Dell Wyse ThinOS Version 8.4 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: 8.4
Release Date: 2018-02
Previous Version: 8.3.2

Contents

Supported platforms

The following table lists the supported hardware platforms:

Table 1. Supported hardware platforms

Platform	Image name
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 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

Platform	Image name
Wyse 5040 AIO thin client with ThinOS (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

BIOS information

The following table lists the BIOS information:

Table 2. BIOS information

Platform	BIOS version
Wyse 3010 thin client	EC 3.02
Wyse 3020 thin client	wloader 7.1_216
Wyse 3030 LT thin client	1.0E
Wyse 3040 thin client	Dell BIOS 1.2.0
Wyse 5010 thin client	3.0T
Wyse 5040 thin client	3.0T
Wyse 5060 thin client	1.0E
Wyse 7010 thin client	3.0T

New features

This section lists the new features introduced in ThinOS 8.4 release:

Security enhancements: Firmware signature

In ThinOS v8.4 release, firmware signature verification is added to enhance firmware security. New INI parameter is introduced to allow downgrade from ThinOS v8.4 firmware to earlier versions.

To know how to downgrade from ThinOS v8.4 using the new INI parameter `VerifySignature=no`, see INI parameters and Troubleshooting.

Bluetooth 4.0 support

Bluetooth 4.0 feature is supported on the ThinOS clients that have Intel wireless chipset 7260 and 7265.

ⓘ **NOTE: Bluetooth 4.0 mouse that was used for validation is the Microsoft ARC touch mouse 1592.**

Supported Bluetooth devices—Keyboard, mouse (3.0 and 4.0), and headset (3.0, only call level audio quality is supported).

Limitations—The following are the limitations:

- Only Bluetooth 4.0 Classic and Bluetooth Low Energy (BLE) are supported.
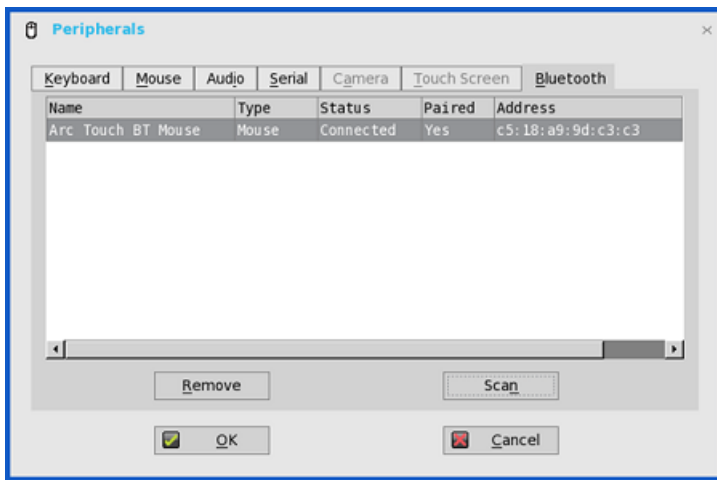- AMP is not supported.

User Interface changes

- In this release, only **Remove** and **Scan** buttons are available in the **Bluetooth** tab.
- Click the **Scan** button to search the Bluetooth devices. Select a device, and then click the **Connect** button. The device is connected automatically.
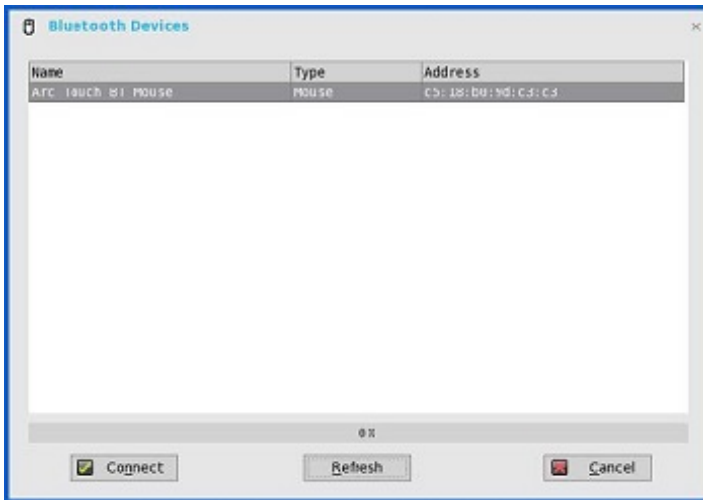
- Click the **Remove** button to disconnect/remove the device.

Package updates

The package versions are updated along with the new firmware. You need to obtain the new packages, and install them with the new firmware for full update of the units.

*   `RTME.i386.pkg` version number is updated to 2.2.42091.

    Version number is updated to match the latest Citrix HDX RealTime Multimedia Engine (RTME) version 2.2.
*   `horizon.i386.pkg` version number is updated to 4.4.42202. This package is introduced to support the VMware Blast protocol on ThinOS. For more information about the Blast implementation on ThinOS, see Dell Wyse ThinOS 8.4 Administrator's Guide.

    *   The version number is updated to match the latest VMware Horizon Client version 4.4.
    *   INI parameter to install this new package is `AddPkg="horizon"`
*   `FR.i386.pkg` version number is updated to 1.18.41564.
*   `TCX.i386.pkg` version number is updated to 7.1.41853.

    The version number is updated to match the TCX FR version 7.1.

ⓘ | **NOTE: The last digits in the package version number are for the ThinOS reference and does not match with the application.**

VMware Blast protocol implementation

VMware Blast display protocol can be used for remote applications and for remote desktops that use virtual machines or shared-session desktops on an RDS host. Use this protocol connection to display the desktop with the Blast protocol. The following configuration is added to display the applicable desktops and applications with only Blast protocols using the VMware View options. Server Default or All Supported options can also be used to list desktops in Blast protocols, as applicable.

1   Go to **Remote Connections** > **Broker Setup**, and then select the broker type as **VMware View**.
2   From the **Connection Protocol** drop-down list, select **Blast Only**.
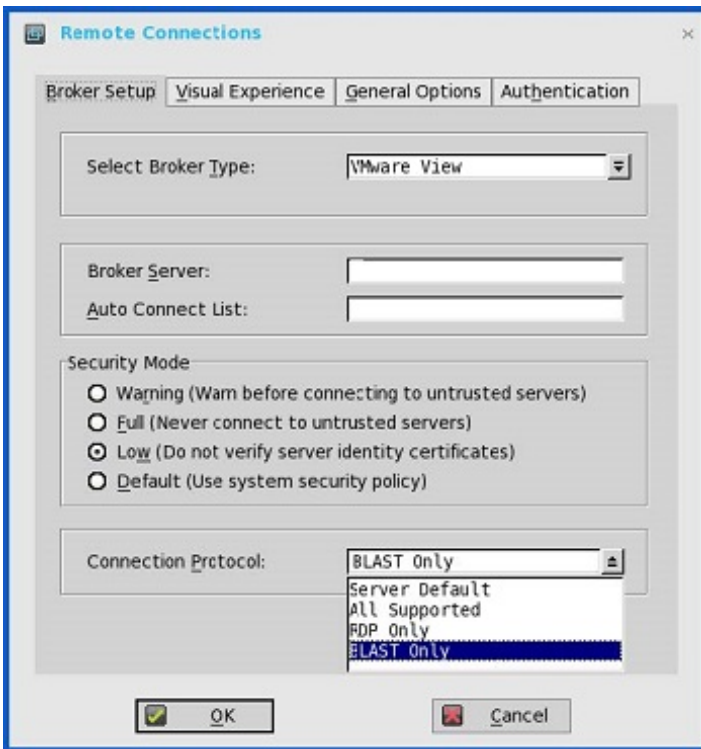
ⓘ **NOTE:**

- A new desktop icon is added for VMware desktops with Blast connection.
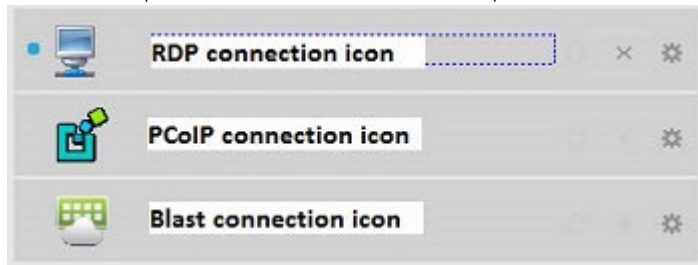
- When you pause the pointer over the connection icons, the corresponding connection protocols are displayed in tooltip. This behavior is designed for RDSH applications. From ThinOS 8.4 release, RDSH application is supported for both PCoIP and Blast protocol. These two protocols share the same application icon, and hence it is necessary for you to pause the pointer over the connection icons to identify its protocol.

The following dialog box displays the Blast connection properties:
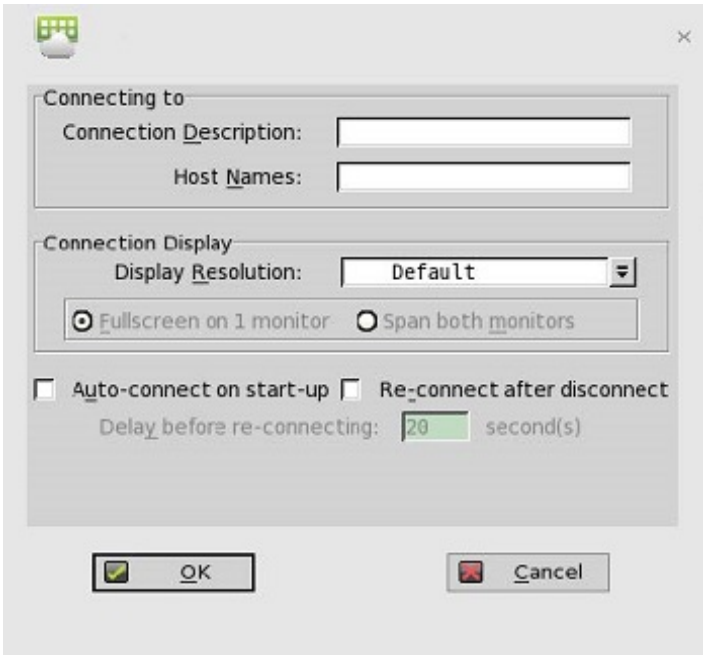
Supported platforms

- 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
- Wyse 7010 thin client with ThinOS

Blast feature matrix

The following table lists the blast feature matrix on ThinOS:

Table 3. Blast feature matrix

Blast features	Support on ThinOS	Comments/ Known issues
H.264 offload	No	Supports release later than ThinOS 8.4
VDI desktops	Yes	N/A
RDSH desktops	Yes	N/A
RDSH applications	Yes	Application window does not support Seamless mode. For example, all applications open in single window because of the VMware limitation.

Blast features	Support on ThinOS	Comments/ Known issues
		RDSH application supports the PCoIP protocol from ThinOS 8.4, with same limitation.
Unified communication	No	Third party plug-ins are not planned
MS VDI plug-in	No	N/A
RTAV	Yes	N/A
Windows media MMR	No	N/A
Flash URL multicast	No	N/A
Printer redirect	Yes	Supports printer redirection, and printer mapping with virtual print.
Smartcard redirect	Yes	N/A
Scanner redirect	No	N/A
Serial port redirect	No	N/A
USB redirect—VDI/ RDSH	Yes	Enabled by default. For more information, see Dell Wyse ThinOS 8.4 Administrator's Guide, available at Dell.com/manuals.
Client drive redirect	No	N/A
Linux desktop	Yes	N/A
Copy Paste text	Yes	See, VMware Horizon server and client configurations/ documentation.
VPN connect	Yes	N/A
AES 128/256	Yes	See, ThinOS AES design.
Multi-display/ 4K/ 32-bit	Yes	See, VMware Blast support information. For example, the pre-requisite is VM video RAM.
ClearType fonts support	Yes	ThinOS supports TrueType fonts
3D display	Yes	See, VMware Blast support information
Blast recovery from network interrupt	Yes	Requires Horizon View agent 7.0.1

Simplified Certificate Enrollment Protocol (SCEP)

Simplified Certificate Enrollment Protocol (SCEP) was designed to be used in a closed network where all end-points are trusted. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner. Within an enterprise domain, it enables network devices that do not run with domain credentials to enroll for certificates from a Certification Authority (CA).

At the end of the transactions defined in this protocol, the network device has a private key and associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.
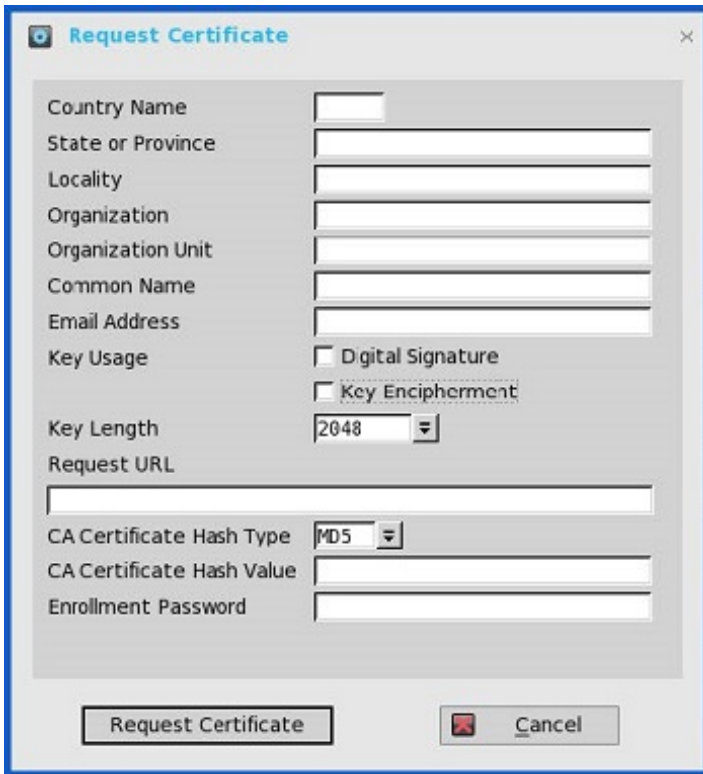
ThinOS is treated as a network device. The functionalities of ThinOS SCEP include manual certificate request, automatic certificate request, and automatic renewal of certificate.

Requesting certificate manually

To request the certificate manually, do the following:

1   Go to **System Tools** > **Certificates** > **Request Certificate**.
       The **Request Certificate** dialog box is displayed.

2   Enter the appropriate values in the **Request Certificate** dialog box, and then click the **Request Certificate** button.

       The certificate request is sent to the server, and the client receives the response from server and installs both CA certificate and client certificate.

3   Click **Ok** to save the changes.

ⓘ **NOTE:**

- If the SCEP server is on Windows Server, the CA certificate HASH provided by MS Windows server is always an MD5 hash type.
- Request server URL must be an HTTP link. Do not add protocol prefix for HTTPS, and so on.
- At present, the Enrollment Password is a clear text field. This will be changed to password mask field in the later release.

Requesting certificate automatically

Use INI parameters to automate the **request and renew** certificate process. Related INI parameters are of global scope and should be used with INI parameter `ScepAutoEnroll`.

For more information about using the INI parameters, refer to the latest *Dell Wyse ThinOS INI Reference guide*.

ICA Self Service Password Reset (SSPR)

You can reset the password or unlock the account after you complete the security questions enrollment.

Supported Environment

- XenDesktop 7.11 and later versions
- Support Storefront server 3.7 and later versions
- Self-Service Password Reset Server 1.0 and later versions

Supported Platforms

- All platforms are supported

Limitations

- Supports only storefront server
- The Legacy Account Self-Service (which needs Account Self-Service Server configured in ThinOS Remote Connections) is independent with this storefront version. Storefront version will cover Legacy Account Self-Service.
- The security question enrollment is not supported in Virtual Desktop Infrastructure (VDI) mode.

Before resetting password/ Unlocking account

Before resetting your password or unlocking your account, you must register for the security questions enrollment. To register your answers for the security questions, do the following:

1   From the PNMenu, click the **Manage Security Questions** option (Classic and StoreFront only).
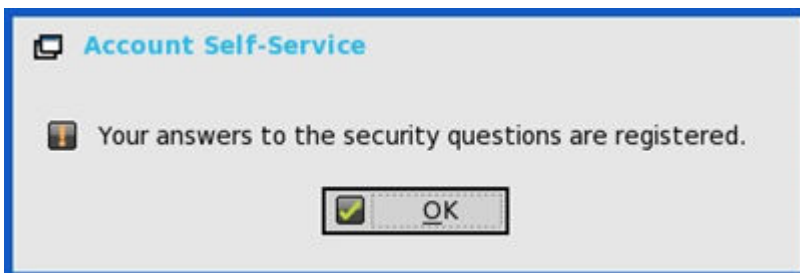
     The **Security Questions Enrollment** window is displayed.
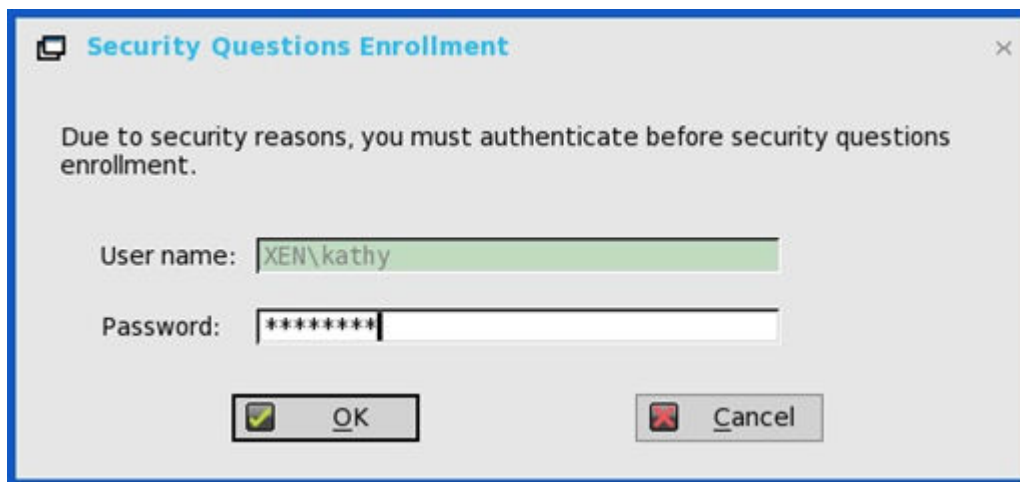
2   Enter the appropriate answers to the question set.
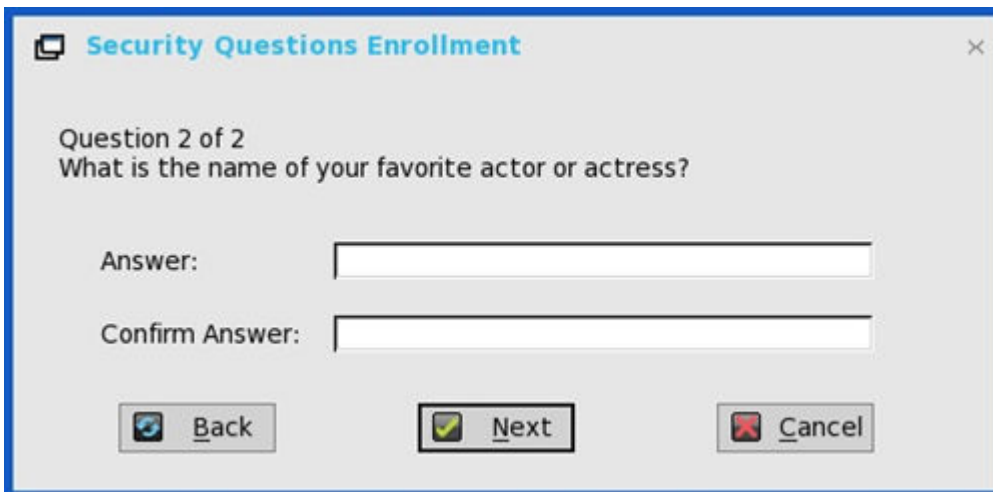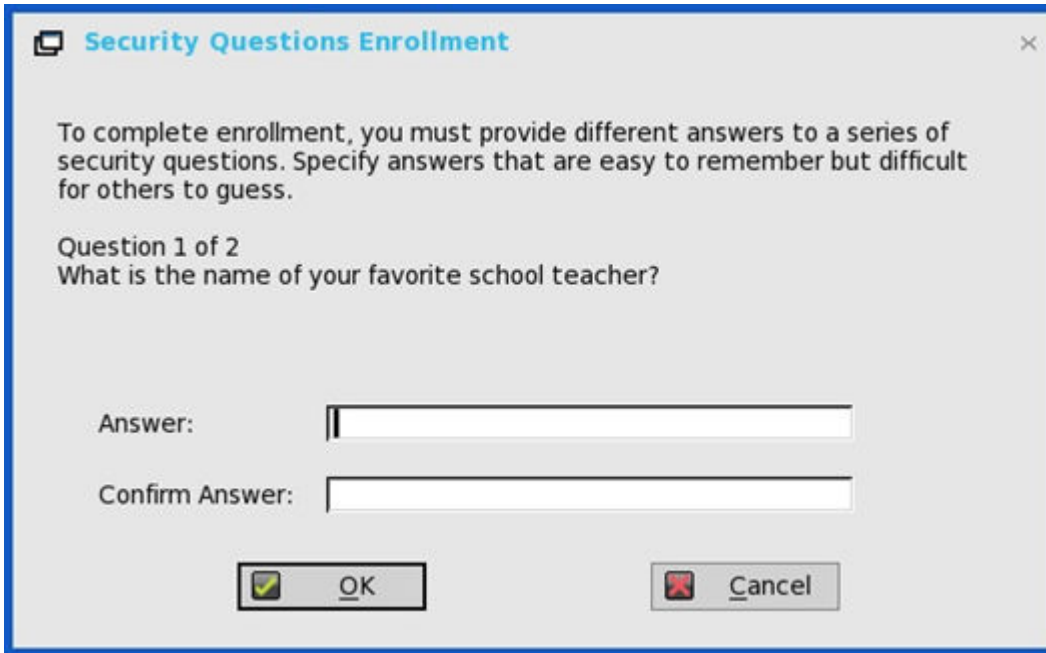
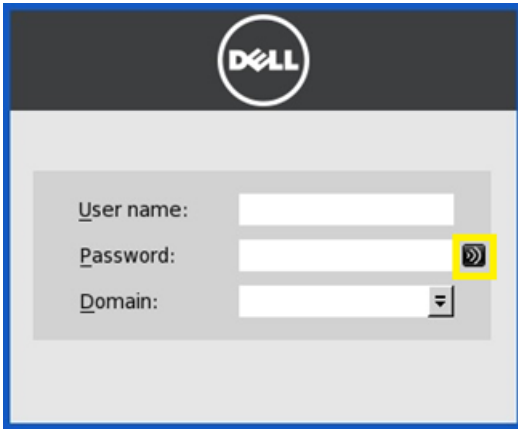3 Click **OK** to register the security questions.

Using Account Self-Service

After the security questions enrollment is complete, when ThinOS is connected to a StoreFront server with Self-Service Password Reset enabled, the **Account Self-Service** icon is displayed in the sign-on window.

ⓘ **NOTE: If you enter wrong password more than four times in the Sign-on window, the client automatically enters the unlock account process.**

1   Click the **Account Self-Service** icon to unlock your account or reset your password.

ⓘ **NOTE: You need to register the security questions for the users before using unlock account or reset password.**

2   Click **Unlock account** or **Reset password** based on your choice, and then click **OK**.
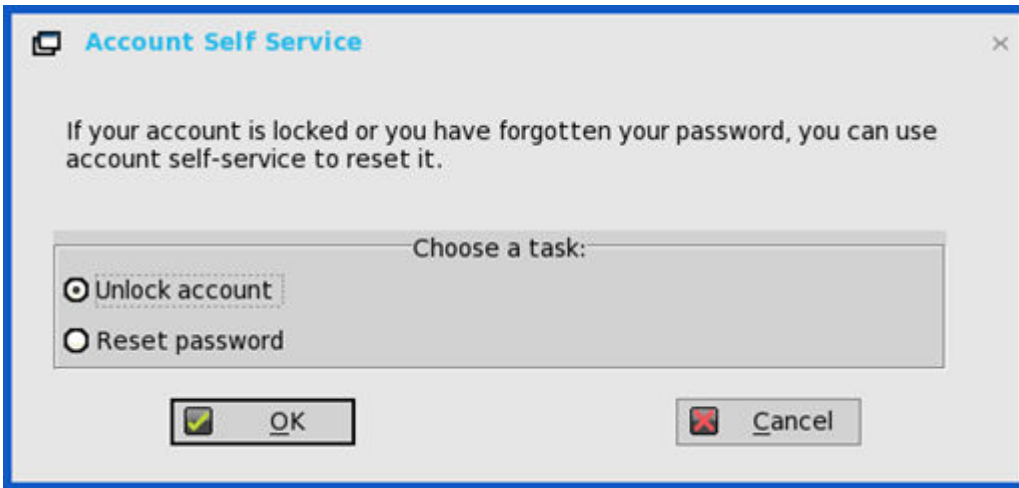
Unlocking account

After you register the security questions, do the following to unlock the account:

1   Choose a task (Unlock account) in **Account Self-Service** window.

2   Enter the user name.

   The **Unlock Account** dialog box is displayed.
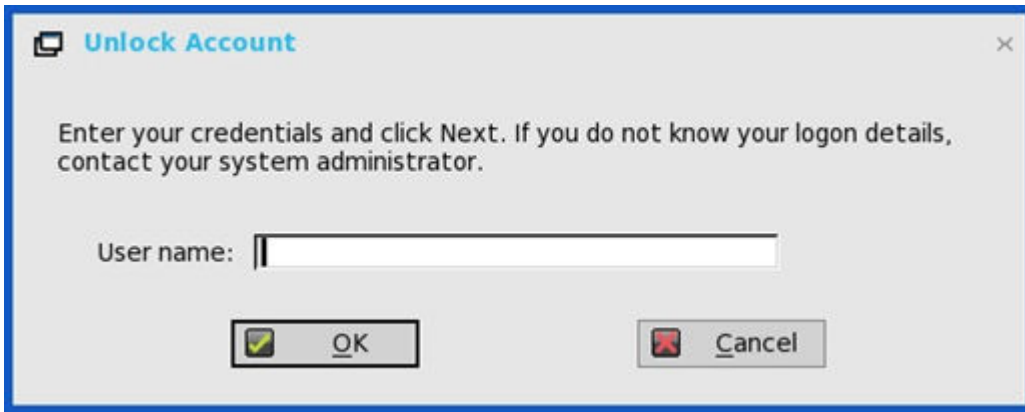
3 Enter the registered answers to the security questions.
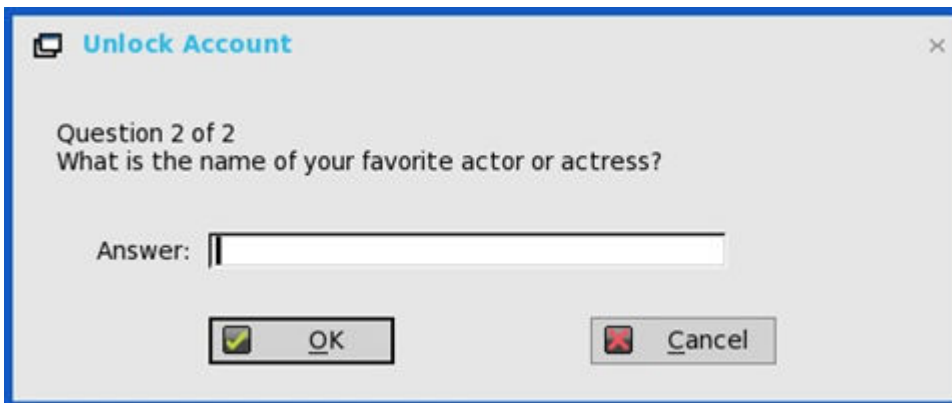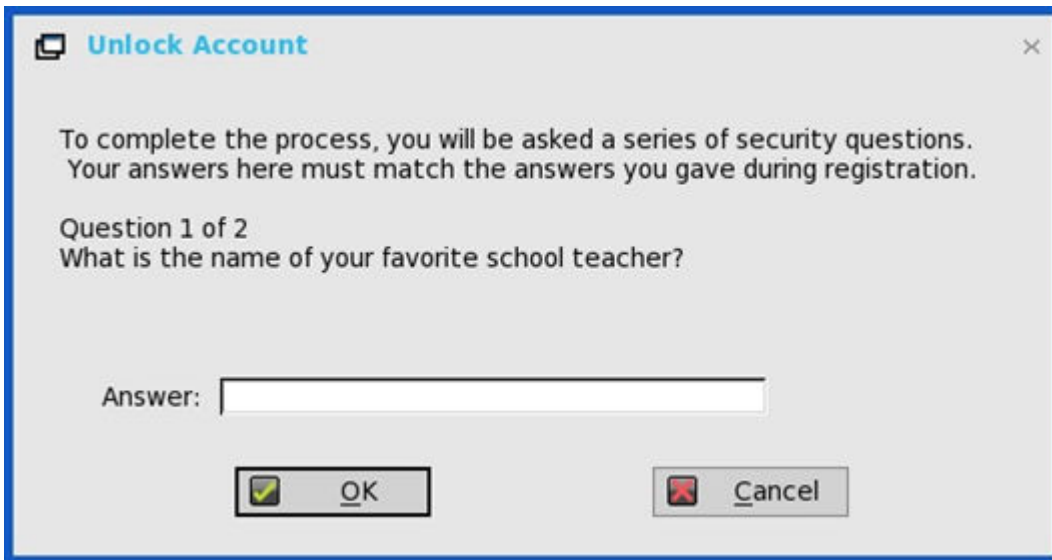
If the provided answers match the registered answers, then the **Unlock Account** dialog box is displayed.

4 Click **OK** to successfully unlock your account.

Unlock Account

All the questions were answered successfully and your account has been unlocked.

☑ OK

ⓘ **NOTE:**

- If the provided answers are incorrect, the following error message is displayed.

Unlock Account ✕

To complete the process, you will be asked a series of security questions. Your answers here must match the answers you gave during registration.

Question 1 of 2
What is the name of your favorite school teacher?

Answer: |

🔴 Your answer to this question was incorrect. Your answer here must match the answer you gave during registration.

☑ OK   ❌ Cancel

- If you provide the wrong answers more than three times, you can not unlock the account or reset the password, and the following error messages are displayed.

Account Self-Service

🔴 Your answer to this question was incorrect. The permitted number of attempts has been reached.

☑ OK

Account Self-Service

🔴 You are temporarily locked out of account self-service. Contact your system administrator.
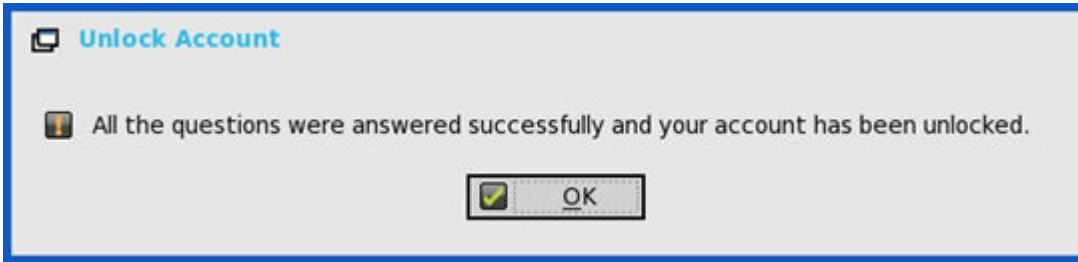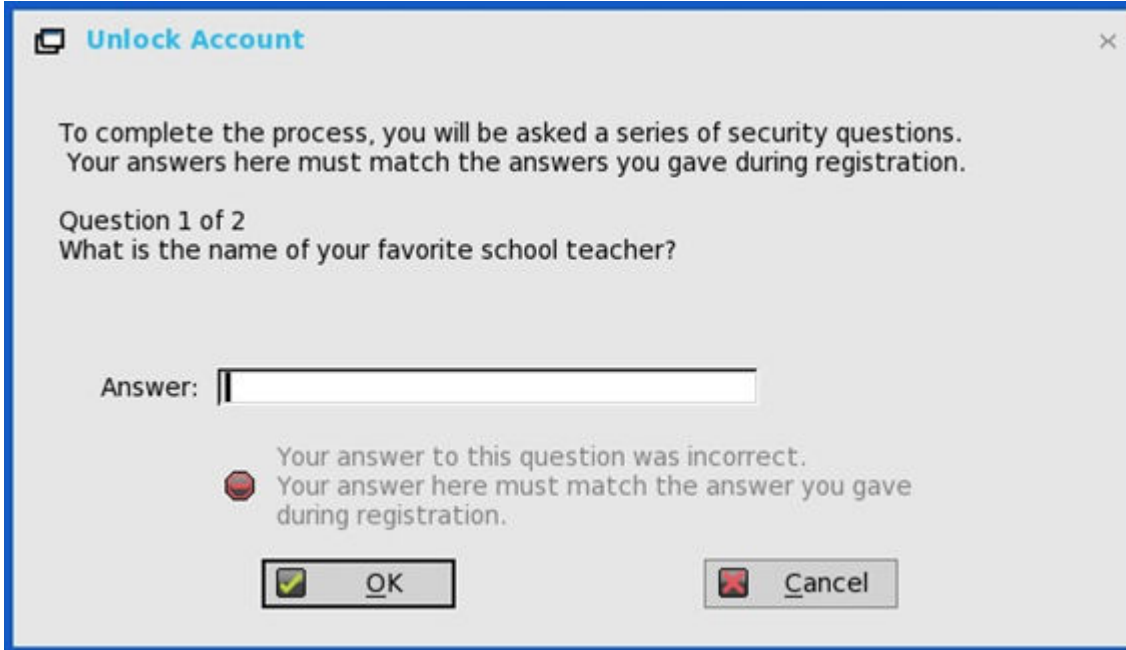
☑ OK
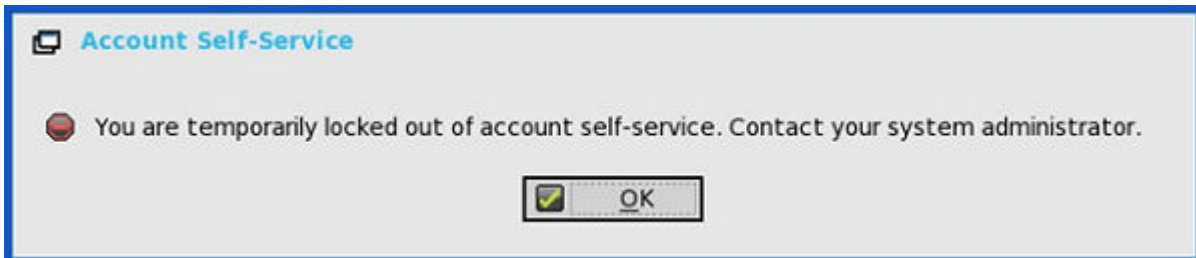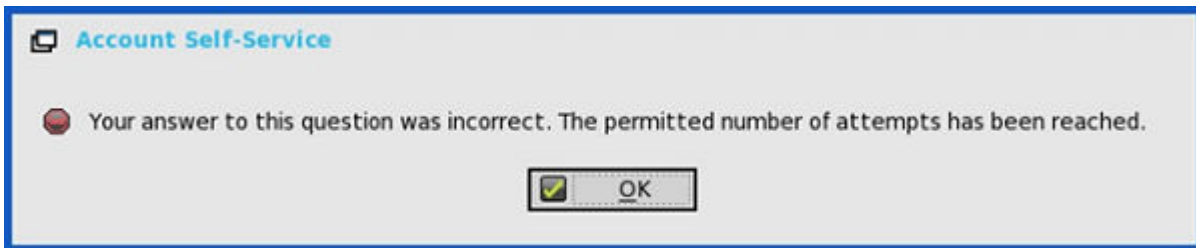
Resetting password

After you register the security questions, do the following to reset the password:

1   Choose a task (Reset password) in **Account Self-Service** window.

2   Enter the user name.

    The **Reset Password** dialog box is displayed.

3   Enter the registered answers to the security questions.

    If the provided answers match the registered answers, then the **Reset Password** dialog box is displayed.
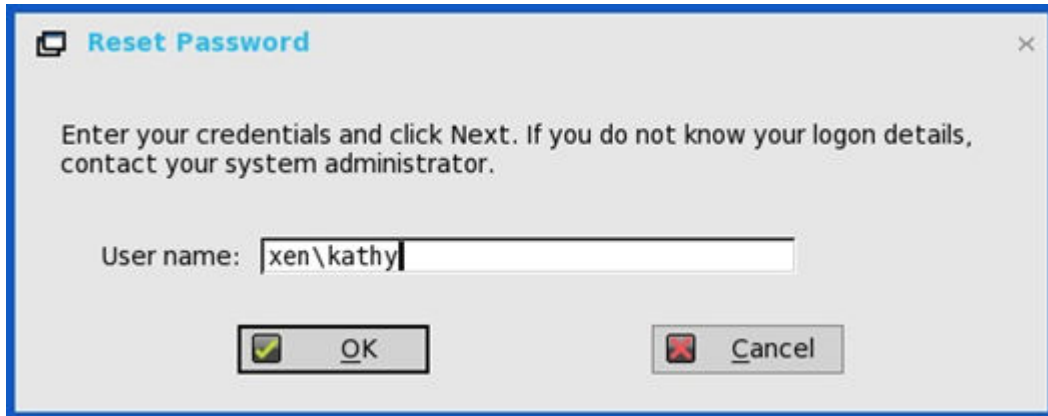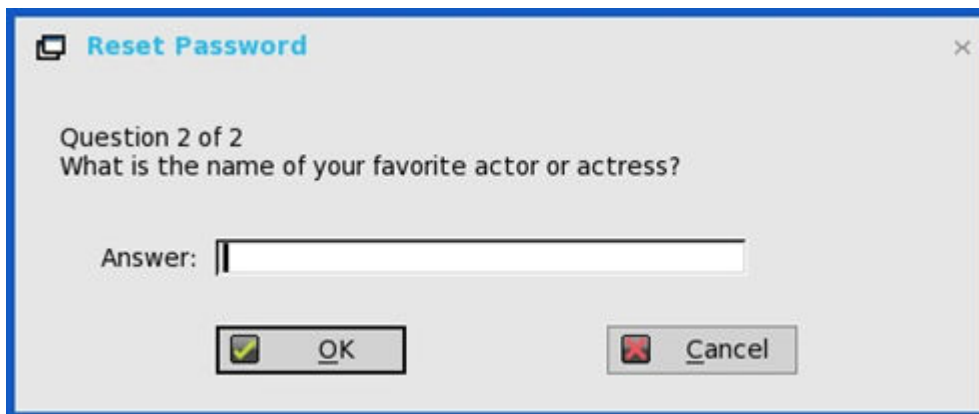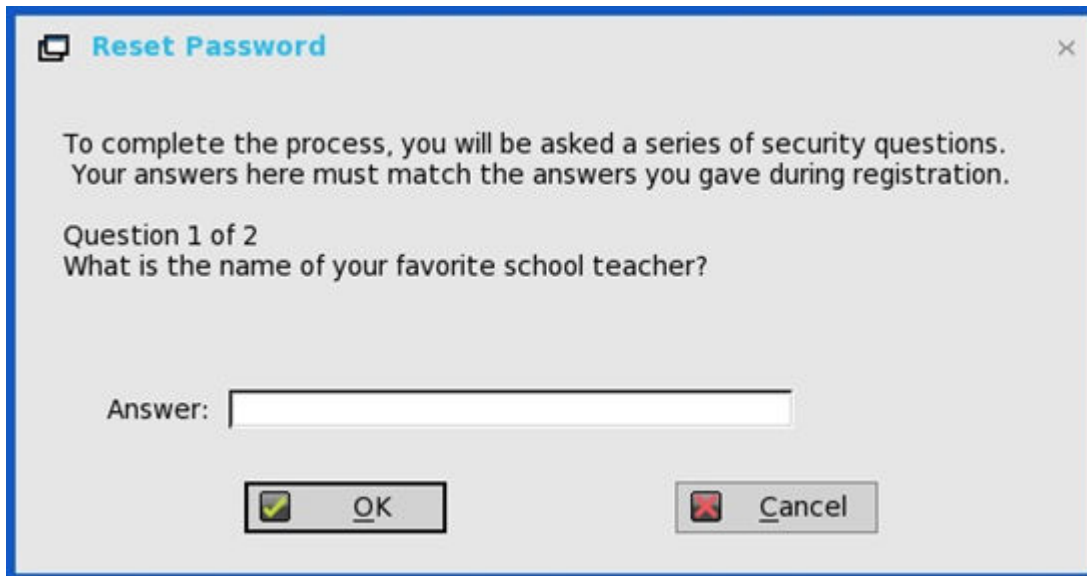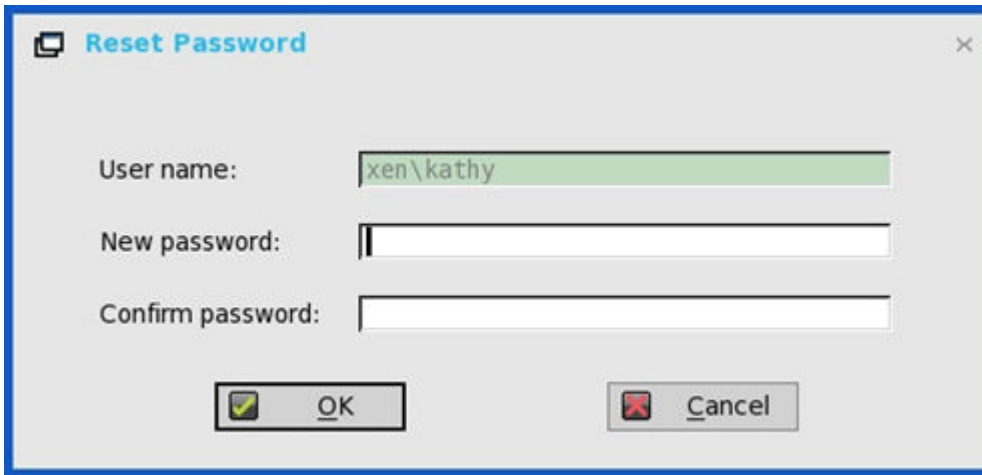
4   Enter and confirm the new password.

5   Click **OK** to successfully change the password.
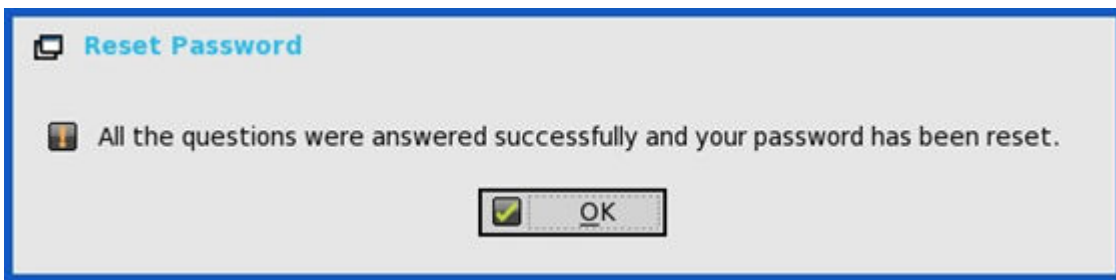
ⓘ **NOTE:**

If you provide the wrong answers, you can not reset the password, and an error message is displayed.

Changing display settings dynamically

From ThinOS 8.4 release, after you change the display settings, the changes will take effect immediately without a system restart.

Single mode user scenario

Go to **System Setup** > **Display** > **General**, and do the following:

1   Change resolution from DDC table or User defined display settings.

2   Change rotation setting from User defined display settings.

When the display settings are changed, the modified settings are applied to the active sessions dynamically. But some of the active sessions disconnect and then reconnect. For example, RDP for Win7 session.

Dual Head user scenario

Go to **System Setup** > **Display** > **Dual Head** and change the settings.

Go to **System Setup** > **Display** > **General**, and do the following:

1   Change resolution from DDC table or User defined display settings.

2   Change rotation setting from User defined display settings.

When the display settings are changed during active sessions, the active sessions do not resize dynamically in the following situations:

- Seamless sessions
- For dual head mode, including:

    - Change from single mode to dual head.
    - Change from dual head to single mode.
    - Change display setting in dual head mode.

To apply the settings, disconnect the session and reconnect it.

QUMU/ ICA Multimedia URL Redirection

QUMU utilizes ICA Multimedia URL Redirection. You are required to install a browser plug-in for this feature to work.

In earlier ThinOS releases, ICA Multimedia URL Redirection was partially supported. In ThinOS 8.4 release, a few enhancements are made to ICA multimedia URL redirection for better performance.

Supported protocols:

- RTPS HLS
- HTTP

Verifying QUMU Multimedia URL Redirection: While the video is playing, a noticeable lag or jump in the video window is observed when you move the browser on the screen or scroll the browser. This behavior indicates that the video is being redirected.

To view the video sample, go to Kickoffdemo75.qumu.com/viewerportal/qumu/home.vp.

HTML5 Video Redirection

HTML5 Video Redirection controls and optimizes the way XenApp and XenDesktop servers deliver HTML5 multimedia web content to users. From XenApp and XenDesktop 7.12, this feature is available for internal web pages only. It requires the addition of JavaScript to the web pages where the HTML5 multimedia content is available, for example, videos on an internal training site.

The following server policies must be enabled:

- Windows Media redirection—By default this option is enabled.
- HTML5 video redirection—By default this option is disabled.

Verifying HTML5 Video Redirection: While the video is playing, a noticeable lag or jump in the video window is observed when you move the browser on the screen or scroll the browser. This behavior indicates that the video is being redirected.

ThinOS event log for RAVE MMR is also displayed.

Sometimes, the initial playback does not work. After several seconds, the video is refreshed automatically, and you need to click playback from start again. During this time, the video will redirect.

Reference documents

- Citrix sample video—Citrix.com/virtualization/hdx/html5-redirect.html.
- ICA Multimedia policy settings——–Docs.citrix.com/en-us/xenapp-and-xendesktop/7-12/policies/reference/ica-policy-settings/multimedia-policy-settings.html.

Citrix HDX RealTime optimization pack 2.2

Support for Citrix RealTime Multimedia Engine (RTME) is updated to latest version 2.2.100.949.

Salient features

- Call Admission Control support
- DSCP/ QoS Configuration
- Ability to turn off version mismatch warnings for acceptable combinations of RealTime Connector and RealTime Media Engine.

In RTME 2.2 version, USB Video Class (UVC) 1.1 and 1.5 Camera hardware encoding / H.264 (CAM) are supported. This feature is applicable for qualified cameras only, for example Logitech C930e.

In the **Call Statistics** window, `Video Codec=H.264(CAM)` is displayed for P2P RTME video call in the **Sent** column.

For group calls with standard SFB, the call statistics displays `Video Codec=H.264-UC(CAM)` in the **Sent** column. This improves video call quality/resolution compared to Video Codec H.264 (SW); for example, P2P video call resolution upgrade from 480 x 270 to 640 x 360.

Guidelines for RTME testing and evaluation

- Best to test calls between similar ThinOS hardware for affirmative results
- Citrix certificate program advises that you check macro blocks score to determine the device capability. Only qualified devices can be tagged as HDX Premium. For more information, see, Citrix documentation.
- If you find any issues, then collect data as shown in the following example:

Test Endpoints #	Test Endpoints #1	Test Endpoints #2
Endpoint Model	Wyse 3030 LT thin client	Wyse 5060 thin client
Endpoint OS and so on.	ThinOS 8.4_005	ThinOS 8.4_005
Display resolution	Single 1920 x 1080	Single 2560 x 1440
USB headset	Plantronics C310	Sennheiser SC70
USB webcam	Logitech C930e	Logitech C930e
XD/XA version	7.12	7.12
VDA OS and so on.	Win 2016	Win10 x64
Policy if any	Not applicable	Not applicable
Network condition	Wired 1000 FX	Wired 1000 FX
RT Connector version	2.2.0.837	2.2.0.837
RTME version	2.2.0.837	2.2.0.837
Video FPS	30.04	30.04
Video resolution	640 x 360	640 x 360
Limited by	CPU speed	CPU speed
Video Codec	Sent: H.264 (CAM) Received: H.264 (SW)	Sent: H.264 (CAM) Received: H.264 (SW)
Audio Codec	G.722.1C*	G.722.1C*

Test Endpoints #	Test Endpoints #1	Test Endpoints #2
Average Data Sent	851	842
Average Data Received	873	827

WDM and CCM updates

Dell Wyse Device Manager (WDM)—ThinOS v8.4 release is compatible with WCM (Dell Wyse Configuration Manager) v1.6. In **WDM** tab of ThinOS, new settings are available for WDM v5.7.2. For more information regarding the settings, see, Dell Wyse ThinOS 8.4 Administrator's Guide, available at Dell.com/manuals.

Dell Cloud Client Manager (CCM)—Add INI parameter to configure WDA rediscovery interval and ignore MQTT connection. For more information, see Dell Wyse 8.4 INI Reference Guide, available at Dell.com/manuals.

INI parameters

The ThinOS v8.4 release contains the following newly added INI parameters:

ⓘ **NOTE: The new INI parameters added in this release are bold faced and the default values are underlined.**

Table 4. INI parameters

Reference	Description	
AutoLoad= {0, 1, 2, 101, 102, 201, 202} **[VerifySignature= {yes, no}]**	**Value**	**Action**
	0	Disable checking for image
	1 (default)	Enable a forced firmware upgrade/ downgrade process.
	2	Enable a comparison/non-forced upgrade only process.
	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.

Reference	Description
	<table><tr><td>202</td><td>Enables firmware upgrade only, but displays a window with OK button before the process; displays a status complete window.</td></tr></table>
	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 the firmware and/or packages can happen, which do not support signature. The default value is yes.
SessionConfig=ICA [TosDscp={Default/CS1/CS2/CS3/CS4/CS5/CS6/CS7/AF11/ AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/AF43/**EF**}	SessionConfig — Specifies the ICA default settings of the optional connection parameters for all ICA sessions. TosDscp — Sets IP DSCP in the TOS fields. For more information, see *TOS_Priority_settings.docx*.
SessionConfig=RDP[TosDscp={Default/CS1/CS2/CS3/CS4/CS5/ CS6/CS7/AF11/AF12/AF13/AF22/AF23/AF31/AF32/AF33/AF42/ AF43/**EF**}]	Set RDP to establish the default setting for RDP sessions. The option "TosDscp" can set IP DSCP in the TOS fields. (CIR 64478). For more information, see *TOS_Priority_settings.docx*.
[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.(CIR 67616) For more information, see *TOS_Priority_settings.docx*.
SignOn= {<u>yes</u>, no, NTLM} **[RequireSmartCard = {yes or force, <u>optional</u>, no}]** **[SignonStatusColor="rrr ggg bbb"]**	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 username.ini must be available in the directory. A WINS server is required by NTLM protocol also. **RequireSmartCard—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.** **Default value is optional.** **SignonStatusColor—The optional keyword SignonStatusColor 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.**
**ScepAutoEnroll = { yes	<u>no</u> }** **AutoRew = { yes	<u>no</u> }** **InstallCACert = { yes	<u>no</u> }** **[CountryName = country]** **[State = state]** **[Location = location]**	**ScepAutoEnroll—This option is to allow client automatically get certificates and renew certificates using SCEP protocol. Configure ScepAutoEnroll to yes to enable client's functionality to auto get certificate.** **AutoRew—Configure AutoRew 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.**

Reference	Description
[Organization = organization_name] [OrganizationUnit = organization_unit] [CommonName = common_name] [Email = email_address] KeyUsage = kay_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]	InstallCACert—Configure InstallCACert to yes to install the root CA's certificate as trusted certificate after successfully getting a client certificate. CountryName, State, Location, Organization, OrganizationUnit, CommonName, Email—These fields 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—KeyUsage is to specify key usage of the client certificate and should be set to a digitalSignature, keyEncypherment or both using a ';' linking these two as digitalSignature;keyEncypherment. KeyLength—KeyLength is to specify the key length of the client certificate in bits, must one of the value in the list. subAltName—subAltName 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—RequestURL is to specify the SCEP server's service URL. This field must be set correctly. CACertHashType—CACertHashType is the hash type used to verify certificate authority's certificate. CACertHash—CACertHash 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, EnrollPwdEnc—EnrollPwd or EnrollPwdEnc is 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 a 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 tries to use these set of settings to automatically get an enrollment password and then use that password to request a certificate. Use ScepAutoEnroll=no AutoRenew=yes to only enable SCEP auto renew; all others parameters are not needed if ScepAutoEnroll is set to no. (i) NOTE: SCEP server's URL must be an HTTP link. Do not add protocol prefix to RequestURL and ScepAdminURL.
DefaultUser = {username, $SYS_VAR}	Specifies the default sign-on user. For more information, see *Dell Wyse ThinOS 8.4 Administrator's Guide.*

DELL

Reference	Description
[Display = {yes, <u>no</u>}]	**Display—If 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 (*).**
CCMEnable = {yes, <u>no</u>} **[IgnoreMqtt = (yes, <u>no</u>)]** [CCMServer=server_address[:port]]	CCMEnable — Yes/no option to enable the Cloud Client Manager Agent. It specifies an IP address or URL address for the CCM server. Default port is 80. Once specified, it is saved in the non-volatile memory. **IgnoreMqtt—If IgnoreMqtt=yes is specified, CCM agent will not connect to MQTT server. Default value is no.** CCMServer — Specifies an 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**
WDAService= <u>yes</u> **[interval = {0-65535}]** **[disableNotice={yes, <u>no</u>}]** **[disableCancel={yes, <u>no</u>}]** **[noticeTime={0-255}]**	WDA Service always runs in the background. If priority is available, WDA discovers the protocol according to it. **interval—If interval is available, WDA rediscovery delay after a failed check-in (both CCM and WDM failed) is changed to interval minutes. The default value is 0. (WDA rediscovery delay is 24 hours).** **For example, if you set WDAService=yes interval=30, WDA rediscovery delay is set as 30 minutes.** **disableNotice—If option is set to yes, then count down prompt will not show when configuration from WDM is received. The default value is no.** **disableCancel—If option is set to yes, there is no possibility to cancel count down prompt for WDM (device is going to reboot).** **noticeTime—If noticeTime is available, the time of countdown prompt is changed to seconds. Default value is 20.** **For example: 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).**
ScreenSaver=value	<table><tr><td>**Value**</td><td>**Delay Before Starting**</td></tr><tr><td>0</td><td>Disabled</td></tr><tr><td>1</td><td>1 Minute</td></tr><tr><td>**3**</td><td>**3 Minutes**</td></tr><tr><td>5</td><td>5 Minutes</td></tr><tr><td>10</td><td>10 Minutes</td></tr><tr><td>15</td><td>15 Minutes</td></tr></table>

Reference	Description	
PRIVILEGE=[None, Low, <u>High</u>] **[EnablePeripherals={keyboard,mouse,audio,serial,camera,touchscreen,bluetooth}]**	Controls operator access to Thin Appliance resources:	
	Parameter	**Operator Privileges**
	None	The **System Setup** selection on the desktop menu is disabled. The **Setup** submenu cannot be displayed. The **Connect Manager, Dialup Manager and PPTP manager** dialog boxes are disabled. The Reset to Factory default checkbox in the Shutdown dialog window is not available
	Low	The **Network and Wireless** selections on the **Setup** submenu are disabled (grayed out). The **Connection Settings** dialog box (opened from **Connect Manager**) is readable but not writable. The Reset to Factory default checkbox in the Shutdown dialog window is disabled.
	<u>High</u> (default)	No restrictions; all thin appliance resources are available.
	EnablePeripherals—If the optional keyword 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.	
ConnectionBroker={default, VMware, Microsoft, Quest, AWS} **[RDCollections={*collect1, collect2,...}]** **[DisableShowDisclaimer=[yes, no]** **[DisableShowServer=[yes, no]** [ConnectionType={Default, All, RDP, PCoIP, **Blast**}]	**RDCollections—The option specifies the collections for Microsoft RD broker. Only the applications/ 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, then all the applications/ desktops are displayed.** **Do the following to get your RemoteApp or Desktops collection name:** 1 **In RDS Server local, go to C:\Users\administrator.RDSS \AppData\Roaming\Microsoft\Workspaces\{xxxx} \Resource, 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]".**	

Reference	Description
	DisableShowDisclaimer—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—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.**
DHCPOptionsRemap={yes, <u>no</u>} [WDMServer={128-254}] [WDMSecurePort={128-254}] [WDMFQDN={128-254}] [CCMGroupKey={128-254}] [CCMServer={128-254}] [CCMMQTTServer={128-254}] [CCMCAValidation[]={128-254}]	If DHCPOptionsRemap=yes, the following parameters can be set. The options value must be between 128 and 254. Each value must be different. These options are used to configure DHCP server tags for WTOS booting. **WDMServer (186) specifies ip address of WDM server.** **WDMServer (192) specifies HTTP port of WDM server.** WDMSecurePort (**190**) specifies HTTPS port of WDM server. WDMFQDN (**194**) specifies the FQDN of WDM server. CCMGroupKey (**199**), CCMServer (**165**), CCMMQTTServer (**166**) and CCMCAValidation (**167**) specify to remap the tags for CCM configuration.
DNSIPVersion={<u>ipv4</u>, ipv6} **[Combined={yes, <u>no</u>}]**	Specify the DNS server and domain. Default IP version is ipv4. **Combined—If option is set to yes, the DNS server will combine the DNS server configured by DHCP and the static one, the DNS domain will use the value configured by DHCP in case of static DNS domain is empty.**
Dualhead={yes, <u>no</u>} **[EnsureDpIsOn ={yes, no}]**	For V-class, C-class, R-class, D-class and X10J/T-class, set to yes to support dual-monitor. **EnsureDpIsOn—The optional keyword is only used for D-class. When EnsureDpIsOn is set to yes, D-class will halt at boot time until DP monitor is plugged in.**
CaradigmServer=vip list **[DisableManualLogon=yes, no]**	A list of VIP addresses with optional TCP port number of Caradigm servers. **DisableManualLogon—The option 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.**
INACTIVE=minutes **[LockTimer=seconds]**	**LockTimer—If the option is set, then 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.**
OneSignServer=onesign_server [AutoAccess={VMW, XD, XA, LOCAL, **RDSHD, RDSHA, RDSHPC**}]	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. **From ThinOS version 8.3_109, ThinOS supports OneSign 5.2 RDSH broker. Set AutoAccess=RDSHD or RDSHA to auto**

Reference	Description
	launch Microsoft type broker. Set RDSHPC to automatically launch the RDP session without broker.

Troubleshooting

- The **base.i386** and **pcoip.i386** packages may not be available on devices:
  - Shipped with ThinOS version 8.4
  - Reimaged with a ThinOS version 8.4 Merlin image using USB imaging tool

Table 5. Affected platforms

Affected platforms	Flash size
Wyse 5010 thin client with ThinOS	4 GB or higher
Wyse 5040 thin client with ThinOS	4 GB or higher
Wyse 7010 thin client with ThinOS	4 GB or higher
Wyse 5010 thin client with PCoIP	4 GB or higher
Wyse 5040 thin client with PCoIP	4 GB or higher

ⓘ **NOTE: Devices with 2 GB flash are not affected by the package issue.**

Problem statement—The following issues are observed on the affected platforms:

- Multimedia performance issues occur because the required codecs are not available.
- PCoIP connections are not started in Horizon View and AWS environments.
- **Package** tab is not available in the **System Tools** menu.

Resolution—Perform one of the following steps to resolve the issue on the affected devices:

- Use the 4 GB Merlin image to flash the devices with 4 GB flash configuration. Use the 8 GB Merlin image to flash the devices with 8 GB and 16 GB flash configurations.
- Install the ThinOS web image (8.4_112 Hot Fix or later) to reload the missing package files. You must install the ThinOS web image by using either a file server, Wyse Device Manager (WDM), or Wyse Management Suite. If the ThinOS web image is stored on a file server or management server, and if the automatic image update option is enabled using the INI parameter `Autoload=1 LoadPkg=1`, then the device automatically installs the **base.i386** and **pcoip.i386** packages during system reboot.
- If you get **signature error** when downgrading from version 8.4 to 8.3, set "`verifysignature`" parameter. For more information about this parameter, see Dell Wyse ThinOS 8.4 INI Reference Guide, available at Dell.com/manuals.
- If you can log in to View Broker, but cannot launch the Blast session, then verify if the Blast pkg is installed on the client. In addition, set the correct DNS server on the **Network step** page.

Fixed issue

None

Known issue

When you upgrade to ThinOS 8.4 using the file server, for example, on Wyse 3040 thin client or Wyse 5060 thin client devices, some existing configuration, such as certificate files for file server/broker, or the wireless/WDM/CCM configuration, if any, may be lost.

Workaround—Use the file server without certificate, and make sure all configurations are available using file server. For example, using INI parameter to install certificate, configure broker/WDM/CCM/wireless and so on.

Testing environment

The following tables display the testing environment for the respective attributes:

CCM	3.0
WDM	5.7.2
Imprivata	5.2.0.15
Caradigm	6.3.1.17
NetScaler	9.3/10.0/10.1/10.5/11.0/11.1
Store Front	2.6/3.6/3.8/3.9
Web Interface	5.4
SecureMatrix	4.1.0

	Win 7	Win 8.1	Win 10	Linux	W2K8R2	W2K12R2	W2K16	APPs
VMware Horizon 7.0/7.1	√	√	√	√	√	√	√	√
XenDesktop 5.6	√							
XenApp 6.5					√			√
XenDesktop/XenApp 7.6	√	√		RedHat 6.6	√	√		√
XenDesktop/XenApp 7.12	√	√	√		√	√	√	√
XenDesktop/XenApp 7.13	√	√	√		√	√	√	√
Amazon WorkSpaces 1.03	√ *							
RDS 2012 R2	√	√	√			√	√	√
RDS 2016							√	√

*AWS Workspace VM OS Windows 7 style is actually based on 2008 R2 RDSH.

XenDesktop/ XenApp	Operating System	RTME	Lync client	Lync server	Skype for Business (SFB) server
6.5	W2K8R2	1.8	Lync 2010	Lync 2013	
7.6	Win 8.1	1.8	Lync 2013	Lync 2013	
	W2K12	2.2	SFB 2015		SFB 2015
7.12	Win 8.1	2.2	SFB 2016		SFB 2015
	Win 10	2.2	SFB 2016		SFB 2015

XenDesktop/ XenApp	Operating System	RTME	Lync client	Lync server	Skype for Business (SFB) server
	W2K16	2.2	SFB 2015		SFB 2015

Peripherals list

This section lists the supported peripheral devices and peripheral eco system.

Table 6. Peripheral devices

Keyboard/ Mouse
Dell KM636 Wireless Keyboard and Mouse
DELL Wireless Keyboard/ Mouse KM632
DELL Wireless Keyboard/ Mouse KM714
Dell Keyboard KB216p / Mouse MS-116p
Dell Mouse MS111-P
Dell Keyboard KB113p
Dell Keyboard KB212-B
Thinkpad Compact Bluetooth Keyboard
Rapoo E6100, Bluetooth
Dell Optical Wireless Mouse – WM123
Dell Wireless Bluetooth Travel Mouse – WM524
Dell WM713 Bluetooth
SpaceNavigator 3D Space Mouse
Logitech K480 Keyboard, Bluetooth
Logitech K400 Plus
Microsoft Arc Touch Mouse 1428
Logitech M557 mouse, Bluetooth
USB Webcam
Logitech C920 HD Pro Webcam
Logitech C930e HD Webcam
Logitech C270 HD Webcam

Logitech BCC950 Conference Camera
Logitech C525 HD Webcam
Logitech USB Webcam 9000
Microsoft LifeCam 3.0 Cinema
Microsoft LifeCam HD-3000
Microsoft LifeCam Studio
Printer
Dell B1265dnf Multifunction Laser Printer
Dell B1165nfw Mono Multifunction Printer
Dell B1163 Mono Multifunction Printer
Dell B2375dnf Mono Laser Multifunction Printer
Dell B2360d Laser Printer
Dell B2360dn Laser Printer
Dell B1260dn Laser Printer
HP LaserJet P2055d
HP LaserJet P2035
EPSON PLQ-20K
HP Color LaserJet CM1312MFP
Mobile device
iPhone 6
HTC one-XL
USB Disk
SanDisk Extreme USB 3.0 16G
SanDisk Cruzer 8 GB
SanDisk USB 3.0 16 GB
Kingston DataTraveler 100 G3
Kingston DataTraveler G3 32 GB
Kingston DTM30 32 GB

Kingston Mini Fun 8 GB
ADATA S107 USB 3.0 16 GB
ADATA S102/ 16 GB
ADATA UV150 USB 3.0 16 GB
PNY USB3.0 16 GB
Sony N50 16 GB
USB Headset
Jabra PRO 9450
SanDisk Extreme USB 3.0 16 GB
Jabra Speak 510 MS, Bluetooth
Jabra PRO 9400BS, Bluetooth
Jabra PRO 935 MS
Jabra UC Voice 550 MS Duo
Jabra BIZ 2300 Duo, USB, MS
Jabra PRO 9400BS, Bluetooth
Jabra UC Voice 750MS Duo Drk
Plantronics BLACKWIRE C310-M, Lync
Plantronics BLACKWIRE C420
Plantronics BLACKWIRE C435-M
Plantronics BLACKWIRE C610
Plantronics BLACKWIRE C710, Bluetooth
Plantronics Voyager Legend UC B235 NA, Bluetooth
Plantronics DA45
Plantronics SupraPlus HW251N
Plantronics DA60
Plantronics P420
Plantronics W440, SAVI, CONVERTIBLE, DECT 6.0 (D100)
Plantronics Calisto P240 D1K3 USB Handset

Plantronics Calisto 620 M, Bluetooth
Plantronics USB DSP DA40(B)
Plantronics 655 DSP
Plantronics List Savi 400 series
SENNHEISER SC 70 USB MS BLACK Binaural UC Headset
SENNHEISER SC 660 Binaural CC&O HS, ED
SENNHEISER SC 260 USB MS II
SENNHEISER SP 10 ML Speakerphone for Lync
SENNHEISER D 10 USB ML-US Wireless DECT Headset
POLYCOM Deskphone CX300
EDIFIER
Monitor
Dell E2416Hb—1920 x 1080
Dell UP3216Qt—3480 x 2160
Dell P2714Hc—1920 x 1080
Dell E2715Hf—1920 x 1080
Dell UZ2315H—1920 x 1080
Dell P4317Qc—3480 x 2160
Dell D2215Hc—1920 x 1080
Dell U2414HB—1920 x 1080
Dell P4317Qc—3480 x 2160
Dell U2415—1920 x 1200
Dell U2412M—1920 x 1200
Dell U2913 WM—2560 x 1080
Dell U2713Hb—2560 x 1440
Dell U2713HM—2560 x 1440
Dell U2713HMt—2560 x 1440
Dell P2815Qf—3840 x 2160

Dell ST2420L—1920 x 1080
Dell 3008WFP—2560 x 1600
Dell U3014t—2560 x 1600
Dell P2715Q—3840 x 2160
DVD ROM
BENQ DVD Drive
Samsung Portable DVD Writer SE-208
Dell DW514
SPEECHMIKE PREMIUM
LFH3610/00
LFH3200/00
LFH3210/00
Cable/Converter
Dell USB Sound Bar AC511
Elo Touch Screen USB
Elo Touch Screen Serial
USB-to-Serial converter U232-P9 V2
Dell DP-VGA Adapter Module: DANBNBC084
Dell DP-DVI Adapter Module: DANARBC084
Dell KDP70 Adapter converts DisplayPort to DVI Module: DANASBC084
Smart card Reader
Dell Keyboard SK-3205—Smart card reader
Dell Keyboard M/N KB813—Smart card reader
OMNIKEY OK Card Man 3121
SmartOS Powered SCR335
HID OMNIKEY 3021
HID OMNIKEY 3121

HID OMNIKEY 5125
HID OMNIKEY 5421
HID OMNIKEY 5325 CL
Gemalto ID Bridge CT710
Cherry Keyboard RS 6600 with Smart card
Cherry Keyboard RS 6700 with Smart card
Cherry Keyboard KC 1000 SC with Smart card
Smart card
Etoken 72K—USB key
Etoken 72K no Java
Etoken 72K Java
Etoken 64K—USB key
Etoken safenet 5100 Java 72k—USB key
Etoken safenet 5110 Java 80k—USB key
ActivIdentity V2
ActivIdentity V1
Gemalto .net V2+
Gemalto ID Prime MD 3810 for TC
Gemalto ID Prime MD 830 for TC
Gemalto ID Prime MD 830 BL2
Gemalto ID Prime MD 830 BL3
Gemalto ID Prime MD 840
Yubico yubikey 4
Cryptovision—Startcus 3.2
SafeSign—Startcus 3.0
SafeSign—Startcus 3.2
Gemalto ID Prime.NET
SiPR

SafeNet SC650
Oberthur ID One 128 v5.5
G&D FIPS 201 SCE 3.2
Gemalto TOPDLGX4 144
Proximity Card Reader
RDR-80581AKU
RDR-80582AKU
RDR-6082AKU
Proximity Card
Card 1: ID 4E3C398E
Card 2: ID 016FE691
Card 3: ID 016B4CAA
Card 4: ID E012FFF8007AA7F8
Finger Print Reader
Finger Print Keyboard ET710
OMNIKEY Reader
OMNIKEY 5025 CL
OMNIKEY 5125
OMNIKEY 5325 CL
OMNIKEY 5326 DFR
OMINIKEY 5427 CK

Table 7. Peripheral eco system

Type	Product
Audio	Dell Pro Stereo Headset UC300 - Lync Certified
Audio	Jabra Pro 935 MS Wireless headset (Mono) - Office Centric
Monitors	Dell 23 Monitor- E2316H
Monitors	Dell 22 Monitor - E2216H
Monitors	Dell 20 Monitor - E2016

Type	Product
Monitors	Dell 24 Monitor - E2417H
Monitors	Dell 19 Monitor - E1916H
Monitors	Dell 20 Monitor - P2016
Monitors	Dell 24 Monitor - P2417H
Monitors	Dell 23 Monitor - P2317H
Monitors	Dell 22 Monitor - P2217H
Monitors	Dell 20 Monitor - P2017H
Monitors	Dell 19 Monitor - P1917S
Monitors	Dell 24 Monitor – U2415
Input devices	Dell USB Wired Keyboard with Smart Card reader - KB813
Input devices	Dell Wireless Keyboard and Mouse - KM636
Input devices	Dell USB Wired Keyboard - KB216
Input devices	Dell Laser USB mouse (Silver & Black) - Naruto
Input devices	Dell USB Wired Optical Mouse - MS116
Printers	Dell Mono Unmanaged Printer - E515dn
Printers	Dell Color Unmanaged Printer - E525w
Printers	Dell Mono Managed Printer - C2660dn