Dell Wyse ThinOS 2303, 2211, 2208, and 2205

Release Notes

March 2023
Rev. A18

Notes, cautions, and warnings

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

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

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

Contents

1

Overview

Dell Wyse ThinOS software is designed to run on a broad array of Dell 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.

Version matrix

The following version matrix lists the platforms supported in each Dell Wyse ThinOS release, and helps you select which version of ThinOS software or ThinOS application package is appropriate for your work environment.

Table 1. Version Matrix

Release version	Release date	Supported platforms	Release Notes
ThinOS 2303 (9.4.1141)	March 2023	• Wyse 3040 Thin Client • Wyse 5070 Thin Client • Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • OptiPlex 3000 Thin Client • Latitude 3420 • OptiPlex 5400 All-in-One • Latitude 3440 • Latitude 5440 • OptiPlex All-in-One 7410	ThinOS 2303

Table 2. Version Matrix

Application package versions	Release date	Supported platforms	Release Notes
Security package for ThinOS 2211	January 2023	• Wyse 3040 Thin Client • Wyse 5070 Thin Client • Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • OptiPlex 3000 Thin Client • Latitude 3420 • Dell OptiPlex 5400 All-in-One	Security Package for ThinOS 2211
ThinOS 2211 (9.3.3099)	December 2022	• Wyse 3040 Thin Client • Wyse 5070 Thin Client • Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • OptiPlex 3000 Thin Client • Latitude 3420 • Dell OptiPlex 5400 All-in-One	ThinOS 2211
ThinOS 2208 (9.3.2102)	August 2022	• Wyse 3040 Thin Client • Wyse 5070 Thin Client • Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • OptiPlex 3000 Thin Client • Latitude 3420 • Dell OptiPlex 5400 All-in-One	ThinOS 2208
Citrix Workspace App 2205, Webex Meetings VDI 42.8 (special release based on 42.6), Webex VDI 42.4,	July 2022	• Wyse 3040 Thin Client • Wyse 5070 Thin Client • Wyse 5470 Thin Client	Citrix Workspace App 2205, WebEx Meetings VDI 42.8, Webex VDI 42.4, Zoom 5.10.2, and Imprivata 7.8 packages for ThinOS 2205

Table 2. Version Matrix (continued)

Application package versions	Release date	Supported platforms	Release Notes
Zoom 5.10.2, and Imprivata 7.8 packages for ThinOS 2205		Wyse 5470 All-in-One Thin Client OptiPlex 3000 Thin Client Latitude 3420	
Security package for ThinOS 2205	June 2022	Wyse 3040 Thin Client Wyse 5070 Thin Client Wyse 5470 Thin Client Wyse 5470 All-in-One Thin Client OptiPlex 3000 Thin Client Latitude 3420	Security package for ThinOS 2205
Cisco Webex Meetings VDI 42.2.8.5	June 2022	Wyse 3040 Thin Client Wyse 5070 Thin Client Wyse 5470 Thin Client Wyse 5470 All-in-One Thin Client OptiPlex 3000 Thin Client Latitude 3420	Cisco Webex Meetings VDI 42.2.8.5

Table 3. Version Matrix

Release version	Release date	Supported platforms	Release Notes
ThinOS 2205 (9.3.1129)	May 2022	Wyse 3040 Thin Client Wyse 5070 Thin Client Wyse 5470 Thin Client Wyse 5470 All-in-One Thin Client OptiPlex 3000 Thin Client Latitude 3420	ThinOS 2205

ThinOS 2303

Release date

March 2023

Release summary

Patches or Add-on releases are created to support existing platforms or software releases, correct defects, make enhancements, or add minor features.

Current version

ThinOS 2303 (9.4.1141)

Previous version

ThinOS 2211 (9.3.3099)

Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2303 (9.4.1141)**

ⓘ **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2303. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.

ⓘ **NOTE:** If you want to downgrade ThinOS 2303 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2303 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

- To further improve the security of ThinOS devices, TLS 1.0 and 1.1 have been removed in ThinOS 2303. If your network or VDI environments still require TLS 1.0 or 1.1, use ThinOS 2211 or earlier versions until you have updated your environment.
- If you get the error **Could not add account. Please check your account and try again.** when logging in to Citrix or **Login failed!** when logging in to VMware, check whether TLS 1.0 or TLS 1.1 is required by your Citrix or VMware Broker agent to log in.
- If you get a wired IEEE802.1x authentication or wireless authentication failure, check whether your network environments require TLS 1.0 or 1.1.
- It is recommended changing the default BIOS password to increase the security posture of your devices.
- There are chances that after the upgrade, the device displays a black screen. You may reboot the device to boot it up correctly.
- From ThinOS 2303, if the thin client is registered in Wyse Management Suite group 1 and you set the Wyse Management Suite group 2 token in group 1 policy, a dialog box is displayed to change the group. Click **Cancel** to change to group 2 immediately. Click **Restart Now** or wait for the 60-second countdown to finish and then reboot to change to group 2.

- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
  - Not display a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - Not display any notification if the new firmware or application is downloaded in the same group.
  - Installs the firmware or package after a reboot.
- If you have installed HID_Fingerprint_Reader package, ensure that you have also installed Citrix_Workspace_App package, or you cannot upgrade to ThinOS version 2303.
- If you configure settings, like brokers, locally in ThinOS 2303 and downgrade to ThinOS 2205 or earlier versions using Wyse Management Suite, the settings are lost.
- If you downgrade to ThinOS 2205 or earlier versions using Wyse Management Suite, reboot the system manually again to set a password locally in ThinOS. Otherwise, passwords, like the broker login password, gets corrupted when rebooting for the first time after downgrading.

Prerequisites for firmware upgrade

- Before you upgrade from ThinOS 9.1.x to ThinOS 2303, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the Wake On LAN command through Wyse Management Suite before using any real-time commands. To use the Wake On LAN command, ensure that the **Wake On LAN** option is enabled in BIOS.

Upgrade from ThinOS 9.1.x to ThinOS 2303 using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the ThinOS 2303 (9.4.1141) firmware to upgrade.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**. The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **OS Firmware Updates**.

   NOTE: If you cannot locate the **OS Firmware Updates** option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse** and select the **ThinOS 9.x** firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.
   The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

   NOTE: There are chances that the upgrade might fail with event log stating **Failed to install**. In such an event, you may reboot the device and upgrade again.

   NOTE: After upgrading to ThinOS 2303, all application packages released prior to ThinOS 2205 are removed automatically. You must install the latest application packages.

   NOTE: There are chances that the ThinOS background might be in blue color and some features may not work. In this case, you have to reboot the device.

Convert Ubuntu with DCA to ThinOS 2303

Prerequisites

Table 4. Supported conversion scenarios

Platform	Ubuntu version	DCA-Enabler version
Latitude 3420	20.04	1.5.0-14 or later
OptiPlex 5400 All-in-One	20.04	1.5.0-14 or later
Latitude 3440	22.04	1.7.0-20 or later
Latitude 5440	22.04	1.7.0-20 or later
OptiPlex All-in-One 7410	22.04	1.7.0-20 or later

Ensure that DCA-Enabler is installed on your Ubuntu devices according to above table. For details on how to install DCA-Enabler in Ubuntu operating system and upgrade it, see *Dell Wyse ThinOS Migration Guide* at www.dell.com/support

- The device must have a factory-installed Ubuntu operating system. If you have custom installed the Ubuntu operating system, you cannot convert it to ThinOS 2303.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2303.
- Ensure that you have connected the device to the external power source using the power adapter.
- Ensure you have enough ThinOS Activation devices licenses on Wyse Management Suite 4.0 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than the device number. If it is not larger, you cannot create the Advanced Policy for conversion.
- The Ubuntu devices must be registered to Wyse Management Suite as generic clients. For details on how to register the generic client to Wyse Management Suite, see *Dell Wyse ThinOS Migration Guide* at www.dell.com/support.
- Ensure you have downloaded the Ubuntu to ThinOS 2303 conversion image.
- Extract the Ubuntu to ThinOS 2303 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.2-dtos0-amd64_signed.tar.gz` and ThinOS image `ThinOS_2303_9.4.1141.pkg`.

  ⓘ **NOTE:** The ThinOS image `ThinOS_2303_9.4.1141.pkg` can be used for downgrade in the future.

Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the Conversion Installer file `DTOS_Ubuntu_Installer_1.2-dtos0-amd64_signed.tar.gz`
3. Go to **Apps & Data** > **OS Image Repository** > **ThinOS 9.x**, and click **Add Firmware file**.
4. Upload the ThinOS image `ThinOS_2303_9.4.1141.pkg`.
5. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
6. Enter the policy name, select the group in which the Ubuntu devices have been registered, and select **Generic Client** as OS type.
7. Click **Add app**, and select the conversion installer file that was uploaded before from the drop-down menu.
8. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
9. Select the platforms you want to convert in the **Platform Filter** drop-down menu.
10. Click **Save**.

    ⓘ **NOTE:** Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
11. In the next window, click **Yes** to schedule a job.
12. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.
13. Click **Schedule**.

    The Conversion Installer file downloads and installs first followed by the ThinOS image. After installation, the device restarts automatically.

    ⓘ **NOTE:** After you register the converted ThinOS device to Wyse Management Suite, the ThinOS activation devices license is consumed automatically.

ⓘ **NOTE:** After conversion, ThinOS 2303 is in the factory default status. ThinOS 2303 must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

ⓘ **NOTE:** If the conversion has failed, you can see the error log table below and reschedule the job. Go to **Jobs** > **Schedule APP Policy** to reschedule the job.

ⓘ **NOTE:** If the conversion has failed, it is recommended to install the ThinOS ISO image.

If there is a **/usr/dtos** folder in your Ubuntu device, you can use the command **cat /var/log/dtos_dca_installer.log** to get the error log.

If there is no **/usr/dtos folder** in your Ubuntu device, go to the **WMS Server Jobs** page to check the error messages.

Table 5. Error Log table

Error Log	Resolution
No AC plugged in	Plug in power adapter, reschedule job
Platform Not Supported	This hardware platform is not supported
Error mounting recovery partition	The Ubuntu image is not a factory image. Reinstall the factory image.
No DHC/ThinOS package in recovery partition	Cannot find the ThinOS image, reschedule job
Error in extracting DHC/ThinOS Future packages	Failed to extract the ThinOS image, reschedule job
Error copying the DHC/ThinOS Future packages to recovery partition	Failed to copy the ThinOS image, reschedule job
ThinOS package verification failed	ThinOS image is not correct, reschedule job with the correct ThinOS image
Not enough space in Recovery Partition	Clear the recovery partition
The free space of Recovery Partition is not enough	Clear the recovery partition

Compatibility

ThinOS application package details

- Citrix_Workspace_App_23.2.0.10.4.pkg
- EPOS_Connect_7.4.0.2.pkg
- HID_Fingerprint_Reader_210217.23.pkg
- VMware_Horizon_2212.8.8.0.21079016.5.pkg
- Identity_Automation_QwickAccess_2.0.4.1.6.pkg
- Imprivata_PIE_7.11.001.0045.48.pkg
- Imprivata_PIE_7.10.002.0009.47.pkg
- Jabra_8.5.5.4.pkg
- Cisco_Jabber_14.1.3.307560.10.pkg
- Teradici_PCoIP_22.09.4.12.pkg
- Cisco_Webex_VDI_43.2.0.25211.4.pkg
- Cisco_Webex_Meetings_VDI_43.2.1.18.5.pkg
- Microsoft_AVD_2.0.2102.pkg
- Zoom_Citrix_5.13.0.22460.2.pkg
- Zoom_Horizon_5.13.0.22460.2.pkg
- Zoom_AVD_5.13.0.22460.2pkg
- ControlUp_VDI_Agent_1.0.0.1.33.pkg
- RingCentral_App_VMware_Plugin_23.1.10.5.pkg
- Common_Printing_1.0.0.23.pkg

NOTE: After upgrading to ThinOS 2303, all application packages released prior to ThinOS 2205 are removed automatically. You must install the latest application packages.

NOTE: You cannot install application packages released prior to ThinOS 2205 on ThinOS 2303, and Installation fails for the first time. After the installation fails, ThinOS does not download the application packages anymore.

Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 4.0
- Configuration UI package 1.9.728

NOTE: Use Wyse Management Suite 4.0 server and Configuration UI package 1.9.728 for the new Wyse Management Suite ThinOS 9.x Policy features.

ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2303 (9.4.1141)—`ThinOS_2303_9.4.1141.pkg`
- Ubuntu to ThinOS 2303 conversion build—`ThinOS_2303_9.4.1141_Ubuntu_Conversion.zip`

BIOS packages

Table 6. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.21.0.pkg
Wyse 5470 Thin Client	bios-5470_1.17.1.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.18.0.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.6.1.pkg
Dell Latitude 3420	bios-Latitude_3420_1.25.1.pkg
Dell OptiPlex 5400 All-in-One	bios-OptiPlex5400AIO_1.1.22.pkg

Tested BIOS version for ThinOS 2303

Table 7. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.21.0
Wyse 5470 All-in-One Thin Client	1.18.0
Wyse 5470 Mobile Thin Client	1.17.1
OptiPlex 3000 Thin Client	1.6.1
Latitude 3420	1.25.1
OptiPlex 5400 All-in-One	1.1.22
Latitude 3440	1.0.1
Latitude 5440	1.0.1
OptiPlex All-in-One 7410	1.0.1

Citrix Workspace app feature matrix

Table 8. Citrix Workspace app feature matrix

Feature		ThinOS 2303 with CWA 2302	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
			Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	HDX webcam is supported but requires a workaround to resolve the no video preview issue. This is a Citrix Workspace app 2302 known issue. For more limitations, see *Dell Wyse ThinOS 2303, 2211, 2208, and 2205 Release Notes* at www.dell.com/support
	Video playback	Supported	There are no limitations in this release.

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco Webex Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebexTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	There are no limitations in this release.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Supported	There are no limitations in this release.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	There are no limitations in this release.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netscaler + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	The following webview login environment configurations support autologin and lock or unlock terminal: ● Citrix Federated Authentication Service SAML with Microsoft Azure Active Directory ● Citrix ADC Native OTP ● Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
New features listed in Citrix Workspace app release notes but not in feature matrix	Microsoft Teams enhancements: App sharing enabled (CWA2209)	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: Enhancements to high DPI support (CWA2209)	Not Supported	Not supported
	Microsoft Teams enhancements: WebRTC SDK upgrade (CWA2209)	Supported	There are no limitations in this release.
	Support for extended keyboard layouts (CWA2209)	Supported	There are no limitations in this release.
	Keyboard input mode enhancements (CWA2209)	Not Supported	Not supported
	Support for authentication using FIDO2 (CWA2209)	Not Supported	Not supported
	Support for secondary ringer(CWA2207	Not Supported	Not supported
	Improved audio echo cancellation support [Technical Preview] (CWA2207)	Not Supported	Not supported
	Composite USB device redirection(CWA2207)	Not Supported	Not supported
	Support for DPI matching [Technical Preview](CWA2207)	Not Supported	Not supported
	Enhancement to improve audio quality (CWA2207)	Not Supported	Not supported
	Provision to disable LaunchDarkly service (CWA2205)	Not Supported	Not supported
	Email-based auto-discovery of store (CWA2205)	Not Supported	Not supported
	Persistent login [Technical Preview] (CWA2205)	Not Supported	Not supported
	Authentication enhancement for Storebrowse (CWA2205)	Not Supported	Not supported
	Support for EDT IPv6 (CWA2203)	Not Supported	Not supported
	Support for TLS protocol version 1.3 (CWA2203)	Not Supported	Not supported
	Custom web stores (CWA2203)	Not Supported	Not supported
	Authentication enhancement experimental feature (CWA2203)	Not Supported	Not supported

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	Keyboard layout synchronization enhancement (CWA2203)	Not Supported	Not supported
	Multi-window chat and meetings for Microsoft Teams (CWA2203)	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams (CWA2112)	Not Supported	Not Supported
	Request control in Microsoft Teams (CWA2112)	Supported	Users on ThinOS client cannot give control to other users. In other words, after the user on the ThinOS client starts sharing screen or content, the option **Give control** is present in the sharing toolbar, but it does not function when you give control to other participant. This is a Microsoft limitation.
	Support for cursor color inverting (CWA2112)	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Enhancement on smart card support (CWA2112)	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Supported	For limitations, see *Dell Wyse ThinOS 2303, 2211, 2208, and 2205 Release Notes* at www.dell.com/support
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106, CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio devices (CWA2012, CWA2010, and CWA2112)	Supported	For limitations, see *Dell Wyse ThinOS 2303, 2211, 2208, and 2205 Release Notes* at www.dell.com/support
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.

Table 8. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2303 with CWA 2302	Limitations
	Inactivity Timeout for Citrix Workspace app [Technical Preview](CWA2302)	Not supported	Not supported
	Screen pinning in custom web stores [Technical Preview](CWA2302)	Not supported	Not supported
	Support for 32-bit cursor [Technical Preview] (CWA2212)	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit exists in Citrix HDX Pro 3D desktop. This issue is also reproduced in Citrix Workspace App Linux binary.
	Addition of client-side jitter buffer mechanism [Technical Preview](CWA2212)	Not supported	Not supported
	Background blurring and replacement for Citrix Optimized Teams [Technical Preview](CWA2212)	Supported	Some of the background images fail to download and cannot take effect in Microsoft Teams optimization mode in Citrix VDI. The issue is also reproduced in Citrix Workspace app Linux binary.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

ThinOS AVD Client Feature Matrix

Table 9. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 2303
Service	Direct connection to Desktop via RDP	Supported
	Remote Desktop Services broker (Local)	Supported
	Windows Virtual Desktop (Azure)	Supported
Session	Desktop	Supported
	Remote App (Integrated)	Not supported
	Remote App (Immersive)	Supported
Input	Keyboard	Supported

Table 9. ThinOS AVD Client Feature Matrix (continued)

Category Supported	Features	ThinOS 2303
	Mouse	Supported
	Single Touch	Supported
Audio Visual	Audio in (microphone)	Supported
	Audio out (speaker)	Supported
	Camera	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
Redirections	Printer	Supported
	SmartCard	Supported
Session Experience	Dynamic Resolution	Supported
	Start Command	Supported
	Desktop Scale Factor	Supported
	Multi-Monitor (All)	Supported
	Restricted full screen session	Supported
	Keyboard Layout Mapping	Supported
	Time Zone Mapping	Supported
	Video/Audio/Online playback	Supported
	Compression	Supported
	Optimize for low speed link	Supported
Graphics (CODECs)	H.264 Hardware Acceleration	Supported
Authentication	TS Gateway	Supported
	NLA	Supported
	SmartCard	Not supported
	Imprivata	Supported

VMware Horizon feature matrix

Table 10. VMware Horizon feature matrix

Feature		ThinOS 2303 with Horizon Client 2212
Broker Connectivity	SSL certificate verification	Supported only with VDI
	Disclaimer dialog	Supported with VDI, RDS Hosted Desktops and Apps
	UAG compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Shortcuts from server	Not supported
	Pre-install shortcuts from server	Not supported
	File type association	Not supported

Table 10. VMware Horizon feature matrix (continued)

Feature		ThinOS 2303 with Horizon Client 2212
	Phone home	Supported with VDI, RDS Hosted Desktops and Apps
Broker Authentication	Password authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Single sign on	Supported with VDI, RDS Hosted Desktops and Apps
	RSA authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Integrated RSA SecurID token generator	Not supported
	Kiosk mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remember credentials	Not supported
	Log in as current user	Not supported
	Nested log in as current user	Not supported
	Log in as current user 1-way trust	Not supported
	OS biometric authentication	Not supported
	Un-authentication access	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Cisco ACS	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – SMS Passcode	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - DUO	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - OKTA	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Microsoft Network Policy	Supported with VDI, RDS Hosted Desktops and Apps
Smart card	x.509 certificate authentication (Smart Card)	Supported with VDI, RDS Hosted Desktops and Apps
	CAC support	Supported with VDI, RDS Hosted Desktops and Apps
	.Net support	Supported with VDI, RDS Hosted Desktops and Apps
	PIV support	Supported with VDI, RDS Hosted Desktops and Apps
	Java support	Not supported
	Purebred derived credentials	Not supported
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI
	Restart	Supported only with VDI
	Log off	Supported with VDI, RDS Hosted Desktops and Apps

Table 10. VMware Horizon feature matrix (continued)

Feature		ThinOS 2303 with Horizon Client 2212
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple connections	Supported with VDI, RDS Hosted Desktops and Apps
	Multi-broker/multi-site redirection - Universal	Not supported
	App launch on multiple end points	Supported with VDI, RDS Hosted Desktops and Apps
	Auto-retry 5+ minutes	Supported with VDI, RDS Hosted Desktops and Apps
	Blast network recovery	Supported with VDI, RDS Hosted Desktops and Apps
	Time zone synchronization	Supported with VDI, RDS Hosted Desktops and Apps
	Jumplist integration (Windows 7-Windows 10)	Not supported
Client Customization	Command line options	Not supported. ThinOS does not publish Command line to users.
	URI schema	Not supported. ThinOS does not publish Command line to users.
	Launching multiple client instances using URI	Not supported. ThinOS does not publish Command line to users.
	Preference file	Not supported. ThinOS does not publish Command line to users.
	Parameter pass-through to RDSH apps	Not supported. ThinOS does not publish Command line to users.
	Non interactive mode	Not supported. ThinOS does not publish Command line to users.
	GPO-based customization	Not supported
Protocols Supported	Blast Extreme	Supported with VDI, RDS Hosted Desktops and Apps
	H.264 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	H.265 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Codec	Supported with VDI, RDS Hosted Desktops and Apps
	JPEG/PNG	Supported with VDI, RDS Hosted Desktops and Apps
	Switch encoder	Supported with VDI, RDS Hosted Desktops and Apps
	BENIT	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Extreme Adaptive Transportation	Supported with VDI, RDS Hosted Desktops and Apps

Table 10. VMware Horizon feature matrix (continued)

Feature		ThinOS 2303 with Horizon Client 2212
	RDP 8.x, 10.x	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP	Supported with VDI, RDS Hosted Desktops and Apps
Features/Extensions/Monitors/Displays	Dynamic display resizing	Supported with VDI, RDS Hosted Desktops and Apps
	VDI windowed mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remote app seamless window	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple monitor support	Supported with VDI, RDS Hosted Desktops and Apps
	External monitor support for mobile	Not supported
	Display pivot for mobile	Not supported
	Number of displays Supported with VDI, RDS Hosted Desktops and Apps	4
	Maximum resolution	3840x2160
	High DPI scaling	Not supported
	DPI sync	Not supported
	Exclusive mode	Not supported
	Multiple monitor selection	Supported with VDI, RDS Hosted Desktops and Apps
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported with VDI, RDS Hosted Desktops and Apps
	Relative mouse	Supported only with VDI
	External Mouse Support	Supported with VDI, RDS Hosted Desktops and Apps
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported with VDI, RDS Hosted Desktops and Apps
	International Keyboard Support	Supported with VDI, RDS Hosted Desktops and Apps
	Input Method local/remote switching	Not supported. ThinOS does not support local input methods.
	IME Sync	Supported with VDI, RDS Hosted Desktops and Apps
Clipboard Services	Clipboard Text	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard Graphics	Not supported
	Clipboard memory size configuration	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard File/Folder	Not supported
	Drag and Drop Text	Not supported

Table 10. VMware Horizon feature matrix (continued)

Feature		ThinOS 2303 with Horizon Client 2212
	Drag and Drop Image	Not supported
	Drag and Drop File/Folder	Not supported
Connection Management	IPv6 only network support	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP IP roaming	Supported with VDI, RDS Hosted Desktops and Apps
Optimized Device Redirection	Serial (COM) Port Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Client Drive Redirection/File Transfer	Not supported. ThinOS local drive is secured and not accessible.
	Scanner (TWAIN/WIA) Redirection	Supported with VDI, RDS Hosted Desktops and Apps. Windows Image Acquisition (WIA) is not supported.
	x.509 Certificate (Smart Card/ Derived Credentials)	Supported with VDI, RDS Hosted Desktops and Apps
	Gyro Sensor Redirection	Not supported
Real-Time Audio-Video	Audio in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Video in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple webcams	Not supported
	Multiple speakers	Not supported
USB Redirection	USB redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnInsert	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnStartup	Supported with VDI, RDS Hosted Desktops and Apps
	Connect/Disconnect UI	Not supported. ThinOS does not support Horizon Menu toolbar in Blast and PCoIP sessions.
	USB device filtering (client side)	Supported with VDI, RDS Hosted Desktops and Apps
	Isochronous Device Support	Supported only with VDI
	Split device support	Supported with VDI, RDS Hosted Desktops and Apps
	Bloomberg Keyboard compatibility	Supported only with VDI
	Smartphone sync	Supported only with VDI
Unified Communications	Skype for business	Supported with VDI, RDS Hosted Desktops and Apps
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Teams	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Meetings	Supported with VDI, RDS Hosted Desktops

Table 10. VMware Horizon feature matrix (continued)

Feature		ThinOS 2303 with Horizon Client 2212
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops and Apps
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops and Apps
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not supported
	Directshow Redirection	Not supported
	URL content redirection	Not supported. ThinOS does not have a native browser to support the function.
	MMR Multiple Audio Output	Not supported
	Browser content redirection	Not supported
Graphics	vDGA	Supported only with VDI
	vSGA	Supported only with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Supported only with VDI
	AMD vGPU	Supported only with VDI
Mobile Support	Client-side soft keyboard	Not supported
	Client-side soft touchpad	Not supported
	Full Screen Trackpad	Not supported
	Gesture Support	Not supported
	Multi-touch Redirection	Not supported
	Presentation Mode	Not supported
	Unity Touch	Not supported
Printing	VMware Integrated Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Location Based Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Native Driver Support	Not supported
Security	FIPS-140-2 Mode Support	Supported with VDI, RDS Hosted Desktops and Apps
	Imprivata Integration	Supported with VDI, RDS Hosted Desktops and Apps
	Opswat agent	Not supported
	Opswat on-demand agent	Not supported
	TLS 1.1/1.2	Supported with VDI, RDS Hosted Desktops and Apps. TLS 1.1 is removed due to security concerns on ThinOS 2303.
	Screen shot blocking	Not supported
	Keylogger blocking	Not supported
Session Collaboration	Session Collaboration	Supported with VDI, RDS Hosted Desktops and Apps

Table 10. VMware Horizon feature matrix (continued)

Feature		ThinOS 2303 with Horizon Client 2212
	Read-only Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
Update	Update notifications	Not supported
	App Store update	Not supported
Other	Smart Policies from DEM	Supported with VDI, RDS Hosted Desktops and Apps
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI—Only basic connection is tested
	Workspace ONE mode	Supported with VDI, RDS Hosted Desktops and Apps
	Nested - basic connection	Supported with VDI, RDS Hosted Desktops and Apps
	DCT Per feature/component collection	Not supported
	Displayed Names for Real-Time Audio-Video Devices	Supported with VDI, RDS Hosted Desktops and Apps
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI
Unified Access Gateway	Authentication Method - Password	Supported
	Authentication Method - RSA SecurID	Supported
	Authentication Method - X.509 Certificate (Smart Card)	Supported
	Authentication Method - Device X.509 Certificate and Passthrough	Supported. **Login Use Smartcard Certificate Only** must be disabled in ThinOS.

For detailed information about the VMware Horizon features, see the Horizon documentation at docs.vmware.com.

New and enhanced features

Citrix Workspace app updates

Citrix Workspace App package version is updated to 23.2.0.10.4.

If you want to install the Citrix Workspace app version 2302 on ThinOS, install this package.

ⓘ **NOTE:** Citrix Security Bulletin Alert CTX477618 does not affect ThinOS clients. For more information, see *Linux Security Bulletin for CVE-2023-24486* at www.citrix.com

ⓘ **NOTE:** Citrix Workspace App package version 23.2.0.10.4 and its new features that are supported by ThinOS 2303 is also supported on ThinOS 2211 (9.3.3099).

Supports 32-bit cursor

- 32-bit cursor is supported on ThinOS 2303 and Citrix Workspace App 2302.
- The black box around the cursor issue is resolved when using 3D applications in HDX 3D Pro VDA desktop.
- There is a black box around the 32-bit cursor in Adobe Acrobat reader in Citrix HDX Pro 3D desktop. This issue is also reproduced in Citrix Workspace App Linux binary.

Supports multiple audio devices by default

- From ThinOS 2303 and Citrix Workspace App 2302, Citrix Workspace app displays all available local audio devices in a session with their names.
- Plug-and-play functionality is also supported.
- Multiple audio devices redirection feature is enabled by default. In other words, `AudioRedirectionV4=True` parameter has already been configured during Citrix Workspace App 2302 package installation. You need not change the Citrix INI settings in Citrix configuration editor in Wyse Management Suite or Admin Policy Tool.
- To disable this feature, do the following:
  1. In Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
  2. In the **Citrix INI Settings**, click **Add Row**.
  3. From the **File** drop-down list, select **module.ini**.
  4. From the **Operation** drop-down list, select **Add or Update**.
  5. In the Section field, enter **`ClientAudio`**.
  6. In the **Key** field, enter **`AudioRedirectionV4`**.
  7. In the **Value** field, enter **`False`**.
  8. Sign out or restart the device for the settings to take effect.

     NOTE: Cisco JVDI does not support multiple audio devices feature, which is a known Cisco limitation. To ensure there is no confusion or mistakes for users who use JVDI in a Citrix environment, multiple audio devices feature is dynamically disabled after JVDI package is installed, and the feature is dynamically enabled after JVDI package is uninstalled.

     NOTE: There is an eight-device limitation on HDX session redirection, which is a Citrix VDA limitation. The total number of playback and recording devices on the thin client must be lesser than or equal to eight to use multiple audio devices redirection feature. If the total number of playback and recording devices on thin client is more than eight, the feature does not work. In that case, some of the audio devices may be missing in HDX session or the audio devices are displayed as Citrix HDX audio.

Support for background blurring and replacement for Microsoft Teams optimized mode

- The feature requires Multi-Window feature as a prerequisite, which is available in VDA 2112 or later versions and Microsoft Teams 1.5.00.11865 or later versions.
- From ThinOS 2303 and Citrix Workspace App 2302, you can blur or change your background by going to **More** > **Apply Background Effects** when you are in a meeting or call.
- **Limitations**:
  - Few background images fail to download and display in Microsoft Teams optimization mode in Citrix VDI. The issue is also reproduced in Citrix Workspace app Linux binary.
  - Sometimes, it takes 2 s to 3 s for the background image to be displayed. The issue is also reproduced in Citrix Workspace app Linux binary.

Support for Request control in Microsoft Teams optimized mode

- From ThinOS 2303 and Citrix Workspace App 2302, you can request control during a Microsoft Teams call or meeting when a participant is sharing the screen. Once you have control, you can make selections, edits, or other modifications to the shared screen.
- To take control when a screen is being shared, click **Request control** at the top of the Microsoft Teams screen. The meeting participant, who is sharing the screen, can either allow or deny your request.
- While you have control, you can make selections, edits, and other modifications to the shared screen. When you are done, click **Stop control**.
- **Limitation**
  - If you are using a ThinOS client, you cannot give control to other users. In other words, after the user on the ThinOS client starts sharing the screen, the option **Give control** is present in the sharing toolbar, but the function does not work after giving control to other participant. This is a Microsoft limitation.

Other Citrix Workspace App Limitations

- If users sign in using NetScaler with OTP authentication, Citrix workspace mode in ThinOS does not take effect.
- Multiple audio devices feature does not work correctly with CWA2302 package on ThinOS 2211 and Cisco Jabber package version 14.1.2.307144.7. Remove the Cisco Jabber package to make multiple audio devices work.
- The following issues also occur in Citrix Workspace app Linux binary:
  - **Select playback device** dropdown list in Citrix session is not refreshing automatically when hot plugging the USB headset and multiple audio devices feature is enabled.

    - There is an eight-device limitation on HDX session redirection, which is a Citrix VDA limitation. The total number of playback and recording devices on the thin client must be lesser than or equal to eight to use multiple audio devices redirection feature.
    - If the total number of playback and recording devices on thin client is more than eight, the feature does not work after signing off and signing in to the Citrix session.
    - **Webex Call failed** error message is displayed when starting a video call using HDX Web Camera with Theora encoder through a VDI fallback mode on WebEx teams application.
    - Some background images fail to download and cannot take effect in Microsoft Teams optimization mode in Citrix VDI sessions.
    - A dark shadow mouse cursor is displayed on VDA2203 desktop during desktop launch or when a remote desktop is in an HDX session through mstsc.exe.
    - There is an echo when in calls or meetings using Microsoft Teams optimized mode on the mobile thin client or AIO thin client with integrated audio devices.
    - HDX webcam is not working inside a Citrix session and there is no video preview in application. As a workaround, do the following:
        1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
        2. In **Citrix INI Settings**, click **Add Row**.
        3. From the **File** drop-down list, select **wfclient.ini**.
        4. From the **Operation** drop-down list, select **Add or Update**.
        5. In the **Section** field, enter `WFClient`.
        6. In the **Key** field, enter `HDXWebCamDelayType`.
        7. In the **Value** field, enter `2`.
        8. In **Citrix INI Settings**, click **Add Row**.
        9. From the File drop-down list, select wfclient.ini.
        10. From the **Operation** drop-down list, select **Add or Update**.
        11. In the **Section** field, enter `WFClient`.
        12. In the **Key** field, enter `HDXWebCamDelayType`.
        13. In the **Value** field, enter `1000`
        14. Sign out or restart the device for the settings to take effect.

        The above workaround is only applicable for Citrix Workspace App 2302.
    - Invert cursor feature is not working in Citrix VDA2212 with Windows 10 operation system and Windows 2019 desktop.
    - Sometimes the mouse cursor of the host is missing when sharing screen and giving control to the user who is working on the ThinOS client in Microsoft Teams optimized mode. As a workaround, click the left button of the mouse in the host desktop.
    - Mouse cursor is displayed as a black block in Adobe Acrobat Reader (32-bit) in Citrix HDX 3D Pro desktop.
    - Microsoft teams audio or video calls have audio issues when logging in to Microsoft Teams from a web browser with BCR enabled.
    - Multimedia redirection (MMR) videos stop responding and there is no audio on devices with Virtual Delivery Agent (VDA) version 2203 and 2206.
    - Citrix Session search tab does not work after clicking the **Device** tab in **Citrix Desktop Viewer** toolbar.
    - Audio issues are noticed when using a redirected USB headset in Citrix session.
    - When playing WMV-9 or WMV-7 videos in .wmp format, the wallpaper of the VDI session is displayed on the video.
- The following new features from Citrix Workspace App 2212 and 2302 are not supported in ThinOS:
    - Inactivity timeout for Citrix Workspace app.
    - Screen pinning in custom web stores.
    - Addition of client-side jitter buffer mechanism.

Microsoft RDP and AVD

Enabling Network Level Authentication (NLA) is optional—If you select the **Enable NLA** checkbox in the **RDP** tab of **Global Connection Settings**, you can verify users before connecting to an RDP session.

NOTE: Disabling NLA locally in the ThinOS client works only in RDP sessions. You should select **Enable NLA** before connecting to RDS sessions. However, **Enable NLA** does not work in AVD sessions.

Microsoft Teams Optimization in RDP sessions (Preview)

NOTE: This is an experimental feature.

- ThinOS 2303 supports media optimization for Microsoft Teams in RDP sessions.
- To enable the Teams optimization feature for AVD, you must meet the following requirements:
  - Install the Microsoft Teams desktop app in RDP protocol sessions. See *Use Microsoft Teams on Azure Virtual Desktop* at www.microsoft.com for more information.
  - Check whether Microsoft Teams has been launched in optimized mode. Click the three dots next to your profile image, and go to **About** > **Version**. If Teams is in optimized mode, a banner that says **AVD Media Optimized** is displayed.
- **Known Issues**
  - Azure sessions stop responding when video calling using Teams.
  - ThinOS local devices are not displayed in Microsoft Teams of RDP protocol sessions.
  - Only one camera is displayed in Microsoft Teams of RDP protocol sessions.

Change in AVD broker settings interface

- Multiple Azure Cloud Workspaces are supported with this release, so **Azure Common (ARMv2)**, **Azure Classic (MS-Prod)**, **Azure US Gov**, and **Azure China** workspaces have been added in **Remote Connections** > **Broker Setup** > **Azure Workspaces** list.
- **Azure Common (ARMv2)** and **Azure Classic (MS-Prod)** supports Azure Cloud, which is the most common workspace.
- **Azure US Gov** (Preview) supports the Azure environment of the US government. This workspace is for preview only.
- **Azure China** (Preview) supports the Azure China 21Vianet environment. This workspace is for preview only.
- **Azure Common (ARMv2)** and **Azure Classic (MS-Prod)** are both selected by default and you can adjust based on your environment. Some environments work with **Azure Common (ARMv2)** only.

Teradici PCoIP update

- Teradici version is updated to 22.09.4.12 in ThinOS 2303.
- **Limitations**
  - Remote Workstation Card PCoIP sessions cannot be connected when using Teradici PCoIP package version 22.09.4.12, which is a known issue from Teradici. If you want to connect to Remote WorkStation card PCoIP sessions, use PCoIP package version 22.04.2.13, which is in the ThinOS 2208 release.
  - When redirecting a USB headset or Nuance Power microphone to a PCoIP session, there is no audio playback.
  - PCoIP sessions take longer to end.
  - When two or more monitors are connected to ThinOS, a PCoIP session is launched, and display settings of ThinOS is changed multiple times, the PCoIP session displays a black screen. As a workaround, you must reconnect the PCoIP session.

Horizon Blast Updates

The Horizon package version is updated to Horizon 2212 in ThinOS 2303.

Unified Access Gateway

- **Device Cert Authentication with Unified Access Gateway and Passthrough**—With the client device certificate authentication feature, Unified Access Gateway authenticates the thin client system. After successful device authentication, you must complete user authentication. For more information about this feature, see the VMware documentation at docs.vmware.com.
  1. Go to **Wyse Management Suite** or **Admin Policy Tool**.
  2. Go to **Login Experience** > **Login Settings**.
  3. Disable **Login Use Smartcard Certificate Only**.
  4. Click **Save**.
  5. Import the PFX certificate into ThinOS.
  6. Configure the Horizon Broker agent with the UAG server address.
  7. Start the Broker agent login process.
  8. Select the certificate to log in.
- **X.509 Certificate Authentication**—You can configure the X.509 certificate authentication in Unified Access Gateway to allow ThinOS to authenticate with certificates. For more information about this feature, see the VMware documentation at docs.vmware.com
  1. Connect the smartcard reader to the ThinOS client.
  2. Configure the Horizon Broker agent with UAG server address.
  3. Insert the smartcard in the smartcard reader.
  4. Select the valid certificate.

5. Enter the PIN to log in.

- **RADIUS Authentication**—RADIUS offers a wide range of third-party, two-factor authentication options. To use RADIUS authentication on Unified Access Gateway, you must have a configured RADIUS server that is accessible on the network from Unified Access Gateway.
  1. Configure the Horizon Broker agent with UAG server address.
  2. Enter the RADIUS username and passcode to log in.
- **RSA SecurID Authentication**—After the Unified Access Gateway appliance is configured as authentication agent in the RSA SecurID server, add the RSA SecurID configuration information to Unified Access Gateway.
  1. Configure the Horizon Broker agent with the UAG server address.
  2. Enter the RSA username and token to log in.
- **SAML Authentication**—If you are using SAML version 2.0 identity provider, you can directly integrate the identity provider with the Unified Access Gateway (UAG) to support Horizon client user authentication. To use SAML third-party integration with UAG, you must use Horizon Connection Server 7.11 or later versions. To integrate the UAG with the identity provider, do the following:
  1. Configure the identity provider with the service provider (UAG) information.
  2. Upload the metadata file of the identity provider to the UAG.
  3. Configure the Horizon settings on the UAG Admin console.

     No additional configuration is required in ThinOS. But, after the Broker agent connection is established, you are prompted to do a third-party authentication.

Table 11. Troubleshooting errors during Horizon login

Error message	Reason	Solution
Unknown username or bad password.	Username or Password is incorrect.	Enter the correct username and password.
Please enter your credentials.	Username or Password is empty.	Do not leave username and password empty.
Your account has expired.	Account is expired.	Check your account status.
Your account is currently disabled.	Account is disabled.	Enable your account.
You are not entitled to use the system!	Account is not entitled in Horizon server.	Entitle your account in Horizon server.
Your password must be changed before logging on.	Account password must be changed.	Update your account password.
Maximum login attempts exceeded.	Too many failed logins.	Not available
Broker connection not secure.	Unsecure HTTP protocol is being used.	It is recommended that you use HTTPS protocol.
This Horizon Connection Server is currently disabled.	Connection Server is disabled.	Enable the connection server in Horizon.
Please insert smartcard or press ESC to retry login.	Smartcard is not inserted.	Insert the smartcard.
Invalid PIN	The smartcard PIN has not been entered.	Do not leave the PIN field empty.
Incorrect PIN	The entered smartcard PIN is incorrect.	Enter the correct smartcard PIN.
Certificate expired. Please select valid certificate and retry.	Smartcard certificate is expired.	Select a valid smartcard.
Access denied. No valid certificate provided	No smartcard inserted during UAG smartcard authentication.	Insert a smartcard or import a valid certificate in ThinOS.
The login was cancelled by user. Press ESC to retry login.	Close web authentication window during workspace one mode login or during third-party IdP authentication.	Press ESC to retry login.
Connect broker timeout	Cannot reach Horizon server through Proxy.	Check your proxy connection.

Table 11. Troubleshooting errors during Horizon login (continued)

Error message	Reason	Solution
Horizon: check tunnel error.	Cannot reach Horizon Tunnel.	Check Horizon tunnel connection.
Access denied	RSA authentication failed.	Enter correct RSA passcode.
	Radius authentication failed.	Enter correct Radius passcode.
Login Failed	Invalid Horizon Broker agent URL	Enter valid Horizon Broker URL.
	Canceled the Disclaimer.	Accept Horizon Disclaimer.
	Canceled the Security Warning window.	Click **Continue** in Security Warning window.
	Did not pass security check.	According to the instructions displayed, enter the required information.
	Smartcard login failed due to incorrect username.	Enter the correct username of the certificate.
	Client Network is down.	Ensure that network is reachable before Horizon Login.

Support for other brokers

You can configure other Broker agents in **Remote Connections**. Leostream, Parallels RAS, and Systancia Workplace Broker agents are supported from ThinOS 2303.

- In the **Select Broker Type** drop-down list under **Remote Connections** > **Broker Setup**, **Other Broker** option has been added that supports Leostream and Parallels RAS brokers.

  ⓘ **NOTE:** ThinOS 2303 provides only experimental support for Systancia Workplace and is going to be supported in future ThinOS releases.
- You can also configure the other Broker agents in Wyse Management Suite and Admin Policy Tool by going to **Broker Settings** > **Other Broker Settings**.
  1. In the **Broker Server** field, you can configure the Broker agent server address by adding the URL of the other Broker agent.
  2. In the **Auto Connect List** field, you can configure the desktop and applications that must be automatically connected.
  3. In the **Notice to Broker Connection**, when using Parallels RAS Broker agent, **Enable Password Variables** must be enabled in **Login Experience** > **Login Session**.
     - The server certificate must be imported in ThinOS before connecting to the Broker agent.
     - The Broker agent URL must be in FQDN format.
     - RDP is supported in other Broker agent sessions only. AVD application package must also be installed.

Leostream

- Leostream connection Broker agent version is 9.0.40.10.
- Leostream agent version is 7.3.8.0.
- Remote Desktop Protocol (RDP) is supported during Leostream desktop sessions. AVD application package must also be installed.

Table 12. Leostream Feature Matrix

RDP/ThinOS	Category Supported	Features	ThinOS 2303
RDP feature	Input	Keyboard	Supported
		Mouse	Supported
		Single touch	Supported
	Session	Desktop	Supported
	Audio Visual	Audio in	Supported

Table 12. Leostream Feature Matrix (continued)

RDP/ThinOS	Category Supported	Features	ThinOS 2303
		Audio out	Supported
		Camera	Supported
	Storage	Folder/Drive Redirection	Supported
	Clipboard	Clipboard (text)	Supported
	Redirections	Printer	Supported
		Smart Card	Supported
	Session Experience	Dynamic Resolution	Supported
		Desktop Scale Factor	Supported
		Multi-Monitor (All)	Supported
		Restricted full screen session	Supported
		Time Zone Mapping	Supported
		Video/Audio/Online playback	Supported
	Graphics (CODECs)	H.264 Support	Supported
ThinOS feature	Login Settings	Username	Supported
		Password	Supported
		Default Domain	Supported
		Single Button Connect	Supported
		Logo for Login Window	Supported
		Show password for login window	Supported
	Session Settings	Session Reconnect	Supported
		Enable NLA	Supported
		Force Span	Supported
		Record From Local	Supported

Systancia Workplace

Systancia Workplace is an application and desktop virtualization solution.

NOTE: ThinOS 2303 provides only experimental support for Systancia Workplace and is going to be supported in future ThinOS releases.

- Supports Systancia Workplace Broker agent.
- Supports RDP for VDI sessions using the Systancia Workplace broker. AVD application package must also be installed.
- **Known Issue**
  - If Systancia Workplace Broker agent does not respond in 5 s, login fails with a timeout error message. As a workaround, log in again when facing the timeout error.

Parallels RAS (Remote Application Server)

- Parallels Remote Application Server (RAS) version is 18.0.22497.
- Remote Desktop Protocol (RDP) is supported during desktop and application sessions. AVD application package must also be installed.

Table 13. Parallels Feature Matrix

RDP/ThinOS	Category Supported	Features	ThinOS 2303
RDP feature	Input	Keyboard	Supported
		Mouse	Supported
		Single touch	Supported
	Session	Desktop	Supported
		Remote App (Immersive)	Supported
	Audio Visual	Audio in	Supported
		Audio out	Supported
		Camera	Supported
	Storage	Folder/Drive Redirection	Supported
	Clipboard	Clipboard (text)	Supported
	Redirections	Printer	Supported
		Smart Card	Supported
	Session Experience	Dynamic Resolution	Supported
		Desktop Scale Factor	Supported
		Multi-Monitor (All)	Supported
		Restricted full screen session	Supported
		Time Zone Mapping	Supported
		Video/Audio/Online playback	Supported
	Graphics (CODECs)	H.264 Support	Supported
ThinOS feature	Login Settings	Username	Supported
		Password	Supported
		Default Domain	Supported
		Single Button Connect	Supported
		Logo for Login Window	Supported
		Show password for login window	Supported
	Session Settings	Session Reconnect	Supported
		Enable NLA	Supported
		Force Span	Supported
		Record From Local	Supported

Imprivata updates

- ThinOS Imprivata_PIE_7.10.002.0009.47.pkg is supported against OneSign server 7.10.000.18.
- ThinOS Imprivata_PIE_7.11.001.0045.48.pkg is supported against OneSign server 7.11.000.5.

Identity Automation

Identity automation package is updated to 2.0.4.1.6.

Cisco Webex Meetings VDI updates

- Cisco Webex Meetings VDI package version is updated to 43.2.1.18.1.
- Added new features:
  - Watermark
  - Background noise cancellation

Cisco Webex VDI update

- Cisco Webex VDI package version is updated to 43.2.0.25211.
- Added new features to Webex Teams VDI:
  - Virtual background
  - Music mode

Cisco Jabber

Cisco Jabber (jVDI) version is updated to 14.1.3.307560.1.

Zoom

Zoom Citrix package version is updated to 5.13.0.22460.1.

RingCentral

RingCentral package version is RcApp_VMwareplugin_22.3.30.1.

ControlUp

ControlUp package version is 1.0.0.1.26.

ThinOS enhancements

Supports Latitude 3440—The following hardware configurations are supported:

Table 14. Hardware configurations that are supported for Latitude 3440

Hardware Type	Hardware
CPU	Intel Celeron 7305
	12th Generation, Intel Core i3-1215U
	13th Generation Intel Core i5-1335U
Memory	8 GB, 1 x 8 GB, DDR4, 3200 MHz
	16 GB, 2 x 8 GB, DDR4, 3200 MHz
Storage	M.2 256 GB, PCIe NVMe, Class 35 SSD
	M.2 512 GB, PCIe NVMe, Class 35 SSD
	M.2 512 GB, PCIe NVMe, Class 40 SSD
Integrated Camera	HD camera
	FHD camera
	FHD IR camera

Table 14. Hardware configurations that are supported for Latitude 3440 (continued)

Hardware Type	Hardware
Wireless	Intel AX211
Display	HD
	FHD
	FHD + touch

The following hardware configurations are not supported for Latitude 3440:

Table 15. Hardware configurations that are not supported for Latitude 3440

Hardware Type	Hardware
Wireless	Realtek 8852BE
Fingerprint	Fingerprint on power button
micro-SIM card slot	micro-SIM card
Discrete GPU	NVIDIA GeForce MX550

Supports Latitude 5440—The following hardware configurations are supported:

Table 16. Hardware configurations that are supported for Latitude 5440

Hardware Type	Hardware
CPU	13th Generation Intel Core i3-1315U
	13th Generation Intel Core i5-1345U
Memory	8 GB, 1 x 8 GB, DDR4, 3200 MHz
	16 GB, 2 x 8 GB, DDR4, 3200 MHz
Storage	M.2 256 GB, PCIe NVMe, SSD
	M.2 512 GB, PCIe NVMe, SSD
Integrated Camera	FHD RGB camera
	FHD IR camera
	FHD IR with EMZA camera
Wireless	Intel AX211
Display	FHD 250 nit
	FHD 400 nit
	FHD 300 nit + touch
Smart Card reader slot	Smart Card reader only

The following hardware configurations are not supported for Latitude 5440:

Table 17. Hardware configurations that are not supported for Latitude 5440

Hardware Type	Hardware
Wireless	Realtek 8852BE
Fingerprint	Fingerprint on power button
micro-SIM card slot	micro-SIM card
Discrete GPU	NVIDIA Graphics
NFC/Contactless smart card reader	NFC/Contactless smart card reader

Table 17. Hardware configurations that are not supported for Latitude 5440 (continued)

Hardware Type	Hardware
Storage	SED storage

Supports OptiPlex All-in-One 7410—The following hardware configurations are supported:

Table 18. Hardware configurations that are supported for OptiPlex All-in-One 7410

Hardware Type	Hardware
CPU	Intel Celeron G6900T
	Intel Pentium Gold G7400T
	Intel Pentium Gold G7400
	13th Generation Intel Core i3-13100
	13th Generation Intel Core i5-13400T
Memory	8 GB, 2 x 4 GB, DDR4, 3200 MHz
	8 GB, 1 x 8 GB, DDR4, 3200 MHz
	16 GB, 2 x 8 GB, DDR4, 3200 MHz
	8 GB, 1 x 8 GB, DDR5, 4800 MHz
	16 GB, 2 x 8 GB, DDR5, 4800 MHz
Storage	M.2 SSD 2230 256GB GEN4*4
Integrated Camera	FHD camera
Wireless	Intel AX201
	Intel AX211
Display	FHD
	FHD + touch

The following hardware configuration is not supported for OptiPlex All-in-One 7410:

Table 19. Hardware configurations that are not supported for OptiPlex All-in-One 7410

Hardware Type	Hardware
SD card slot	SD card
Storage	SED storage
Storage	HDD storage
Wireless	Realtek RTL8852BE
HDMI out	HDMI out port

Asset Tag in System Information window

- Added **Asset Tag** parameter in the **System Information** window. The parameter is displayed only when **Asset Tag** is set in BIOS settings.
- Added **$AT** variable in Wyse Management Suite and Admin Policy Tool for **Asset Tag**.**$AT** can be used as a terminal name, and the length is limited to 32 characters. **Asset Tag** is also displayed in the Wyse Management Suite device details tab.

New OS, BIOS, Application update process—Servicing mode

- Updated the order from **OS** > **BIOS** > **Application** to **BIOS** > **OS** > **Application**. After BIOS update, ThinOS reboots and then continues to update the operating system. After operating system update, ThinOS reboots and then continues to update the application.
- Removed the bottom-right download progress window. The operating system and BIOS downloads in the background and is installed in servicing mode. Applications are both downloaded and installed in servicing mode.

- When ThinOS enters servicing mode, ThinOS automatically logs off when you are logged in. You cannot log in until the update process is finished.
- If the update fails, ThinOS automatically exits servicing mode after a countdown. You can also click **Exit** to exit the mode manually. After exiting the servicing mode, you can log in to continue your work.
- The applications that fail to update are displayed in the failed application list.
- If you update an invalid application package, like trying to install an application released prior or as part of ThinOS 2205, the update fails. Reboot your device and the device does not download and install the invalid application package again.
- If you do not connect power adapter to the ThinOS client, the update fails with a 60-seconds countdown error **AC power is not connected**.
  - If you connect the power adapter in 60 seconds, ThinOS exits servicing mode and then enters servicing mode again to continue the update process.
  - If you do not connect the power adapter in 60 seconds, ThinOS exits servicing mode after the countdown is complete. You must reboot and update again.
- If the network disconnects during application package download, ThinOS waits for 45 seconds
  - If network is recovered in 45 seconds, the current downloading application package is ignored and the next application package begins to install. After the other application packages are updated, the client automatically reboots and downloads the application package that was not downloaded in the beginning.
  - If network is not recovered in 45 seconds, a message is displayed stating that the application package list has failed to install. You can connect network and reboot to update again.

Wyse Management Suite group change behavior update—From ThinOS 2303, if the thin client is registered in Wyse Management Suite group 1 and you change it to Wyse Management Suite group 2, a dialog box is displayed to change the group. Click **Cancel** to change to group 2 immediately. Click **Restart Now** or wait for the 60-second countdown to finish and then reboot to change to group 2.

NOTE: If you set policies that require reboot to take effect in group 2, you must reboot again manually.

Complete device log from Wyse Management Suite server— You can fetch client logs from the Wyse Management Suite server, and these logs are the same as the logs which are exported to the client.

Supports Apple AirPods Bluetooth audio profiles—The following Bluetooth profiles are applicable for all Bluetooth headsets except Jabra Elite 3 Bluetooth headset:

- Headset Profile (HSP) and Handsfree Profile (HFP): When listening in on a call and when recording calls on Zoom, Webex, Teams, and so on, you can select these profiles.
- Advanced Audio Distribution Profile (A2DP): When listening to audio on your thin client, you can select this A2DP profile. A2DP profile supports stereo quality audio and is meant for playing music. You cannot record audio and use microphone simultaneously with this profile.

Supports Jabra Elite 3—Jabra Elite 3 Bluetooth headset supports only unified communication calls. But, all Bluetooth headsets take time to respond during unified communication calls on ThinOS and Ubuntu operating systems.

Event log improvement—Improved wired IEEE802.1x authentication and wireless authentication event log.

Citrix Program Neighborhood Agent icon update—Citrix Program Neighborhood Agent icon in classic modern mode is changed to Citrix Workspace icon.

Net iD smart card firmware update—Updated the Net iD smart card firmware version to 6.8.5.20.

SMB printer update—If the SMB printer username, password, and domain fields do not have a defined value, the client fetches it from the VDI login credentials for this field. If one of the values is already defined, the client retains the value.

Scheduled shutdown or reboot settings update—Once a scheduled shutdown or reboot job is created, a message on the client event log is displayed and the client check-in to the Wyse Management Suite server is not affected. If the client is powered on during the scheduled shutdown or reboot time range, the scheduled reboot or shutdown job happens in the same time range on another day.

Supports Common Printing package— Common Printing is a collection of tools supporting different types of printers and printer classes like PS, TXT, PCL4, PCL5, PCL6.

- The feature supports papersize management, lossless compression of scanned pages, and color management.
- Various printer driver sand software are a part of the Common Printing package.
- The feature also supports various printing formats such as PDF, PNG, JPG, TIFF.
- **Limitation**: When USB printer mapping occurs, random printing occurs. As a workaround, use UPD printing Print Drivers of the Citrix Universal Print Driver (UPD) Component,

Change in BIOS settings after fresh installation or conversion—If you convert a device from another operating system to ThinOS 2303 or install the ThinOS 2303 recovery image, ThinOS changes BIOS settings when booting for the first time:

- BIOS password: Set to **Fireport**
- SATA/NVMe Operation: Set to **AHCI/NVMe**

- Integrated NIC: Set to **Enabled** (set to disable PXE boot support)
- Wake-on-LAN: Set to **LAN only**

  For OptiPlex 3000 Thin Client with SFP module, the option is set to **LAN or SFP NIC**.

- Enable Secure Boot: Set to **ON**
- Enable USB Boot Support: Set to **OFF**
- Enable USB Wake Support: Set to **ON**
- Deep Sleep Control: Set to **Disabled**

  ⓘ **NOTE:** Only the devices with BIOS password **Fireport** or an empty password field apply these changes in BIOS settings.

Performance History—**Performance Retrospective** is renamed to **Performance History** in the **Troubleshooting** window of **General** tab.

OpenVPN

- ThinOS 2303 supports OpenVPN.
- To configure OpenVPN, do the following:
  1. Open the **VPN Manager** window.
  2. Click **OpenVPN**.
  3. Click **Add icon** to add OpenVPN.
  4. Upload the OVPN config file in **APT/WMS** > **Network Configuration** > **VPN Settings** > **VPN** > **Open VPN config**.

Fortinet VPN—Fortinet is supported in ThinOS 2303 and is added in **Open Connect** > **Protocol**.

Bluetooth tab in Peripherals—**Bluetooth** tab has been moved after **Audio** tab in **Peripherals** window.

Disable keyboard keys—You can disable keys a to z, 0 to 9, and PrintScreen key on the keyboard.

ⓘ **NOTE:** Enter `PrtScn` to disable the PrintScreen key. Do not enter `PrintScreen`.

Supports Multi-Steam Transport (MST) or Daisy Chaining—The following table displays the platforms that support MST along with the maximum resolution that is supported when two or three monitors are connected:

Table 20. MST and Maximum resolution

System	Maximum resolution for two monitors	Maximum resolution for three monitors
Latitude 3440/5440	2 x 2560x1440	3 x 1920x1080
OptiPlex All-in-One 7410	4K + 2560 x 1440	3 x (2560 x 1440)

ⓘ **NOTE:** DisplayPort and Type-C port supports MST; HDMI port does not support MST.

Limitations for Multi-Steam Transport (MST)

- If you enable MST on monitors, display audio does not work.
- If you reboot with multiple monitors connected, the monitors may display a black screen. As a workaround, unplug and plug in the monitor again.
- If you connect two or three monitors with MST and plug out the monitors, ThinOS stops responding for 15 s or 30 s. When ThinOS stops responding, do not plug in the monitor again. Wait for ThinOS to recover and then plug in the monitor.
- If the default resolution of the monitors is more than the maximum resolution that can be supported, the ThinOS client stops responding.

Calibration tab

- Added a **Calibration** tab in **Client Settings** > **Peripherals**.
- If you plug in an external touch monitor to the client without an integrated screen, **Calibration** can be enabled.
- Click the **Calibrate** button to start the calibration and then click **+** one by one until the calibration is finished.
- You can use the calibration function on only one screen.

Supports docking stations—The following docks and systems are supported:

- **Dell Dock - WD19/WD19S/WD19TB(Thunderbolt port is not supported)**

Table 21. Platforms that support WD19 and their maximum resolution

System	Maximum resolution for one monitor	Maximum resolution for two monitors	Maximum resolution for three monitors
Wyse 5470	4K 30 Hz	2 x (1920 x 1080)	Not Applicable
Latitude 3420	4K 30 Hz	2 x (2560 x 1440)	3 x (1920 x 1080)
Latitude 3440	4K 30 Hz	2 x (2560 x 1440)	3 x (1920 x 1080)

- **Dell Thunderbolt Dock - WD22TB4**

Table 22. Systems that support WD22TB4 and their maximum resolution

System	Maximum resolution for one monitor	Maximum resolution for two monitors	Maximum resolution for three monitors
Latitude 5440	4K 60 Hz	4K + (2560 x 1440)	4K + 2 x (2560 x 1440)

- **Limitations**
  - If multiple monitors are connected, display audio does not work.
  - Do not hot plug monitors to the docking station as this causes a black screen issue. You can hot plug the docking station instead.
  - HDMI port and Type-C port cannot support two monitors simultaneously. Only one of these ports can be used as a display device at a time.
  - If you connect two or three monitors on the docking station and plug out the docking station, ThinOS stops responding for 15 s or 30 s. When ThinOS stops responding, do not plug in the docking station again. Wait for ThinOS to recover and then plug in the docking station
  - If the default resolution of the monitors on the docking station is larger than the maximum supported resolution, the ThinOS client stops responding. For example, if you connect three monitors with default resolution of 4 K with WD19S dock and then connect the dock to Latitude 3440, the client stops responding.

Allow server list—If the Wyse Management Suite server is not in the allow server list and you check in it in **Central configuration** location, **Server is not in allow list!** error message is displayed and the client cannot check in. Wyse Management Suite continues to be connected with the managed group if it has failed to connect to a server that is not in allow list.

Updates for locally-configured LPD service in VDI session—If the LPD service is configured in the local **Printer Setup** window, you must restart the client for the LPD service to work in the VDI session.

Updates to Admin Policy Tool and Wyse Management Suite policy settings

NOTE: Wyse Management Suite 4.0 server and Configuration UI package 1.9.728 are required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

- **TLS Control**—TLS 1.2 is the only option available in ThinOS 2303. TLS 1.0 and 1.1 have been removed from the TLS protocol list in **Privacy & Security** > **Security Policy** from ThinOS 2303. TLS 1.0 and 1.1 only applies to ThinOS 2211.

  To improve the security of ThinOS devices, few outdated and less-secure ciphers are removed. It is recommended to disable deprecated ciphers to strengthen security if your environment does not require them:

Table 23. Cipher List and their security status

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Secure
ECDHE-RSA-AES256-SHA384	Secure
ECDHE-RSA-AES128-SHA	Secure
ECDHE-RSA-AES256-SHA	Secure

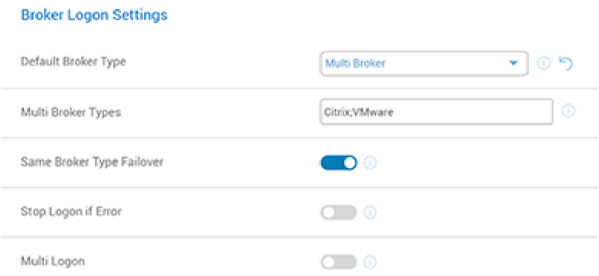
Table 23. Cipher List and their security status (continued)

Ciphers	Security Status
DHE-RSA-AES128-GCM-SHA256	Secure
DHE-RSA-AES256-GCM-SHA384	Secure
DHE-RSA-AES128-SHA256	Secure
DHE-RSA-AES256-SHA256	Secure
DHE-RSA-AES128-SHA	Secure
DHE-RSA-AES256-SHA	Secure
AES128-SHA256	Removed
AES256-SHA256	Removed
AES128-SHA	Removed
AES256-SHA	Removed
AES128-GCM-SHA256	Removed
AES256-GCM-SHA384	Removed
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Secure
ECDHE-ECDSA-AES256-SHA384	Secure
ECDHE-ECDSA-AES128-SHA	Secure
ECDHE-ECDSA-AES256-SHA	Secure
DHE-PSK-AES128-GCM-SHA256	Deprecated
DHE-PSK-AES256-GCM-SHA256	Deprecated
DHE-PSK-AES128-CBC-SHA256	Deprecated
DHE-PSK-AES256-CBC-SHA384	Deprecated
DHE-PSK-AES128-CBC-SHA	Deprecated
DHE-PSK-AES256-CBC-SHA	Deprecated
ECDHE-PSK-AES128-CBC-SHA	Deprecated
ECDHE-PSK-AES256-CBC-SHA	Deprecated
ECDHE-PSK-AES128-CBC-SHA256	Deprecated
ECDHE-PSK-AES256-CBC-SHA384	Deprecated
PSK-AES128-GCM-SHA256	Deprecated
PSK-AES256-GCM-SHA384	Deprecated
PSK-AES128-CBC-SHA	Deprecated
PSK-AES256-CBC-SHA	Deprecated
PSK-AES128-CBC-SHA256	Deprecated
PSK-AES256-CBC-SHA384	Deprecated
RSA-PSK-AES128-GCM-SHA256	Deprecated
RSA-PSK-AES256-GCM-SHA384	Deprecated
RSA-PSK-AES128-CBC-SHA	Deprecated

Table 23. Cipher List and their security status (continued)

Ciphers	Security Status
RSA-PSK-AES256-CBC-SHA	Deprecated
RSA-PSK-AES128-CBC-SHA256	Deprecated
RSA-PSK-AES256-CBC-SHA384	Deprecated
ECDHE-ECDSA-CHACHA20-POLY1305	Deprecated
ECDHE-RSA-CHACHA20-POLY1305	Deprecated
DHE-RSA-CHACHA20-POLY1305	Deprecated
RSA-PSK-CHACHA20-POLY1305	Deprecated
DHE-PSK-CHACHA20-POLY1305	Deprecated
ECDHE-PSK-CHACHA20-POLY1305	Deprecated
PSK-CHACHA20-POLY1305	Deprecated
SRP-RSA-AES-256-CBC-SHA	Deprecated
SRP-AES-256-CBC-SHA	Deprecated
SRP-RSA-AES-128-CBC-SHA	Deprecated
SRP-AES-128-CBC-SHA	Deprecated
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACHA20_POLY1305_SHA256	Deprecated

- **Granular Control of Troubleshooting in Account Privileges**—Added **Granular Control of Troubleshooting** in **Privacy & Security** > **Account Privileges**. When you enable Troubleshooting with Customize privilege level, you can select the tabs in this drop-down list to enable them.
- **New BIOS pages**—Added new BIOS pages for Dell Latitude 3440, Dell Latitude 5440, and OptiPlex All-in-One 7410.
- **Deep Sleep Control**—Added **Deep Sleep Control** option in Dell Wyse 5070 and Dell Wyse 5470 AIO BIOS pages.
- **Wake on LAN - LAN or SFP NIC**—Added **LAN or SFP NIC** in **Wake on LAN** drop-down list in Dell OptiPlex 3000 Thin Client BIOS and set it as the default value. If you set **Wake on LAN** value as **LAN or SFP NIC**:
  - On thin clients with SFP, BIOS is set as **LAN or SFP NIC**.
  - On thin clients without SFP, BIOS is set as **LAN only**.
- **PXE Boot Support and Secure Boot Enable**—Changed the default value of **PXE Boot Support** from **Enabled** to **Disabled** and default value of **Secure Boot Enable** from **Disabled** to **Enabled** for all system BIOS pages.
- **Select Auto Renew Time Frame**—Added **Select Auto Renew Time Frame** under **Privacy & Security** > **SCEP** > **Enable Auto Renew**. The values for this option ranges from 10% to 100%, and the default value is set at 50%.
- **Enable NLA**—The **Enable NLA** option is in **Session Settings** > **RDP and AVD Session Settings**, and by default the option is enabled. If enabled, you can verify users before connecting to an RDP session.
- **Microsoft Teams Optimization**—This option is in **Session Settings**>**RDP and AVD Session Settings**, and by default the option is enabled. If enabled, the AVD media of Microsoft Teams is optimized in RDP protocol sessions. If disabled, the AVD media of Microsoft Teams is not connected. You must restart Microsoft Teams reboot for this option to take effect.
- **Stop Logon If error**
  - In **Broker Settings** > **Global Broker Settings** if you select the **Default Broker Type** as **Citrix Virtual Apps and Desktop**, the name of policy is changed from **Multi Domain** to **Stop Logon If Error**. There is no change in function as this is merely a change in the policy name.
  - For ThinOS 2211 or earlier versions, in **Broker Settings** > **Global Broker Settings** if you select the **Default Broker Type** as **Citrix Virtual Apps and Desktop**, the **Multi Domain** policy is displayed only when you enable the **Multi Farm** policy.
  - On ThinOS 2303 and later versions, in **Broker Settings** > **Global Broker Settings** if you select the **Default Broker Type** as **Citrix Virtual Apps and Desktop**, the **Stop Logon If Error** policy is displayed only when **Multi Logon** policy is disabled.
- **Multi Broker**—Added **Multi Broker** option for the **Default Broker Type** field in **Broker Settings** > **Global Broker Settings**. With this option you can use **Same Broker Type Failover**, **Stop Logon if Error**, **Multi Logon**, **Sequential Domain**, and other multibroker features when signing in.



Broker Logon Settings

Default Broker Type: Multi Broker

Multi Broker Types: Citrix;VMware

Same Broker Type Failover: ●

Stop Logon if Error: ○

Multi Logon: ○

Figure 1. Multi Broker in Broker Logon Settings

- **Multi Broker Types**—You can set the logging in sequence of the Broker agent type. Use a semicolon to separate different Broker agent types including Citrix, VMware, RDS, Other, Teradici, and Amazon. The default value of this policy is **Citrix; VMware**. The value in this parameter is case insensitive.
- **Same Broker Type Failover**—Enabling this policy enables failover sign-on when connecting to one Broker agent type. When the policy is enabled, only the first valid Broker agent of the same protocol logs in. If disabled, all valid Broker agents of the same protocol can log in.
- **Stop Logon if Error**—This policy is displayed only when **Multi Logon** policy is disabled. You can enable this policy to stop the logging in process and raise an error when login has failed when using a Broker agent. The policy is disabled by default.
- **Multi Logon**—Enabling this policy gives you the option to enter multiple credentials in case multiple Broker agent types are specified. By disabling this policy, you can log in to the specified Broker agent type with only one credential. The policy is enabled by default.

  > **NOTE:** When the **Multi Logon** policy is enabled, a different Broker agent logon page is displayed in the login window when waiting to enter credentials. When logging in using Multi Farm policy with Multi Logon disabled, only the general ThinOS login window is displayed.

  > **NOTE:** When the ThinOS client is locked with multiple Broker agents, you can use any password of the different Broker agents to unlock the client.
- **Sequential Domain**—This policy is displayed only when Multi Logon policy is enabled. You can enable this policy to authenticate all domains configured in **Login Settings** > **Domain List**. The policy is disabled by default.

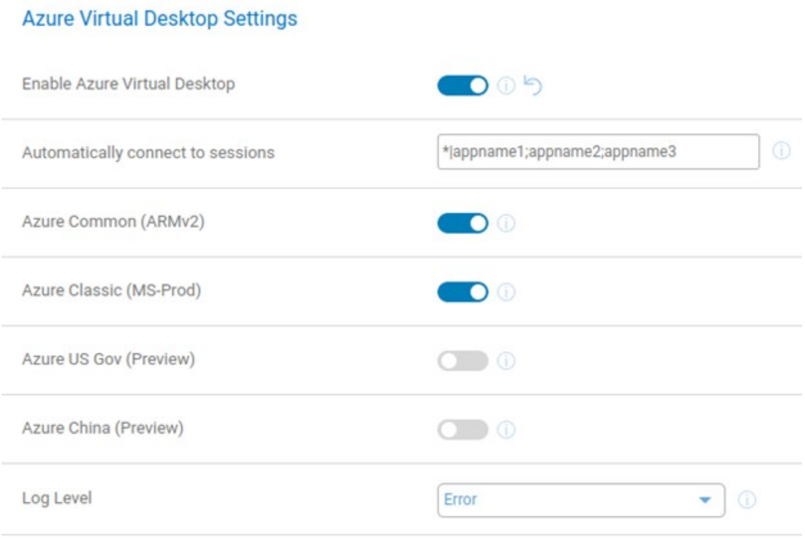
- **Added input validation for SMB printer host URL, printer name, and queue**—The SMB printer host URL format is `\\host\printer`, If the URL format does not match, the policy is not saved. The special characters ``-_@%^*() +=~?/.,:` `` are only allowed for the below fields:
  - Local Printer Settings - Name
  - LPD Printer Settings - Queue, Name
  - SMB Printer Settings - Local Name
- **Enable Expert Mode Log**—This option is in **Services** > **Troubleshooting Settings** and is disabled by default. If you enable this option, the full event logs are displayed in **System Information** under **Event Log**.
- **Clear Logs on Shutdown or Reboot**—This option is in **Services** > **Troubleshooting Settings** and is disabled by default. If you enable this option, ThinOS clears the logs or coredump files when shutting down or rebooting the client.
- **Disable Floatbar**—Added **Disable Floatbar** in **Personalization** > **User Experience Settings**. When the system mode is set to **Modern** mode and **Disable Floatbar** is enabled, the floatbar is disabled and the floatbar can only be displayed by pressing Windows key on the keyboard when focus is on the ThinOS desktop.
- **Show Taskbar when mouse, Delay Taskbar Activation in Milliseconds**—Added a new option **Show Taskbar when mouse, Delay Taskbar Activation in Milliseconds** in **Personalization** > **User Experience Settings**
  - When the system mode is set to **Classic** mode and **Hide Taskbar** is enabled, you can also set the **Show Taskbar when mouse** option to show the taskbar when moving the mouse.
  - If you want to delay when the taskbar is displayed, you can set **Show Taskbar when mouse** to **Delay** and set the value of **Delay Taskbar Activation in Milliseconds** to **Delay Taskbar**. This delays the display of the taskbar.
  - If the value of **Delay Taskbar Activation in Milliseconds** is set to **0**, taskbar is disabled and can only be displayed by pressing Windows key on the keyboard when the focus is on the ThinOS desktop.
- **Enable Performance History**—**Enable Performance Retrospective** is renamed to **Enable Performance History** in **Services** > **Troubleshooting Settings**.
- **OpenVPN configuration**—The option is added to **Network Configuration** > **VPN Settings** > **VPN**, and this option is used to upload the .ovpn files required to connect to the VPN servers.
- **OpenVPN**—Added OpenVPN in **Network Configuration** > **VPN Settings** > **VPN Connection Settings**. Here are the steps to add OpenVPN in VPN connection settings:
  1. Click **Add Row**.

2. Select **OpenVPN** in **Type** list.
3. Enter the required information and import the `.ovpn` file.
4. Click **Save & Publish**.

Here are the steps to connect to OpenVPN:

1. Power on the thin client.
2. Go to **Admin Policy Tool** > **Advanced > Network Configuration** > **VPN Settings** > **Upload OpenVPN Config File** > **Save & Publish**
3. Go to **System Settings** > **VPN Manager**.
4. Click **Open VPN**.
5. Click **+** to add the VPN details.
6. In the **Name** field, enter `Test`.
7. In the **Server** field, enter `vpn.devconnectprogram.com`.
8. In **Type**, select **OVPN Config File**.
9. Enter the username and password.
10. Select **OVPN file** from the drop-down list.
11. Click **OK**.

- **Change in Azure Virtual Desktop Settings interface**—ThinOS has made interface changes to support multiple Azure Clouds, so the Admin Policy Tool or Wyse Management Suite page also has corresponding changes:



Azure Virtual Desktop Settings

Enable Azure Virtual Desktop	☑
Automatically connect to sessions	*|appname1;appname2;appname3
Azure Common (ARMv2)	☑
Azure Classic (MS-Prod)	☑
Azure US Gov (Preview)	□
Azure China (Preview)	□
Log Level	Error

Figure 2. Azure Virtual Desktop Settings

- **Enable Fast Disconnect key for Sign Off**—Added a new policy **Enable Fast Disconnect key for Sign Off** in **Personalization** > **Shortcut Keys**. If **Enable Fast Disconnect key for Sign Off** option is enabled, pressing the key that is defined in **Fast Disconnect Key** policy disconnects all sessions and returns to logon window.
- **Timer When Plugged in**—Changed the default value of **Timer When Plugged in** in **System Settings** > **Power Sleep Settings** from 30 minutes to 15 minutes.
- **Enable Display Port Audio**—Added new option **Enable Display Port Audio** in **Peripheral Management** > **Audio**. Enable or disable this option to enable or disable the display audio feature on all platforms except 3040.
- **Added The Maximum Retries for Downloading File and The Interval Time for Each Retry options for WDA Settings**—**The Maximum Retries for Downloading** specifies the maximum retries for downloading file from each Wyse Management Suite file repository. The supported values are from one to nine, while the default is three. **The Interval Time for Each Retry** specifies the random interval in seconds before each retry occurs. The supported value is zero to 600, while the default value is zero.

Tested environments matrix

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

Table 24. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.0 547
Configuration UI package for Wyse Management Suite	WMS 4.0 547: 1.9.728
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 25. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows 11	Windows Server 2016	Windows Server 2019	Windows Server 2022	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Tested	Not tested	Tested	Tested	Not tested	Tested
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2212	Tested	Tested	Tested	Tested	Tested	Tested

Table 26. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2016 APPs	Windows Server 2019 APPs	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Not tested	Tested	Tested	Not tested	Tested—Only basic connection is tested on Ubuntu 20.04
VMware Horizon 2206	Tested	Tested	Tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2209	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested	Not tested	Not tested
VMware Horizon 2212	Not tested	Not tested	Tested	Tested	Tested	Tested	Tested	Tested	Not tested

Table 27. Test environment – VMware Horizon Cloud

Horizon Cloud	Windows 10	Windows Server 2016
Build Version: 19432376	Horizon Agent Installer - 21.3.0.19265453	Horizon Agent Installer - 21.3.0.19265453

Table 28. Test environment—Microsoft RDP

Microsoft RDP	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
Remote Desktop Services 2016	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2019	Not tested	Tested	Not tested	Not tested	Not tested	Tested	Tested

Table 29. Test environment—AVD

Azure Virtual Desktop	Windows 11	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
2019 (MS-Prod)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested
2020 (ARMv2)	Tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested

Table 30. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2) Citrix Virtual Apps and Desktops 7 2212	Windows 10	2.9.500	2.9.500	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				
	Windows server 2022				

Table 31. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 32. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	14.1.3.307560.10	14.1.3.57560	14.1.4.57561
	Windows server 2016			
	Windows server 2019			

Table 32. Tested environment—JVDI (continued)

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2) Citrix Virtual Apps and Desktops 7 2212	Windows server 2022			

Table 33. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	14.1.3.57560.10	14.1.3.57560	14.1.4.57561
	Windows server 2016			
	Windows server 2019			

Table 34. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2) Citrix Virtual Apps and Desktops 7 2212	Windows 10	5.13.0.22460.2	5.13.0 (22460)
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 35. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	5.13.0.22460.2	5.13.0 (22460)
	Windows server 2016		
	Windows server 2019		

Table 36. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.13.0.22460.2	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		

Table 37. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2) Citrix Virtual Apps and Desktops 7 2212	Windows 10	43.2.0.25211.4	43.2.0.24639
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 38. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	43.2.0.25211.4	43.2.0.24639
	Windows server 2016		
	Windows server 2019		

Table 39. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2) Citrix Virtual Apps and Desktops 7 2212	Windows 10	43.2.1.18.5	43.2
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 40. Tested environment—Cisco Webex Meetings

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2209	Windows 10	43.2.1.18.5	43.2
	Windows server 2016		
	Windows server 2019		

Table 41. Tested environment—RingCentral

VMWare VDI	Operating system	RingCentral Package
Horizon 2111 Horizon View 7.13.2	Windows 10	23.1.10.5
	Windows server 2016	
	Windows server 2019	

Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

NOTE: The supported peripherals are not limited to the peripherals devices listed in this section.

Table 42. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

Product Category	Peripherals	3040	5070	5470 AIO	5470
Audio Devices	Dell Pro Stereo Headset – UC150 – Skype for Business	Supported	Supported	Not Available	Supported
	Dell Pro Stereo Headset - Skype for Business - UC350	Supported	Supported	Supported	Supported
	Dell Professional Sound Bar (AE515M)	Supported	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Not Available	Supported	Not Available	Not Available

Table 42. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Not Available	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Not Available	Supported	Supported
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0	Not Available	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	DellUSB Wired Optical Mouse - MS116	Supported	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported

Table 42. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white	Not Available	Not Available	Not Available	Not Available
	SEAL SHIELD MEDICAL GRADE OPTICAL (Mouse)	Not Available	Not Available	Not Available	Not Available
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white	Not Available	Not Available	Not Available	Not Available
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white	Not Available	Not Available	Not Available	Not Available
	Dell Wireless Mouse - WM126_BLACK - Rosewood	Not Available	Not Available	Not Available	Not Available
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Not Available	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Not Available	Supported	Not Available	Supported
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI - DBQAUBC064 - DBQAUBC064	Not Available	Supported	Not Available	Not Available

Table 42. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Not Available	Supported	Not Available	Not Available
	Trendnet USB to Serial Converter RS-232	Not Available	Supported	Supported	Supported
	Dell Adapter - HDMI to DVI - DAUARBN004 - DAUARBN004	Not Available	Not Available	Not Available	Supported
	Dell Adapter - HDMI to VGA - DAUBNBC084 - DAUBNBC084	Not Available	Not Available	Not Available	Supported
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232	Not Available	Not Available	Supported	Supported
Displays	E1916H	Supported	Supported	Supported	Not Available
	E2016H	Supported	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported	Supported
	E2216H	Not Available	Supported	Supported	Supported
	E2216Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2218HN	Supported	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported	Supported
	E2318H	Supported	Supported	Supported	Supported
	E2318HN	Not Available	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported	Supported
	E2420HS	Not Available	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported	Supported
	E2720HS	Not Available	Supported	Supported	Supported
	P2016	Not Available	Supported	Not Available	Not Available
	P1917S	Supported	Supported	Not Available	Not Available
	P2017H	Supported	Not Available	Not Available	Not Available
	P2018H	Not Available	Not Available	Not Available	Supported
	P2217	Supported	Supported	Not Available	Not Available
	P2217H	Supported	Supported	Not Available	Not Available
	P2219H	Supported	Supported	Not Available	Supported
	P2219HC	Supported	Supported	Not Available	Supported

Table 42. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	P2317H	Supported	Supported	Not Available	Not Available
	P2319H	Not Available	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Supported	Not Available
	P2417H	Supported	Supported	Not Available	Not Available
	P2418D	Supported	Not Available	Not Available	Not Available
	P2418HT	Supported	Supported	Supported	Not Available
	P2418HZ	Supported	Supported	Not Available	Not Available
	P2419H	Supported	Supported	Supported	Supported
	P2419HC	Supported	Supported	Not Available	Supported
	P2421D	Supported	Supported	Not Available	Supported
	P2421DC	Not Available	Supported	Not Available	Supported
	P2719H	Supported	Supported	Supported	Supported
	P2719HC	Supported	Supported	Not Available	Supported
	P2720D	Supported	Supported	Not Available	Supported
	P2720DC	Not Available	Supported	Not Available	Supported
	P3418HW	Supported	Supported	Supported	Not Available
	P4317Q	Not Available	Supported	Supported	Not Available
	MR2416	Supported	Supported	Not Available	Not Available
	U2415	Supported	Supported	Supported	Not Available
	U2419H	Supported	Supported	Supported	Supported
	U2419HC	Supported	Supported	Not Available	Supported
	U2518D	Supported	Supported	Supported	Not Available
	U2520D	Supported	Supported	Supported	Supported
	U2718Q (4K)	Supported	Supported	Supported	Supported
	U2719D	Supported	Supported	Supported	Supported
	U2719DC	Supported	Supported	Not Available	Supported
	U2720Q	Supported	Supported	Supported	Supported
	U2721DE	Not Available	Supported	Supported	Supported
	U2421HE	Not Available	Not Available	Supported	Supported
	U4320Q	Not Available	Supported	Supported	Supported
	U4919DW	Not Available	Supported	Not Available	Not Available
Networking	Add On 1000 Base-T SFP transceiver (RJ-45)	Not Available	Supported	Not Available	Not Available
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Not Available	Supported

Table 42. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
Storage	Dell Portable SSD, USB-C 250GB	Not Available	Supported	Not Available	Supported
	Dell External Tray Load ODD (DVD Writer)	Not Available	Supported	Not Available	Supported
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported	Supported
	Sun microsystem SCR 3311	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Not Available	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Not Available	Supported	Not Available	Supported
Printers	Dell Color Multifunction Printer - E525w	Supported	Not Available	Not Available	Not Available
	Dell Color Printer-C2660dn	Supported	Supported	Not Available	Not Available
	Dell Multifunction Printer - E515dn	Supported	Not Available	Not Available	Not Available

Supported ecosystem peripherals for Latitude 3420

Table 43. Supported ecosystem peripherals for Latitude 3420

Product Category	Peripherals
Displays	Dell U3419W
	Dell 24 Monitor E2420HS - E2420HS
	Dell U2718Q
	Dell U2719D
	Dell P2719H
	Dell P2715Q
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W ⓘ **NOTE:** Bluetooth connection is not supported.
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W

Table 43. Supported ecosystem peripherals for Latitude 3420 (continued)

Product Category	Peripherals
	Dell Keyboard KB216
Audio Devices	Dell Pro Stereo Headset - UC150 - UC150 - Lemmy - UC150
	Dell Pro Stereo Headset UC350
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Supported ecosystem peripherals for Latitude 3440

ⓘ **NOTE:** The supported peripherals are not limited to the peripherals devices listed in this section.

Table 44. Supported ecosystem peripherals for Latitude 3440

Product Category	Peripherals
Monitors	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 27 Monitor - E2723HN - E2723HN
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Bluetooth connection is not supported.)
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Keyboard KB216
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022
	Dell Pro Webcam - Falcon - WB5023
Docking station	Dell USB-C Dock - WD19S 130W - Salomon S - WD19S 130W
Cables, Dongles, Adapters	Dell 7-in-1 USB-C Multiport Adapter - Slayer 3 MLK - DA310
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Supported ecosystem peripherals for Latitude 5440

ⓘ **NOTE:** The supported peripherals are not limited to the peripherals devices listed in this section.

Table 45. Supported ecosystem peripherals for Latitude 5440

Product Category	Peripherals
Monitors	Dell 27 USB-C HUB Monitor - P2723DE - P2723DE
	Dell Collaboration 24 Monitor - C2423H - C2423H
	Dell U3219Q (Does not support Type C to HDMI convertor)
Input Devices	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Keyboard KB216
Audio/Video	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Speakerphone - Mozart - SP3022
	Dell Pro Webcam - Falcon - WB5023

Table 45. Supported ecosystem peripherals for Latitude 5440 (continued)

Product Category	Peripherals
	Dell Pro Stereo Headset UC350
Docking station	Dell Thunderbolt 4 Dock - WD22TB4 - Salomon TBT MLK - WD22TB4
Cables, Dongles, Adapters	Dell 7-in-1 USB-C Multiport Adapter - Slayer 3 MLK - DA310

Supported ecosystem peripherals for OptiPlex 3000 Thin Client

ⓘ **NOTE:** The supported peripherals are not limited to the peripherals devices listed in this section.

Table 46. Supported ecosystem peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio Devices	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Headset - Cortez - WH3022.
	Logitech BRIO 4K Ultra HD Webcam - 960-001105 - 960-001105
	Logitech C525 HD Webcam - 960-000715 - 960-000715
	Logitech C930e HD Webcam - 960-000971 - 960-000971
	Dell Pro Stereo Soundbar - AE515M - AE515M - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - AC511M - AC511M - Potential M
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P
Input Devices	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
Displays	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell 24 Monitor - P2422H - P2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE

Table 46. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell 27 Monitor - P2722H - P2722H
	Dell 22 Monitor - P2222H - P2222H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell 20 Monitor E2020H - E2020H
	Dell 27 Monitor - P2720D - P2720D
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell 24 Monitor E2420HS - E2420HS
	Dell 27 Monitor - P2720D - P2720DC
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 27 Monitor E2720HS - E2720H
	Dell 27 Monitor E2720H - E2720HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 19 Monitor E1920H - E1920H
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell 24 Monitor E2420H - E2420H
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Supported ecosystem peripherals for OptiPlex 5400 All-in-One

Table 47. Supported ecosystem peripherals for OptiPlex 5400 All-in-One

Product Category	Peripherals
Displays	Dell 24 Monitor - P2421D
	Dell UltraSharp 24 Monitor - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Keyboard KB216

Table 47. Supported ecosystem peripherals for OptiPlex 5400 All-in-One (continued)

Product Category	Peripherals
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Supported ecosystem peripherals for OptiPlex All-in-One 7410

ⓘ **NOTE:** The supported peripherals are not limited to the peripherals devices listed in this section.

Table 48. Supported ecosystem peripherals for OptiPlex All-in-One 7410

Product Category	Peripherals
Monitors	Dell 24 Monitor - P2423D - P2423D
	Dell UltraSharp 24 Monitor - U2422H - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Keyboard KB216
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Third-party supported peripherals

Table 49. Third-party supported peripherals

Product Category	Peripherals
Audio Devices	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth （ link 360 ）
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Support USB only, not support Bluetooth)
	Plantronics Blackwire 5220 Series
	Plantronics AB J7 PLT
	Plantronics Blackwire C5210
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Calisto P820-M
	Plantronics Voyager 6200 UC

Table 49. Third-party supported peripherals (continued)

Product Category	Peripherals
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER SC 660 USB ML
	SENNHEISER USB SC230
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SP 10 ML Speakerphone for Lync
	Sennheiser SDW 5 BS-EU
	Logitech S-150
	POLYCOM Deskphone CX300
	PHILIPS - analog
	Logitech h150 - analog
	LFH3610/00 SPEECH MIKE PREMIUM (only support redirect)
	Nuance PowerMic II (Recommend redirecting whole device)
	Olympus RecMic DR-2200 (Recommend redirecting whole device)
	Apple AirPods (2nd generation)
	Apple AirPods (3rd generation)
	Apple AirPods Pro (1st generation)
	Jabra elite 3
Input Devices	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	ELO ET2202L-2UWA-0-BL-G
Camera	Logitech C920 HD Pro Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Logitech C930e HD Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C910 HD Pro Webcam
	Logitech C925e Webcam
	Poly EagleEye Mini webcam
	Logitech BRIO 4K Webcam
	Jabra PanaCast 4K Webcam
Storage	SanDisk cruzer 8 GB

Table 49. Third-party supported peripherals (continued)

Product Category	Peripherals
	SanDisk cruzer 16G
	SanDisk USB 3.1 and Type-C 16 GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32 GB
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	IDBridge CT31 PIV
	Gemalto IDBridge CT710
	GemPC Twin
Proximity card readers	RFIDeas RDR-6082AKU
	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80
	Imprivata HDW-IMP-82
	Imprivata HDW-IMP-82-BLE
	OMNIKEY 5025CL
	OMNIKEY 5326 DFR
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM
	OMNIKEY 5325 CL
	KSI-1700-SX Keyboard

Table 49. Third-party supported peripherals (continued)

Product Category	Peripherals
Fingerprint readers	KSI-1700-SX Keyboard
	Imprivata HDW-IMP-1C
	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader
Printers	HP M403D
	Brother DCP-7190DW
	Lexmark X864de
	HP LaserJet P2055d
	HP Color LaserJet CM1312MFP
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR (BLEdongle)
Teradici remote cards	Teradic host card 2220
	Teradic host card 2240
Others	Intuos Pro Wacom
	Wacom One
	Infinity IN-USB-2 Foot pedal

Known issues and Limitations with PowerMic devices

- Nuance PowerMic sound dictation does not work properly in PCoIP sessions. This causes the Dragon Medical One (DMO) software to stop responding after some time.
- Hot plugging in or plugging out the PowerMic device when it is working may cause the DMO software to stop responding. As a workaround, relaunch the software.
- It is recommended to use full redirection of the whole device in Blast and Citrix sessions. If you split redirect some buttons in Blast and Citrix sessions and plug out and plug-in PowerMic, the device is not recognized. In Blast sessions, you must also disable Bluetooth redirection or it ThinOS works abnormally.
- PowerMic stops working in the DMO software inside VMware PCoIP sessions after inserting a USB drive to the thin client. This issue occurs only if the USB drive is redirected. As a workaround, use USB disk Map settings instead of USB disk Redirection.
- PowerMic does not redirect to VMware PCoIP sessions when you do the following in sequence:
  1. Sign off from the Broker agent without closing an application.
  2. Disconnect and connect PowerMic to a different USB port.
  3. Sign into the Broker agent again.
- PowerMic does not work in DMO software after disconnecting PowerMic II and connecting PowerMic III when a VMware PCoIP session is open.
- The mouse pointer is not displayed in VMware PCoIP sessions when using PowerMic As a workaround, sign out and sign into the Broker agent.

Workaround

Workaround for the above mentioned limitations are:

- If you are using Power Mic 2 and 3, you must enable **Allow USB Imaging Family Device** and add `0x05541001`, `NoDriver` in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Session Settings > Session Settings**.
- If you are using Power Mic 4, you must enable **Allow USB Imaging Family Device** and add `0x05540064`, `NoDriver` in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Session Settings > Session Settings**.

Fixed issues

Table 50. Fixed issues

Issue ID	Description
DTOS-16250	Critical user interface error upon booting—CIPS-30559 and CIPS-29435
DTOS-16181	Group selection window is taking time to load in OptiPlex 3040—CIPS-30504.
DTOS-16002	Thin client is not locking when using the key combination Ctrl+Alt+Number/Lock/Delete—CIPS-30409.
DTOS-15951	Keyboard does not work within EPIC software—CIPS-30336.
DTOS-15948	Imprivata Logoff does not work properly—CIPS-30296.
DTOS-15905	RDP connection cannot be deleted when privilege level is set to **Custom**—CIPS-30334.
DTOS-15884	New connections can be added when privilege level is set to **None**—CIPS-30263.
DTOS-15880	Ethernet or Network settings do not get updated on OptiPlex 3000 Thin Client—CIPS-30312.
DTOS-15719	Azure virtual desktop connection fails to load resources with some user accounts—CIPS-30247.
DTOS-15718	Cannot add account when logging in to AVD sessions—CIPS-30239.
DTOS-15636	VDI session is not displayed in AVD session—CIPS-28216.
DTOS-15558	AVD session disconnects when browsing graphical websites—CIPS-30126.
DTOS-15474	**DHCP OT 12** hostname is not taken as expected in ThinOS 9—CIPS-30004.
DTOS-15458	The **Change password** dialog box does not prompt or stops responding—CIPS-29828.
DTOS-15457	Desktop icons are not displayed after logging into Azure—CIPS-29800.
DTOS-15132	Some users get **Download ARMv2 feeds failed** error message—CIPS-29697.
DTOS-15031	Taskbar covers the bottom of published apps in ThinOS 2208 with dual monitors that are connected in **Classic** Mode—CIPS-29126.
DTOS-14795	Audio Manual Override does not work in Wyse Management Suite with ThinOS 9—CIPS-29669.
DTOS-14772	RDP session disconnects when Ctrl+C key combination is used inside the VDI session—CIPS-29723.
DTOS-14755	User cannot log in to RDP broker—CIPS-29291.
DTOS-14733	RDP session disconnects when copying 24-digit string—CIPS-29663.
DTOS-14337	Unable to authenticate Citrix session using SafeNet AT SC650 Smartcard | ThinOS 2208 | 5070—CIPS-29513
DTOS-14278	Copy-Paste functionality does not work as expected with Citrix published apps in devices with ThinOS versions later than 9.x—CIPS-29125.
DTOS-14183	Critical user interface error upon booting—CIPS-29435
DTOS-14123	RDP connection attempt keeps prompting for credentials—CIPS-29136.
DTOS-14037	Need advice on how to Schedule Shutdown or Reboot Settings and the interactions for ThinOS in Wyse Management Suite—CIPS-29087.

Table 50. Fixed issues (continued)

Issue ID	Description
DTOS-13808	Unable to get issuer certificate with Storefront—CIPS-29078
DTOS-13765	Taskbar cuts off the bottom of Citrix published App window—CIPS-27798.
DTOS-13732	**Cannot resolve host name** error message is displayed when devices are in **Select group** or a child group—CIPS-28978.
DTOS-13536	Keyboard does not work within Epic Software—CIPS-28986.
DTOS-13482	Cannot change language by pushing a toggle key on the Korean keyboard—CIPS-28900.
DTOS-13407	Unable to log in to WVD desktop while connecting through ARMv2 with ThinOS 2208—CIPS-28860
DTOS-13307	Wyse application displays as rendering or updating on the backend Citrix VDI session in ThinOS 2208—CIPS-28645.
DTOS-13233	Imported ThinOS 2208 local config does not contain the admin password—CIPS-28766.
DTOS-12798	ThinOS 2205 and 2208 cannot connect through RDS gateway when a port is provided—CIPS-28530.
DTOS-12682	Canon DR-C225 or C225W USB Scanner does not work as expected in Citrix sessions—CIPS-28403.
DTOS-12633	Display of Legal Notice causes Blast-published applications to not connect—CIPS-28474.
DTOS-12626	Keyboard-Mouse switch and mouse movement fails on ThinOS 2208 with IHSE Draco U—CIPS-28441.
DTOS-12340	If privilege level is set to **Custom**, user can edit connections in ThinOS 9.x—CIPS-28167.
DTOS-12188	ThinOS 9.3.1129 (Blast) sends the wrong client keyboard layout to Horizon Agent 7.13 installed on a Windows 10 system—CIPS-28078.
DTOS-12163	Azure EMR Application (Allscripts) has rendering, updating, and focus issues—CIPS-26724.
DTOS-11985	Bluetooth enumeration and redirection does not work—CIPS-27870.
DTOS-11084	After upgrading to ThinOS 9.x, ThinOS client does not get TSCAL licenses—CIPS-25980
DTOS-15033	SMB printing does not work when printer username and password field is blank. Enter VDI broker credentials.
DTOS-15032	Manual override default username, password, domain fields are not populated using Imprivata authentication.
DTOS-16278	Unable to unlock the Horizon session with Machine Certification through UAG on 5070 devices with ThinOS 2211—CIPS-30548.
DTOS-14363	**Error: The session id is expired, please retry to log in the broker** error message is displayed on 5070 devices with ThinOS 9.3—CIPS-29534.
DTOS-14439	When Fast Disconnect option is set to **SignOff**, the functionality differs between ThinOS 9.x and 8.6.
DTOS-13698	Unable to hide or disable the domain login field with Imprivata config in ThinOS 9.x
DTOS-12114	ThinOS cloud sign-in screen displays a white screen when network connection is lost.
DTOS-14000	No desktops available
DTOS-14093	PCL5 printer protocol is supported in RDS sessions on ThinOS 2303—CIPS-29222
DTOS-12907	Printer redirects to Microsoft Publisher Imagesetter in RDP sessions on OptiPlex 3000 with ThinOS 9.3.1129—CIPS-27566.
DTOS-16072	EAP process is not complete before thin client gets DHCP address—CIPS-28925.
DTOS-16004	Touchscreen calibration is not available in ThinOS 2211 on OptiPlex thin clients—CIPS-30294.

Table 50. Fixed issues (continued)

Issue ID	Description
DTOS-13471	USB scanner and other USB devices stop working after powering off or on the ThinOS device in Citrix session—CIPS-26088.
DTOS-15908	Keyboard randomly stops working in EPIC hyperspace application on OptiPlex 300 with ThinOS 2211—CIPS-30345.
DTOS-15950	Azure virtual desktop connection fails to load resources with some user accounts—CIPS-30249.
DTOS-15717	OptiPlex 3000 thin client with Intel AX210 card cannot connect to WiFi 6E 6 GHz—CIPS-30233.
DTOS-15330	SAML2 credentials during Horizon login is not valid on ThinOS 2208—CIPS-28688.
DTOS-12621	ELO Accutouch 2218 on OptiPlex 3040 does not work or calibrate in ThinOS 9.3. The touchscreen works properly in ThinOS 8.6—CIPS-27958.

Known issues

Table 51. Known issues

Issue ID	Description	Workaround
DTOS-16325	When changing playback devices from Headset to HD Audio-1, the Volume icon on system tray does not display correct device in Classic mode.	Adjust volume, playback device name is updated.
DTOS-16239	HD audio and USB, Bluetooth, Wireless headsets are not listed in AVD Microsoft Teams calls when multiple audio devices are connected. You can only use the ThinOS default audio device.	No workaround
DTOS-16238	Saved recording device details do not show up in event log after plugging in and plugging out the USB headset.	No workaround
DTOS-16234	HD audio-2 is shown in Latitude 3440 thin client playback or record device list.	No workaround
DTOS-16224	AirPods has no audio in PCoIP session and disappears locally in ThinOS.	No workaround
DTOS-16223	Bluetooth headset does not work and audio plays on the client when switching the VMware Blast session to PCoIP session.	No workaround
DTOS-16207	Admin Policy Tool shows a blank page when clicking **Browse** button to upload a valid application package. For example, `Citrix_22.12.0.12_1_signed.pkg`	Open the admin policy tool again.
DTOS-15999	Both **Cancel** and **Open** button is not displayed in **Open Files** page when clicking **Browse** button and a .cer format certificate from a USB device is in the admin policy tool page.	No workaround
DTOS-15923	Mapped printer prints two pieces of paper in RDP printing or LPD service in RDP.	This issue occurs only on Brother DCP-7190 DW Printer.
DTOS-15911	When USB devices redirection is disabled or exclude audio devices and exclude video devices is enabled, audio, and video devices are redirected into VMware Blast Windows 11 session.	No Workaround
DTOS-15759	Redirected camera does not work smoothly and flickers in Citrix session on OptiPlex 3000.	Configure camera mapping instead.

Table 51. Known issues (continued)

Issue ID	Description	Workaround
DTOS-15747	Unable to swap C2423H monitor camera in VMware Blast sessions.	No Workaround
DTOS-15676	Local graphical interface launch performance in ThinOS 2303 is partially higher than 2208 release version data.	No Workaround
DTOS-15231	PCoIP time out dialog box cannot be closed.	Restart ThinOS.
DTOS-15199	**Integrated Webcam FHD** is displayed two times in Webex Teams, jVDI, Zoom and Webex meetings in the **Devices** drop-down list.	No Workaround
DTOS-15120	Dummy file is displayed in RDP VDI session.	No Workaround
DTOS-14987	Unable to increase audio more than 30% on Dell U3223QZ Monitor.	No Workaround
DTOS-14982	A black screen is observed when launching RDP sessions and changing Orientation to **Portrait** with 1368x768 resolution.	Minimize and restore the RDP session.
DTOS-14966	With Latitude 5440, hot plugging external monitors connected to a WD22TB4 dock results in a black screen.	Reboot with WD22TB4 connected.
DTOS-14844	Timezone that is set in OOBE screen is not displayed in event log.	Restart the client, and the correct time zone is displayed in the event log.
DTOS-14695	VMware Horizon shows a black screen when changing from **Mirror** mode to **Span** mode with two monitors connected.	Set the two screens to the same resolution.
DTOS-14671	APT window is not adjusted in portrait and portrait (flipped).	Use the default resolution of the monitor.
DTOS-14020	After dynamic adjustment, the Blast session is displayed only on the main display and not on second monitor.	Set the second screen as main screen.
DTOS-11652	Some cameras do not work during Microsoft teams call when connected to the USB port on the side of OptiPlex 5400 AIO i7 client.	No Workaround
DTOS-11052	If you plug out an analog headset, the integrated microphone on Latitude 3420 does not work for several seconds.	No Workaround
DTOS-14482	Blast session does not launch in **Window** mode for 3840X2160 resolution on a 4 K monitor.	Use session in Full screen.
DTOS-14461	Mouse gets locked in browser when playing YouTube videos.	The issue does not occur with Bluetooth or 3.5 mm headsets.
DTOS-16669	Audio does not work during record and playback after client is rebooted.	Switch profile to **Streaming** and back to **UC** profile for the device to work.
DTOS-14434	Troubleshooting window is closed when user tries to enable or disable **Capture Debug logs** option.	No Workaround
DTOS-16653	Wake-on-LAN dose not work on OptiPlex 7410 AIO with Realtek RJ45 port.	No Workaround
DTOS-16214	The external 4 K monitor (U2723QX, U2720Q) connected to HDMI port of client displays a black screen after restarting the client.	Turn on **Fast Wakeup** option on monitor.
DTOS-16725	If sleep mode and DisplayPort audio are both enabled, the terminal stops responding for around 5 s when launching any type of VDI session.	Either disable sleep mode or DisplayPort audio.

4

Security package for ThinOS 2211

Release summary

Patch or add-on releases are created to support the existing hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on shipping hardware platforms. This package fixes the following security issues:

- CVE-2022-40304
- CVE-2022-40303
- CVE-2022-43680
- CVE-2017-14634
- CVE-2018-13419
- CVE-2018-19662
- CVE-2018-19661
- CVE-2017-6892
- CVE-2018-19432
- CVE-2018-19758
- CVE-2019-3832
- CVE-2018-13139
- CVE-2017-14246
- CVE-2017-8363
- CVE-2017-14245
- CVE-2017-8365
- CVE- 2017-8361
- CVE-2017-12562
- CVE-2017-8362
- CVE-2019-20367
- CVE-2022-36067

This package is only applicable for ThinOS 2211 (9.3.3099).

Version

Security_Addon_2211_009.pkg

Release date

January 2023

Supported platforms and BIOS versions

The thin clients and their BIOS versions that are supported as part of this release are as follows:

Table 52. Supported platforms and BIOS versions

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.20.0

Table 52. Supported platforms and BIOS versions (continued)

Platform name	BIOS version
Wyse 5470 All-in-One Thin Client	1.17.0
Wyse 5470 Mobile Thin Client	1.16.1
OptiPlex 3000 Thin Client	1.5.3
Latitude 3420 with ThinOS	1.23.2
OptiPlex 5400 All-in-One	1.1.17

Important notes

- The security package is only applicable for ThinOS 2211 (9.3.3099). You need not install this stand-alone package on later ThinOS versions as they contain this fix by default.
- After you install **Security_Addon_2211_009.pkg**, do not uninstall it from ThinOS 2211. If you uninstall the package, the security fix gets removed.
- When you upgrade ThinOS 2211 that has **Security_Addon_2211_009.pkg** installed, to the next version of ThinOS, the package is removed by default. The security fix is included as part of the next ThinOS version.

  ⓘ **NOTE:** If the package is not removed automatically after the upgrade, restart the thin client.

Download the application package

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device.
3. Select the product from the searched results to load the product page.
4. On the product support page, click **Drivers & downloads**.
5. Select the operating system as **ThinOS**.
6. Locate the application package that you require.
7. Download the application package file.

Install the application package using Wyse Management Suite

Prerequisites

- Upgrade the ThinOS firmware to version 2211.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the application package. See, Download the application package.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.

   ⓘ **NOTE:** If you cannot locate the **Application Package Updates** option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse**, and select **Security_Addon_2211_009.pkg**.
6. From the drop-down menu, select the uploaded application package.
7. Click **Save & Publish**.
   The thin client downloads the package to install and restarts.

Results

The security package is installed, and the security issue is fixed.

Security vulnerability changes

- Updated libxml from version 2.9.14 to 2.10.3 to fix the security issue CVE-2022-40304 and CVE-2022-40303.
- Updated expat from version 2.4.8 to 2.5.0 to fix the security issue CVE-2022-43680.
- Updated libsndfile from version 1.0.28 to 1.1.0 to fix the security issue CVE-2017-14634, CVE-2018-13419, CVE-2018-19662, CVE-2018-19661, CVE-2017-6892, CVE-2018-19432, CVE-2018-19758, CVE-2019-3832, CVE-2018-13139, CVE-2017-14246, CVE-2017-8363, CVE-2017-14245, CVE-2017-8365, CVE- 2017-8361, CVE-2017-12562, and CVE-2017-8362.
- Updated libbsd version 0.9.1 to fix the security issue CVE-2019-20367.
- Updated vm2 version 3.9.10 to fix the security issue CVE-2022-36067.

Tested environments matrix

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

Table 53. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	4.0 526
Configuration UI package for Wyse Management Suite	1.9.532
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 54. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows 11	Windows Server 2016	Windows Server 2019	Windows Server 2022	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5)	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2203LTSR	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2206	Tested	Tested	Tested	Tested	Tested	Tested

Table 55. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2016 APPs	Windows Server 2019 APPs	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested

Table 55. Test environment—VMware Horizon (continued)

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2016 APPs	Windows Server 2019 APPs	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Not tested	Tested	Tested	Not tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Not tested	Tested	Tested	Not tested	Tested—Only basic connection is tested on Ubuntu 20.04
VMware Horizon 2206	Tested	Tested	Tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2209	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested	Not tested	Not tested

Table 56. Test environment – VMware Horizon Cloud

Horizon Cloud	Windows 10	Windows Server 2016
Build Version: 19432376	Horizon Agent Installer - 21.3.0.19265453	Horizon Agent Installer - 21.3.0.19265453

Table 57. Test environment—Microsoft RDP

Microsoft RDP	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
Remote Desktop Services 2016	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2019	Not tested	Tested	Not tested	Not tested	Not tested	Tested	Tested

Table 58. Test environment—AVD

Azure Virtual Desktop	Windows 11	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
2019 (MS-Prod)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested
2020 (ARMv2)	Tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested

Table 59. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	2.9.500	2.9.500	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				
	Windows server 2022				

Table 59. Tested environment—Skype for Business (continued)

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 2206					

Table 60. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 61. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	14.1.2.307144_7	14.1.2.307144	14.1.2.57135
	Windows server 2016			
	Windows server 2019			
	Windows server 2022			

Table 62. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10	14.1.2.307144_7	14.1.2.307144_7	14.1.2.307144_7
	Windows server 2016			
	Windows server 2019			

Table 63. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	5.11.9.21750.8	5.11.9 (21750)
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 64. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106 VMware Horizon View 7.13.2	Windows 10	5.11.9.21750.8	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		

Table 65. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.11.9.21750.5	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		

Table 66. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	42.10.0.23814_5	42.10.0.23814
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 67. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10	42.10.0.23814_5	42.10.0.23814
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 68. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	42.10.5.15_3	42.10
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 69. Tested environment—Cisco Webex Meetings

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2111	Windows 10	42.10.5.15_3	42.10
	Windows server 2016		
	Windows server 2019		

Table 70. Tested environment—RingCentral

VMware VDI	Operating system	RingCentral Package
Horizon 2111 Horizon View 7.13.2	Windows 10	22.2.30.44745.1
	Windows server 2016	
	Windows server 2019	

5

ThinOS 2211

Release date

December 2022

Release summary

Patches or Add-on releases are created to support existing platforms or software releases, correct defects, make enhancements, or add minor features.

Current version

ThinOS 2211 (9.3.3099)

Previous version

ThinOS 2208 (9.3.2102)

Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2211 (9.3.3099)**

ⓘ **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2211. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x

ⓘ **NOTE:** If you want to downgrade ThinOS 2211 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2211 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

- In ThinOS 2211, TLS 1.0 and 1.1 are disabled by default. If you want to use TLS 1.0 and 1.1 to connect to any server, you can enable 1.0 and 1.1 using Wyse Management Suite policy. TLS 1.0 and 1.1 is going to be removed in future releases. If you are still using TLS 1.0 and 1.1, update your environment to deploy future releases.
- If you have Wyse Management Suite version 3.8 or earlier, you cannot enable TLS 1.0 and 1.1 using Wyse Management Suite policy. You must update to Wyse Management Suite 4.0.

ⓘ **NOTE:** If you get the error **Could not add account. Please check your account and try again.** when logging in to Citrix or **Login failed!** when logging in to VMware, check whether TLS 1.0 or TLS 1.1 is required by your Citrix or VMware Broker agent to log in.

- There are chances that after the upgrade the device displays a black screen. You may reboot the device to boot it up correctly.
- If the thin client is registered in Wyse Management Suite group 1 and you set Wyse Management Suite group 2 token in group 1 policy, then the group 2 token is applied on GUI but the thin client will still be in group 1. You must reboot the thin client to change the thin client to Wyse Management Suite group 2.

> **NOTE:** Dell Technologies recommends that you set both new ThinOS firmware and new application packages in Group 1, so that thin client installs the files, automatically reboots, and changes to Group 2.

- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
  - Not display a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - Not display any notification if the new firmware or application is downloaded in the same group.
  - Installs the firmware or package after a reboot.
- If you have installed HID_Fingerprint_Reader package, ensure that you have also installed Citrix_Workspace_App package, or you cannot upgrade to ThinOS version 2211.
- If you configure settings, like brokers, locally in ThinOS 2211 and downgrade to ThinOS 2205 or earlier versions using Wyse Management Suite, the settings are lost.
- If you downgrade to ThinOS 2205 or earlier versions using Wyse Management Suite, reboot the system manually again to set a password locally in ThinOS. Otherwise, the password may not be clear.

Prerequisites for firmware upgrade

- Before you upgrade from ThinOS 9.1.x to ThinOS 2211, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the Wake On LAN command through Wyse Management Suite before using any real-time commands. To use the Wake On LAN command, ensure that the Wake On LAN option is enabled in BIOS.

Upgrade from ThinOS 9.1.x to ThinOS 2211 using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the ThinOS 2211 (9.3.3099) firmware to upgrade.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**. The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **OS Firmware Updates**.

   > **NOTE:** If you cannot locate the **OS Firmware Updates** option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse** and select the **ThinOS 2211** firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.
   The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

   > **NOTE:** There are chances that the upgrade might fail with event log stating **Failed to install**. In such an event, you may reboot the device and upgrade again.

   > **NOTE:** To optimize security, application performance, and stability, a design change has been made in ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer

supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

ⓘ **NOTE:** There are chances that the ThinOS background might be in blue color and some features may not work. In this case, you have to reboot the device.

Convert Ubuntu 20.04 with DCA to ThinOS 2211

The conversion is supported on Latitude 3420 and OptiPlex 5400 All-in-One.

Prerequisites

- If you have a device that is running Ubuntu 20.04 operating system, ensure that DCA-Enabler 1.5.0-14 or later versions is installed. For details on how to install DCA-Enabler in Ubuntu operating system and upgrade it, see Dell Wyse ThinOS Migration Guide at www.dell.com/support.

  ⓘ **NOTE:** The device must have a factory-installed Ubuntu 20.04 operating system. If you have custom installed the Ubuntu operating system, you cannot convert it to ThinOS 2211.
- Wyse Management Suite version 3.7 or later versions must be used to convert to ThinOS 2211.
- Ensure that you have connected the device to the external power source using the power adapter.
- Ensure you have enough ThinOS Activation devices licenses on Wyse Management Suite 3.7 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than the device number. If it is not larger, you cannot create the Advanced Policy for conversion.
- The Ubuntu 20.04 devices must be registered to Wyse Management Suite as generic clients. For details on how to register the generic client to Wyse Management Suite, see Dell Wyse ThinOS Migration Guide at www.dell.com/support.
- Ensure you have downloaded the Ubuntu 20.04 to ThinOS 2211 conversion image.
- Extract the Ubuntu 20.04 to ThinOS 2211 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.1-dtos4-amd64_signed.tar.gz` and ThinOS image `ThinOS_2211_9.3.3099.pkg`.

  ⓘ **NOTE:** The ThinOS image `ThinOS_2211_9.3.3099.pkg` can be used for downgrade in the future.

Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the Conversion Installer file `DTOS_Ubuntu_Installer_1.1-dtos4-amd64_signed.tar.gz`
3. Go to **Apps & Data** > **OS Image Repository** > **ThinOS 9.x**, and click **Add Firmware file**.
4. Upload the ThinOS image `ThinOS_2211_9.3.3099.pkg`.
5. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
6. Enter the policy name, select the group in which the Ubuntu devices have been registered, and select **Generic Client** as OS type.
7. Click **Add app**, and select the conversion installer file that was uploaded before from the drop-down menu.
8. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
9. Select the platforms you want to convert in the **Platform Filter** drop-down menu.
10. Click **Save**.

    ⓘ **NOTE:** Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
11. In the next window, click **Yes** to schedule a job.
12. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.
13. Click **Schedule**.

    The Conversion Installer file downloads and installs first followed by the ThinOS image. After installation, the device restarts automatically.

    ⓘ **NOTE:** After you register the converted ThinOS device to Wyse Management Suite, the ThinOS activation devices license is consumed automatically.

    ⓘ **NOTE:** After conversion, ThinOS 2211 is in the factory default status. ThinOS 2211 must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

ⓘ **NOTE:** If the conversion has failed, you can see the error log table below and reschedule the job. Go to **Jobs** > **Schedule APP Policy** to reschedule the job.

If there is a **/usr/dtos** folder in your Ubuntu 20.04 device, you can use the command **cat /var/log/dtos_dca_installer.log** to get the error log. If the conversion has failed, it is recommended to install ThinOS ISO image.

If there is no **/usr/dtos folder** in your Ubuntu 20.04 device, go to the **WMS Server Jobs** page to check the error messages.

Table 71. Error Log table

Error Log	Resolution
No AC plugged in	Plug in power adapter, reschedule job
Platform Not Supported	This hardware platform is not supported
Error mounting recovery partition	The Ubuntu image is not a factory image. Reinstall the factory image.
No DHC/ThinOS package in recovery partition	Cannot find the ThinOS image, reschedule job
Error in extracting DHC/ThinOS Future packages	Failed to extract the ThinOS image, reschedule job
Error copying the DHC/ThinOS Future packages to recovery partition	Failed to copy the ThinOS image, reschedule job
ThinOS package verification failed	ThinOS image is not correct, reschedule job with the correct ThinOS image
Not enough space in Recovery Partition	Clear the recovery partition
The free space of Recovery Partition is not enough	Clear the recovery partition

Convert WES to ThinOS 2211

Supported platforms that can convert to ThinOS 2211 are Wyse 5070 Thin Client, Wyse 5470 Mobile Thin Client, and Wyse 5470 All-in-One Thin Client.

Prerequisites

- Ensure you are running Windows 10 Enterprise LTSC 2019 version 10.04.08.05.22.00.
- You must use Wyse Management Suite 4.0 or later versions.
- Ensure that there are enough ThinOS Activation licenses on devices with Wyse Management Suite 4.0 or later versions.
- Create a group in Wyse Management Suite with a group token.
- You must be registered to Wyse Management Suite.
- Ensure that you have downloaded the WES to ThinOS 2211 conversion image `ThinOS_2211_9.3.3099_WES_Conversion.zip`.

Steps

1. Extract the conversion image `ThinOS_2211_9.3.3099_WES_Conversion.zip` to get the .exe file and copy this exe file to the Wyse Management Suite 4.0 or later version server repository.

   The path to upload the conversion image is **Repository Location** > **repository** > **osImages** > **zipped**.
2. On the Wyse Management Suite page, go to **Portal Administration** > **File Repository**, select the repository, and click **Sync Files**. Wait for the synchronization to complete.
3. Ensure that the conversion image is in the repository by going to **Apps & Data** > **OS Image Repository** > **WES/ThinLinux**.
4. Go to **Apps & Data** > **OS Image Policies** > **WES/ThinLinux**, click **Add Policy**.
5. Enter the policy name.
6. Select the group that WES devices are registered to and select **WES** as **OS type**.
7. Select **WIE10** as **OS Subtype Filter**.
8. Select the conversion image as **OS Image**.
9. Select **Force this version as Rule**.

10. In the **Apply Policy Automatically** drop-down list, select **Do not apply automatically**.
11. Click **Save**.
    A dialog box is displayed to schedule a job.
12. Click **Yes** to schedule a job.
13. Select **Immediately** from the **Run** drop-down list in the **App Policy Job** dialog box.
14. Click **Preview**.
15. Click **Schedule** when the next dialog box is displayed.

    ⓘ **NOTE:** After conversion, ThinOS is in factory default status. You must register ThinOS to Wyse Management Suite manually or by DHCP/DNS discovery.

    ⓘ **NOTE:** After you register the converted ThinOS devices to Wyse Management Suite, the ThinOS Activation devices license is consumed.

Compatibility

ThinOS application package details

- Cisco_Jabber_14.1.2.307144.7.pkg
- Cisco_Webex_Meetings_VDI_42.10.5.15.3.pkg
- Cisco_Webex_VDI_42.10.0.23814.5.pkg
- Citrix_Workspace_App_22.9.0.21.3.pkg
- ControlUp_VDI_Agent_1.0.0.1.26.pkg
- EPOS_Connect_7.2.0.29149.1.pkg
- HID_Fingerprint_Reader_210217.18.pkg
- Identity_Automation_QwickAccess_2.0.3.1.1.pkg
- Imprivata_PIE_7.9.000.0023.1162.pkg
- Jabra_8.5.5.1.pkg
- Microsoft_AVD_1.9.2017.pkg
- RingCentral_App_VMware_Plugin_22.3.30.1.pkg
- Teradici_PCoIP_22.07.3.16.pkg
- VMware_Horizon_2209.8.7.0.20616018.3.pkg
- Zoom_AVD_5.11.9.21750.5.pkg
- Zoom_Citrix_5.11.9.21750.8.pkg
- Zoom_Horizon_5.11.9.21750.8.pkg

ⓘ **NOTE:** To optimize security, application performance, and stability, a design change has been made from ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 4.0
- For the Configuration UI package version, refer to the upcoming Wyse Management Suite 4.0 release.

ⓘ **NOTE:** Use Wyse Management Suite 4.0 server for the new Wyse Management Suite ThinOS 9.x Policy features.

ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2211 (9.3.3099)—`ThinOS_2211_9.3.3099.pkg`
- Ubuntu 20.04 to ThinOS 2211 conversion build—`ThinOS_2211_9.3.3099_Ubuntu_Conversion.zip`

- WES to ThinOS 2211 conversion build— `ThinOS_2211_9.3.3099_WES_Conversion.zip`

BIOS packages

Table 72. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.20.0.pkg
Wyse 5470 Thin Client	bios-5470_1.16.1.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.17.0.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.5.3.pkg
Dell Latitude 3420	bios-Latitude_3420_1.23.2.pkg
Dell OptiPlex 5400 All-in-One	bios-OptiPlex5400AIO_1.1.17.pkg

NOTE: BIOS upgrade requires a display screen (integrated or external) without which the update fails. In this case, you cannot install the BIOS package again. You must install another BIOS version.

Tested BIOS version for ThinOS 2211

Table 73. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.20.0
Wyse 5470 All-in-One Thin Client	1.17.0
Wyse 5470 Mobile Thin Client	1.16.1
OptiPlex 3000 Thin Client	1.5.3
Latitude 3420	1.23.2
OptiPlex 5400 All-in-One	1.1.17

Citrix Workspace app feature matrix

Table 74. Citrix Workspace app feature matrix

Feature		ThinOS 2211 with CWA 2209	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	Webcam redirection works for both 32-bit and 64-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser or 64-bit browser to verify webcam redirection online. For example, www.webcamtests.com. For further details, refer to the Dell Wyse ThinOS Administrator's Guide.
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
			Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco Webex Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebexTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
			Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	There are no limitations in this release.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Supported	There are no limitations in this release.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	There are no limitations in this release.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netscaler + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	The following webview login environment configurations support autologin and lock or unlock terminal: ● Citrix Federated Authentication Service SAML with Microsoft Azure Active Directory ● Citrix ADC Native OTP

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
			- Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Microsoft Teams enhancements: App sharing enabled (CWA2209)	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: Enhancements to high DPI support (CWA2209)	Not Supported	Not supported
	Microsoft Teams enhancements: WebRTC SDK upgrade (CWA2209)	Supported	There are no limitations in this release.
	Support for extended keyboard layouts (CWA2209)	Supported	There are no limitations in this release.

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
	Keyboard input mode enhancements (CWA2209)	Not Supported	Not supported
	Support for authentication using FIDO2 (CWA2209)	Not Supported	Not supported
	Support for secondary ringer(CWA2207	Not Supported	Not supported
	Improved audio echo cancellation support [Technical Preview] (CWA2207)	Not Supported	Not supported
	Composite USB device redirection(CWA2207)	Not Supported	Not supported
	Support for DPI matching [Technical Preview](CWA2207)	Not Supported	Not supported
	Enhancement to improve audio quality (CWA2207)	Not Supported	Not supported
	Provision to disable LaunchDarkly service (CWA2205)	Not Supported	Not supported
	Email-based auto-discovery of store (CWA2205)	Not Supported	Not supported
	Persistent login [Technical Preview] (CWA2205)	Not Supported	Not supported
	Authentication enhancement for Storebrowse (CWA2205)	Not Supported	Not supported
	Support for EDT IPv6 (CWA2203)	Not Supported	Not supported
	Support for TLS protocol version 1.3 (CWA2203)	Not Supported	Not supported
	Custom web stores (CWA2203)	Not Supported	Not supported
	Authentication enhancement experimental feature (CWA2203)	Not Supported	Not supported
	Keyboard layout synchronization enhancement (CWA2203)	Not Supported	Not supported
	Multi-window chat and meetings for Microsoft Teams (CWA2203)	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams (CWA2112)	Not Supported	Not Supported
	Request control in Microsoft Teams (CWA2112)	Not Supported	Not supported
	Support for cursor color inverting (CWA2112)	Supported	For limitations, see the Dell Wyse ThinOS Version

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
			2205 Administrator's Guide at www.dell.com/support.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	There are no limitations in this release.
	Enhancement on smart card support (CWA2112)	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Supported	There are no limitations in this release.
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106, CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported

Table 74. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2211 with CWA 2209	Limitations
	Multiple audio devices (CWA2012, CWA2010, and CWA2112)	Supported	If JVDI package is installed in ThinOS, audio devices cannot be switched in the applications in session and the session is disconnected when users open the **Recording devices** list at the Windows sound. If you want to use multiple ICA audio devices, it is recommended that you do not install the VDI package.
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

ThinOS AVD Client Feature Matrix

Table 75. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 2211
Service	Direct connection to Desktop via RDP	Supported
	Remote Desktop Services broker (Local)	Supported

Table 75. ThinOS AVD Client Feature Matrix (continued)

Category Supported	Features	ThinOS 2211
	Windows Virtual Desktop (Azure)	Supported
Session	Desktop	Supported
	Remote App (Integrated)	Not supported
	Remote App (Immersive)	Supported
Input	Keyboard	Supported
	Mouse	Supported
	Single Touch	Supported
Audio Visual	Audio in (microphone)	Supported
	Audio out (speaker)	Supported
	Camera	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
Redirections	Printer	Supported
	SmartCard	Supported
Session Experience	Dynamic Resolution	Supported
	Start Command	Supported
	Desktop Scale Factor	Supported
	Multi-Monitor (All)	Supported
	Restricted full screen session	Supported
	Keyboard Layout Mapping	Supported
	Time Zone Mapping	Supported
	Video/Audio/Online playback	Supported
	Compression	Supported
	Optimize for low speed link	Supported
Graphics (CODECs)	H.264 Hardware Acceleration	Supported
Authentication	TS Gateway	Supported
	NLA	Not supported
	SmartCard	Not supported
	Imprivata	Supported

VMware Horizon feature matrix

Table 76. VMware Horizon feature matrix

Feature		ThinOS 2211 with Horizon Client 2209
Broker Connectivity	SSL certificate verification	Supported only with VDI
	Disclaimer dialog	Supported with VDI, RDS Hosted Desktops and Apps

Table 76. VMware Horizon feature matrix (continued)

Feature		ThinOS 2211 with Horizon Client 2209
	UAG compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Shortcuts from server	Not supported
	Pre-install shortcuts from server	Not supported
	File type association	Not supported
	Phone home	Supported with VDI, RDS Hosted Desktops and Apps
Broker Authentication	Password authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Single sign on	Supported with VDI, RDS Hosted Desktops and Apps
	RSA authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Integrated RSA SecurID token generator	Not supported
	Kiosk mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remember credentials	Not supported
	Log in as current user	Not supported
	Nested log in as current user	Not supported
	Log in as current user 1-way trust	Not supported
	OS biometric authentication	Not supported
	Un-authentication access	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Cisco ACS	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – SMS Passcode	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - DUO	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - OKTA	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Microsoft Network Policy	Supported with VDI, RDS Hosted Desktops and Apps
Smart card	x.509 certificate authentication (Smart Card)	Supported with VDI, RDS Hosted Desktops and Apps
	CAC support	Supported with VDI, RDS Hosted Desktops and Apps
	.Net support	Supported with VDI, RDS Hosted Desktops and Apps
	PIV support	Supported with VDI, RDS Hosted Desktops and Apps
	Java support	Not supported
	Purebred derived credentials	Not supported

Table 76. VMware Horizon feature matrix (continued)

Feature		ThinOS 2211 with Horizon Client 2209
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI
	Restart	Supported only with VDI
	Log off	Supported with VDI, RDS Hosted Desktops and Apps
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple connections	Supported with VDI, RDS Hosted Desktops and Apps
	Multi-broker/multi-site redirection - Universal	Not supported
	App launch on multiple end points	Supported with VDI, RDS Hosted Desktops and Apps
	Auto-retry 5+ minutes	Supported with VDI, RDS Hosted Desktops and Apps
	Blast network recovery	Supported with VDI, RDS Hosted Desktops and Apps
	Time zone synchronization	Supported with VDI, RDS Hosted Desktops and Apps
	Jumplist integration (Windows 7-Windows 10)	Not supported
Client Customization	Command line options	Not supported
	URI schema	Not supported
	Launching multiple client instances using URI	Not supported
	Preference file	Not supported
	Parameter pass-through to RDSH apps	Not supported
	Non interactive mode	Not supported
	GPO-based customization	Not supported
Protocols Supported	Blast Extreme	Supported with VDI, RDS Hosted Desktops and Apps
	H.264 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	H.265 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps—Except OptiPlex 3000 and Latitude 3420 with ThinOS.
	Blast Codec	Supported with VDI, RDS Hosted Desktops and Apps
	JPEG/PNG	Supported with VDI, RDS Hosted Desktops and Apps
	Switch encoder	Supported with VDI, RDS Hosted Desktops and Apps
	BENIT	Supported with VDI, RDS Hosted Desktops and Apps

Table 76. VMware Horizon feature matrix (continued)

Feature		ThinOS 2211 with Horizon Client 2209
	Blast Extreme Adaptive Transportation	Supported with VDI, RDS Hosted Desktops and Apps
	RDP 8.x, 10.x	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP	Supported with VDI, RDS Hosted Desktops and Apps
Features/Extensions Monitors/ Displays	Dynamic display resizing	Supported with VDI, RDS Hosted Desktops and Apps
	VDI windowed mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remote app seamless window	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple monitor support	Supported with VDI, RDS Hosted Desktops and Apps
	External monitor support for mobile	Not supported
	Display pivot for mobile	Not supported
	Number of displays Supported with VDI, RDS Hosted Desktops and Apps	4
	Maximum resolution	3840x2160
	High DPI scaling	Not supported
	DPI sync	Not supported
	Exclusive mode	Not supported
	Multiple monitor selection	Supported with VDI, RDS Hosted Desktops and Apps
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported with VDI, RDS Hosted Desktops and Apps
	Relative mouse	Supported only with VDI
	External Mouse Support	Supported with VDI, RDS Hosted Desktops and Apps
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported with VDI, RDS Hosted Desktops and Apps
	International Keyboard Support	Supported with VDI, RDS Hosted Desktops and Apps
	Input Method local/remote switching	Not supported
	IME Sync	Supported with VDI, RDS Hosted Desktops and Apps
Clipboard Services	Clipboard Text	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard Graphics	Not supported
	Clipboard memory size configuration	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard File/Folder	Not supported

Table 76. VMware Horizon feature matrix (continued)

Feature		ThinOS 2211 with Horizon Client 2209
	Drag and Drop Text	Not supported
	Drag and Drop Image	Not supported
	Drag and Drop File/Folder	Not supported
Connection Management	IPv6 only network support	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP IP roaming	Supported with VDI, RDS Hosted Desktops and Apps
Optimized Device Redirection	Serial (COM) Port Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Client Drive Redirection/File Transfer	Not supported
	Scanner (TWAIN/WIA) Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	x.509 Certificate (Smart Card/ Derived Credentials)	Supported with VDI, RDS Hosted Desktops and Apps
	Gyro Sensor Redirection	Not supported
Real-Time Audio-Video	Audio in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Video in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple webcams	Not supported
	Multiple speakers	Not supported
USB Redirection	USB redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnInsert	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnStartup	Supported with VDI, RDS Hosted Desktops and Apps
	Connect/Disconnect UI	Not supported
	USB device filtering (client side)	Supported with VDI, RDS Hosted Desktops and Apps
	Isochronous Device Support	Supported only with VDI
	Split device support	Supported with VDI, RDS Hosted Desktops and Apps
	Bloomberg Keyboard compatibility	Supported only with VDI
	Smartphone sync	Supported only with VDI
Unified Communications	Skype for business	Supported with VDI, RDS Hosted Desktops and Apps
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Teams	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Meetings	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops and Apps

Table 76. VMware Horizon feature matrix (continued)

Feature		ThinOS 2211 with Horizon Client 2209
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops and Apps
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not supported
	Directshow Redirection	Not supported
	URL content redirection	Not supported
	MMR Multiple Audio Output	Not supported
	Browser content redirection	Not supported
Graphics	vDGA	Supported only with VDI
	vSGA	Supported only with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Supported only with VDI
	AMD vGPU	Supported only with VDI
Mobile Support	Client-side soft keyboard	Not supported
	Client-side soft touchpad	Not supported
	Full Screen Trackpad	Not supported
	Gesture Support	Not supported
	Multi-touch Redirection	Not supported
	Presentation Mode	Not supported
	Unity Touch	Not supported
Printing	VMware Integrated Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Location Based Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Native Driver Support	Not supported
Security	FIPS-140-2 Mode Support	Supported with VDI, RDS Hosted Desktops and Apps
	Imprivata Integration	Supported with VDI, RDS Hosted Desktops and Apps
	Opswat agent	Not supported
	Opswat on-demand agent	Not supported
	TLS 1.1/1.2	Supported with VDI, RDS Hosted Desktops and Apps
	Screen shot blocking	Not supported
	Keylogger blocking	Not supported
Session Collaboration	Session Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
	Read-only Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
Update	Update notifications	Not supported

Table 76. VMware Horizon feature matrix (continued)

Feature		ThinOS 2211 with Horizon Client 2209
	App Store update	Not supported
Other	Smart Policies from DEM	Supported with VDI, RDS Hosted Desktops and Apps
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI—Only basic connection is tested
	Workspace ONE mode	Supported with VDI, RDS Hosted Desktops and Apps
	Nested - basic connection	Supported with VDI, RDS Hosted Desktops and Apps
	DCT Per feature/component collection	Not supported
	Displayed Names for Real-Time Audio-Video Devices	Supported with VDI, RDS Hosted Desktops and Apps
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI

For detailed information about the VMware Horizon features, see the Horizon documentation at docs.vmware.com.

New and enhanced features

Citrix Workspace app updates

Citrix Workspace App package version is updated to 22.9.0.21.3.

ⓘ **NOTE:** If you want to install the Citrix Workspace app version 2209 on ThinOS, install this package.

Supports virtual display layout

From ThinOS 2211 and Citrix Workspace App 2209, virtual display layout on VDA is supported. The virtual display configuration interface helps you to define a virtual display layout per session monitor on the VDA, in a live session. This feature allows you to split each session monitor independently into multiple virtual monitors. You can split the session into eight virtual monitors on the remote desktop. Also, you can update the session primary monitor and DPI settings for the displays.

The virtual display configuration is stored per user per client device, which has persisted across session resize, session disconnect or reconnect, and session logoff or login. The configured virtual display layout reset occurs on a session resize and change in the number of session monitors.

Before configuring the virtual display layout on VDA, keep in mind the following points:

- Single-session or multisession operating system VDA is supported.
- The graphics status indicator policy must be enabled.
- VDA version 2019 or later (Dell Technologies qualified VDA 2203 LTSR and 2206).

  ⓘ **NOTE:** Only desktop sessions can be configured.

Follow these steps to configure your virtual display layout on VDA:

1. Right-click the graphics status indicator icon from the system tray and select **Configure virtual displays**.

   The virtual display configuration interface is launched.

2. Right-click a virtual display to mark it as the primary monitor.
3. Use the DPI drop-down list to set a preferred scaling factor for the virtual display.

   You can draw horizontal or vertical lines to separate the screen into virtual monitors. The screen is split according to specified percentages of the session monitor resolutions.

4. After defining a virtual display layout, click **OK** to save the layout, or **Cancel** to discard the changes.

Use **Reset** to undo the configuration and restore the original layout.

Log in to Citrix ADC using MFA with SAML, OKTA as IDP, and Citrix FAS for SSO to VDA

From ThinOS 2211 and Citrix Workspace App 2209, you can log in to Citrix Application Delivery Controller (ADC) through Multiple Factors Authentication (MFA) with Security Assertion and Markup Language (SAML), using OKTA as the identity provider, and Citrix FAS for Single Sign-On (SSO) to VDA.

1. From the desktop menu, go to **System setup** > **Remote Connections**.

   The Remote Connections dialog box is displayed.

2. Click the **Broker Setup** tab and select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list.
3. Enter the Citrix ADC gateway server URL in the **Broker Server** field. You can also configure other options.
4. Click **OK**.

   The NetScaler gateway Webview login window is displayed and, you are redirected to Okta IDP for authentication.

5. Enter the user credentials with UPN format and password.

   If you have not registered your phone with Okta Verify, you are prompted to setup MFA.

6. Select **Enter a code** or **Get a push notification** security method using Okta Verify application.
7. Launch the Okta Verify application on your phone.
   - If you selected **Enter a code** previously, enter the code in the Citrix ADC login window and click **Verify**.
   - If you selected **Get a push notification**, approve the push notification on your phone once you get it.
8. If the authentication is successful, you are logged into Citrix ADC.

   NOTE: ThinOS does not support Okta Single Sign-On (SSO) with Certificate Authentication.

Support for extended keyboard layouts

From ThinOS 2211 and Citrix Workspace App 2209, Japanese 106 keyboard, Portuguese ABNT/ABNT2 keyboards, and Multimedia keyboards are supported in Citrix VDI sessions. The Scancode keyboard input mode supports the extended keyboard layouts along with all keyboard layout synchronization modes.

This feature is disabled by default. To enable the extended keyboard layouts in Citrix VDI session, ensure that the Scancode keyboard input mode is configured, and do the following:

1. In **Admin Policy Tool** or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In **Citrix INI Settings**, click **Add Row**.
3. From the **File** drop-down list, select **wfclient.ini**.
4. From the **Operation** drop-down list, select **Add or Update**.
5. In the **Section** field, enter **WFClient**.
6. In the **Key** field, enter **KeyboardEventMode**.
7. In the **Value** field, enter **Scancode**.
8. Sign out or restart the device for the settings to take effect.

   NOTE: Ensure that the setting **Enabled Volume Control for Client Volume** is disabled in Admin Policy Tool or Wyse Management Suite policy. Otherwise, the Multimedia keyboards do not work.

Citrix Workspace App Limitations

- In the server operating system VDA desktop (such as Windows server 2016, 2019, and 2022), if audio and video devices are required to be redirected into a session, ensure that the following registry settings are configured in session:
  - HKLM\Software\Citrix\PortICA\GenericUSB key and REG_DWORD value **UsbAudioEnabled** is set to 1.
  - HKLM\Software\Citrix\PortICA\GenericUSB key and REG_DWORD value **UsbVideoEnabled** is set to 1.
  - If audio and video devices redirection in server operating system VDA is not required, ensure **UsbAudioEnabled** and **UsbVideoEnabled** is set to 0.
- For thin clients that have the default time zone as **UTC+0(UTC)** in ThinOS 2208 and earlier versions, the Windows 11 VDA session may face display flickering issues after upgrading to ThinOS 2211. To resolve this, change the time zone or set the UTC+0 (UTC) time zone to **others** and then set it back to **UTC+0 (UTC)** from Admin Policy Tool or Wyse Management Suite policy.
- Relative mouse feature does not work in Citrix Workspace App on ThinOS.
- Citrix webview auto login does not work after rebooting the client, when the user credentials are configured through Wyse Management Suite.
- The following new features from Citrix Workspace App 2209 are not supported in ThinOS:
  - Microsoft Teams enhancements: Enhancements to high DPI support

    - Keyboard input mode enhancements
    - Support for authentication using FIDO2

Known issues in Linux Citrix Workspace app binary

- Multimedia Redirection (MMR) video stops responding, and there is no audio with Citrix VDA 2203 and VDA 2206.
- When playing videos in Windows Media Video (WMV) version 9 or version 7 format, the wallpaper of the VDI session is displayed in the video.
- If the Microsoft Teams optimization option is disabled, the audio and video devices in Microsoft Teams device settings are displayed as **None**.
- Microsoft LifeCam Cinema camera name is displayed as **Generic** in **Citrix toolbar** > **Devices** > **Manage devices**.
- When trying to play .WMP format 4 K videos in Citrix, there are audio issues and no video is displayed.
- Audio issue with Microsoft Teams during audio or video calls when using a browser.
- Mouse cursor is not displayed correctly in Word in ICA Windows 2022 desktop.
- Invert cursor is not working in ICA Windows 2022 desktop.
- Dual monitor setup does not work when RDP client is published using Citrix application.
- The webview login screen stops responding, and a white screen is displayed after network connection is lost.
- The integrated audio speakers on Wyse 5470 thin clients emit an echo during calls or meeting. As a workaround, use a USB headset.
- If there is a Microsoft Teams call or meeting happening between a Wyse 5470 thin client and a thin client that is or is not Wyse 5470 thin client, you may encounter audio issues when you enable the camera. You can change the default settings to troubleshoot the audio issues by doing the following:
    1. In the Citrix JSON Settings, click **Add Row**.
    2. From the **File** drop-down list, **select hdx_rtc_engine/config.json**.
    3. From the **Operation** drop-down list, select **Add or Update**.
    4. In the **Key** field, enter **`EnableAEC`**.
    5. In the **Value** field, enter **`0`**.
    6. Follow steps one to three again.
    7. In the **Key** field, enter **`EnableAGC`**.
    8. In the **Value** field, enter **`0`**.
    9. Follow steps one to three again.
    10. In the **Key** field, enter **`EnableNS`**.
    11. In the **Value** field, enter **`0`**.
    12. Sign out or restart the device for the settings to take effect.

Microsoft Teams updates

From ThinOS 2211 and Citrix Workspace App 2209, App sharing is enabled in Microsoft Teams optimization mode. You can share an application using the Screen sharing feature in Microsoft Teams. The feature is applicable on Citrix Virtual Apps and Desktops 2109 and later.

ⓘ **NOTE:** If the **Use video codec for compression** Citrix policy is set as **For the entire screen**, app sharing is not available. You can use other video codecs instead. The issue also occurs in Linux Citrix Workspace app binary.

Microsoft RDP and AVD

SmartCard redirection—From ThinOS 2211 and AVD package version 1.9, SmartCard can be redirected in RDP and AVD sessions.

Printer update in RDP/AVD session—If you want to map a printer to the RDP/AVD session, install the specific driver in the RDP/AVD session before mapping.

ⓘ **NOTE:** The printer supports only PostScript (PS) drivers in RDP/AVD session.

Teradici PCoIP update

- Teradici version is updated to 22.07.3.16 in ThinOS 2211.

- It is recommended that you deploy Teradici virtual audio driver in PCoIP session. If your USB or Bluetooth headset does not work in PCoIP session, deploy the Teradici virtual audio driver in PCoIP session.
- **Known Issues**
  - Remote Workstation Card PCoIP session cannot be connected when using Teradici PCoIP package 22.07.3.16. If you want to connect to the Remote WorkStation card PCoIP session, use PCoIP package version 22.04.2.13 that was in the ThinOS 2208 release.
  - There is a 15-second delay when reconnecting to previous PCoIP sessions that have Horizon Agent and Imprivata Agent installed. The issue is fixed in VMware Horizon 7.13.2, 8.5, or later versions with an additional registry key change that is required on the virtual machine. For more information, see *Delay in reconnecting to Horizon desktop when HTML Access and Imprivata OneSign are in use (85892)* at www.vmware.com/docs.
  - Entering Sleep mode may cause ThinOS to stop responding in PCoIP sessions when connected to a USB headset or when a monitor is connected to the thin client using Type-C cable. This issue only occurs in PCoIP sessions on Horizon Broker agents, Teradici Cloud Access Broker agents, and Amazon WorkSpaces.

Horizon Blast Updates

- The Horizon package version is updated to Horizon 2209 in ThinOS 2211 release.
- **Supports Multi-session for a published application**—When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log in to the server from different client devices.

  For example, if you open a published application in multi-session mode on client A, and then open the same published application on client B, the published application remains open on client A, and a new session of the published application opens on client B. If multi-session mode is disabled, which means that client is in single-session mode, the published application session on client A disconnects and reconnects on client B. If the multi-session mode is set as Enable (Enforced) or Enabled (Default On), ThinOS launches the multi-session mode.
- **Limitations and Known Issues**
  - Some camera names are not displayed correctly in Horizon Skype for Business. This is a VMware limitation.
  - VMware Horizon Login Broker agent window displays a Tunnel error after client reboot. As a workaround, leave the password field empty in **Remote Connections** > **General Options**.

Imprivata updates

- ThinOS Imprivata_PIE_7.9.000.0023.1162.pkg is supported against OneSign server 7.9.000.11 with ThinOS 2211 release.
- **Known issue**: Saved default credentials do not passthrough to the Imprivata PIW login window.

Identity Automation

- Identity automation package is updated to 2.0.3.1.
- **Supports PIN Reset**—You can reset your PIN from the ThinOS login window by clicking **Forgot your PIN**. ThinOS must match the configuration ID with the profile ID that enabled the PIN reset. You must set the configuration ID to 1.

  NOTE: To enable PIN rest, Lynx server version 1.7.0.6 is required.

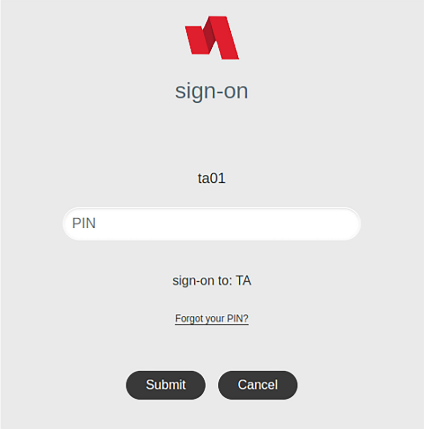


Figure 3. PIN Reset in ThinOS login

Cisco Webex Meetings VDI updates

- Cisco Webex Meetings VDI package version is updated to 42.10.5.15.3.
- **Added meeting action sounds**—A sound is played for participants joining a meeting, leaving a meeting, raising hand, receiving a message, and waiting in the lobby.

Cisco Webex VDI update

- Cisco Webex VDI package version is updated to 42.10.0.23814.5.
- **Added new features**:
  - Preview of shared content.
  - Choose the skin tone for your reactions.
  - See more in thumbnail videos.
  - Maximize what you see when content is shared.
  - Identify whether a meeting participant is internal, external, or unverified.
  - Hosts can set a stage view for all meeting participants.

Cisco Jabber

Cisco Jabber version is updated to 14.1.2.307144.7.

Zoom

- Zoom Citrix and Horizon package version is updated to 5.11.9.21750.8.
- Zoom AVD package is also supported in 5.11.9.21750.5.
- **Limitation**— Citrix Zoom package does not work using UDP port 88xx.

RingCentral

- RingCentral package version, RcApp_VMwareplugin_22.2.30.44745.1, is supported in ThinOS 2211.
- RingCentral supports Audio only.
- For Citrix, you can install citrix-vda-policy (Windows Batch File) in a VDI session. No additional package is required by the client.
- For VMware, you can install the RingCentral package on ThinOS Client locally and the VMware plugin in VDI session.

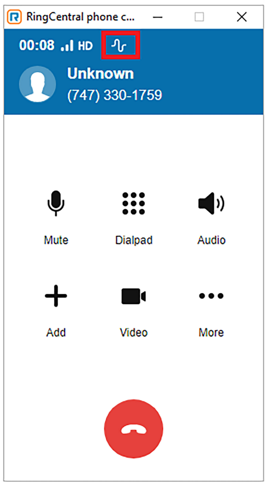


Figure 4. RingCentral

ControlUp

NOTE: Ensure you have Windows or later versions and VMware Horizon Client 5.0.0 and later version on your system.

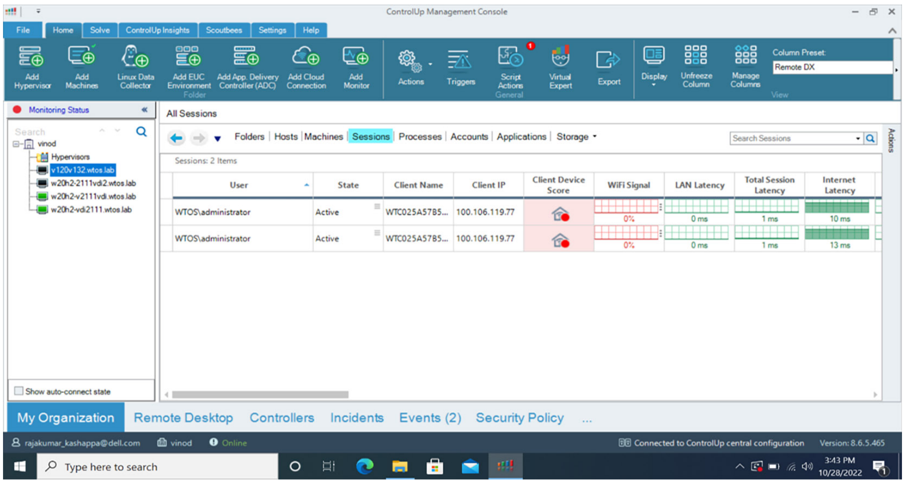
Prerequisites:

- ControlUp Package and ControlUp agent must be installed on the ThinOS client.
- VMware or Citrix VDA must be launched.

Steps:

1. Launch ControlUp console that is already installed on your desktop.
2. In the ControlUp console, connect the machine that is launched on the client.
3. Go to **Sessions** tab and select **Remote DX** from the column dropdown at the upper right corner.
4. In **Remote DX**, you can see the client information such as **Client Name**, **Client IP**, **LAN Latency**, and so on

ControlUp version 1.0.0.1.26 is supported in ThinOS 2211. ControlUp helps in analyzing client and VDI resources.



Sessions: 2 Items

User	State	Client Name	Client IP	Client Device Score	WiFi Signal	LAN Latency	Total Session Latency	Internet Latency
WTOS\administrator	Active	WTC025A57B5...	100.106.119.77		0%	0 ms	1 ms	10 ms
WTOS\administrator	Active	WTC025A57B5...	100.106.119.77		0%	0 ms	1 ms	13 ms

Figure 5. ControlUp Management Console

ThinOS enhancements

1. **Admin mode login event on Wyse Management Suite 4.0 server**—If you enable admin mode in Wyse Management Suite policy by going to **Privacy & Security** > **Account Privileges** and then login, a login event is recorded. This event is recorded in Wyse Management Suite 4.0 server, whether the login is successful or not.
2. **Fail to change BIOS settings event on Wyse Management Suite 4.0 server**—If you publish the BIOS policy from Wyse Management Suite 4.0 server with a wrong BIOS password, a failure event is recorded. This event is recorded in Wyse Management Suite 4.0 server.
3. **Supports new MIB tree in SNMPV3** —ThinOS supports MIB tree 1.3.6.1.4.1.714.1.2.6.1.2.0 to send message to client, and the message character count is increased to 255 characters. ThinOS also supports MIB tree 1.3.6.1.4.1.714.1.2.6.1.1.0 to reboot the client. The reboot client behaviors are as follows:
   - Set to **0**: Reboot immediately
   - Set to **x**: Reboot after x minutes (x is integer)
   - Set to **-1**: Cancel reboot

   NOTE: If you set 1.3.6.1.4.1.714.1.2.6.1.1.0 to reboot the client, you cannot set another value to change the reboot timer directly. You must set the value to **-1** to cancel the reboot first, and then set another value to reboot again.
4. **LPD service for printer**—A thin client can be configured to provide Line Printer Daemon (LPD) services, making the thin client a printer server on the network. The LPD printer service is applied with LPT printer and SMB printer.

   NOTE: The LPD service for printer is not supported in AVD/RDP session on ThinOS 2211.
5. **Performance Retrospective**—You can enable **Enable Performance Retrospective** option in **APT/WMS** > **Advanced** > **Services** > **Troubleshooting Settings**. When you click **Performance Retrospective** in the **General** tab of the **Troubleshooting** dialog box, CPU, Memory, and Disk data is displayed.

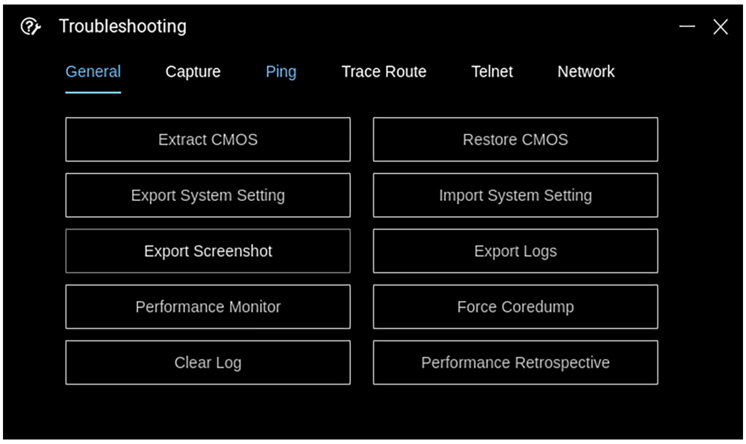


Figure 6. Performance Retrospective option in Troubleshooting

When you click **Networking**, Network data like ENET and WLAN is displayed, and the data starts from terminal boot. Five-minute data is displayed by default, and you can select a time span in the list by using **Prev** and **Next** buttons.

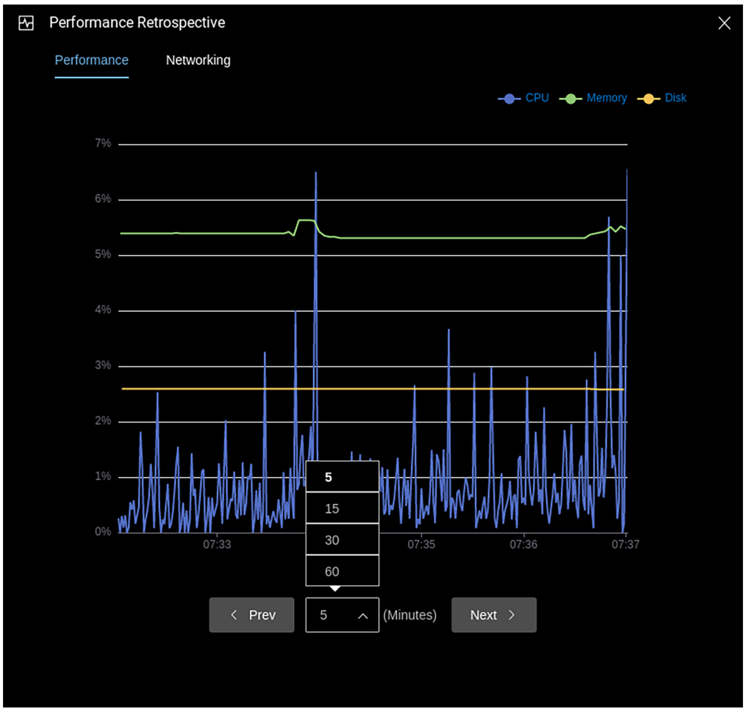


Figure 7. Network data in Performance Retrospective

6. **VDI with Web Authentication updates**
   - **Web Authentication Auto Login update**: After setting the default credentials in **Remote Connections** > **General Options**, when you connect to a VDI Broker agent that uses Web Authentication, the default credentials passes through to the web page automatically.
   - **Lock/Unlock Terminal when using Web Authentication method**
     - In ThinOS 2208 (9.3.2102), after logging into a VDI Broker agent with Web Authentication and locking the ThinOS session, you must set a temporary password to unlock the system.
     - From ThinOS 2211 (9.3.3099) onwards, a temporary password is not required. You can use the password that is used at the time of logging in to unlock the system directly.
   - **Tested scenarios**: In case any other (or custom) web authentication pages are used, correct caching of the credentials, which results in behavior similar to ThinOS 2208 or earlier versions, cannot be guaranteed . The tested scenarios are as follows:
     - Citrix Federated Authentication Service SAML with Microsoft Azure Active Directory
     - Citrix ADC Native OTP
     - Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA
     - Horizon Workspace One Mode (On-premises)

    - Horizon Workspace One Mode (WS1 Access)
    - Horizon Workspace One Mode (WS1 Access) with OKTA IDP
    - VMware Unified Access Gateway with OKTA IDP
    - VMware Unified Access Gateway with Microsoft Azure IDP
    - Azure Virtual desktop Broker agent

7. **Updated the First Boot Wizard import configuration password character limit from eight to nine**—When importing the system settings configuration in First Boot Wizard, the minimum password character limit is nine characters.
8. **VPN Update**—GlobalProtect with .pfx certificate feature is added.
9. **Secure MQTT connection** for the **Wyse Management Suite cloud server**—When the client checks in to the Wyse Management Suite cloud server, the MQTT connection is routed to a secure MQTT connection. If the secure MQTT connection fails, the cloud server falls back to a nonsecure MQTT connection.
10. **SCEP renewal interval update**—If the client fails to renew the certificate, the SCEP renewal interval changes from 20 s to 12 hours.
11. **Enabled SD card support on OptiPlex 5400 All-in-One**—The SD card slot on OptiPlex 5400 All-in-One is not a USB port. You cannot redirect SD card to VDI sessions. You can only map the SD card to Citrix and RDP sessions as a disk.
12. **SMB printer update**— If the SMB printer credentials field is left empty, the client uses the login credentials (not the web login authentication credentials) as the SMB printer credentials.

    NOTE: In the local printer setup window, if you want to do a local SMB printer test, you must first add and save the SMB credentials manually, and then do a test print.
13. After logging in using Citrix, VMware, or Microsoft webview Broker agent on the client, the last username that was used to log in is recorded in the Wyse Management Suite server device list page and device details page.

Updates to Admin Policy Tool and Wyse Management Suite policy settings

NOTE: Wyse Management Suite 4.0 is required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

1. **WINS Server** —Added new option **WINS Server** in **Network Configuration** > **DNS Settings**. If you disable **Only use DNS configuration set in DHCP**, you can set **WINS Server**

    NOTE: ThinOS only supports one WINS server.
2. **SNMP Server List**—Added a new option **SNMP Server List** in **Network Configuration** > **SNMPV3 Settings**. You can set four SNMP servers.
    - If you leave this option blank, any SNMP server can access ThinOS.
    - If you set the SNMP server, only the SNMP servers in the list can access ThinOS.
3. **TLS Control**—Added new options **TLS Min Protocol**, **TLS Max Protocol**, and **Select Ciphers to disable** in **Privacy & Security** > **Security Policy**. These options require a reboot to take effect.
    - If you select the minimum TLS version in **TLS Min Protocol** and maximum TLS version in **TLS Max Protocol**, ThinOS uses the TLS versions in the scope for connection.

        NOTE: With the next release, TLS 1.0 and 1.1 are going to be removed.

        If you select the TLS ciphers in **Select Ciphers to disable**, ThinOS does not use these ciphers for connection.
    - Wired and wireless authentication ignores the TLS control settings. Authentication servers decide the TLS versions and ciphers.

        NOTE: In the next release, wired and wireless authentication is going to follow TLS control settings. Ensure that your wired and wireless environment support TLS 1.2.
    - Wyse Management Suite server connection ignores the TLS control settings. Wyse Management Suite servers decide the TLS versions and ciphers.
    - Imprivata OneSign ProveID Embedded ignores the TLS control settings. OneSign servers decide the TLS versions and ciphers.
    - Identity Automation ignores the TLS control settings. HealthCast Lynx servers decide the TLS versions and ciphers.
    - Web browser login always uses TLS 1.2 version or later.
    - If the TLS version in **TLS Max Protocol** is lower than **TLS Min Protocol**, after saving, the new values revert to the original values.
4. **Reason For RDP/AVD Session Disconnect is displayed**—The default value is **Enable** in **Session Settings** > **RDP and AVD Session Settings**. When an RDP/AVD session gets disconnected, a dialog box displays the reason for disconnection.

This dialog box stops the session auto reconnect process, so disable this feature if you prefer to auto reconnect to the session.

5. **Hide Taskbar**—Added a new option **Hide Taskbar** in **Personalization** > **User Experience Settings** > **System Mode**. This option is for classic mode only. If you enable this option, the taskbar at the bottom is hidden when ThinOS is not logged in or if you try to maximize a window. You can move the mouse cursor to the bottom to show the taskbar.

   NOTE: This option is designed for seamless use of the application. If you are using the desktop in full screen mode, it is recommended to disable it. Otherwise, when you move the mouse cursor to the bottom, ThinOS taskbar covers the Windows desktop taskbar.

6. **Manual Override for Closing the Lid**—Added a new option **Manual Override** in **System Settings** > **Power Sleep Settings** > **Closing the Lid (MTC only)**. When the option is enabled, you can change the value of **When I close the lid** on the ThinOS client by going to **System Preferences** > **Power and Sleep**. After that, the ThinOS client does not apply the policy of Closing the Lid from Wyse Management Suite anymore.
7. **Manual Override Login Settings** — Added **Manual Override Login Settings** in **Advanced** > **Login Experience** > **Login Settings** > **Default Credentials**. By default, the option is disabled.
   - If **Manual Override** is disabled, the settings in **Advanced** > **Login Experience** > **Login Settings** > **Default Credentials** from Wyse Management Suit take priority.
   - If **Manual Override** is enabled, **Manual Override Policy** is displayed and by default, it is **By group**. Another option is **By parameters**. When **Manual Override Policy** is enabled, the changes of local default credentials in **Remote Connections** > **General Options** takes priority.
     - If **Manual Override** is enabled **By group** and local default credentials are changed, all the policy changes made in **WMS** > **Advanced** > **Login Experience** > **Login Settings** > **Default Credentials** are prevented.
     - If **Manual Override** is enabled **By parameters** and local default credentials are changed, only the conflicting settings in **Advanced** > **Login Experience** > **Login Settings** > **Default Credentials** from Wyse Management Suite server are prevented.
8. **UC Virtual Channel settings**— Unified Communication Virtual Channel Settings are added in **Citrix Session Settings**, **Blast Session Settings**, and **RDP and AVD Session Settings**.
   - UC Virtual Channel settings in **Citrix Session Settings**

     NOTE: The UC Virtual Channel settings do not apply to ThinOS versions later than 9.1.2101 but earlier than or equal to 2208 (9.3.2102). These settings are supported again from ThinOS 2211 and later. From ThinOS 2211, the default values of all UC virtual channel settings have been changed to **Enabled**.

     NOTE: When the UC virtual channels are disabled, the Unified Communication software on ThinOS uses the fallback mode, which uses the HDX webcam and HDX audio. Using the fallback mode consumes more remote desktop resources such as CPU, GPU, RAM, and Network.

     NOTE: Enabling or disabling the UC plug-in settings in **VDI Configuration Editor** > **Citrix Configuration Editor** is deprecated from ThinOS 2211.

     For ThinOS 9.1.2101 or earlier versions, see ThinOS 9.1 Administrator's Guide at www.dell.com/support on the number of allowed virtual channels and tested combinations of Unified Communication optimizations.

     a. On the ThinOS client, open **Admin Policy Tool**, or go to the ThinOS 9.x policy settings in Wyse Management Suite.
     b. In the **Advanced** tab, expand **Session Settings**, and click **Citrix Session Settings**.
     c. In the **UC Virtual Channel Settings** section, enable or disable one or more Unified Communications (UC) virtual channels as per your preference. The available options are:
        - Microsoft Teams Optimization
        - HDX RealTime Media Engine for Microsoft Skype for Business
        - Zoom Meetings Optimization
        - Cisco Jabber Softphone for VDI (JVDI)
        - Cisco Webex Meetings for VDI
        - Cisco Webex VDI (formerly Cisco Webex Teams)

     d. Sign out or restart the device for the settings to take effect.

     The following UC virtual channels labels are renamed in ThinOS 2211 Admin Policy Tool and Wyse Management Suite version 4.0 using the Configuration UI package vxxxxx:
     - **RTME for Skype for Business** is renamed to **HDX RealTime Media Engine for Microsoft Skype for Business**.
     - **JVDI for Cisco Jabber** is renamed to **Cisco Jabber Softphone for VDI (JVDI)**.
     - **Cisco Webex Meetings for VDI** is renamed to **Cisco Webex Meetings for VDI**.
     - **Cisco Webex Teams for VDI** is renamed to **Cisco Webex VDI** (formerly Cisco Webex Teams).
   - UC Virtual Channel settings in **Blast Session Settings**

     a. On the ThinOS client, open **Admin Policy Tool**, or go to the ThinOS 9.x policy settings in Wyse Management Suite.

b. In the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.

c. In the **UC Virtual Channel Settings** section, enable or disable one or more Unified Communications (UC) virtual channels as per your preference. The available options are:

  - Microsoft Teams Optimization
  - VMware Virtualization Pack for Skype for Business
  - Zoom Meetings Optimization
  - Cisco Jabber Softphone for VDI (JVDI)
  - Cisco Webex Meetings for VDI
  - Cisco Webex VDI (formerly Cisco Webex Teams)

d. Sign out or restart the device for the settings to take effect.

- UC Virtual Channel settings in **RDP and AVD Session Settings**

a. On the ThinOS client, open **Admin Policy Tool**, or go to the ThinOS 9.x policy settings in Wyse Management Suite.

b. In the **Advanced** tab, expand **Session Settings**, and click **RDP and AVD Session Settings**.

c. In the **UC Virtual Channel Settings** section, enable or disable one or more Unified Communications (UC) virtual channels as per your preference. Zoom Meetings Optimization is the only available optimization.

d. Sign out or restart the device for the settings to take effect.

> ⓘ **NOTE:** It is recommended that the UC Virtual Channel Settings be kept as **Enabled**. From ThinOS 2211 onwards, if you disable the UC Virtual Channel Setting, the UC fallback mode is used. The video and audio quality degrades, and the system performance is affected.

9. **Supports showing pictures from File Server option**—You can configure this option in **WMS/APT** > **Personalization** > **Screen Saver Settings** > **Showing Pictures** > **File Server option**. If **File server option** is enabled, the client can download the screensaver images from the IIS file server.

The option supports only HTTPS protocol. **File server option** also supports anonymous authentication and basic authentication on the IIS server.

> ⓘ **NOTE:** The file server timer is the time taken to sync the file between client and server timer. Before the sync happens, the screen saver uses the last saved pictures or the default picture. After the sync happens, the screen saver applies the new pictures next time.

If the Enable CA validation option is enabled, the URL must be used with a fully qualified domain name (FQDN) and not IP. The URL must also use a domain signed certificate only.

10. **Supports enabling LPD Service setting in printer**—To configure this setting go to **WMS/APT** > **Peripheral Management** > **Printer** > **Local Printer Settings and SMB Printer Settings** > **Enable LPD Service**.

If enabled, the client can be configured to provide Line Printer Daemon (LPD) services, that is, the client can work as a printer server on the network.

> ⓘ **NOTE:** LPD service for LPT and SMB is not supported in AVD/RDP sessions.

11. **Enable Group Change Notice**—Added **Enable Group Change Notice** in **Services** > **WDA Settings**. If this option is enabled, a dialog box is not displayed when changing the group on the thin client.
12. **Enable Performance Retrospective**— Added **Enable Performance Retrospective** in **APT/WMS** > **Advanced** > **Services** > **Troubleshooting Settings**. By default, the option is disabled. When enabled, you must first specify the device for performance retrospective and the **Performance Retrospective** button, which is in **Troubleshooting** window of the **General** tab can be enabled.

Tested environments matrix

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

Table 77. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	4.0
Configuration UI package for Wyse Management Suite	Refer to upcoming Wyse Management Suite 4.0 release
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 78. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows 11	Windows Server 2016	Windows Server 2019	Windows Server 2022	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5)	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2203LTSR	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2206	Tested	Tested	Tested	Tested	Tested	Tested

Table 79. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2016 APPs	Windows Server 2019 APPs	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Not tested	Tested	Tested	Not tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Not tested	Tested	Tested	Not tested	Tested—Only basic connection is tested on Ubuntu 20.04
VMware Horizon 2206	Tested	Tested	Tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2209	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested	Not tested	Not tested

Table 80. Test environment – VMware Horizon Cloud

Horizon Cloud	Windows 10	Windows Server 2016
Build Version: 19432376	Horizon Agent Installer - 21.3.0.19265453	Horizon Agent Installer - 21.3.0.19265453

Table 81. Test environment—Microsoft RDP

Microsoft RDP	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
Remote Desktop Services 2016	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2019	Not tested	Tested	Not tested	Not tested	Not tested	Tested	Tested

Table 82. Test environment—AVD

Azure Virtual Desktop	Windows 11	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
2019 (MS-Prod)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested
2020 (ARMv2)	Tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested

Table 83. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	2.9.500	2.9.500	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				
	Windows server 2022				

Table 84. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 85. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	14.1.2.307144_7	14.1.2.307144	14.1.2.57135
	Windows server 2016			
	Windows server 2019			
	Windows server 2022			

Table 86. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	14.1.2.307144_7	14.1.2.307144_7	14.1.2.307144_7
	Windows server 2016			
	Windows server 2019			

Table 86. Tested environment—JVDI (continued)

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon View 7.13.2				

Table 87. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	5.11.9.21750.8	5.11.9 (21750)
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 88. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106 VMware Horizon View 7.13.2	Windows 10	5.11.9.21750.8	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		

Table 89. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.11.9.21750.5	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		

Table 90. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR Citrix Virtual Apps and Desktops 7 2206	Windows 10	42.10.0.23814_5	42.10.0.23814
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 91. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10	42.10.0.23814_5	42.10.0.23814_5
	Windows server 2016		
	Windows server 2019		

Table 92. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	42.10.5.15_3	42.10
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 93. Tested environment—Cisco Webex Meetings

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106	Windows 10	42.10.5.15_3	42.10
	Windows server 2016		
	Windows server 2019		

Table 94. Tested environment—RingCentral

VMWare VDI	Operating system	RingCentral Package
Horizon 2111 Horizon View 7.13.2	Windows 10	22.2.30.44745.1
	Windows server 2016	
	Windows server 2019	

Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

NOTE: The supported peripherals are not limited to the peripherals devices listed in this section.

Table 95. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

Product Category	Peripherals	3040	5070	5470 AIO	5470
Audio Devices	Dell Pro Stereo Headset – UC150 – Skype for Business	Supported	Supported	Not Available	Supported
	Dell Pro Stereo Headset - Skype for Business - UC350	Supported	Supported	Supported	Supported
	Dell Professional Sound Bar (AE515M)	Supported	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Not Available	Supported	Not Available	Not Available
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Not Available	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Not Available	Supported	Supported

Table 95. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Not Available	Supported	Supported
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0	Not Available	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	DellUSB Wired Optical Mouse - MS116	Supported	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white	Not Available	Not Available	Not Available	Not Available
	SEAL SHIELD MEDICAL GRADE OPTICAL (Mouse)	Not Available	Not Available	Not Available	Not Available

Table 95. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white	Not Available	Not Available	Not Available	Not Available
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white	Not Available	Not Available	Not Available	Not Available
	Dell Wireless Mouse - WM126_BLACK - Rosewood	Not Available	Not Available	Not Available	Not Available
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Not Available	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Not Available	Supported	Not Available	Supported
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI - DBQAUBC064 - DBQAUBC064	Not Available	Supported	Not Available	Not Available
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Not Available	Supported	Not Available	Not Available
	Trendnet USB to Serial Converter RS-232	Not Available	Supported	Supported	Supported

Table 95. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Adapter - HDMI to DVI - DAUARBN004 - DAUARBN004	Not Available	Not Available	Not Available	Supported
	Dell Adapter - HDMI to VGA - DAUBNBC084 - DAUBNBC084	Not Available	Not Available	Not Available	Supported
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232	Not Available	Not Available	Supported	Supported
Displays	E1916H	Supported	Supported	Supported	Not Available
	E2016H	Supported	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported	Supported
	E2216H	Not Available	Supported	Supported	Supported
	E2216Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2218HN	Supported	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported	Supported
	E2318H	Supported	Supported	Supported	Supported
	E2318HN	Not Available	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported	Supported
	E2420HS	Not Available	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported	Supported
	E2720HS	Not Available	Supported	Supported	Supported
	P2016	Not Available	Supported	Not Available	Not Available
	P1917S	Supported	Supported	Not Available	Not Available
	P2017H	Supported	Not Available	Not Available	Not Available
	P2018H	Not Available	Not Available	Not Available	Supported
	P2217	Supported	Supported	Not Available	Not Available
	P2217H	Supported	Supported	Not Available	Not Available
	P2219H	Supported	Supported	Not Available	Supported
	P2219HC	Supported	Supported	Not Available	Supported
	P2317H	Supported	Supported	Not Available	Not Available
	P2319H	Not Available	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Supported	Not Available
	P2417H	Supported	Supported	Not Available	Not Available
	P2418D	Supported	Not Available	Not Available	Not Available

Table 95. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	P2418HT	Supported	Supported	Supported	Not Available
	P2418HZ	Supported	Supported	Not Available	Not Available
	P2419H	Supported	Supported	Supported	Supported
	P2419HC	Supported	Supported	Not Available	Supported
	P2421D	Supported	Supported	Not Available	Supported
	P2421DC	Not Available	Supported	Not Available	Supported
	P2719H	Supported	Supported	Supported	Supported
	P2719HC	Supported	Supported	Not Available	Supported
	P2720D	Supported	Supported	Not Available	Supported
	P2720DC	Not Available	Supported	Not Available	Supported
	P3418HW	Supported	Supported	Supported	Not Available
	P4317Q	Not Available	Supported	Supported	Not Available
	MR2416	Supported	Supported	Not Available	Not Available
	U2415	Supported	Supported	Supported	Not Available
	U2419H	Supported	Supported	Supported	Supported
	U2419HC	Supported	Supported	Not Available	Supported
	U2518D	Supported	Supported	Supported	Not Available
	U2520D	Supported	Supported	Supported	Supported
	U2718Q (4K)	Supported	Supported	Supported	Supported
	U2719D	Supported	Supported	Supported	Supported
	U2719DC	Supported	Supported	Not Available	Supported
	U2720Q	Supported	Supported	Supported	Supported
	U2721DE	Not Available	Supported	Supported	Supported
	U2421HE	Not Available	Not Available	Supported	Supported
	U4320Q	Not Available	Supported	Supported	Supported
	U4919DW	Not Available	Supported	Not Available	Not Available
Networking	Add On 1000 Base-T SFP transceiver (RJ-45)	Not Available	Supported	Not Available	Not Available
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Not Available	Supported
Storage	Dell Portable SSD, USB-C 250GB	Not Available	Supported	Not Available	Supported
	Dell External Tray Load ODD (DVD Writer)	Not Available	Supported	Not Available	Supported

Table 95. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported	Supported
	Sun microsystem SCR 3311	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Not Available	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Not Available	Supported	Not Available	Supported
Printers	Dell Color Multifunction Printer - E525w	Supported	Not Available	Not Available	Not Available
	Dell Color Printer- C2660dn	Supported	Supported	Not Available	Not Available
	Dell Multifunction Printer - E515dn	Supported	Not Available	Not Available	Not Available

Supported ecosystem peripherals for OptiPlex 3000 Thin Client

NOTE: The supported peripherals are not limited to the peripherals devices listed in this section.

Table 96. Supported ecosystem peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio Devices	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Headset - Cortez - WH3022.
	Logitech BRIO 4K Ultra HD Webcam - 960-001105 - 960-001105
	Logitech C525 HD Webcam - 960-000715 - 960-000715
	Logitech C930e HD Webcam - 960-000971 - 960-000971
	Dell Pro Stereo Soundbar - AE515M - AE515M - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - AC511M - AC511M - Potential M
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P

Table 96. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
Input Devices	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
Displays	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell 24 Monitor - P2422H - P2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell 27 Monitor - P2722H - P2722H
	Dell 22 Monitor - P2222H - P2222H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell 20 Monitor E2020H - E2020H
	Dell 27 Monitor - P2720D - P2720D
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell 24 Monitor E2420HS - E2420HS
	Dell 27 Monitor - P2720D - P2720DC
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 27 Monitor E2720HS - E2720H
	Dell 27 Monitor E2720H - E2720HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 19 Monitor E1920H - E1920H

Table 96. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell 24 Monitor E2420H - E2420H
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Supported ecosystem peripherals for Latitude 3420

Table 97. Supported ecosystem peripherals for Latitude 3420

Product Category	Peripherals
Displays	Dell 24 Monitor E2420HS - E2420HS
	Dell U3419W
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W ⓘ **NOTE:** Bluetooth connection is not supported.
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
Audio Devices	Dell Pro Stereo Headset - UC150 - UC150 - Lemmy - UC150
	Dell Pro Stereo Headset UC350

Supported ecosystem peripherals for OptiPlex 5400 All-in-One

Table 98. Supported ecosystem peripherals for OptiPlex 5400 All-in-One

Product Category	Peripherals
Displays	Dell 24 Monitor - P2421D
	Dell UltraSharp 24 Monitor - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022

Other supported peripherals

Table 99. Other supported peripherals

Product Category	Peripherals
Audio Devices	Dell Pro Stereo Headset UC350
	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth

Table 99. Other supported peripherals (continued)

Product Category	Peripherals
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth （ link 360 ）
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Support USB only, not support Bluetooth)
	Plantronics Blackwire 5220 Series
	Plantronics AB J7 PLT
	Plantronics Blackwire C5210
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Calisto P820-M
	Plantronics Voyager 6200 UC
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER SC 660 USB ML
	SENNHEISER USB SC230
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SP 10 ML Speakerphone for Lync
	Sennheiser SDW 5 BS-EU
	Logitech S-150
	POLYCOM Deskphone CX300
	PHILIPS - analog
	Logitech h150 - analog
	LFH3610/00 SPEECH MIKE PREMIUM (only support redirect)
	Nuance PowerMic II (Recommend redirecting whole device)
	Olympus RecMic DR-2200 (Recommend redirecting whole device)
Input Devices	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123
	Dell Keyboard KB216p
	Dell wireless Keyboard/mouse KM632
	Dell wireless Keyboard/mouse KM714
	Dell Keyboard KB212-B
	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard

Table 99. Other supported peripherals (continued)

Product Category	Peripherals
	Rapoo E6100, Bluetooth
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	Dell U2718Q (3840x2160)
	Dell U2719D(1920x1080)
	Dell P2719H (1920*1080)
	Dell P2715Q(3840x2160)
	Dell S2719HS (1920x1080)
	Dell S2817Q(3840x2160)
	Dell U2713HM (2560x1440)
	Dell U2718Q(3840x2160)
	Dell P2418HZ
	Dell U3219Q (3840x2160) (Does not support Type C to HDMI convertor)
	Dell P2415Q(3840X2160)
	ELO ET2202L-2UWA-0-BL-G
Camera	Logitech C920 HD Pro Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Logitech C930e HD Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C910 HD Pro Webcam
	Logitech C925e Webcam
	Poly EagleEye Mini webcam
	Logitech BRIO 4K Webcam
	Jabra PanaCast 4K Webcam
Storage	SanDisk cruzer 8 GB
	SanDisk cruzer 16G
	SanDisk USB 3.1 and Type-C 16 GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32 GB
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Dell External Tray Load ODD (Agate) (DVD Writer)
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A

Table 99. Other supported peripherals (continued)

Product Category	Peripherals
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	Dell keyboard KB813 (Smartcard reader)
	Dell Keyboard SK-3205 (Smartcard reader)
	IDBridge CT31 PIV
	Gemalto IDBridge CT710
	GemPC Twin
Proximity card readers	RFIDeas RDR-6082AKU
	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80
	Imprivata HDW-IMP-82
	Imprivata HDW-IMP-82-BLE
	OMNIKEY 5025CL
	OMNIKEY 5326 DFR
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM
	OMNIKEY 5325 CL
	KSI-1700-SX Keyboard
Fingerprint readers	KSI-1700-SX Keyboard
	Imprivata HDW-IMP-1C
	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader
Printers	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer

Table 99. Other supported peripherals (continued)

Product Category	Peripherals
	Dell B2360d Laser Printer
	HP M403D
	Brother DCP-7190DW
	Dell B2360dn Laser Printer
	Lexmark X864de
	HP LaserJet P2055d
	HP Color LaserJet CM1312MFP
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR (BLEdongle)
Teradici remote cards	Teradic host card 2220
	Teradic host card 2240
Others	Intuos Pro Wacom
	Wacom One

Known issues and Limitations with PowerMic devices

- Nuance PowerMic sound dictation does not work properly in PCoIP sessions. This causes the Dragon Medical One (DMO) software to stop responding after some time.
- Hot plugging in or plugging out the PowerMic device when it is working may cause the DMO software to stop responding. As a workaround, relaunch the software.
- It is recommended to use full redirection of the whole device in Blast and Citrix sessions. If you split redirect some buttons in Blast and Citrix sessions and plug out and plug-in PowerMic, the device is not recognized. In Blast sessions, you must also disable Bluetooth redirection or it ThinOS works abnormally.
- PowerMic stops working in the DMO software inside VMware PCoIP sessions after inserting a USB drive to the thin client. This issue occurs only if the USB drive is redirected. As a workaround, use USB disk Map settings instead of USB disk Redirection.
- PowerMic does not redirect to VMware PCoIP sessions when you do the following in sequence:
  1. Sign off from the Broker agent without closing an application.
  2. Disconnect and connect PowerMic to a different USB port.
  3. Sign into the Broker agent again.
- PowerMic does not work in DMO software after disconnecting PowerMic II and connecting PowerMic III when a VMware PCoIP session is open.
- The mouse pointer is not displayed in VMware PCoIP sessions when using PowerMic As a workaround, sign out and sign into the Broker agent.

Workaround

Workaround for the above mentioned limitations are:

- If you are using Power Mic 2 and 3, you must enable **Allow USB Imaging Family Device** and add 0x05541001, NoDriver in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Session Settings > Session Settings**.
- If you are using Power Mic 4, you must enable **Allow USB Imaging Family Device** and add 0x05540064, NoDriver in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Session Settings > Session Settings**.

Fixed issues

Table 100. Fixed issues

Issue ID	Description
DTOS-13752	Need a demo build for SNMP V3 reboot functionality—CIPS-28285.
DTOS-13733	In ThinOS 2208 and Citrix Workspace Application 2208, CTRL + F2 does not work in Citrix Session—CIPS-29001.
DTOS-13697	VDI disconnection (shutdown timer) issue—CIPS-29051
DTOS-13378	LPD Printer mapping properly but does not print—CIPS-28733.
DTOS-13308	**DelayReboot** option is not present in ThinOS 9.x versions, which was available in ThinOS 8.6—CIPS-28768.
DTOS-13232	Local login dialog box displays over the Azure Authentication dialog box—CIPS-28692 and 28811.
DTOS-13180	ThinOS 9.1.6108: Thin clients stop responding, and there is an issue connecting to the network. Citrix login page takes more than five minutes to be displayed—CIPS-28770.
DTOS-13034	Connection issues with OptiPlex 3000 devices after updating to ThinOS 2208 from ThinOS 9.1_4097—CIPS-28667.
DTOS-12827	Horizon Unified Access Gateway (UAG) with Azure Multifactor Authentication (MFA) or non-MFA has login issues with some groups—CIPS-28524.
DTOS-12726	ThinOS does not automatically log in to the Citrix Broker agent—CIPS-28146.
DTOS-12631	Need a demo build for SNMP V3 reboot functionality—CIPS-28285.
DTOS-12614	Unable to launch from the client desktop selection on ThinOS 2208—CIPS-28335
DTOS-12567	Issues when Horizon desktop pools have spaces in their name—CIPS-28332.
DTOS-12565	Cannot launch sessions from Workspace One on Wyse 5070 with ThinOS 2208—CIPS-28105.
DTOS-12470	Firmware and package download speed is reduced after upgrading to ThinOS 9.1.6108 or later versions—CIPS-28245 and 28160.
DTOS-12400	Group Auto assignment using a rule does not work after factory reset on Wyse 5070 thin client with ThinOS 2208—CIPS-28262.
DTOS-12401	Devices using unsupported group tokens must be reimaged through USB to connect to Wyse Management Suite again. This issue occurs on Wyse 5070 with ThinOS 2208—CIPS-28261.
DTOS-12380	When the device is in Sleep mode, **Enable auto log off** functions even when not enabled. This occurs on Wyse 5070 with ThinOS 9.3.1129.
DTOS-12348	Cannot launch session from Workspace ONE Intelligent Hub—CIPS-28176.
DTOS-12346	AVD Idle Timeout issues in ThinOS 9.3.1129.
DTOS-12325	Dell C2422HE Monitor Volume dialog box always shows 30% on Wyse 5070 with ThinOS 9.3.1129 or 2208—CIPS-28161.
DTOS-12257	Barcode scanners unable to scan barcodes after upgrading to ThinOS 9.x versions—CIPS-27985
DTOS-12255	US International keyboard layout issues after migrating from ThinOS 8.x to 9.x—CIPS-28142
DTOS-12194	After connecting to a Blast session, a dialog box with **The connection to the remote computer ended**. Is displayed on Wyse 3040 with ThinOS 9.3.1129.
DTOS-12148	Select Group Change Issues—CIPS-27991

Table 100. Fixed issues (continued)

Issue ID	Description
DTOS-11902	SMB printer does not work in a session until a test print is done on the local client—CIPS-27893.
DTOS-11807	The **?** Key is inaccessible while using ABNT2 Layout on Bloomberg keyboard for Wyse 5070—CIPS-27403.
DTOS-11806	Green artifacts are displayed on the incoming video when using Teams in web browsers with BCR enabled—CIPS-27430.
DTOS-11742	RDS-published applications do not appear when there are more than 100 applications displayed on the thin client with ThinOS 9 versions—CIPS-27740.
DTOS-11568	**Missed heartbeat threshold exceed** message is displayed, and session disconnects on thin clients with ThinOS 2205—CIPS-27748.
DTOS-11566	Audio instability issues—CIPS-26969
DTOS-11475	Blast session does not expand to the second monitor after waking from Sleep mode or turning on after power off—CIPS-27529.
DTOS-11312	Printer maps to **MS Publisher Imagesetter** in RDP sessions on OptiPlex 3000 with ThinOS 9.3.1129—CIPS-27566.
DTOS-10858	ThinOS does not reconnect using credentials set in the policy—CIPS-26653.
DTOS-10453	Thin Client cannot launch resources from Workspace ONE Intelligent Hub—CIPS-27193.
DTOS-10452	Default Username and Password does not persist when configured in APT on ThinOS 2205.
DTOS-10291	Audio stops working after thin client has been idle for an extended time—CIPS-27143.
DTOS-10290	After setting HP LaserJet 4500 as default printer in Citrix Published Apps and logging off, the default printer reverts to another printer—CIPS-26818 and 27285.
DTOS-9890	Audio device changes automatically when monitor wakes from Sleep—CIPS-26833.
DTOS-9797	Select Group does not work on ThinOS 9.x Policy with Imprivata Enabled—CIPS-26929.
DTOS-9688	Need option for thin clients to register with DNS or WINS—CIPS-26770.
DTOS-5738	USB headset issue after resuming from Sleep mode—CIPS-24678 and 26833
DTOS-12576	Keyboard with dedicated calculator key does not open calculator in Citrix—CIPS-28274.
DTOS-13545	Smartcard authentication to Citrix desktop fails—CIPS-27470
DTOS-6928	Shortcut keys in Cherry keyboard do not work in ThinOS 9.x—CIPS-22863.
DTOS-13032	A second RDP authentication dialog box is displayed with prepopulated credentials after initial successful authentication—CIPS-28460.
DTOS-8120	Multiple authentication prompts are displayed for Azure Multifactor Authentication (MFA)—CIPS-26123

Known issues

Table 101. Known issues

Issue ID	Description	Workaround
DTOS-13728	A gray screen appears when launching VMware Blast applications.	This is a VMware limitation.
DTOS-13676	Horizon Login window with error message is displayed for a long time after logging in to Horizon and Azure successfully.	Wait for some time and do not close the login window.
DTOS-13575	After turning on or off the **PIP/PBP** option, audio does not work.	HDMI or DisplayPort audio works after reboot.

Table 101. Known issues (continued)

Issue ID	Description	Workaround
DTOS-13519	Unable to decrease the audio locally on Dell U4924DW monitor.	There is no workaround in this release.
DTOS-13518	After waking from Sleep, audio does not work locally on Dell U4924DW monitor.	There is no workaround in this release.
DTOS-13511	Two mouse pointers are displayed in an RDP session after modifying the Desktop scale factor in RDP tab.	There is no workaround in this release.
DTOS-13465	Screen alignment is not proper after logging in to Citrix with Imprivata PIE enabled and dual displays are configured in span mode.	Configure the external DisplayPort-connected display as the main display.
DTOS-13439	The RDP session stops responding when plugging in the camera and launching the Camera application	Jabra PanaCast and Polycom EagleEye Mini Camera are not supported in RDP sessions.
DTOS-13426	The locale cannot be set to the default value when disabled through Wyse Management Suite.	There is no workaround in this release.
DTOS-13396	The VMware Blast session cannot launch after disconnecting from the network when using a Broker agent.	Sign off from the Broker agent and sign in again.
DTOS-13352	Unlocking the terminal with the wrong password.	Do not enable **Use the same user and password for RADIUS and Windows authentication** in Horizon Connection Server.
DTOS-13121	The side wheel of the mouse does not work.	The side wheel of the mouse is not supported in remote sessions.
DTOS-12930	After connecting two external cameras to the rear ports of Wyse 5070 thin client, only one camera works.	There is no workaround in this release.
DTOS-12142	After uploading the INI file and enabling Jabra firmware update in APT, the firmware update works only once after clicking **Save & Publish**.	Use Wyse Management Suite policy instead of admin policy tool.
DTOS-11538	VMware PCoIP sessions give out a crackling sound.	There is no workaround in this release.
DTOS-9847	Microsoft Teams application on Wyse 5470 has audio issues when sharing screen.	Do not enable camera during Microsoft Teams calls or meetings, and do not move applications quickly when sharing screen.

6

ThinOS 2208

Release date

November 2022

Release summary

Patches or Add-on releases are created to support existing platforms or software releases, correct defects, make enhancements, or add minor features.

Current version

ThinOS 2211 (9.3.3xxx)

Previous version

ThinOS 2208 (9.3.2102)

Firmware upgrade

The following firmware upgrade scenarios are supported:

- 9.1.3129 or later versions > ThinOS 2208 (9.3.2102)

> **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2208.

> **NOTE:** If you want to downgrade ThinOS 2208 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2208 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

- There are chances that after the upgrade the device displays a black screen. You may reboot the device to boot it up correctly.
- If the thin client is registered in Wyse Management Suite group 1 and you set Wyse Management Suite group 2 token in group 1 policy, then the group 2 token is applied on GUI but the thin client will still be in group 1. You must reboot the thin client to change the thin client to Wyse Management Suite group 2.

  > **NOTE:** Dell Technologies recommends that you set both new ThinOS firmware and new application packages in Group 1, so that thin client installs the files, automatically reboots, and changes to Group 2.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:

  - Not display a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - Not display any notification if the new firmware or application is downloaded in the same group.
  - Installs the firmware or package after a reboot.
- If you have installed HID_Fingerprint_Reader package, ensure that you have also installed Citrix_Workspace_App package, or you cannot upgrade to ThinOS version 2208.
- If you configure settings, like brokers, locally in ThinOS 2208 and downgrade to ThinOS 2205 or earlier versions using Wyse Management Suite, the settings are lost.
- If you downgrade to ThinOS 2205 or earlier versions using Wyse Management Suite, reboot the system manually again to set a password locally in ThinOS. Otherwise, the password may not be clear.

Prerequisites for firmware upgrade

- Before you upgrade from ThinOS 9.x to ThinOS 2208, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the Wake On LAN command through Wyse Management Suite before using any real-time commands. To use the Wake On LAN command, ensure that the Wake On LAN option is enabled in BIOS.

Upgrade from ThinOS 9.1.x to ThinOS 2208 using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the ThinOS 2208 (9.3.2102) firmware to upgrade.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**. The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **OS Firmware Updates**.

   ⓘ **NOTE:** If you cannot locate the **OS Firmware Updates** option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse** and select the **ThinOS 2208** firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.
   The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

   ⓘ **NOTE:** There are chances that the upgrade might fail with event log stating **Failed to install**. In such an event, you may reboot the device and upgrade again.

   ⓘ **NOTE:** To optimize security, application performance, and stability, a design change has been made in ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

   ⓘ **NOTE:** There are chances that the ThinOS background might be in blue color and some features may not work. In this case, you have to reboot the device.

Convert Ubuntu 20.04 with DCA to ThinOS 2208

The conversion is supported on Latitude 3420 and OptiPlex 5400 All-in-One.

Prerequisites

- If you have a device that is running Ubuntu 20.04 operating system, ensure that DCA-Enabler 1.5.0-14 or later versions is installed. For details on how to install DCA-Enabler in Ubuntu operating system and upgrade it, see Dell Wyse ThinOS Migration Guide at www.dell.com/support.

  ⓘ **NOTE:** The device must have a factory-installed Ubuntu 20.04 operating system. If you have custom installed the Ubuntu operating system, you cannot convert it to ThinOS 2208.
- Wyse Management Suite version 3.7 or later versions must be used to convert to ThinOS 2208.
- Ensure that you have connected the device to the external power source using the power adapter.
- Ensure you have enough ThinOS Activation devices licenses on Wyse Management Suite 3.7 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than the device number. If it is not larger, you cannot create the Advanced Policy for conversion.
- The Ubuntu 20.04 devices must be registered to Wyse Management Suite as generic clients. For details on how to register the generic client to Wyse Management Suite, see Dell Wyse ThinOS Migration Guide at www.dell.com/support.
- Ensure you have downloaded the Ubuntu 20.04 to ThinOS 2208 conversion image.
- Extract the Ubuntu 20.04 to ThinOS 2208 conversion image to get the Conversion Installer file **DTOS_Ubuntu_Installer_1.1-dtos4-amd64_signed.tar.gz** and ThinOS image **ThinOS_2208_9.3.2102.pkg**.

  ⓘ **NOTE:** The ThinOS image **ThinOS_2208_9.3.2102.pkg** can be used for downgrade in the future.

Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the Conversion Installer file **DTOS_Ubuntu_Installer_1.1-dtos4-amd64_signed.tar.gz**
3. Go to **Apps & Data** > **OS Image Repository** > **ThinOS 9.x**, and click **Add Firmware file**.
4. Upload the ThinOS image **ThinOS_2208_9.3.2102.pkg**.
5. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
6. Enter the policy name, select the group in which the Ubuntu devices have been registered, and select **Generic Client** as OS type.
7. Click **Add app**, and select the conversion installer file that was uploaded before from the drop-down menu.
8. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
9. Select the platforms you want to convert in the **Platform Filter** drop-down menu.
10. Click **Save**.

    ⓘ **NOTE:** Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
11. In the next window, click **Yes** to schedule a job.
12. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.
13. Click **Schedule**.

    The Conversion Installer file downloads and installs first followed by the ThinOS image. After installation, the device restarts automatically.

    ⓘ **NOTE:** After you register the converted ThinOS device to Wyse Management Suite, the ThinOS activation devices license is consumed automatically.

    ⓘ **NOTE:** After conversion, ThinOS 2208 is in the factory default status. ThinOS 2208 must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

    ⓘ **NOTE:** If the conversion has failed, you can see the error log table below and reschedule the job. Go to **Jobs** > **Schedule APP Policy** to reschedule the job.

    If there is a **/usr/dtos** folder in your Ubuntu 20.04 device, you can use the command **cat /var/log/dtos_dca_installer.log** to get the error log. If the conversion has failed, it is recommended to install ThinOS ISO image.

    If there is no **/usr/dtos folder** in your Ubuntu 20.04 device, go to the **WMS Server Jobs** page to check the error messages.

Table 102. Error Log table

Error Log	Resolution
No AC plugged in	Plug in power adapter, reschedule job
Platform Not Supported	This hardware platform is not supported
Error mounting recovery partition	The Ubuntu image is not a factory image. Reinstall the factory image.
No DHC/ThinOS package in recovery partition	Cannot find the ThinOS image, reschedule job
Error in extracting DHC/ThinOS Future packages	Failed to extract the ThinOS image, reschedule job
Error copying the DHC/ThinOS Future packages to recovery partition	Failed to copy the ThinOS image, reschedule job
ThinOS package verification failed	ThinOS image is not correct, reschedule job with the correct ThinOS image
Not enough space in Recovery Partition	Clear the recovery partition
The free space of Recovery Partition is not enough	Clear the recovery partition

Compatibility

ThinOS application package details

- Citrix_Workspace_App_22.7.0.20.2.pkg
- Epos_Connect_7.2.0.29149.1.pkg
- HID_Fingerprint_Reader_210217.18.pkg
- VMware_Horizon_2206.8.6.0.20094634.1.pkg
- Identity_Automation_QwickAccess_2.0.2.1.0.pkg
- Imprivata_PIE_7.8.000.0008.1161.pkg
- Imprivata_PIE_7.9.000.0023.1162.pkg
- Jabra_8.5.5.1.pkg
- Cisco_Jabber_14.1.1.306904.1.pkg
- Teradici_PCoIP_22.04.2.13.pkg
- Cisco_Webex_VDI_42.6.0.22645.1.pkg
- Cisco_Webex_Meetings_VDI_42.8.2.8.1.pkg
- Microsoft_AVD_1.8.1819.pkg
- Zoom_Citrix_5.10.6.21295.2.pkg
- Zoom_Horizon_5.10.6.21295.2.pkg

NOTE: To optimize security, application performance, and stability, a design change has been made in ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 3.8.181
- Configuration UI package 1.9.72

NOTE: Upgrade ThinOS 2208 ConfigUI first before upgrading to ThinOS 2208 operating system firmware.

ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2208 (9.3.2102)—**ThinOS_2208_9.3.2102.pkg**
- Ubuntu 20.04 + DCA 1.5.0-14 to ThinOS 2208 conversion build
  - **ThinOS_2208_9.3.2102_Conversion.zip**—Dell Latitude 3420 and Dell OptiPlex 5400 All-in-One

BIOS packages

Table 103. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.18.0.pkg
Wyse 5470 Thin Client	bios-5470_1.15.0.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.14.1.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.2.0.pkg
Dell Latitude 3420	bios-Latitude_3420_1.18.0.pkg
Dell OptiPlex 5400 All-in-One	bios-OptiPlex5400AIO_1.0.9.pkg

Tested BIOS version for ThinOS 2208

Table 104. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.18.0
Wyse 5470 All-in-One Thin Client	1.14.1
Wyse 5470 Mobile Thin Client	1.15.0
OptiPlex 3000 Thin Client	1.2.0
Latitude 3420	1.18.0
OptiPlex 5400 All-in-One	1.0.9

Citrix Workspace app feature matrix

Table 105. Citrix Workspace app feature matrix

Feature		ThinOS 2208 with CWA 2207	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	Webcam redirection works for both 32-bit and 64-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser or 64-bit browser to verify webcam redirection online. For example, www.webcamtests.com. For further details, refer to the Dell Wyse ThinOS Administrator's Guide.
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information,

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
			see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco Webex Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebexTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
			configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netscaler + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Support for secondary ringer(CWA2207	Not Supported	Not supported
	Improved audio echo cancellation support [Technical Preview] (CWA2207)	Not Supported	Not supported
	Composite USB device redirection(CWA2207)	Not Supported	Not supported
	Support for DPI matching [Technical Preview](CWA2207)	Not Supported	Not supported

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	Enhancement to improve audio quality (CWA2207)	Not Supported	Not supported
	Provision to disable LaunchDarkly service (CWA2205)	Not Supported	Not supported
	Email-based auto-discovery of store (CWA2205)	Not Supported	Not supported
	Persistent login [Technical Preview] (CWA2205)	Not Supported	Not supported
	Authentication enhancement for Storebrowse (CWA2205)	Not Supported	Not supported
	Support for EDT IPv6 (CWA2203)	Not Supported	Not supported
	Support for TLS protocol version 1.3 (CWA2203)	Not Supported	Not supported
	Custom web stores (CWA2203)	Not Supported	Not supported
	Authentication enhancement experimental feature (CWA2203)	Not Supported	Not supported
	Keyboard layout synchronization enhancement (CWA2203)	Not Supported	Not supported
	Multi-window chat and meetings for Microsoft Teams (CWA2203)	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams (CWA2112)	Not Supported	Not Supported
	Request control in Microsoft Teams (CWA2112)	Not Supported	Not supported
	Support for cursor color inverting (CWA2112)	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	There are no limitations in this release.
	Enhancement on smart card support (CWA2112)	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Supported	There are no limitations in this release.
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106, CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio devices(CWA2012, CWA2010, and CWA2112)	Not supported	If JVDI package is installed in ThinOS, audio devices cannot be switched in the applications in session and the session is disconnected when users open the **Recording devices** list at the Windows sound. If you want to use multiple ICA audio devices, it is recommended that you do not install the VDI package.
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.

Table 105. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2208 with CWA 2207	Limitations
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

ThinOS AVD Client Feature Matrix

Table 106. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 9.3
Service	Direct connection to Desktop via RDP	Supported
	Remote Desktop Services broker (Local)	Supported
	Windows Virtual Desktop (Azure)	Supported
Session	Desktop	Supported
	Remote App (Integrated)	Not supported
	Remote App (Immersive)	Supported
	Multiple connections	Supported
Input	Keyboard	Supported
	Mouse	Supported
	Single Touch	Supported
Audio Visual	Audio in (microphone)	Supported
	Audio out (speaker)	Supported

Table 106. ThinOS AVD Client Feature Matrix (continued)

Category Supported	Features	ThinOS 9.3
	Camera	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
Redirections	Printer	Supported
Session Experience	Dynamic Resolution	Supported
	Start Command	Supported
	Desktop Scale Factor	Supported
	Multi-Monitor (All)	Supported
	Restricted full screen session	Supported
	Keyboard Layout Mapping	Supported
	Time Zone Mapping	Supported
	Video/Audio/Online playback	Supported
	Compression	Supported
	Optimize for low speed link	Supported
Graphics (CODECs)	H.264 Hardware Acceleration	Supported
Authentication	TS Gateway	Supported
	NLA	Not supported
	SmartCard	Not supported
	Imprivata	Supported

New and enhanced features

Citrix Workspace app updates

- Citrix Workspace App package version is updated to 22.7.0.20.2.

NOTE: If you want to install the Citrix Workspace app version 2207 on ThinOS, install this package.

- **Multi-window chat and meetings for Microsoft Teams**—From ThinOS 2208 and Citrix Workspace App 2207 onwards, multiwindow chat and meetings for Microsoft Teams is supported.

  NOTE: Ensure that you have Citrix Workspace App package version 22.7.0.20.2 or later, VDA 2112 or later, and Microsoft Teams 1.5.00.11865 or later. A sign-out, sign in, and restart from Microsoft Teams is also required.

- **Webcam redirection for 64-bit applications**— From ThinOS 2208 and Citrix Workspace App 2207 onwards, webcam redirection or HDX RealTime Webcam Video Compression is supported for 64-bit applications. Webcam redirection works for 32-bit and 64-bit applications, like Skype, GoToMeeting. Use a 32-bit browser or 64-bit browser to verify webcam redirection online. By default, ThinOS only supports webcam redirection feature for 32-bit apps. To enable webcam redirection for 64-bit apps, do the following:

  1. In Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced tab** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
  2. In the **Citrix INI settings**, click **Add Row**.
  3. From the **File** drop-down list, select **wfclient.ini**.
  4. From the **Operation** drop-down list, select **Add or Update** .
  5. In the **Section** field, enter **WFClient**.

6. In the Key field, enter **HDXH264InputEnabled**.
7. In the Value field, enter **True**.
8. Sign out or restart the device for the settings to take effect.

- RTME (Citrix HDX Realtime Media Engine) is updated to 2.9.500-2802.
- **USB device redirection with Citrix Desktop Viewer**—From ThinOS 2208 and Citrix Workspace App 2207, **Devices** section is displayed in**Citrix Desktop Viewer**. To redirect the USB devices from the **Devices** section to the session, do the following:
  1. In a desktop session, go to **Desktop Viewer** under **Devices**. The USB devices are displayed.
  2. Select the USB device that you want to redirect.

  To redirect the USB devices from the **Preferences** section to the session, do the following:
  1. Go to **Preferences** > **Devices**. The USB devices are displayed.
  2. Select the **Redirect** check boxes next to the devices.
  3. Click **OK**.

  > **NOTE:** Clear the required menu item or check boxes next to the devices to disconnect a device from session. By clearing the menu items or check boxes, the devices are mapping in session.

  Limitations of USB device redirection with Citrix Desktop Viewer
  - By default, only USB disk, USB storage, USB DVD ROM can be used to redirect or map into a session.
  - By default, the printer, audio, video devices, and composite devices such as Bloomberg keyboard are restricted by policy to redirect to session as these devices are controlled by Admin Policy Tool or WMS policy. You can allow the devices to redirect to session from Admin Policy Tool or Wyse Management Suite by going to **Advanced** > **Session Settings** > **Global Session Settings** or by going to **Advanced** > **Peripheral Management** > **USB Redirection Settings**. These devices are allowed to redirect or disconnect from the **Devices** section in Citrix Desktop Viewer.
- **Citrix Workspace App Limitations**
  - The following new features from Citrix Workspace App 2207 are not supported in ThinOS.
    - Support for secondary ringer
    - Improved audio echo cancellation support
    - Composite USB device redirection
    - Support for DPI matching
    - Improved audio quality

    The following issues also occur in Linux Citrix Workspace app binary:
  - When doing OKTA authentication to NetScaler, the locked account does not get the error message **Incorrect password** and **Your account is temporarily locked**.
  - HD Pro Webcam C920 does not work during Webex Teams VDI video calls.
  - An error message **Webex Call failed** is displayed when starting a video call using HDX Web Camera through a VDI fallback mode Webex Teams application.
  - Sometimes, nothing can be entered using the keyboard on the Browser Content Redirection (BCR) page or VDA desktop.
  - When UDP audio is enabled, Multiple Media Redirection (MMR) video stops responding, and there is no audio.
  - When playing a video through VLC Media Player, the audio is distorted. The issue occurs only on OptiPlex 5400 All-in-One.
  - The test cursor is not blinking in Command Prompt in the VDA server.
  - Citrix Desktop View Toolbar Preferences and Devices window is displayed locally on ThinOS.
  - When playing videos using VLC Media Player in Citrix VDI, Citrix sessions stop responding for about 10 s.
  - Dell Webcam WB5023 camera cannot redirect to Citrix VDA desktop.
  - Citrix session VDA displays **Connection Interrupted** after plugging out and plugging in a redirected Samsung smartphone.
  - USB audio device redirection with Windows Server 2022 fails.
  - When using redirection with Dell WB7022 USB camera, there is no video output.
  - Citrix Desktop toolbar does not work in ICA Desktop VDI session.
  - When the mouse pointer is placed on a blank screen, the screen shows a tooltip on the Home button window in Citrix Workspace mode.
  - When playing Multiple Media Redirection (MMR) video in VDA2203 desktop, the video stops responding.
  - Sharing your screen during a Microsoft Teams video meeting disconnects the call.
  - The mouse cursor is not displayed properly in Word in ICA Windows server 2022 desktop.
  - Invert cursor option does not work in ICA Windows server 2022 desktop.

Azure Virtual Desktop (AVD) updates

AVD auto login— Set the default credentials in **Remote Connections** > **General Option**, and enable the Azure Virtual Desktop Broker agent. When you reboot the client, you need not enter the credentials again, as the client automatically logs in using the AVD Broker agent.

AVD auto connect list— Enter the name of the connection that is displayed in **Connection Manager** to automatically connect after you log in the AVD Broker agent. You can enter more than one connection name. Each connection name is separated by a semicolon and is case-sensitive.

Teradici PCoIP update

- Teradici version is updated to 22.04.2.13 in ThinOS 2208.
- **Support for PCoIP display real time refresh**— There is no need to disconnect and reconnect to PCoIP session to have a new display setting take effect. The PCoIP session adjusts the display settings in real time when changed. This is applicable in the following scenarios:
  - Hot plugging in or plug out a monitor.
  - Changing the resolution in display settings.
  - Rotating the monitor in display settings.
  - Closing and reopening the lid when session is launched.

Horizon Blast Updates

- HD Pro Webcam C920 and Logitech BCC950 Conference Camera do not work on Webex Teams VDI video call. The issue also occurs in Horizon Linux Clients.
- Wyse 3040 Thin Client uses H264 software decoder and MMR/H264/HEVC is not supported on Horizon Client 2206 with ThinOS 2208.

Limitations and Known Issues

- Camera names are not displayed correctly in Horizon SFB due to a VMware limitation.
- Blast session may not launch due to a compatibility issue with the Zoom Horizon package. The workaround for the issue is to go to **Systems Tools** > **Packages** and delete the **Zoom Horizon** package.
- HEVC is not supported in this release.
- The following limitations are applicable only on OptiPlex 5400 All-in-One:
  - ThinOS may reboot unexpectedly when disconnecting the blast session that has a redirected camera.
  - If the USB port on the side is used for connecting to a camera, some cameras do not work during Microsoft Teams or Cisco JVDI calls. This is a hardware limitation. Connect the camera to a rear USB port for the camera to function during Microsoft Teams or Cisco JVDI calls.

Imprivata updates

- **Imprivata virtual channel support in AVD**— AVD session supports Imprivata virtual channels with this release. When you log in to an AVD session using Imprivata PIW or Imprivata PIE, you can enroll using a proximity card and fingerprint in the Imprivata agent in AVD session. You can also log in through the Imprivata agent by tapping the proximity card or using your fingerprint.
- The Imprivata PIE application support matrix is as follows:

Table 107. Supported and Tested Matrix on ThinOS 2205

ThinOS PIE application	OneSign Server	
	version 7.8.000.11	version 7.9.000.11
7.8.000.0008.1161	yes	N/A
7.9.000.0023.1162	N/A	yes

Cisco Webex Meetings VDI updates

- Cisco Webex Meetings VDI package version is updated to 42.8.2.8 (special release based on 42.6).
- Supports **Virtual Background/Blur image** from this release.

  ⓘ **NOTE:** You may see version 42.8.2.8 in ThinOS Packages Details. This is just a special update of 42.6 version.

Cisco Webex Meetings VDI feature matrix

Table 108. Cisco Webex Meetings optimization feature matrix

Scenarios	ThinOS 2208 (9.3.2102)
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Lock meeting	Supported
Return meeting	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—To everyone	Supported
Chat—To specified participants	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Share one of the applications	Supported
Share screen—Switch share content	Supported

Table 108. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 2208 (9.3.2102)
Share screen—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported
Participant	Supported
Close Participant	Supported
Invite and Remind	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Names in video calls automatically hidden when not speaking	Supported
Show all names/Hide all names/Show participants without video	Supported
Increase or Decrease Video size	Supported
Virtual Background/Blur image	Supported
VDI Meetings can display and extend participant grid view from 3x3 to 5x5	Not tested

Cisco Webex Meetings VDI limitations

- If a user increases the zoom percentage to 213%, the shared screens of other users are not visible.
- While viewing the shared video from others, zooming percentage varies automatically from 103% to 220%. The issue is observed on Wyse 5070 standard thin client and Latitude 3420 with ThinOS.
- When a user moves the shared screen from another user in a side-by-side layout, there is an issue with the user interface.
- When a user minimizes and restores the meeting session, there is a delay in viewing the videos from other users.
- While sharing screen, if you play a local or online video, the shared video is not clear for other users.
- When a user is already sharing the screen and if a new user joins the meeting, the screen sharing gets delayed.
- On Wyse 5470 All-in-One thin clients, the shared video from another user stops responding.
- Virtual background preview window does not move smoothly while moving the videos setting window in Wyse 5470 thin client.
- A gray patch is displayed on the window screen when a user shares screen on a **WebEx Meetings** call.
- When you join a **WebEx Meetings** call, an error message that states cannot start, or join the meeting is displayed.

Cisco Webex VDI update

- Cisco Webex VDI package version is updated to 42.6.0.22645.1.
- Added a new feature to remove a user from a conference call.

Cisco Webex VDI feature matrix

Table 109. Cisco Webex optimization feature matrix

Scenarios	ThinOS 2208 (9.3.2102)
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Chat—To everyone	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Not Supported
Breakout sessions (Create Breakout room under Teams Tab join Manually)	Supported
Support—Request Desktop Control	Not Supported
Support—Request Application Control	Not Supported
Stop share screen	Supported
Participant	Supported
Remove Participant	Supported

Table 109. Cisco Webex optimization feature matrix (continued)

Scenarios	ThinOS 2208 (9.3.2102)
Invite and Remind	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Names in Video-Automatically Hide names when not Speaking,	Supported
Virtual Background/Blur image	Not Supported

Cisco Webex VDI limitations

The following features are not supported:

- 911 Wireless Location Reporting (CER)
- Automatically Optimize Shared Content
- Background noise reduction
- Blur and virtual background
- ICE support for media optimization
- Music Mode
- The down arrow does not work in **Audio** and **Video** options in Webex Teams.

Zoom updates

- Zoom Citrix package version is updated to 5.10.6.21295.2
- Zoom Horizon package version is updated to 5.10.6.21295.2
- **Added support for gesture recognition**— Admins can enable users to provide reactions to speakers using hand gesture recognition during meetings.

Fixed issues

- An issue where the audio from a focused share session could be heard when new participants joined has been fixed.
- Changing the display view to a grid for the side panel may result in the **Mute** option not being displayed for all participants. Now, the Mute button is displayed for all participants.
- For the Linux VDI Plugin, the virtual background selection tab was incorrectly displayed when virtual backgrounds were disabled in the web configuration.
- The text displayed for the **Unmute** option was incorrect when using the **Request permission to Unmute participants** option.
- The dialog box to pick a color for the **I have a green screen** option was not allowing the user to select a color. This issue occurred when the dialog box was opened while video was being displayed in a meeting.

Zoom feature matrix

Table 110. Zoom feature matrix

Scenarios	ThinOS 2208 (9.3.2102)
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported

Table 110. Zoom feature matrix (continued)

Scenarios	ThinOS 2208 (9.3.2102)
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Chat—To everyone	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Not Supported
Breakout sessions (Create Breakout room under Teams Tab join Manually)	Supported
Support—Request Desktop Control	Not Supported
Suppor—Request Application Control	Not Supported
Stop share screen	Supported
Participant	Supported
Remove Participant	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Virtual Background/Blur image	Supported

Zoom limitation

The performance is low while using hardware platforms with 2 core processors. Use platforms with 4 core processors to avoid performance issues.

ThinOS enhancements

- Supports ET2201L IntelliTouch ZB (Worldwide) - E382790 and ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473 ELO touch monitors.
- **Supports OptiPlex 5400 All-in-One**
  - The following hardware configurations are supported:

Table 111. Hardware configurations that are supported for OptiPlex 5400 All-in-One

Hardware Type	Hardware
CPU	Intel Pentium Gold G7400, 6 MB cache, 2 cores, 4 threads, up to 3.70 GHz, 46 W
	Intel Pentium Gold G7400T, 6 MB cache, 2 cores, 4 threads, up to 3.10 GHz, 35 W
	12th Generation Intel Core i3-12100, 12 MB cache, 4 cores, 8 threads, 3.30 GHz to 4.30 GHz, 60 W
	12th Generation Intel Core i3-12100T, 12 MB cache, 4 cores, 8 threads, 2.20 GHz to 4.10 GHz, 35 W
	12th Generation Intel Core i3-12300, 12 MB cache, 4 cores, 8 threads, 3.50 GHz to 4.40 GHz, 60 W
	12th Generation Intel Core i3-12300T, 12 MB cache, 4 cores, 8 threads, 2.30 GHz to 4.20 GHz, 35 W
	12th Generation Intel Core i5-12400, 18 MB cache, 6 cores, 12 threads, 2.50 GHz to 4.40 GHz, 65 W
	12th Generation Intel Core i5-12400T, 18 MB cache, 6 cores, 12 threads, 1.80 GHz to 4.20 GHz, 35 W
	12th Generation Intel Core i5-12500, 18 MB cache, 6 cores, 12 threads, 3 GHz to 4.60 GHz, 65 W
	12th Generation Intel Core i5-12500T, 18 MB cache, 6 cores, 12 threads, 2 GHz to 4.40 GHz, 35 W
	12th Generation Intel Core i5-12600, 18 MB cache, 6 cores, 12 threads, 3.30 GHz to 4.80 GHz, 65 W
	12th Generation Intel Core i5-12600T, 18 MB cache, 6 cores, 12 threads, 2.10 GHz to 4.60 GHz, 35 W
	12th Generation Intel Core i7-12700, 25 MB cache, 12 cores, 20 threads, 2.10 GHz to 4.90 GHz, 65 W
	12th Generation Intel Core i7-12700T, 25 MB cache, 12 cores, 20 threads, 1.40 GHz to 4.60 GHz, 35 W
Memory	4 GB, 1 x 4 GB, DDR4, 3200 MHz
	8 GB, 1 x 8 GB, DDR4, 3200 MHz
	16 GB, 1 x 16 GB, DDR4, 3200 MHz
	16 GB, 2 x 8 GB, DDR4, 3200 MHz
	32 GB, 1 x 32 GB, DDR4, 3200 MHz
	32 GB, 2 x 16 GB, DDR4, 3200 MHz
	64 GB, 2 x 32 GB, DDR4, 3200 MHz
Storage	1 TB, 5400 RPM, 2.5-inch, SATA, HDD
	2 TB, 5400 RPM, 2.5-inch, SATA, HDD
	500 GB, 7200 RPM, 2.5-inch, SATA, HDD
	500 GB, 7200 RPM, 2.5-inch, SATA, HDD, Self-Encrypting, Opal 2.0, FIPS
	1 TB, 7200 RPM, 2.5-inch, SATA, HDD
	256 GB, M.2 2230, PCIe NVMe Gen3 x4, SSD, Class 35
	512 GB, M.2 2230, PCIe NVMe Gen3 x4, SSD, Class 35

Table 111. Hardware configurations that are supported for OptiPlex 5400 All-in-One (continued)

Hardware Type	Hardware
	1 TB, M.2 2230, PCIe NVMe Gen3 x4, SSD, Class 35
	256 GB, M.2 2230, PCIe NVMe Gen3 x4, SSD, Self-Encrypting, Opal 2.0, FIPS, Class 35
	512 GB, M.2 2280, PCIe NVMe Gen4 x4, SSD, Class 40
	1 TB, M.2 2280, PCIe NVMe Gen4 x4, SSD, Class 40
	2 TB, M.2 2280, PCIe NVMe Gen4 x4, SSD, Class 40
	512 GB, M.2 2280, PCIe NVMe Gen3 x4, SSD, Self-Encrypting, Opal 2.0, FIPS, Class 40
	1 TB, M.2 2280, PCIe NVMe Gen3 x4, SSD, Self-Encrypting, Opal 2.0, FIPS, Class 40
Wireless	Intel AX201
	Intel AX211
Integrated Camera	FHD camera
	IR camera
Display	23.8 in., FHD 1920 x 1080, 60 Hz, anti-glare, touch
	23.8 in., FHD 1920 x 1080, 60 Hz, anti-glare, nontouch
Optional DVD	Optional DVD on Stand

  - The following hardware configurations are not supported for OptiPlex 5400 All-in-One:

Table 112. Hardware configurations that are not supported for OptiPlex 5400 All-in-One

Hardware Type	Hardware
Wireless	Realtek RTL8822CE
Media-card reader	SD 4.0 card slot

- **ThinOS Limitations on OptiPlex 5400 All-in-One**
  - Few applications have an audio issue when recording with the integrated microphone.
  - Sleep mode is not supported.
  - HDMI-in port is not supported, so OptiPlex 5400 All-in-One with ThinOS cannot be used as a monitor.

  NOTE: You must have ThinOS Activation devices license for OptiPlex 5400 All-in-One to enable VDI function.

  NOTE: If you do not connect the network cable, you can only connect to the Wi-Fi. ThinOS may not detect the network controller, which means ThinOS cannot connect to the Wyse Management Suite server. You must connect the network cable and reboot to recover the network controller to ensure ThinOS can connect to the Wyse Management Suite server.
- **Improvements over Latitude 3420**
  - Supports integrated microphone.
  - Supports Dell DA310 7-in-1 USB-C Multiport Adapter.
  - Supports DellWD19 docking station.
    - Do not hot plug monitors on Dell WD19 as a black screen may be displayed. You can hot plug the Dell WD19 docking station.
    - If you hot plug the Dell WD19 dock, display audio through the dock does not work. You must reboot with Dell WD19 connected to use the display audio, which works only with one monitor connected to Dell WD19.
  - Supports Type-C port display audio.

    NOTE: Latitude 3420 supports audio through one display only. If displays are connected using both HDMI and Type-C, the Type-C display audio takes priority.
- **Power adapter is required to complete operating system firmware, application packages, or BIOS firmware installation**— Operating system firmware, application packages, or BIOS firmware cannot be installed without power

adapter, and an error message **Skip upgrade since AC power is not connected or disk space is not enough** is displayed in event log .

- **Light theme for Modern mode** — The theme can be enabled in Wyse Management Suite policy by going to **Personalization** > **Experience Settings** > **Color scheme for Modern mode**.
- **Removed local ThinOS window icons from modern mode floatbar**— In the previous release, few ThinOS local windows have icons on the modern mode floatbar, like the System Information window. These icons are removed, and only VDI icons will be on the floatbar.

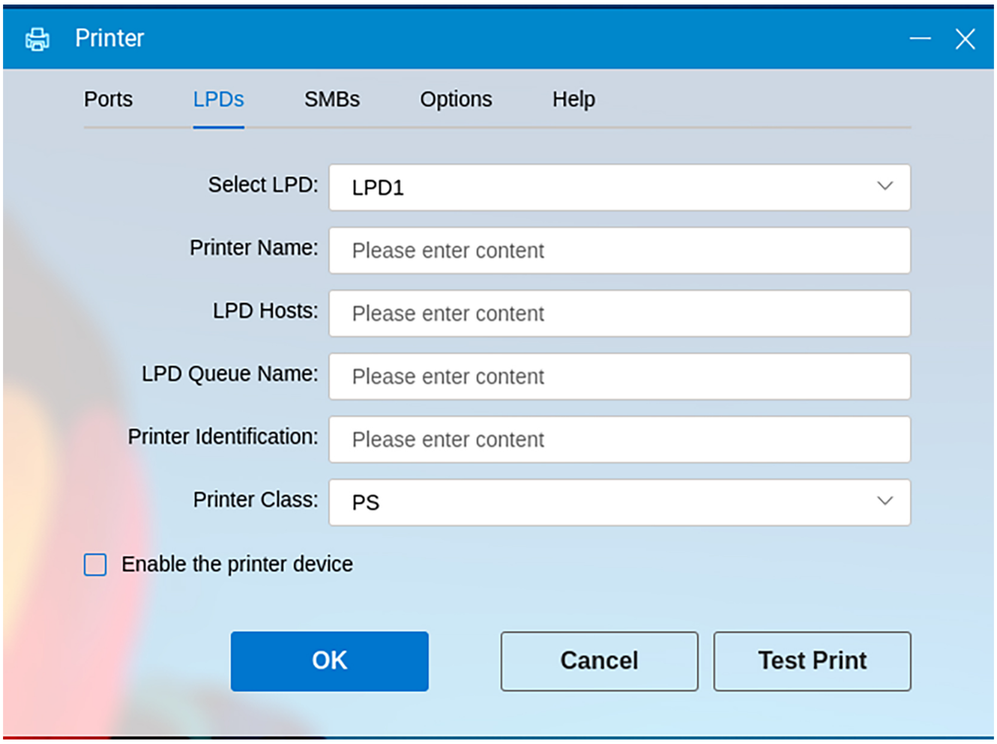
  NOTE: Only window icons are removed from the top of floatbar. Button icons at the bottom are not changed.
- Added transparency in classic mode
- Default desktop background Image is changed.
- **SNMPV3 is added and supported**— SNMPV3 in ThinOS requires a security level with both authentication and privacy. This setting can be configured in Wyse Management Suite policy by going to **Network Configuration** > **SNMPV3 Settings**. ThinOS supports MIB tree 1.3.6.1.2.1 but not 1.3.6.1.2.1.10, 1.3.6.1.2.1.4.20.1.5, and 1.3.6.1.2.1.4.21.1.10. ThinOS supports private MIB tree 1.3.6.1.4.1.714 as below:

  NOTE: ThinOS 2208 only supports Set and Get operations.

Table 113. MIB

Serial Number	1.3.6.1.4.1.714.1.2.6.2.1
Undefined yet	1.3.6.1.4.1.714.1.2.6.2.2
Undefined yet	1.3.6.1.4.1.714.1.2.6.2.3
Network speed	1.3.6.1.4.1.714.1.2.6.2.4
Network Gateway	1.3.6.1.4.1.714.1.2.6.2.5
DHCP setting (1 as enabled, 0 as disabled)	1.3.6.1.4.1.714.1.2.6.2.6
DNS setting (1 as static, 0 as dynamic)	1.3.6.1.4.1.714.1.2.6.2.7
DNS server	1.3.6.1.4.1.714.1.2.6.2.8

- **Updated the settings in System Preferences > Power and Sleep**— If the thin client does not support sleep mode, **Sleep** option is not displayed in the dropdown list and the default value is **Power off** with the timer **Disabled**.
- **Changed DNS SRV record to DNS/DHCP Discover**— The name **DNS SRV record** is renamed to **DNS/DHCP Discover** in **Central Configuration** of the client menu. There is no functional change.
- **Changed the order of options in LPDs**— In **Printer Setup** > **LPDs** of the client menu, the order of the options are changed.



Select LPD: LPD1

Printer Name: Please enter content

LPD Hosts: Please enter content

LPD Queue Name: Please enter content

Printer Identification: Please enter content

Printer Class: PS

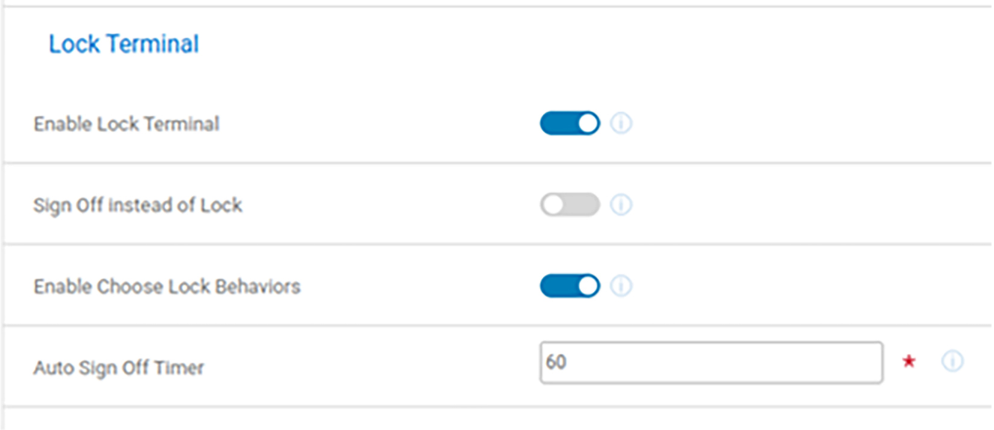
□ Enable the printer device

Figure 8. LPDs tab in Printer

- **Changed the audio device priority when manual override is enabled**— When manual override is enabled, audio device priority does not change. To give priority to an audio device, select the audio device from the dropdown list manually. If the audio device is already selected in the dropdown list, choose another audio device in the list and change it back to the first audio device.
- **Default Wyse Management Suite URLs added in drop-down list in the OOBE - Import Configuration page**— In the OOBE - Import Configuration page, a drop-down list is added. The following two Wyse Management Suite URLs are shown by default.

  us1.wysemanagementsuite.com

  eu1.wysemanagementsuite.com
- **Updated the password policy when exporting logs**— When exporting logs from **Troubleshooting**, the password must include upper and lower case letters, numbers, and one or more special characters in "!@#$%^&*-_". The minimum length of the password should be nine characters.
- **Lock Terminal enhancement**— A new group is created in Wyse Management Suite or Admin Policy Tool for Lock Terminal.



Enable Lock Terminal ●

Sign Off instead of Lock ○

Enable Choose Lock Behaviors ●

Auto Sign Off Timer 60 *

Figure 9. Lock Terminal in Wyse Management Suite

This group contains below parameters:

1. **Enable Lock Terminal**: This option enables the thin client to be locked. The default value of this parameter is **ON**. The previous name of this parameter was **Lock Terminal** under the group **Login Experience**.

ⓘ **NOTE:** If the lock terminal option is disabled from ThinOS policy, the local terminal command from Wyse Management Suite ignores this option and locks the thin client.

2. **Sign Off instead of Lock**: When web authentication or an anonymous user signs in, you can configure the thin client to sign off instead of lock. The default value of this parameter is **OFF**. The previous name of this parameter is **Sign Off Automatically when Lock Terminal** under group **Screen Saver Settings**

   ⓘ **NOTE:** If **Enable Lock Terminal** is **OFF**, this parameter is not shown and configured.

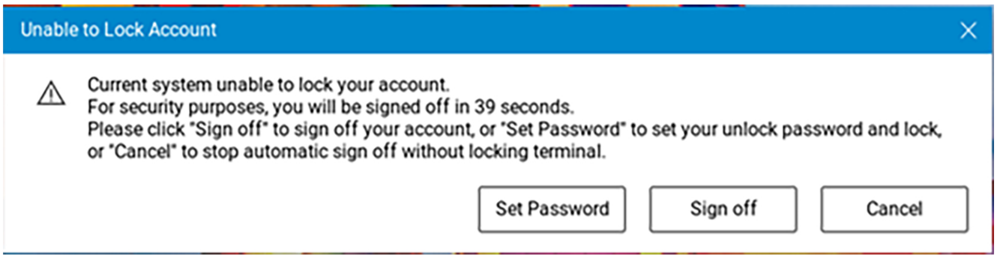
3. **Enable Choose Lock Behaviors**: When web authentication or an anonymous user signs in, you can configure the thin client to display a dialog box to set the unlock password, sign off, or cancel lock. The default value of this parameter is **ON**.

   ⓘ **NOTE:** If **Sign Off instead of Lock** is **ON**, this parameter is not shown and configured. This parameter does not take effect when no web authentication or anonymous login is detected.

4. **Auto Sign Off Timer**: You can set auto sign-off timer from 10 s to 600 s. The default value of this parameter is **60**.

   ⓘ **NOTE:** If **Enable Choose Lock Behaviors** is **OFF**, this parameter is not shown and configured.

- **Enable Lock Terminal**: If **Enable Lock Terminal** is **ON**, the **Lock Terminal** option is displayed and selected in ThinOS shutdown menu. If **Enable Lock Terminal** is **OFF**, the **Lock Terminal** option is disabled in the ThinOS shutdown menu. You cannot lock the terminal from ThinOS shutdown menu or using the ThinOS system shortcut Ctrl + Alt + Left/Right.
- **Lock Terminal on Web Authentication and Anonymous Logon user cases**: ThinOS supports None broker agent Logon and various Web Authentication scenarios in VDI Logon. After ThinOS 2208 release, Lock Terminal will be supported in the following user cases:
  - Broker is None
  - Login AVD broker
  - Horizon Workspace One Mode
  - Horizon Anonymous Login
  - Horizon Kiosk mode
  - Horizon Azure + UAG broker
  - Horizon OKTA + UAG broker
  - Citrix Storefront Anonymous Login
  - Citrix Azure AD broker
  - Citrix OTP broker
  - Citrix Cloud with Web authentication
- **New features of Lock Terminal in Web Authentication and None broker agent login**
  - After selecting **Lock Terminal** in ThinOS shutdown menu or using the ThinOS system shortcut Ctrl + Alt + Left/Right, the **Unable to Lock Account** window is displayed.



Unable to Lock Account

Current system unable to lock your account.
For security purposes, you will be signed off in 39 seconds.
Please click "Sign off" to sign off your account, or "Set Password" to set your unlock password and lock,
or "Cancel" to stop automatic sign off without locking terminal.

Figure 10. Unable to Lock Account window

  - Once the countdown is over, terminal signs off.
  - When the **Cancel** button is clicked, the **Lock Terminal** operation is cancelled.
  - After the **Set Password** button is clicked, the **Set Unlock Password** window is displayed. You can follow the password complexity requirements to set a one-time password, which can be used to unlock the terminal.

ⓘ **NOTE:** Instead of **Sign Off** if **Lock** is **ON**, the terminal signs off when selecting **Lock Terminal** option from ThinOS shutdown menu or using the ThinOS system shortcut Ctrl + Alt + Left/Right.

ⓘ **NOTE:** If **Enable Choose Lock Behaviors** is **OFF**, the **Lock Terminal** function is disabled. **Lock Terminal** is disabled in ThinOS shutdown menu. The ThinOS system shortcut Ctrl + Alt + Left/Right does not work either.

- **SMB printer credentials updated for VDI logon credentials and variables**
  - If there is an SMB printer configuration in Wyse Management Suite, then the Wyse Management Suite SMB printer configuration always has a higher priority than the local SMB printer configuration.
  - If you want to always pass the VDI logon credentials to the SMB credentials, use `$UN`, `$PW`, and `$DN` as the SMB printer username, password, and domain respectively on the Wyse Management Suite server or locally if there is no Wyse Management Suite configuration.

- If the SMB printer username, password, and domain fields are left empty on the Wyse Management Suite server or locally, after the VDI logon on the client, the VDI logon credentials do not pass to the SMB printer credentials.
- If you want to use the same SMB printer credentials for all client users, configure the SMB printer common credentials (non-variables) on the Wyse Management Suite server or locally if there is no Wyse Management Suite configuration.

  NOTE: After configuring $UN, $PW, and $DN as the SMB printer username, password, and domain on the Wyse Management Suite server on the client, the SMB printer credentials are empty before VDI logon on the client.

Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **DNS/DHCP Discover**—Change the option name from **DNS Discover** to **DNS/DHCP Discover** in **Services** > **WDA Settings**. The option can enable or disable ThinOS clients ability to discover Wyse Management Suite settings from both DNS and DHCP.
- **Force Discover**—Added a new option **Force Discover** in **Services** > **WDA Settings**. If the option is enabled, ThinOS client can discover Wyse Management Suite settings from DNS/DHCP and register the client even if it is already registered to Wyse Management Suite. Enable **DNS/DHCP Discover** for this option to take effect.
- **Color scheme for Modern mode**— Added a new option **Color scheme for Modern mode** in **Personalization** > **Experience Settings**. The **Light** theme is applied when **Light** option is selected.
- **Sleep Mode**— Added a new option **Sleep Mode** in **System Settings** > **Power Sleep Settings**. If disabled, the sleep function is disabled on the ThinOS client, and the sleep option is removed on all the ThinOS local windows. If you publish sleep policies from Wyse Management Suite on the ThinOS client in **System Preferences** > **Power and Sleep** the value is set as **Power off** and the **Timer** is set as **Disabled**.
- **Firmware Update Logic**— Added a new option **Firmware Update Logic** in **Firmware** > **OS Firmware Updates**. When **Any different firmware** is selected, the client upgrades or downgrades to another operating system version. When **New firmware only** is selected, the client upgrades to a newer operating system version and cannot downgrade to an older operating system version.
- **Deep Sleep Control for OptiPlex 3000 Thin Client**— Added a new option **Deep Sleep Control** in **BIOS** > **Dell OptiPlex 3000 Thin Client**. If you set the value to **Disabled**, you can wake the client on LAN from the power off status. If set to other values, you cannot wake the client on LAN from the power off status.
- **BIOS settings page for OptiPlex 5400 AIO**—Added a BIOS settings page to control the BIOS options for OptiPlex 5400 All-in-One.
- **Added Keyboard Error Detection, Fastboot, Extend BIOS POST time options**— Added new options **Fastboot** and **Extend BIOS POST time** in BIOS for all platforms and added **Keyboard Error Detection** in BIOS for non-laptop platforms.
- **SNMPV3 Settings**—Added **SNMPV3 Settings** in **Network Configuration**. Enable **SNMP Enable** and set validate settings to make the ThinOS client an SNMPV3 agent.
- **RDS Web Login**—Added a new option **RDS Web Login** in **Broker Settings** > **Microsoft Remote Desktop Settings**. The default value is disabled. If enabled, Remote Desktop Service authentication uses the web login method instead of NTLM.
- **Automatically connect to sessions**: Added a new input box **Automatically connect to sessions** in **Broker Settings** > **Azure Virtual Desktop Settings**. **Specify Connection Name** is displayed in **Connection Manager** or on the client desktop to connect automatically.

  NOTE: The name of the connection is case-sensitive. Use a semicolon to separate multiple connections to be launched automatically.
- **Hold key audio warnings countdown**— Added a new option **Hold key audio warnings countdown** in **Peripheral Management** > **Keyboard** > **Keyboard Settings**. An audio beep is played on the current playback device when the timeout value (in milliseconds) has been reached after long pressing a key on the keyboard. Supported values are 0 to 20000, where 0 means disabled.
- **Hold key audio warnings beep repeat time**— Added a new option **Hold key audio warnings beep repeat time** in **Peripheral Management** > **Keyboard** > **Keyboard Settings**. You can specify the interval in milliseconds when the repetitive beeps are played. The supported values are 0 to 5000, where 0 means no beep repetition.
- **Added Single Button Connect settings**— You must set the default username, password, or domain and then enable **Single Button Connect** under the policy **Login Experience**> **Login Settings**> **Default Credentials**. The client does not log in to the VDI Broker agent automatically, but the default username, password, or domain is populated. After clicking the login button, the client logs in to the VDI Broker agent. The four configurations below are hidden and do not take effect:
  - Disable Default User on Login Console
  - Disable Default password on Login Console
  - Disable Default Domain on Login Console
  - Clear User

- **Added Single Connection setting**—The **Single Connection** setting is added in **Session Settings** > **Global Session Settings** > **Advanced Settings** page. By default, the setting is disabled. If enabled, the client is limited to one active desktop. If you try to launch the second or more desktops, the event log displays an error message. If there is an auto connection list that contains multiple desktops, only one desktop is allowed to autoconnect. Logging off or disconnecting the active desktop and connecting another desktop is allowed, but you can only launch one desktop simultaneously. This setting is only applicable for desktop sessions and there is no restriction for published applications. When **Single Connection** is enabled or disabled from Admin Policy Tool or Wyse Management Suite policy, signing off from the Broker agent or restarting the client makes the setting take effect.
- **Added Only Show and Launch the OnDesktop Session Type setting**— **Only Show and Launch the OnDesktop Session Type** setting is added in **Session Settings** > **Global Session Settings** > **Display Settings** page. The setting enables the launch of **OnDesktop** defined session type in **Connection Manager** with **Classic** mode or on the menu bar with **Modern** mode. The setting is enabled by default. Here are a few scenarios:

Table 114. Expected behaviors of different configurations in Admin Policy Tool or Wyse Management Suite

Configuration in Admin Policy Tool or Wyse Management Suite	Expected behaviors
Only Show and Launch the OnDesktop Session Type=yes OnDesktop=All	Classic Mode: All resources list on ThinOS desktop and Connection Manager Modern Mode: All resources list on the menu bar. The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should be roamed to ThinOS.
Only Show and Launch the OnDesktop Session Type=yes OnDesktop=None	Classic Mode: No resources list on ThinOS desktop and Connection Manager Modern Mode: No resources list on the menu bar. Only the applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should not be roamed to ThinOS.
Only Show and Launch the OnDesktop Session Type=yes OnDesktop=Desktops Only	Classic Mode: Only desktops list on ThinOS desktop and Connection Manager Modern Mode: Only desktops list on the menu bar. The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the applications should not be roamed to ThinOS. If there is only one desktop, the desktop is auto launched when logging in to the Broker agent. You do not need to add the desktop to the auto connection list.
Only Show and Launch the OnDesktop Session Type=yes OnDesktop=Applications Only	Classic Mode: Only applications list on ThinOS desktop and Connection Manager Modern Mode: Only applications list on the menu bar. The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the Desktop should not be roamed to ThinOS. If user has only one application, it is auto launched when logging in to the Broker agent. You do not need to add the application to the auto connection list.
Only Show and Launch the OnDesktop Session Type=yes OnDesktop=Specific Applications/Desktops	Classic Mode: Only specified resources on the ThinOS desktop and Connection Manager Modern Mode: Only specified resources on the menu bar.

Table 114. Expected behaviors of different configurations in Admin Policy Tool or Wyse Management Suite (continued)

Configuration in Admin Policy Tool or Wyse Management Suite	Expected behaviors
	The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, session roaming is supported for specific applications or desktops only in ThinOS. If user only has one desktop or one application that is in the specific applications or desktops list, it is auto launched when logging in to the Broker agent. You do not need to add the desktop or application to the auto connection list.
Only Show and Launch the OnDesktop Session Type=no OnDesktop=All	Classic Mode: All resources list on the ThinOS desktop and Connection Manager Modern Mode: All resources list on the menu bar The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should be roamed to ThinOS.
Only Show and Launch the OnDesktop Session Type=no OnDesktop=None	Classic Mode: No resources list on the ThinOS desktop and all resources list on Connection Manager Modern Mode: All resources list on the menu bar The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should be roamed to ThinOS.
Only Show and Launch the OnDesktop Session Type=no OnDesktop=Desktops Only	Classic Mode: Only desktops list on the ThinOS desktop and all resources list on Connection Manager. Modern Mode: All resources list on the menu bar. The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should be roamed to ThinOS.
Only Show and Launch the OnDesktop Session Type=no On Desktop=Applications Only	Classic Mode: Only applications list on the ThinOS desktop and all resources list on Connection Manager Modern Mode: All resources list on the menu bar. The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should be roamed to ThinOS.
Only Show and Launch the OnDesktop Session Type=no OnDesktop=Specific Applications/Desktops	Classic Mode: Specified resources on ThinOS desktop and all resources list on Connection Manager. Modern Mode: All resources list on the menu bar. The applications or desktops on Auto Connect List can be auto launched. When connections are roamed from a device that did not have the icon restrictions, the connection to the desktop and applications should be roamed to ThinOS.

- **Application Package updates category**—Click **Browse** to upload application packages. All application packages are in the same drop-down list in 2205 and earlier versions. From ThinOS 2208, categories are added to improve the application packages visibility. All application packages go to the following defined categories:
  1. Citrix
     - Citrix Workspace App

2. VMware
    - VMware Horizon
3. Microsoft
    - Microsoft AVD
4. Zoom
    - Zoom Citrix
    - Zoom Horizon
5. Cisco
    - Cisco Jabber
    - Cisco Webex Meetings VDI
    - Cisco Webex VDI
6. Dell
    - Security Addon
    - Hotfix
7. Third Party
    - Teradici PCoIP
    - Imprivata PIE
    - Jabra
    - EPOS Connect
    - HID Fingerprint Reader
    - Identity Automation QwickAccess
8. Other
    - Application packages that are not predefined in ThinOS 2208 yet

    For each category, there is one switch option **Install/Uninstall** on the left and one drop-down list **Not Selected** by default on the right. Click the drop-down list, and the uploaded versions of the application package is displayed. You can select only one version in the list and the drop-down list title changes to the package name and repository.

    NOTE: For **Other** category, you can select multiple application packages and versions, as the application packages are not predefined yet. Once you have the application packages in **Other** category, it is recommended you upgrade the Wyse Management Suite configUI. The new Wyse Management Suite configUI sets the application packages in the new category.

    If the switch option is set to **Install**, the selected application package version in the drop-down list is published to the ThinOS client to install.

    If the switch option is set to **Uninstall**, the application package drop-down list is disabled, and the application package is uninstalled from the ThinOS client.

- **Added Edit Screen Saver in System Preferences**— The option can be displayed by going to **Admin Policy Tool** > **Privacy & Security** > **Account Privileges**, selecting **Customize** from privilege level drop down list, and enabling **System Preferences**. If **System Preferences** is enabled,**Edit Screen Saver** is enabled by default. If **Edit Screen Saver** is disabled, you cannot change and configure the screen saver settings from the client menu **System Preferences**.
- **Added 5900, by default, to the VNC service VNCD TCP Port text field**—Go to **Service** > **VNC Service**, and **5900** is displayed in the VNCD TCP Port text field. From ThinOS 2208, the default value is displayed as 5900.
- **Data validation on Proxy Server URL**— Go to **Network Configuration** > **Proxy Settings**, add a proxy row. The Proxy Server URL text field has data validation and cannot be saved if you cannot pass data validation.
- **Lock Terminal**— **Lock Terminal** group has been added in **Login Experience** > **Login Settings**. There are four settings in this group.
    - **Enable Lock Terminal**: This setting was in **Login Experience** group, now it is moved to **Lock Terminal** group.
    - **Sign off instead of Lock**: This setting was called **Sign Off Automatically when Lock Terminal** in **Personalization** > **Screen Saver** page. Now it is moved to **Lock Terminal** group.
    - **Enable Choose Lock Behaviors**: This is a new setting. When WebAuth or an anonymous user signs on, you can configure to display a dialog box to set the unlock password, sign off directly, or cancel the lock.
    - **Auto Sign Off Timer** – This is a new setting. You can set the auto sign-off timer from 10 s to 600 s.
- **DHCP option 42 enable**— Added a new option **DHCP option 42 enable** in **Network Configuration** > **DHCP Settings**. Enable this option and the time server that is defined in DHCP server option 42 takes effect. After rebooting, the event log displays **Use DHCP NTP Servers: xxxxxx**, **Update time: xxxxxx**, where the date and time syncs with the time server.

    NOTE: When this option is enabled, the time server that is defined in DHCP server option 42 takes priority.

- **Changed the default value from enabled to disabled for the Map Disks**— In **Session Settings**>**Global Session Settings** > **Local Resources and USB Redirection** > **Map Disks**, the default value has been changed from enabled to disabled.

  NOTE: If you do not change Map Disks default value on the last ConfigUI, you must enable the **Map Disks** option again after upgrading to the ThinOS 2208 ConfigUI.

Tested environments matrix

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

Table 115. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.8 181
Configuration UI package for Wyse Management Suite	1.9.72
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 116. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2022	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5)	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2203LTSR	Tested	Tested	Tested	Tested	Tested

Table 117. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Tested	Tested	Tested—Only basic connection is tested on Ubuntu 20.04

Table 118. Test environment – VMware Horizon Cloud

Horizon Cloud	Windows 10	Windows Server 2016
Build Version: 19432376	Horizon Agent Installer - 21.3.0.19265453	Horizon Agent Installer - 21.3.0.19265453

Table 119. Test environment—Microsoft RDP

Microsoft RDP	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
Remote Desktop Services 2016	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2019	Not tested	Tested	Not tested	Not tested	Not tested	Tested	Tested

Table 120. Test environment—AVD

Azure Virtual Desktop	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
2019 (MS-Prod)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested
2020 (ARMv2)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested

Table 121. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	2.9.500	2.9.500	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				
	Windows server 2022				

Table 122. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 123. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	14.1.1.306904.1	14.1.1.306904	14.1.1.306904
	Windows server 2016			
	Windows server 2019			
	Windows server 2022			

Table 124. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12	Windows 10	14.1.1.306904.1	14.1.1.306904	14.1.1.306904
	Windows server 2016	14.1.1.306904.1	14.1.1.306904	14.1.1.306904
	Windows server 2019	14.1.1.306904.1	14.1.1.306904	14.1.1.306904

Table 124. Tested environment—JVDI (continued)

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2				

Table 125. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	5.10.6.21295.2	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 126. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106 VMware Horizon View 7.13.2	Windows 10	5.10.6.21295.2	5.10.6(21295)
	Windows server 2016		
	Windows server 2019		

Table 127. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	42.6.0.22645.1	42.6.0.22645
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 128. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10	42.6.0.22645.1	42.6.0.22645
	Windows server 2016		
	Windows server 2019		

Table 129. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	42.8.2.8.1 (special release based on 42.6)	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.8 to 42.xxx.
	Windows server 2016		
	Windows server 2019		

Table 129. Tested environment—Cisco Webex Meetings (continued)

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
	Windows server 2022		

Table 130. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106	Windows 10	42.2.6.11.3	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6. Webex Meeting does not work well with Horizon 2111. This is a Cisco limitation.
	Windows server 2016		
	Windows server 2019		

Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

NOTE: The supported peripherals are not limited to the peripherals devices listed in this section.

Table 131. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

Product Category	Peripherals	3040	5070	5470 AIO	5470
Audio Devices	Dell Pro Stereo Headset – UC150 – Skype for Business	Supported	Supported	Not Available	Supported
	Dell Pro Stereo Headset - Skype for Business - UC350	Supported	Supported	Supported	Supported
	Dell Professional Sound Bar (AE515M)	Supported	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Not Available	Supported	Not Available	Not Available
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Not Available	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Not Available	Supported	Supported

Table 131. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	DellUSB Wired Optical Mouse - MS116	Supported	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Not Available	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Not Available	Supported	Not Available	Supported

Table 131. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI - DBQAUBC064 - DBQAUBC064	Not Available	Supported	Not Available	Not Available
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Not Available	Supported	Not Available	Not Available
	Trendnet USB to Serial Converter RS-232	Not Available	Supported	Supported	Supported
	Dell Adapter - HDMI to DVI - DAUARBN004 - DAUARBN004	Not Available	Not Available	Not Available	Supported
	Dell Adapter - HDMI to VGA - DAUBNBC084 - DAUBNBC084	Not Available	Not Available	Not Available	Supported
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232	Not Available	Not Available	Supported	Supported
Displays	E1916H	Supported	Supported	Supported	Not Available
	E2016H	Supported	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported	Supported
	E2216H	Not Available	Supported	Supported	Supported
	E2216Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2218HN	Supported	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported	Supported
	E2318H	Supported	Supported	Supported	Supported
	E2318HN	Not Available	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported	Supported
	E2420HS	Not Available	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported	Supported

Table 131. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	E2720HS	Not Available	Supported	Supported	Supported
	P2016	Not Available	Supported	Not Available	Not Available
	P1917S	Supported	Supported	Not Available	Not Available
	P2017H	Supported	Not Available	Not Available	Not Available
	P2018H	Not Available	Not Available	Not Available	Supported
	P2217	Supported	Supported	Not Available	Not Available
	P2217H	Supported	Supported	Not Available	Not Available
	P2219H	Supported	Supported	Not Available	Supported
	P2219HC	Supported	Supported	Not Available	Supported
	P2317H	Supported	Supported	Not Available	Not Available
	P2319H	Not Available	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Supported	Not Available
	P2417H	Supported	Supported	Not Available	Not Available
	P2418D	Supported	Not Available	Not Available	Not Available
	P2418HT	Supported	Supported	Supported	Not Available
	P2418HZ	Supported	Supported	Not Available	Not Available
	P2419H	Supported	Supported	Supported	Supported
	P2419HC	Supported	Supported	Not Available	Supported
	P2421D	Supported	Supported	Not Available	Supported
	P2421DC	Not Available	Supported	Not Available	Supported
	P2719H	Supported	Supported	Supported	Supported
	P2719HC	Supported	Supported	Not Available	Supported
	P2720D	Supported	Supported	Not Available	Supported
	P2720DC	Not Available	Supported	Not Available	Supported
	P3418HW	Supported	Supported	Supported	Not Available
	P4317Q	Not Available	Supported	Supported	Not Available
	MR2416	Supported	Supported	Not Available	Not Available
	U2415	Supported	Supported	Supported	Not Available
	U2419H	Supported	Supported	Supported	Supported
	U2419HC	Supported	Supported	Not Available	Supported
	U2518D	Supported	Supported	Supported	Not Available
	U2520D	Supported	Supported	Supported	Supported
	U2718Q (4K)	Supported	Supported	Supported	Supported
	U2719D	Supported	Supported	Supported	Supported
	U2719DC	Supported	Supported	Not Available	Supported
	U2720Q	Supported	Supported	Supported	Supported
	U2721DE	Not Available	Supported	Supported	Supported

Table 131. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	U2421HE	Not Available	Not Available	Supported	Supported
	U4320Q	Not Available	Supported	Supported	Supported
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Not Available	Supported
Storage	Dell Portable SSD, USB-C 250GB	Not Available	Supported	Not Available	Supported
	Dell External Tray Load ODD (DVD Writer)	Not Available	Supported	Not Available	Supported
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported	Supported
	Sun microsystem SCR 3311	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Not Available	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Not Available	Supported	Not Available	Supported
Printers	Dell Color Multifunction Printer - E525w	Supported	Not Available	Not Available	Not Available
	Dell Color Printer- C2660dn	Supported	Supported	Not Available	Not Available
	Dell Multifunction Printer - E515dn	Supported	Not Available	Not Available	Not Available

Supported ecosystem peripherals for OptiPlex 3000 Thin Client

ⓘ **NOTE:** The supported peripherals are not limited to the peripherals devices listed in this section.

Table 132. Supported ecosystem peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio Devices	Dell Slim Soundbar - Ariana - SB521A

Table 132. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell Pro Stereo Headset - Cortez - WH3022.
	Logitech BRIO 4K Ultra HD Webcam - 960-001105 - 960-001105
	Logitech C525 HD Webcam - 960-000715 - 960-000715
	Logitech C930e HD Webcam - 960-000971 - 960-000971
	Dell Pro Stereo Soundbar - AE515M - AE515M - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - AC511M - AC511M - Potential M
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P
Input Devices	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
Displays	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell 24 Monitor - P2422H - P2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell 27 Monitor - P2722H - P2722H
	Dell 22 Monitor - P2222H - P2222H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell 20 Monitor E2020H - E2020H
	Dell 27 Monitor - P2720D - P2720D
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell 24 Monitor E2420HS - E2420HS

Table 132. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell 27 Monitor - P2720D - P2720DC
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 27 Monitor E2720HS - E2720H
	Dell 27 Monitor E2720H - E2720HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 19 Monitor E1920H - E1920H
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell 24 Monitor E2420H - E2420H
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316

Supported ecosystem peripherals for Latitude 3420

Table 133. Supported ecosystem peripherals for Latitude 3420

Product Category	Peripherals
Displays	Dell 24 Monitor E2420HS - E2420HS
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W ⓘ **NOTE:** Bluetooth connection is not supported.
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
Audio Devices	Dell Pro Stereo Headset - UC150 - UC150 - Lemmy - UC150
Docking Stations	Dell 7-in-1 USB-C Multiport Adapter - DA310
	Dell Docking Station WD19

Supported ecosystem peripherals for OptiPlex 5400 All-in-One

Table 134. Supported ecosystem peripherals for OptiPlex 5400 All-in-One

Product Category	Peripherals
Displays	Dell 24 Monitor - P2421D
	Dell UltraSharp 24 Monitor - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022

Other supported peripherals

Table 135. Other supported peripherals

Product Category	Peripherals
Audio Devices	Dell Pro Stereo Headset UC350
	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth (link 360)
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Support USB only, not support Bluetooth)
	Plantronics Blackwire 5220 Series
	Plantronics AB J7 PLT
	Plantronics Blackwire C5210
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Calisto P820-M
	Plantronics Voyager 6200 UC
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER SC 660 USB ML
	SENNHEISER USB SC230
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SP 10 ML Speakerphone for Lync
	Sennheiser SDW 5 BS-EU
	Logitech S-150
	POLYCOM Deskphone CX300
	PHILIPS - analog
	Logitech h150 - analog
	LFH3610/00 SPEECH MIKE PREMIUM (only support redirect)
	Nuance PowerMic II (Recommend redirecting whole device)
	Olympus RecMic DR-2200 (Recommend redirecting whole device)
Input Devices	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123
	Dell Keyboard KB216p
	Dell wireless Keyboard/mouse KM632
	Dell wireless Keyboard/mouse KM714

Table 135. Other supported peripherals (continued)

Product Category	Peripherals
	Dell Keyboard KB212-B
	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E610 0, Bluetooth
	RS232/Serial-USB adapters using FTDI or PROLIFIC chipsets
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	Dell U2718Q (3840x2160)
	Dell U2719D(1920x1080)
	Dell P2719H (1920*1080)
	Dell P2715Q(3840x2160)
	Dell S2719HS (1920x1080)
	Dell S2817Q(3840x2160)
	Dell U2713HM (2560x1440)
	Dell U2718Q(3840x2160)
	Dell P2418HZ
	Dell U3219Q (3840x2160) (Does not support Type C to HDMI convertor)
	Dell U3419W (3440 x1440)
	Dell P2415Q(3840X2160)
	ELO ET2202L-2UWA-0-BL-G
Camera	Logitech C920 HD Pro Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Logitech C930e HD Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C910 HD Pro Webcam
	Logitech C925e Webcam
	Poly EagleEye Mini webcam
	Logitech BRIO 4K Webcam
	Jabra PanaCast 4K Webcam
Storage	SanDisk cruzer 8 GB
	SanDisk cruzer 16G
	SanDisk USB 3.1 and Type-C 16 GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32 GB

Table 135. Other supported peripherals (continued)

Product Category	Peripherals
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Dell External Tray Load ODD (Agate) (DVD Writer)
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	Dell keyboard KB813 (Smartcard reader)
	Dell Keyboard SK-3205 (Smartcard reader)
	IDBridge CT31 PIV
	Gemalto IDBridge CT710
	GemPC Twin
Proximity card readers	RFIDeas RDR-6082AKU
	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80
	Imprivata HDW-IMP-82
	Imprivata HDW-IMP-82-BLE
	OMNIKEY 5025CL
	OMNIKEY 5326 DFR
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM
	OMNIKEY 5325 CL
	KSI-1700-SX Keyboard
Fingerprint readers	KSI-1700-SX Keyboard

Table 135. Other supported peripherals (continued)

Product Category	Peripherals
	Imprivata HDW-IMP-1C
	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader
Printers	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer
	Dell B2360d Laser Printer
	HP M403D
	Brother DCP-7190DW
	Dell B2360dn Laser Printer
	Lexmark X864de
	HP LaserJet P2055d
	HP Color LaserJet CM1312MFP
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR (BLEdongle)
Teradici remote cards	Teradic host card 2220
	Teradic host card 2240
Others	Intuos Pro Wacom
	Wacom One

Supported smart cards

Table 136. Supported smart cards

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	G&D SCE 3.2
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Giesecke and Devrient SmartCafe Expert 7.0 (T=0)

Table 136. Supported smart cards (continued)

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840
ID Prime MD v 4.0.2 (Gemalto 840)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K
ID Prime MD v 4.1.3 (Gemalto 3811)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940
Etoken Java (aladdin)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.0 T=0/1 0V300
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_6.1.6	cv act sc/interface CSP	Giesecke & Devrient StarCos 3.2
N/A (Buypass BelDu)	Net iD 6.8.3.21, 2.0.48	Net iD - CSP	BelDu 6.0.4
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.3.21, 2.0.48	Net iD - CSP	IDPrime SIS 4.0.2
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)

Fixed issues

Table 137. Fixed issues

Issue ID	Description
DTOS-7861	Azure Directory account locks after entering a single invalid password in Remote Desktop Service—CIPS-25858
DTOS-8048	Bluetooth devices do not connect on ThinOS 9.1.1—CIPS-26094
DTOS-8713	After upgrading to WTOS 9.1.5, the Belkin KVM switch does not work—CIPS-26231 and CIPS-26334
DTOS-8826	Unable to launch Desktop using Horizon UAG on ThinOS 9.1.6108—CIPS-26373-
DTOS-8980	Touch fails on ThinOS 9 with eGalaxTouch P80H84—CIPS-24558
DTOS-9064	Unable to set multiple addresses for direct RDP sessions—CIPS-26456
DTOS-9234	Wyse 3040 locks after tapping in or off five to six Imprivata sessions on ThinOS 9.1.90685—CIPS-26533
DTOS-9238	SSID Reporting in Wyse Management Suite does not work—CIPS-26312
DTOS-9447	Remote Desktop Service connection does not work when **Logon On To** has been configured in Active Directory—CIPS-26643
DTOS-9505	Connection to Citrix Desktop does not work when using keywords—CIPS-26584
DTOS-9506	Users have to double-click OK to validate the password change in WTOS 9.1 Citrix—CIPS-26650
DTOS-9542	CAPS, NUM, and SCROLL lights of Bloomberg keyboards do not switch off or on—CIPS-26700
DTOS-9572	Fingerprint reader fails to authenticate and enumerate when connected before booting—CIPS-26710
DTOS-9646	3D Connexion SpaceMouse Pro that is connected to OptiPlex 3000 does not work when connected before booting—CIPS-26479
DTOS-9671	CIPS-26704 | CPU 0 is used when using Imprivata/Citrix
DTOS-9672	Password Reset Prompt Issue—CIPS-26804
DTOS-9693	Script Tell Signature Tool 1550 does not work consistently in Citrix sessions—CIPS-26790
DTOS-9706	Imprivata PIE session window closes sometimes on ThinOS 9.1.6108—CIPS-26652
DTOS-9742	Citrix session keyboard sync issues in ThinOS 9.1.6108—CIPS-26875
DTOS-9878	Wyse 5070 device cannot hide domain name field, or domain name cannot be entered automatically on Wyse Management Suite WTOS9.1.6108—CIPS-26764
DTOS-9892	Bloomberg keyboard does not display the first character that is typed after booting—CIPS-26963
DTOS-9916	EAP authentication does not work after firmware update to ThinOS 9.1.6108—CIPS-26978
DTOS-9918	New user cannot reset password on first attempt while completing RSA Security initial setup—CIPS-26835
DTOS-9930	Both desktop and applications are opening when roaming between thin and fat clients—CIPS-26828
DTOS-9938	ThinOs 2205 connection drops when bandwidth usage is high—CIPS-27036
DTOS-10162	AWS login error **Create Socket failed** is displayed—CIPS-26965
DTOS-10189	Azure SAML Authentication error—CIPS-26807
DTOS-10211	EULA acceptance after every reset of the device—CIPS-27159

Table 137. Fixed issues (continued)

Issue ID	Description
DTOS-10268	Remote shadowing devices take 10 minutes to get an error when wrong VNC password is entered—CIPS-26898
DTOS-10335	After updating to ThinOS 2205, RDWEB password cannot be changed—CIPS-27202
DTOS-10336	Unable to use screen saver if turn off display is disabled—CIPS-27229
DTOS-10337	Direct External Connection to the NetScaler/ADC double authentication—CIPS-25673
DTOS-10385	In Wyse 5070 devices with ThinOS 9.3.1129, **Enable Auto Log Off** does not work when Inactive Timeout value is not 0. This issue is not there in 9.1.6108—CIPS-27132
DTOS-10597	**Shut Down Device After Log off** does not work when **Inactive Timeout** is not set to the default value—CIPS-27287
DTOS-10624	Cannot log in after logging off or disconnecting from session when using Imprivata PIE and Citrix—CIPS-26704
DTOS-11007	Root partition decryption failure on OptiPlex 3000— CIPS-26863
DTOS-11008	RSA token does not work after upgrading from ThinOS 9.1.3129—CIPS-27350
DTOS-11148	Float-bar position changes after VDI login screen is displayed—CIPS-27417
DTOS-11181	Dot 1x automatically changes to MAC-based authentication protocol on ThinOS 2205—CIPS-27557
DTOS-11198	Added option to **Edit Screen Saver** with Custom privilege level
DTOS-11344	Garbled characters in Microsoft Access when using RDP—CIPS-27569
DTOS-11350	Idle Session Timeout does not work in ThinOS 2205—CIPS-27623
DTOS-11450	Serial to USB redirection issues with Horizon VMware using Blast session—CIPS-27561
DTOS-11503	Black spot on top of the Epic application on ThinOS 2205—CIPS-27500
DTOS-11540	WTOS-9 KVM Avocent SVKM120-202 does not work with ThinOS—CIPS-27602
DTOS-11653	VDI disconnects on ThinOS 9.x due to Module.ini not being updated properly—CIPS-27788
DTOS-11666	In ThinOS 9.3.1129, the float bar setting is not sticking—CIPS-27759
DTOS-11732	In ThinOS 2205, the internal audio is saved as default when no headset is connected and manual overwrite is set in a group—CIPS-27660
DTOS-11743	Enable auto logoff feature with Citrix and Imprivata does not work after firmware update to ThinOS 2205—CIPS-27761
DTOS-11747	Reconnect feature stops working after firmware update—CIPS-27711
DTOS-11884	**UI restart** message is displayed when connected to a Cisco ISE 802.1x enabled network—CIPS-26306
DTOS-11913	ThinOS 2205 uses HD Audio-1 as default if it comes into a group where manual overwrite is selected and headset is connected later on OptiPlex 5070 devices with ThinOS 9.3.1129—CIPS-27813
DTOS-11927	Disable print screen setting does not work with ThinOS 2205—CIPS-27894
DTOS-11947	VMware Blast VDI Configuration Editor does not work as expected—CIPS-27811
DTOS-12018	Unable to move float bar to the right side of screen—CIPS-27988
DTOS-11585	Jabra direct implementation does not work in ThinOS 2205—CIPS-27427
DTOS-11220	Special characters (§ € ß ü Ü ö Ö ä Ä) do not work when used in passwords with RDS connection Broker agent—CIPS-27474
DTOS-11833	PFX with special characters fails to import in ThinOS 2205, specifically $ and #—CIPS-27852

Known issues

Table 138. Known issues

Issue ID	Description	Workaround
DTOS-10869	Dell Latitude 3420 cannot support 4K resolution at 60 Hz.	There is no workaround in this release. This is a hardware limitation.
DTOS-10932	The second screen connected to Dell OptiPlex 5400 All-in-One with i3 processor using an HDMI port displays a blank screen.	Use a monitor with 4K resolution at 30 Hz.
DTOS-10282	SD card does not work in Dell OptiPlex 5400 All-in-One.	There is no workaround in this release.
DTOS-10296	Poly EagleEye Mini webcam does not work with some resolutions.	Disable Optimize for CPU, set resolution to 1280x720 or 1920x1080, and click OK.
DTOS-11816	Global Connection Setting screen is displayed behind the devices screen.	Close the Citrix Devices window.
DTOS-11792	The icon of WebAuth is in white color and cannot be seen properly in Light mode.	This is a user interface issue and does not impact functioning.
DTOS-11019	In Span mode, when APT is launched, a portion of the APT window flickers in the secondary monitor.	This is a user interface issue and does not impact functioning.
DTOS-9644	When the same build is uploaded for the second time from Admin Policy Tool, a successful message is displayed.	This is a user interface issue and does not impact functioning.
DTOS-11988	Error message update is required when logging in using an invalid AWS registration code.	Correct the registration code.
DTOS-12112	An error message **Package not installed** is not displayed when launching Citrix Broker agent without Citrix Workspace app installed.	Ensure that Citrix Workspace app package is installed.
DTOS-11893	The mouse focus is not left in the AVD web login interface.	Wait for sometime after the AVD Web login interface is displayed.
DTOS-12011	Enabling **Single Connection** option launches a second RDP session or more desktop sessions.	There is no issue if the second RDP session is added from Wyse Management Suite.
DTOS-11983	After disconnecting the VDI session with fast disconnect key, no event log is observed and the online audio plays in the background.	This does not impact functioning. Wait for the audio to stop and relaunch a new session.
DTOS-10962	After dynamic adjustment rotation, the blast session only shows on the main display and not on both the displays.	Close and relaunch the blast session.
DTOS-11075	PCoIP VDI session is not displayed properly when clicking the maximize button 3–4 times on the top, right side of the window.	Restore or maximize again, and the PCoIP session displays properly.
DTOS-11500	Black patterns are displayed when sharing YouTube videos in a Microsoft Teams video call.	Do not share YouTube videos with BCR enabled in a Microsoft Teams video call.
DTOS-11737	Connection Manager maximizes when default settings are minimized in APT.	There is no workaround in this release.
DTOS-11915	Pressing the Tab key causes the Scan, IPv4 Config, or IPv6 Config buttons to display incorrectly.	Click the buttons using mouse.
DTOS-10221	No space is given for system tools import certificate window.	This is a user interface issue and does not impact functioning.
DTOS-11415	In the login window **Username & Username field box**, words do not change when selecting other languages like Deutsch, Italiano, or Japanese.	Log in and log off, the username field refreshes to the correct language.

Table 138. Known issues (continued)

Issue ID	Description	Workaround
DTOS-9650	Cannot sign on Broker agent when plugging in two same e-Token 5100 smartcards.	Do not use the same smartcard model with same smartcard type simultaneously.
DTOS-10125	After disconnecting the Wi-Fi, the status is shown as connected.	Wait for one minute, the status refreshes.
DTOS-10605	User Interface padding issue on the scan button in Bluetooth section	This is a user interface issue and does not impact functioning.
DTOS-11072	**Login Expire Time** text field accepts string values without displaying any validation criteria alert.	This is an input validation issue and does not impact functioning.
DTOS-11877	After clicking view certificate, the network setup window closes.	Reopen the network setup window.
DTOS-306	Mouse cursor information dialog box is not displayed on ThinOS 9.0.	Use the nondefault description of the Citrix session.
DTOS-11940	Yellow color border line is displayed in central configuration on ThinOS 9.3.2079 on OptiPlex 5400 All-in-One.	This is a user interface issue and does not impact functioning.
DTOS-11127	USB Disk information is displayed in Printer Name and Printer Identification.	Reconfigure the printer name and identification.
DTOS-11891	There are Zoom error messages in event log after resetting to factory default settings.	Reboot the terminal again.
DTOS-10501	Only one display audio option is shown after plugging in two monitors through HDMI and Type-C port on Latitude 3420.	There is no workaround in this release.
DTOS-10219	The mouse cursor stops responding after turning on restarting Dell OptiPlex 5400 All-in-One.	There is no workaround in this release.
DTOS-11052	After plugging out the analog headset, the integrated microphone on Latitude 3420 does not work for several seconds.	There is no workaround in this release.
DTOS-10834	Display audio through Dell WD19 dock does not work.	There is no workaround in this release.
DTOS-10529	On Dell U4323Q display, the HDMI or DisplayPort audio does not work, after replugging the Type-C cable.	After hot plug, restart the client.
DTOS-10438	Multiple audio devices do not work after signing off and signing in through the Broker agent in Citrix session even after updating the Citrix INI settings in APT.	Do not use more than two headsets if you have enabled multiple audio devices.
DTOS-7403	The supported Frames per Second (FPS) for HDX webcam is inoperative on ThinOS.	There is no workaround in this release.
DTOS-10711	Only four audio devices are displayed in Windows sound settings inside VDI of 2203 Broker agent when AudioRedirectionV4 is enabled in Thin Client.	Do not use more than two headsets if you have enabled multiple audio devices.

7

Citrix Workspace App 2205, Webex Meetings VDI 42.8 (special release based on 42.6), Webex VDI 42.4, Zoom 5.10.2, and Imprivata 7.8 packages for ThinOS 2205

Release summary

Patch or add-on releases are created to support the existing hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on shipping hardware platforms.

Version

Citrix_Workspace_App_22.5.0.16.3.pkg

Cisco_Webex_Meetings_VDI_42.8.2.8.1.pkg

Cisco_Webex_VDI_42.4.1.22585.1.pkg (formerly Cisco Webex Teams)

Zoom_Citrix_5.10.2.21113.7.pkg

Zoom_Horizon_5.10.2.21113.8.pkg

Imprivata_PIE_7.8.000.0008.1161.pkg

Release date

July 2022

Supported platforms

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- OptiPlex 3000 Thin Client
- Latitude 3420 with ThinOS

Important notes

- Supported hardware platforms must have at least CPU with 4 cores to use the virtual background feature in Webex Meetings VDI.
- Upgrade the ThinOS firmware to ThinOS 2205 before you install the application packages.
- Cisco Webex Meetings VDI, Cisco Webex VDI, and Zoom are qualified for Citrix VDI on ThinOS 2205 (9.3.1129) with Citrix Workspace app package 22.5.0.16.3.
- Cisco Webex Meetings VDI, Cisco Webex VDI, and Zoom are qualified for VMware Blast VDI on ThinOS 2205 (9.3.1129) with VMware Horizon package 2203.8.5.0.19586897.4.

Installing the application package

Download the application packages

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device.
3. Select the product from the searched results to load the product page.
4. On the product support page, click **Drivers & downloads**.
5. Select the operating system as **ThinOS**.
6. Locate the application packages that you require.
7. Download each application package file.

Install the application package using Wyse Management Suite

Prerequisites

- Upgrade the ThinOS firmware to ThinOS 2205 before you install the application packages.
- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.

  ⓘ **NOTE:** If you have an existing group with a valid group token, you can register the thin client to the same group.
- Ensure you have downloaded the application packages. See, Download the application package.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The Configuration Control | ThinOS window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.

   ⓘ **NOTE:** If you cannot locate the **Application Package Updates** option under the **Standard** tab, use the **Advanced** tab.
5. Click **Browse** and select the ThinOS 9.x application package to upload.
6. From the **Select the ThinOS Application(s) to deploy** drop-down menu, select the uploaded application package.
7. Click **Save & Publish**.
   The thin client downloads the package to install and restarts. The package version is upgraded.

Compatibility

Application package information

- Supported ThinOS application packages—The following ThinOS packages are qualified by Dell Technologies.
  - Citrix_Workspace_App_22.5.0.16.3.pkg
  - Cisco_Webex_Meetings_VDI_42.8.2.8.1.pkg
  - Cisco_Webex_VDI_42.4.1.22585.1.pkg (formerly Cisco Webex Teams)
  - Zoom_Citrix_5.10.2.21113.7.pkg
  - Zoom_Horizon_5.10.2.21113.8.pkg
  - Imprivata_PIE_7.8.000.0008.1161.pkg
- Supported Firmware—ThinOS 2205 (9.3.1129).

NOTE: For information about other packages, see ThinOS application package details in the **ThinOS 2205 Release Notes**.

Previous versions

- Citrix_Workspace_App_22.3.0.24.6.pkg
- Cisco_Webex_Meetings_VDI_42.2.8.5.1.pkg
- Cisco_Webex_VDI_41.12.0.20899.3.pkg (formerly Cisco Webex Teams)
- Zoom_Citrix_5.9.6.20931.7.pkg
- Zoom_Horizon_5.9.6.20931.7.pkg
- Imprivata_PIE_7.7.000.0007.1143
- Imprivata_PIE_7.5.000.0003.1144

Citrix Workspace app feature matrix

Table 139. Citrix Workspace app feature matrix

Feature		ThinOS 2205	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Limited support	VDA2203 LTSR desktop session randomly gets disconnected during launch or during daily use. For more information, see the limitations of Webcam redirection feature.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Limited Support	Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. The feature only works on mobile thin clients, such as 5470 and 3420 mobile thin clients from ThinOS 2205 with CWA2205. This is a Citrix binary limitation. The users who use VDA2203 VDI desktop with HDX webcam in 32-bit applications will have session disconnection issues. The issue is also reproduced in CWA 2205 Linux binary [CVADHELP-20223]. ThinOS 2205 does not support webcam redirection with 64-bit applications. For further details, refer to the Dell Wyse ThinOS Administrator's Guide at www.dell.com/support. .
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco Webex Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebexTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 2205

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
			Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (For example, CAC or PIV)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect or Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Provision to disable LaunchDarkly service (CWA2205)	Not Supported	Not supported
	Email-based auto-discovery of store (CWA2205)	Not Supported	Not supported
	Persistent login [Technical Preview] (CWA2205)	Not Supported	Not supported
	Authentication enhancement for Storebrowse (CWA2205)	Not Supported	Not supported
	Support for EDT IPv6 (CWA2203)	Not Supported	Not supported
	Support for TLS protocol version 1.3 (CWA2203)	Not Supported	Not supported
	Custom web stores (CWA2203)	Not Supported	Not supported

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Authentication enhancement experimental feature (CWA2203)	Not Supported	Not supported
	Keyboard layout synchronization enhancement (CWA2203)	Not Supported	Not supported
	Multi-window chat and meetings for Microsoft Teams (CWA2203)	Not Supported	Not supported
	Dynamic e911 in Microsoft Teams (CWA2112)	Not Supported	Not Supported
	Request control in Microsoft Teams (CWA2112)	Not Supported	Not supported
	Support for cursor color inverting (CWA2112)	Supported	There are no limitations in this release.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	There are no limitations in this release.
	Enhancement on smart card support (CWA2112)	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Not supported	Not supported
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported

Table 139. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106, and CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio devices (CWA2012, CWA2010, and CWA2112)	Not supported	Not supported
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support (CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

New and enhanced features

Citrix Workspace app updates

Citrix Workspace app package version is updated to 22.5.0.16.3 . This package is intended for users who want to install the Citrix Workspace app version 2205 on ThinOS.

RTME (Citrix HDX Realtime Media Engine) version is updated to 2.9.500-2802.

The following are the Citrix Workspace app limitations and known issues:

- If VDA2203 LTSR desktop is used with HDX webcam in 32-bit applications, the session disconnects. This issue is also observed in the Citrix Workspace app Linux binary—CVADHELP-20223.
- 64-bit applications with HDX webcam in ThinOS are not supported
- The following new features from Citrix Workspace app 2205 are not supported:
  - Provision to disable LaunchDarkly service
  - Email-based auto-discovery of store
  - Persistent login [Technical Preview]
  - Authentication enhancement for Storebrowse
- Test cursor does not blink in command prompt of server operating system VDA as it does in Windows 2016 and 2019. The issue is also reproduced in CWA 2205 Linux binary.

Cisco Webex Meetings VDI updates

- Cisco Webex Meetings VDI package version is updated to 42.8.2.8.1.
- Supports **Virtual Background/Blur image** from this release.

  ⓘ **NOTE:** You may see version 42.8.2.8 in ThinOS Packages Details. This is just a special update of 42.6 version.

Cisco Webex Meetings VDI feature matrix

Table 140. Cisco Webex Meetings optimization feature matrix

Scenarios	ThinOS 2205
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Lock meeting	Supported

Table 140. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 2205
Return meeting	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—To everyone	Supported
Chat—To specified participants	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Share one of the applications	Supported
Share screen—Switch share content	Supported
Share screen—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported
Participant	Supported
Close Participant	Supported
Invite and Remind	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Names in video calls automatically hidden when not speaking	Supported
Show all names/Hide all names/Show participants without video	Supported
Increase or Decrease Video size	Supported
Virtual Background/Blur image	Supported
VDI Meetings can display and extend participant grid view from 3x3 to 5x5	Not tested

Cisco Webex Meetings VDI limitations

- If a user increases the zoom percentage to 213%, the shared screens of other users are not visible.

- While viewing the shared video from others, zooming percentage varies automatically from 103% to 220%. The issue is observed on Wyse 5070 standard thin client and Latitude 3420 with ThinOS.
- When a user moves the shared screen from another user in a side-by-side layout, there is an issue with the user interface.
- When a user minimizes and restores the meeting session, there is a delay in viewing the videos from other users.
- While sharing screen, if you play a local or online video, the shared video is not clear for other users.
- When a user is already sharing the screen and if a new user joins the meeting, the screen sharing gets delayed.
- On Wyse 5470 All-in-One thin clients, the shared video from another user stops responding.
- Virtual background preview window does not move smoothly while moving the videos setting window in Wyse 5470 thin client.
- A gray patch is displayed on the window screen when a user shares screen on a **Webex Meetings** call.
- When you join a **Webex Meetings** call, an error message that states cannot start, or join the meeting is displayed.

Cisco Webex VDI update

Cisco Webex VDI package version is updated to 42.4.1.22585.1.

Cisco Webex VDI feature matrix

Table 141. Cisco Webex optimization feature matrix

Scenarios	ThinOS 2205
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Chat—To everyone	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Annotates	Supported

Table 141. Cisco Webex optimization feature matrix (continued)

Scenarios	ThinOS 2205
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Not Supported
Breakout sessions (Create Breakout room under Teams Tab join Manually)	Supported
Support—Request Desktop Control	Not Supported
Support—Request Application Control	Not Supported
Stop share screen	Supported
Participant	Supported
Remove Participant	Supported
Invite and Remind	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Names in Video-Automatically Hide names when not Speaking,	Supported
Virtual Background/Blur image	Not Supported

Cisco Webex VDI limitations

The following features are not supported:

- 911 Wireless Location Reporting (CER)
- Automatically Optimize Shared Content
- Background noise reduction
- Blur and virtual background
- ICE support for media optimization
- Music Mode

Zoom updates

- Zoom Citrix package version is updated to 5.10.2.21113.7.
- Zoom Horizon package version is updated to 5.10.2.21113.8.
- **Remote camera control**—Supports far end camera control.
- **VDI Statistics tab improvements**—More information about the status indication for missing or incompatible VDI plugins are added to the Statistics dialog in the VDI tab. You can view the information about when and why a session is running in fallback mode.

Zoom feature matrix

Table 142. Zoom feature matrix

Scenarios	ThinOS 2205
Join meeting	Supported
Audio call	Supported
Video call	Supported

Table 142. Zoom feature matrix (continued)

Scenarios	ThinOS 2205
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Chat—To everyone	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Not Supported
Breakout sessions (Create Breakout room under Teams Tab join Manually)	Supported
Support—Request Desktop Control	Not Supported
Suppor—Request Application Control	Not Supported
Stop share screen	Supported
Participant	Supported
Remove Participant	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Virtual Background/Blur image	Supported

Zoom fixed issues and limitation

The following issues are resolved:

- Fixed the issue where the audio from a focused shared session could be heard when new participants join.

- Fixed the issue where changing the display view to a grid for the side panel results in the Mute option not being presented for all participants. Mute option is now displayed for all participants.
- Fixed the issue where the virtual background selection tab for the Linux VDI plug-in was displayed incorrectly when virtual backgrounds were disabled in web configuration.
- Fixed the issue where the text displayed for the unmute option was incorrect while using the **Request permission to Unmute participants** option.
- Fixed the issue with the dialog to pick a color for the **I have a green screen option**. The issue is observed when the dialog was opened while a video is being displayed in a meeting, the user is unable to select a color.

Zoom limitation—The performance will be low while using hardware platforms with 2 cores CPU. Use platforms with 4 cores CPU to avoid performance issues.

Imprivata PIE update

Imprivata package version is updated to 7.8.000.0008.1161.

Known issues

Table 143. Known issues

Issue ID	Description	Workaround
DTOS-10652	Cisco Webex Meetings application becomes unresponsive during a call, and displays a pop-up window.	You must close the application first. Do not close the application from the task manager.
DTOS-10175	Audio quality is poor while using Bluetooth or Wireless headset on Wyse 5070 extended thin clients.	Use USB headsets instead of Bluetooth.
DTOS-11054	Logitech Camera (C922 Pro Stream webcam) does not work in a Cisco Webex VDI unified communications call.	There is no workaround in this release.

Tested environments matrix

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

Table 144. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.7 458
Imprivata OneSign	7.8
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 145. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2203LTSR	Tested	Tested	Tested	Tested

Table 146. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Tested	Tested	Tested—Only basic connection is tested on Ubuntu 20.04.

Table 147. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10 Windows server 2016 Windows server 2019	2.9.500	2.9.500	Skype for Business 2016	Skype for Business 2015

Table 148. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10 Windows server 2016 Windows server 2019	5.10.2.21113.7	5.10.2(21113)

Table 149. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10 Windows server 2016 Windows server 2019	5.10.2.21113. 8	5.10.2(21113)

Table 150. Tested environment—Cisco Webex VDI

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10 Windows server 2016 Windows server 2019	42.4.1.22585.1	42.4.0.21893

Table 151. Tested environment—Cisco Webex VDI

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	42.4.1.22585.1	42.4.0.21893
	Windows server 2016		
	Windows server 2019		

Table 152. Tested environment—Cisco Webex Meetings VDI

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU5) Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	42.8.2.8.1 (special release based on 42.6)	42.8
	Windows server 2016		
	Windows server 2019		

Table 153. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	42.8.2.8.1 (special release based on 42.6)	42.8
	Windows server 2016		
	Windows server 2019		

8

Security package for ThinOS 2205

Release summary

Patch or add-on releases are created to support the existing hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on shipping hardware platforms. This package updates the **underscore** package from version 1.9.1 to 1.13.3 to fix the arbitrary code injection security vulnerability CVE-2021-23358. This security package is only applicable for ThinOS 2205 (9.3.1129).

Version

Security_Addon_2205_1.0.0.3.pkg

Release date

June 2022

Supported platforms

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- OptiPlex 3000 Thin Client
- Latitude 3420

Important notes

- The security package is only applicable for ThinOS 2205 (9.3.1129). Future ThinOS releases will contain this fix.
- After you install **Security_Addon_2205_1.0.0.3.pkg**, do not uninstall it from ThinOS 2205. If you uninstall the package, the security fix gets removed.
- When you upgrade ThinOS 2205 that has **Security_Addon_2205_1.0.0.3.pkg** installed, to the next version of ThinOS, the package will be removed by default. The security fix is included as part of the next ThinOS version.

  NOTE: If the package is not removed automatically after the upgrade, restart the thin client.

Tested BIOS details

Table 154. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.17.0
Wyse 5470 All-in-One Thin Client	1.15.0
Wyse 5470 Mobile Thin Client	1.14.0

Table 154. Tested BIOS details (continued)

Platform name	BIOS version
OptiPlex 3000 Thin Client	1.0.2
Latitude 3420 with ThinOS	1.16.1

If you are upgrading BIOS on the Wyse 5470 Thin Client, ensure that you have connected the device to the external power source using the power adapter. If you do not connect the power adapter, BIOS update fails. In this event, connect an external power source and reboot twice to install BIOS.

NOTE: When you use the BIOS upgrade feature for the first time, the BIOS package downloads even if the existing BIOS version is the same version that is uploaded.

Download the application package

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device.
3. Select the product from the searched results to load the product page.
4. On the product support page, click **Drivers & downloads**.
5. Select the operating system as **ThinOS**.
6. Locate the application package that you require.
7. Download the application package file.

Install the application package using Wyse Management Suite

Prerequisites

- Upgrade the ThinOS firmware to version 2205.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the application package. See, Download the application package.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS window** is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.

   NOTE: If you cannot locate the **Application Package Updates** option under the **Standard** tab, use the **Advanced** tab.

5. Click **Browse**, and select **Security_Addon_2205_1.0.0.3.pkg**.
6. From the drop-down menu, select the uploaded application package.
7. Click **Save & Publish**.
   The thin client downloads the package to install and restarts. The security package is installed.

Security vulnerability changes

This package updates the **underscore** package from version 1.9.1 to 1.13.3 to fix the arbitrary code injection security vulnerability CVE-2021-23358. This security package is only applicable for ThinOS 2205 (9.3.1129).

Tested environments matrix

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

Table 155. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.7 458
Configuration UI package for Wyse Management Suite	1.8 136
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 156. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2112	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2203LTSR	Tested	Tested	Tested	Tested

Table 157. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Tested	Tested	Tested—Only basic connection is tested on Ubuntu 20.04

Table 158. Test environment—VMware Horizon Cloud

Horizon Cloud	Windows 10	Windows Server 2016
Build Version: 19432376	Horizon Agent Installer - 21.3.0.19265453	Horizon Agent Installer - 21.3.0.19265453

Table 159. Test environment—Microsoft RDP

Microsoft RDP	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
Remote Desktop Services 2016	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2019	Not tested	Tested	Not tested	Not tested	Not tested	Tested	Tested

Table 160. Test environment—AVD

Azure Virtual Desktop	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
2019 (MS-Prod)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested
2020 (ARMv2)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested

Table 161. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	2.9.400	2.9.400	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				

Table 162. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 163. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	14.0.3.306553.1	14.1.0.306686_4	14.1.0.56686
	Windows server 2016			
	Windows server 2019			

Table 164. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10	14.1.0.306686_4	14.1.0.56686	14.1.0.306686_4
	Windows server 2016			
	Windows server 2019			

Table 165. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	5.9.6.20931.7	5.9.6(20931)
	Windows server 2016		
	Windows server 2019		

Table 166. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106 VMware Horizon View 7.13.2	Windows 10	5.9.6.20931.7	5.9.6(20931)
	Windows server 2016		
	Windows server 2019		

Table 167. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	41.12.0.20899	41.12.0.20899.3
	Windows server 2016		
	Windows server 2019		

Table 168. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10	41.12.0.20899	41.12.0.20899.3
	Windows server 2016		
	Windows server 2019		

Table 169. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	42.2.6.11.3	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6.
	Windows server 2016		
	Windows server 2019		

Table 170. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106	Windows 10	42.2.6.11.3	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6. Webex Meeting does not work well with Horizon 2111. This is a Cisco limitation.
	Windows server 2016		
	Windows server 2019		

Cisco Webex Meetings VDI 42.2.8.5

Release summary

Patch or add-on releases are created to support the existing hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on shipping hardware platforms.

Current version

Cisco_Webex_Meetings_VDI_42.2.8.5.1.pkg

Release date

June 2022

Supported platforms

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- OptiPlex 3000 Thin Client
- Latitude 3420 with ThinOS

Important notes

- Upgrade the ThinOS firmware to ThinOS 2205 (9.3.1129) before you install the application packages.
- Cisco Webex Meetings VDI is qualified for Citrix VDI on ThinOS 2205 (9.3.1129) with Citrix Workspace app package 22.3.0.24.6.
- Cisco Webex Meetings VDI is qualified for VMware Horizon VDI on ThinOS 2205 (9.3.1129) with VMware Horizon app package 2203.8.5.0.19586897.4

Installing the application package

Download the application package

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device.
3. Select the product from the searched results to load the product page.
4. On the product support page, click **Drivers & downloads**.
5. Select the operating system as **ThinOS**.
6. Locate the application package that you require.

7. Download the application package file.

Install the application package using Wyse Management Suite

Prerequisites

- Upgrade the ThinOS firmware to ThinOS 2205 (9.3.1129) before you install the application package.
- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.

  NOTE: If you have an existing group with a valid group token, you can register the thin client to the same group.
- Ensure you have downloaded the application packages. See, Download the application package.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**. The Configuration Control | ThinOS window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.

   NOTE: If you cannot locate the **Application Package Updates** option under the **Standard** tab, use the **Advanced** tab.
5. Click **Browse** and select the application package to upload.
6. From the drop-down menu, select the uploaded application package.
7. Click **Save & Publish**.
   The thin client downloads the package to install and restarts. The package version is upgraded.

Compatibility

Application package information

- Supported ThinOS application packages—**Cisco_Webex_Meetings_VDI_42.2.8.5.1.pkg** is qualified by Dell Technologies.
- Supported Firmware—ThinOS 2205 (9.3.1129).

NOTE: For information about other packages, see ThinOS application package details in the **ThinOS 2205 Release Notes**.

Previous versions

Cisco_Webex_Meetings_42.2.6.11.3.pkg

Cisco Webex Meetings optimization feature matrix

Table 171. Cisco Webex Meetings optimization feature matrix

Scenarios	ThinOS 2205
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported

Table 171. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 2205
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Lock meeting	Supported
Return meeting	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—To everyone	Supported
Chat—To specified participants	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Share one of the applications	Supported
Share screen—Switch share content	Supported
Share screen—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported
Participant	Supported
Close Participant	Supported
Invite and Remind	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported

Table 171. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 2205
Names in video calls automatically hidden when not speaking	Supported
Show all names/Hide all names/Show participants without video	Supported
Increase or Decrease Video size	Supported
Virtual Background/Blur image	Not supported
VDI Meetings can display and extend participant grid view from 3x3 to 5x5	Not tested

Cisco Webex Meetings optimization limitation

Green patch or lines appear during screen share and while using the white board.

New and enhanced features

Cisco Webex Meetings VDI package version is updated to 42.2.8.5.1. Fixed the issue where audio is choppy when two or more users are in a call.

Tested environments matrix

The following tables display the tested server versions for this release. The supported versions are not limited to the tested versions. ThinOS is compatible backward and forward with server versions:

Table 172. Tested environment—Cisco Webex Meetings VDI

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	42.2.8.5.1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6.
	Windows server 2016		
	Windows server 2019		

Table 173. Tested environment—Cisco Webex Meetings VDI

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 2111	Windows 10	42.2.8.5.1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6. Webex Meeting does not work well with Horizon 2111. This is a Cisco limitation.
	Windows server 2016		
	Windows server 2019		

10

ThinOS 2205

Release date

May 2022

Release summary

Patches or Add-on releases are created to support existing platforms or software releases, correct defects, make enhancements, or add minor features.

Few hardware configurations are not supported for Latitude 3420. There are also a few limitations for Latitude 3420. For the full list of these configurations and limitations, see **Hardware configurations that are not supported for Latitude 3420** and **ThinOS Limitations on Latitude 3420** in the ThinOS enhancements section.

ⓘ **NOTE:** Install the security package **Security_Addon_2205_1.0.0.3.pkg** for ThinOS 2205 to fix the security vulnerability issue CVE-2021-23358. See Security package for ThinOS 2205.

Current version

ThinOS 2205 (9.3.1129)

Previous version

ThinOS 9.1.6108

Firmware upgrade

The following firmware upgrade scenarios are supported:

- ThinOS 9.1.3129 or later versions > ThinOS 2205 (9.3.1129)

ⓘ **NOTE:** If you are using earlier versions of ThinOS 8.6, upgrade to ThinOS 8.6_807 and apply the latest BIOS updates before upgrading to ThinOS 9.1.6108. Then, you can upgrade to ThinOS 2205 from 9.1.6108. If you are using earlier versions of ThinOS 9.x, you must first upgrade to ThinOS 9.1.3129 or later versions before upgrading to ThinOS 2205.

ⓘ **NOTE:** On thin clients with ThinOS 9.x versions earlier than ThinOS 9.1.6108, upgrade the OS image and upgrade the BIOS after the OS image is successfully upgraded. Do not upgrade the BIOS and the OS image together. If you upgrade the BIOS and the OS image together, the BIOS upgrade is ignored, and you cannot upgrade the BIOS to the ignored version anymore. You must upgrade the BIOS to another version.

ⓘ **NOTE:** If you want to downgrade ThinOS to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2205 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

- There are chances that after the upgrade the device displays a black screen. You may reboot the device to boot it up correctly.
- If the thin client is registered in Wyse Management Suite group 1 and you set Wyse Management Suite group 2 token in group 1 policy, then the group 2 token is applied on GUI but the thin client will still be in group 1. You must reboot the thin client to change the thin client to Wyse Management Suite group 2.

  ⓘ **NOTE:** Dell Technologies recommends that you set both new ThinOS firmware and new application packages in Group 1, so that thin client installs the files, automatically reboots, and changes to Group 2.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
  - Not display a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - Not display any notification if the new firmware or application is downloaded in the same group.
  - Installs the firmware or package after a reboot.
- If you have installed HID_Fingerprint_Reader package, ensure that you have also installed Citrix_Workspace_App package, or you cannot upgrade to ThinOS version 2205.
- If you configure settings, like brokers, locally in ThinOS and downgrade to ThinOS 6108 or earlier versions using Wyse Management Suite, the settings are lost.
- If you downgrade to ThinOS 6108 or earlier versions using Wyse Management Suite, reboot the system manually again to set a password locally in ThinOS. Otherwise, the password may not be clear.

Prerequisites for firmware upgrade

- Before you migrate from ThinOS 9.x to ThinOS 2205, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the Wake On LAN command through Wyse Management Suite before using any real-time commands. To use the Wake On LAN command, ensure that the Wake On LAN option is enabled in BIOS.

Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
- Download the new version of the firmware to upgrade.

Steps

1. Go to the **Groups & Configs** page and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**. The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **OS Firmware Updates**.

   ⓘ **NOTE:** If you cannot locate the **OS Firmware Updates** option under the **Standard** tab, use the **Advanced** tab.
5. Click **Browse** and select the new version of the firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.
   The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

ⓘ **NOTE:** There are chances that the upgrade might fail with event log stating **Failed to install**. In such an event, you may reboot the device and upgrade again.

ⓘ **NOTE:** To optimize security, application performance, and stability, a design change has been made in ThinOS 2205 when installing third-party applications, like Citrix Workspace App, VMware Horizon, and Microsoft AVD. Third-party applications released as part of ThinOS 2205 use a different shared library search path than older third-party package versions. Because of this optimization, third-party packages that are released before ThinOS 2205 are no longer supported with ThinOS 2205 or later versions. Install the latest version of the required third-party application after you upgrade to ThinOS 2205 or later versions.

ⓘ **NOTE:** There are chances that the ThinOS background might be in blue color and some features may not work. In this case, you have to reboot the device.

Convert Ubuntu 20.04 with DCA to ThinOS 2205 or 2208

Prerequisites

- If you have a device that is running Ubuntu 20.04 operating system, ensure that DCA-Enabler 1.5.0-14 or later versions is installed. For details on how to install DCA-Enabler in Ubuntu operating system and upgrade it, see Dell Wyse ThinOS Migration Guide at www.dell.com/support.

  ⓘ **NOTE:** The device must have a factory-installed Ubuntu 20.04 operating system. If you have custom installed the Ubuntu operating system, you cannot convert it to ThinOS 2205 or 2208.

  ⓘ **NOTE:** There are some languages that do not support the conversion from Ubuntu to ThinOS 2205. Dell Technologies recommends you to set Ubuntu to English language for the conversion process.
- Wyse Management Suite version 3.7 or later versions must be used to convert to ThinOS 2205 or 2208.
- Ensure that you have connected the Ubuntu device to the external power source using the power adapter.
- Ensure you have enough ThinOS Activation devices licenses on Wyse Management Suite 3.7 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than the Ubuntu device number. If it is not larger, you cannot create the Advanced Policy for conversion.
- The Ubuntu 20.04 devices must be registered to Wyse Management Suite as generic clients. For details on how to register the generic client to Wyse Management Suite, see Dell Wyse ThinOS Migration Guide at www.dell.com/support.
- Ensure you have downloaded the Ubuntu 20.04 to ThinOS 2205 or 2208 conversion image.
- Extract the Ubuntu 20.04 to ThinOS 2205 or 2208 conversion image to get the Conversion Installer file. **DTOS_Ubuntu_Installer_x.x-dtosx-amd64_signed.tar.gz** and ThinOS image **ThinOS_YYMM_9.x.pkg**.

  ⓘ **NOTE:** The ThinOS image **ThinOS_YYMM_9.x.pkg** can be used for downgrade in the future.

Supported platforms: Latitude 3420 and OptiPlex 5400 All-in-One

Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the Conversion Installer file **DTOS_Ubuntu_Installer_x.x-dtosx-amd64_signed.tar.gz**
3. Go to **Apps & Data** > **OS Image Repository** > **ThinOS 9.x**, and click **Add Firmware file**.
4. Upload the ThinOS image **ThinOS_YYMM_9.x.pkg**.
5. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
6. Enter the policy name, select the group in which the Ubuntu device has been registered, and select **Generic Client** as OS type.
7. Select the platforms you want to convert in the **Platform Filter** drop-down menu.
8. Click **Add app**, and select the conversion installer file that was uploaded before from the drop-down menu.
9. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
10. Click **Save**.

    ⓘ **NOTE:** Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
11. In the next window, click **Yes** to schedule a job.

12. Select **Immediately** in the **Run** drop-down menu in the **App Policy Job** window and click **Preview**.
13. Click **Schedule**.
    The Conversion Installer file downloads and installs first followed by the ThinOS image on the Ubuntu device. After installation, the device restarts automatically.

    ⓘ **NOTE:** After you register the converted ThinOS device to Wyse Management Suite, the ThinOS activation devices license is consumed automatically.

    ⓘ **NOTE:** After conversion, ThinOS is in the factory default status. ThinOS must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

    ⓘ **NOTE:** If the conversion has failed, you can see the error log table below and reschedule the job. Go to **Jobs** > **Schedule APP Policy** to reschedule the job. If the conversion has failed, it is recommended you install the ISO image.

    If there is a **/usr/dtos** folder in your Ubuntu 20.04 device, you can use the command **cat /var/log/dtos_dca_installer.log** to get the error log.

    If there is no **/usr/dtos folder** in your Ubuntu 20.04 device, go to the **WMS Server Jobs** page to check the error messages.

Table 174. Error Log table

Error Log	Resolution
No AC plugged in	Plug in power adapter, reschedule job
Platform Not Supported	This hardware platform is not supported
Error mounting recovery partition	The Ubuntu image is not a factory image. Reinstall the factory image.
No DHC/ThinOS package in recovery partition	Cannot find the ThinOS image, reschedule job
Error in extracting DHC/ThinOS Future packages	Failed to extract the ThinOS image, reschedule job
Error copying the DHC/ThinOS Future packages to recovery partition	Failed to copy the ThinOS image, reschedule job
ThinOS package verification failed	ThinOS image is not correct, reschedule job with the correct ThinOS image
Not enough space in Recovery Partition	Clear the recovery partition
The free space of Recovery Partition is not enough	Clear the recovery partition

Compatibility

ThinOS application package details

- Cisco_Jabber_14.1.0.306686.4.pkg
- Cisco_Webex_Meetings_42.2.6.11.3.pkg
- Cisco_Webex_VDI_41.12.0.20899.3.pkg (formerly called Cisco Webex Teams)
- Citrix_Workspace_App_22.3.0.24.6.pkg
- Epos_Connect_7.0.0.19336.3.pkg
- HID_Fingerprint_Reader_210217.17.pkg
- Jabra_8.5.1.13.pkg
- Microsoft_AVD_1.7.1540.pkg
- Teradici_PcoIP_22.01.5.72.pkg
- VMware_Horizon_2203.8.5.0.19586897.4.pkg
- Zoom_Citrix_5.9.6.20931.7.pkg
- Zoom_Horizon_5.9.6.20931.7.pkg
- Imprivata_PIE_7.5.000.0003.1144.pkg
- Imprivata_PIE_7.7.000.0007.1143.pkg
- Ildentity_Automation_QwickAccess_2.0.1.0.3.pkg

NOTE: After upgrading to ThinOS 2205, all old application packages are removed automatically. The old application packages can be downloaded but installation fails the first time. After this, the old application packages cannot be downloaded anymore. You must install the latest application packages.

Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 3.7.458
- Configuration UI package 1.8.133

ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2205 (9.3.1129)—**ThinOS_2205_9.3.1129.pkg**
- Ubuntu 20.04 + DCA 1.5.0-14 to ThinOS 2205 conversion build
    - **ThinOS_2205_9.3.1129_Conversion.zip**—Dell Latitude 3420

BIOS packages

Table 175. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.17.0.pkg
Wyse 5470 Thin Client	bios-5470_1.14.0.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.15.0.pkg
Latitude 3420	bios-Latitude_3420_1.16.1.pkg

Tested BIOS version for ThinOS 2205

Table 176. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.17.0
Wyse 5470 All-in-One Thin Client	1.15.0
Wyse 5470 Mobile Thin Client	1.14.0
OptiPlex 3000 Thin Client	1.0.2
Latitude 3420	1.16.1

If you are upgrading BIOS on the Wyse 5470 Thin Client, ensure that you have connected the device to the external power source using the power adapter. If you do not connect the power adapter, BIOS update fails. In this event, connect an external power source and reboot twice to install BIOS.

NOTE: Do not downgrade the BIOS on Wyse 5470 Thin Client. If you downgrade, a BIOS downgrade failure message is displayed whenever you reboot your client.

If you are upgrading BIOS on Latitude 3420 , ensure that you have connected the device to the external power source using the power adapter. If you do not connect the power adapter, BIOS update fails. In this event, you cannot reinstall the BIOS package.

Citrix Workspace app feature matrix

Table 177. Citrix Workspace app feature matrix

Feature		ThinOS 2205	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
			Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Limited Support	Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. The feature only works on mobile thin clients,such as 5470 and 3420 mobile thin clients from ThinOS

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
			2205 with CWA2203. This is a Citrix binary limitation. ThinOS 2205 does not support webcam redirection with 64-bit applications. For further details, refer to the Dell Wyse ThinOS Administrator's Guide.
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco Webex Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebexTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
			Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
			Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Active Directory	Supported	There are no limitations in this release.
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Support for EDT IPv6 (CWA2203)	Not Supported	Not supported
	Support for TLS protocol version 1.3 (CWA2203)	Not Supported	Not supported
	Custom web stores (CWA2203)	Not Supported	Not supported
	Authentication enhancement experimental feature (CWA2203)	Not Supported	Not supported
	Keyboard layout synchronization enhancement (CWA2203)	Not Supported	Not supported
	Multi-window chat and meetings for Microsoft Teams (CWA2203)	Not Supported	Not supported
	Dynamic e911 in Microsoft Teams (CWA2112)	Not Supported	Not Supported
	Request control in Microsoft Teams (CWA2112)	Not Supported	Not supported
	Support for cursor color inverting (CWA2112)	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at www.dell.com/support.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	There are no limitations in this release.
	Enhancement on smart card support (CWA2112)	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Not supported	Not supported
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106, CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio devices(CWA2012, CWA2010, and CWA2112)	Not supported	If JVDI package is installed in ThinOS, audio devices cannot be switched in the applications in session and the session is disconnected when users open the **Recording devices** list at the Windows sound. If you want to use multiple ICA audio devices, it is recommended that you do not install the VDI package.
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported

Table 177. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2205	Limitations
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

VMware Horizon feature matrix

Table 178. VMware Horizon feature matrix

Feature		ThinOS 2205
Broker Connectivity	SSL certificate verification	Supported only with VDI
	Disclaimer dialog	Supported with VDI, RDS Hosted Desktops and Apps
	UAG compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Shortcuts from server	Not supported
	Pre-install shortcuts from server	Not supported
	File type association	Not supported
	Phone home	Supported with VDI, RDS Hosted Desktops and Apps
Broker Authentication	Password authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Single sign on	Supported with VDI, RDS Hosted Desktops and Apps
	RSA authentication	Supported with VDI, RDS Hosted Desktops and Apps

Table 178. VMware Horizon feature matrix (continued)

Feature		ThinOS 2205
	Integrated RSA SecurID token generator	Not supported
	Kiosk mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remember credentials	Not supported
	Log in as current user	Not supported
	Nested log in as current user	Not supported
	Log in as current user 1-way trust	Not supported
	OS biometric authentication	Not supported
	Un-authentication access	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Cisco ACS	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – SMS Passcode	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - DUO	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - OKTA	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Microsoft Network Policy	Supported with VDI, RDS Hosted Desktops and Apps
Smart card	x.509 certificate authentication (Smart Card)	Supported with VDI, RDS Hosted Desktops and Apps
	CAC support	Supported with VDI, RDS Hosted Desktops and Apps
	.Net support	Supported with VDI, RDS Hosted Desktops and Apps
	PIV support	Supported with VDI, RDS Hosted Desktops and Apps
	Java support	Not supported
	Purebred derived credentials	Not supported
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI
	Restart	Supported only with VDI
	Log off	Supported with VDI, RDS Hosted Desktops and Apps
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple connections	Supported with VDI, RDS Hosted Desktops and Apps
	Multi-broker/multi-site redirection - Universal	Not supported
	App launch on multiple end points	Supported with VDI, RDS Hosted Desktops and Apps

Table 178. VMware Horizon feature matrix (continued)

Feature		ThinOS 2205
	Auto-retry 5+ minutes	Supported with VDI, RDS Hosted Desktops and Apps
	Blast network recovery	Supported with VDI, RDS Hosted Desktops and Apps
	Time zone synchronization	Supported with VDI, RDS Hosted Desktops and Apps
	Jumplist integration (Windows 7-Windows 10)	Not supported
Client Customization	Command line options	Not supported
	URI schema	Not supported
	Launching multiple client instances using URI	Not supported
	Preference file	Not supported
	Parameter pass-through to RDSH apps	Not supported
	Non interactive mode	Not supported
	GPO-based customization	Not supported
Protocols Supported with VDI, RDS Hosted Desktops and Apps	Blast Extreme	Supported with VDI, RDS Hosted Desktops and Apps
	H.264 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	H.265 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps—Except OptiPlex 3000 and Latitude 3420 with ThinOS.
	Blast Codec	Supported with VDI, RDS Hosted Desktops and Apps
	JPEG/PNG	Supported with VDI, RDS Hosted Desktops and Apps
	Switch encoder	Supported with VDI, RDS Hosted Desktops and Apps
	BENIT	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Extreme Adaptive Transportation	Supported with VDI, RDS Hosted Desktops and Apps
	RDP 8.x, 10.x	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP	Supported with VDI, RDS Hosted Desktops and Apps
Features/Extensions Monitors/Displays	Dynamic display resizing	Supported with VDI, RDS Hosted Desktops and Apps
	VDI windowed mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remote app seamless window	Supported with VDI, RDS Hosted Desktops and Apps

Table 178. VMware Horizon feature matrix (continued)

Feature		ThinOS 2205
	Multiple monitor support	Supported with VDI, RDS Hosted Desktops and Apps
	External monitor support for mobile	Not supported
	Display pivot for mobile	Not supported
	Number of displays Supported with VDI, RDS Hosted Desktops and Apps	4
	Maximum resolution	3840x2160
	High DPI scaling	Supported only with VDI
	DPI sync	Supported with VDI, RDS Hosted Desktops and Apps
	Exclusive mode	Not supported
	Multiple monitor selection	Supported with VDI, RDS Hosted Desktops and Apps
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported with VDI, RDS Hosted Desktops and Apps
	Relative mouse	Supported only with VDI
	External Mouse Support	Supported with VDI, RDS Hosted Desktops and Apps
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported with VDI, RDS Hosted Desktops and Apps
	International Keyboard Support	Supported with VDI, RDS Hosted Desktops and Apps
	Input Method local/remote switching	Not supported
	IME Sync	Supported with VDI, RDS Hosted Desktops and Apps
Clipboard Services	Clipboard Text	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard Graphics	Not supported
	Clipboard memory size configuration	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard File/Folder	Not supported
	Drag and Drop Text	Not supported
	Drag and Drop Image	Not supported
	Drag and Drop File/Folder	Not supported
Connection Management	IPv6 only network support	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP IP roaming	Supported with VDI, RDS Hosted Desktops and Apps
Optimized Device Redirection	Serial (COM) Port Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Client Drive Redirection/File Transfer	Not supported

Table 178. VMware Horizon feature matrix (continued)

Feature		ThinOS 2205
	Scanner (TWAIN/WIA) Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	x.509 Certificate (Smart Card/ Derived Credentials)	Supported with VDI, RDS Hosted Desktops and Apps
	Gyro Sensor Redirection	Not supported
Real-Time Audio-Video	Audio in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Video in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple webcams	Not supported
	Multiple speakers	Not supported
USB Redirection	USB redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnInsert	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnStartup	Supported with VDI, RDS Hosted Desktops and Apps
	Connect/Disconnect UI	Not supported
	USB device filtering (client side)	Supported with VDI, RDS Hosted Desktops and Apps
	Isochronous Device Support	Supported only with VDI
	Split device support	Supported with VDI, RDS Hosted Desktops and Apps
	Bloomberg Keyboard compatibility	Supported only with VDI
	Smartphone sync	Supported only with VDI
Unified Communications	Skype for business	Supported with VDI, RDS Hosted Desktops and Apps
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Teams	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Meetings	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops and Apps
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops and Apps
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not supported
	Directshow Redirection	Not supported
	URL content redirection	Not supported
	MMR Multiple Audio Output	Not supported
	Browser content redirection	Not supported
Graphics	vDGA	Supported only with VDI

Table 178. VMware Horizon feature matrix (continued)

Feature		ThinOS 2205
	vSGA	Supported only with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Supported only with VDI
	AMD vGPU	Supported only with VDI
Mobile Support	Client-side soft keyboard	Not supported
	Client-side soft touchpad	Not supported
	Full Screen Trackpad	Not supported
	Gesture Support	Not supported
	Multi-touch Redirection	Not supported
	Presentation Mode	Not supported
	Unity Touch	Not supported
Printing	VMware Integrated Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Location Based Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Native Driver Support	Not supported
Security	FIPS-140-2 Mode Support	Supported with VDI, RDS Hosted Desktops and Apps
	Imprivata Integration	Supported with VDI, RDS Hosted Desktops and Apps
	Opswat agent	Not supported
	Opswat on-demand agent	Not supported
	TLS 1.1/1.2	Supported with VDI, RDS Hosted Desktops and Apps
	Screen shot blocking	Not supported
	Keylogger blocking	Not supported
Session Collaboration	Session Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
	Read-only Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
Update	Update notifications	Not supported
	App Store update	Not supported
Other	Smart Policies from DEM	Supported with VDI, RDS Hosted Desktops and Apps
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI—Only basic connection is tested
	Workspace ONE mode	Supported with VDI, RDS Hosted Desktops and Apps
	Nested - basic connection	Supported with VDI, RDS Hosted Desktops and Apps
	DCT Per feature/component collection	Not supported

Table 178. VMware Horizon feature matrix (continued)

Feature		ThinOS 2205
	Displayed Names for Real-Time Audio-Video Devices	Supported with VDI, RDS Hosted Desktops and Apps
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI

For detailed information about the VMware Horizon features, see the Horizon documentation at docs.vmware.com.

ThinOS AVD Client Feature Matrix

Table 179. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 9.3.1129 with AVD 1.7_1524
Service	Direct connection to Desktop via RDP	Supported
	Remote Desktop Services (On-Prem)	Not supported
	Windows Virtual Desktop (Azure)	Supported
Session	Desktop	Supported
	Remote App (Integrated)	Supported
	Remote App (Immersive)	Supported
	Multiple connections	Supported
Input	Keyboard	Supported
	Mouse	Supported
Audio Visual	Audio in (microphone)	Supported
	Audio out (speaker)	Supported
	Camera	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
	Clipboard (file)	Supported
Redirections	Printer	Supported
	SmartCard	Not supported
Session Experience	Dynamic Resolution	Supported
	Multi-Monitor (All)	Supported
	Multi-Monitor (Specified Subset)	Supported
	Restricted full screen session	Supported
Graphics (CODECs)	H.264 Hardware Acceleration	Supported

New and enhanced features

Citrix Workspace app updates

Multiple audio devices—From ThinOS 2205 and Citrix Workspace App 2203 onwards, Citrix Workspace app displays the names of all available local audio devices in a session. In addition, plug-and-play support for Bluetooth and HDMI audio devices is also provided. This feature is disabled by default. To enable this feature, do the following:

1. In Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced tab** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In the Citrix INI settings, click **Add Row**.
3. From the **File** drop-down list, select **module.ini**.
4. From the **Operation** drop-down list, select **Add or Update** .
5. In the **Section** field, enter **ClientAudio** .
6. In the Key field, enter **AudioRedirectionV4**.
7. In the Value field, enter **True**.
8. Sign out or restart the device for the settings to take effect.

Smart card reader enhancement—Smart card plug-and-play functionality is enabled by default from Citrix Workspace app 2112 and ThinOS 9.1.5067. From ThinOS 2205 and Citrix Workspace app 2203, you can disable the smart card plug-and-play functionality. To disable the functionality, do the following:

1. In Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced tab** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In the Citrix INI settings, click **Add Row**.
3. From the **File** drop-down list, select **module.ini**.
4. From the **Operation** drop-down list, select **Add or Update** .
5. In the **Section** field, enter **SmartCard**.
6. In the Key field, enter **DriverName**.
7. In the Value field, enter **VDSCARD.DLL**.
8. Sign out or restart the device for the settings to take effect.

Citrix Workspace app limitations

- If VDA2203 LTSR desktop is used with HDX webcam in 32-bit applications, the session disconnects. The issue also occurs in Linux Citrix Workspace app binary.
- If JVDI package is installed in ThinOS, audio devices cannot be switched in the applications in session, and the session is disconnected when you open **Windows** > **Sound** and go to the Recording devices list. If you want to use multiple ICA audio devices, it is recommended that you do not install the JVDI package.
- HDX webcam redirection works for 32-bit applications. The feature only works on mobile thin clients, such as 5470 and 3420 mobile thin clients from ThinOS 2205 with CWA2203. This is a Citrix binary limitation. If you are using Wyse 3040, 5070, or OptiPlex 3000 devices, it is recommended that you use ThinOS 9.1.6108 version with CWA2109. ThinOS 2205 does not support webcam redirection with 64-bit applications.
- The smartcard login window will refresh two times after accessing the network from Sleep mode. You must wait until you see the refreshed user login window, and then enter the PIN. Otherwise, an error message **Unknown error** is displayed and the login with smartcard fails.
- If you are on call or in a meeting on Wyse 5470 thin client using Microsoft Teams, you may face audio issues when sharing your screen. As a workaround, do not enable camera during calls or meetings, and the host with Wyse 5470 client must not move applications quickly in ICA sessions.
- 1080p Multimedia Redirection (MMR) videos stop responding and audio is missing in ICA sessions on networks with low bandwidth. The issue also occurs in Linux Citrix Workspace app binary.
- Qumu videos with Browser Content Redirection (BCR) enabled, may fail with an error message **An error has occurred**. As a workaround, play the video again. The issue also occurs in Linux Citrix Workspace app binary.
- Windows task bar is displayed while playing Qumu videos with Browser Content Redirection (BCR) enabled in full-screen mode. The issue also occurs in Linux Citrix Workspace app binary.
- Green patches or lines appear when playing videos on VLC Media Player or in a web browser online. The issue also occurs in Linux Citrix Workspace app binary.
- The progress bar is not displayed in desktop sessions after switching the keyboard language on the thin client and setting the keyboard layout to Dynamic Sync. The issue also occurs in Linux Citrix Workspace app binary.
- If Microsoft Teams optimization is disabled in a device with Windows server 2019 VDA, Microsoft Teams restarts automatically during calls or meetings. The issue also occurs in Linux Citrix Workspace app binary.

- The cursor color inverting function continues to work after disabling the cursor invert feature by setting the value to **Do not use video codec** for the **Use video codec for compression** policy in Citrix Studio. The issue also occurs in Linux Citrix Workspace app binary.

Unified Communications update

- Cisco Webex Meetings VDI package version is updated to 42.2.6.11.3.

Table 180. Cisco Webex Meetings optimization feature matrix

Scenarios	ThinOS 2205
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Lock meeting	Supported
Return meeting	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—To everyone	Supported
Chat—To specified participants	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported
Share screen—Whiteboard	Supported
Share screen—Share one of the applications	Supported
Share screen—Switch share content	Supported
Share screen—Annotates	Supported

Table 180. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 2205
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported
Participant	Supported
Close Participant	Supported
Invite and Remind	Supported
Layout Grid/Stack/Side by Side and Full-screen view	Supported
Names in video calls automatically hidden when not speaking	Supported
Show all names/Hide all names/Show participants without video	Supported
Increase or Decrease Video size	Supported
Virtual Background/Blur image	Not supported
VDI Meetings can display and extend participant grid view from 3x3 to 5x5	Not tested

Limitations

- ○ The performance is low on clients or virtual desktop interfaces with two cores. Use four core clients or virtual desktop interfaces to avoid performance issues.
- ○ There is an audio issue where the volume goes low and high.

- Cisco Webex Teams VDI package version is updated to 41.12.0.20899.3.
- Zoom version is updated to 5.9.6.20931.7.
- Cisco JVDI version is updated to 14.1.0.306686.4.

VMware Horizon update

- If you configure the Kiosk account user **Client Mac** as the ThinOS default user, you can login to the Horizon broker automatically.
- **VMware Horizon Client 2203 New Features**
  - In virtual desktop sessions, the Real-Time Audio-Video feature displays the actual names of redirected devices with (VDI) appended. (For example, C670i FHD Webcam (VDI).
  - You can use touchscreen gestures in remote desktop and application sessions. Touchscreen functionality is supported in full-screen mode and window mode and can also work with the Horizon Client user interface.

NOTE:

1. The touch function does not work properly when relative mouse is enabled.
2. Swiping down the screen using the touchscreen is not supported in desktop and application sessions.
3. Gesture feature is not supported in desktop and application sessions.
4. Multi touch is not supported.

VMware Horizon Blast limitations

- HEVC is not supported in Horizon Blast sessions on Latitude 3420 and OptiPlex 3000 Thin Clients.
- Microsoft Teams in Blast sessions may not display the incoming call window for calls. This issue also occurs on VMware Horizon Linux client running Ubuntu operating system.
- When using the Real-Time Audio-Video (RTAV) feature in Horizon PCoIP sessions, there may be noise.

Teradici PCoIP update

- Teradici PCoIP version 22.01.5.72 is supported in ThinOS 2205.
- The audio does not work when the device is connected to a Remote Workstation Card. This is a limitation from Teradici. For more details, see Software Client for Linux 22.01.3 Release Notes.

  NOTE: You must use PCoIP package version 21.03.1 if audio functionality is required with the Remote Workstation Card.
- **USB Redirection in a PCoIP session**—In PCoIP sessions, ensure that the Group Policy is enabled for the USB redirection to work. Do the following to enable the Group Policy Object (GPO) feature:
  1. Open a PCoIP session and press WIN+R to open the **Run** window.
  2. Enter `gpedit.msc` to open the Local Group Policy Editor.
  3. Go to **Computer Configuration** > **Administrative Templates** > **PCoIP Session Variables** > **Not Overridable Administrator Settings**.
  4. Open **Configure PCoIP USB allowed and unallowed device rules**.
  5. Select **Enable**.
  6. Click **Apply**

     NOTE: Enabling the GPO feature in a PCoIP session can be done using both VMware Horizon and Teradici Cloud Access brokers. Third-party vendors do not support USB redirection for Teradici Remote Workstation Card and Amazon WorkSpaces sessions.

Imprivata update

- ThinOS 2205 supports IMP-82-BLE and IMP-82 proximity card readers.
- The Imprivata PIE application support matrix is as follows:

Table 181. Supported and Tested Matrix on ThinOS 2205

ThinOS PIE application	OneSign Server	
	version 7.5.005.25	version 7.7.002.15
7.5.0000.0003.1144	yes	N/A
7.7.0000.0007.1143	N/A	yes

- The log level of PIW is updated in ThinOS 2205 and Wyse Management Suite 3.7, and the levels 4 and 5 are removed. If level 4 or 5 is configured in the previous build, an unexpected string is displayed in the log level drop- down list. It is recommended that you change the log level in Wyse Management Suite or ATP again after ThinOS upgrade.

NOTE: Do not hot plug the card reader as the system stops responding. Plug in the card reader before enabling the Imprivata PIE feature or starting the system.

ThinOS enhancements

- **Added ThinOS Activation devices licenses in Wyse Management Suite**—The licenses must be used in the following two scenarios:
  - Devices that are converted from other operating systems must use the ThinOS activation licenses to enable VDI function. Without the ThinOS activation license, you cannot log in to any Broker agent on the devices. The ThinOS activation licenses are used automatically when registering to Wyse Management Suite.
  - Non-PCoIP ThinOS clients that are upgraded from ThinOS 8.6 can use ThinOS Activation license to enable the PCoIP function. Go to **Services** > **WDA Settings** > **Enable PCoIP Activation License** to enable this option in ThinOS 9.x policy. Restart your device for the function to take effect.

NOTE: Once ThinOS Activation devices licenses are consumed, you cannot restore them. The licenses are permanently applied on the ThinOS clients.

NOTE: If the ThinOS clients are reset to factory default settings, the licenses are not cleared, and the ThinOS clients function as usual.

NOTE: If you recover the ThinOS clients through ISO images or merlin images, the licenses are cleared. You must register the devices to the same Wyse Management Suite server that you used before to reactivate them. ThinOS clients use the original licenses and do not consume new licenses. For Non-PCoIP ThinOS clients, you must also enable **Enable PCoIP Activation License** option in ThinOS 9.x policy to reactivate the licenses.

- **Supports Latitude 3420**

  NOTE: You must have ThinOS Activation devices license for Latitude 3420 to enable VDI function.

  - The following hardware configurations are supported:

Table 182. Hardware configurations that are supported for Latitude 3420

Hardware Type	Hardware
CPU	11th Generation Intel Celeron 6305U, 4 MB Cache, 2 Core, 2 Threads, 1.80 GHz, 15 W
	11th Generation Intel Core i3-1115G4, 6 MB Cache, 2 Core, 4 Threads, 3.0 GHz to 4.10 GHz, 15 W
	11th Generation Intel Core i5-1135G7, 8 MB Cache, 4 Core, 8 Threads, 2.40 GHz to 4.20 GHz, 15 W
	11th Generation Intel Core i5-1145G7, 8 MB Cache, 4 Core, 8 Threads, 2.60 GHz to 4.40 GHz, 15 W
	11th Generation Intel Core i7-1165G7, 12 MB Cache, 4 Core, 8 Threads, 2.80 GHz to 4.70 GHz, 15 W
Memory	4 GB, 1 x 4 GB, DDR4, 3200 MHz
	8 GB, 1 x 8 GB, DDR4, 3200 MHz
	8 GB, 2 x 4 GB, DDR4, 3200 MHz
	16 GB, 1 x 16 GB, DDR4, 3200 MHz
	16 GB, 2 x 8 GB, DDR4, 3200 MHz
Storage	M.2 2230, 128 GB, PCIe NVMe Gen3 x4, Class 35 SSD
	M.2 2230, 256 GB, PCIe NVMe Gen3 x4, Class 35 SSD
	M.2 2230, 512 GB, PCIe NVMe Gen3 x4, Class 35 SSD
	M.2 2280, 256 GB, PCIe NVMe Gen3 x4, Class 40 SSD
	M.2 2280, 1 TB, PCIe NVMe Gen3 x4, Class 40 SSD
Wireless	Intel AX201, 2x2 MIMO, 2.40 Gbps, 2.40 Ghz/5 GHz, Wi-Fi 6 (WiFi 802.11ax), Bluetooth 5.1
Integrated Camera	HD RGB camera
	HD RGB-IR camera
	FHD RGB-IR camera
Display	14 inch, HD 1366 x 768, 60 Hz, nontouch
	14 inch, FHD 1920 x 1080, 60 Hz, nontouch
	14 inch, FHD 1920 x 1080, 60 Hz, touch
Media-card reader	micro-SD 3.0 card

  - The following hardware configurations are not supported for Latitude 3420:

Table 183. Hardware configurations that are not supported for Latitude 3420

Hardware Type	Hardware
Storage	2.5-inch, 1 TB, 5400 RPM, SATA, HDD
	2.5-inch, 500 GB, 7200 RPM, SATA, HDD
Wireless	Qualcomm QCA61x4A, 2x2, MIMO, 867 Mbps, 2.40 Ghz/5 GHz, Wi-Fi 5 (WiFi 802.11ac), Bluetooth 5.0
Discrete GPU	NVIDIA GeForce MX450, 2 GB GDDR5
Ethernet	Integrated Intel WGI219
Fingerprint	Fingerprint on power button
Optional Mobile Broadband Options	Intel XMM 7360 LTE-Advanced (DW5820e) (eSim capable)
	Intel XMM 7360 LTE-Advanced (DW5820e) for Turkey
	Intel XMM 7360 LTE-Advanced (DW5820e) for AT&T, Verizon & Sprint, US
External uSIM card	External uSIM card

- The following hardware configurations are not confirmed whether they support Latitude 3420 or not:

Table 184. Hardware configurations not confirmed about support for Latitude 3420

Hardware Type	Hardware
CPU	10th Generation Intel Core i3-1005G1, 4 MB Cache, 2 Core, 4 Threads, 2.40 GHz to 3.40 GHz, 15 W
Memory	32 GB, 2 x 16 GB, DDR4, 3200 MHz
Storage	M.2 2280, 512 GB, PCIe NVMe Gen3 x4, Class 40 SSD
	M.2 2280, 512 GB, PCIe NVMe Gen3 x4, Intel® Optane™ Storage

- **ThinOS Limitations on Latitude 3420**
  - The integrated microphone is not supported.
  - Dell WD19 docking station and Dell DA310 USB-C Mobile Adapter are not supported.
  - 4K 60Hz display resolution is not supported. Monitors with default resolution 4K 60Hz downgrades to 30Hz, 24Hz, or lower resolution.
  - Type-C port display audio is not supported.
  - Sleep mode is not supported.
- **Camera Update**—Added support for MJPEG format.

  NOTE: If there is no camera in ThinOS or if there is a camera but the **Enable Camera** option is disabled in Admin Policy Tool or Wyse Management Suite, an error message **Camera tab is disabled as no devices are connected/camera permission is disabled** is displayed and the Camera tab is disabled.
- Added the wireless IP address information in the Wi-Fi icon tooltips.
- Added the ability to update the current connected wireless SSID settings from Wyse Management Suite policy. The updated settings take effect after reconnecting.
- Added an eye icon on the **Import your ThinOS configuration** page for WMS Prefix and Group key. Clicking the eye icon can show the masked and unmasked values.
- **Printer setup window update**—On the 5070 extended client, COM1 and COM2 port must not be set as the same Printer Identification for the com printer to work.
- **System Tools update**—Updated the peripherals list description in the **Devices** tab.
- Added support for ELO ET2202L-2UWA-0-BL-G touch screen monitor.
- **Added Wyse Management Suite server drop-down list in ThinOS Central Configuration client menu**—If you change the Wyse Management Suite server to any other server in the dropdown list, the server you entered cannot be saved. The drop-down list includes two items:
  - us1.wysemanagementsuite.com
  - eu1.wysemanagementsuite.com

- **SMB Printer behavior update**—When you log in to a Broker agent, the SMB credentials are taken from the Broker agent login credentials, and these credentials are used for printing.

  ⓘ **NOTE:** The Broker agent sign-in credentials are expected to have priority over Wyse Management Suite credentials.

Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **Enable PCoIP Activation License**—Added **Enable PCoIP Activation License** option in **Services** > **WDA Settings**. This option is disabled by default and must be enabled to enable the PCoIP function on Non-PCoIP Thin clients. Restart your client for the option to take effect. This option consumes your ThinOS Activation devices licenses.
- **Enable On Screen**—The **Enable On Screen** option is disabled by default. Go to **Advanced** > **Session Settings** > **RDP and AVD Session Settings** > **Direct RDP Settings** > **Add Row**. Add the RDP direct connection, enable the **Fullscreen**, and **Enable On Screen** options. Select the monitor number in the **OnScreen** and launch the RDP direct connection. The RDP session displays in this monitor as fullscreen.

  ⓘ **NOTE:** If the monitor number selected in the **OnScreen** list is not on the ThinOS Display window list, the RDP direct session displays fullscreen on the last monitor.
- **Manual Override Camera Device**—Added **Manual Override Camera Device** option, which is disabled by default. Go to **Advanced** > **Peripheral Management** > **Camera** > **Camera Settings** to enable the option. If the option is enabled, the camera that is selected on ThinOS locally takes priority. This prevents the camera settings in the Wyse Management Suit server from overwriting the locally configured camera device until Manual Override is disabled.
- **Default Camera**—Go to **Advanced** > **Peripheral Management** > **Camera** > **Camera Settings** to set the default camera. Use full label, VID:PID, substring, or any valid regex and the setting matches the best available camera label based on available substring. If a default camera is found and manual override is disabled, this setting disables camera selection on the local ThinOS device.
- Added **MJPEG** in the **Camera Format** list.
- **Delay Floatbar Activation in Milliseconds**—You can now change the input value to a range between 70 and 60000. To change the value, go to **Personalization** > **User Experience Settings** > **Delay Floatbar Activation in Milliseconds**
- **Turn Off the Display**—A new option, **Turn Off the Display**, has been added when you go to **Advanced** > **Personalization** > **Screen Saver**. The display turns off after some time and the screen saver is displayed. This option is available for Screen Saver Type Moving Image, Showing Pictures, and Playing Video.
- VNC Service
  - Go to **Advanced** > **Services** > **VNC Service**.
  - Turn on **Enable VNC Daemon** and **Enable VNC Prompt**.
  - Change the default value from **Accept** to **Reject** for the **Select Timeout Type** option.
  - Change the default value from **0** to **10** for the **Timeout** option.

    ⓘ **NOTE:** There is no functional change with this update from the previous ThinOS release.
- **DHCP option 252 enable**—Added **DHCP option 252 enable** in **Network Configuration** > **DHCP Settings**. You can enable or disable the proxy settings from DHCP option 252 using this option.
- Added the BIOS settings page to control the BIOS options for Latitude 3420.

  ⓘ **NOTE:** If you publish the BIOS settings policy through Wyse Management Suite on Latitude 3420, the policy will not sync to Admin Policy Tool. The policy takes effect in BIOS Setup directly.
- Changed the value range to **0-18446744073709551615** minutes in **Broker Settings** > **Citrix Virtual Apps and Desktops Settings** > **Login Expire Time**. **0** means follow server timeout policy.

  ⓘ **NOTE:** This policy only works when logging in to Citrix StoreFront server or Citrix NetScaler server with LDAP authentication.
- **Disable Default Password on Login Console**—Added the **Disable Default Password on Login Console** option in **Login Experience** > **Login Settings**.

  ⓘ **NOTE:** MFA token and Smartcard PIN are not impacted with this option.
- **SMB Printer**—The username field supports special characters in **Peripheral Management** > **Printers** > **SMB Printer**
- The accepted length of Amazon WorkSpaces registration code is updated from 255 to 1023 characters in Wyse Management Suite, Local Admin Policy Tool, and ThinOS.
- **Login Use SmartCard Certification Only**—In **Login Experience** > **Login Settings**, the **Login Use SmartCard Certification Only** option is enabled by default.
- **Enable logging level**—Removed 4, 5 from **Login Experience** > **3rd Party Authentication** > **3rd Party Authentication Settings** > **Enable logging level** drop-down list.

- **Hide On Startup**—Added **Hide On Startup** in **Peripheral Management** > **Mouse**. If you enable this option, mouse pointer will be hidden until you move the mouse, after you reboot the client.

Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

NOTE: The supported peripherals are not limited to the peripherals devices listed in this section.

Table 185. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

Product Category	Peripherals	3040	5070	5470 AIO	5470
Audio Devices	Dell Pro Stereo Headset – UC150 – Skype for Business	Supported	Supported	Not Available	Supported
	Dell Pro Stereo Headset - Skype for Business - UC350	Supported	Supported	Supported	Supported
	Dell Professional Sound Bar (AE515M)	Supported	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Not Available	Supported	Not Available	Not Available
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Not Available	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available

Table 185. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	DellUSB Wired Optical Mouse - MS116	Supported	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Not Available	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Not Available	Supported	Not Available	Supported
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070	Not Available	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI - DBQAUBC064 - DBQAUBC064	Not Available	Supported	Not Available	Not Available

Table 185. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Not Available	Supported	Not Available	Not Available
	Trendnet USB to Serial Converter RS-232	Not Available	Supported	Supported	Supported
	Dell Adapter - HDMI to DVI - DAUARBN004 - DAUARBN004	Not Available	Not Available	Not Available	Supported
	Dell Adapter - HDMI to VGA - DAUBNBC084 - DAUBNBC084	Not Available	Not Available	Not Available	Supported
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232	Not Available	Not Available	Supported	Supported
Displays	E1916H	Supported	Supported	Supported	Not Available
	E2016H	Supported	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported	Supported
	E2216H	Not Available	Supported	Supported	Supported
	E2216Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2218HN	Supported	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported	Supported
	E2318H	Supported	Supported	Supported	Supported
	E2318HN	Not Available	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported	Supported
	E2420HS	Not Available	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported	Supported
	E2720HS	Not Available	Supported	Supported	Supported
	P2016	Not Available	Supported	Not Available	Not Available
	P1917S	Supported	Supported	Not Available	Not Available
	P2017H	Supported	Not Available	Not Available	Not Available
	P2018H	Not Available	Not Available	Not Available	Supported
	P2217	Supported	Supported	Not Available	Not Available
	P2217H	Supported	Supported	Not Available	Not Available
	P2219H	Supported	Supported	Not Available	Supported
	P2219HC	Supported	Supported	Not Available	Supported

Table 185. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	P2317H	Supported	Supported	Not Available	Not Available
	P2319H	Not Available	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Supported	Not Available
	P2417H	Supported	Supported	Not Available	Not Available
	P2418D	Supported	Not Available	Not Available	Not Available
	P2418HT	Supported	Supported	Supported	Not Available
	P2418HZ	Supported	Supported	Not Available	Not Available
	P2419H	Supported	Supported	Supported	Supported
	P2419HC	Supported	Supported	Not Available	Supported
	P2421D	Supported	Supported	Not Available	Supported
	P2421DC	Not Available	Supported	Not Available	Supported
	P2719H	Supported	Supported	Supported	Supported
	P2719HC	Supported	Supported	Not Available	Supported
	P2720D	Supported	Supported	Not Available	Supported
	P2720DC	Not Available	Supported	Not Available	Supported
	P3418HW	Supported	Supported	Supported	Not Available
	P4317Q	Not Available	Supported	Supported	Not Available
	MR2416	Supported	Supported	Not Available	Not Available
	U2415	Supported	Supported	Supported	Not Available
	U2419H	Supported	Supported	Supported	Supported
	U2419HC	Supported	Supported	Not Available	Supported
	U2518D	Supported	Supported	Supported	Not Available
	U2520D	Supported	Supported	Supported	Supported
	U2718Q (4K)	Supported	Supported	Supported	Supported
	U2719D	Supported	Supported	Supported	Supported
	U2719DC	Supported	Supported	Not Available	Supported
	U2720Q	Supported	Supported	Supported	Supported
	U2721DE	Not Available	Supported	Supported	Supported
	U2421HE	Not Available	Not Available	Supported	Supported
	U4320Q	Not Available	Supported	Supported	Supported
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Not Available	Supported
Storage	Dell Portable SSD, USB-C 250GB	Not Available	Supported	Not Available	Supported

Table 185. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell External Tray Load ODD (DVD Writer)	Not Available	Supported	Not Available	Supported
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported	Supported
	Sun microsystem SCR 3311	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Not Available	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Not Available	Supported	Not Available	Supported
Printers	Dell Color Multifunction Printer - E525w	Supported	Not Available	Not Available	Not Available
	Dell Color Printer- C2660dn	Supported	Supported	Not Available	Not Available
	Dell Multifunction Printer - E515dn	Supported	Not Available	Not Available	Not Available

Supported ecosystem peripherals for OptiPlex 3000 Thin Client

ⓘ **NOTE:** The supported peripherals are not limited to the peripherals devices listed in this section.

Table 186. Supported ecosystem peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio Devices	Dell Pro Stereo Headset - Cortez - WH3022
	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Soundbar - AE515M - AE515M - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - AC511M - AC511M - Potential M
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P
	Dell Premier Wireless ANC Headset - Blazer - WL7022
	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Slim Conferencing Soundbar - Lizzo - SB522A
	Dell Speakerphone - Mozart - SP3022

Table 186. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync - 202652-02 - 202652-02
Input Devices	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Bluetooth connection is not supported)
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_GREY - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_WHITE - MS116 - MS116 - Sapphire
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_Grey - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_WHITE - KB216 - KB216 - Rusty
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819 (Fingerprint reader is not supported)
	Dell Wireless Keyboard and Mouse - Auburn MLK - KM3322W
Displays	Dell 22 Monitor - P2222H - P2222H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell 20 Monitor E2020H - E2020H
	Dell 19 Monitor E1920H - E1920H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 23 Monitor - P2319H - P2319H - P2319H

Table 186. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q (Type C to HDMI convertor is not supported)
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 22 Monitor - E2223HN - E2223HN
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - DW316 - Agate - DW316
	Apricorn 1TB Aegis Padlock 256-bit AES Encrypted Hard Drive
	Western Digital My Passport Ultra 1TB , Black - WDBYNN0010BBK-WESN - WDBYNN0010BBK-WESN
Camera	Logitech BRIO 4K Ultra HD Webcam - 960-001105 - 960-001105
	Logitech C525 HD Webcam - 960-000715 - 960-000715
	Logitech C930e HD Webcam - 960-000971 - 960-000971
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

Supported ecosystem peripherals for Latitude 3420

Table 187. Supported ecosystem peripherals for Latitude 3420

Product Category	Peripherals
Displays	Dell 24 Monitor E2420HS - E2420HS
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W ⓘ **NOTE:** Bluetooth connection is not supported.
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
Audio Devices	Dell Pro Stereo Headset - UC150 - UC150 - Lemmy - UC150

Other supported peripherals

Table 188. Other supported peripherals

Product Category	Peripherals
Audio Devices	Jabra BIZ 2400 Duo USB MS
	Jabra EVOLVE UC VOICE 750
	Jabra Evolve 75
	Jabra Engage 75
	Jabra GN2000
	Jabra Pro 9450
	Jabra Speak 510 MS Bluetooth
	Jabra UC SUPREME MS Bluetooth (link 360)
	LFH3610/00 Speechmike Premium (Only supports redirect)
	Logitech S-150
	Logitech h150 - analog
	Nuance PowerMic II (Recommend redirecting whole device)
	Olympus RecMic DR-2200 (Recommend redirecting whole device)
	PHILIPS - analog
	POLYCOM Deskphone CX300
	Plantronics AB J7 PLT
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Blackwire 5220 Series
	Plantronics Blackwire C5210
	Plantronics Calisto P820-M
	Plantronics SAVI W740/Savi W745 (Supports USB only and does not support Bluetooth)
	Plantronics Voyager 6200 UC
	EPOS | SENNHEISER D 10 USB ML-US Wireless DECT Headset
	EPOS | SENNHEISER SC 40 USB MS
	EPOS | SENNHEISER SC 660 USB ML
	EPOS | SENNHEISER SDW 5 BS-EU
	EPOS | SENNHEISER SP 10 ML Speakerphone for Lync
	EPOS | SENNHEISER USB SC230
Input Devices	Bloomberg Keyboard STB 100 - redirect to use function keys
	Dell Keyboard KB212-B
	Dell Keyboard KB216p
	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123

Table 188. Other supported peripherals (continued)

Product Category	Peripherals
	Dell Wireless Keyboard/mouse KM632
	Dell Wireless Mouse - WM126 - black
	Dell wireless Keyboard/mouse KM714
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white
	Microsoft Arc Touch Mouse 1428
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
	Seal Shield Medical Grade Optical Mouse
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white
	SpaceMouse Pro
	SpaceNavigator 3D Space Mouse
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	Dell U2713HM
	Dell U3419W
	Dell U4919DW
	Dell P2715Q
	Dell S2719HS
	Dell S2817Q
	ELO ET2202L-2UWA-0-BL-G
Camera	Jabra PanaCast 4K Webcam
	Logitech C910 HD Pro Webcam
	Logitech C920 HD Pro Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C925e Webcam
	Microsoft LifeCam HD-3000
	Poly EagleEye Mini webcam **NOTE:** Certain resolutions are not supported by some software. You must manually change the resolution to 1280x720 or 1920x1080 in the ThinOS local client.
Storage	Bano type-c 16B
	Kingston DT microDuo 3C 32 GB
	Kingston DTM30 32 GB
	Kingston DataTraveler G3 8 GB
	SanDisk Cruzer 16 GB
	SanDisk Cruzer 8 GB

Table 188. Other supported peripherals (continued)

Product Category	Peripherals
	SanDisk USB 3.1 and Type-C 16 GB
	SanDisk Ultra Fit 32 GB
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Dell Keyboard SK-3205 with smart card reader
	GemPC Twin
	Gemalto IDBridge CT710
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	IDBridge CT31 PIV
	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	SmartOS powered SCR3310
	SmartOS powered SCR335
Proximity card readers	RFIDeas RDR-6082AKU
	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80
	Imprivata HDW-IMP-82
	Imprivata HDW-IMP-82-BLE
	OMNIKEY 5025CL
	OMNIKEY 5326 DFR
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM
	OMNIKEY 5325 CL
	KSI-1700-SX Keyboard
Fingerprint readers	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader

Table 188. Other supported peripherals (continued)

Product Category	Peripherals
	Imprivata HDW-IMP-1C
	KSI-1700-SX Keyboard
Printers	Brother DCP-7190DW—works on Citrix only but not Blast
	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer
	Dell B2360d Laser Printer
	Dell B2360dn Laser Printer
	HP Color LaserJet CM1312MFP
	HP LaserJet P2055d
	HP M403D— works on Citrix only but not Blast
	Lexmark X864de- tested on LPD only
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR—BLEdongle
Teradici remote cards	Teradici host card 2220
	Teradici host card 2240
Others	Intuos Pro Wacom
	Wacom One

Supported smart cards

Table 189. Supported smart cards

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	G&D SCE 3.2
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Giesecke and Devrient SmartCafe Expert 7.0 (T=0)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840
ID Prime MD v 4.0.2 (Gemalto 840)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B

Table 189. Supported smart cards (continued)

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K
ID Prime MD v 4.1.3 (Gemalto 3811)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940
Etoken Java (aladdin)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.0 T=0/1 0V300
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_6.1.6	cv act sc/interface CSP	Giesecke & Devrient StarCos 3.2
N/A (Buypass BelDu)	Net iD 6.8.3.21, 2.0.48	Net iD - CSP	BelDu 6.0.4
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.3.21, 2.0.48	Net iD - CSP	IDPrime SIS 4.0.2
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)

Tested environments matrix

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

Table 190. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.7 458
Configuration UI package for Wyse Management Suite	1.8 133
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 191. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2112	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2203LTSR	Tested	Tested	Tested	Tested

Table 192. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Tested	Not tested	Not tested
VMware Horizon 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Tested	Tested	Tested—Only basic connection is tested on Ubuntu 20.04

Table 193. Test environment – VMware Horizon Cloud

Horizon Cloud	Windows 10	Windows Server 2016
Build Version: 19432376	Horizon Agent Installer - 21.3.0.19265453	Horizon Agent Installer - 21.3.0.19265453

Table 194. Test environment—Microsoft RDP

Microsoft RDP	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
Remote Desktop Services 2016	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2019	Not tested	Tested	Not tested	Not tested	Not tested	Tested	Tested

Table 195. Test environment—AVD

Azure Virtual Desktop	Windows 7	Windows 10	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	APPs
2019 (MS-Prod)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested
2020 (ARMv2)	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Tested

Table 196. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	2.9.400	2.9.400	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				

Table 197. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 198. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10	14.1.0.306686.4	14.1.0	14.1.0
	Windows server 2016			
	Windows server 2019			

Table 199. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	14.1.0.306686_4	14.1.0.56686	14.1.0.306686_4
	Windows server 2016	14.1.0.306686_4	14.1.0.56686	14.1.0.306686_4
	Windows server 2019	14.1.0.306686_4	14.1.0.56686	14.1.0.306686_4

Table 199. Tested environment—JVDI (continued)

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon View 7.13.2				

Table 200. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10 Windows server 2016 Windows server 2019	5.9.6.20931.7	5.9.6(20931)

Table 201. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106 VMware Horizon View 7.13.2	Windows 10 Windows server 2016 Windows server 2019	5.9.6.20931.7	5.9.6(20931)

Table 202. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112 Citrix Virtual Apps and Desktops 7 2203 LTSR	Windows 10 Windows server 2016 Windows server 2019	41.12.0.20899.3	41.12.0.20899.3

Table 203. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111 VMware Horizon View 7.13.2	Windows 10 Windows server 2016 Windows server 2019	41.12.0.20899.3	41.12.0.20899.3

Table 204. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10 Windows server 2016 Windows server 2019	42.2.6.11.3	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6.

Table 204. Tested environment—Cisco Webex Meetings (continued)

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 2203 LTSR			

Table 205. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106	Windows 10	42.2.6.11.3	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 42.2 to 42.6. Webex Meeting does not work well with Horizon 2111. This is a Cisco limitation.
	Windows server 2016		
	Windows server 2019		

Fixed issues

Table 206. Fixed issues

Issue ID	Description
DTOS-9317	The second monitor cannot be set as primary monitor after upgrading to ThinOS 9.1.6 on Wyse 5470—CIPS-26502.
DTOS-9316	Proxy settings do not work with the new firmware—CIPS-26370.
DTOS-9065	Citrix Account Lockout does not work in ThinOS 9.1.6108 on Wyse 5070—CIPS-26455.
DTOS-9047	Citrix published application opening with scroll bars in ThinOS 9.1.6108 on Wyse 3040—CIPS-26263.
DTOS-9030	Direct RDP connection on-screen feature is missing on ThinOS 9.x—CIPS-26377.
DTOS-9026	Integrated webcam redirection causes RDS session to stop responding in Thin OS 9.1.6108—CIPS-26452.
DTOS-8997	Auto-Suggestions or Predictive Typing causes typing to pause in ThinOS 9.1.6108 on Wyse 5070—CIPS-26399.
DTOS-8993	Ctrl + Y key combination does not work in Microsoft Office application in ThinOS 9.1.
DTOS-8819	Unable to hide the floatbar—CIPS-26294.
DTOS-8720	BIOS update through Wyse Management Suite fails—CIPS-26321.
DTOS-8644	Citrix sessions resume on one screen only when screen saver is enabled—CIPS-26240.
DTOS-8634	NetScaler client certificate authentication does not work in ThinOS 9.1.6108—CIPS- 26213.
DTOS-8627	CWA package download fails on slow network connections in ThinOS 9.1.6108—CIPS-26234.
DTOS-8625	PCoIP disconnects randomly—CIPS-26287.
DTOS-8600	Black screen issue while connecting to VMware Blast Session in ThinOS 9—CIPS-26245.
DTOS-8563	Issue with SSID in Wyse Management Suite policy—CIPS-26223.
DTOS-8435	Monitor arrangement issue after updating to ThinOS 9.1.6108—CIPS-26219.
DTOS-8205	Manual override settings for wireless connections are not saved after reboot in ThinOS 9.1.6108—CIPS-26168.
DTOS-8141	Mouse wheel scrolling issue in AVD when set to one line—CIPS-25943.
DTOS-8125	Issue with automatic wireless certificate update on ThinOS 9.1.6—CIPS-26054.

Table 206. Fixed issues (continued)

Issue ID	Description
DTOS-8116	After factory reset, the Wyse Management Suite server is not picked up in ThinOS 9.1.6108—CIPS-26128.
DTOS-8052	Cannot resolve hostname—CIPS- 26127.
DTOS-8051	User has to know that pressing Esc button refreshes the connection and brings back the web-based login page in ThinOS 9.1.1—CIPS-26098.
DTOS-8050	The MFA login page is truncated, and user has to maximize or increase the size of the web-based login window in ThinOS 9.1.1—CIPS-26099.
DTOS-8049	The company logo disappears in the login window while switching between subgroups in ThinOS 9.1.1—CIPS-26095.
DTOS-7940	User accounts are locked after one wrong password attempt—CIPS-26033.
DTOS-7930	Imprivata login issues in ThinOS 9.1.6108 on Wyse 3040—CIPS-26012.
DTOS-7900	Manual Overwrite feature does not work when using WiFi and Wyse Management Suite Select group is used in ThinOS 9.1.6108 on Wyse 5470—CIPS-26007.
DTOS-7862	Latency Issues with Cerner applications—CIPS-26016.
DTOS-7817	If domain forces NTLMv2 authentication in ThinOS 9.1.x., SCEP does not work.
DTOS-7796	Monitor sleep mode is not available on ThinOS 9.1—CIPS-25909.
DTOS-7795	SCEP admin username and password in ThinOS 9.1 with NTLMv1 is not pulling the enrollment password—CIPS-25955.
DTOS-7709	Device does not save credentials in Citrix sessions that go beyond 18-21 hours—CIPS-25849.
DTOS-7708	Alt + Left or Right arrow does not function in Citrix published applications in ThinOS 9.1.5067.
DTOS-7706	VNC double input within direct RDP full HD session—CIPS-25928.
DTOS-7650	Last user is not reporting correctly in Wyse Management Suite in WMS Public Cloud 3.3.1 29.
DTOS-7537	Desktop Scale Factor does not work while configuring locally in ThinOS 9.1.4234—CIPS-24799.
DTOS-7518	Mouse pointer issue in PCoIP sessions—CIPS-25729.
DTOS-7513	Mouse pointer always appears on device desktop—CIPS-25770.
DTOS-7454	Ping tests and connection requests fail on WTOS9.0+ when using Windows NLB in Multicast mode.
DTOS-7437	Issue with Direct External Connection to the NetScaler/ADC double authentication—CIPS-25673.
DTOS-7411	System shows RTME optimization activating and deactivating sporadically—CIPS-25662.
DTOS-7395	F4 key does not lock Imprivata session—CIPS-22691.
DTOS-7392	Random reboot issues while connected to Citrix session on Wyse 5470—CIPS-25691.
DTOS-7315	Support for multiple audio devices in ThinOS—CIPS-25666.
DTOS-7232	DHCP Lease Expiration causes the session to disconnect in ThinOS 9.1.5067 on Wyse 5070—CIPS-25516.
DTOS-6963	Kiosk account logs out instead of locking—CIPS-22691.
DTOS-6950	Issue with mouse performance using Blast—CIPS-22201.
DTOS-6940	If username contains special characters, AVD login fails.

Table 206. Fixed issues (continued)

Issue ID	Description
DTOS-6828	Imprivata 2FA authentication issues in ThinOS 9.1.4234—CIPS-24367.
DTOS-6777	Webcam redirection in Azure RDP session stops responding—CIPS-25172.
DTOS-5835	When setting **Default Broker Type** to **Citrix**, entering the broker server URL, and Citrix Workspace mode is enabled, Wyse 5470 stops responding with an autologin loop—CIPS-24524.
DTOS-5436	RDP Session fails to launch in ThinOS 9.x—CIPS-22368.
DTOS-5174	Sign On credentials are not sent to the SMB printer setup—CIPS-24113.
DTOS-7322	OnScreen setting for direct RDP connections is missing for ThinOS 9.x firmware—CIPS-25350.
DTOS-8739	RDP session stops responding with odd cursor in ThinOS 9.1.6108 with AVD version 1.6.1402.
DTOS-6979	Odd cursor behavior in Microsoft Excel in PCOIP session with ThinOS 9.1—CIPS-24713.

Known issues

Table 207. Known issues

Issue ID	Description	Workaround
DTOS-9729	The autofill USB printer identification value is incorrect.	Remove the vid:0xxxxx pid:0xxxxx manually or push the printer settings with correct printer identification from Wyse Management Suite server. Or, you can reset the client to factory default settings first and then plug in the printer
DTOS-9697	You have to enter the password twice when connecting to a VPN server that uses a self-signed certificate.	There is no workaround in this release.
DTOS-9603	In Citrix, the window display size is incorrect when you restore the window after maximizing Notepad.	There is no workaround in this release.
DTOS-9477	Blast VDI session in window mode shows two mouse pointers when you maximize.	Workaround is to launch the Blast session in full screen
DTOS-9421	BIOS update on Latitude 3420 with low battery and not connected to power source fails and cannot be updated again.	A future BIOS update will fix this issue.
DTOS-9378	Copy and Paste functionality between Citrix HDX Desktop and RDP sessions do not work.	There is no workaround in this release.
DTOS-9286	Two black lines appear on-screen when screen sharing during Cisco JVDI calls.	There is no workaround in this release.
DTOS-9073	When connecting RDS PC session in Imprivata PIE, you cannot open the certificate information after clicking **View Certificate**.	There is no workaround in this release.
DTOS-9035	You cannot add jabra.ini from APT.	Add jabra.ini from Wyse Management Suite.
DTOS-9014	PIE is stuck on the Onesign background after signing off Citrix session on Latitude 3420.	Reboot the client.
DTOS-8995	Type C to HDMI adapter does not work on ThinOS.	Do not use the convertor; connect to the monitor directly.

Table 207. Known issues (continued)

Issue ID	Description	Workaround
DTOS-8982	Wyse 5470 Mobile Thin Client restarts when you connect two external 4 K monitors with a dock.	Dell WD19 dock supports only one 4K 30 Hz or two 1920x1080 resolution monitors. Connect one monitor, change its resolution to 1920x1080 first, and then connect the next.
DTOS-8969	Horizon VDI session window does not display on 4 K external monitor, which is being used as the main monitor, in Span mode.	Do not change the primary monitor to secondary monitor.
DTOS-8924	Blast session is not disconnected after removing the smart card with **Kill session** smartcard setting.	There is no workaround in this release.
DTOS-8831	VDI session is not launched after clicking **Connect** but VDI details are displayed in Blast configuration settings and active session dialog box is also displayed while signing off the Broker agent.	Reboot the client.
DTOS-8766	Connect the external monitor to Latitude 3420 to play video and the external monitor flashes.	Use other display resolutions as this issue occurs only on 3840x1600.
DTOS-8598	The display resolution is not shown from Latitude client to the external touch screen monitor when connected with a dock.	Do not use the dock.
DTOS-8579	DisplayPort audio through Type-C does not work on Latitude 3420.	There is no workaround in this release.
DTOS-8572	While sharing the screen during Cisco Webex Teams meeting in VDI session, an additional window is displayed in the Modern mode and Classic mode toolbar.	An additional window is displayed that does not affect the functionality.
DTOS-8510	In a dual monitor setup, the second monitor is black when moving windows to it.	Do not use Type-C cable to connect this monitor. Use DisplayPort cable instead.
DTOS-8136	The prefix https/http is case-sensitive in Citrix and VMware Broker agent server URL field.	Use lowercase for the prefix https and http in VDI Broker agent server URL field.
DTOS-7190	After the client restarts, the Bluetooth device is connected again, but the connection status that is displayed is incorrect.	Reconnect the device to show the status correctly. There is no impact to functionality.
DTOS-7189	Added AllowAudioInput, which is used to control HDX webcam redirection to APT/Wyse Management Suite VDI setting block list.	This is a Citrix HDX webcam redirection feature that is enabled for 32-bit applications by default. You do not have to change any setting in Admin policy tool or Wyse Management Suite.
DTOS-8521	After hot plugging Wyse 5070, one external monitor displays a black screen after restarting both the monitors.	There is no workaround in this release.
DTOS-10296	Poly EagleEye Mini webcam does not work with some resolutions.	Disable Optimize for CPU and set resolution to 1280x720 or 1920x1080.

11

Resources and support

Accessing documents using the product search

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, `Wyse 3040 thin client` or `Wyse ThinOS`. A list of matching products is displayed.
3. Select your product.
4. Click **Documentation**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to www.dell.com/support.
2. Click **Browse all products**.
3. Click **Thin Clients**.
4. Click the desired category, either **Wyse Hardware** or **Wyse Software**.
5. Click the desired product.
6. Click **Documentation**.

12

Contacting Dell

Prerequisites

ⓘ **NOTE:** If you do not have an active internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

About this task

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell sales, technical support, or customer service issues:

Steps

1. Go to www.dell.com/support.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.