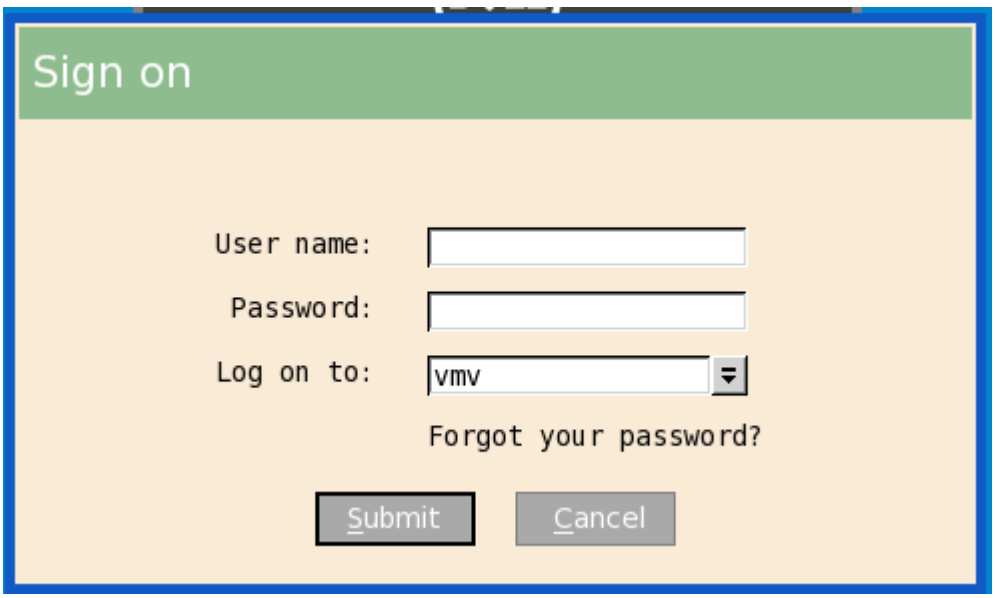

Figure 3. Manual login and lock/unlock terminal

- **Proximity card login and lock/unlock terminal**
  - After the proximity card is registered, tap the card at a terminal to login.

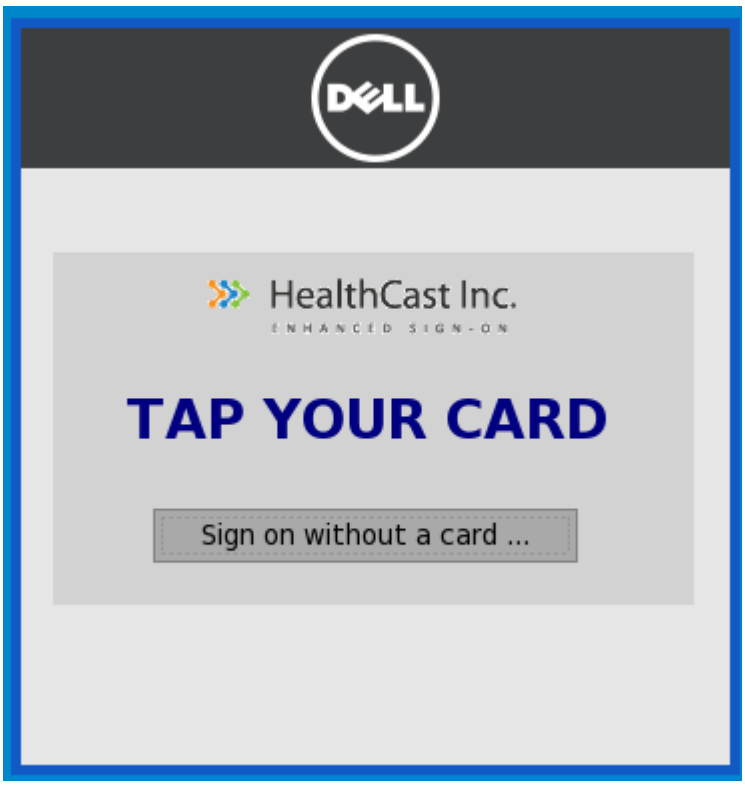

Figure 4. Login

You can lock the session to secure it, but leave the remote session connected for fast access when you return. To do this, tap the proximity card and the session is locked.

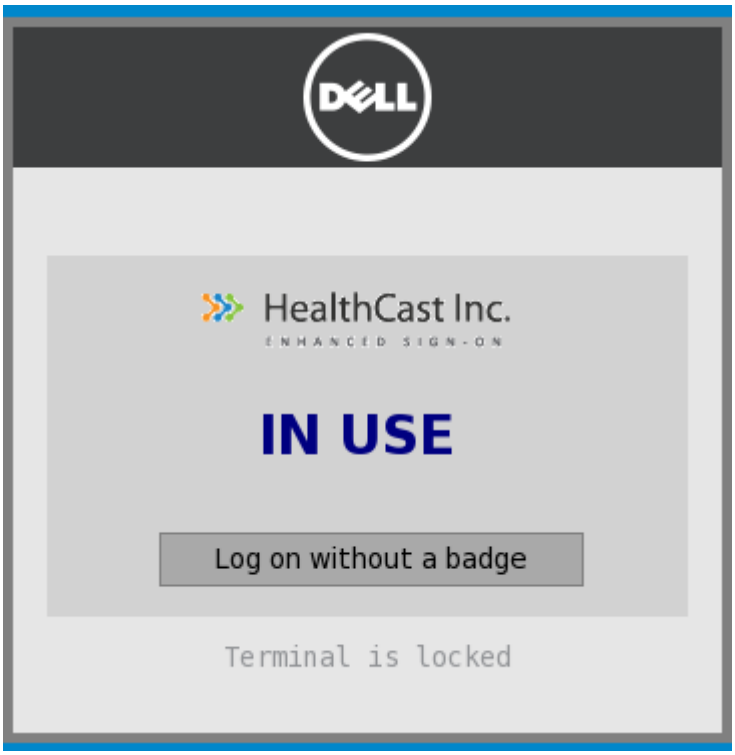

Figure 5. Lock terminal

To resume the session, tap the card again.

- **Walk away**
  - Terminals can be configured to lock or log off sessions that have been left open. The time that elapses before automatic lock or log off can be set by an administrator using the convenient web administration application.
- **Tap-Over**
  - If a session is locked or left open, a second user can tap their own proximity card and this disconnects the first session and log the second user into their own unique session.
- **Forgotten card**
  - If you forget your card at home, you can receive a temporary card and register it for the day using the same easy registration process mentioned above.
- Lost or stolen card
  - If you report a card as lost or stolen, an administrator can immediately disable the card using the convenient web administration application. This prevents anyone else from using it.
- **Self-Service Password Reset (SSPR)**
  - If SSPR enabled by an administrator, you can register for SSPR and reset your passwords without calling the help desk.

Figure 6. SSPR enrollment

- **Easy to use web-based administration tool**
  - Administrators can quickly and easily configure settings, manage proximity cards, and users using a web-based administration tool.

CCM features

ThinOS supports the following CCM features:

- Support for the ThinOS client login to CCM server console.
- Support for the ThinOS client packages installation by using On-Premises Services in CCM server console.
- New CCM discovery method
  - **DNS SRV record** check box in **Central Configuration** > **WDA** > **CCM** UI. By default, the check box is selected. Thin client obtains CCM values through DNS server, and try to register into the CCM server.
  - If the check box selection is canceled, then the thin client does not try to obtain the CCM values through DNS server.
  - To create DNS records in DNS server, use the following information:

#CCM server URL

DNS Record Type: `DNS SRV`

Record Name: `_WMS_MGMT._TCP.<Domain>`

Value Returned: `WDMNG Server URL`

Example: **_WMS_MGMT._TCP.WDADEV.com**

MQTT Server URL

DNS Record Type: `DNS SRV`

Record Name: `_WMS_MQTT._TCP.<Domain>`

Value Returned: `CCM Server URL`

Example: **_WMS_MQTT._TCP.WDADEV.com**

Group Token

DNS Record Type: `DNS Text`

Record Name: `_WMS_GROUPTOKEN.<Domain>`

Value Returned: `Group Token` (as String)

Example: **_WMS_GROUPTOKEN .WDADEV.com**

CA Validation

DNS Record Type: `DNS Text`

Record Name: `_WMS_CAVALIDATION.<Domain>`

Value Returned: `TRUE or FALSE` (as String)

Example: **_WMS_CAVALIDATION.WDADEV.com**

Updates to RTME

RTME 2.0.100 is updated to a newer version 2.1.200—Citrix HDX RealTime Optimization Pack 2.1.200 for Microsoft Skype for Business.

ThinOS supports RTME version 1.8 (for Lync) and 2.1.200 (for Skype for Business) from this release. ThinOS RTME package/client supports video codec H.264-UC, and audio codec SILK introduced by RTME 2.1. For more information about RTME 2.1 features, go to Docs.citrix.com/en-us/hdx-optimization/2-1.

Known issues and suggestions:

- When using Webcam such as, C930 with RTME 2.1, the incoming video may appear late. For example, the video may be displayed after 5–10 seconds, or a blue video is displayed instead.
- The video sent from client in call is decided by capabilities of both endpoints in the call. Sending higher video from one client does not mean that the client has better capability than the other one in call.

Support for Imprivata SSO solution on ARM platforms

Imprivata SSO solution is supported for ARM platforms (Wyse 3010 thin client and Wyse 3020 thin client series) from this release.

INI parameters

This release contains the following newly added INI parameters:

Table 3. INI parameters

Parameter	Description
SignOn={yes,no, NTLM} [MaxConnect=max] [ConnectionManager={maximize, **minimize**, hide}] [EnableOK={**no**, yes}] [DisableGuest={**no**, yes}] [DisablePassword={**no**, yes}] [LastUserName={**no**, yes}] [RequireSmartCard={**no**, yes}] [SCRemovalBehavior= {-1, **0**, 1}] [SaveLastDomainUser={yes, no, 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}] [SCShowOptions={yes, **no**}] [DisableSignoff={yes, **no**}]	Yes/no option to enable the sign-on process. Default is yes. If set to NTLM, user can be authenticated with 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. The optional keyword MaxConnect sets the maximum number of connects that are allowed to be specified in the wnos.ini and username.ini together. The range allowed for the "max" is 100 to 2000. If the value is greater than 2000, 2000 is set instead. If the value is lesser than 100, 100 is set instead. The default maximum value is 216 entries. (CIR37285) The optional keyword ConnectionManager sets the state of connection manager while sign on (After 5.0.006). The following optional keywords are valid after 5.0.010. The optional keyword EnableOK is set to display OK and Cancel button in sign-on window The optional keyword AutoConnectTimeout sets the timeout for auto connect published applications. The range is 10 seconds to 300 seconds. The default is 30 seconds The optional keyword DisableGuest sets whether guest sign-on is disabled or not. The optional keyword DisablePassword is set to disable password box and new password check box in sign-on window. The optional keyword LastUserName is set to display the last sign-on username after the user logs off. The optional keyword RequireSmartCard is set to enable force logon with smartcard The optional keyword SaveLastDomainUser is set to save the username and domain into NVRAM, after successful sign on. So during the next reboot, the username and domain saved in the NVRAM is displayed in sign on server as default username and domain, if no Default User is set in wnos.ini. The size of domain\username is limited to 32. If input domain \username size is greater than 32, it will be truncated and then saved into NVRAM. If SaveLastDomainUser=user, only username is saved into NVRAM.

Parameter	Description
[SFZeroButtons={yes, **no**}]	If SaveLastDomainUser=domain, only domain name is saved into NVRAM. (CIR57726) The optional keyword SCRemovalBehavior configures the behaviors after the smart card is plugged out from the terminal. SCRemovalBehavior — Default is 0. Specifies what happens after a smart card is removed. -1 — If smartcard is removed then client has no action. Whether the session can be used or not, totally depends on the server policy. 0 — System logs off. 1 — System locks and can be unlocked only when the same certificate is used with the smart card. The optional keyword DefaultINI configures a file name which is in default folder of username ini files. If the {username}.ini is not found, this file will be loaded by default. (CIR51869) The optional keyword IconGroupStyle configures the icon group style on the desktop. PNAgent published applications can be configured with client folder in 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. In this case, there is an "Up to 1 Level" icon on top. Clicking this icon will get back to the up level folder contents. (CIR54333) The optional keyword IconGroupLayout configures the direction of the icon group on desktop. The default is vertical. The optional keyword PasswordVariables I s set to support variable mapping ($TN, $UN etc) for password. The optional keyword LockTerminal configures the lockup terminal. The default is yes. If LockTerminal=no, the function of locking terminal is disabled. You can right-click on the desktop or click the Shutdown option --> Lock Terminal, to disable the Lock Terminal. Also, it disables the lock terminal even if "ScreenSaver=_minutes_ LockTerminal=yes" is set. The option keyword ExpireTime configures the expiration time. The range is 1 minute to 480 minutes. The default is 0 which means no expiration. If the value is greater than 480, 480 is set instead. If the value is smaller than 0, 0 is set instead. After sign on or launching a connection, start counting the expiration time. After the expiration time is reached, launch a session by clicking icon or menu or connection manager. The user will view a message box to enter password. But the open sessions still remain open. Only if the password is same as original sign on password, the session will be launched.

Parameter	Description
	If the terminal is locked and unlocked by using password, start counting the sign on expiration time again. If the default value yes is set, then when you unlock the system, the system will refresh PNA list to verify the password. Set the value to no to disable the behavior of refresh. (CIR63666) The optional keyword SCShowCNName is set to yes to forcibly use the CN name of the certificate as the user name when using smartcard sign on. By default, the UPN name is used as the user name. The optional keyword SCSecurePINEntry is set to yes to enable Secure PIN entry function for pkcs15 card with Cherry keyboard. The default value is no. The optional keyword DisableEditDomain is set to yes to stop typing in the domain box manually. Typing the character @ or \ as the format domain\user and user@domain in username box are not allowed. The option AdGroupPreFix is only valid, when you configure SignOn=NTLM. If the option is configured, then zero Clinet will verify all AD group names to which the 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 exits, before loading user specific ini. For example, if the sign no user is user_111 in a domain, 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 exists, it will be loaded. If the option ClearUser is set to yes, the username is cleared during a failed login, and if it is set to no the username is retained. The default value is no. If the option DisableSignoff is set to yes, signoff button is disabled from shutdown option and connection manager window, also disables the logoff button on StoreFront desktop. If the option SFZeroButtons is set to yes the buttons (shutdown, login etc.) at the bottom of signon window are displayed like Zero mode when you set StoreFront style.
Proxy={yes, no} AppList={ccm;fr;rtme} [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 via proxy. Both CCM, FR, and RTME are supported. The application name is separated with semicolon. 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. The option User and Password can support system variables. Because CCM runs before sign on, it is not appropriate to use $UN and $PW.

Parameter	Description
	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
HealthCastServer=vip list [LogLevel={0,1,2,3}] [SecurityMode={**default**, full, warning, low}] [ClientCertificate=certificate file name]	A list of VIP addresses with optional TCP port number of HealthCast servers. 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, drop the connection. If set to warning, the SSL connection need 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 will not be checked. The value will be persistent, the default value of the setting is **default**. ClientCertificate option specify the client certificate file name during SSL connection between Healthcast server and client.
CCMEnable={yes, no} [CCMServer=<server_address>] [GroupPrefix=<prefix>] [GroupKey=<hashkey>] [MQTTServer=<mqtt_address>[:<mqtt_port>]] [AdvancedConfig={no, yes}] [CCMDefault={no, yes}] [Override={no, yes}] [CAValidation=(yes, no)] [Discover=(yes, no)]	**Default is no.** **CCMEnable** — Yes/no option to enable the Cloud Client Manager **CCMServer** — Specifies a IP address or URL address for the Cloud Client Manager server. Once specified, it is saved in the non-volatile memory. Default port is 80. **GroupPrefix and GroupKey** — The options GroupPrefix and GroupKey compose the group code of the Cloud Client Manager server. Once specified, it is saved in the non-volatile memory. **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. Default MQTT port is 1883. **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=[None, Low, High] [LockDown= {no, yes}] [HideSysInfo={no, yes}] [HidePPP={no, yes}] [HidePN={no, yes}] [EnableNetworkTest={no, yes}]." **CCMDefault** — **Default is no.**

Parameter	Description
	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 (https:// us1.cloudclientmanager.comus1.cloudclientmanager.com) and default MQTT server (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. Groupkey priority policy is listed as below: The Groupkey can technically be applied in many places. Below are the different places you can configure the group key in order of priority that is if #1 is defined it will override #2 etc. 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 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. **NOTE: 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` If CAValidation=yes is specified, CCM agent will check the certficate if connected to https server. **Default value is yes.**. If Discover=yes is specified, CCM agent will discover CCM server, MQTT server and CA validation from DNS Record. **Default value is yes**.
[DHCPOptionsRemap={no, yes}] [DisableOption12={no, yes}] [FileServer={128 to 254}] [RootPath={128 to 254}] [FtpUserName={128 to 254}] [FtpPassWord={128 to 254}] [WDMServer={128 to 254}] [WDMPort={128 to 254}]	Default is no. **DHCPOptionsRemap** — Specifies whether or not the following options can be set. 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.

Parameter	Description
[PnliteServer={128 to 254}] [DomainList={128 to 254}] [VDIBroker-{248 to 254}] [Discover={yes, no}] [WDMSecurePort={128 to 254}] [WDMFQDN={128-254}] [CCMGroupKey={128-254}] [CCMServer={128-254}] [CCMMQTTServer={128-254}] [CCMCAValidation={128-254}]	If you set different value for DisableOption12 from the value in NVRAM, the system will automatically reboot to make the value valid. (CIR36891) **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. **WDMSecurePort**—Specifies the HTTPS port of WDM server. **WDMFQDN** — Specifies the Fully Qualified Domain Name (FQDN) of the WDM server. CCMGroupKey, CCMServer, CCMMQTTServer and CCMCAValidation specify to remap the tags for CCM configuration.
ConnectionBroker={default, VMware, Microsoft, Quest, AWS} [IgnoreProfile={yes, no,}] [SecurityMode={Default,Low,Warning,Full}] [EnableVWGateway]={yes, no} [VWGateway]=url [ConnectionType]={Default, All, RDP, PCoIP}] [EnableVDMCredSSP]={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**. 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	Description
	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. EnableVDMCredSSP=yes option enables the RDP NLA mode connection when you launch VMware View broker session. The default value is no. EnableVDMCredSSP=yes only works when disable view security tunnel is in the server side.
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}] [CAGAuthMethod={LDAP+RSA, RSA+LDAP}] [RequestIconDataCount={0-65535}] [DefaultSettings={XenApp, XenDesktop}] [SmartcardPassthrough={**yes**, no}] [StoreFront={**no**, yes}] PnliteServer=List of {IP address, DNS names, or URLs}	**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** section 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.

Parameter	Description
	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

Parameter	Description
	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 will replace the default CitrixReceiver WTOS/1.0 during Netscaler login. You can use WTOS/1.0 as your Netscaler Session Policy and can set this INI to keep your Netscaler policy configuration(CIR89871).
SignOn={**yes**,no, NTLM} [MaxConnect=max] [ConnectionManager={maximize, **minimize,** hide}] [EnableOK={**no**, yes}] [DisableGuest={**no**, yes}] [DisablePassword={**no**, yes}] [LastUserName={**no**, yes}] [RequireSmartCard={**no**, yes}] [SCRemovalBehavior= {-1, **0**, 1}] [SaveLastDomainUser={yes, no, 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}]	Yes/no option to enable the sign-on process. Default is yes. If set to NTLM, user can be authenticated with 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. The optional keyword **MaxConnect** sets the maximum number of connects that are allowed to be specified in the wnos.ini and username.ini together. The range allowed for the “max” is 100 to 2000. If the value is greater than 2000, 2000 is set instead. If the value is lesser than 100, 100 is set instead. The default maximum value is 216 entries. (CIR37285) The optional keyword **ConnectionManager** sets the state of connection manager while sign on (After 5.0.006). The following optional keywords are valid after 5.0.010. The optional keyword EnableOK is set to display OK and Cancel button in sign-on window The optional keyword AutoConnectTimeout sets the timeout for auto connect published applications. The range is 10 seconds to 300 seconds. The default is 30 seconds The optional keyword DisableGuest sets whether guest sign-on is disabled or not. The optional keyword DisablePassword is set to disable password box and new password check box in sign-on window. The optional keyword LastUserName is set to display the last sign-on username after the user logs off. The optional keyword RequireSmartCard is set to enable force logon with smartcard

Parameter	Description
[SCSecurePINEntry={**no**, yes}] [AutoConnectTimeout={10-300}] [DisableEditDomain={yes, no}] [AdGroupPrefix=adgrpnameprefix] [ClearUser={yes, no}]	The optional keyword SaveLastDomainUser is set to save the username and domain into NVRAM, after successful sign on. So during the next reboot, the username and domain saved in the NVRAM is displayed in sign on server as default username and domain, if no Default User is set in wnos.ini. The size of domain\username is limited to 32. If input domain \username size is greater than 32, it will be truncated and then saved into NVRAM. If SaveLastDomainUser=user, only username is saved into NVRAM. If SaveLastDomainUser=domain, only domain name is saved into NVRAM. (CIR57726) The optional keyword SCRemovalBehavior configures the behaviors after the smart card is plugged out from the terminal. **SCRemovalBehavior** — Default is **0**. Specifies what happens after a smart card is removed. **-1** — If smartcard is removed then client has no action. Whether the session can be used or not, totally depends on the server policy. **0** — System logs off. **1** — System locks and can be unlocked only when the same certificate is used with the smart card. The optional keyword DefaultINI configures a file name which is in default folder of username ini files. If the {username}.ini is not found, this file will be loaded by default. (CIR51869) The optional keyword IconGroupStyle configures the icon group style on the desktop. PNAgent published applications can be configured with client folder in 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. In this case, there is an "Up to 1 Level" icon on top. Clicking this icon will get back to the up level folder contents. (CIR54333) The optional keyword IconGroupLayout configures the direction of the icon group on desktop. The default is vertical. The optional keyword PasswordVariables I s set to support variable mapping ($TN, $UN etc) for password. The optional keyword LockTerminal configures the lockup terminal. The default is yes. If LockTerminal=no, the function of locking terminal is disabled. You can right-click on the desktop or click the Shutdown option --> Lock Terminal, to disable the Lock Terminal. Also, it disables the lock terminal even if "ScreenSaver=_minutes_ LockTerminal=yes" is set.

Parameter	Description
	The option keyword ExpireTime configures the expiration time. The range is 1 minute to 480 minutes. The default is 0 which means no expiration. If the value is greater than 480, 480 is set instead. If the value is smaller than 0, 0 is set instead. After sign on or launching a connection, start counting the expiration time. After the expiration time is reached, launch a session by clicking icon or menu or connection manager. The user will view a message box to enter password. But the open sessions still remain open. Only if the password is same as original sign on password, the session will be launched. If the terminal is locked and unlocked by using password, start counting the sign on expiration time again. If the default value yes is set, then when you unlock the system, the system will refresh PNA list to verify the password. Set the value to no to disable the behavior of refresh. (CIR63666) The optional keyword SCShowCNName is set to yes to forcibly use the CN name of the certificate as the user name when using smartcard sign on. By default, the UPN name is used as the user name. The optional keyword SCSecurePINEntry is set to yes to enable Secure PIN entry function for pkcs15 card with Cherry keyboard. The default value is no. The optional keyword DisableEditDomain is set to yes to stop typing in the domain box manually. Typing the character @ or \ as the format domain\user and user@domain in username box are not allowed. The option **AdGroupPreFix** is only valid, when you configure SignOn=NTLM. If the option is configured, then zero Clinet will verify all AD group names to which the 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 exits, before loading user specific ini. For example, if the sign no user is user_111 in a domain, 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 exists, it will be loaded. If the option ClearUser is set to yes the username is cleared when login fails, and if set to no, username is retained. The default value is no.

System variables

The following system variables can be used with some options of the Connect parameter:

Table 4. System variables

Option	Value
$SN	Serial number
$MAC	MAC address
$IP	IP address (for example: 10.151.120.15)

Option	Value
$IPOCT4	The fourth octet of IP Address (for example, if IP is 10.151.120.15, the fourth octet is 15)
$DHCP(extra_dhcp_option)	Extra dhcp options for Windows CE unit, including 169, 140, 141, 166, 167. For example, set a string test169 for option tag 169 in DHCP server, and set TerminalName=$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).
$FIP	IP Address with xxx.xxx.xxx.xxx (for example, 010.151.120.015)
$UN	Sign-on username
$PW	Sign on password
$TN	Terminal name
$DN	Sign-on domain name
$WPUN	PEAP/MSCHAPv2 username (802.1x dependent)
$WPPW	PEAP/MSCHAPv2 password (802.1x dependent)
$WPDN	PEAP/MSCHAPv2 domain name (802.1x dependent)
$SUBNET	Subnet notation. The format is {network_address}_{network_mask_bits}. For example, if the ip address is 10.151.120.15, network mask is 255.255.255.0,10.151.120.0_24.
&Right($xx, i) or &Left($xx, i)	Specifies whether the variable is to be read from left or right. The $xx is any of above parameters. The parameter i is digits for the offset of right/left.

NOTE: 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 are supported.

Fixed issues

The following section lists the fixed issues:

Table 5. Fixed issues

CIR number	Summary
CIR89347	ThinOS Imprivata tap to lock function does not allow tap over to function with **suspendaction=0**.
CIR89116	Xenith replacement by the Wyse ThinOS clients
CIR89244	ThinOS UI customizations
CIR78372	Field length in the Legal Notice dialog is extended.

CIR number	Summary
CIR89166	VDI broker initialization failed when using an F5 load balancer in APM mode.
CIR89039	WCM: Popup on receiving configuration is disabled.
CIR89388	Wireless roaming failures after upgrading to 8.3.
CIR89259	RefreshTimeOut setting enhancements
CIR89345	Unable to connect Citrix XenDesktop after Netscaler 11.x upgrade.
CIR89745	5010 WLAN configuration reliability enhancements
CIR89160	**Device=cmos bluetooth=no** command replacement
CIR89255	Dual display does not work properly with Dell U3415w monitors.
CIR87358	Text file display reliability enhancements
CIR88396	Enhancement to allow low privilege users, the ability to rename clients
CIR89446	Connection issues to Citrix StoreFront if there is a Hidden Store
CIR89886	Connect issues to Storefront if there is an Unauthenticated Store
CIR89821	Video playback of wmv files are not smooth
CIR90069	Starcos 3.2 Smartcards are not functioning with certain card readers.
CIR89358	D10D does not automatically reboot when hardware configurations are used in a username.ini file.
CIR89407	**FileServer=** is not working when defined in a username.ini.
CIR86078	Subnet handling improvements
CIR89789	USB Disks in ICA cannot access on an empty USB storage device.
CIR90004	USB Disks in ICA cannot access on an empty USB storage device.
CIR89376	R10LE upgrades from 8.0_512 to 8.3_011 require a manual powering cycling of the device.
CIR89426	R10LE upgrades from 8.0_512 to 8.3_011 require a manual powering cycling of the device.
CIR89546	R10LE upgrades from 8.0_512 to 8.3_011 require a manual powering cycling of the device.
CIR89777	R10LE upgrades from 8.0_512 to 8.3_011 require a manual powering cycling of the device.

CIR number	Summary
CIR89436	Message file **SYS_Passwd_Invalid** variable has different value compared to 2.0_512.
CIR89793	Caradigm does not function with spaces in the password.
CIR89553	Imprivata 5.2 support to add RDSH broker configurations.
CIR89585	Aladdin eToken 72K(Java) device support issues
CIR89586	VMware Horizon pool, Russian names are displayed as **????????** on the ThinOS desktop.
CIR89778	Active published applications minimize when a new Citrix published application is launched.
CIR89830	Active published applications minimize when a new Citrix published application is launched.
CIR89157	Active published applications minimize when a new Citrix published application is launched.
CIR89759	Enhancement to support C series 2 GB and 4 GB clients (converted C90LE7 units)
CIR89706	Smartcard Certificate Authentication is not passed to IE store in a Windows 10.2 RDP session.
CIR89182	Smartcard Certificate Authentication is not passed to IE store in a Windows 10.2 RDP session.
CIR89831	Roaming fails on 5010 with ThinOS, and the device displays weak wireless signal.
CIR89882	Roaming fails on 5010 with ThinOS, and the device displays weak wireless signal.
CIR89947	Reliability improvements
CIR89873	Username field is cleared, if wrong password is entered.
CIR89881	Reliability improvements VDTW30N
CIR89842	Cisco Wi-Fi Leap Authentication Improvements
CIR90038	Wireless reliability improvements
CIR89720	CMOS Management issues when extracting and restoring CMOS settings
CIR90104	Language Bar does not display Swiss language correctly
CIR89103	CCM ThinOS package support
CIR89104	CCM ThinOS package support
CIR89105	CCM ThinOS package support

CIR number	Summary
CIR87492	CCM ThinOS package support
CIR89794	CCM ThinOS package support
CIR89860	**Failed to change the password!** error when you are configuring RSA pin
CIR89989	CCM preferences not honored if FileServer and WDM fields have content and the CCM validation button is used
CIR89871	Ability to specify ThinOS HTTP User-Agent header for Netscaler profiles
CIR89708	When an Analog headset is removed the internal speakers will emit sound, even when the speaker is configuration is set to disabled
CIR90003	Reliability Improvements
CIR89798	Extra lines show up in Microsoft Excel
CIR89728	NumLock issue with ThinOS when connected to an RDP session
CIR89984	ThinOS OpenConnect VPN client unable to communicate outside the VPN subnet
CIR90047	ThinOS OpenConnect VPN client unable to communicate outside the VPN subnet
CIR90199	BIOS update security improvements
CIR89073	Device=CMOS commands do not function after 5010 is updated to 3.0P BIOS.
CIR89496	Citrix session disconnects when accessing USB disks
CIR90252	Add NLA support for RDP connections to Win7 desktops on ThinOS
CIR90245	DST end setting is not configuring the correct end date.
CIR89472	Imprivata USB Finterprint reader support for ARM based client devices.
CIR89522	Imprivata USB Finterprint reader support for ARM based client devices.
CIR89809	D10D sound issue in Lync and other apps.
CIR90140	Audio quality improvements with VDI sessions.
CIR88628	Citrix session sharing does not work on all firmware versions after 8.0_306.
CIR89553	Imprivata 5.2 support to add RDSH support.
CIR89717	Microsoft Server 2016 RDSH/RDVH validation.

CIR number	Summary
CIR89364	Jabra Evolve 65 noise issue when using bluetooth and wireless.
CIR90006	Multimedia improvements
CIR90152	Citrix Session - Video distortion
CIR89803	WDM Profile Manager improvements
CIR89580	RTME 2.0 Citrix Video stream improvements
CIR89705	D10D LPD device improvements
CIR89987	HP LJ1200 does not work with 8.3_014 firmware
CIR90349	Cannot set mouse pointer option on Virtual Machine
CIR90210	Display artifacts with 3030LT connecting to Citrix XA 6.5
CIR89867	T10 Transparent cursor issue
CIR90497	3030LT usb - com port mapping issues when using multiple USB to serial cables
CIR89912	Citrix Windows close when pressing F2
CIR90607	Additional DHCP Option mappings to System Variables
CIR90671	Error if German umlaut is used in password for Imprivata login
CIR89848	Signoff improvements
CIR89864	Multimedia improvements
CIR89865	Multimedia improvements
CIR90637	Reliability improvements, hub_daemon handling
CIR89627	Added Plantronics W740 SAVI 3IN1 support