Rev. A00
2018 - 03

Dell Wyse ThinOS Version 8.5_012 and ThinOS Lite Version 2.5_012 Hotfix 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 8.5_012 and ThinOS Lite 2.5_012
Release Date: March 2018
Previous Version: ThinOS 8.5_009 and ThinOS Lite 2.5_009

Contents

Feature updates

This release note contains information about the following feature updates:

- GUI enhancement—Earlier when the connection to https file server fails in full security mode, a dialog box is displayed which prompts you to click **OK**. In this release, the feature is updated to display a tooltip at the bottom-right of the screen.
- Updates to H.264 decoder on ThinOS—The following table describes the performance of H.264 decoder in VMware Horizon sessions that use the VMware Blast display protocol:

Table 1. Blast H.264 decoding

Screen resolution within VMware Horizon Blast session	Blast H.264 decoding in VMware Horizon Blast session	Summary
Session display width is less than or equal to 1920 pixels.	Blast H.264 decoding is always enabled.	Horizon client uses Blast H.264 decoding even if the H.264 decoder setting is disabled using GUI or INI options.
Session display width is greater than 1920 pixels.	Blast H.264 decoding is disabled by default. You can enable Blast H.264	By default, Horizon client does not use Blast H.264 decoding. If the Blast H.264

Screen resolution within VMware Horizon Blast session	Blast H.264 decoding in VMware Horizon Blast session	Summary
	decoding either on the ThinOS GUI or by deploying the INI parameter.	decoder setting is enabled on ThinOS, then the Horizon client uses H.264 decoding. Enabling H.264 may downgrade the session performance.

Supported platforms

The following table lists the supported hardware platforms:

Table 2. Supported platforms

Platform	Image
Wyse 3010 thin client with ThinOS—T10	DOVE_boot
Wyse 3010 zero client for Citrix	T00_xen.bin
Wyse 3020 thin client with ThinOS—T10D	T10D_wnos
Wyse 3020 zero client for Citrix	T00D_xen
Wyse 3030 LT thin client with ThinOS	U10_wnos
Wyse 3030 LT thin client with PCoIP	PU10_wnos
Wyse 3040 thin client with ThinOS	A10Q_wnos
Wyse 3040 thin client with PCoIP	PA10Q_wnos
Wyse 5010 thin client with ThinOS—D10D	ZD10_wnos
Wyse 5010 thin client with PCoIP—D10DP	PD10_wnos
Wyse 5010 zero client for Citrix	ZD00_xen
Wyse 5040 AIO thin client—5212	ZD10_wnos
Wyse 5040 AIO thin client with PCoIP—5213	PD10_wnos
Wyse 5060 thin client with ThinOS	D10Q_wnos
Wyse 5060 thin client with PCoIP	PD10Q_wnos
Wyse 7010 thin client with ThinOS—Z10D	ZD10_wnos

Fixed issues

The following are the fixed issues in this release:

Table 3. Fixed issues

CIR	Description
CIR93220	Icons display order controls for applications and desktops published using Citrix Receiver.
CIR94701	VNC port number can be defined using ThinOS.
CIR94758	General reliability is enhanced—hub_daemon.
CIR94456	DEVICE_SECURITY parameter issue is observed that results in boot failures when the parameter is defined in an INCLUDE file.
CIR89252	Support for ReinerSCT Cyberjack e-com devices.

CIR	Description
CIR93969/CIR95622	PCoIP package extraction issue—VMware session launch failures after a firmware update.
CIR94139	Display issue is observed that affect terminal emulator application display.
CIR94214	When a VM is restarted, a window is displayed with incorrect message.
CIR94800	USB Mass Storage devices with GPT format are not recognized.
CIR94200	Support for HID Crescendo c1150 smartcard devices.
CIR94406	Crescendo 11xx Active Identity V2 profile support is added.
CIR93427	Incorrect ARP is sent after obtaining an IP address from DHCP.
CIR94286	Improved recording quality issue associated to Aten USB switch when using a Jabra PRO9460 device.
CIR94690	Functionality to define UNC paths for firmware and BIOS upgrade file locations.
CIR94860	`Screensaver` parameter lock functionality is enhanced to enable lock terminal with no defined type.
CIR94943	Event log grammar issue associated to the `SecurityPolicy` parameter is resolved.
CIR94849	Smartcard login fail with OCSP configured for domain controller kerberos certificates is resolved.
CIR94955	High resolution videos do not play with Windows Media Player in a Citrix XenDesktop session.
CIR94594	3840 x 1600 monitor resolution is added in Wyse 5060 thin clients.
CIR95067	EAP-PEAP negotiation failures due to TLS version checking is resolved.
CIR95256	Sensitivity issues pertaining to DHCP option 199 is observed—Wyse Management Suite Group.
CIR95326	DHCP option 199 results in client resets to factory defaults are resolved.
CIR95008	General reliability is enhanced—Page fault callout.
CIR95315	Default ThinOS desktop wallpaper is displayed during each boot before loading the bitmap defined in the configuration file.
CIR94255	General reliability is enhanced—Wyse Management Suite agent.
CIR94216	Ability to disable WIFI scans is added.
CIR94915	Display of security warning messages on the initial boot after a reset to factory defaults is resolved.
CIR95438	Issue preventing file server access after a reset to factory defaults is resolved.
CIR95410	SCEP enrollment password limit extended from 28 to 63 characters.
CIR94595	Invert functionality of the mouse scroll wheel when using Blast and PCoIP protocols is resolved.
CIR95006	Desktop icon display controls are added when using a VMware View Broker Blast in Classic desktop mode.
CIR95019	General reliability is enhanced—HUEWEI P8.
CIR92442	Issue where the client automatically adds: 443 to the URL when connecting to an https file server is resolved.
CIR94370/CIR93368	Local Flash security is enhanced to protect ThinOS system files.

CIR	Description
CIR95358	General reliability is enhanced.
CIR93701	Added functionality to disable `AutoSignoff=Yes` when a session connection fails.
CIR95226	Imprivata WebAPI enhancement to reduce the number of transactions to the OneSign server.
CIR95311	Changed Citrix Receiver version in Citrix monitor to display the same version in the user interface.
CIR93929	Wireless issue where DHCP renew/rebind is enabled after each roam.
CIR94913	Differentiated services do not function when using Skype.
CIR94026	The \ key on the 109 Japanese keyboard does not send a value when using Blast protocol.
CIR95634	In Wyse 3040 thin client, the wireless units do not associate to access points using channels 120, 124, and 128.
CIR95624	In Wyse 3040 thin client, the wireless roaming delay periods when roaming between access points are improved.
CIR95476	AutoStart (auto connect) fails when you are using Imprivata OneSign.
CIR95649	Drive letter mapping fails with SD card reader.
CIR95712	General reliability is enhanced—VDGUSBN.
CIR93039	Functionality to manage desktop icon ordering is added.
CIR92843	Support for the Safenet SC650 smartcard.
CIR95671	General reliability is enhanced—hub_daemon.
CIR95524	The client automatically adds: 80 to the URL when connecting to an http file server.
CIR95488	General reliability is enhanced—Page fault.
CIR95450	Resolved an issue preventing NLA logon using Gemalto IDPrime.Net smartcards.
CIR94433	In Wyse 3040 thin client, 5 GHz wireless network reliability is enhanced.
CIR93303	Blast sessions freeze when thin client is idle—VMware / AppStack.
CIR93020	Users can enter credentials before the group profile is loaded.
CIR94634	Wireless reliability is enhanced.
CIR94986	The \ key is ignored when using Blast Extreme protocol.
CIR95030	Firmware upgrade affects wireless configurations.
CIR94068	In Wyse 5060 thin client BIOS support is upgraded to version 1.0E.
CIR93081	BIOS password limit extended to 15 characters.
CIR93926	Multi-Touch support is added.
CIR94400	In Wyse 3040 thin client, the screen display distorts if the monitor is turned off and then turned on.
CIR95675	Memory allocation issue results in free memory with less than 10 percent warning messages.
CIR95386	Wireless performance is improved.
CIR94785	SCEP issue while using Venafi.
CIR95727	Issues are preventing https SCEP enrollment.

CIR	Description
CIR93244	Event log message is enhanced to improve WDM status reporting.
CIR94201	Moving the client to a new Wyse Management Suite group causes network settings to reset to factory defaults.

Packages

The following table lists the packages:

Table 4. Packages

Package name	Version
FR	1.20.46089
Horizon	4.6.47367
RTME	2.3.44433
TCX	7.1.41853

INI parameters

The following table lists the INI parameters:

Table 5. INI parameters

Parameters	Description
PRIVILEGE=[None, Low, High] [LockDown= {no, yes}] [HideSysInfo={no, yes}] [HidePPP={no, yes}] [HidePN={no, yes}] [HideConnectionManager={no, yes}] [EnableNetworkTest={no, yes}] [EnableTrace={no, yes}] [ShowDisplaySettings={no, yes}] [EnableKeyboardMouseSettings={no, yes}] [KeepDHCPRequestIP={no, yes}] [SuppressTaskBar={no, yes, auto}] [EnablePrinterSettings={no, yes}] [CoreDump={ide, disabled] [EnableNetworkSetup={yes, no}] [DisableNetworkOptions={yes, no}]	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. The Connect Manager can be enabled by using the HideConnectionManager=no option, however, the user cannot create a 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 socket and reboot.

Parameters	Description
[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}] *HideWlanScan=[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]	**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 disables the G key reset on start 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 takes 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 connection or edit an existing connection. **EnableNetworkTest**—Default is **no**. Yes/no option to enable the Network Test. **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.

Parameters	Description
	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 you use this parameter in a wnos.ini file, it is 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 disables 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 is 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 is enabled. If the optional DisableNetworkOptions=yes is set at the same time, the options table is disabled. If the optional EnableSystemPreferences=yes is set with Privilege={none, low}, the system preferences setup is enabled. If the optional DisableTerminalName=yes is set at the same time, the terminal name field is disabled. If the optional DisableSerial=yes is set with Privilege={none, low}, the serial table in peripherals setup is enabled. **DisableChangeDateTime**—If the optional DisableChangeDateTime is set, the function of changing date and time locally is disabled. For example, if you right-click the time label in taskbar, nothing is displayed. The **Change Date and Time** button in System Preference is invisible. **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.

Parameters	Description
	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 is 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 is enabled. If there are camera and/or bluetooth devices, the camera and/or bluetooth tab are enabled. 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. **HideWlanScan**—HideWlanScan is used to disable WiFi scan in lockdown mode. The default value is no. **TCPTosDscp**—TCPTosDscp is used to set TOS field for all TCP packets when it is not preconfigured by other INI settings. **UDPTosDscp**—UDPTosDscp is used to set TOS field for all UDP packets when it is not preconfigured by other INI settings.
AutoSignoff={no, yes, 2–60}* [Shutdown={no, yes}] [Reboot={no, yes}]	Default is no. AutoSignoff—Yes/no option to automatically sign out a user when the last opened session is closed. 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. **AutoSignOff**—AutoSignOff can configure a value from 2 to 60. This value represents the number of seconds a particular session must be active before calling AutoSignOff parameter.
SessionConfig=ALL	**SessionConfig**—Specifies the default settings of the optional connection parameters for all sessions.

Parameters	Description
[unmapprinters={no, yes}]	**unmapprinters**—Default is **no**. Yes/no option to un-map printers.
[unmapserials={no, yes}]	**unmapserials**—Default is **no**. Yes/no option to un-map serials.
[smartcards={no, yes}]	**smartcards**—Default is **no**. Yes/no option to use smartcards.
[mapdisks={no, yes}]	**mapdisks**—Default is **no**. Yes/no option to map disks.
[disablesound={no, yes, 2}]	**disablesound**—Default is **no**. Yes/no option to disable sound. If value is set to 2, the sound at remote computer is disabled.
[unmapusb={no, yes}]	**unmapusb**—Default is **no**. Yes/no option to un-map USBs.
[DisksReadOnly={no, yes}]	**DisksReadOnly**—Default is **no**. Yes/no option to mount mass storage disks as read-only.
[MouseQueueTimer={0–99}]	**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={no, yes}]	**WyseVDA**—Default is **no**. Yes/no option to enable Virtual Desktop Accelerator for all ICA and RDP sessions.
[WyseVDA_PortRange=startPort, endPort]	**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={no, yes}]	**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 are saved into nvram, if EnableLocal parameter is set to yes in wnos.ini.
[DefaultColor={0,1,2}]	**DefaultColor**—Specifies the default color depth to use for the session 0=256, 1=High color, 2=True Color.
[VUSB_DISKS={yes, no}] [VUSB_AUDIO={yes, no}] [VUSB_VIDEO={yes, no}] [VUSB_PRINTER={yes, no}]	**VUSB_DISKS, VUSB_AUDIO, VUSB_VIDEO, and VUSB_PRINTER**—Default **no**. Specifies if these USB devices are redirected to the server using TCX Virtual USB or ICA or RDP USB redirection. 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={no, yes}]	**FullScreen**—Default is **no**. Specifies the default screen mode. When you use FullScreen in a Dual Screen mode, the session is displayed in span mode
[Resolution={default, vga_resolution}]	**Resolution**—Default is **default**. Specifies the session resolution. For example, 640 x 480 and other supported resolutions. Default sets the resolution to the native resolution of the monitor. Setting the resolution to a value smaller than the native 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}]	
* [OnDesktop={default, all, none, desktops, applications, ondesktop_list}	

Parameters	Description
	of the monitor, allows 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 connects 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 functions. 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, see Msdn.microsoft.com/en-us/library/windows/desktop/dd318693(v=vs.85).aspx. **SessionLogoffTimeout**—Setting SessionLogoffTimeout value forces all sessions to log off 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 out waits for 30 seconds for all sessions to complete logoff, then, automatically session logs off. Broker sign out continues. 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 the desktop. The default value is no, and the original state of Group Sessions is cleared. **OnDesktop**—This parameter specifies the connections displayed on the desktop. It enhances ondesktop options for **SessionConfig=ICA** so that the VDI brokers are also compatible with ondesktop options. If the connection is not displayed in desktop, it is still added to the connection manage list. If AutoConnectList is set in the VDIServer statement, all connections configured in AutoConnectList parameter are displayed. The connections are displayed on desktop as default. The connections can be controlled using the following values: · all—display all, same as default. · none—does not display desktops. · desktops—display only desktops.

Parameters	Description
	• applications—display only applications. The others are handled as a ondesktop_list. For example, if you set ondesktop=word; excel, only Word and Excel applications are displayed. The ondesktop_list also supports wildcard * such as AutoConnectList parameter in VDIServer. For example, if the value is set to ondesktop=*IE*, any application that includes the string IE is displayed. For example—farm1:IE, farm2:IExplore
*device=mtouch [mult_touch={yes, no}] [mult_jitter={5-50}]	The parameter specifies the ThinOS multi-touch monitor setting. The value mult-touch=yes enables you to use multi touch devices. The default value is yes. For mult-jitter, select a larger value if you do not prefer double-click. Select a smaller value for a better user experience. The default value is 30.
ScepAutoEnroll={yes, no} AutoRenew={yes, no} InstallCACert={yes, no} [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} 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]	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. 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**—This option is to specify the SCEP server's service URL. This field must be set correctly. The default protocol for SCEP service is HTTP and data security is ensured by SCEP itself. You can also add the prefix https://, if SCEP service is deployed on HTTPS in your environment.* **CACertHashType**—This option is the hash type used to verify certificate authority's certificate. This option must be set to MD5 or SHA1 or SHA256.*

Parameters	Description
	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 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 link. Do not add protocol prefix to RequestURL and ScepAdminURL.**

NOTE: INI parameter with an asterisk is a newly added parameter.