

# **Dell ThinOS 2311, 2308, 2306, and 2303**

## Release Notes



## 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.

<b>Chapter 1: Overview</b> .....	<b>9</b>
<b>Chapter 2: Version matrix</b> .....	<b>10</b>
<b>Chapter 3: ThinOS 2311 (9.4.4130)</b> .....	<b>12</b>
Release details.....	12
ThinOS application and BIOS package details.....	12
Tested BIOS versions .....	13
What's new.....	13
<b>Chapter 4: Citrix Workspace App 2309 for ThinOS 2311</b> .....	<b>15</b>
Release date.....	15
Release summary.....	15
Current version.....	15
Previous version.....	15
Supported application package, firmware, and systems.....	15
Supported application package .....	15
Supported Firmware.....	15
Upgrade the application package using Wyse Management Suite.....	16
Citrix Workspace App updates.....	16
<b>Chapter 5: ThinOS 2311 (9.4.4123)</b> .....	<b>18</b>
Release date.....	18
Release summary.....	18
Current version.....	18
Previous version.....	18
Firmware upgrade.....	18
Important notes.....	18
Prerequisites for firmware upgrade.....	19
Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite.....	19
Convert Ubuntu with DCA to ThinOS 2311 (9.4.4123).....	20
ThinOS application package details.....	21
BIOS packages.....	22
Tested BIOS versions.....	23
New updates.....	23
<b>Chapter 6: VMware Horizon Client 2309 and Zoom Horizon 5.16 packages for ThinOS 2311</b> .....	<b>24</b>
Release date.....	24
Release summary.....	24
Current version.....	24
Previous versions.....	24
Tested BIOS versions.....	25
Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite.....	25
VMware Horizon feature matrix.....	25

New features.....	31
VMware Horizon Updates.....	31
Tested environment matrix.....	31

**Chapter 7: ThinOS 2311 (9.4.4106) ..... 33**

Release date.....	33
Release summary.....	33
Current version.....	33
Previous version.....	33
Firmware upgrade.....	33
Important notes.....	33
Prerequisites for firmware upgrade.....	36
Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite.....	36
Convert Ubuntu with DCA to ThinOS 2311.....	36
Compatibility.....	38
ThinOS application package details.....	38
Wyse Management Suite and Configuration UI package.....	39
ThinOS build details.....	39
Tested BIOS version for ThinOS 2311.....	40
Citrix Workspace app feature matrix.....	40
ThinOS AVD Client Feature Matrix.....	51
VMware Horizon feature matrix.....	52
New and enhanced features.....	57
Citrix Workspace app updates.....	57
Microsoft RDP and AVD.....	58
Teradici PCoIP.....	59
VMware Horizon Updates.....	59
Identity Automation updates.....	59
Cisco WebEx Meetings VDI update .....	59
Cisco Webex VDI update.....	59
Zoom.....	60
ControlUp.....	60
Systancia Workplace Broker.....	60
ThinOS enhancements.....	61
Updates to Admin Policy Tool and Wyse Management Suite policy settings.....	63
Tested environments matrix.....	64
Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO.....	68
Supported ecosystem peripherals for OptiPlex 3000 Thin Client.....	73
Supported ecosystem peripherals for Latitude 3420.....	75
Supported ecosystem peripherals for OptiPlex 5400 All-in-One.....	76
Supported ecosystem peripherals for Latitude 3440.....	76
Supported ecosystem peripherals for Latitude 5440.....	76
Supported ecosystem peripherals for OptiPlex All-in-One 7410.....	77
Supported ecosystem peripherals for OptiPlex All-in-One 7420.....	77
Third-party supported peripherals.....	77
Supported smart cards.....	81
Fixed Issues.....	83
Known Issues.....	85

<b>Chapter 8: Citrix Workspace App 2308 for ThinOS 2308.....</b>	<b>86</b>
Release date.....	86
Release summary.....	86
Current version.....	86
Previous version.....	86
Supported application package, firmware, and systems.....	86
Supported application package .....	86
Supported Firmware.....	86
Upgrade the application package using Wyse Management Suite.....	87
Citrix Workspace app feature matrix.....	87
Citrix Workspace app updates.....	99
Tested environments matrix.....	99
<b>Chapter 9: ThinOS 2308.....</b>	<b>102</b>
Release date.....	102
Release summary.....	102
Current version.....	102
Previous version.....	102
Firmware upgrade.....	102
Important notes.....	102
Prerequisites for firmware upgrade.....	105
Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite.....	105
Convert Ubuntu with DCA to ThinOS 2308.....	105
Compatibility.....	107
ThinOS application package details.....	107
Wyse Management Suite and Configuration UI package.....	108
ThinOS build details.....	108
Tested BIOS version for ThinOS 2308.....	108
Citrix Workspace app feature matrix.....	109
ThinOS AVD Client Feature Matrix.....	120
VMware Horizon feature matrix.....	121
New and enhanced features.....	126
Citrix Workspace app updates.....	126
Teradici PCoIP.....	127
VMware Horizon Updates.....	127
Imprivata updates.....	128
Cisco WebEx Meetings VDI update .....	129
Cisco Webex VDI update.....	129
Zoom.....	129
RingCentral.....	129
ControlUp.....	129
Common Printing.....	129
ThinOS enhancements.....	129
Updates to Admin Policy Tool and Wyse Management Suite policy settings.....	130
Tested environments matrix.....	130
Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO.....	134
Supported ecosystem peripherals for Latitude 3420.....	139
Supported ecosystem peripherals for Latitude 3440.....	140

Supported ecosystem peripherals for Latitude 5440.....	140
Supported ecosystem peripherals for OptiPlex 3000 Thin Client.....	140
Supported ecosystem peripherals for OptiPlex 5400 All-in-One.....	143
Supported ecosystem peripherals for OptiPlex All-in-One 7410.....	143
Third-party supported peripherals.....	143
Supported smart cards.....	147
Fixed Issues.....	149
Known Issues.....	151

**Chapter 10: ThinOS 2306..... 153**

Release date.....	153
Release summary.....	153
Current version.....	153
Previous version.....	153
Firmware upgrade.....	153
Important notes.....	153
Prerequisites for firmware upgrade.....	156
Upgrade from ThinOS 9.1.x to later versions using Wyse Management Suite.....	156
Convert Ubuntu with DCA to ThinOS 2306.....	156
Convert Windows 10 IoT to ThinOS 2306.....	158
Convert ThinLinux to ThinOS 2306.....	159
Compatibility.....	160
ThinOS application package details.....	160
Wyse Management Suite and Configuration UI package.....	161
ThinOS build details.....	161
Tested BIOS version for ThinOS 2306.....	162
Citrix Workspace app feature matrix.....	162
ThinOS AVD Client Feature Matrix.....	173
VMware Horizon feature matrix.....	174
New and enhanced features.....	179
Citrix Workspace app updates.....	179
Microsoft RDP and AVD.....	182
Teradici PCoIP.....	183
VMware Horizon Updates.....	184
Imprivata updates.....	185
Cisco WebEx Meetings VDI update .....	185
Cisco Webex VDI update.....	185
Zoom.....	185
RingCentral.....	186
Avaya agent.....	186
ControlUp.....	186
Liquidware.....	186
ThinOS enhancements.....	186
Updates to Admin Policy Tool and Wyse Management Suite policy settings.....	190
Tested environments matrix.....	192
Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO.....	195
Supported ecosystem peripherals for Latitude 3420.....	200
Supported ecosystem peripherals for Latitude 3440.....	201
Supported ecosystem peripherals for Latitude 5440.....	201
Supported ecosystem peripherals for OptiPlex 3000 Thin Client.....	202

Supported ecosystem peripherals for OptiPlex 5400 All-in-One.....	204
Supported ecosystem peripherals for OptiPlex All-in-One 7410.....	204
Third-party supported peripherals.....	205
Supported smart cards.....	208
Fixed Issues.....	211
Security fixes.....	213
Known Issues.....	213
<b>Chapter 11: Cisco Webex Meetings VDI 43.2 and Cisco Webex VDI 43.2 for ThinOS 2303.....</b>	<b>215</b>
Release summary.....	215
Supported platforms.....	215
Important notes.....	215
Installing the application package.....	216
Download the application package.....	216
Install the application package using Wyse Management Suite.....	216
Compatibility.....	216
Application package information.....	216
Previous versions.....	216
Cisco Webex Meetings VDI updates.....	217
Cisco Webex Meetings VDI feature matrix.....	217
Cisco Webex Meetings VDI limitations.....	218
Cisco Webex VDI update.....	218
Cisco Webex VDI feature matrix.....	218
Cisco Limitations.....	220
New and enhanced features.....	220
Tested environments matrix.....	220
<b>Chapter 12: ThinOS 2303.....</b>	<b>222</b>
Release date.....	222
Release summary.....	222
Current version.....	222
Previous version.....	222
Firmware upgrade.....	222
Important notes.....	222
Prerequisites for firmware upgrade.....	223
Upgrade from ThinOS 9.1.x to ThinOS 2303 using Wyse Management Suite.....	223
Convert Ubuntu with DCA to ThinOS 2303.....	224
Compatibility.....	225
ThinOS application package details.....	225
Wyse Management Suite and Configuration UI package.....	226
ThinOS build details.....	226
Tested BIOS version for ThinOS 2303.....	226
Citrix Workspace app feature matrix.....	227
ThinOS AVD Client Feature Matrix.....	236
VMware Horizon feature matrix.....	237
New and enhanced features.....	243
Citrix Workspace app updates.....	243
Microsoft RDP and AVD.....	245
Teradici PCoIP update.....	246

Horizon Blast Updates.....	246
Support for other brokers.....	248
Imprivata updates.....	250
Identity Automation.....	251
Cisco Webex Meetings VDI updates.....	251
Cisco Webex VDI update.....	251
Cisco Jabber.....	251
Zoom.....	251
RingCentral.....	251
ControlUp.....	251
ThinOS enhancements.....	251
Updates to Admin Policy Tool and Wyse Management Suite policy settings.....	257
Tested environments matrix.....	261
Supported ecosystem peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO.....	265
Supported ecosystem peripherals for Latitude 3420.....	270
Supported ecosystem peripherals for Latitude 3440.....	270
Supported ecosystem peripherals for Latitude 5440.....	271
Supported ecosystem peripherals for OptiPlex 3000 Thin Client.....	271
Supported ecosystem peripherals for OptiPlex 5400 All-in-One.....	274
Supported ecosystem peripherals for OptiPlex All-in-One 7410.....	274
Third-party supported peripherals.....	274
Supported smart cards.....	278
Fixed issues.....	279
Known issues.....	282

**Chapter 13: Resources and support..... 284**

**Chapter 14: Contacting Dell.....285**



# 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 that are supported in each Dell ThinOS release. The matrix helps you select which version of ThinOS software or ThinOS application package is appropriate for your work environment.

**Table 1. Version Matrix**

Application package versions	Release date	Supported platforms	Release Notes
ThinOS 2311	March 2024 / January 2024 / November 2023	<ul style="list-style-type: none"> <li>• Wyse 3040 Thin Client</li> <li>• Wyse 5070 Thin Client</li> <li>• Wyse 5470 Thin Client</li> <li>• Wyse 5470 All-in-One Thin Client</li> <li>• OptiPlex 3000 Thin Client</li> <li>• Latitude 3420</li> <li>• OptiPlex 5400 All-in-One</li> <li>• Latitude 3440</li> <li>• Latitude 5440</li> <li>• Latitude 5450</li> <li>• OptiPlex All-in-One 7410</li> <li>• OptiPlex All-in-One 7420</li> </ul>	ThinOS 2311 (9.4.4130) / ThinOS 2311 (9.4.4123) / ThinOS 2311 (9.4.4106)

**Table 2. Version Matrix**

Application package versions	Release date	Supported platforms	Release Notes
ThinOS 2308 (9.4.3087)	August 2023	<ul style="list-style-type: none"> <li>• Wyse 3040 Thin Client</li> <li>• Wyse 5070 Thin Client</li> <li>• Wyse 5470 Thin Client</li> <li>• Wyse 5470 All-in-One Thin Client</li> <li>• OptiPlex 3000 Thin Client</li> <li>• Latitude 3420</li> <li>• OptiPlex 5400 All-in-One</li> <li>• Latitude 3440</li> <li>• Latitude 5440</li> <li>• OptiPlex All-in-One 7410</li> </ul>	ThinOS 2308

**Table 3. Version Matrix**

Application package versions	Release date	Supported platforms	Release Notes
ThinOS 2306 (9.4.2103)	June 2023	<ul style="list-style-type: none"> <li>• Wyse 3040 Thin Client</li> <li>• Wyse 5070 Thin Client</li> <li>• Wyse 5470 Thin Client</li> <li>• Wyse 5470 All-in-One Thin Client</li> <li>• OptiPlex 3000 Thin Client</li> <li>• Latitude 3420</li> <li>• OptiPlex 5400 All-in-One</li> <li>• Latitude 3440</li> <li>• Latitude 5440</li> <li>• OptiPlex All-in-One 7410</li> </ul>	ThinOS 2306

**Table 4. Version Matrix**

<b>Application package versions</b>	<b>Release date</b>	<b>Supported platforms</b>	<b>Release Notes</b>
ThinOS 2303 (9.4.1141)	March 2023	<ul style="list-style-type: none"><li>● Wyse 3040 Thin Client</li><li>● Wyse 5070 Thin Client</li><li>● Wyse 5470 Thin Client</li><li>● Wyse 5470 All-in-One Thin Client</li><li>● OptiPlex 3000 Thin Client</li><li>● Latitude 3420</li><li>● OptiPlex 5400 All-in-One</li><li>● Latitude 3440</li><li>● Latitude 5440</li><li>● OptiPlex All-in-One 7410</li></ul>	<a href="#">ThinOS 2303</a>

# ThinOS 2311 (9.4.4130)

## Release details

### Release date

March 2024

### 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 2311 (9.4.4130)

## ThinOS application and BIOS package details

For ThinOS 9.4.4130, it is recommended to install the latest application packages from the below table.

**Table 5. ThinOS application package details**

ThinOS application package details
Cisco_Jabber_14.2.0.308051.8.pkg
Cisco_WebEx_Meetings_VDI_43.10.2.11.2.pkg
Cisco_WebEx_VDI_43.10.0.27605.1.pkg
Citrix_Workspace_App_23.9.0.24.11.pkg
Common_Printing_1.0.0.26.pkg
ControlUp_VDI_Agent_2.2.5.pkg
EPOS_Connect_7.7.0.2.pkg
HID_Fingerprint_Reader_210217.24.pkg
Identity_Automation_QwickAccess_2.0.4.1.6.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.5.6.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.6.2.4.3.pkg
Microsoft_AVD_2.3.2266.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_23.06.2.18.pkg
VMware_Horizon_2306.8.10.0.21964631.5 .pkg

**Table 5. ThinOS application package details (continued)**

ThinOS application package details
VMware_Horizon_ClientSDK_2306.8.10.0.21964631.20.pkg
Zoom_AVD_5.16.0.24280.1.pkg
Zoom_Citrix_5.16.0.24280.1.pkg
Zoom_Horizon_ 5.15.2.23760.3.pkg

## Tested BIOS versions

The following table contains the tested BIOS version for ThinOS 9.4.4130.

**Table 6. Tested BIOS versions**

Supported platform	Tested BIOS version
Dell Latitude 5450	1.0.2

## What's new

Supports new platform Latitude 5450.

**Table 7. Supported hardware configurations for Latitude 5450**

Product Category	Peripherals
CPU	Intel Core i3-1315U
	Intel Core i5-1335U
	Intel Core i5-1345U
	Intel Core Ultra 5 125U
	Intel Core Ultra 5 135U
	Intel Core Ultra 5 125H
	Intel Core Ultra 5 135H
Memory	8 GB x 1
	8 GB x 2
	16 GB x 1
	16 GB x 2
Storage	M.2 2230 - 256G
	M.2 2230 - 512G
Camera	FHD RGB
	FHD IR
	FHD IR with EMZA
Wireless	Intel AX211
Display	FHD 250 nit
	FHD 400 nit
	FHD Touch 300 nit
Smart Card reader slot	Smart Card reader only

**Table 8. Hardware configurations not supported on Latitude 5450**

<b>Product Category</b>	<b>Peripherals</b>
Discrete GPU	NVIDIA Graphics
Storage	SED storage
Wireless	Realtek Wireless
Fingerprint	Fingerprint on power button
NFC or Contactless smart card reader	NFC or Contactless smart card reader
WWAN	WWAN

# Citrix Workspace App 2309 for ThinOS 2311

## Release date

February 2024

## 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

Citrix\_Workspace\_App\_23.9.0.24.11.pkg


## Previous version

Citrix\_Workspace\_App\_23.9.0.24.4.pkg

## Supported application package, firmware, and systems

### Supported application package

Citrix\_Workspace\_App\_23.9.0.24.11.pkg

 **NOTE:** For information about other packages, see ThinOS application package details in the [ThinOS 2311 \(9.4.4123\) Release Notes](#).

### Supported Firmware


ThinOS 2311 (9.4.4123)

**Table 9. Supported systems**

Platform model
Wyse 3040 Thin Client
Wyse 5070 Thin Client
Wyse 5470 All-in-One Thin Client
Wyse 5470 Mobile Thin Client
Dell OptiPlex 3000 Thin Client
Dell Latitude 3420

**Table 9. Supported systems (continued)**

Platform model
Dell OptiPlex 5400 All-in-One
Dell Latitude 3440
Dell Latitude 5440
Dell OptiPlex All-in-One 7410
Dell OptiPlex All-in-One 7420

 **NOTE:** Upgrade the ThinOS firmware to ThinOS 2311 (9.4.4123) before installing the application packages.

## Upgrade the application package using Wyse Management Suite

### Prerequisites

- Ensure that you are running ThinOS 2311 (9.4.4123) 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.

### 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**.
5. Click **Application Package Updates**

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

6. Click **Browse** and select the new version of the ThinOS package to upload.
7. From the **Citrix Workspace App** list, select the uploaded ThinOS package from the dropdown list.
8. Click **Save & Publish**.  
The thin client downloads the package, installs it, and then restarts. The firmware version is upgraded.

## Citrix Workspace App updates

Citrix Workspace App package version is updated to 23.9.0.24.11.

## Removed the Authentication using FIDO2 when connecting to on-premises stores feature

- The **Authentication using FIDO2 when connecting to on-premises stores** option is removed in the Citrix Workspace App 23.9.0.24.11 package to avoid the Citrix Enterprise Browser (CEB) security issue in ThinOS.
- If you enable **WebLogin Use External Browser** with **CEB** value in **External Browser Type** from Admin Policy Tool or Wyse Management Suite policy, ThinOS cannot log in to the Citrix broker using FIDO2 authentication.

## Limitation

If you have installed Citrix Jabber with Citrix Workspace App 23.9.0.24.4 and upgraded to Citrix Workspace App 23.9.0.24.11, the Citrix multiple audio feature is enabled. But, Cisco JVDI does not support the Citrix multiple audio feature.



**Workaround:** To disable the feature, uninstall and reinstall the Citrix Jabber package.

# ThinOS 2311 (9.4.4123)

## Release date

January 2024

## 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

### Release Name

ThinOS 2311 (9.4.4123)

### Release Build

ThinOS\_2311\_9.4.4123.pkg

### Ubuntu 20.04 to ThinOS 2311 conversion build

ThinOS\_2311\_9.4.4123\_Ubuntu\_Conversion.zip

## Previous version

ThinOS 2311 (9.4.4106)

## Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2311 (9.4.4123)**

## Important notes

- If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2311. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.
- If you want to downgrade ThinOS 2311 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.
- If you are using small disk devices like Wyse 3040 with 8 GB, it is recommended that the operating system firmware and application packages be upgraded in separate steps. Upgrading them simultaneously may cause upgrade failures due to insufficient disk space. If you still fail to upgrade the operating system firmware and application packages, uninstall some application packages to free disk space and try again.

- There are chances that after the upgrade, the device displays a black screen. 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.

**NOTE:** From ThinOS 2303, **Live Update** is disabled, but the thin client can download the operating system firmware and BIOS firmware in the background. However, the thin client cannot complete installation 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 turn on the thin client from a turn off state
- When you change the Wyse Management Suite group
- When a new firmware or an application notification is displayed on your thin client and if you click **Next Reboot**, the following is observed:
  - If you have changed the Wyse Management Suite group and if the files are downloaded from the new group, a notification is not displayed.
  - If the new firmware or application is downloaded in the same group, a notification is not displayed.
  - After a reboot, the firmware or application is automatically installed.
- If you have installed the `HID_Fingerprint_Reader` package, ensure that you have also installed the `Citrix_Workspace_App` package, or you cannot upgrade to the latest ThinOS version.
- If you configure settings, like brokers, locally in ThinOS 2311 and downgrade to ThinOS 2308 or earlier versions using Wyse Management Suite, the settings are lost.
- If you downgrade to ThinOS 2308 or earlier versions using Wyse Management Suite, reboot the device manually again to set a password locally in ThinOS. Otherwise, passwords, like the Broker agent login password, get corrupted when rebooting for the first time after downgrading.

## Prerequisites for firmware upgrade

Before you upgrade from ThinOS 9.1.x to ThinOS 2311, turn on the device and disable the sleep mode. If the device 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 the 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, reboot the device and upgrade again.
- NOTE:** Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2311. Install the latest application packages.
- NOTE:** If you are using small disk devices like Wyse 3040 with 8 GB disk, ignore ThinOS 9.4.4106 firmware and use ThinOS 9.4.4123 firmware.

## Convert Ubuntu with DCA to ThinOS 2311 (9.4.4123)

### Prerequisites

**Table 10. Supported conversion scenarios**

Platform	Ubuntu version	DCA-Enabler version
Latitude 3420	20.04	1.7.1-61 or later
OptiPlex 5400 All-in-One	20.04	1.7.1-61 or later
Latitude 3440	22.04	1.7.1-61 or later
Latitude 5440	22.04	1.7.1-61 or later
OptiPlex All-in-One 7410	22.04	1.7.1-61 or later
OptiPlex All-in-One 7420	22.04	1.7.1-61 or later

Ensure that DCA-Enabler is installed on your Ubuntu devices according to the above table. For details on how to install DCA-Enabler in the Ubuntu operating system and upgrade it, see *Dell ThinOS 2311, 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support)

- NOTE:** Microsoft AVD package that is released before ThinOS 2311 is removed automatically after upgrading to ThinOS 2311. Install the latest Microsoft AVD package.
- 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 2311.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2311.
- 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 ThinOS 2311, 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support).
- Ensure you have downloaded the Ubuntu to ThinOS 2311 conversion image.
- Extract the Ubuntu to ThinOS 2311 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.3-dtos3-amd64_signed.tar.gz` and ThinOS image `ThinOS_2311_9.4.4123.pkg`.
- NOTE:** The ThinOS image `ThinOS_2311_9.4.4123.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_1.3-dtos3-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_2311_9.4.4123.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 that 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 2311 is in the factory default status. ThinOS 2311 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 11. Error Log table**

Error Log	Resolution
No AC plugged in	Plug in the power adapter and reschedule the 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	Unable to find the ThinOS image, reschedule the 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.

## ThinOS application package details

For ThinOS 2311, it is recommended to install the latest application packages from the below table.

**Table 12. ThinOS application package details**

Supported Application Packages
Cisco_Jabber_14.2.0.308051.8.pkg
Cisco_WebEx_Meetings_VDI_43.10.2.11.2.pkg
Cisco_WebEx_VDI_43.10.0.27605.1.pkg
Citrix_Workspace_App_23.9.0.24.11.pkg

**Table 12. ThinOS application package details (continued)**

<b>Supported Application Packages</b>
Common_Printing_1.0.0.26.pkg
ControlUp_VDI_Agent_2.2.5.pkg
EPOS_Connect_7.7.0.2.pkg
HID_Fingerprint_Reader_210217.24.pkg
Identity_Automation_QwickAccess_2.0.4.1.6.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.5.6.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.6.2.4.3.pkg
Microsoft_AVD_2.3.2266.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_23.06.2.18.pkg
VMware_Horizon_2306.8.10.0.21964631.5.pkg
VMware_Horizon_ClientSDK_2306.8.10.0.21964631.20.pkg
Zoom_AVD_5.16.0.24280.1.pkg
Zoom_Citrix_5.16.0.24280.1.pkg
Zoom_Horizon_5.15.2.23760.3.pkg

**Important notes**

- After upgrading to ThinOS 2311, all application packages that are released before ThinOS 2205 are removed automatically. You must install the latest application packages.
- You cannot install application packages that are released before ThinOS 2205 on ThinOS 2311, and installation fails for the first time. After the installation fails, ThinOS does not download the application packages anymore.
- After upgrading to ThinOS 2311, the Microsoft AVD package that is released before ThinOS 2311 is removed automatically. You must install the latest Microsoft AVD package.

## BIOS packages

**Table 13. BIOS packages**

<b>Platform model</b>	<b>Package file name</b>
Wyse 5070 Thin Client	bios-5070_1.26.0.pkg
Wyse 5470 Thin Client	bios-5470_1.21.0.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.22.0.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.13.2.pkg
Dell Latitude 3420	bios-Latitude_3420_1.31.0.pkg
Dell Latitude 3440	bios-Latitude3440_1.7.0.pkg
Dell OptiPlex All-in-One 7410	bios-OptiPlexAIO7410_1.8.0.pkg

# Tested BIOS versions

Table 14. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.26.0
Wyse 5470 All-in-One Thin Client	1.22.0
Wyse 5470 Mobile Thin Client	1.21.0
OptiPlex 3000 Thin Client	1.13.2
Latitude 3420	1.31.0
OptiPlex 5400 All-in-One	1.1.29
Latitude 3440	1.7.0
Latitude 5440	1.3.0
OptiPlex AIO 7410	1.8.0

## New updates

### Few ThinOS 2311 units are reporting smaller disk space

#### Issue Analysis

- For devices that adopt the screen saver file server feature, the downloaded figures from the file server saves on disk before ThinOS 2311 release.
- From ThinOS 2311 (9.4.4106), the files are no longer saved on disk and moved to memory for functioning.
- However, the upgrade process does not clear the previously saved files on disk.
- It is considered better to clear those saved files on disk during the upgrade process.
- After upgrading to 9.4.4106, the computer creates disk snapshot files on the disk that are 1-1.5 GB to prepare for new features in future releases .
- The feature is disabled in this version to reduce impact on smaller disk devices like Wyse 3040 with 8 GB disk.
- This feature is going to be refined in future releases for large disk devices only.

#### Resolution

- Disable the snapshots creation function and delete the created snapshots on disk, if any, as specified above.
- Delete the screen saver figures saved on disk as specified above.
- Enable the installation of the disk clean package for devices with a small disk space.

### Smartcard PIN prompt issue inside VDI connection

**Issue Analysis**—Few special software environments require a customized smartcard behavior to enable the PIN prompt for application authentication inside a VDI connection.

**Resolution**—Rewrite the smartcard behavior to reduce race conditions.

# VMware Horizon Client 2309 and Zoom Horizon 5.16 packages for ThinOS 2311

## Release date

December 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

### Horizon Client Package

- VMware\_Horizon\_2309.8.11.0.22660930.5.pkg
- VMware\_Horizon\_ClientSDK\_2309.8.11.0.22660930.6.pkg

### Zoom Horizon Package

- Zoom\_Horizon\_5.16.0.24280.2.pkg

## Notes

- For information about other packages, see [ThinOS application package details](#).
- After upgrade to ThinOS 2311, all application packages that are released before ThinOS 2205 are removed automatically. You must install the latest application packages.
- You cannot install application packages older than ThinOS 2205 on ThinOS 2311, and installation fails for the first time. After that ThinOS does not download the application packages.

## Previous versions

- VMware\_Horizon\_2306.8.10.0.21964631.5.pkg
- VMware\_Horizon\_ClientSDK\_2306.8.10.0.21964631.20.pkg
- Zoom\_Horizon\_5.15.2.23760.3.pkg



# Tested BIOS versions

**Table 15. Tested BIOS details**

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.26.0
Wyse 5470 All-in-One Thin Client	1.22.0
Wyse 5470 Mobile Thin Client	1.21.0
OptiPlex 3000 Thin Client	1.13.2
Latitude 3420	1.31.0
OptiPlex 5400 All-in-One	1.1.29
Latitude 3440	1.7.0
Latitude 5440	1.3.0
OptiPlex AIO 7410	1.8.0

## 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 **Application Package Updates**.

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

5. Click **Browse**.
6. Select the application package to upload.  
Ensure that the switch option of the application package is set to **INSTALL**.
7. Expand the application package list, and select the uploaded version.
8. Click **Save & Publish**.  
The thin client downloads the package to install and restarts. The package version is upgraded.

## VMware Horizon feature matrix

**Table 16. VMware Horizon session and client package versions**

Horizon	Package version
Horizon Session SDK	VMware_Horizon_2309.8.11.0.22660930.5.pkg

**Table 16. VMware Horizon session and client package versions (continued)**

Horizon	Package version
Horizon Client SDK	VMware_Horizon_ClientSDK_2309.8.11.0.22660930.6.pkg

**Table 17. VMware Horizon feature matrix**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Broker Connectivity	SSL certificate verification	Supported	Supported
	Disclaimer dialog	Supported	Supported
	UAG compatibility	Supported	Partially Supported
	Shortcuts from server	Not Supported	Not Supported
	Pre-install shortcuts from server	Not Supported	Not Supported
	File type association	Not Supported	Not Supported
	Phonehome	Supported	Supported
Broker Authentication	Password authentication	Supported	Supported
	SAML authentication	Supported	Supported
	Single sign on	Supported	Supported
	RSA authentication	Supported	Partially Supported
	Integrated RSA SecurID token generator	Not Supported	Not Supported
	Radius - Cisco ACS	Supported	Supported
	Radius - SMS Passcode	Supported	Supported
	Radius - DUO	Supported	Supported
	Radius - OKTA	Supported	Supported
	Radius - Microsoft Network Policy	Supported	Supported
	Radius - Cisco Identity Services Engine	Supported	Supported
	Kiosk mode	Supported	Supported
	Remember credentials	Supported	Supported
	Log in as current user	Not Supported	Not Supported
	Nested log in as current user	Not Supported	Not Supported
	Log in as current user 1-way trust	Not Supported	Not Supported
	OS biometric authentication	Not Supported	Not Supported
	Windows Hello	Not Supported	Not Supported
Unauthentication access	Supported	Supported	
Smartcard	x.509 certificate authentication (Smart Card)	Supported	Partially Supported
	CAC support	Supported	Partially Supported
	.Net support	Supported	Supported
	PIV support	Supported	Partially Supported

**Table 17. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Java support	Supported	Supported
	Purebred derived credentials	Not Supported	Not Supported
	Device Cert auth with UAG	Supported	Not Supported
Desktop Operations	Reset	Only supported with VDI	Only supported with VDI
	Restart	Only supported with VDI	Only supported with VDI
	Log off	Supported	Supported
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported	Supported
	Multiple connections	Supported	Supported
	Multi-broker/multi-site redirection - Universal	Not Supported	Not Supported
	App launch on multiple end points	Supported	Supported
	Auto-retry 5+ minutes	Supported	Supported
	Blast network recovery	Supported	Supported
	Time zone synchronization	Supported	Supported
	Jumplist integration (Windows 7-Windows 10)	Not Supported	Not Supported
Client Customization	Command line options	Not Supported	Not Supported
	URI schema	Not Supported	Not Supported
	Launching multiple client instances using URI	Not Supported	Not Supported
	Preference file	Not Supported	Not Supported
	Parameter pass-through to RDSH apps	Not Supported	Not Supported
	Non interactive mode	Not Supported	Not Supported
	GPO-based customization	Not Supported	Not Supported
Protocols supported	Blast Extreme	Supported	Supported
	H.264 - HW decode	Supported	Supported
	H.265 - HW decode	Supported	Supported
	Blast Codec	Supported	Supported
	JPEG / PNG	Supported	Supported
	Switch encoder	Supported	Supported
	BENIT	Supported	Supported
	Blast Extreme Adaptive Transportation	Supported	Supported
	RDP 8.x, 10.x	Supported	Not Supported
	PCoIP	Supported	Supported
	Features / Extensions Monitors / Displays	Dynamic display resizing	Supported
VDI windowed mode		Supported	Supported
Remote app seamless window		Supported	Supported

**Table 17. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Multiple monitor support	Supported	Supported
	External monitor support for mobile	Not Supported	Not Supported
	Display pivot for mobile	Not Supported	Not Supported
	Number of displays supported	4	4
	Maximum resolution	3840x2160	3840x2160
	High DPI scaling	Not Supported	Not Supported
	DPI sync	Not Supported	Not Supported
	Exclusive mode	Not Supported	Not Supported
	Multiple monitor selection	Supported	Supported
Input Device (Keyboard / Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported	Supported
	Relative mouse	Only supported with VDI	Only supported with VDI
	External Mouse Support	Supported	Supported
	Local buffer text input box	Not Supported	Not Supported
	Keyboard Mapping	Supported	Supported
	International Keyboard Support	Supported	Supported
	Input Method local/remote switching	Not Supported	Not Supported
	IME Sync	Supported	Supported
Clipboard Services	Clipboard Text	Supported	Supported
	Clipboard Graphics	Not Supported	Not Supported
	Clipboard memory size configuration	Supported	Supported
	Clipboard File/Folder	Not Supported	Not Supported
	Drag and Drop Text	Not Supported	Not Supported
	Drag and Drop Image	Not Supported	Not Supported
	Drag and Drop File/Folder	Not Supported	Not Supported
Connection Management	IPv6 only network support	Supported	Supported
	PCoIP IP roaming	Supported	Supported
Optimized Device Redirection	Serial (COM) Port Redirection	Supported	Supported
	Client Drive Redirection/File Transfer	Not Supported	Not Supported
	Scanner (TWAIN/WIA) Redirection	Supported	Supported
	x.509 Certificate (Smart Card/Derived Credentials)	Supported	Supported
	Storage Drive Redirection	Not Supported	Not Supported
	Gyro Sensor Redirection	Not Supported	Not Supported

**Table 17. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Real-Time Audio-Video	Audio input (microphone)	Supported	Supported
	Video input (webcam)	Supported	Supported
	Multiple webcams and microphones	Not Supported	Not Supported
	Multiple speakers	Not Supported	Not Supported
USB Redirection	USB redirection	Supported	Supported
	Policy: ConnectUSBOnInsert	Supported	Supported
	Policy: ConnectUSBOnStartup	Supported	Supported
	Connect/Disconnect UI	Not Supported	Not Supported
	USB device filtering (client side)	Supported	Supported
	Isochronous Device Support	Only supported with VDI	Only supported with VDI
	Split device support	Supported	Supported
	Bloomberg Keyboard compatibility	Only supported with VDI	Only supported with VDI
	Smartphone sync	Only supported with VDI	Only supported with VDI
Unified Communications	Skype for business	Not Supported	Not Supported
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Teams	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Meeting	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams HID Headset	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not Supported	Not Supported
	Directshow Redirection	Not Supported	Not Supported
	URL content redirection	Not Supported	Not Supported
	MMR Multiple Audio Output	Not Supported	Not Supported
	UNC path redirection	Not Supported	Not Supported
	Browser content redirection	Not Supported	Not Supported
Graphics	vDGA	Only supported with VDI	Only supported with VDI
	vSGA	Only supported with VDI	Only supported with VDI

**Table 17. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	NVIDIA GRID vGPU	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Only supported with VDI	Only supported with VDI
	AMD vGPU	Only supported with VDI	Only supported with VDI
Mobile Support	Client-side soft keyboard	Not Supported	Not Supported
	Client-side soft touchpad	Not Supported	Not Supported
	Full Screen Trackpad	Not Supported	Not Supported
	Gesture Support	Not Supported	Not Supported
	Multi-touch Redirection	Not Supported	Not Supported
	Presentation Mode	Not Supported	Not Supported
	Unity Touch	Not Supported	Not Supported
Printing	VMware Integrated Printing	Supported	Supported
	Location Based Printing	Supported	Supported
	Native Driver Support	Not Supported	Not Supported
Security	FIPS-140-2 Mode Support	Supported	Supported
	Imprivata Integration	Supported	Supported
	Opswat agent	Not Supported	Not Supported
	Opswat on-demand agent	Not Supported	Not Supported
	TLS 1.1/1.2	Supported	Supported
	Screen shot blocking	Not Supported	Not Supported
	Keylogger blocking	Not Supported	Not Supported
Session Collaboration	Session Collaboration	Supported	Supported
	Read-only Collaboration	Supported	Supported
Updates	Update notifications	Not Supported	Not Supported
	App Store update	Not Supported	Not Supported
Other	Smart Policies from DEM	Supported	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported	Supported
	Nested - basic connection	Supported	Supported
	DCT Per feature/component collection	Not Supported	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported	Supported
	Auth Method - RSA SecurID	Supported	Supported

**Table 17. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Auth Method - X.509 Certificate (Smart Card)	Supported	Not Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported	Not Supported
	Auth Method - RADIUS	Supported	Supported
	Auth Method - SAML - 3rd Party Identity Provider	Supported	Supported

For detailed information about the VMware Horizon features, see the Horizon documentation at [docs.vmware.com](https://docs.vmware.com).

## New features

### VMware Horizon Updates

#### Horizon Client

Horizon Client 2309 is supported and the package versions are updated to the following:

- **VMware\_Horizon\_2309.8.11.0.22660930.5.pkg**
- **VMware\_Horizon\_ClientSDK\_2309.8.11.0.22660930.6.pkg**

#### Zoom Horizon

Zoom Horizon package is updated to **Zoom\_Horizon\_5.16.0.24280.2** with the following features and enhancements:

- Redesigned the annotation toolbar.
- Enhanced the Window merge-in feature.
- Teams chat thread summary with Zoom AI Companion.
- Redesigned captioning controls.
- Enhanced the Question and Answer usability during webinars.

## Tested environment matrix

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

**Table 18. Tested environment—General components**

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.2
Configuration UI package for Wyse Management Suite	1.10.240

**Table 19. 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 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested

**Table 19. 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 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
VMware Horizon 2303	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested
VMware Horizon 2306	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested

**Table 20. 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 21. Test environment – VMware Horizon Cloud version 2**

Horizon Cloud v2	Company Domain	Windows 10	Identity Provider	
www.cloud.vmware horizon.com	Hcseuc	Tested	Azure	Tested
			WS1 Access	Not tested

**Table 22. Tested environment—Zoom**

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 3209	Windows 10	5.16.0.24280.2	5.16 (24280)
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		



# ThinOS 2311 (9.4.4106)

## Release date

November 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 2311 (9.4.4106)

## Previous version

ThinOS 2308 (9.4.3087)

## Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2311 (9.4.4106)**

**i** **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2311. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.

**i** **NOTE:** If you want to downgrade ThinOS 2311 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2311, 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support). For the steps to access documents, see [Resources and support](#).

## Important notes

- Some features and product environments that are not tested by Dell Technologies are found to be working with other users. These features or product environments have been marked as **Not Qualified**.
- If you are using small disk devices like Wyse 3040 with 8 GB, it is recommended that the operating system firmware and application packages be upgraded in separate steps. Upgrading them simultaneously may cause upgrade failures due to insufficient disk space. If you still fail to upgrade the operating system firmware and application packages, uninstall some application packages to free disk space and try again.
- To further improve the security of ThinOS devices, from 2311, ThinOS uses OpenSSL version 3.0, and the default TLS security level is 1. If your environment requires a legacy OpenSSL version (like SHA1 certification), change the TLS security level to 0 in Wyse Management Suite policy by going to **Privacy & Security > Security Policy**. Legacy OpenSSL versions are not supported on future ThinOS versions. If a Legacy OpenSSL version is required, update your environment.
- To further improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are going to be removed in the next release. Some TLS ciphers are not secure and are subject to change in the next release.


**Table 23. TLS Cipher list**

<b>Ciphers</b>	<b>Security Status</b>
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Not secure and subject to change in the next release
ECDHE-RSA-AES256-SHA384	Not secure and subject to change in the next release
ECDHE-RSA-AES128-SHA	Not secure and subject to removal in next release
ECDHE-RSA-AES256-SHA	Not secure and subject to removal in next release
DHE-RSA-AES128-GCM-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES256-GCM-SHA384	Not secure and subject to removal in next release
DHE-RSA-AES128-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES256-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES128-SHA	Not secure and subject to removal in next release
DHE-RSA-AES256-SHA	Not secure and subject to removal in next release
AES128-SHA256	Removed in ThinOS 2303
AES256-SHA256	Removed in ThinOS 2303
AES128-SHA	Removed in ThinOS 2303
AES256-SHA	Removed in ThinOS 2303
AES128-GCM-SHA256	Removed in ThinOS 2303
AES256-GCM-SHA384	Removed in ThinOS 2303
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Not secure and subject to change in the next release
ECDHE-ECDSA-AES256-SHA384	Not secure and subject to change in the next release
ECDHE-ECDSA-AES128-SHA	Not secure and subject to removal in next release
ECDHE-ECDSA-AES256-SHA	Not secure and subject to removal in next release
DHE-PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES256-GCM-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
DHE-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
DHE-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES128-CBC-SHA256	Not secure and subject to change in the next release
ECDHE-PSK-AES256-CBC-SHA384	Not secure and subject to change in the next release
PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
PSK-AES256-GCM-SHA384	Not secure and subject to removal in next release
PSK-AES128-CBC-SHA	Not secure and subject to removal in next release

**Table 23. TLS Cipher list (continued)**

Ciphers	Security Status
PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
RSA-PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
RSA-PSK-AES256-GCM-SHA384	Not secure and subject to removal in next release
RSA-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
RSA-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
RSA-PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
RSA-PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
ECDHE-ECDSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
ECDHE-RSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
DHE-RSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
RSA-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
DHE-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
ECDHE-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
SRP-RSA-AES-256-CBC-SHA	Not secure and subject to removal in next release
SRP-AES-256-CBC-SHA	Not secure and subject to removal in next release
SRP-RSA-AES-128-CBC-SHA	Not secure and subject to removal in next release
SRP-AES-128-CBC-SHA	Not secure and subject to removal in next release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

- 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.

 **NOTE:** From ThinOS 2303, **Live Update** is disabled, but the thin client can download the operating system firmware and BIOS firmware in the background. However, the thin client cannot complete installation 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 turn on the thin client from a turn off state
- When you change the Wyse Management Suite group
- When a new firmware or an application notification is displayed on your thin client and if you click **Next Reboot**, the following is observed:
  - If you have changed the Wyse Management Suite group and if the files are downloaded from the new group, a notification is not displayed.
  - If the new firmware or application is downloaded in the same group, a notification is not displayed.
  - After a reboot, the firmware or application is automatically installed.

- If you have installed the `HID_Fingerprint_Reader` package, ensure that you have also installed the `Citrix_Workspace_App` package, or you cannot upgrade to the latest ThinOS version.
- If you configure settings, like brokers, locally in ThinOS 2311 and downgrade to ThinOS 2308 or earlier versions using Wyse Management Suite, the settings are lost.
- If you downgrade to ThinOS 2308 or earlier versions using Wyse Management Suite, reboot the device manually again to set a password locally in ThinOS. Otherwise, passwords, like the Broker agent 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 2311, turn on the device and disable the sleep mode. If the device 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 the 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, reboot the device and upgrade again.

**NOTE:** Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2311. Install the latest application packages.

**NOTE:** If you are using small disk devices like Wyse 3040 with 8 GB disk, ignore ThinOS 9.4.4106 firmware and use ThinOS 9.4.4123 firmware. See [ThinOS 2311 \(9.4.4123\)](#) for more details.

## Convert Ubuntu with DCA to ThinOS 2311

### Prerequisites

**Table 24. Supported conversion scenarios**

Platform	Ubuntu version	DCA-Enabler version
Latitude 3420	20.04	1.7.1-61 or later
OptiPlex 5400 All-in-One	20.04	1.7.1-61 or later

**Table 24. Supported conversion scenarios (continued)**

Platform	Ubuntu version	DCA-Enabler version
Latitude 3440	22.04	1.7.1-61 or later
Latitude 5440	22.04	1.7.1-61 or later
OptiPlex All-in-One 7410	22.04	1.7.1-61 or later
OptiPlex All-in-One 7420	22.04	1.7.1-61 or later

Ensure that DCA-Enabler is installed on your Ubuntu devices according to the above table. For details on how to install DCA-Enabler in the Ubuntu operating system and upgrade it, see *Dell ThinOS 2311, 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support)

**NOTE:** Microsoft AVD package that is released before ThinOS 2311 is removed automatically after upgrading to ThinOS 2311. Install the latest Microsoft AVD package.

- 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 2311.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2311.
- 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 ThinOS 2311, 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support).
- Ensure you have downloaded the Ubuntu to ThinOS 2311 conversion image.
- Extract the Ubuntu to ThinOS 2311 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.3-dtos3-amd64_signed.tar.gz` and ThinOS image `ThinOS_2311_9.4.4106.pkg`.

**NOTE:** The ThinOS image `ThinOS_2311_9.4.4106.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_1.3-dtos3-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_2311_9.4.4106.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 that you want to convert in the **Platform Filter** drop-down menu.
10. Click **Save**.
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 2311 is in the factory default status. ThinOS 2311 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 25. Error Log table**

Error Log	Resolution
No AC plugged in	Plug in the power adapter and reschedule the 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	Unable to find the ThinOS image, reschedule the 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

For ThinOS 2311, it is recommended to install the latest application packages from the below table.

**Table 26. ThinOS application package details**

Supported Application Packages
Cisco_Jabber_14.2.0.308051.8.pkg
Cisco_WebEx_Meetings_VDI_43.10.2.11.2.pkg
Cisco_WebEx_VDI_43.10.0.27605.1.pkg
Citrix_Workspace_App_23.9.0.24.11.pkg
Common_Printing_1.0.0.26.pkg
ControlUp_VDI_Agent_2.2.5.pkg
EPOS_Connect_7.7.0.2.pkg
HID_Fingerprint_Reader_210217.24.pkg
Identity_Automation_QwickAccess_2.0.4.1.6.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.5.6.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.6.2.4.3.pkg
Microsoft_AVD_2.3.2266.pkg

**Table 26. ThinOS application package details (continued)**

Supported Application Packages
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_23.06.2.18.pkg
VMware_Horizon_2306.8.10.0.21964631.5.pkg
VMware_Horizon_ClientSDK_2306.8.10.0.21964631.20.pkg
Zoom_AVD_5.16.0.24280.1.pkg
Zoom_Citrix_5.16.0.24280.1.pkg
Zoom_Horizon_5.15.2.23760.3.pkg

**Important notes**

- After upgrading to ThinOS 2311, all application packages that are released before ThinOS 2205 are removed automatically. You must install the latest application packages.
- You cannot install application packages that are released before ThinOS 2205 on ThinOS 2311, and installation fails for the first time. After the installation fails, ThinOS does not download the application packages anymore.
- After upgrading to ThinOS 2311, the Microsoft AVD package that is released before ThinOS 2311 is removed automatically. You must install the latest Microsoft AVD package.
- If an application package fails to install with an error **invalid cache** in the event log, do a soft reset and install the package again.

## Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 4.2
- Configuration UI package 1.10.240

**i** | **NOTE:** Use Wyse Management Suite 4.2 server for the new Wyse Management Suite ThinOS 9.x Policy features.

**i** | **NOTE:** Configuration UI package 1.10.240 is embedded with Wyse Management Suite 4.2 server.

## ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2311 (9.4.4106)—ThinOS\_2311\_9.4.4106.pkg
- Ubuntu to ThinOS 2311 conversion build—ThinOS\_2311\_9.4.4106\_Ubuntu\_Conversion.zip

## BIOS packages

**Table 27. BIOS package**

Platform model	Package file name
Wyse 5070 Thin Client	bios-5070_1.26.0.pkg
Wyse 5470 Thin Client	bios-5470_1.21.0.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.22.0.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.13.2.pkg
Dell Latitude 3420	bios-Latitude_3420_1.31.0.pkg
Dell Latitude 3440	bios-Latitude3440_1.7.0.pkg
Dell OptiPlex All-in-One 7410	bios-OptiPlexAIO7410_1.8.0.pkg

# Tested BIOS version for ThinOS 2311

**Table 28. Tested BIOS details**

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.26.0
Wyse 5470 All-in-One Thin Client	1.22.0
Wyse 5470 Mobile Thin Client	1.21.0
OptiPlex 3000 Thin Client	1.13.2
Latitude 3420	1.31.0
OptiPlex 5400 All-in-One	1.1.29
Latitude 3440	1.7.0
Latitude 5440	1.3.0
OptiPlex AIO 7410	1.8.0

# Citrix Workspace app feature matrix

**Table 29. Citrix Workspace app feature matrix**

Feature	ThinOS 2311 with CWA 2309	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 Secure Private Access	Not Supported	Not Supported
	Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Not Supported	Not Supported
	SaaS/Web apps with SSO	Not Supported	Not Supported
	Citrix Mobile Apps	Not Supported	Not Supported
	App Personalization service	Not Supported	Not Supported
Workspace 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.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	Not Supported	Not Supported
	Citrix Auto updates	Not Supported	Not Supported
	Client App Management	Not Supported	Not Supported



**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
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.
	SDWAN support	Not Supported	Not Supported
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	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.
	TWAIN 2.0	Not supported	Not supported
HDX Integration	Local App Access	Not Supported	Not Supported
	Multi-touch	Not Supported	Not Supported
	Mobility Pack	Not Supported	Not Supported
	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.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	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

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
			recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	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+.
	File open in Citrix Workspace app	Not Supported	Not supported. No local file explorer on ThinOS.
	Location Based Services (Location available via API-description)	Not Supported	Not Supported
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	There are no limitations in this release.
	Video playback	Supported	There are no limitations in this release.
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Skype for business Optimization pack	Supported	Not support through proxy server
	Cisco Jabber Unified Communications Optimization	Supported	For more information, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Unified Communication Cisco WebEx Meetings Optimization	Supported	Dell Technologies recommends to wait for 10 s 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

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
			authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Unified Communication Cisco WebEx VDI Optimization	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 <a href="http://www.dell.com/support">www.dell.com/support</a>
	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 <a href="http://www.dell.com/support">www.dell.com/support</a>
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
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

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
	Remote Access via Citrix Gateway	Supported	The following webview login environment configuration supports user auto-login and lock/unlock terminal: Citrix Federated Authentication Service, SAML with Microsoft Azure Active Directory (except the authentication using FIDO2), Citrix ADC Native OTP, Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA (except the authentication using FIDO2), and Citrix ADC with PingID SAML MFA
	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.
	App Protection	Not supported	Not supported
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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	Not supported	Not supported
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 29. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2311 with CWA 2309	Limitations
User Cert Auth via NetScaler Gateway (via Browser Only)	Not supported	Not supported
User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
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)	Not supported	Not supported
ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor authentications are not qualified.
ADC Full VPN	Not supported	Not supported
ADC 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	Not supported	Not supported
Single Sign on to Citrix Mobile apps	Not supported	Not supported
Anonymous Store Access	Supported	There are no limitations in this release.
Netscaler + RSA	Not qualified	Not qualified
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 qualified	Not qualified
Netscaler load balance	Not supported	Not supported
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported There are no limitations in this release.

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session 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 setting in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	HTTPS protocol support for proxy server	Not Supported	Not Supported
	Support for IPv6 UDT with DTLS	Not Supported	Not Supported
	Script to verify system requirements for Windows Media Player redirection	Not Supported	Not Supported
	App Protection support for ARM64 devices	Not Supported	Not Supported
	Added support for playing short tones in optimized Microsoft Teams	Not Supported	Not Supported
	Support for IPv6 TCP with TLS	Not Supported	Not Supported

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2311 with CWA 2309	Limitations
Prerequisites for cloud authentication	Supported	There are no limitations in this release.
Enhancement on 32-bit cursor support	Supported	There are no limitations in this release.
Enhancement to support keyboard layout synchronization for GNOME 42	Not Supported	Not Supported
Client IME for East Asian languages	Not Supported	Not Supported
Support for authentication using FIDO2 when connecting to on-premises stores	Not Supported	Not Supported
Copy and paste files and folders between two virtual desktops	Not Supported	Not Supported
Support for ARM64 architecture	Not Supported	Not Supported
Addition of client-side jitter buffer mechanism	Not Supported	Not Supported
Support for more than 200 groups in Azure AD	Not Supported	Not Supported
Hardware acceleration support for optimized Microsoft Teams	Not Supported	Not Supported
Enhancement to sleep mode for optimized Microsoft Teams call	Not Supported	Not Supported
Background blurring for webcam redirection	Not Supported	Not Supported
Configure path for Browser Content Redirection overlay Browser temp data storage	Not Supported	From CWA2305, Citrix browser content redirection CEF cache file is changed from default .ICAClient to /tmp/citrix
Support for new PIV cards	Not Supported	Not Supported
Microsoft Teams enhancements-Limiting video resolutions	Not Supported	Not Supported
Microsoft Teams enhancements-Configuring a preferred network interface	Not Supported	Not Supported
Inactivity Timeout for Citrix Workspace app	Not Supported	Not Supported
Screen pinning in custom web stores	Not Supported	Not Supported

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2311 with CWA 2309	Limitations
Support for 32-bit cursor	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit still 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	Not Supported	Not Supported
Background blurring and replacement for Citrix Optimized Teams	Supported	There are no limitations in this release.
Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.
Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported
Support for extended keyboard layouts	Supported	There are no limitations in this release.
Keyboard input mode enhancements	Not Supported	Not Supported
Support for authentication using FIDO2 in HDX session	Supported	There are no limitations in this release.
Support for secondary ringer	Supported	There are no limitations in this release.
Improved audio echo cancellation support	Not Supported	Not Supported
Composite USB device redirection	Not Supported	Not Supported
Support for DPI matching	Not Supported	Not Supported
Enhancement to improve audio quality	Not Supported	Not Supported
Provision to disable LaunchDarkly service	Not Supported	Not Supported
Email-based auto-discovery of store	Not Supported	Not Supported
Persistent login	Not Supported	Not Supported
Authentication enhancement for Storebrowse	Not Supported	Not Supported
Support for EDT IPv6	Not Supported	Not Supported
Support for TLS protocol version 1.3	Not Supported	Not Supported



**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
	Custom web stores	Not Supported	Not Supported
	Authentication enhancement experimental feature	Not Supported	Not Supported
	Keyboard layout synchronization enhancement	Not Supported	Not Supported
	Multi-window chat and meetings for Microsoft Teams	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
	Request control in Microsoft Teams	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 work when you give control to other participant. This is a Microsoft limitation.
	Support for cursor color inverting	Supported	Invert cursor does not work in Citrix VDA 2212, VDA 2203 CU2, VDA2303 Windows 10 and Windows 2019 desktop. This issue also occurs in Citrix Workspace app Linux binary.
	Microsoft Teams enhancement to echo cancellation	Supported	For limitations, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a>
	Enhancement on smart card support	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit	Supported	There are no limitations in this release.
	Support for custom web stores	Not Supported	Not Supported
	Workspace with intelligence	Not Supported	Not Supported
	Session reliability enhancement	Supported	There are no limitations in this release.
	Enhancement to logging	Supported	There are no limitations in this release.
	Adaptive audio	Supported	There are no limitations in this release.
	Storebrowse enhancement for service continuity	Not Supported	Not Supported
	Global App Config Service	Not Supported	Not Supported

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2311 with CWA 2309	Limitations
EDT MTU discovery	Not Supported	Not Supported
Creating custom user-agent strings in network request	Not Supported	Not Supported
Feature flag management	Not Supported	Not Supported
Battery status indicator	Supported	There are no limitations in this release.
Service continuity	Not Supported	Not Supported
User Interface enhancement	Not Supported	Not Supported
Pinning multi-monitor screen layout	Not Supported	Not Supported
Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported
Multiple audio	Supported	Multiple audio devices feature is not supported by Cisco JVDI. This is Cisco known limitation. To eliminate confusion or mistakes, multiple audio devices feature is dynamically disabled after JVDI package installed, and it is dynamically enabled after JVDI package is uninstalled. Only Citrix VDA 2308 and later versions support 12 audio devices. The previous VDA version still has the 8 audio devices limitation. This is Citrix limitation
Citrix logging	Supported	There are no limitations in this release.
Cryptographic update	Not Supported	Not Supported
Transparent user interface (TUI)	Not Supported	Not Supported
GStreamer 1.x supportexperimental feature	Supported	There are no limitations in this release.
App indicator icon	Not Supported	Not Supported
Latest webkit support	Supported	There are no limitations in this release.
Bloomberg audio redirection	Supported	There are no limitations in this release.
Bloomberg v4 keyboard selective redirection support	Supported	There are no limitations in this release.
Multiple monitors improvement	Not Supported	Not Supported
Error messages improvement	Not Supported	Not Supported

**Table 29. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2311 with CWA 2309	Limitations
	Log collection enhancement	Not Supported	Not Supported
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 30. ThinOS AVD Client Feature Matrix**

Category Supported	Features	ThinOS 2311
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
	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
	USB (General)	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

**Table 30. ThinOS AVD Client Feature Matrix (continued)**

Category Supported	Features	ThinOS 2311
	Time Zone Mapping	Supported
	Video/Audio/Online playback	Supported
	Compression	Supported
	Optimize for low speed link	Supported
Graphics (CODECs)	H.264 Hardware Acceleration	Supported
Unified Communications	Microsoft Teams Optimization	Experimental support
	Zoom Cloud Meeting Optimization	Supported
Authentication	TS Gateway	Supported
	NLA	Supported
	SmartCard	Limited support
	Imprivata	Supported

## VMware Horizon feature matrix

**Table 31. VMware Horizon session and client package versions**

Horizon	Package version
Horizon Session SDK	VMware_Horizon_2306.8.10.0.21964631.3.pkg
Horizon Client SDK	VMware_Horizon_ClientSDK_2306.8.10.0.21964631.6.pkg

**Table 32. VMware Horizon feature matrix**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Broker Connectivity	SSL certificate verification	Supported	Supported
	Disclaimer dialog	Supported	Supported
	UAG compatibility	Supported	Partially Supported
	Shortcuts from server	Not Supported	Not Supported
	Pre-install shortcuts from server	Not Supported	Not Supported
	File type association	Not Supported	Not Supported
	Phonehome	Supported	Supported
Broker Authentication	Password authentication	Supported	Supported
	SAML authentication	Supported	Supported
	Single sign on	Supported	Supported
	RSA authentication	Supported	Partially Supported
	Integrated RSA SecurID token generator	Not Supported	Not Supported
	Radius - Cisco ACS	Supported	Supported
	Radius - SMS Passcode	Supported	Supported
	Radius - DUO	Supported	Supported
	Radius - OKTA	Supported	Supported

**Table 32. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Radius - Microsoft Network Policy	Supported	Supported
	Radius - Cisco Identity Services Engine	Supported	Supported
	Kiosk mode	Supported	Supported
	Remember credentials	Supported	Supported
	Log in as current user	Not Supported	Not Supported
	Nested log in as current user	Not Supported	Not Supported
	Log in as current user 1-way trust	Not Supported	Not Supported
	OS biometric authentication	Not Supported	Not Supported
	Windows Hello	Not Supported	Not Supported
	Unauthentication access	Supported	Supported
Smartcard	x.509 certificate authentication (Smart Card)	Supported	Partially Supported
	CAC support	Supported	Partially Supported
	.Net support	Supported	Supported
	PIV support	Supported	Partially Supported
	Java support	Supported	Supported
	Purebred derived credentials	Not Supported	Not Supported
	Device Cert auth with UAG	Supported	Not Supported
Desktop Operations	Reset	Only supported with VDI	Only supported with VDI
	Restart	Only supported with VDI	Only supported with VDI
	Log off	Supported	Supported
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported	Supported
	Multiple connections	Supported	Supported
	Multi-broker/multi-site redirection - Universal	Not Supported	Not Supported
	App launch on multiple end points	Supported	Supported
	Auto-retry 5+ minutes	Supported	Supported
	Blast network recovery	Supported	Supported
	Time zone synchronization	Supported	Supported
	Jumplist integration (Windows 7-Windows 10)	Not Supported	Not Supported
Client Customization	Command line options	Not Supported	Not Supported
	URI schema	Not Supported	Not Supported
	Launching multiple client instances using URI	Not Supported	Not Supported
	Preference file	Not Supported	Not Supported

**Table 32. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Parameter pass-through to RDSH apps	Not Supported	Not Supported
	Non interactive mode	Not Supported	Not Supported
	GPO-based customization	Not Supported	Not Supported
Protocols supported	Blast Extreme	Supported	Supported
	H.264 - HW decode	Supported	Supported
	H.265 - HW decode	Supported	Supported
	Blast Codec	Supported	Supported
	JPEG / PNG	Supported	Supported
	Switch encoder	Supported	Supported
	BENIT	Supported	Supported
	Blast Extreme Adaptive Transportation	Supported	Supported
	RDP 8.x, 10.x	Supported	Not Supported
	PCoIP	Supported	Supported
Features / Extensions Monitors / Displays	Dynamic display resizing	Supported	Supported
	VDI windowed mode	Supported	Supported
	Remote app seamless window	Supported	Supported
	Multiple monitor support	Supported	Supported
	External monitor support for mobile	Not Supported	Not Supported
	Display pivot for mobile	Not Supported	Not Supported
	Number of displays supported	4	4
	Maximum resolution	3840x2160	3840x2160
	High DPI scaling	Not Supported	Not Supported
	DPI sync	Not Supported	Not Supported
	Exclusive mode	Not Supported	Not Supported
	Multiple monitor selection	Supported	Supported
Input Device (Keyboard / Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported	Supported
	Relative mouse	Only supported with VDI	Only supported with VDI
	External Mouse Support	Supported	Supported
	Local buffer text input box	Not Supported	Not Supported
	Keyboard Mapping	Supported	Supported
	International Keyboard Support	Supported	Supported
	Input Method local/remote switching	Not Supported	Not Supported
	IME Sync	Supported	Supported
Clipboard Services	Clipboard Text	Supported	Supported

**Table 32. VMware Horizon feature matrix (continued)**

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

**Table 32. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Cisco WebEx Meeting	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams HID Headset	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not Supported	Not Supported
	Directshow Redirection	Not Supported	Not Supported
	URL content redirection	Not Supported	Not Supported
	MMR Multiple Audio Output	Not Supported	Not Supported
	UNC path redirection	Not Supported	Not Supported
	Browser content redirection	Not Supported	Not Supported
Graphics	vDGA	Only supported with VDI	Only supported with VDI
	vSGA	Only supported with VDI	Only supported with VDI
	NVIDIA GRID vGPU	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Only supported with VDI	Only supported with VDI
	AMD vGPU	Only supported with VDI	Only supported with VDI
Mobile Support	Client-side soft keyboard	Not Supported	Not Supported
	Client-side soft touchpad	Not Supported	Not Supported
	Full Screen Trackpad	Not Supported	Not Supported
	Gesture Support	Not Supported	Not Supported
	Multi-touch Redirection	Not Supported	Not Supported
	Presentation Mode	Not Supported	Not Supported
	Unity Touch	Not Supported	Not Supported
Printing	VMware Integrated Printing	Supported	Supported
	Location Based Printing	Supported	Supported
	Native Driver Support	Not Supported	Not Supported
Security	FIPS-140-2 Mode Support	Supported	Supported
	Imprivata Integration	Supported	Supported
	Opsswat agent	Not Supported	Not Supported
	Opsswat on-demand agent	Not Supported	Not Supported
	TLS 1.1/1.2	Supported	Supported
	Screen shot blocking	Not Supported	Not Supported
	Keylogger blocking	Not Supported	Not Supported
Session Collaboration	Session Collaboration	Supported	Supported



**Table 32. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Read-only Collaboration	Supported	Supported
Updates	Update notifications	Not Supported	Not Supported
	App Store update	Not Supported	Not Supported
Other	Smart Policies from DEM	Supported	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported	Supported
	Nested - basic connection	Supported	Supported
	DCT Per feature/component collection	Not Supported	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported	Supported
	Auth Method - RSA SecurID	Supported	Supported
	Auth Method - X.509 Certificate (Smart Card)	Supported	Not Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported	Not Supported
	Auth Method - RADIUS	Supported	Supported
	Auth Method - SAML - 3rd Party Identity Provider	Supported	Supported

For detailed information about the VMware Horizon features, see the Horizon documentation at [docs.vmware.com](https://docs.vmware.com).

## New and enhanced features

### Citrix Workspace app updates

Citrix Workspace App (CWA) package version is updated to 23.9.0.24.11.

- **Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT)**
  - From ThinOS 2311 and Citrix Workspace App package 23.9.0.24.11, Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT) is supported.
  - MTU increases the reliability and compatibility of the EDT protocol and provides an improved user experience.
  - MTU Discovery enables EDT to automatically determine the Maximum Transmission Unit (MTU) when establishing a session.
  - This prevents EDT packet fragmentation that might result in performance degradation or failure to establish a session.
  - System requirements:
    - Citrix Virtual Delivery Agent (VDA) 2003 and later
    - Citrix Workspace app package version 23.9.0.24.11 and later
    - Session reliability enabled
  - MTU Discovery is enabled by default. To disable EDT MTU Discovery, configure the following registry values and restart the VDA:
    - Key: **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**

- Value name: **MtuDiscovery**
- Value type: **DWORD**
- Value data: **0**

**i** **NOTE:** This setting is machine-wide and affects all sessions connecting from a supported client.

- To configure Maximum Segment Size (MSS) when using EDT on networks with nonstandard MTU, do the following:
  1. You can set the EDT MTU Discovery Registry key value below to disabled (value 0) and restart the VDA.
    - Key: **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**
    - Value name: **MtuDiscovery**
    - Value type: **DWORD**
    - Value data: **0**

**i** **NOTE:** If the value is **1**, then MTU discovery is enabled. If the value is **0**, MTU discovery is disabled.
  2. You can also configure the MTU or MSS rates manually by doing the following:
    - a. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.
    - b. In **Citrix INI Settings**, click **Add Row**.
    - c. From the **File** drop-down list, select **All\_Regions.ini**.
    - d. From the **Operation** drop-down list, select **Add or Update**.
    - e. In the **Section** field, enter **Network\UDT**.
    - f. In the **Key** field, enter **edtMSS**.
    - g. In the **Value** field, enter a value, such as **1480**. The MTU value must be determined for each network independently and is not a one-size-fits-all solution.
    - h. Sign out or restart the device for the settings to take effect.

**i** **NOTE:** By design, Citrix Workspace App does not support disable EDT MTU Discovery from the client side. You can enable or disable EDT MTU Discovery on VDA.
- **Fixed issues with Disk Map To setting**—From ThinOS 2311, you need not plug-in a USB disk device before logging in to the broker. With this fix, there is an empty USB-mapping disk drive that is displayed in session if you do not plug in the USB disk.
- **Multiple audio devices enhancement**
  - The multiple audio devices feature from Citrix VDA2308 supports 12 audio devices.
  - The total number of playback and recording devices on a thin client must be lesser than or equal to 12 to use multiple audio devices.
  - If the total number of playback and recording devices on a thin client is more than 12, multiple audio devices does not work properly.

**i** **NOTE:** Only Citrix VDA 2308 and later versions support 12 audio devices. The previous VDA version still has the eight audio devices limitation.
- **Citrix Workspace App Limitations that also occur in the Linux Citrix Workspace app binary**
  - Microsoft Teams transfer call window is hidden behind the Video window.
  - Audio issue with Citrix UDP through Citrix ADC gateway.

## Microsoft RDP and AVD

- **Supports Remote App Integrated feature**
  - Remote applications are displayed in Windows mode and is integrated with the local window manager as if they are running locally.
  - After logging into the broker, the connection display settings for remote app sessions are consistent when the **Seamless** option is selected in **Display Resolution** dropdown with Windows mode enabled.
- **Supports split redirection of AVD USB redirection**
  - Go to **APT/WMS > Advanced > Session Settings > RDP and AVD Session Settings > Force USB Devices Redirection** and enter the **VID:PID-classID** value.
  - For example, **0561 : 554c-03** where the interface **03** is redirected into session and the other interfaces are not redirected. **03** is the HID-related interface.
- **Known issues**
  - The AVD package of ThinOS 2311 cannot be installed to the previous ThinOS release and ThinOS 2311 automatically deletes the previously released AVD packages.

- When Desktop Scale Factor is set to 400 or 500, the mouse pointer is not displayed in the RDP Windows 2016 VDI desktop.
- For the Remote App Integrated feature, **Reconnect After Disconnect** functionality does not work until all applications that are published by the same server are closed.

## Teradici PCoIP

- Teradici version is updated to 23.06.2.9 in ThinOS 2311.
- The RTAV plug-in has been deprecated with PCoIP package version 23.06.2.9. If you have to use the mapping camera, use the Horizon client SDK package.

## VMware Horizon Updates

- **ThinOS Horizon Client SDK updates**
  - ThinOS Horizon Client Session SDK package version is the same as ThinOS 2308.
  - The Horizon Client SDK package is updated to **VMware\_Horizon\_ClientSDK\_2306.8.10.0.21964631.18.pkg**.
- **Supports Horizon KIOSK Mode with a specified password**
  - Use the VMware Horizon administrator guide document to configure the KIOSK mode client with a specified password.
  - In ThinOS, use the account name **Client Mac** and the previously specified password can log in to the Horizon server.
- **Scanner redirection settings**
  - **Allow USB Image Family Device redirection** in Wyse Management Suite policy is updated; you cannot use scanner redirection in a Blast session by enabling this setting. To avoid confusion, update the policy name and tooltip. Then, the settings is applied to iPhone and Samsung mobile devices or other devices with Class ID 06.
  - If you want to enable or disable scanner redirection, enable or disable **Exclude Vid/Pid USB Device Redirection** or **Include Vid/Pid USB Device Redirection** in **Advanced > Session Settings > Blast Session Settings**.
- **Known Issues**
  - If ThinOS 5070 systems are used at 3840x2160 resolution, the performance decreases.
  - If ThinOS 5070 systems are used at 3840x2160 resolution, moving an application window is slow, especially when playing local videos.

## Identity Automation updates

- There is no change to the Identity Automation package version.
- **NOTE:** The broker server must be in the same domain as the Identity Automation server.
- **Supports Multiple Identity Automation servers on ThinOS**
  - On ThinOS, a new setting **Show Select Group Tray** has been added in **Advanced > Login Experience > Login Settings**. The default value is disabled.
  - After enabling the setting, an icon is displayed on the ThinOS system taskbar. You can use the select group function by clicking this icon.
  - The icon is not displayed on the system taskbar after logging in successfully.
  - For Identity Automation, you can configure a different Identity Automation server in a different group and switch between Identity Automation servers by selecting another group.
  - **Limitation:** When the setting is enabled, tap-over in Identity Automation only works in the same Identity Automation server. Tapping over between different Identity Automation servers is not supported. If you want to tap in with another Identity Automation server, log off from the current user and switch to another Identity Automation server through the select group icon.

## Cisco WebEx Meetings VDI update

- Cisco WebEx Meetings VDI package version has been updated to 43.10.2.11.2.

## Cisco Webex VDI update

- Cisco WebEx VDI package version is updated to 43.10.0.27605.1.

- **New features**

- Create a space for the group to talk.
- Turnoff Read Receipts: A read receipt lets you know who has seen a message.
- Changing Profile status: You can set the status to **Busy** or **Do not Disturb**.
- Notification sounds when someone is waiting in the lobby.
- Move Meeting to another desktop.

## Zoom

- Zoom Citrix package version is updated to 5.16.0.24280.1.
- Zoom AVD package version is updated to 5.16.0.24280.1.
- **New Features**
  - Redesigned annotation toolbar
  - Enhanced window merge-ins
  - Team Chat Thread Summary with Zoom AI Companion
  - Redesigned captioning controls
  - Enhanced Q&A usability in a webinar

## ControlUp

- The ControlUp package `ControlUp_VDI_Agent_2.2.5` supports analyzing the client and VDI resources.

## Systancia Workplace Broker

- Systancia Workplace Broker agent version is updated to 6.1 SP4.
- To access the broker, enter the URL **FQDN/applidixml/broker.asp**.
- Supports RDP for VDI sessions using the Systancia Workplace broker. AVD application package must also be installed.

**Table 33. Systancia Workplace broker feature matrix**

RDP/ThinOS	Category Supported	Feature	ThinOS 2311
RDP	Input	Keyboard	Supported
		Mouse	
		Single Touch	
	Session	Keyboard	
		Mouse	
	Audio Visual	Single Touch	
		Desktop	
		Remote App (Immersive)	
	Storage	Audio in	
	Clipboard	Audio out	
	Redirections	Camera	
		Folder/Drive Redirection	
	Session Experience	Clipboard (text)	
		Printer	
Smart Card			
Dynamic Resolution			

**Table 33. Systancia Workplace broker feature matrix (continued)**

RDP/ThinOS	Category Supported	Feature	ThinOS 2311
	Graphics (CODECs)	Desktop Scale Factor	
		Multi-Monitor (All)	
		Restricted full screen session	
		Time Zone Mapping	
		Video/Audio/Online playback	
		H.264 Hardware Acceleration	
ThinOS	Login Settings	Username	Supported
		Password	
		Default Domain	
		Single Button Connect	
		Logo for Login Window	
		Show the password for the login window	
	Session Settings	Session Reconnect	
		Enable NLA	
		Force Span	
		Record From Local	

## ThinOS enhancements

- **Security improvement for FIPS**—After enabling FIPS, you cannot use the 1024 key-size certificate for wired or wireless EAP-TLS authentication. 2048 or larger key-size certificate is required for EAP-TLS authentication with FIPS enabled.
- **Supports disabling Windows key**—You can disable the Windows key in the **Peripherals** window of the **Keyboard** tab from ThinOS 2311. To disable, enter **WIN** in **Disable keys** option, and click **OK**.
- **Added Bluetooth icon on ThinOS taskbar** —Clicking the Bluetooth icon displays the connection status of the Bluetooth device. If the Bluetooth of the thin client is not available, the Bluetooth icon is not displayed.
- **Added Enable Automatic Switching option**—The option is added in the **Peripherals** window of the **Bluetooth** tab and is selected by default when connecting a Bluetooth headset. The Bluetooth audio profile also automatically sets to **Streaming (A2DP)**. But if a session launches any UC applications, the microphone of the Bluetooth headset works and the Bluetooth audio profile automatically changes to **UC(HSP/HFP)**.
- **Added a new option PCL6 for Printer Class**—In the printer setup window, there is a new option **PCL6** for printer class. The option is only applicable for specific driver usage in ICA and AVD/RDP sessions.
- **Supports Wave job from Wyse Management Suite server**—The client can support scheduling a Wave job from a Wyse Management Suite server to install Firmware, BIOS, and applications.
  - **NOTE:** Do not set Firmware, BIOS, Application policy in the groups you want to schedule the Wave job, and do not enable **Auto merge & publish after completion** in Wave.
- **Changed the name of the button from Install Now to Update Now**—When you receive the Firmware, BIOS, applications update policy from the Wyse Management Suite server, **Install Now** is changed to **Update Now** in the dialog box.
- **Supports WiFi 6E**—The WiFi 6E regions that are supported on ThinOS are as follows:

**Table 34. WiFi6E regions and versions**

Region	First supported ThinOS version
Morocco	ThinOS 2311
Australia and New Zealand	ThinOS 2306
Chile	ThinOS 2306

**Table 34. WiFi6E regions and versions (continued)**

Region	First supported ThinOS version
Malaysia	ThinOS 2306
United Kingdom and EU	ThinOS 2303
United States of America	ThinOS 2205

• **Supports OptiPlex All-in-One 7420**

- The following hardware configurations are supported:

**Table 35. Configurations supported on OptiPlex All-in-One 7420**

Hardware Type	Hardware
CPU	Intel - 300
	Intel - 300T
	Intel - I3-14100
	Intel - I3-14100T
	Intel - i3-12100T
	Intel - i5-12500T
	Intel - I5-14500
	Intel - I5-14500T
	Intel - I5-14600
	Intel - I5-14600T
Memory	8 GB x 1
	8 GB x 2
	16 GB x 1
	16 GB x 2
	32 GB x 1
Storage	M.2 2230 256GB Class 35
	M.2 2230 512GB Class 35
	M.2 2230 512GB Class 40
Camera	FHD + HDR
Wireless	Intel AX201
	Intel AX211
Display	FHD
	FHD + Touch

- The following hardware configurations are not supported:

**Table 36. Configurations not supported on OptiPlex All-in-One 7420**

Hardware Type	Hardware
SD card slot	SD card
Storage	SED storage
	Hard drive storage
Wireless	Realtek wireless

**Table 36. Configurations not supported on OptiPlex All-in-One 7420 (continued)**

Hardware Type	Hardware
HDMI in	HDMI in port

## Updates to Admin Policy Tool and Wyse Management Suite policy settings

**NOTE:** Wyse Management Suite 4.2 server is required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

- **Added Show Username in Lock Terminal**—Added an option **Show Username** in **Login Experience > Login Settings > Lock Terminal**.
- **Added Show Select Group Tray**
  - Added a setting **Show Select Group Tray** in **Advanced > Login Experience > Login Settings**.
  - The default value is disabled.
  - After the setting is enabled, ThinOS moves some groups from the login window to the ThinOS system taskbar.
  - You can also sync with Wyse Management Suite in real-time when adding or removing a child group.
  - The setting applies to all types of brokers and third party logins of ThinOS.
  - Ensure that each child group has enabled the setting when using this feature.
- **Updated Item name and tooltips of Allow USB Image Family Device redirection**—The policy name in **Advanced > Session Settings > Blast Session Settings** is updated to **Allow USB Image Family Device redirection**. The policy is applicable for iPhone, Samsung, and other devices with class ID 06.
- **Added WebLogin Use External Browser and External Browser Type**—Added a setting **WebLogin Use External Browser** and **External Browser Type** in **Broker Settings > Citrix Virtual Apps and Desktops Settings** to enable FIDO2 security key to log in to Citrix NetScaler using Citrix Enterprise Browser (CEB) browser.
- **Added RDP Audio Playback**—The option is in **Advanced > Session Settings > RDP and AVD Session Settings**, and it determines the audio playback mode. The option works for the sessions that are published in broker.
- **Added Enable Auto Switching**—The option is in **Advanced > Network Configuration > Bluetooth Settings**, and the default value is **Enable**.
- **Added a new option PCL6 for Printer Class**—In the printer setup window, there is a new option **PCL6** for printer class. The option is only applicable for specific driver usage in ICA and AVD/RDP sessions.
- **Added Enable Schedule Update**
  - The option is in **Services > WDA Settings** and helps schedule a time to update the Firmware, BIOS, and Applications.
  - If you click **Cancel** or **x**, the device updates after the next reboot.
  - If you click **OK** to close the schedule update window, the device updates at the scheduled time.
  - If you soft reset the device, you can remove the scheduled time.
  - You can also change the current time of the client, which is later than the scheduled time. For example, if the current time is 9:00 AM, the scheduled update time is 9:20 AM, and you change the local time on your system to a new time 9:30 AM, the device updates immediately.
- **Added Enable Group Change on Next Reboot**
  - The option is in **Services > WDA Settings**.
  - If enabled, when moving devices between groups, policies from the new group on the Wyse Management Suite server is applied to the client only after restart.
- **Updated Item names for Scheduled Reboot/Scheduled Shutdown Settings**—The option is in **Advanced > System Settings**, where you can choose between **Scheduled Reboot**, **Scheduled Shutdown Settings**, **Reboot**, **Shutdown Week**, **No changes to Reboot**, or **Shutdown Week Offset**. The values are also changed to **+1 Week**, **+2 Weeks**, **+3 Weeks**, **+4 Weeks**.
- **Added Bluetooth icon**—The option is in **Privacy & Security > Account Privileges**. When enabled, you can see the Bluetooth icon on the taskbar.
- **Added Self Service**—Self-Service option is added in **Broker Settings > Global Broker Settings**. You can add your self-service URL, and ThinOS creates a link icon in the VDI menu. Click the link icon to open the self-service website.
  - **NOTE:** You must add the self-service URL with the prefix **https://**.
- **Added TLS Security Level**—Added **TLS Security Level** in **Privacy & Security > Security Policy**. The default level is 1.

- **Added Allow Legacy Renegotiation**—Added **Allow Legacy Renegotiation** in **Privacy & Security > Security Policy**. When enabled, ThinOS allows initial connection and renegotiation between OpenSSL and unpatched legacy servers. When disabled, ThinOS cannot connect to the servers.
- Added a BIOS page for Dell OptiPlex All-in-One 7420.
- **Updated VNC service to Remote Shadow Settings and added Remote Shadow Protocol option in P2P protocol**
  - Updated the option name **Enable VNC Daemon** to **Allow Remote Shadow**.
  - Updated the option name **Password** to **Remote Shadow Password** and changed the password field length requirement from eight characters to a minimum of nine characters.
  - Updated the option name **Enable VNC Prompt** to **Enable Remote Shadow Prompt**.
  - Added Remote Shadow Protocol **P2P Protocol** for Remote Shadow Protocols, which allows you to launch the remote shadow to the client from the Wyse Management Suite cloud server.
  - VNC Protocol and P2P Protocol cannot be applied simultaneously; select only one protocol to apply it.
  - VNC Protocol and P2P Protocol use the same password field. If you are upgrading from ThinOS 2308 and earlier and want to update any policy of **Remote Shadow Settings**, add at least one more character to the **Remote Shadow Password** field. Then, you can save and publish the policies. The VNC protocol uses the first eight characters, and the P2P Protocol uses the whole Remote Shadow Password.
  - Do not configure the P2P Protocol in the admin policy tool; it can only be configured from the Wyse Management Suite server.
  - **Limitation:** The option only supports to launch Remote Shadow P2P connection from the Wyse Management Suite server to the client with a single monitor. For multiple monitors, the option only supports viewing from the Wyse Management Suite cloud server.

**NOTE:** If you change the resolution of the client, restart the client and launch the Remote Shadow P2P connection from the Wyse Management Suite cloud server.

## Tested environments matrix

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

**Table 37. Tested environment—General components**

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.2
Configuration UI package for Wyse Management Suite	1.10.240
Citrix ADC (formerly NetScaler)	13.0
StoreFront	1912 LTSR and later

**Table 38. 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 (CU3)	Tested	Tested	Tested	Tested	Not tested	Tested
Citrix Virtual Apps and Desktops 7 2308	Tested	Tested	Tested	Tested	Not tested	Tested

**Table 39. 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 7.13.1	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested	Not tested	Not tested



**Table 39. 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 2022 APPs	Ubuntu 20.04
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
VMware Horizon 2303	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested
VMware Horizon 2306	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested

**Table 40. 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 41. Test environment – VMware Horizon Cloud version 2**

Horizon Cloud v2	Company Domain	Windows 10	Identity Provider	
www.cloud.vmware horizon.com	Hcseuc	Tested	Azure	Tested
			WS1 Access	Not tested

**Table 42. Test environment—Microsoft RDP**

Microsoft RDP	Windows 10	Windows 2012 R2	Windows 2016	Windows 2019	Windows 2022	APPs
Remote Desktop Services 2019	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2022	Tested	Not tested	Not tested	Not tested	Tested	Tested

**Table 43. Test environment—AVD**

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

**Table 44. Test environment—Windows 365 cloud PC**

Windows 365	Windows 10	Windows 11	Linux
Enterprise	Not tested	Tested	Not tested

**Table 45. 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)	Windows 10	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3)	Windows server 2019				
Citrix Virtual Apps and Desktops 7 2308	Windows server 2022 (Not tested)				

**Table 46. Tested environment—JVDI**

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	14.2.0.308051.8	14.2.1.58150	14.2.0.58008
	Windows 11			
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3)	Windows server 2016			
	Windows server 2019			
Citrix Virtual Apps and Desktops 7 2308	Windows server 2022 (Not tested)			

**Table 47. Tested environment—JVDI**

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 2209	Windows 10	14.2.0.308051.8	14.2.1.58150	14.2.0.58008
	Windows server 2016			
VMware Horizon View 7.13.2	Windows server 2019			

**Table 48. Tested environment—Zoom**

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	5.16.0.24280.1	5.16(24280)
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3)	Windows server 2016		
Citrix Virtual Apps and Desktops 7 2308	Windows server 2019		
	Windows server 2022 (Not tested)		

**Table 49. Tested environment—Zoom**

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 2209	Windows 10	5.15.2.23760.3	5.15.2 (23760)
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		

**Table 50. Tested environment—Zoom**

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.16.0.24280.1	5.16(24280)
	Windows server 2016		
	Windows server 2019		

**Table 51. Tested environment—Cisco Webex Teams**

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.10.0.27605.1	43.10.0.27605
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3)	Windows server 2016		
	Windows server 2019		
Citrix Virtual Apps and Desktops 7 2308	Windows server 2022 (Not tested)		

**Table 52. Tested environment—Cisco Webex Teams**

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 2209	Windows 10	43.10.0.27605.1	43.10.0.27605
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		

**Table 53. Tested environment—Cisco Webex Meetings**

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.10.2.11.2	43.10.2.11
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3)	Windows server 2016		
	Windows server 2019		
Citrix Virtual Apps and Desktops 7 2308	Windows server 2022 (Not tested)		

**Table 54. Tested environment—Cisco Webex Meetings**

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12	Windows 10	43.10.2.11.2	43.10.2.11
VMware Horizon 2209	Windows server 2016		
	Windows server 2019		

**Table 55. Tested environment—RingCentral**

VMware VDI	Operating system	RingCentral Package
Horizon 2111	Windows 10	23.2.20.4
Horizon View 7.13.2	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 56. 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 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

**Table 56. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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
	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

**Table 56. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

Product Category	Peripherals	3040	5070	5470 AIO	5470
	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
	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

**Table 56. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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
	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

**Table 56. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

Product Category	Peripherals	3040	5070	5470 AIO	5470
	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
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



**Table 56. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

Product Category	Peripherals	3040	5070	5470 AIO	5470
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 57. 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
	Stereo Headset WH1022 (Presto)
	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

**Table 57. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**


Product Category	Peripherals
	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
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726
	Dell Bluetooth Travel Mouse - MS700 - Black
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 19 Monitor E1920H - E1920H
	Dell 20 Monitor E2020H - E2020H
	Dell 22 Monitor - E2223HN - E2223HN
	Dell 22 Monitor - P2222H - P2222H
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 24 Monitor - P2422H - P2422H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 Monitor - P2722H - P2722H
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ

**Table 57. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE
	Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
	Dell UltraSharp 27 Monitor - U2724D - U2724D
	Dell UltraSharp 27 Thunderbolt Hub Monitor - U2724DE - U2724DE
Storage	Dell USB Slim DVD +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 Pro Webcam - Falcon - WB5023
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

## Supported ecosystem peripherals for Latitude 3420

**Table 58. 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  <b>NOTE:</b> 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 station	Dell Dock - WD19
Cables, Dongles, Adapters	Dell 7-in-1 USB-C Multiport Adapter - Slayer 3 MLK - DA310

## Supported ecosystem peripherals for OptiPlex 5400 All-in-One

**Table 59. 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

## Supported ecosystem peripherals for Latitude 3440

**Table 60. Supported ecosystem peripherals for Latitude 3440**

Product Category	Peripherals
Displays	Dell 24 USB-C Hub Monitor - P2422HE
	Dell 27 Monitor - 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
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

## Supported ecosystem peripherals for Latitude 5440

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

**Table 61. Supported ecosystem peripherals for Latitude 5440**

Product Category	Peripherals
Monitors	Dell 27 USB-C HUB Monitor - P2723DE
	Dell Collaboration 24 Monitor - C2423H
Input Devices	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
Audio/Video	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Speakerphone - Mozart - SP3022
	Dell Pro Webcam - Falcon - WB5023

**Table 61. Supported ecosystem peripherals for Latitude 5440 (continued)**

Product Category	Peripherals
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 All-in-One 7410

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

**Table 62. Supported ecosystem peripherals for OptiPlex All-in-One 7410**

Product Category	Peripherals
Monitors	Dell 24 Monitor - P2423D
	Dell UltraSharp 24 Monitor - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022

## Supported ecosystem peripherals for OptiPlex All-in-One 7420

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

**Table 63. Supported ecosystem peripherals for OptiPlex All-in-One 7420**

Product Category	Peripherals
Monitors	Dell 24 Monitor - P2423D
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W

## Third-party supported peripherals

**Table 64. 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

**Table 64. Third-party supported peripherals (continued)**

Product Category	Peripherals
	Plantronics SAVI W740/Savi W745 (Support USB only, not support Bluetooth)
	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)
	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 ET2201L IntelliTouch ZB (Worldwide) - E382790
	Elo ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473
	Elo PCAP E351600 - ET2202L-2UWA-0-BL-G
Camera	Logitech C920 HD Pro Webcam

**Table 64. Third-party supported peripherals (continued)**

Product Category	Peripherals
	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 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 CT30 V2 Gemalto IDBridge CT30 V3 Gemalto IDBridge CT710 GemPC Twin

**Table 64. Third-party supported peripherals (continued)**

<b>Product Category</b>	<b>Peripherals</b>
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
	Imprivata HDW-IMP-80-MINI
	Imprivata HDW-IMP-82-MINI
	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	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 in VMware PCoIP sessions, add **0x05541001, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.
- If you are using Power Mic 4 in VMware PCoIP sessions, add **0x05540064, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.

## Supported smart cards

**Table 65. Supported smart cards**

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2	Supported	Supported	Supported
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c	Supported	Supported	Supported
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8	Supported	Supported	Not Available
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 7.0 (T=0)	Supported	Supported	Not Available

**Table 65. Supported smart cards (continued)**

<b>Smart Card info from ThinOS event log</b>	<b>Smart Card Middleware in VDI</b>	<b>Provider (CSP)</b>	<b>Card type</b>	<b>Citrix</b>	<b>VMware (works for Blast and PCoIP, not RDP)</b>	<b>RDS (works for broker login, and not in sessions)</b>
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available

**Table 65. Supported smart cards (continued)**

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	G&D STARCOS 3.0 T=0/1 0V300	Supported	Not Available	Supported
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2	Supported	Not Available	Supported
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Enhanced Cryptographic Provider v1.0	YubiKey 4.3.3	Supported	Not Available	Supported
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Enhanced Cryptographic Provider v1.0	YubiKey 4.3.3	Supported	Not Available	Supported
cv cryptovision gmbh (c) v1.0ns	cv_act_scint erface_7.1.15	cv act sc/ interface CSP	G&D STARCOS 3.2	Supported	Not Available	Supported
N/A (Buypass BelDu)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	BelDu 6.0.4	Supported	Not Available	Supported
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	IDPrime SIS 4.0.2	Supported	Not Available	Supported
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)	Supported	Supported	Supported
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)	Supported	Supported	Supported

## Fixed Issues

**Table 66. Fixed issues**

Issue ID	Description
DTOS-21963	Audio is low while using Jabra headset in Webex meetings.
DTOS-21923	Connectivity issues with 5070 Thin clients connection to the Ethernet port of the Dell WD22TB4 dock.
DTOS-21486	Horizon SDK displays certificate errors when <b>Security Mode</b> is set to <b>Warning</b> or <b>Full</b> .
DTOS-21331	On OptiPlex 3000 systems, AVD and Microsoft Teams Unified Communication Optimization does not work.
DTOS-21325	On OptiPlex 3000 systems with ThinOS 2308, the supported OMNIKEY 5321 V2 is not redirected to Citrix VDI .

**Table 66. Fixed issues (continued)**

Issue ID	Description
DTOS-21303	On OptiPlex 3000 systems with ThinOS 2308, the AVD password character + is not recognized in AVD-RDWEB login.
DTOS-21224	In Imprivata login, you must enter the PIN twice when logging in for the first time to set or store the PIN.
DTOS-21205	Certificate issue while connecting to VMware environment with client SDK on ThinOS 9.x.
DTOS-21197	On 5070 systems with ThinOS 2211, the AVC H.264 encoding does not seem to be leveraged.
DTOS-20666	In ThinOS 2308, a <b>Could not load account</b> error message is displayed in Citrix sessions after upgrade.
DTOS-20584	PowerMic does not redirect into AVD sessions.
DTOS-20567	Citrix Password Reset field is blank.
DTOS-20556	ThinOS VNC Server ends connection with Eggplant software client.
DTOS-20496	Devices do not communicate with Wyse Management Server.
DTOS-20260	RDP missing credentials dialog box is displayed when session reconnect is set to more than five s.
DTOS-20247	VMware Linux login restriction issues on ThinOS 2306.
DTOS-20246	If an expired certificate is removed, Wyse Management Server does not get the information.
DTOS-20239	Unable to use the disabled key configuration to disable the <b>WIN</b> key.
DTOS-20204	Keyboard commands for copy or paste intermittently do not work after updating firmware and packages.
DTOS-20203	Dell Slim Soundbar SB522A does not map audio to RDP sessions.
DTOS-19837	PCL-6 class is not available in the Admin Policy Tool or Wyse Management Server configuration on ThinOS 9.
DTOS-19544	On OptiPlex thin clients with ThinOS 2306, Published Apps take 20-30 s to launch.
DTOS-19241	The mouse cursor leaves trails on the screen in the EPIC application.
DTOS-18848	ThinOS 9 maps the disk specifically to a drive letter.
DTOS-22026	Static IP for WiFi adapter is invisible and deleted after WiFi profile is deleted.
DTOS-21329	VMware KIOSK login does not work when manually entering a password.
DTOS-21305	System variables cannot be used in the certificate name in VPN settings.

# Known Issues

Table 67. Known Issues

Key	Summary	Workaround
DTOS-22261	After connecting the uplink cable to Latitude 5440, you cannot increase or decrease the volume using C2423H Monitor Touch button in a dual monitor setup.	Adjust volume using ThinOS user interface.
DTOS-21889	An incorrect event log status is displayed for launched Citrix VDA sessions.	Not Available
DTOS-21731	In Zoom, you cannot turn off the external camera after first attempt.	Replug the USB device.
DTOS-21723	After signing off from the AVD Session, the redirected USB devices do not come back to the local session.	Not Available
DTOS-21685	Microsoft Teams video of a user from an AVD session stops responding while sharing the screen in a VMware session.	Not Available
DTOS-21319	In Horizon Client SDK, the Microsoft Teams transfer window appears behind the video frame.	Not Available
DTOS-21127	Disable wired IEEE802.1x Authentication in the user interface is automatically enabled when <b>Save &amp; Publish</b> is clicked in the Admin Policy Tool.	Not Available
DTOS-20863	On OptiPlex 3000 systems with Intel Celeron processor, you cannot extract the CMOS settings.	Not Available
DTOS-20234	No logs are reported to the Wyse Management Suite server when uninstalling the package from Wyse Management Suite Firmware policy.	Not Available
DTOS-20228	While switching the audio in Microsoft Teams, videos in calls and meetings stops responding in other clients.	Not Available
DTOS-22644	Profile switching does not work after disabling and enabling the <b>Enable Auto Switching Profile</b> option while sharing the screen.	Restart the client.
DTOS-22640	AirPods Pro 2 does not work properly after disconnecting and reconnecting.	Restart the client.

# Citrix Workspace App 2308 for ThinOS 2308

## Release date

September 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

Citrix\_Workspace\_App\_23.8.0.39.1.pkg


## Previous version

Citrix\_Workspace\_App\_23.7.0.17.4.pkg

## Supported application package, firmware, and systems

### Supported application package

Citrix\_Workspace\_App\_23.8.0.39.1.pkg

 **NOTE:** For information about other packages, see ThinOS application package details in the [ThinOS 2308 \(9.4.3087\)](#) Release Notes.

### Supported Firmware

ThinOS 2308 (9.4.3087)

**Table 68. Supported systems**

Platform model
Wyse 5070 Thin Client
Wyse 5470 Thin Client
Wyse 5470 All-in-One Thin Client
OptiPlex 3000 Thin Client
Dell Latitude 3420
Dell OptiPlex 5400 All-in-One

**Table 68. Supported systems (continued)**

Platform model
Dell Latitude 3440
Dell Latitude 5440
Dell OptiPlex All-in-One 7410

**i** **NOTE:** Upgrade the ThinOS firmware to ThinOS 2308 (9.4.3087) before you install the application packages.

## Upgrade the application package using Wyse Management Suite

### Prerequisites

- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.
  - i** **NOTE:** If you have an existing group with a valid group token, you can register the thin client to the same group.
- Ensure that you have downloaded the ThinOS 9.x 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 **OS Firmware Updates**.
  - i** **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.

## Citrix Workspace app feature matrix

**Table 69. Citrix Workspace app feature matrix**

Feature	ThinOS 2308 with CWA 2308	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 Secure Private Access	Not Supported	Not Supported
	Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Not Supported	Not Supported
	SaaS/Web apps with SSO	Not Supported	Not Supported
	Citrix Mobile Apps	Not Supported	Not Supported
	App Personalization service	Not Supported	Not Supported

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
Workspace 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.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	Not Supported	Not Supported
	Citrix Auto updates	Not Supported	Not Supported
	Client App Management	Not Supported	Not Supported
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.
	SDWAN support	Not Supported	Not Supported
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	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.
	TWAIN 2.0	Not supported	Not supported
HDX Integration	Local App Access	Not Supported	Not Supported
	Multi-touch	Not Supported	Not Supported
	Mobility Pack	Not Supported	Not Supported
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.



**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	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.
	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+.
	File open in Citrix Workspace app	Not Supported	Not supported. No local file explorer on ThinOS.
	Location Based Services (Location available via API-description)	Not Supported	Not Supported
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	There are no limitations in this release.
	Video playback	Supported	There are no limitations in this release.
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Skype for business Optimization pack	Supported	Not support through proxy server

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
	Cisco Jabber Unified Communications Optimization	Supported	For more information, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Unified Communication Cisco WebEx Meetings Optimization	Supported	Dell Technologies recommends to wait for 10 s 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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Unified Communication Cisco WebEx VDI Optimization	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 <a href="http://www.dell.com/support">www.dell.com/support</a>
	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 <a href="http://www.dell.com/support">www.dell.com/support</a>
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
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 configuration support user auto-login and lock/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 Citrix ADC with PingID SAML MFA
	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.
App Protection	Not supported	Not supported	
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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	Not supported	Not supported
Authentication	Federated Authentication (SAML/Azure AD)	Supported	There are no limitations in this release.

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2308 with CWA 2308	Limitations
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)	Not supported	Not supported
User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
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)	Not supported	Not supported
ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor authentications are not qualified.
ADC Full VPN	Not supported	Not supported
ADC 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	Not supported	Not supported
Single Sign on to Citrix Mobile apps	Not supported	Not supported
Anonymous Store Access	Supported	There are no limitations in this release.
Netscaler + RSA	Not qualified	Not qualified
Citrix cloud + Azure Active Directory	Not supported	Not supported

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
	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 qualified	Not qualified
	Netscaler load balance	Not supported	Not supported
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported	There are no limitations in this release.
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session 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 setting in ThinOS	Supported	There are no limitations in this release.	
New features listed in Citrix Workspace app release notes but not in feature matrix	HTTPS protocol support for proxy server	Not Supported	Not Supported
	Support for MJPEG webcams	Not Supported	Not Supported

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
	Supports system certificate paths for SSL connection	Not Supported	Not Supported
	Enhanced virtual channel SDK	Not Supported	Not Supported
	Support for keyboard shortcut to switch between Full-screen and Window mode	Not Supported	Not Supported
	Policy tampering detection	Not Supported	Not Supported
	Webcam redirection and service continuity support for ARM64 devices	Not Supported	Not Supported
	Enable Packet Loss Concealment to improve audio performance	Not Supported	Not Supported
	Multi-touch support	Not Supported	Not Supported
	Support for IPv6 UDT with DTLS	Not Supported	Not Supported
	Script to verify system requirements for Windows Media Player redirection	Not Supported	Not Supported
	App Protection support for ARM64 devices	Not Supported	Not Supported
	Added support for playing short tones in optimized Microsoft Teams	Not Supported	Not Supported
	Support for IPv6 TCP with TLS	Not Supported	Not Supported
	Prerequisites for cloud authentication	Supported	There are no limitations in this release.
	Enhancement on 32-bit cursor support	Supported	There are no limitations in this release.
	Enhancement to support keyboard layout synchronization for GNOME 42	Not Supported	Not Supported
	Client IME for East Asian languages	Not Supported	Not Supported
	Support for authentication using FIDO2 when connecting to on-premises stores	Not Supported	Not Supported
	Copy and paste files and folders between two virtual desktops	Not Supported	Not Supported
	Support for ARM64 architecture	Not Supported	Not Supported
	Addition of client-side jitter buffer mechanism	Not Supported	Not Supported

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2308 with CWA 2308	Limitations
Support for more than 200 groups in Azure AD	Not Supported	Not Supported
Hardware acceleration support for optimized Microsoft Teams	Not Supported	Not Supported
Enhancement to sleep mode for optimized Microsoft Teams call	Not Supported	Not Supported
Background blurring for webcam redirection	Not Supported	Not Supported
Configure path for Browser Content Redirection overlay Browser temp data storage	Not Supported	From CWA2305, Citrix browser content redirection CEF cache file is changed from default .ICAClient to /tmp/citrix
Support for new PIV cards	Not Supported	Not Supported
Microsoft Teams enhancements-Limiting video resolutions	Not Supported	Not Supported
Microsoft Teams enhancements-Configuring a preferred network interface	Not Supported	Not Supported
Inactivity Timeout for Citrix Workspace app	Not Supported	Not Supported
Screen pinning in custom web stores	Not Supported	Not Supported
Support for 32-bit cursor	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit still 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	Not Supported	Not Supported
Background blurring and replacement for Citrix Optimized Teams	Supported	There are no limitations in this release.
Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.
Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2308 with CWA 2308	Limitations
Support for extended keyboard layouts	Supported	There are no limitations in this release.
Keyboard input mode enhancements	Not Supported	Not Supported
Support for authentication using FIDO2 in HDX session	Supported	There are no limitations in this release.
Support for secondary ringer	Supported	There are no limitations in this release.
Improved audio echo cancellation support	Not Supported	Not Supported
Composite USB device redirection	Not Supported	Not Supported
Support for DPI matching	Not Supported	Not Supported
Enhancement to improve audio quality	Not Supported	Not Supported
Provision to disable LaunchDarkly service	Not Supported	Not Supported
Email-based auto-discovery of store	Not Supported	Not Supported
Persistent login	Not Supported	Not Supported
Authentication enhancement for Storebrowse	Not Supported	Not Supported
Support for EDT IPv6	Not Supported	Not Supported
Support for TLS protocol version 1.3	Not Supported	Not Supported
Custom web stores	Not Supported	Not Supported
Authentication enhancement experimental feature	Not Supported	Not Supported
Keyboard layout synchronization enhancement	Not Supported	Not Supported
Multi-window chat and meetings for Microsoft Teams	Supported	There are no limitations in this release.
Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
Request control in Microsoft Teams	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 work when you give control to



**Table 69. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2308 with CWA 2308	Limitations
		other participant. This is a Microsoft limitation.
Support for cursor color inverting	Supported	<p>The following issues also occur in the Linux Citrix Workspace app binary:</p> <p>Sometimes, the I-shaped cursor disappears when the thin client is connected to a single monitor. As a workaround, signoff from your VDA desktop but do not disconnect the desktop.</p> <p>The I-shaped cursor is displayed in one monitor but disappears in another when the invert cursor option is enabled</p>
Microsoft Teams enhancement to echo cancellation	Supported	For limitations, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a>
Enhancement on smart card support	Supported	There are no limitations in this release.
Webcam redirection for 64-bit	Supported	There are no limitations in this release.
Support for custom web stores	Not Supported	Not Supported
Workspace with intelligence	Not Supported	Not Supported
Session reliability enhancement	Supported	There are no limitations in this release.
Enhancement to logging	Supported	There are no limitations in this release.
Adaptive audio	Supported	There are no limitations in this release.
Storebrowse enhancement for service continuity	Not Supported	Not Supported
Global App Config Service	Not Supported	Not Supported
EDT MTU discovery	Not Supported	Not Supported
Creating custom user-agent strings in network request	Not Supported	Not Supported
Feature flag management	Not Supported	Not Supported
Battery status indicator	Supported	There are no limitations in this release.
Service continuity	Not Supported	Not Supported
User Interface enhancement	Not Supported	Not Supported
Pinning multi-monitor screen layout	Not Supported	Not Supported

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
	Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported
	Multiple audio	Supported	Multiple audio devices feature is not supported by Cisco JVDI. This is Cisco known limitation. To eliminate confusion or mistakes, multiple audio devices feature is dynamically disabled after JVDI package installed, and it is dynamically enabled after JVDI package is uninstalled. There is an 8 device limitation to be redirected to HDX session. That means the total number of playback and record devices on thin client must be <= 8, so that you are able to use multiple audio devices. If the total number of playback and record devices on thin client > 8, multiple audio devices do not work, and some of the audio devices may be missing in HDX session or the audio devices are displayed as Citrix HDX audio. This is Citrix VDA limitation.
	Citrix logging	Supported	There are no limitations in this release.
	Cryptographic update	Not Supported	Not Supported
	Transparent user interface (TUI)	Not Supported	Not Supported
	GStreamer 1.x supportexperimental feature	Supported	There are no limitations in this release.
	App indicator icon	Not Supported	Not Supported
	Latest webkit support	Supported	There are no limitations in this release.
	Bloomberg audio redirection	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support	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.

**Table 69. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2308	Limitations
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

## Citrix Workspace app updates

Citrix Workspace App (CWA) package version is updated to 23.8.0.39.1.

- Inverted cursor issue**—Citrix Workspace App 2308 fixes the inverted cursor disappearing issue when the thin client is connected to a single monitor. If the inverted cursor does not work in a single monitor after configuring the **InvertCursorEnabled=True** in **[Thinwire3.0]** section in the **wfclient.ini** configuration file, you can enable the 32-bit cursor by doing the following:
  - In Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.
  - In the **Citrix INI Settings**, click **Add Row**.
  - From the **File** drop-down list, select **wfclient.ini..**
  - From the **Operation** drop-down list, select **Add or Update**.
  - In the **Section** field, enter **Thinwire3.0**.
  - In the **Key** field, enter **Cursor32bitSupport**.
  - In the **Value** field, enter **True**.
  - Sign out or restart the device for the settings to take effect.
- Topaz Signature Pad issue**—Fixed the issue where the Topaz Signature Pad does not work properly in a second hop scenario. See [ThinOS 2308](#) section in the release notes to configure the Topaz Signature Pad in Citrix Configuration Editor.

### Citrix Workspace App Limitations

- The following issues also occur in the Linux Citrix Workspace app binary:
  - Sometimes, the I-shaped cursor disappears when the thin client is connected to a single monitor. As a workaround, signoff from your VDA desktop but do not disconnect the desktop.
  - The I-shaped cursor is displayed in one monitor but disappears in another when the invert cursor option is enabled.
- The following new features from Citrix Workspace app 2308 are not supported:
  - HTTPS protocol for proxy server
  - MJPEG webcams
  - System certificate paths for SSL connection
  - Enhanced virtual channel SDK
  - Keyboard shortcut to switch between Full-screen and Window mode
  - Policy tampering detection
  - Webcam redirection and service continuity support for ARM64 devices
  - Packet Loss Concealment to improve audio performance
  - Multi-touch

## Tested environments matrix

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

**Table 70. Tested environment—General components**

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.1 548 and WMS 4.1.1
Configuration UI package for Wyse Management Suite	1.10.207
Citrix ADC (formerly NetScaler)	13.0
StoreFront	1912 LTSR and later versions

**Table 71. 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	Not tested	Tested
Citrix Virtual Apps and Desktops 7 2305	Tested	Tested	Tested	Tested	Not tested	Tested

**Table 72. 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 2305	Windows 10	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
	Windows server 2019				
	Windows server 2022 (Not tested)				

**Table 73. Tested environment—JVDI**

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber 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 2305	Windows 10	14.1.4.307909.3	14.1.4.57909	14.1.4.57561
	Windows 11			
	Windows server 2016			
	Windows server 2019			
	Windows server 2022 (Not tested)			

**Table 74. 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 2305	Windows 10	5.15.2.23760.2	5.15.2 (23760)
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

**Table 75. Tested environment—Cisco Webex Teams**

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.4.0.25788.2	43.4.0.25959

**Table 75. Tested environment—Cisco Webex Teams (continued)**

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2) Citrix Virtual Apps and Desktops 7 2305	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

**Table 76. 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 2305	Windows 10	43.6.5.20.1	43.2.7.10
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

# ThinOS 2308

## Release date

August 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 2308 (9.4.3087)

## Previous version

ThinOS 2306 (9.4.2103)

## Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2308 (9.4.3087)**

**i** **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2308. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.

**i** **NOTE:** If you want to downgrade ThinOS 2308 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support). For the steps to access documents, see [Resources and support](#).

## Important notes

- Some features and product environments that are not tested by Dell Technologies are found to be working with other users. These features or product environments have been marked as **Not Qualified**.
- To further improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are going to be removed in the next release. Some TLS ciphers are not secure and are subject to change in the next release.

**Table 77. TLS Cipher list**

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Not secure and subject to change in the next release
ECDHE-RSA-AES256-SHA384	Not secure and subject to change in the next release


**Table 77. TLS Cipher list (continued)**

<b>Ciphers</b>	<b>Security Status</b>
ECDHE-RSA-AES128-SHA	Not secure and subject to removal in next release
ECDHE-RSA-AES256-SHA	Not secure and subject to removal in next release
DHE-RSA-AES128-GCM-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES256-GCM-SHA384	Not secure and subject to removal in next release
DHE-RSA-AES128-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES256-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES128-SHA	Not secure and subject to removal in next release
DHE-RSA-AES256-SHA	Not secure and subject to removal in next release
AES128-SHA256	Removed in ThinOS 2303
AES256-SHA256	Removed in ThinOS 2303
AES128-SHA	Removed in ThinOS 2303
AES256-SHA	Removed in ThinOS 2303
AES128-GCM-SHA256	Removed in ThinOS 2303
AES256-GCM-SHA384	Removed in ThinOS 2303
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Not secure and subject to change in the next release
ECDHE-ECDSA-AES256-SHA384	Not secure and subject to change in the next release
ECDHE-ECDSA-AES128-SHA	Not secure and subject to removal in next release
ECDHE-ECDSA-AES256-SHA	Not secure and subject to removal in next release
DHE-PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES256-GCM-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
DHE-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
DHE-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES128-CBC-SHA256	Not secure and subject to change in the next release
ECDHE-PSK-AES256-CBC-SHA384	Not secure and subject to change in the next release
PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
PSK-AES256-GCM-SHA384	Not secure and subject to removal in next release
PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
RSA-PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release

**Table 77. TLS Cipher list (continued)**

Ciphers	Security Status
RSA-PSK-AES256-GCM-SHA384	Not secure and subject to removal in next release
RSA-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
RSA-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
RSA-PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
RSA-PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
ECDHE-ECDSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
ECDHE-RSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
DHE-RSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
RSA-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
DHE-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
ECDHE-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
SRP-RSA-AES-256-CBC-SHA	Not secure and subject to removal in next release
SRP-AES-256-CBC-SHA	Not secure and subject to removal in next release
SRP-RSA-AES-128-CBC-SHA	Not secure and subject to removal in next release
SRP-AES-128-CBC-SHA	Not secure and subject to removal in next release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

- 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.

 **NOTE:** In ThinOS 2303, **Live Update** is disabled, but the thin client can download the operating system firmware and BIOS firmware in the background. However, the thin client cannot complete installation 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 turn on the thin client from a turn off state
- When you change the Wyse Management Suite group
- When a new firmware or an application notification is displayed on your thin client and if you click **Next Reboot**, the following is observed:
  - If you have changed the Wyse Management Suite group and if the files are downloaded from the new group, a notification is not displayed.
  - If the new firmware or application is downloaded in the same group, a notification is not displayed.
  - After a reboot, the firmware or application is automatically installed.
- If you have installed the `HID_Fingerprint_Reader` package, ensure that you have also installed the `Citrix_Workspace_App` package, or you cannot upgrade to the latest ThinOS version.
- If you configure settings, like brokers, locally in ThinOS 2308 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 device manually again to set a password locally in ThinOS. Otherwise, passwords, like the Broker agent 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 2308, turn on the device and disable the sleep mode. If the device 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 the 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:** Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2308. Install the latest application packages.

## Convert Ubuntu with DCA to ThinOS 2308

### Prerequisites

**Table 78. Supported conversion scenarios**

Platform	Ubuntu version	DCA-Enabler version
Latitude 3420	20.04	1.7.0-20 or later
OptiPlex 5400 All-in-One	20.04	1.7.0-20 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 the above table. For details on how to install DCA-Enabler in the Ubuntu operating system and upgrade it, see *Dell ThinOS 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support)

 **NOTE:** Microsoft AVD package that is released before ThinOS 2311 is removed automatically after upgrading to ThinOS 2311. Install the latest Microsoft AVD package.

- 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 2308.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2308.
- 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 ThinOS 2308, 2306, and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support).
- Ensure you have downloaded the Ubuntu to ThinOS 2308 conversion image.
- Extract the Ubuntu to ThinOS 2308 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.2-dtos0-amd64_signed.tar.gz` and ThinOS image `ThinOS_2308_9.4.3087.pkg`.

**NOTE:** The ThinOS image `ThinOS_2308_9.4.3087.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_2306_9.4.3087.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 that 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 2308 is in the factory default status. ThinOS 2308 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 79. 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

**Table 79. Error Log table (continued)**


Error Log	Resolution
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

**Table 80. ThinOS application package details**

Supported Application Packages
Cisco_Jabber_14.1.4.307909.3.pkg
Cisco_WebEx_Meetings_VDI_43.6.1.25.1.pkg
Cisco_WebEx_VDI_43.4.0.25788.2.pkg
Citrix_Workspace_App_23.7.0.17.4.pkg
Common_Printing_1.0.0.26.pkg
ControlUp_VDI_Agent_2.2.2.pkg
EPOS_Connect_7.4.0.2.pkg
HID_Fingerprint_Reader_210217.23.pkg
Identity_Automation_QwickAccess_2.0.4.1.6.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.5.6.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.6.2.4.3.pkg
Microsoft_AVD_2.2.2196.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_23.04.1.13.pkg
VMware_Horizon_2306.8.10.0.21964631.3.pkg
VMware_Horizon_ClientSDK_2306.8.10.0.21964631.6.pkg
Zoom_AVD_5.15.2.23760.3.pkg
Zoom_Citrix_5.15.2.23760.2.pkg
Zoom_Horizon_5.15.2.23760.3.pkg

 **NOTE:** For ThinOS 2308, it is recommended to install the latest application packages in the above table.

**NOTE:** After upgrading to ThinOS 2308, 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 2308, 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 4.1.1
- Configuration UI package 1.10.207

**NOTE:** Use Wyse Management Suite 4.1.1 server and Configuration UI package 1.10.207 for the new Wyse Management Suite ThinOS 9.x Policy features.

## ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2308 (9.4.3xxx)—ThinOS\_2308\_9.4.3xxx.pkg
- Ubuntu to ThinOS 2308 conversion build—ThinOS\_2308\_9.4.3xxx\_Ubuntu\_Conversion.zip

## BIOS packages

Table 81. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.24.0.pkg
Wyse 5470 Thin Client	bios-5470_1.20.0.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.21.0.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.13.2.pkg
Dell Latitude 3420	bios-Latitude_3420_1.29.0.pkg
Dell OptiPlex 5400 All-in-One	bios-OptiPlex5400AIO_1.1.29.pkg
Dell Latitude 3440	bios-Latitude3440_1.5.1.pkg
Dell Latitude 5440	bios-Latitude5440_1.5.0.pkg
Dell OptiPlex All-in-One 7410	bios-OptiPlexAIO7410_1.5.1.pkg

## Tested BIOS version for ThinOS 2308

Table 82. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.24.0
Wyse 5470 All-in-One Thin Client	1.21.0
Wyse 5470 Mobile Thin Client	1.20.0
OptiPlex 3000 Thin Client	1.13.2
Latitude 3420	1.29.0
OptiPlex 5400 All-in-One	1.1.29
Latitude 3440	1.5.1

**Table 82. Tested BIOS details (continued)**

Platform name	BIOS version
Latitude 5440	1.5.0
OptiPlex All-in-One 7410	1.5.1

## Citrix Workspace app feature matrix

**Table 83. Citrix Workspace app feature matrix**

Feature		ThinOS 2308 with CWA 2307	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 Secure Private Access	Not Supported	Not Supported
	Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Not Supported	Not Supported
	SaaS/Web apps with SSO	Not Supported	Not Supported
	Citrix Mobile Apps	Not Supported	Not Supported
	App Personalization service	Not Supported	Not Supported
Workspace 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.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	Not Supported	Not Supported
	Citrix Auto updates	Not Supported	Not Supported
	Client App Management	Not Supported	Not Supported
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.
	SDWAN support	Not Supported	Not Supported
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
	Session Sharing	Supported	There are no limitations in this release.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	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.
	TWAIN 2.0	Not supported	Not supported
HDX Integration	Local App Access	Not Supported	Not Supported
	Multi-touch	Not Supported	Not Supported
	Mobility Pack	Not Supported	Not Supported
	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.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	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.
	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+.
	File open in Citrix Workspace app	Not Supported	Not supported. No local file explorer on ThinOS.
Location Based Services (Location available via API-description)	Not Supported	Not Supported	

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
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	There are no limitations in this release.
	Video playback	Supported	There are no limitations in this release.
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Skype for business Optimization pack	Supported	Not support through proxy server
	Cisco Jabber Unified Communications Optimization	Supported	For more information, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Unified Communication Cisco WebEx Meetings Optimization	Supported	Dell Technologies recommends to wait for 10 s 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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
Unified Communication Cisco WebEx VDI Optimization	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	

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
			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 <a href="http://www.dell.com/support">www.dell.com/support</a>
	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 <a href="http://www.dell.com/support">www.dell.com/support</a>
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
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	<p>The following webview login environment configuration support user auto-login and lock/unlock terminal.</p> <ul style="list-style-type: none"> <li>Citrix Federated Authentication Service</li> <li>SAML with Microsoft Azure Active Directory</li> <li>Citrix ADC Native OTP</li> <li>Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA</li> <li>Citrix ADC with PingID SAML MFA</li> </ul>



**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	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.
	App Protection	Not supported	Not supported
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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	Not supported	Not supported
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)	Not supported	Not supported
	User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
	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)	Not supported	Not supported	

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
	ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor authentications are not qualified for ThinOS 2306.
	ADC Full VPN	Not supported	Not supported
	ADC 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	Not supported	Not supported
	Single Sign on to Citrix Mobile apps	Not supported	Not supported
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not qualified	Not qualified
	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 qualified	Not qualified
	Netscaler load balance	Not supported	Not supported
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported	There are no limitations in this release.
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session 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 setting in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	HTTPS protocol support for proxy server	Not Supported	Not Supported
	Support for IPv6 UDT with DTLS	Not Supported	Not Supported
	Script to verify system requirements for Windows Media Player redirection	Not Supported	Not Supported
	App Protection support for ARM64 devices	Not Supported	Not Supported
	Added support for playing short tones in optimized Microsoft Teams	Not Supported	Not Supported
	Support for IPv6 TCP with TLS	Not Supported	Not Supported
	Prerequisites for cloud authentication	Supported	There are no limitations in this release.
	Enhancement on 32-bit cursor support	Supported	There are no limitations in this release.
	Enhancement to support keyboard layout synchronization for GNOME 42	Not Supported	Not Supported
	Client IME for East Asian languages	Not Supported	Not Supported
	Support for authentication using FIDO2 when connecting to on-premises stores	Not Supported	Not Supported

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2308 with CWA 2307	Limitations
Copy and paste files and folders between two virtual desktops	Not Supported	Not Supported
Support for ARM64 architecture	Not Supported	Not Supported
Addition of client-side jitter buffer mechanism	Not Supported	Not Supported
Support for more than 200 groups in Azure AD	Not Supported	Not Supported
Hardware acceleration support for optimized Microsoft Teams	Not Supported	Not Supported
Enhancement to sleep mode for optimized Microsoft Teams call	Not Supported	Not Supported
Background blurring for webcam redirection	Not Supported	Not Supported
Configure path for Browser Content Redirection overlay Browser temp data storage	Not Supported	From CWA2305, Citrix browser content redirection CEF cache file is changed from default .ICAClient to /tmp/citrix
Support for new PIV cards	Not Supported	Not Supported
Microsoft Teams enhancements-Limiting video resolutions	Not Supported	Not Supported
Microsoft Teams enhancements-Configuring a preferred network interface	Not Supported	Not Supported
Inactivity Timeout for Citrix Workspace app	Not Supported	Not Supported
Screen pinning in custom web stores	Not Supported	Not Supported
Support for 32-bit cursor	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit still 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	Not Supported	Not Supported
Background blurring and replacement for Citrix Optimized Teams	Supported	There are no limitations in this release.
Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
	Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported
	Support for extended keyboard layouts	Supported	There are no limitations in this release.
	Keyboard input mode enhancements	Not Supported	Not Supported
	Support for authentication using FIDO2 in HDX session	Supported	There are no limitations in this release.
	Support for secondary ringer	Supported	There are no limitations in this release.
	Improved audio echo cancellation support	Not Supported	Not Supported
	Composite USB device redirection	Not Supported	Not Supported
	Support for DPI matching	Not Supported	Not Supported
	Enhancement to improve audio quality	Not Supported	Not Supported
	Provision to disable LaunchDarkly service	Not Supported	Not Supported
	Email-based auto-discovery of store	Not Supported	Not Supported
	Persistent login	Not Supported	Not Supported
	Authentication enhancement for Storebrowse	Not Supported	Not Supported
	Support for EDT IPv6	Not Supported	Not Supported
	Support for TLS protocol version 1.3	Not Supported	Not Supported
	Custom web stores	Not Supported	Not Supported
	Authentication enhancement experimental feature	Not Supported	Not Supported
	Keyboard layout synchronization enhancement	Not Supported	Not Supported
	Multi-window chat and meetings for Microsoft Teams	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
	Request control in Microsoft Teams	Supported	Users on ThinOS client cannot give control to other

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2308 with CWA 2307	Limitations
		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 work when you give control to other participant. This is a Microsoft limitation.
Support for cursor color inverting	Supported	Invert cursor does not work in Citrix VDA 2212, VDA 2203 CU2, VDA2303 Windows 10 and Windows 2019 desktop. This issue also occurs in Citrix Workspace app Linux binary.
Microsoft Teams enhancement to echo cancellation	Supported	For limitations, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a>
Enhancement on smart card support	Supported	There are no limitations in this release.
Webcam redirection for 64-bit	Supported	There are no limitations in this release.
Support for custom web stores	Not Supported	Not Supported
Workspace with intelligence	Not Supported	Not Supported
Session reliability enhancement	Supported	There are no limitations in this release.
Enhancement to logging	Supported	There are no limitations in this release.
Adaptive audio	Supported	There are no limitations in this release.
Storebrowse enhancement for service continuity	Not Supported	Not Supported
Global App Config Service	Not Supported	Not Supported
EDT MTU discovery	Not Supported	Not Supported
Creating custom user-agent strings in network request	Not Supported	Not Supported
Feature flag management	Not Supported	Not Supported
Battery status indicator	Supported	There are no limitations in this release.
Service continuity	Not Supported	Not Supported
User Interface enhancement	Not Supported	Not Supported
Pinning multi-monitor screen layout	Not Supported	Not Supported

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
	Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported
	Multiple audio	Supported	Multiple audio devices feature is not supported by Cisco JVDI. This is Cisco known limitation. To eliminate confusion or mistakes, multiple audio devices feature is dynamically disabled after JVDI package installed, and it is dynamically enabled after JVDI package is uninstalled. There is an 8 device limitation to be redirected to HDX session. That means the total number of playback and record devices on thin client must be $\leq 8$ , so that you are able to use multiple audio devices. If the total number of playback and record devices on thin client $> 8$ , multiple audio devices do not work, and some of the audio devices may be missing in HDX session or the audio devices are displayed as Citrix HDX audio. This is Citrix VDA limitation.
	Citrix logging	Supported	There are no limitations in this release.
	Cryptographic update	Not Supported	Not Supported
	Transparent user interface (TUI)	Not Supported	Not Supported
	GStreamer 1.x supportexperimental feature	Supported	There are no limitations in this release.
	App indicator icon	Not Supported	Not Supported
	Latest webkit support	Supported	There are no limitations in this release.
	Bloomberg audio redirection	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support	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.

**Table 83. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2308 with CWA 2307	Limitations
	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 84. ThinOS AVD Client Feature Matrix**

Category Supported	Features	ThinOS 2308
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
	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
	USB (General)	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



**Table 84. ThinOS AVD Client Feature Matrix (continued)**

Category Supported	Features	ThinOS 2308
Authentication	TS Gateway	Supported
	NLA	Supported
	SmartCard	Limited support
	Imprivata	Supported

## VMware Horizon feature matrix

**Table 85. VMware Horizon session and client package versions**

Horizon	Package version
Horizon Session SDK	VMware_Horizon_2306.8.10.0.21964631.3.pkg
Horizon Client SDK	VMware_Horizon_ClientSDK_2306.8.10.0.21964631.6.pkg

**Table 86. VMware Horizon feature matrix**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Broker Connectivity	SSL certificate verification	Supported	Supported
	Disclaimer dialog	Supported	Supported
	UAG compatibility	Supported	Partially Supported
	Shortcuts from server	Not Supported	Not Supported
	Pre-install shortcuts from server	Not Supported	Not Supported
	File type association	Not Supported	Not Supported
	Phonehome	Supported	Supported
Broker Authentication	Password authentication	Supported	Supported
	SAML authentication	Supported	Supported
	Single sign on	Supported	Supported
	RSA authentication	Supported	Partially Supported
	Integrated RSA SecurID token generator	Not Supported	Not Supported
	Radius - Cisco ACS	Supported	Supported
	Radius - SMS Passcode	Supported	Supported
	Radius - DUO	Supported	Supported
	Radius - OKTA	Supported	Supported
	Radius - Microsoft Network Policy	Supported	Supported
	Radius - Cisco Identity Services Engine	Supported	Supported
	Kiosk mode	Supported	Supported
	Remember credentials	Supported	Supported
	Log in as current user	Not Supported	Not Supported

**Table 86. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Nested log in as current user	Not Supported	Not Supported
	Log in as current user 1-way trust	Not Supported	Not Supported
	OS biometric authentication	Not Supported	Not Supported
	Windows Hello	Not Supported	Not Supported
	Unauthentication access	Supported	Supported
Smartcard	x.509 certificate authentication (Smart Card)	Supported	Partially Supported
	CAC support	Supported	Partially Supported
	.Net support	Supported	Supported
	PIV support	Supported	Partially Supported
	Java support	Supported	Supported
	Purebred derived credentials	Not Supported	Not Supported
	Device Cert auth with UAG	Supported	Not Supported
Desktop Operations	Reset	Only supported with VDI	Only supported with VDI
	Restart	Only supported with VDI	Only supported with VDI
	Log off	Supported	Supported
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported	Supported
	Multiple connections	Supported	Supported
	Multi-broker/multi-site redirection - Universal	Not Supported	Not Supported
	App launch on multiple end points	Supported	Supported
	Auto-retry 5+ minutes	Supported	Supported
	Blast network recovery	Supported	Supported
	Time zone synchronization	Supported	Supported
	Jumplist integration (Windows 7-Windows 10)	Not Supported	Not Supported
Client Customization	Command line options	Not Supported	Not Supported
	URI schema	Not Supported	Not Supported
	Launching multiple client instances using URI	Not Supported	Not Supported
	Preference file	Not Supported	Not Supported
	Parameter pass-through to RDSH apps	Not Supported	Not Supported
	Non interactive mode	Not Supported	Not Supported
	GPO-based customization	Not Supported	Not Supported
Protocols supported	Blast Extreme	Supported	Supported
	H.264 - HW decode	Supported	Supported
	H.265 - HW decode	Supported	Supported

**Table 86. VMware Horizon feature matrix (continued)**

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

**Table 86. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Connection Management	IPv6 only network support	Supported	Supported
	PCoIP IP roaming	Supported	Supported
Optimized Device Redirection	Serial (COM) Port Redirection	Supported	Supported
	Client Drive Redirection/File Transfer	Not Supported	Not Supported
	Scanner (TWAIN/WIA) Redirection	Supported	Supported
	x.509 Certificate (Smart Card/Derived Credentials)	Supported	Supported
	Storage Drive Redirection	Not Supported	Not Supported
	Gyro Sensor Redirection	Not Supported	Not Supported
Real-Time Audio-Video	Audio input (microphone)	Supported	Supported
	Video input (webcam)	Supported	Supported
	Multiple webcams and microphones	Not Supported	Not Supported
	Multiple speakers	Not Supported	Not Supported
USB Redirection	USB redirection	Supported	Supported
	Policy: ConnectUSBOnInsert	Supported	Supported
	Policy: ConnectUSBOnStartup	Supported	Supported
	Connect/Disconnect UI	Not Supported	Not Supported
	USB device filtering (client side)	Supported	Supported
	Isochronous Device Support	Only supported with VDI	Only supported with VDI
	Split device support	Supported	Supported
	Bloomberg Keyboard compatibility	Only supported with VDI	Only supported with VDI
Smartphone sync	Only supported with VDI	Only supported with VDI	
Unified Communications	Skype for business	Not Supported	Not Supported
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Teams	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Meeting	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams HID Headset	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops

**Table 86. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not Supported	Not Supported
	Directshow Redirection	Not Supported	Not Supported
	URL content redirection	Not Supported	Not Supported
	MMR Multiple Audio Output	Not Supported	Not Supported
	UNC path redirection	Not Supported	Not Supported
	Browser content redirection	Not Supported	Not Supported
Graphics	vDGA	Only supported with VDI	Only supported with VDI
	vSGA	Only supported with VDI	Only supported with VDI
	NVIDIA GRID vGPU	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Only supported with VDI	Only supported with VDI
	AMD vGPU	Only supported with VDI	Only supported with VDI
Mobile Support	Client-side soft keyboard	Not Supported	Not Supported
	Client-side soft touchpad	Not Supported	Not Supported
	Full Screen Trackpad	Not Supported	Not Supported
	Gesture Support	Not Supported	Not Supported
	Multi-touch Redirection	Not Supported	Not Supported
	Presentation Mode	Not Supported	Not Supported
	Unity Touch	Not Supported	Not Supported
Printing	VMware Integrated Printing	Supported	Supported
	Location Based Printing	Supported	Supported
	Native Driver Support	Not Supported	Not Supported
Security	FIPS-140-2 Mode Support	Supported	Supported
	Imprivata Integration	Supported	Supported
	Opswat agent	Not Supported	Not Supported
	Opswat on-demand agent	Not Supported	Not Supported
	TLS 1.1/1.2	Supported	Supported
	Screen shot blocking	Not Supported	Not Supported
	Keylogger blocking	Not Supported	Not Supported
Session Collaboration	Session Collaboration	Supported	Supported
	Read-only Collaboration	Supported	Supported
Updates	Update notifications	Not Supported	Not Supported
	App Store update	Not Supported	Not Supported
Other	Smart Policies from DEM	Supported	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)	Supported with VDI (Only basic connection is tested)

**Table 86. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Workspace ONE mode	Supported	Supported
	Nested - basic connection	Supported	Supported
	DCT Per feature/component collection	Not Supported	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported	Supported
	Auth Method - RSA SecurID	Supported	Supported
	Auth Method - X.509 Certificate (Smart Card)	Supported	Not Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported	Not Supported
	Auth Method - RADIUS	Supported	Supported
	Auth Method - SAML - 3rd Party Identity Provider	Supported	Supported

For detailed information about the VMware Horizon features, see the Horizon documentation at [docs.vmware.com](https://docs.vmware.com).

## New and enhanced features

### Citrix Workspace app updates

Citrix Workspace App (CWA) package version is updated to 23.7.0.17.4, and the package can install the Citrix Workspace App version 2307 on ThinOS.

- **Citrix HDX Realtime Media Engine (RTME)**—From Citrix Workspace app 2307, the RTME version is updated to 2.9.700-3000.
- **Support for secondary ringer in Microsoft teams optimized mode**
  - From ThinOS 2308 and Citrix Workspace app 2307, you can use the secondary ringer feature to select a secondary device on which you want to get the incoming call notification when Microsoft Teams is in optimized mode.
  - You cannot set a secondary ringer in the following cases:
    1. When you are not connected to more than one audio device.
    2. When the peripheral is not available (for example, a Bluetooth headset).
  - **NOTE:** The feature is available only after the roll-out of a future update from Microsoft Teams. To know when the update is rolled-out by Microsoft, see the Microsoft 365 road map. You can also see [www.citrix.com](https://www.citrix.com) for more details.
- **Citrix Workspace App Limitations**
  - Browser Content Redirection (BCR) takes long to load and play 4 K videos.
  - You can log in to Citrix server when the typed Citrix server address is invalid. For example, **https://FQDN/citrix/store/invalid**.
  - Sometimes, the fully redirected USB devices cannot be detected in an ICA session when users quickly launch, disconnect, or reconnect the session. The issue also occurs when using Imprivata to badge on and off the Citrix broker. Wait for more than 1 minute to reconnect the session or badge on the broker.
  - The following issues also occur in the Linux Citrix Workspace app binary:
    - ICA session disconnection is slow.
    - Failure to launch an ICA session from NetScaler when EDT is disabled from Citrix policy but **HDXOverUDP** is set as **Preferred** in client side.

- Invert cursor does not work from Citrix VDA2212.
- Microsoft Teams video image is stretched.
- The following new features from Citrix Workspace App 2307 are not supported in ThinOS:
  - HTTPS protocol support for proxy server.
  - Support for IPv6 UDT with DTLS.
  - Script to verify system requirements for Windows Media Player redirection.
  - App Protection support for ARM64 devices.
  - Support for playing short tones in optimized Microsoft Teams.

## Teradici PCoIP

- Teradici version is updated to 23.04.1.13 in ThinOS 2308.
- **PCoIP Ultra**
  - From ThinOS 2308 and Teradici PCoIP version 23.04.1.11, PCoIP Ultra by CPU is supported in PCoIP sessions on Teradici PCoIP agent version 19.5 or later.
  - PCoIP Ultra is optimized for lossless support with bit-exact color accuracy and preservation of content detail at the highest frame rates.
  - With PCoIP Ultra protocol enhancements, your experience with remote workstations is faster and more interactive.
  - **NOTE:** The CPUs on both the agent and the client machines must support the AVX2 instruction set.
  - **Limitation:** PCoIP Ultra is not supported on ThinOS 3040, 5070, 5470 AIO, 5470 MTC, and OptiPlex 3000 systems.
  - PCoIP Ultra can be used for those who require CPU-optimized delivery of 4 K Ultra HD, high-framerate video playback with efficient scaling across multicore CPUs leveraging AVX2 instruction sets.
  - To enable PCoIP Ultra features, turn on one of the following GPO settings in the PCoIP session:
    1. Open **Local Group Policy Editor** in the Teradici session.
    2. Open the **Run** dialog box using the Windows key and R key combination.
    3. Enter **gpedit.msc**.
    4. Click **Enter**.
    5. In the left pane, go to **Administrative Templates > PCoIP Session Variables**.
    6. Double-click **Configure PCoIP Ultra**.
    7. Select **Enabled**.
    8. Configure PCoIP Ultra to **CPU Offload** or **Automatic Offload**.
    9. Click **OK**.
    10. Close **Local Group Policy Editor**.

PCoIP Ultra settings take effect in the next PCoIP session.
  - **PCoIP Codec Indicator**—When enabling **PCoIP Ultra**, an on-screen indicator at the bottom-left corner of the screen is displayed. A dark blue dot indicates PCoIP Ultra CPU optimization.

## VMware Horizon Updates

- The Horizon package version is updated to Horizon Client 2306.8.10. in ThinOS 2308.
- Upgrade the Horizon package version to 2306.8.10.0.21964631 along with the ThinOS 2308 root image.
- **NOTE:** ThinOS Horizon Package VMware\_Horizon\_2303.8.9.0.21435420.3.pkg, VMware\_Horizon\_ClientSDK\_2303.8.9.0.21435420.16.pkg, and earlier versions are not compatible with ThinOS 2308 firmware image. You must install the latest Horizon package along with the ThinOS 2308 firmware update.
- **ThinOS Horizon Client SDK updates**
  - ThinOS Horizon Client SDK package version is updated to 2306.8.10.0.21964631.6.
  - Supports UAG with Radius authentication.
  - Supports UAG with SAML authentication.
  - Supports UAG with RSA SecurID authentication.
  - Supports quick disconnection in Horizon Blast sessions.
  - **Fixed issues**
    - Fixed the issue where Radius authentication does not authenticate your credentials after one failure attempt.
    - Fixed the Scanner Redirection issue.
    - Fixed the issue where Blast session disappears after changing the display mode.

- Features that are not supported in ThinOS Horizon Client SDK:
  - Horizon Cloud Next Gen connection
  - RDP session connection
  - Credential security service provider
  - Device certificate authentication
- **HID headset controls with optimized VDI Microsoft Teams**
  - You can use the buttons on your USB headset to begin and end audio and video calls on Microsoft Teams in Blast sessions in optimized mode.
  - No other special settings are required.
- **Supports Silent Launch**
  - When starting a session or application, you can choose to not display the launch session or application message. Select **Silent Launch** from the graphics interface or Wyse Management Suite settings.
  - In the ThinOS graphics interface, go to **Global Connection Settings > Session > Setting common to all sessions**, and check the **Silent Launch** checkbox. The default value is cleared.
  - In Wyse Management Suite settings, go to **Advanced > Session Settings > Global Session Settings > Advanced Settings**, and enable **Silent Launch**. The default value is disabled.
- **Supports PingID authentication in Horizon UAG**
  - ThinOS 9 supports PingID authentication in VMware Horizon with UAG VDI.
  - Before using PingID authentication, configure **PingID** as **Identity Provider** in VMware UAG, and add the VMware UAG application in PingID.
  - Follow these steps to log in to a VMware Horizon session using PingID authentication:
    1. Configure the Horizon server in the **ThinOS Broker Setup** page.
    2. Save the changes and reboot the client.
 

During ThinOS horizon connection initialization, the ThinOS web authentication page opens.
    3. Enter your PingID credentials.
 

ThinOS web authentication page closes automatically, and the Horizon login window opens.
    4. Enter your Horizon account credentials.
- **Default launcher in Horizon Workspace One Mode**—The default launcher is ThinOS Horizon Client when using Horizon Workspace One Mode, regardless of how it is configured in the **Preference** page.
- **VMware Horizon Limitations**
  - If you are unable to access the Samsung Galaxy S21 and Google Pixel 4a, follow these steps and add the configuration in Wyse Management Suite:
    1. Go to **Advanced > VDI Configuration Editor > Horizon Blast Configuration Editor**.
    2. In **Add Horizon Blast Key-Value Settings**, click **+Add Row**.
    3. In **File**, select **etc config**.
    4. In **Operation**, select **Add or Update**.
    5. Enter `usb.quirks.device0`.
    6. Enter `0x<vid>:0x<pid> skip-reset, skip-refresh, skip-setconfig, e.g., 0x04e8:0x6865 skip-reset, skip-refresh, skip-setconfig`
    7. Click **Save and Publish**.

## Imprivata updates

- The latest supported application version on ThinOS is `Imprivata_PIE_7.11.001.0045.48.pkg`.
- **Added Log out button**—With the latest update, you can log out of a locked ThinOS Imprivata PIW window. You can log out of the OneSign connection by clicking **Log off**.
- **Proximity Card Reader configurations**
  - ThinOS supports proximity cards with four configurations.
  - To verify the configurations, do the following:
    1. Go to **OneSign Server > Computer Policy**.
    2. Configure Card Readers Configuration 1 to 4
    3. Click **Save**.
    4. Configure OneSign server in ThinOS.
    5. Plug in the Proximity Card Reader.
    6. Log in to the OneSign server.



7. Plug out the reader.
8. Plug in the Windows system.
9. Open `pcProxConfig` to check the configurations.

## Cisco WebEx Meetings VDI update

- Cisco WebEx Meetings VDI package version has been updated to 43.6.1.25.1.
- Supports VMware Horizon 2306.

## Cisco Webex VDI update

- Cisco WebEx VDI package version is the same as ThinOS 2306, and the version is 43.4.0.25788\_2.

## Zoom

- Zoom Citrix package version is updated to 5.15.2.23760\_2.
- Zoom Horizon package version is updated to 5.15.2.23760\_3.
- Zoom AVD package version is updated to 5.15.2.23760\_3.
- **New error logging**—Included the VDI Plugin Connection Error code in Windows Management Instrumentation (WMI).
- Added an option to hide the call quality banner for Zoom phone.
- Added a registry key to prevent poor network connection, which may affect audio quality.

## RingCentral

- RingCentral package version is the same as ThinOS 2306, and the version is 23.2.20.1.


## ControlUp


- The ControlUp package `ControlUp_VDI_Agent_2.2.2` supports analyzing the client and VDI resources.
- WiFi data is displayed on the client.

## Common Printing

- Common Printing package version is updated to 1.0.0.26.

## ThinOS enhancements


- **Improvements to Operating system, BIOS, Application update process**
    - **Added battery capacity checking before system update process**
      - If the battery charge is lower than 50%, the update process does not start even when the power adapter is connected. Once the device is charged to 50%, the update process starts.
      - If the battery charge is 50% or higher, the update process starts even when the power adapter is not connected.
-  **NOTE:** When a new firmware or application notification is displayed on your thin client and you click **Next Reboot**, then after reboot the update process starts even when the battery charge is lower than 50%.
- **Scheduled App policy update**—If the power adapter is not connected to the client, the Scheduled App policy is ignored on the client.
  - **Activation License field**—Added **Activation License** field in **System Information > About** tab. If the value is **Inactive**, then the device needs a ThinOS Activation License from Wyse Management Suite server to enable the login function.
  - **Power on logo update**—To distinguish from BIOS Dell logo, **Loading** is displayed under the Dell logo when ThinOS is booting.

 **NOTE:** When booting, you may see the Dell Loading logo twice.

- **Added input validation for some printer fields**—Special characters / ? are not allowed in **LPD Queue Name** field in **LPD Printer settings**, **Printer Name** field in **Local Printer settings**, and **Printer Name** field in **SMB Printer settings**.

## Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **Enable Notice Window Resizable**—Added **Enable Notice Window Resizable** in **Login Experience > Login Settings**. When you enable this option, the text of the notice file automatically resizes the dialog box to show as much text as possible.
- **Silence Launch**—Added **Silence Launch** in **Advanced > Session Settings > Global Session Settings > Advanced Settings**. The default value is disabled. When enabled, a message about session or application launch is not displayed after starting the session or application.
- **Added input validation for some printer fields**—The special characters / ? cannot be used in **LPD Queue Name** field in **LPD Printer settings**, **Printer Name** field in **Local Printer settings**, and **Printer Name** field in **SMB Printer settings**.
- **Configuration 3 and 4 in RFIdeas Reader**—Configuration 3 and 4 are added under **RFIdeas Reader Settings** when **Set Card Type** is enabled.
- **Kerberos Realm**—The field is added in **Advanced > Privacy & Security > Kerberos**. If the field is empty, the client uses the UPN suffix as the Kerberos realm.
- **Use Only WMS Defined Wireless Configurations**—Added **Use Only WMS Defined Wireless Configurations** in **Network Configuration > Wireless Settings**. When enabled, all wireless SSIDs that are not defined in the Wyse Management Suite policy is removed from the ThinOS client.
- **Disk Map To**
  - Added **Disk Map To** setting in **Session Settings > Citrix Session Settings**.
  - You can only enter A to Z capital characters, and duplicate characters are omitted. For example, if you enter **GGZZEE**, only **GZE** is retained. The number of disks mapped to the session depends on the number of valid letters provided. If no letter is provided, all disks are mapped to the session with default driver letters.
  - Limitations:
    - If the **MapDiskTo** setting is configured, the mapped disk drive in an ICA session cannot be removed after plugging out the USB disk.
    - **Disk Map To** setting does not work when USB disk is not plugged in to the client before logging in to the Citrix broker.
- **Added Citrix USB File Settings in Citrix Configuration Editor**
  - You can configure the USB device redirection using the **Citrix USB File Settings** in Citrix Configuration Editor.
  - From ThinOS 2308, only the below setting is supported, to fully redirect the Topaz Signature pad into an ICA session:
    1. In the **Key** field, enter **CONNECT**.
    2. In the **Value** field, enter **vid=0403 pid=6001 disableselectconfig=1**.

 **NOTE:** The VID PID in the **Value** field must be replaced by the VID PID of your Topaz Signature pad.
  - The parameter **disableselectconfig** is supported in Citrix Workspace App 2308. With ThinOS 2308 and Citrix Workspace App 2307, the parameter **disableselectconfig** does not work.
  - If you have already configured Citrix USB File Settings to fully redirect the device, do not configure **USB Redirection** in **Peripheral Management > USB Redirection > vUSB Force Redirect**.

## Tested environments matrix

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

**Table 87. Tested environment—General components**

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.1 548 and WMS 4.1.1
Configuration UI package for Wyse Management Suite	1.10.207
Citrix ADC (formerly NetScaler)	13.0

**Table 87. Tested environment—General components (continued)**

Component	Version
StoreFront	1912 LTSR and later versions

**Table 88. 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	Not tested	Tested
Citrix Virtual Apps and Desktops 7 2305	Tested	Tested	Tested	Tested	Not tested	Tested

**Table 89. 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 7.13.1	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
VMware Horizon 2303	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested
VMware Horizon 2306	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested

**Table 90. 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 91. Test environment – VMware Horizon Cloud version 2**

Horizon Cloud v2	Company Domain	Windows 10	Identity Provider	
www.cloud.vmware horizon.com	Hcseuc	Tested	Azure	Tested
			WS1 Access	Not tested

**Table 92. Test environment—Microsoft RDP**

Microsoft RDP	Windows 10	Windows 2012 R2	Windows 2016	Windows 2019	Windows 2022	APPs
Remote Desktop Services 2019	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2022	Tested	Not tested	Not tested	Not tested	Tested	Tested

**Table 93. Test environment—AVD**

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

**Table 94. Test environment—Windows 365 cloud PC**

Windows 365	Windows 10	Windows 11	Linux
Enterprise	Not tested	Tested	Not tested

**Table 95. 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)	Windows 10	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2019				
Citrix Virtual Apps and Desktops 7 2305	Windows server 2022 (Not tested)				

**Table 96. Tested environment—JVDI**

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	14.1.4.307909.3	14.1.4.57909	14.1.4.57561
	Windows 11			
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016			
	Windows server 2019			
Citrix Virtual Apps and Desktops 7 2305	Windows server 2022 (Not tested)			

**Table 97. Tested environment—JVDI**

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

**Table 98. Tested environment—Zoom**

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	5.15.2.23760.2	5.15.2 (23760)
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016		
Citrix Virtual Apps and Desktops 7 2305	Windows server 2019		
	Windows server 2022 (Not tested)		

**Table 99. Tested environment—Zoom**

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 2209	Windows 10	5.15.2.23760.2	5.15.2(23760)
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		

**Table 100. Tested environment—Zoom**

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.15.2.23760.3	5.15.2(23760)
	Windows server 2016		
	Windows server 2019		

**Table 101. Tested environment—Cisco Webex Teams**

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.4.0.25788.2	43.4.0.25959
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016		
Citrix Virtual Apps and Desktops 7 2305	Windows server 2019		
	Windows server 2022 (Not tested)		

**Table 102. Tested environment—Cisco Webex Teams**

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 2209	Windows 10	43.4.0.25788.2	43.4.0.25959
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		

**Table 103. Tested environment—Cisco Webex Meetings**

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.6.5.20.1	43.2.7.10
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016		
Citrix Virtual Apps and Desktops 7 2305	Windows server 2019		
	Windows server 2022 (Not tested)		

**Table 104. Tested environment—Cisco Webex Meetings**

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12	Windows 10	43.6.5.20.1	43.2.7.10
VMware Horizon 2209	Windows server 2016		
	Windows server 2019		

**Table 105. Tested environment—RingCentral**

VMware VDI	Operating system	RingCentral Package
Horizon 2111	Windows 10	23.2.20.1
Horizon View 7.13.2	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 106. 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

**Table 106. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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
	Dell USB 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

**Table 106. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Not Available	Supported	Not Available	Not Available



**Table 106. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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	
P2317H	Supported	Supported	Not Available	Not Available	
P2319H	Not Available	Supported	Not Available	Supported	

**Table 106. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**


Product Category	Peripherals	3040	5070	5470 AIO	5470
	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
Storage	Dell Portable SSD, USB-C 250GB	Not Available	Supported	Not Available	Supported

**Table 106. 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 Latitude 3420

**Table 107. 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  <b>NOTE:</b> 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 station	Dell Dock - WD19
Cables, Dongles, Adapters	Dell 7-in-1 USB-C Multiport Adapter - Slayer 3 MLK - DA310

# Supported ecosystem peripherals for Latitude 3440

**Table 108. Supported ecosystem peripherals for Latitude 3440**

Product Category	Peripherals
Displays	Dell 24 USB-C Hub Monitor - P2422HE
	Dell 27 Monitor - 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
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

# Supported ecosystem peripherals for Latitude 5440

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

**Table 109. Supported ecosystem peripherals for Latitude 5440**

Product Category	Peripherals
Monitors	Dell 27 USB-C HUB Monitor - P2723DE
	Dell Collaboration 24 Monitor - C2423H
Input Devices	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
Audio/Video	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Speakerphone - Mozart - SP3022
	Dell Pro Webcam - Falcon - WB5023
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 110. Supported ecosystem peripherals for OptiPlex 3000 Thin Client**

Product Category	Peripherals
Audio Devices	Dell Pro Stereo Headset - Cortez - WH3022
	Dell Slim Soundbar - Ariana - SB521A

**Table 110. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	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 Stereo Headset WH1022 (Presto) 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 Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726 Dell Bluetooth Travel Mouse - MS700 - Black
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S Dell 19 Monitor - P1917S - P1917S - P1917S Dell 19 Monitor E1920H - E1920H Dell 20 Monitor E2020H - E2020H Dell 22 Monitor - E2223HN - E2223HN

**Table 110. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	Dell 22 Monitor - P2222H - P2222H
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 24 Monitor - P2422H - P2422H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 Monitor - P2722H - P2722H
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE
	Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
Storage	Dell USB Slim DVD +/- RW Drive - DW316 - DW316 - Agate - DW316
	Apricorn 1TB Aegis Padlock 256-bit AES Encrypted Hard Drive

**Table 110. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	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 Pro Webcam - Falcon - WB5023
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

## Supported ecosystem peripherals for OptiPlex 5400 All-in-One

**Table 111. 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

## 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 112. Supported ecosystem peripherals for OptiPlex All-in-One 7410**

Product Category	Peripherals
Monitors	Dell 24 Monitor - P2423D
	Dell UltraSharp 24 Monitor - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022

## Third-party supported peripherals

**Table 113. Third-party supported peripherals**

Product Category	Peripherals
Audio Devices	Jabra GN2000
	Jabra PRO 9450

**Table 113. Third-party supported peripherals (continued)**

Product Category	Peripherals
	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 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)
	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



**Table 113. Third-party supported peripherals (continued)**

<b>Product Category</b>	<b>Peripherals</b>
Displays	Elo ET2201L IntelliTouch ZB (Worldwide) - E382790
	Elo ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473
	Elo PCAP E351600 - 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
	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

**Table 113. Third-party supported peripherals (continued)**

Product Category	Peripherals
	Gemalto IDBridge CT30 V2
	Gemalto IDBridge CT30 V3
	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
	Imprivata HDW-IMP-80-MINI
	Imprivata HDW-IMP-82-MINI
	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	HP M403D
	Brother DCP-7190DW
	Lexmark X864de
	HP LaserJet P2055d
	HP Color LaserJet CM1312MFP
	BLED112HDW-IMP-IIUR (BLEdongle)
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 in VMware PCoIP sessions, add **0x05541001, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.
- If you are using Power Mic 4 in VMware PCoIP sessions, add **0x05540064, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.

## Supported smart cards

Table 114. Supported smart cards

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2	Supported	Supported	Supported
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c	Supported	Supported	Supported
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5	Supported	Supported	Not Available

**Table 114. Supported smart cards (continued)**

<b>Smart Card info from ThinOS event log</b>	<b>Smart Card Middleware in VDI</b>	<b>Provider (CSP)</b>	<b>Card type</b>	<b>Citrix</b>	<b>VMware (works for Blast and PCoIP, not RDP)</b>	<b>RDS (works for broker login, and not in sessions)</b>
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8	Supported	Supported	Not Available
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 7.0 (T=0)	Supported	Supported	Not Available
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported

**Table 114. Supported smart cards (continued)**

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	G&D STARCOS 3.0 T=0/1 0V300	Supported	Not Available	Supported
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2	Supported	Not Available	Supported
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Enhanced Cryptographic Provider v1.0	YubiKey 4.3.3	Supported	Not Available	Supported
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Enhanced Cryptographic Provider v1.0	YubiKey 4.3.3	Supported	Not Available	Supported
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_7.1.15	cv act sc/ interface CSP	G&D STARCOS 3.2	Supported	Not Available	Supported
N/A (Buypass BelDu)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	BelDu 6.0.4	Supported	Not Available	Supported
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	IDPrime SIS 4.0.2	Supported	Not Available	Supported
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)	Supported	Supported	Supported
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)	Supported	Supported	Supported

## Fixed Issues

**Table 115. Fixed issues**

Issue ID	Description
DTOS-19865	Wi-Fi EAP-PEAP (MSCHAPv2) does not work after reboot on OptiPlex 3000.
DTOS-19667	Specific USB to Serial adapter is not connected as COM port in ThinOS.
DTOS-19627	ThinOS 9.x unlock menu username noncase sensitive vulnerability.

**Table 115. Fixed issues (continued)**

Issue ID	Description
DTOS-19546	Hide Cursor on startup is not working on ThinOS 2306 in Wyse 5070.
DTOS-19376	Incorrect Citrix credentials through Citrix gateway causes issues on ThinOS 2306.
DTOS-19309	ELO ET1723L PCAP monitor does not work in ThinOS.
DTOS-19281	Select group RDP issues on ThinOS 9.4.2103 in Wyse 5070.
DTOS-18971	Unable to Unlock using Yubikey Smartcard in ThinOS 9 (Works in ThinOS8)
DTOS-18925	Topaz Signature fails to redirect to EPIC application.
DTOS-18889	Citrix session loses focus on the EPIC application.
DTOS-18877	<b>Invalid password, please enter password to retry message</b> is displayed when Imprivata service is down on ThinOS 2303.
DTOS-18875	Connection timeout message displayed when attempting to connect to direct RDP session.
DTOS-18871	Auto launch of application through Imprivata does not work as expected.
DTOS-18865	Keyboard randomly stops working in EPIC application.
DTOS-18847	Thin clients take around 30 s to reestablish wireless connection when roaming to a new access point.
DTOS-18836	Magtek swipe reader not redirecting into RDP on ThinOS 9.x
DTOS-18711	Keyboard randomly stops working in EPIC hyperspace application in Citrix session.
DTOS-18710	End-user agreement notice format is missing the Resizable=Yes parameter in ThinOS 2303
DTOS-18623	Graphical issues when using RDP to connect to RHEL8 on ThinOS 2303 in Wyse 5070
DTOS-18622	Microsoft RDS RemoteApp issue on ThinOS 9.x
DTOS-18621	30 s to disconnect from a Citrix session with a Dymo 450 printer connected on ThinOS 2303.
DTOS-18618	Multiple screens are shared as one screen in the Microsoft Teams application from AVD session.
DTOS-18617	Reauthentication window does not have the Logo set.
DTOS-18555	Poly EagleEye Mini camera green status indicator remains on OptiPlex systems with ThinOS 2303.
DTOS-18554	SmartCard Redirection is not working in the RDP session.
DTOS-18414	The screen stops responding or disconnects from VMware session after a few hours.
DTOS-18281	Horizon blast session fails to load Nvidia codec with ThinOS 9.
DTOS-17727	Proximity badge reader stops working after firmware update.
DTOS-17633	CAC card does not work in RDS session.
DTOS-17579	The default password fails to stay in the login window after disabling Single Button Connect.

**Table 115. Fixed issues (continued)**

Issue ID	Description
DTOS-17524	Horizon Scanner redirection: Fujitsu FI-8170 is not detected by ThinOS and is not redirected.
DTOS-17015	Ping latency is higher than ThinOS 9.1 in ThinOS 2211.
DTOS-16934	Fujitsu SP-1120N is not displayed in Scanner Redirection (Blast) in Wyse 5070 with ThinOS 9.1.4234.
DTOS-16846	WiFi roaming disconnects the RDP connection.
DTOS-16537	RDP mapped SmartCard (reader) takes 15 minutes to read the content of a card.
DTOS-14411	Incorrect Keyboard layout in the VDI should be NLE (Belgium) instead of FR (BEFR).

## Known Issues

**Table 116. Known Issues**

Key	Summary	Workaround
DTOS-20228	While switching audio in Microsoft Team Calls and Meeting, the video stops responding in other clients.	Turn the video OFF and ON again.
DTOS-19783	Touchpad does not work after waking Latitude 5440 or 3440 from Sleep mode when touchpad is being used before going into Sleep mode with the session launched.	Use a wired mouse or reboot client when the issue happens. Or, do not keep moving the mouse using touchpad before the system goes into Sleep mode.
DTOS-19903	Dell Logo displays three times while upgrading the build from 9.4.3053 to 9.4.3054.	Not Applicable
DTOS-19426	Share screen does not work on calls in Microsoft Teams, when the display resolution is 1920 x 1200.	Avoid using resolution 1920 x 1200 in Teams screen sharing.
DTOS-18552	Powermic-IV does not work properly with playback in PColP protocol sessions.	Not Applicable
DTOS-19516	The cursor does not move when using the trackball on the SpeechMike in PColP desktop.	Enable the relative mouse in the PColP icon.
DTOS-19613	The client reboots instead of shutting down after pressing the power button when connecting the special USB hub.	Do not use the USB hub.
DTOS-19584	Sometimes, Citrix session fails to launch after add wfclient.ini in APT.	Reboot the terminal.
DTOS-16503	Jabra Elite or Airpods Local Audio timer display is not smooth.	Not Applicable
DTOS-19991	Wyse 5070 Extended Pentium client takes more time to reboot.	Not Applicable
DTOS-19900	HID Ominkey 5422 compatibility issues.	Not Applicable
DTOS-19700	ThinOS local menu color is incorrect after login PIW.	Reopen the local menu.
DTOS-19931	Click Next, which reboots the client to install a package, installs when the battery is lower than 50%.	Connect power adapter.
DTOS-19620	Display Layout will merge once after changing the resolution.	Change the position of the display block manually.

**Table 116. Known Issues (continued)**

<b>Key</b>	<b>Summary</b>	<b>Workaround</b>
DTOS-20050	Copy and paste from ThinOS to session does not work.	Not Applicable
DTOS-19626	Failure to copy and paste image content from one ICA session to another ICA session.	Not Applicable



# ThinOS 2306

## Release date

June 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 2306 (9.4.2103)

## Previous version

ThinOS 2303 (9.4.1141)

## Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2306 (9.4.2103)**

**i** **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2306. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.

**i** **NOTE:** If you want to downgrade ThinOS 2306 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell Wyse ThinOS Version 2306 and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support). For the steps to access documents, see [Resources and support](#).

## Important notes

- Some features and product environments that are not tested by Dell Technologies are found to be working with other users. These features or product environments have been marked as **Not Qualified**.
- To further improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are going to be removed in the next release. Some TLS ciphers are not secure and are subject to change in the next release.

**Table 117. TLS Cipher list**

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Not secure and subject to change in the next release
ECDHE-RSA-AES256-SHA384	Not secure and subject to change in the next release


**Table 117. TLS Cipher list (continued)**

<b>Ciphers</b>	<b>Security Status</b>
ECDHE-RSA-AES128-SHA	Not secure and subject to removal in next release
ECDHE-RSA-AES256-SHA	Not secure and subject to removal in next release
DHE-RSA-AES128-GCM-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES256-GCM-SHA384	Not secure and subject to removal in next release
DHE-RSA-AES128-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES256-SHA256	Not secure and subject to removal in next release
DHE-RSA-AES128-SHA	Not secure and subject to removal in next release
DHE-RSA-AES256-SHA	Not secure and subject to removal in next release
AES128-SHA256	Removed in ThinOS 2303
AES256-SHA256	Removed in ThinOS 2303
AES128-SHA	Removed in ThinOS 2303
AES256-SHA	Removed in ThinOS 2303
AES128-GCM-SHA256	Removed in ThinOS 2303
AES256-GCM-SHA384	Removed in ThinOS 2303
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Not secure and subject to change in the next release
ECDHE-ECDSA-AES256-SHA384	Not secure and subject to change in the next release
ECDHE-ECDSA-AES128-SHA	Not secure and subject to removal in next release
ECDHE-ECDSA-AES256-SHA	Not secure and subject to removal in next release
DHE-PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES256-GCM-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
DHE-PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
DHE-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
DHE-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
ECDHE-PSK-AES128-CBC-SHA256	Not secure and subject to change in the next release
ECDHE-PSK-AES256-CBC-SHA384	Not secure and subject to change in the next release
PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release
PSK-AES256-GCM-SHA384	Not secure and subject to removal in next release
PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
RSA-PSK-AES128-GCM-SHA256	Not secure and subject to removal in next release

**Table 117. TLS Cipher list (continued)**

Ciphers	Security Status
RSA-PSK-AES256-GCM-SHA384	Not secure and subject to removal in next release
RSA-PSK-AES128-CBC-SHA	Not secure and subject to removal in next release
RSA-PSK-AES256-CBC-SHA	Not secure and subject to removal in next release
RSA-PSK-AES128-CBC-SHA256	Not secure and subject to removal in next release
RSA-PSK-AES256-CBC-SHA384	Not secure and subject to removal in next release
ECDHE-ECDSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
ECDHE-RSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
DHE-RSA-CHACHA20-POLY1305	Not secure and subject to removal in next release
RSA-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
DHE-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
ECDHE-PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
PSK-CHACHA20-POLY1305	Not secure and subject to removal in next release
SRP-RSA-AES-256-CBC-SHA	Not secure and subject to removal in next release
SRP-AES-256-CBC-SHA	Not secure and subject to removal in next release
SRP-RSA-AES-128-CBC-SHA	Not secure and subject to removal in next release
SRP-AES-128-CBC-SHA	Not secure and subject to removal in next release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

- 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.

 **NOTE:** In ThinOS 2303, **Live Update** is disabled, but the thin client can download the operating system firmware and BIOS firmware in the background. However, the thin client cannot complete installation 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 turn on the thin client from a turn 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 the HID\_Fingerprint\_Reader package, ensure that you have also installed the Citrix\_Workspace\_App package, or you cannot upgrade to ThinOS version 2306.
- If you configure settings, like brokers, locally in ThinOS 2306 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 device manually again to set a password locally in ThinOS. Otherwise, passwords, like the Broker agent 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 2306, turn on the device and disable the sleep mode. If the device 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 the 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:** Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2306. Install the latest application packages.

## Convert Ubuntu with DCA to ThinOS 2306

### Prerequisites

**Table 118. Supported conversion scenarios**

Platform	Ubuntu version	DCA-Enabler version
Latitude 3420	20.04	1.7.0-20 or later
OptiPlex 5400 All-in-One	20.04	1.7.0-20 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 ThinOS 2306 and 2303 Migration Guide* at [www.dell.com/support](http://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 2306.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2306.
- 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 ThinOS 2306 and 2303 Migration Guide* at [www.dell.com/support](http://www.dell.com/support).
- Ensure you have downloaded the Ubuntu to ThinOS 2306 conversion image.
- Extract the Ubuntu to ThinOS 2306 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.2-dtos0-amd64_signed.tar.gz` and ThinOS image `ThinOS_2306_9.4.2103.pkg`.

**NOTE:** The ThinOS image `ThinOS_2306_9.4.2103.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_2306_9.4.2103.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 2306 is in the factory default status. ThinOS 2306 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 119. 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

**Table 119. Error Log table (continued)**

Error Log	Resolution
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 Windows 10 IoT to ThinOS 2306

### Prerequisites

- **Supported scenarios**

**Table 120. Supported conversion scenarios**

Platform	Windows 10 IoT version	WDA version
Wyse 5070 Thin Client	Windows 10 Enterprise 2019 LTSC-MR2	14.6.9.x
Wyse 5470 All-in-One Thin Client		
Wyse 5470 Mobile Thin Client		
OptiPlex 3000 Thin Client	Windows 10 IoT Enterprise LTSC 2021	

- Ensure that you are running Windows 10 IoT version and WDA version according to above table.
- You must use Wyse Management Suite 4.1 or later versions.
- Ensure that there are enough ThinOS Activation device licenses on Wyse Management Suite 4.1 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The Windows IoT devices must be registered to Wyse Management Suite.
- Ensure that the power adapter is connected to the device.
- Ensure that you have downloaded the Windows IoT to ThinOS 2306 conversion image.
- Extract the Windows IoT to ThinOS 2306 conversion image to get the Conversion Installer file `ThinOS_Conversion_Tool.exe` and the ThinOS image `ThinOS_2306_9.4.2103.pkg`.

### Steps

1. Copy the conversion Installer file `ThinOS_Conversion_Tool.exe` to the Wyse Management Suite 4.1 or later version server repository. The server can be located by going to **Repository Location > repository > thinClientApps**.
2. On the Wyse Management Suite page, go to **Portal Administration > File Repository**.
3. Select the repository and click **Sync Files**. Wait for the synchronization to complete.
4. Go to **Apps & Data > OS Image Repository > ThinOS 9.x**.
5. Click **Add Firmware file**.
6. Upload the ThinOS image `ThinOS_2306_9.4.2103.pkg`.
7. Go to **Apps & Data > App Policies > Thin Client**.
8. Click **Add Advanced Policy**.
9. Enter the policy name, and select the Windows 10 IoT devices registered group.
10. Select **WinIoT** as **OS type**.
11. Check the **Show conversion packages** checkbox.
12. Click **Add app**, and select the conversion Installer file from the drop-down list.
13. Enter `/qn` in the **Install Parameters** field.
14. Click **Add app**, and select the ThinOS image file from the drop-down list.
15. Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
16. Click **Save**.
17. When prompted, click **Yes** to schedule a job.

18. For the **Run** option in **App Policy Job window**, select **Immediately**.

19. Click **Preview**.

20. Click **Schedule** in the next window.

The Windows IoT devices download the Conversion Installer file and the ThinOS image after which, installation begins. After rebooting four times, the conversion is complete, and the device auto boots to ThinOS.

### Important Notes

- If device is not connected to a power adapter, conversion fails.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than Windows IoT device number, or you cannot create Advanced Policy for conversion.
- After conversion, ThinOS is in factory default status. You must register ThinOS to Wyse Management Suite manually or by DHCP/DNS discovery.
- After you register the converted ThinOS devices to Wyse Management Suite, the ThinOS Activation devices license is consumed. After consuming the license, the conversion job is completed.
- If conversion fails, resolve the issue according to error log at `C:\Wyse\Dtos\TRT\DtosConversion.log` and reschedule the job from **Jobs > Schedule APP Policy**. If conversion fails, It is recommended that you install the ThinOS ISO image.

### Limitations

- If the Trusted Platform module (TPM) is locked, conversion fails. If you see the message **Error : Clear the TPM Manually from BIOS Settings and retrigger Conversion from WMS** in `DtosConversion.log`, clear the TPM manually in BIOS setup. Go to **BIOS Setup > Security > TPM** and check the **Clear** checkbox.
- If the message **A configuration change was requested to clear this computer's TPM (Trusted Platform Module)** is displayed, press the F12 key to clear the TPM and continue conversion process.

## Convert ThinLinux to ThinOS 2306

### Prerequisites

- **Supported scenarios**

**Table 121. Supported conversion scenarios**

Platform	ThinLinux version	WDA version
Wyse 3040 Thin Client	2.2.1.04	3.5.2-05
Wyse 5070 Thin Client		
Wyse 5470 Mobile Thin Client		

- Ensure that you are running ThinLinux version and WDA version according to above table.
- You must use Wyse Management Suite 4.1 or later versions.
- Ensure that there are enough ThinOS Activation device licenses on Wyse Management Suite 4.1 or later versions.
- Create a group in Wyse Management Suite with a group token.
- The ThinLinux devices must be registered to Wyse Management Suite.
- Ensure that the power adapter is connected to the device.
- Ensure that you have downloaded the ThinLinux to ThinOS 2306 conversion image.
- Extract the ThinLinux to ThinOS 2306 conversion image to get the Conversion Installer file `merlin-nonpxe_4.1.1-01_amd64.deb` and the ThinOS image `ThinOS_2306_9.4.2103_TL_Conversion.exe`.

### Steps

1. Copy the conversion Installer file `merlin-nonpxe_4.1.1-01_amd64.deb` to the Wyse Management Suite 4.1 or later version server repository. The server can be located by going to **Repository Location > repository > thinClientApps**.
2. Copy the conversion image `ThinOS_2306_9.4.2103_TL_Conversion.exe` to the Wyse Management Suite 4.1 or later version server repository. The server can be located by going to **Repository Location > repository > osimages > zipped**.
3. On Wyse Management Suite page, go to **Portal Administration > File Repository**.
4. Select the repository and click **Sync Files**. Wait for the synchronization to complete.
5. Go to **Apps & Data > App Policies > Thin Client**
6. Click **Add Advanced Policy**.

7. Enter the policy name and select the group with registered ThinLinux devices.
8. Select **ThinLinux** as **OS type**
9. Click **Add app**, and select the conversion Installer file from the drop-down list.
10. Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
11. Click **Save**.
12. When prompted, click **Yes** to schedule a job.
13. For the **Run** option in **App Policy Job window**, select **Immediately**.
14. Click **Preview**.
15. Click **Schedule** in the next window.  
The ThinLinux device downloads the conversion Installer file after which, installation begins.
16. Ensure that the conversion image is in the repository by going to **Apps & Data > OS Image Repository > WinIoT/ThinLinux**
17. Go to **Apps & Data > OS Image Policies > WinIoT/ThinLinux** and click **Add Policy**.
18. Enter the policy name, and select the ThinLinux devices registered group.
19. Select **ThinLinux** as **OS type**
20. Select **ThinLinux 2.x** as **OS Subtype Filter**.
21. Select **OS Image** as the conversion image.
22. Select **Force this version as Rule**.
23. Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
24. Click **Save**.
25. When prompted, click **Yes** to schedule a job.
26. For the **Run** option in **App Policy Job** window, select **Immediately**.
27. Click **Preview**.
28. Click **Schedule** in the next window.  
The ThinLinux device downloads the conversion image after which, installation begins. After installation, the devices automatically reboot to ThinOS.

**Important Notes**

- If device is not connected to a power adapter, conversion fails.
- The ThinOS Activation devices license number of Wyse Management Suite must be larger than ThinLinux device number, or you cannot create Advanced Policy for conversion.
- After conversion, ThinOS is in factory default status. You must register ThinOS to Wyse Management Suite manually or by DHCP/DNS discovery.
- After you register the converted ThinOS devices to Wyse Management Suite, the ThinOS Activation devices license is consumed. After consuming the license, the conversion job is completed.

## Compatibility

### ThinOS application package details

**Table 122. ThinOS application package details**

Supported Application Packages
Cisco_Jabber_14.1.3.307560.10.pkg
Cisco_WebEx_Meetings_VDI_43.2.5.22.1.pkg
Cisco_WebEx_VDI_43.4.0.25788.2.pkg
Citrix_Workspace_App_23.5.0.58.1.pkg
Common_Printing_1.0.0.23.pkg
ControlUp_VDI_Agent_1.0.0.1.34.pkg
EPOS_Connect_7.4.0.2.pkg



**Table 122. ThinOS application package details (continued)**

Supported Application Packages
HID_Fingerprint_Reader_210217.23.pkg
Identity_Automation_QwickAccess_2.0.4.1.6.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.5.4.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.6.2.4.3.pkg
Microsoft_AVD_2.1.2164.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_23.04.1.9.pkg
VMware_Horizon_2303.8.9.0.21435420.3.pkg
VMware_Horizon_ClientSDK_2303.8.9.0.21435420.16.pkg
Zoom_AVD_5.14.0.23370.2.pkg
Zoom_Citrix_5.14.0.23370.1.pkg
Zoom_Horizon_5.14.0.23370.1.pkg

- NOTE:** For ThinOS 2306, it is recommended to install the latest application packages in the above table.
- NOTE:** After upgrading to ThinOS 2306, 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 2306, 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 4.1
- Configuration UI package 1.9.986
- NOTE:** Use Wyse Management Suite 4.1 server and Configuration UI package 1.9.986 for the new Wyse Management Suite ThinOS 9.x Policy features.

## ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 2306 (9.4.2103)—ThinOS\_2306\_9.4.2103.pkg
- Ubuntu to ThinOS 2306 conversion build—ThinOS\_2306\_9.4.2103\_Ubuntu\_Conversion.zip
- Windows 10 IoT to ThinOS 2306 conversion build—ThinOS\_2306\_9.4.2103\_WinIoT\_Conversion.zip
- ThinLinux to ThinOS 2306 conversion build—ThinOS\_2306\_9.4.2103\_ThinLinux\_Conversion.zip

## BIOS packages

**Table 123. BIOS package**

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.22.0.pkg
Wyse 5470 Thin Client	bios-5470_1.18.1.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.19.0.pkg
OptiPlex 3000 Thin Client	bios-Op3000TC_1.9.1.pkg

**Table 123. BIOS package (continued)**

Platform model	Package filename
Dell Latitude 3420	bios-Latitude_3420_1.27.0.pkg
Dell OptiPlex 5400 All-in-One	bios-OptiPlex5400AIO_1.1.24.pkg
Dell Latitude 3440	bios-Latitude3440_1.3.0.pkg
Dell Latitude 5440	bios-Latitude5440_1.3.0.pkg
Dell OptiPlex All-in-One 7410	bios-OptiPlexAIO7410_1.3.1.pkg

## Tested BIOS version for ThinOS 2306

**Table 124. Tested BIOS details**

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.22.0
Wyse 5470 All-in-One Thin Client	1.19.0
Wyse 5470 Mobile Thin Client	1.18.1
OptiPlex 3000 Thin Client	1.9.1
Latitude 3420	1.27.0
OptiPlex 5400 All-in-One	1.1.24
Latitude 3440	1.3.0
Latitude 5440	1.3.0
OptiPlex All-in-One 7410	1.3.1

## Citrix Workspace app feature matrix

**Table 125. Citrix Workspace app feature matrix**

Feature	ThinOS 2306 with CWA 2303	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)	Not supported	Not supported
	Citrix Secure Private Access	Not supported	Not supported
	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

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2306 with CWA 2303	Limitations
	App Personalization service	Not supported	Not supported
Workspace 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.
	Global App Config service (Workspace)	Not supported	Not supported
	Global App Config service (StoreFront)	Not supported	Not supported
	App Store Updates/Citrix Auto updates	Not supported	Not supported
	Client App Management	Not supported	Not supported
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.
	Session Sharing	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	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	Not supported	Not supported
	Multi-touch	Not supported	Not supported
	Mobility pack	Not supported	Not supported
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2306 with CWA 2303	Limitations
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Bi-directional Content redirection	Not supported	Not supported
	URL redirection	Not supported	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.
	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+.
	File open in Citrix Workspace app	Not supported	Not supported. No local file explorer on ThinOS.
	Location Based Services (Location available through API description)	Not supported	Not supported
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	There are no limitations in this release.
	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 Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2306 with CWA 2303	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 Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2306 with CWA 2303	Limitations
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	Not supported	Not supported
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)	Not supported	Not supported
	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)	Not supported	Not supported
	ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2306 with CWA 2303	Limitations
		authentications are not qualified for ThinOS 2306.
NetScaler Full VPN	Not supported	Not supported
ADC 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	Not supported	Not supported
Single Sign on to Citrix Mobile apps	Not supported	Not supported
Anonymous Store Access	Supported	There are no limitations in this release.
Netscaler + RSA	Not qualified	Not qualified
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 qualified	Not qualified
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
	SHA2 Cert	Supported There are no limitations in this release.
	Smart Access	Not supported
	Remote Access via Citrix Gateway	Supported The following webview login environment configurations support autologin and lock or unlock terminal: <ul style="list-style-type: none"> <li>● Citrix Federated Authentication Service SAML with Microsoft Azure Active Directory</li> <li>● Citrix ADC Native OTP</li> </ul>

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2306 with CWA 2303	Limitations
			<ul style="list-style-type: none"> <li>• Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA</li> <li>• Citrix ADC with PingID SAML MFA</li> </ul>
	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.
	App Protection	Not supported	Not supported
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported	There are no limitations in this release.
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session 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 setting in ThinOS	Supported	There are no limitations in this release.



**Table 125. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2306 with CWA 2303	Limitations
New features listed in Citrix Workspace app release notes but not in feature matrix	Support for IPv6 TCP with TLS	Not Supported	Not Supported
	Prerequisites for cloud authentication	Supported	There are no limitations in this release.
	Enhancement on 32-bit cursor support	Supported	There are no limitations in this release.
	Enhancement to support keyboard layout synchronization for GNOME 42	Not Supported	Not Supported
	Client IME for East Asian languages	Not Supported	Not Supported
	Support for authentication using FIDO2 when connecting to on-premises stores	Not Supported	Not Supported
	Copy and paste files and folders between two virtual desktops	Not Supported	Not Supported
	Support for ARM64 architecture	Not Supported	Not Supported
	Addition of client-side jitter buffer mechanism	Not Supported	Not Supported
	Support for more than 200 groups in Azure AD	Not Supported	Not Supported
	Hardware acceleration support for optimized Microsoft Teams	Not Supported	Not Supported
	Enhancement to sleep mode for optimized Microsoft Teams call	Not Supported	Not Supported
	Background blurring for webcam redirection	Not Supported	Not Supported
	Configure path for Browser Content Redirection overlay Browser temp data storage	Not Supported	From CWA2305, Citrix browser content redirection CEF cache file is changed from default .ICAClient to /tmp/citrix
	Support for new PIV cards	Not Supported	Not Supported
	Microsoft Teams enhancements-Limiting video resolutions	Not Supported	Not Supported
	Microsoft Teams enhancements-Configuring a preferred network interface	Not Supported	Not Supported
Inactivity Timeout for Citrix Workspace app	Not Supported	Not Supported	

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2306 with CWA 2303	Limitations
Screen pinning in custom web stores	Not Supported	Not Supported
Support for 32-bit cursor	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit still 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	Not Supported	Not Supported
Background blurring and replacement for Citrix Optimized Teams	Supported	There are no limitations in this release.
Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.
Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported
Support for extended keyboard layouts	Supported	There are no limitations in this release.
Keyboard input mode enhancements	Not Supported	Not Supported
Support for authentication using FIDO2 in HDX session	Supported	There are no limitations in this release.
Support for secondary ringer	Not Supported	Not Supported
Improved audio echo cancellation support	Not Supported	Not Supported
Composite USB device redirection	Not Supported	Not Supported
Support for DPI matching	Not Supported	Not Supported
Enhancement to improve audio quality	Not Supported	Not Supported
Provision to disable LaunchDarkly service	Not Supported	Not Supported
Email-based auto-discovery of store	Not Supported	Not Supported
Persistent login	Not Supported	Not Supported
Authentication enhancement for Storebrowse	Not Supported	Not Supported
Support for EDT IPv6	Not Supported	Not Supported

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2306 with CWA 2303	Limitations
Support for TLS protocol version 1.3	Not Supported	Not Supported
Custom web stores	Not Supported	Not Supported
Authentication enhancement experimental feature	Not Supported	Not Supported
Keyboard layout synchronization enhancement	Not Supported	Not Supported
Multi-window chat and meetings for Microsoft Teams	Supported	There are no limitations in this release.
Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
Request control in Microsoft Teams	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 work when you give control to other participant. This is a Microsoft limitation.
Support for cursor color inverting	Supported	Invert cursor does not work in Citrix VDA 2212, VDA 2203 CU2, VDA2303 Windows 10 and Windows 2019 desktop. This issue also occurs in Citrix Workspace app Linux binary.
Microsoft Teams enhancement to echo cancellation	Supported	For limitations, see the <i>Dell Wyse ThinOS Administrator's Guide</i> at <a href="http://www.dell.com/support">www.dell.com/support</a>
Enhancement on smart card support	Supported	There are no limitations in this release.
Webcam redirection for 64-bit	Supported	There are no limitations in this release.
Support for custom web stores	Not Supported	Not Supported
Workspace with intelligence	Not Supported	Not Supported
Session reliability enhancement	Supported	There are no limitations in this release.
Enhancement to logging	Supported	There are no limitations in this release.
Adaptive audio	Supported	There are no limitations in this release.

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2306 with CWA 2303	Limitations
Storebrowse enhancement for service continuity	Not Supported	Not Supported
Global App Config Service	Not Supported	Not Supported
EDT MTU discovery	Not Supported	Not Supported
Creating custom user-agent strings in network request	Not Supported	Not Supported
Feature flag management	Not Supported	Not Supported
Battery status indicator	Supported	There are no limitations in this release.
Service continuity	Not Supported	Not Supported
User Interface enhancement	Not Supported	Not Supported
Pinning multi-monitor screen layout	Not Supported	Not Supported
Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported
Multiple audio	Supported	Multiple audio devices feature is not supported by Cisco JVDI. This is Cisco known limitation. To eliminate confusion or mistakes, multiple audio devices feature is dynamically disabled after JVDI package installed, and it is dynamically enabled after JVDI package is uninstalled. There is an 8 device limitation to be redirected to HDX session. That means the total number of playback and record devices on thin client must be $\leq 8$ , so that you are able to use multiple audio devices. If the total number of playback and record devices on thin client $> 8$ , multiple audio devices do not work, and some of the audio devices may be missing in HDX session or the audio devices are displayed as Citrix HDX audio. This is Citrix VDA limitation.
Citrix logging	Supported	There are no limitations in this release.
Cryptographic update	Not Supported	Not Supported
Transparent user interface (TUI)	Not Supported	Not Supported

**Table 125. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2306 with CWA 2303	Limitations	
	GStreamer 1.x supportexperimental feature	Supported	There are no limitations in this release.
	App indicator icon	Not Supported	Not Supported
	Latest webkit support	Supported	There are no limitations in this release.
	Bloomberg audio redirection	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support	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 126. 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
	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

**Table 126. ThinOS AVD Client Feature Matrix (continued)**

Category Supported	Features	ThinOS 2303
	USB (General)	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	Limited support
	Imprivata	Supported

## VMware Horizon feature matrix

**Table 127. VMware Horizon session and client package versions**

Horizon	Package version
Horizon Session SDK	VMware_Horizon_2303.8.9.0.21435420. 3 .pkg
Horizon Client SDK	VMware_Horizon_ClientSDK_2303.8.9.0.21435420 . 16 .pkg

**Table 128. VMware Horizon feature matrix**

Category	Feature	Horizon Session SDK	Horizon Client SDK
Broker Connectivity	SSL certificate verification	Supported	Supported
	Disclaimer dialog	Supported	Supported
	UAG compatibility	Supported	Partially Supported
	Shortcuts from server	Not Supported	Not Supported
	Pre-install shortcuts from server	Not Supported	Not Supported
	File type association	Not Supported	Not Supported
	Phonehome	Supported	Supported
Broker Authentication	Password authentication	Supported	Supported
	SAML authentication	Supported	Supported
	Single sign on	Supported	Supported
	RSA authentication	Supported	Partially Supported

**Table 128. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Integrated RSA SecurID token generator	Not Supported	Not Supported
	Radius - Cisco ACS	Supported	Partially Supported
	Radius - SMS Passcode	Supported	Partially Supported
	Radius - DUO	Supported	Partially Supported
	Radius - OKTA	Supported	Partially Supported
	Radius - Microsoft Network Policy	Supported	Partially Supported
	Radius - Cisco Identity Services Engine	Supported	Partially Supported
	Kiosk mode	Supported	Supported
	Remember credentials	Supported	Supported
	Log in as current user	Not Supported	Not Supported
	Nested log in as current user	Not Supported	Not Supported
	Log in as current user 1-way trust	Not Supported	Not Supported
	OS biometric authentication	Not Supported	Not Supported
	Windows Hello	Not Supported	Not Supported
	Unauthentication access	Supported	Supported
Smartcard	x.509 certificate authentication (Smart Card)	Supported	Partially Supported
	CAC support	Supported	Not Tested
	.Net support	Supported	Supported
	PIV support	Supported	Not Tested
	Java support	Supported	Supported
	Purebred derived credentials	Not Supported	Not Supported
	Device Cert auth with UAG	Supported	Not Supported
Desktop Operations	Reset	Only supported with VDI	Only supported with VDI
	Restart	Only supported with VDI	Only supported with VDI
	Log off	Supported	Supported
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported	Supported
	Multiple connections	Supported	Supported
	Multi-broker/multi-site redirection - Universal	Not Supported	Not Supported
	App launch on multiple end points	Supported	Supported
	Auto-retry 5+ minutes	Supported	Supported
	Blast network recovery	Supported	Supported
	Time zone synchronization	Supported	Supported

**Table 128. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Jumplist integration (Windows 7-Windows 10)	Not Supported	Not Supported
Client Customization	Command line options	Not Supported	Not Supported
	URI schema	Not Supported	Not Supported
	Launching multiple client instances using URI	Not Supported	Not Supported
	Preference file	Not Supported	Not Supported
	Parameter pass-through to RDSH apps	Not Supported	Not Supported
	Non interactive mode	Not Supported	Not Supported
	GPO-based customization	Not Supported	Not Supported
Protocols supported	Blast Extreme	Supported	Supported
	H.264 - HW decode	Supported	Supported
	H.265 - HW decode	Supported	Supported
	Blast Codec	Supported	Supported
	JPEG / PNG	Supported	Supported
	Switch encoder	Supported	Supported
	BENIT	Supported	Supported
	Blast Extreme Adaptive Transportation	Supported	Supported
	RDP 8.x, 10.x	Supported	Not Supported
	PCoIP	Supported	Supported
Features / Extensions Monitors / Displays	Dynamic display resizing	Supported	Supported
	VDI windowed mode	Supported	Supported
	Remote app seamless window	Supported	Supported
	Multiple monitor support	Supported	Supported
	External monitor support for mobile	Not Supported	Not Supported
	Display pivot for mobile	Not Supported	Not Supported
	Number of displays supported	4	4
	Maximum resolution	3840x2160	3840x2160
	High DPI scaling	Not Supported	Not Supported
	DPI sync	Not Supported	Not Supported
	Exclusive mode	Not Supported	Not Supported
Multiple monitor selection	Supported	Supported	
Input Device (Keyboard / Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported	Supported
	Relative mouse	Only supported with VDI	Only supported with VDI
	External Mouse Support	Supported	Supported
	Local buffer text input box	Not Supported	Not Supported



**Table 128. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Keyboard Mapping	Supported	Supported
	International Keyboard Support	Supported	Supported
	Input Method local/remote switching	Not Supported	Not Supported
	IME Sync	Supported	Supported
Clipboard Services	Clipboard Text	Supported	Supported
	Clipboard Graphics	Not Supported	Not Supported
	Clipboard memory size configuration	Supported	Supported
	Clipboard File/Folder	Not Supported	Not Supported
	Drag and Drop Text	Not Supported	Not Supported
	Drag and Drop Image	Not Supported	Not Supported
	Drag and Drop File/Folder	Not Supported	Not Supported
Connection Management	IPv6 only network support	Supported	Supported
	PCoIP IP roaming	Supported	Supported
Optimized Device Redirection	Serial (COM) Port Redirection	Supported	Supported
	Client Drive Redirection/File Transfer	Not Supported	Not Supported
	Scanner (TWAIN/WIA) Redirection	Supported	Supported
	x.509 Certificate (Smart Card/Derived Credentials)	Supported	Supported
	Storage Drive Redirection	Not Supported	Not Supported
	Gyro Sensor Redirection	Not Supported	Not Supported
Real-Time Audio-Video	Audio input (microphone)	Supported	Supported
	Video input (webcam)	Supported	Supported
	Multiple webcams and microphones	Not Supported	Not Supported
	Multiple speakers	Not Supported	Not Supported
USB Redirection	USB redirection	Supported	Supported
	Policy: ConnectUSBOnInsert	Supported	Supported
	Policy: ConnectUSBOnStartup	Supported	Supported
	Connect/Disconnect UI	Not Supported	Not Supported
	USB device filtering (client side)	Supported	Supported
	Isochronous Device Support	Only supported with VDI	Only supported with VDI
	Split device support	Supported	Supported
	Bloomberg Keyboard compatibility	Only supported with VDI	Only supported with VDI

**Table 128. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Smartphone sync	Only supported with VDI	Only supported with VDI
Unified Communications	Skype for business	Not Supported	Not Supported
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Teams	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Meeting	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not Supported	Not Supported
	Directshow Redirection	Not Supported	Not Supported
	URL content redirection	Not Supported	Not Supported
	MMR Multiple Audio Output	Not Supported	Not Supported
	UNC path redirection	Not Supported	Not Supported
	Browser content redirection	Not Supported	Not Supported
Graphics	vDGA	Only supported with VDI	Only supported with VDI
	vSGA	Only supported with VDI	Only supported with VDI
	NVIDIA GRID vGPU	Supported with VDI, RDS Hosted Desktops	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Only supported with VDI	Only supported with VDI
	AMD vGPU	Only supported with VDI	Only supported with VDI
Mobile Support	Client-side soft keyboard	Not Supported	Not Supported
	Client-side soft touchpad	Not Supported	Not Supported
	Full Screen Trackpad	Not Supported	Not Supported
	Gesture Support	Not Supported	Not Supported
	Multi-touch Redirection	Not Supported	Not Supported
	Presentation Mode	Not Supported	Not Supported
	Unity Touch	Not Supported	Not Supported
Printing	VMware Integrated Printing	Supported	Supported
	Location Based Printing	Supported	Supported
	Native Driver Support	Not Supported	Not Supported
Security	FIPS-140-2 Mode Support	Supported	Supported
	Imprivata Integration	Supported	Supported

**Table 128. VMware Horizon feature matrix (continued)**

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Opswat agent	Not Supported	Not Supported
	Opswat on-demand agent	Not Supported	Not Supported
	TLS 1.1/1.2	Supported	Supported
	Screen shot blocking	Not Supported	Not Supported
	Keylogger blocking	Not Supported	Not Supported
Session Collaboration	Session Collaboration	Supported	Supported
	Read-only Collaboration	Supported	Supported
Updates	Update notifications	Not Supported	Not Supported
	App Store update	Not Supported	Not Supported
Other	Smart Policies from DEM	Supported	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported	Supported
	Nested - basic connection	Supported	Supported
	DCT Per feature/component collection	Not Supported	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported	Supported
	Auth Method - RSA SecurID	Supported	Not Supported
	Auth Method - X.509 Certificate (Smart Card)	Supported	Not Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported	Not Supported
	Auth Method - RADIUS	Supported	Not Supported
	Auth Method - SAML - 3rd Party Identity Provider	Supported	Not Supported

For detailed information about the VMware Horizon features, see the Horizon documentation at [docs.vmware.com](https://docs.vmware.com).

## New and enhanced features

### Citrix Workspace app updates

Citrix Workspace App (CWA) package version is updated to 23.5.0.58.1.

**i NOTE:** If you use older ThinOS images such as ThinOS 2303 with CWA2305 or ThinOS 2306 with older CWA versions such as CWA2302, Microsoft Teams Virtual background images feature does not work . You must use the compatible ThinOS image and CWA package.

**Citrix HDX Realtime Media Engine (RTME)**—From Citrix Workspace app 2305, RTME version is updated to 2.9.600-2900.

**Support for dynamic e911 in Microsoft Teams optimized mode**—From ThinOS 2306 and Citrix Workspace App 2305, Citrix Workspace app supports dynamic emergency calling. The notification is provided based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client running on the VDA. By default, dynamic e911 is enabled. For more information, go to [www.citrix.com](http://www.citrix.com).

**Support for FIDO2 authentication in HDX session**—From ThinOS 2306 and Citrix Workspace App 2305, you can authenticate within an HDX session using password-less FIDO2 security keys. FIDO2 security keys enable enterprise employees to authenticate to apps or desktops that support FIDO2 without entering a username or password. FIDO2 only supports 64-bit application. Currently, YubiKey 5 NFC device is qualified with ThinOS 2306. Before using FIDO2 security keys, ensure the following:

- Ensure that your FIDO2 device is mapped in the HDX session to use the FIDO2 authentication with FIDO2 virtual channel.
- Citrix Workspace App version must be 2305 or later.
- Citrix Virtual Apps and Desktops version must be 2009 or later.
- VDA version must be 2009 or later.
- Windows 10 version must be 1809 or later for installing VDA.
- Windows Server must be 2019 or later for installing VDA.
- FIDO2 Redirection policy must be enabled.
- Web browser in VDA such as Firefox, Chrome, Edge (version >=105)

By default, FIDO2 authentication is disabled. To enable FIDO2 authentication, 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 **module.ini**.
4. From the **Operation** drop-down list, select **Add or Update**.
5. In the **Section** field, enter **ICA 3.0**.
6. In the **Key** field, enter **FIDO2**.
7. In the **Value** field, enter **On**.
8. Sign out or restart the device for the settings to take effect.

For more information, go to [www.citrix.com](http://www.citrix.com). **Citrix ADC (NetScaler) login with PingID Multi Factor Authentication**—From ThinOS 2306 and Citrix Workspace App 2305, you can log in to Citrix ADC (NetScaler) with PingID Multi Factor Authentication.

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 PingIdentity for authentication.

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

When you log in for the first time to PingID, a download link and QR code is displayed that helps install the authenticator application in your phone.


6. Launch the PingID application on your phone and **Slide up** in the application to complete the authentication.

**Wacom Intuos S pen mapping and redirection in HDX sessions**—From ThinOS 2306 and Citrix Workspace App 2305, Wacom Intuos S pen can map or redirect in HDX sessions. The device information of Wacom Intuos S pen is Class ID-VID: 056a, PID: 0374 by Dell Technologies qualified. Before configuring USB device redirection, install Wacom Tablet software in your VDI session. To configure USB redirection on ThinOS, do the following:

1. On the ThinOS client, open Admin Policy Tool or go to the Wyse Management Suite policy settings.
2. In the **Advanced** tab, expand **Peripheral Management Settings**, and click **USB Redirection Settings**.
3. Click **Add Row** next to **vUSB Force Redirect** and enter **0x056a0374** in **vUSB Force Redirect** field.
4. Click **Save & Publish**.
5. Sign out or restart the device for the settings to take effect.

To configure USB mapping on ThinOS, do the following:

1. On the ThinOS client, open Admin Policy Tool or go to the Wyse Management Suite policy settings.
2. In the **Advanced** tab, expand **Peripheral Management Settings**, and click **USB Redirection Settings**.
3. Click **Add Row** next to **vUSB Force Local** and enter **0x056a0374** in **vUSB Force Local** field. Click **Save & Publish**.
4. Sign out or restart the device for the settings to take effect.

 **NOTE:** If the Wacom Intuos S pen mapping and redirection is not working, plug out and plug in the device to the thin client.

**32-bit cursor**—From ThinOS 2306 and Citrix Workspace App 2305, you can disable the support for 32-bit cursor, which is enabled by default. To disable support for 32-bit cursor, 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 **Thinwire3.0**.
6. In the **Key** field, enter **Cursor32bitSupport**.
7. In the **Value** field, enter **False**.
8. Sign out or restart the device for the settings to take effect.

**Citrix browser content redirection**—From ThinOS 2306 and Citrix Workspace app 2305, Citrix browser content redirection CEF cache file is changed from the default **.ICAClient** to **/tmp/citrix**. CEF cache file in **/tmp/citrix** is cleared when you log out.

**EDT**—From ThinOS 2306 and Citrix Workspace app 2305, HDX Enlightened Data Transport can be disabled using Citrix Configuration Editor. Follow these steps to disable the feature:

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.
2. In the Citrix ICA File Settings, click **Add Row**.
3. In the **Key** field, enter **HDXOverUDP**.
4. In the **Value** field, enter **Off**.
5. Sign out or restart the device for the settings to take effect.

To enable HDX Enlightened Data Transport using Citrix Configuration Editor, 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 the Citrix ICA File Settings, click **Add Row**.
3. In the **Key** field, enter **HDXOverUDP**.
4. In the **Value** field, enter **Preferred**.
5. Sign out or restart the device for the settings to take effect.

**Citrix Server IP Address display**—From ThinOS 2306 and Citrix Workspace app 2305, the Citrix Server IP address is displayed when hovering over the connection icon in the ThinOS taskbar. The enhancement is only supported when you connect to Citrix StoreFront server to launch a session.

### Citrix Workspace App Limitations

- Latitude 3420 Celeron 2 cores thin client does not support JVDI and Microsoft Teams video call or meetings. If you enable camera on Latitude 3420 Celeron 2 cores thin client during UC calls or meetings, the client CPU utilization reaches 100%.
- If you connected to a session using NetScaler, the Citrix Server IP Address is not displayed when hovering over the connection icon.
- The following new features from Citrix Workspace App 2303 and 2305 are not supported in ThinOS:
  - IPv6 TCP with TLS.
  - Keyboard layout synchronization for GNOME 42.
  - Client IME for East Asian languages.
  - Authentication using FIDO2 when connecting to on-premises stores.
  - Copying and pasting files and folders between two virtual desktops.
  - ARM64 architecture
  - Addition of client-side jitter buffer mechanism.
  - More than 200 groups in Azure AD
  - Hardware acceleration for optimized Microsoft Teams
  - Sleep mode for optimized Microsoft Teams call.
  - Background blurring for webcam redirection.
  - Configure path for Browser Content Redirection overlay Browser temp data storage.
  - New PIV cards.
  - Microsoft Teams enhancements
    - Limiting video resolutions.
    - Configuring a preferred network interface.
- The following issues also occur in Linux Citrix Workspace app binary:
  - When playing Multimedia Redirection (MMR) videos in VDA2203 and VDA2212 desktop, the video stops responding.

- Repeat playback function does not work for some of Multimedia Redirection (MMR) videos.
- Multiple windows open after fast forwarding and rewinding a Multimedia Redirection (MMR) video in Windows Media Player when playing.
- If JVDI package is installed, the secondary ringer in Microsoft Teams does not work.
- Audio issues occur when using a redirected USB headset to play the server rendered online audio.
- If you configure nondefault camera resolution in ThinOS, graphics issues occurs in 32-bit applications with theora encoder configured.

## Microsoft RDP and AVD

**USB redirection in RDP protocol session**—The steps for USB redirection are as follows:

1. Select **USB device redirection** in **Global Connection Settings** window.
2. Choose what type of device that you want to redirect:

**Table 129. Device redirection**

Device type	Description
Exclude disk devices	Select the check box if you do not want disk devices to be redirected to the remote session.
Exclude printer devices	Select the check box if you do not want printer devices to be redirected to the remote session.
Exclude audio devices	Select the check box if you do not want audio devices to be redirected to the remote session.
Exclude video devices	Select the check box if you do not want video devices to be redirected to the remote session.

3. Launch the RDP protocol session.

**NOTE:** The USB disk devices are redirected by default from ThinOS 2306. If you want to map the USB disk devices, select **Exclude disk devices**, and select **Disks** in RDP **Session Properties** window in the **Options** tab.

### Known Issues

- Microsoft RDS redirected USB Headset audio does not work in session when playing local or online videos.
- The camera does not work in RDP sessions when the camera is redirected into the RDP session.
- The audio device, which is redirected in RDP sessions, is not released when disconnected from RDP sessions.

**Force USB Devices Redirection**—To force redirect a device into the RDP protocol session, go to **WMS/APT > Session Settings > RDP and AVD Session Settings** and enter the VID/PID of the device.

### SmartCard Login

- From ThinOS 2306, SmartCard Login is supported for Microsoft Remote Desktop Services broker only.
- The broker login and Single Sign-on to session are two different steps. The single sign-on to session is not supported in this release.
- You cannot enter an RDS remote session using SmartCard. When the remote session is launched, you have to enter the credentials and not the SmartCard PIN.
- You cannot log in to the Azure Virtual Desktop broker using SmartCard.
- You cannot log in directly to an RDP session using SmartCard.
- If you want to use the SmartCard to log in to an RDP protocol session, you should set the KDC and Kerberos Domain Center Hostname in **APT > Advanced > Privacy & Security > Kerberos**.
- In ThinOS 2306, your domain account name is same as in the UPN, and the domain name is the same as the UPN suffix. This is the only supported setup for ThinOS 2306.
- **Known Issue:** SmartCard login fails when RDS Web Login is enabled in **WMS/APT > Advanced > Broker Settings > Microsoft Remote Desktop Settings**.

**NOTE:** If you want to use SmartCard to log in to RDP protocol sessions, set KDC and Kerberos Domain Center Hostname in **APT/ WMS > Advanced > Privacy & Security > Kerberos**.

**Changed the Use RD Gateway setting checkbox**—RD Gateway changed from checkbox to dropdown list. The dropdown list for RDP direct connection has **Don't use an RD Gateway** and **Always use an RD Gateway** options. The default value is **Always use an RD Gateway**. The dropdown list for Remote Desktop Service has **Don't use an RD Gateway**, **Always use an RD Gateway**, and **Use an RD Gateway if a direct connection failed**. The default value is **Use an RD Gateway if a direct connection failed**.

**Windows 365 cloud PC** —From ThinOS 2306, Windows 365 cloud PCs are supported. To log in to the cloud PC, do the following:

1. Open **Remote Connection**, select **Azure Virtual Desktop** in **Select Broker Type** list.
2. Check the **Enable Azure Virtual Desktop** checkbox.
3. Check the **Azure Common (ARMv2)** checkbox.
4. Click **OK**.
5. In the ThinOS web login interface, enter your Windows 365 cloud PC credentials.
6. Click **LOGIN**.

The cloud PC icon is displayed in ThinOS.

**i** **NOTE:** If there is only one Cloud PC session for this account, the Cloud PC session autoconnects when logging in successfully.

**Table 130. Windows 365 Cloud PC feature list**

Category	Features	ThinOS 2306
Session	Desktop	Supported
Input	Keyboard	Supported
	Mouse	Supported
	Single touch	Supported
Audio Visual	Audio in	Supported
	Audio out	Supported
	Camera	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
Redirections	Printer	Supported
	SmartCard	Supported
	USB devices	Supported
Session Experience	Dynamic Resolution	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 Support	Supported
Authentication	TS Gateway	Supported

## Teradici PCoIP

- Teradici version is updated to 23.04.1.9 in ThinOS 2306.
- Remote Workstation Card PCoIP sessions can be connected when using Teradici PCoIP package 23.04.1.9.
- **Limitation:** Teradici version 23.04.1.9 is not supported on ThinOS 2303(9.4.1141) or earlier version.

# VMware Horizon Updates

The Horizon package version is updated to Horizon 2303 in ThinOS 2306.

## Horizon Client SDK

**Table 131. Horizon Client SDK version and package**

SDK version	Package details
Horizon Client SDK version	2303.8.9.0.21435420
ThinOS Horizon Client SDK package version	VMware_Horizon_ClientSDK_2303.8.9.0.21435420.16.pkg

- As part of ThinOS 2306, a new, experimental Horizon Client package is released based on the Horizon Client SDK.
- Both the experimental Client SDK-based version and the Session SDK-based version is part of ThinOS 2306.
- In future releases, Session SDK-based client is not going to be released and Experimental tag is going to be removed from Client SDK-based Horizon Client.

### Other supported features

- Imprivata virtual channel in Horizon PCoIP sessions.
- MultiMedia Redirection (MMR) in Horizon PCoIP sessions.
- UC Optimization in Horizon PCoIP sessions.

### Known Issues and Limitations

- Negative user scenarios of RSA or MFA Radius authentications are not supported.
- UAG with Radius, RSA, X.509 Certificate is not supported.
- Tunnel bypass (CSSP) is not completely supported.
- The username hint feature of Smart card authentication is not completely supported.
- Horizon Cloud v2 (Next Generation) is not supported.
- Windows Group Policy in VDI session is not required for USB redirection in Horizon PCoIP session.
- Horizon PCoIP USB redirection configuration in Wyse Management Suite or Admin Policy Tool is not supported.

## Horizon Cloud Service Next Gen

- Horizon Cloud Service Next Gen helps you monitor the desktops and applications of all your cloud-connected Horizon deployments.
- In ThinOS 2306, only Horizon **VMware\_Horizon\_2303.8.9.0.21435420.3.pkg** package supports Horizon Cloud Service Next Gen.
- Follow these steps to configure Horizon Cloud Service Next Gen in ThinOS:
  1. Go to **Remote Connections > Broker Setup > VMware Horizon > Broker Server** text field and configure Horizon Cloud Service Next Gen URL.
  2. Connect to the Horizon broker from ThinOS login window.
  3. In the Horizon Cloud Service Next Gen web page, enter your company domain in the **Use Company Domain** field.
  4. Click **Continue**.
  5. Enter your username and password.

After the authentication is completed, desktop resources are displayed in ThinOS.


- Important notes:
  - **Sign in privately if you are using a shared device** option is not supported.
  - The link **To see the full list of VMware Horizon Clients, click here** does not work.
  - The link **For help with VMware Horizon, click here** does not work.
  - Logging in to Horizon Cloud Service Next Gen the first few times may take longer than usual.

## Horizon TureSSO

- Horizon TureSSO is supported with this release.
- After logging in to VMware Workspace One using RSA SecurID or RADIUS authentication, or a third-party identity provider using a Unified Access Gateway, you do not have to enter the Active Directory credentials to use a virtual desktop or published desktop or application.
- Before using TureSSO, follow Setting Up TureSSO at [docs.vmware.com](https://docs.vmware.com) to setup the SSO in your Horizon environment.
- Ensure that these key roles and components are configured:
  - Horizon Connection Server



- Enrollment Server
- VMware Workspace One
- Unified Access Gateway
- Third-party identity provider
- From ThinOS client side, no additional configuration is required. However, you must configure the Horizon broker URL in **ThinOS > Remote Connections > Broker Setup > VMware Horizon > Broker Server** field.

 **NOTE:** Windows Group Policy in VDI session is not required for USB redirection in Horizon PCoIP sessions.

## Imprivata updates

The latest supported application version on ThinOS is Imprivata\_PIE\_7.11.001.0045.48.pkg. It is recommended to use OneSign server 7.11 when using the ThinOS PIE feature. Do not use OneSign server 7.12 as there may be compatibility issues between PIE and OneSign.

### AVD broker support in ThinOS PIW mode

- Microsoft Azure Virtual Desktop is supported in ThinOS PIW.
- To configure Microsoft AVD in ThinOS, do the following:
  1. Go to **Admin Policy Tool/WMS > Login Experience > 3rd party Authentication** page.
  2. Configure OneSign server but do not enable **ProveID Embedded Mode**.
  3. Select **Local Setting** from **Automate access to**.
  4. Go to **Admin Policy Tool/WMS > Broker Settings > Global Broker Settings** page.
  5. Select **Azure Virtual Desktop** from **Default broker type**.
  6. Go to **Admin Policy Tool/WMS > Broker Settings > Azure Virtual Desktop Settings** page.
  7. Enable **Azure Virtual Desktop**.
  8. Reboot the client.
  9. Login to PIW with the available account.

The AVD web authentication window is displayed.

10. Enter the username and password to log in to AVD.

### Email support in PIW/AVD login

- OneSign server 7.12 is required for the feature.
- The account must have an email that is configured from Active Directory, and then the email can log in to Azure Virtual Desktop. The password must be same as the account password. OneSign server must also have this account already.
- To use this feature, do the following:
  1. Follow the steps of AVD support in PIW to configure ThinOS.
  2. Log in to ThinOS PIW with the account and password.

The AVD web authentication window is displayed and logs in automatically with the email of the account.

## Cisco WebEx Meetings VDI update

There is no new update with ThinOS 2306. See Cisco Webex Meetings VDI 43.2 for ThinOS 2303 on [www.dell.com/support](http://www.dell.com/support) for more information.

## Cisco Webex VDI update

Cisco WebEx VDI package version is updated to 43.4.0.25788\_2.

### Fixed Issues

- When you enable the virtual background in Webex VDI application, the application stops responding.
- When sharing your screen, the microphone does not work for some time when connected to WiFi.

## Zoom

Zoom package versions are updated to the following versions:

- Zoom Citrix package version is updated to 5.14.0.23370.1.
- Zoom Horizon package version is updated to 5.14.0.23370.1.
- Zoom AVD package version is updated to 5.14.0.23370.2.

**Zoom Mesh** feature for Webinars and Events is added with this release.

## RingCentral

RingCentral package version is updated to RcApp\_VMwareplugin\_23.2.20\_1.

## Avaya agent

Avaya agent for ThinOS is supported from ThinOS 2306. You can download *Avaya Agent for Desktop 2.0.6.25.3006* from *Software Downloads* in [www.support.avaya.com/support](http://www.support.avaya.com/support).

## ControlUp

ControlUp package version is updated to 1.0.0.1.34 and supports analyzing the client and VDI resources.

## Liquidware

ThinOS 2306 supports Liquidware Stratusphere UX Connector ID Agent. You can enable Liquidware Stratusphere UX Connector ID Agent and set the URL in the Wyse Management Suite policy **Device Monitoring** page.

## ThinOS enhancements

**New hardware configurations for Latitude 3440**—The following hardware configurations are supported in ThinOS 2306:

**Table 132. Hardware configurations that are supported for Latitude 3440**

Hardware Type	Hardware
CPU	Intel Celeron 7305
	12th Gen Intel Core i3-1215U
	13th Gen Intel Core i3-1315U
	13th Gen Intel Core i5-1335U
	13th Gen Intel Core i5-1345U
Memory	8 GB, 1 x 8 GB, DDR4, 3200 MHz
	16 GB, 2 x 8 GB, DDR4, 3200 MHz
	16 GB, 1 x 16 GB, DDR4, 3200 MHz
	32 GB, 2 x 16 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
Wireless	Intel AX211

**Table 132. Hardware configurations that are supported for Latitude 3440 (continued)**

Hardware Type	Hardware
Display	HD
	FHD
	FHD + touch

**New hardware configurations for Latitude 5440**—The following hardware configurations are supported in ThinOS 2306:

**Table 133. Hardware configurations that are supported for Latitude 5440**

Hardware Type	Hardware
CPU	13th Gen Intel Core i3-1315U
	12th Gen Intel Core i5-1235U
	12th Gen Intel Core i5-1245U
	13th Gen Intel Core i5-1335U
	13th Gen Intel Core i5-1345U
	13th Gen Intel Core i5-1340P
	13th Gen Intel Core i5-1350P
Memory	8 GB, 1 x 8 GB, DDR4/DDR5
	16 GB, 2 x 8 GB, DDR4/DDR5
	16 GB, 1 x 16 GB, DDR4/DDR5
	32 GB, 2 x 16 GB, DDR4/DDR5
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	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

**New hardware configurations for OptiPlex AIO 7410**—The following hardware configurations are supported in ThinOS 2306:

**Table 134. Hardware configurations that are supported for OptiPlex AIO 7410**

Hardware Type	Hardware
CPU	Intel Celeron G6900T
	Intel Pentium Gold G7400T
	Intel Pentium Gold G7400
	13th Gen Intel Core i3-13100
	13th Gen Intel Core i3-13100T

**Table 134. Hardware configurations that are supported for OptiPlex AIO 7410 (continued)**

Hardware Type	Hardware
	13th Gen Intel Core i5-13400
	13th Gen Intel Core i5-13400T
	13th Gen Intel Core i5-13500
	13th Gen Intel Core i5-13500T
	13th Gen Intel Core i5-13600
	13th Gen Intel Core i5-13600T
Memory	8 GB, 1 x 8 GB, DDR4/DDR5
	16 GB, 2 x 8 GB, DDR4/DDR5
	16 GB, 1 x 16 GB, DDR4/DDR5
	32 GB, 1 x 32 GB, DDR4/DDR5
	32 GB, 2 x 16 GB, DDR4/DDR5
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	FHD camera
Wireless	Intel AX201
	Intel AX211
Display	FHD
	FHD + touch

**Improvements to Operating system, BIOS, Application update process**

- **Added package download status icon**—The operating system, BIOS, and applications are downloaded in the background and installed in servicing mode. Click the package download status icon to check the download status.
  - **NOTE:** The icon is displayed only when there is an operating system, BIOS, or applications downloading from the Wyse Management Suite server. The icon is not displayed when entering servicing mode or changing group.
- **Added battery icon in servicing mode for mobile devices.**

**Dynamic CPU speed**—In **System information** window, the CPU Speed is changed dynamically.

**Wyse Management Suite Security Compliance alerts**—In some scenarios, the client displays the following security compliance alerts:

**Table 135. Security compliance alerts**

Security alert message	Meaning	Resolution
Device is using deprecated ciphers.	ThinOS client is connecting to the network with deprecated TLS ciphers.	Update the network environment to use secure TLS ciphers.
Default BIOS password has not been changed.	The BIOS password field of the ThinOS client is empty or has the default password Fireport.	Go to <b>BIOS &gt; Platform &gt; Enable Admin Password &gt; New BIOS Admin Password</b> and change the BIOS password in the ThinOS 9.x policy.
Admin Mode is not enabled, or Privilege Level is high.	Admin mode is not enabled, or privilege level is set to <b>High</b> on ThinOS client.	Enable <b>Admin Mode</b> and set <b>Privilege Level to None</b> or <b>Customize</b> in ThinOS 9.x policy under <b>Privacy &amp; Security &gt; Account Privileges</b>

**Factory reset and Soft reset**—In the **Shutdown** window, under **Rest the system setting**, there are two new options:

- **Factory reset** clears all configurations and the OOBE First Boot window is displayed.
- **Soft reset** clears all configurations, except network, certificate, and Wyse Management Suite. The OOBE First Boot window is not displayed. **Soft Reset** is also added in Wyse Management Suite server command list.

 **NOTE:** Soft reset clears the Ethernet speed and DHCP options.

**Get the device log from the Wyse Management Suite server**—You can upload the network trace and coredump file from the client to the Wyse Management Suite server. You can upload ThinOS logs file to the remote repository, which is registered to the Wyse Management Suite server.

**Updates to resolution of the display setup window**—When connecting a monitor through Display Data Channel (DDC) with 800 x 600 and 640 x 480 resolution to the client, then 800 x 600 and 640 x 480 is listed on the resolution list of the display setup window.

**Sync with file server immediately when checking in the client to the Wyse Management Suite server**—When using **File Server** for the screen saver type **Showing Pictures**, the client syncs with the file server immediately when checking in the client to the Wyse Management Suite server.

**Power on logo**—When powering on or rebooting the ThinOS client, a ThinOS Dell logo is displayed after BIOS Dell logo.

**Manage Known Networks**—Added a new option **Manage Known Networks** in the WiFi icon display window. Clicking this option displays all manually added wireless SSIDs. If you select one SSID, you can click **Forget** to remove it or **Properties** to modify it.

 **NOTE:** The wireless SSIDs published from Wyse Management Suite and Admin Policy Tool are not shown in the **Manage Known Networks** list.

**LPD printing on local Printer Setup window or Wyse Management Suite/Admin Policy Tool** —For LPD network printing, in the local **Printer Setup** window in LPDs settings, **LPD Queue Name** must be entered as **auto** or **generic**. In Wyse Management Suite or Admin Policy Tool, in LPD Printer Settings, **Queue** must be entered as **auto** or **generic**. For LPD server printing, you must enable LPD service on the client and use LPD printing in another client. In the local **Printer Setup** window in LPDs settings, **LPD Queue Name** value must be any value except **auto** and **generic**. In Wyse Management Suite or Admin Policy Tool, in LPD Printer Settings, **Queue** value must be any value except **auto** and **generic**.

**Basic or Expert mode**—In the event log interface, you can switch between Basic or Expert mode:

**Table 136. Log level and type**

Log Level	Importance	Displayed in event log (User mode)	Displayed in event log (Expert mode)	Log Type
Audit	All security relevant events must be logged such as user authentication, authorization, access change in configuration, and so on.	Yes	Yes	INFO
Fatal	One or more key business functionalities are not working and the whole system does not fulfill the business functionalities.	Yes	Yes	ERROR
Notice	An event happened; the event is purely informative for the end user.	Yes	Yes	INFO
Error	One or more functionalities are not working, preventing some functionalities from working correctly.	Yes	Yes	ERROR
Warn	Unexpected behavior happened inside the application, but it is	Yes	Yes	WARN

**Table 136. Log level and type (continued)**

Log Level	Importance	Displayed in event log (User mode)	Displayed in event log (Expert mode)	Log Type
	continuing its work and the key business features are operating as expected.			
Troubleshooting	Trouble shooting messages that are not shown in the event log and log file even if the default log level is defined in	No	Yes	DEBUG
Debug	A log level for events is considered to be useful during software debugging when more granular information is needed.	No	No	DEBUG
Verbose	A log level describing events and showing step-by-step execution of your code that can be ignored during the standard operation but may be useful during extended debugging sessions.	No	No	DEBUG

**Characters that are not supported in printer setting** —In **Settings > Printer Setup**, the following fields do not support some characters:

**Table 137. Special characters**

Special Characters	Field location
` " ' % _	<b>Printer Name</b> field in Ports settings
` " ' % _ ? /	<b>Printer Name</b> field in LPDs Settings
` " ' % _	<b>Printer Name</b> field in SMBs settings

**Show Alerts for ThinOS Device Certificate Expiry**—The Wyse Management Suite server can display alerts for ThinOS device certificates that are expiring in 1 - 120 days. The information can be found on the Wyse Management Suite server dashboard.

**Supports manual override of monitor settings when switching groups**—If the client has enabled the manual override of the monitor settings in the current group, and the client has triggered the manual override by changing a monitor setting on the client menu Display setup window after switching to a new group with manual override enabled, then all existing monitor settings remain intact.

**Enable timeout option for Touchpad**— When **Enable timeout** is disabled in ThinOS 2303 and earlier versions, the touchpad can always move. When the option is disabled in ThinOS 2306 and later versions, the touchpad cannot move for sometime after a key is used on the keyboard, except function keys.

## Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **Reset the system settings**—Added **Reset the system settings** in **Privacy & Security > Account Privileges**. When enabled, you can factory reset or soft reset the system settings.

- **Enable 5070 HD Audio 2**—Added **Enable 5070 HD Audio 2** in **Peripheral Management > Audio**. When you disabled, HD Audio 2 is disabled on 5070 devices.
- **Manual Override option position changed in Monitor Settings**—In **Peripheral Management > Monitor**, the **Manual Override** option is moved to the top of **Monitor Settings**.
- **Default value for Reboot Day or Shutdown Day**—In **System Settings > Scheduled Reboot** or **Scheduled Shutdown**, the **Reboot Day** or **Shutdown Day** dropdown selects all days from Sunday to Saturday instead of having none of the days selected.
- **Characters that are not supported in printer setting** — In **Peripheral Management > Printers**, the following fields do not support the characters ` " ' % \ \_ :
  - Local Printer: Name
  - LPD Printer: Name and Queue
  - SMB Printer: Local Name
- **WebLogin Timeout**—Added **WebLogin Timeout** in **Broker Settings > Citrix Virtual Apps and Desktops Settings**. You can enter the number of minutes, ranging between 0 and 300, that specifies when to automatically close the WebLogin page and reconnect to the broker. **0** means ThinOS WebLogin Timeout is disabled.
- **Citrix Configuration Editor updates**
  - **Citrix Keyboard Layout Settings** in Citrix Configuration Editor is deprecated from ThinOS 2306 and Citrix Workspace App 2305.
  - Added **Citrix ICA File Settings** in Citrix Configuration Editor. Enabling and disabling EDT is supported from ThinOS 2306 and Citrix Workspace App 2305.
- **New Application Package categories**—Added **Avaya Agent for Desktop** and **Liquidware Stratusphere UX Connector ID Agent** application package categories.
- **Device Monitoring**—Added a new page **Device Monitoring** with **Liquidware Stratusphere UX Connector ID Agent** and **URL** options.
- **Delay Auto Login in seconds**— Added **Delay Auto Login in seconds** in **Advanced > Login Experience > Login Settings**. The default value is 0, which means that if the default user credentials are set, you can log in automatically after the thin client boots. If you enter a delay time value in seconds, the auto login starts after the delay.
- **Force USB Devices Redirection**—The option is added in **Advanced > Session Settings > RDP and AVD Session Settings**. Devices with specified vendor and product IDs can be redirected using the option. The format of the setting is **vid1:pid1[#vid2:pid2] . . .**. You must specify the ID numbers in hexadecimal. For example, **0561:554c**. The delimiter between multiple devices is the pound sign #.
- **Enable Direct RDP Gateway**—The option is added in **Advanced > Session Settings > RDP and AVD Session Settings** and is enabled by default. The option works when adding RDP direct connections in ThinOS locally. When the option is changed, the default settings for RDP direct connection gateway is set.
- **Enable Terminal Services Gateway**—The option is added in **Advanced > Session Settings > RDP and AVD Session Settings**. The default value is **Use an RD Gateway if a direct connection failed**. When the option is changed, the default settings for RDP direct connection gateway is set.
- **Remote Desktop Services Gateway port**—The option is added in **Advanced > Session Settings > RDP and AVD Session Settings**. The option is for setting the Remote Desktop Services Gateway port in ThinOS. If not set, the default value is 443.
- **Kerberos Key Distribution Center (KDC)**
  - The option is in **Advanced > Privacy & Security > Kerberos**.
  - **Kerberos Key Distribution Center**: Full DNS or IP address of the machine running Kerberos Key Distribution Center service for logon user's domain, usually the domain controller.
  - **Kerberos Domain Center Hostname**: The option is in **Advanced > Privacy & Security > Kerberos**. Enter the Kerberos PKInit KDC hostname, used to verify AS REP X509 ext.3 SAN.
  - **Kerberos Reverse DNS**: The option is in **Advanced > Privacy & Security > Kerberos**. Kerberos Reverse DNS resolves theserver hostname, and is disabled by default.
  - **Kerberos trusted CA**: The option is in **Advanced > Privacy & Security > Kerberos**. Enter the trusted CA subject name, which only needs to match partially. Matching anchors are used by Kerberos to verify AS-REP. At least three characters must be included. Tags like country (/C), organization (/O), organizational unit (/OU), distinguished name, qualifier (/DC), state or province name(/ST), common name(/CN) are not taken into account.
- **Bluetooth Audio profile**—The option is in **Advanced > Network Configuration > Bluetooth Setting**, the default value is **UC(HSP/HFP)**.
- **Clear Logs After Logs Exported**—The option is in **Advanced > Services > Troubleshooting Settings** and is disabled by default. If users export logs successfully using the option, the logs are automatically cleared.
- **Unlock Terminal Count**—Added **Unlock Terminal Count** in **Advanced > Login Experience > Login Settings**. The policy limits the number of tries for unlocking the terminal. If the number of retries exceeds the set number, you can retry again after 15 minutes or sign off or restart the thin client.

 **NOTE:** The policy only takes effect during normal log in and does not work when Smartcard is used.

- **Connection Timeout**—In **Advanced > Login Broker Settings > Citrix Virtual Apps and Desktop Settings**, the **Timeout** policy name is changed to **Connection Timeout**. The change is only to the name and has no effect on functionality.
- **Blast Configuration Editor**—Added new option `/etc/vmware/viewagent-custom.conf` in **VDI Configuration Editor > Horizon Blast Configuration Editor > Add Horizon Blast Key-Value Settings > File**. The option allows you to configure more settings for VMware Horizon blast.

## Tested environments matrix

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

**Table 138. Tested environment—General components**

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.0 550 and WMS 4.1 536
Configuration UI package for Wyse Management Suite	1.9.986
Citrix ADC (formerly NetScaler)	13.0
StoreFront	1912 LTSR and later versions

**Table 139. 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 140. 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 7.13.1	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 140. 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 2022 APPs	Ubuntu 20.04
VMware Horizon 2303	Not tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Not tested

**Table 141. 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 142. Test environment – VMware Horizon Cloud version 2**

Horizon Cloud v2	Company Domain	Windows 10	Identity Provider	
www.cloud.vmware horizon.com	Hcseuc	Tested	Azure	Tested
			WS1 Access	Not tested

**Table 143. Test environment—Microsoft RDP**

Microsoft RDP	Windows 10	Windows 2012 R2	Windows 2016	Windows 2019	Windows 2022	APPs
Remote Desktop Services 2019	Tested	Not tested	Not tested	Tested	Not tested	Tested
Remote Desktop Services 2022	Tested	Not tested	Not tested	Not tested	Tested	Tested

**Table 144. Test environment—AVD**

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

**Table 145. Test environment—Windows 365 cloud PC**

Windows 365	Windows 10	Windows 11	Linux
Enterprise	Not tested	Tested	Not tested

**Table 146. 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)	Windows 10	2.9.600	2.9.600	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2019				
	Windows server 2022				
Citrix Virtual Apps and Desktops 7 2212					

**Table 147. 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	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
VMware Horizon 2106	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
VMware Horizon 2111	Windows server 2019	Not tested	Not tested	Not tested	Not tested

**Table 148. 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 11			
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016			
Citrix Virtual Apps and Desktops 7 2212	Windows server 2019			
	Windows server 2022			

**Table 149. Tested environment—JVDI**

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

**Table 150. Tested environment—Zoom**

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	5.14.0.23370.1	5.14.0 (23370)
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016		
Citrix Virtual Apps and Desktops 7 2212	Windows server 2019		
	Windows server 2022		

**Table 151. Tested environment—Zoom**

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 2209	Windows 10	5.14.0.23370.1	5.14.0 (23370)
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		

**Table 152. Tested environment—Zoom**

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.14.0.23370.1	5.14.0 (23370)
	Windows server 2016		

**Table 152. Tested environment—Zoom (continued)**

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
	Windows server 2019		

**Table 153. Tested environment—Cisco Webex Teams**

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.4.0.25788.2	43.4.0.25959
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016		
	Windows server 2019		
Citrix Virtual Apps and Desktops 7 2212	Windows server 2022		

**Table 154. Tested environment—Cisco Webex Teams**

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 2209	Windows 10	43.4.0.25788.2	43.2.0.24639
VMware Horizon View 7.13.2	Windows server 2016		
	Windows server 2019		

**Table 155. Tested environment—Cisco Webex Meetings**

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	43.2.5.22.1	43.2
	Windows 11		
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2016		
	Windows server 2019		
Citrix Virtual Apps and Desktops 7 2212	Windows server 2022		

**Table 156. Tested environment—Cisco Webex Meetings**

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12	Windows 10	43.2.5.22.1	43.2
VMware Horizon 2209	Windows server 2016		
	Windows server 2019		

**Table 157. Tested environment—RingCentral**

VMware VDI	Operating system	RingCentral Package
Horizon 2111	Windows 10	23.2.20.1
Horizon View 7.13.2	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 158. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
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 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

**Table 158. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	Dell USB 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
	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

**Table 158. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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 158. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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 158. 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
	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
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 159. Supported ecosystem peripherals for Latitude 3420**

Product Category	Peripherals
Displays	Dell 24 Monitor E2420HS - E2420HS



**Table 159. Supported ecosystem peripherals for Latitude 3420 (continued)**

Product Category	Peripherals
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W  <b>NOTE:</b> 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 station	Dell Dock - WD19
Cables, Dongles, Adapters	Dell 7-in-1 USB-C Multiport Adapter - Slayer 3 MLK - DA310

## Supported ecosystem peripherals for Latitude 3440

**Table 160. Supported ecosystem peripherals for Latitude 3440**

Product Category	Peripherals
Displays	Dell 24 USB-C Hub Monitor - P2422HE
	Dell 27 Monitor - 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
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

## Supported ecosystem peripherals for Latitude 5440

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

**Table 161. Supported ecosystem peripherals for Latitude 5440**

Product Category	Peripherals
Monitors	Dell 27 USB-C HUB Monitor - P2723DE
	Dell Collaboration 24 Monitor - C2423H
Input Devices	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
Audio/Video	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Speakerphone - Mozart - SP3022
	Dell Pro Webcam - Falcon - WB5023
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 162. 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
	Stereo Headset WH1022 (Presto)
	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
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726

**Table 162. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	Dell Bluetooth Travel Mouse - MS700 - Black
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 19 Monitor E1920H - E1920H
	Dell 20 Monitor E2020H - E2020H
	Dell 22 Monitor - E2223HN - E2223HN
	Dell 22 Monitor - P2222H - P2222H
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 24 Monitor - P2422H - P2422H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 Monitor - P2722H - P2722H
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE	
Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q	
Dell UltraSharp 27 Monitor - U2722D - U2722D	
Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE	

**Table 162. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**


Product Category	Peripherals
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
Storage	Dell USB Slim DVD +/- 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 Pro Webcam - Falcon - WB5023
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

## Supported ecosystem peripherals for OptiPlex 5400 All-in-One

**Table 163. 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

## 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 164. Supported ecosystem peripherals for OptiPlex All-in-One 7410**

Product Category	Peripherals
Monitors	Dell 24 Monitor - P2423D
	Dell UltraSharp 24 Monitor - U2422H
Input Devices	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022

# Third-party supported peripherals

Table 165. 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 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)
	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

**Table 165. Third-party supported peripherals (continued)**

Product Category	Peripherals
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	Elo ET2201L IntelliTouch ZB (Worldwide) - E382790
	Elo ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473
	Elo PCAP E351600 - 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
	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

**Table 165. Third-party supported peripherals (continued)**

Product Category	Peripherals
	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 CT30 V2 Gemalto IDBridge CT30 V3 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 Imprivata HDW-IMP-80-MINI Imprivata HDW-IMP-82-MINI 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	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

**Table 165. Third-party supported peripherals (continued)**

Product Category	Peripherals
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 in VMware PCoIP sessions, add **0x05541001, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.
- If you are using Power Mic 4 in VMware PCoIP sessions, add **0x05540064, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.

## Supported smart cards

**Table 166. Supported smart cards**

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2	Supported	Supported	Supported
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c	Supported	Supported	Supported
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4	Supported	Supported	Not Available



**Table 166. Supported smart cards (continued)**

<b>Smart Card info from ThinOS event log</b>	<b>Smart Card Middleware in VDI</b>	<b>Provider (CSP)</b>	<b>Card type</b>	<b>Citrix</b>	<b>VMware (works for Blast and PCoIP, not RDP)</b>	<b>RDS (works for broker login, and not in sessions)</b>
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8	Supported	Supported	Not Available
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 7.0 (T=0)	Supported	Supported	Not Available
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported

**Table 166. Supported smart cards (continued)**

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	G&D STARCOS 3.0 T=0/1 0V300	Supported	Not Available	Supported
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2	Supported	Not Available	Supported
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Enhanced Cryptographic Provider v1.0	YubiKey 4.3.3	Supported	Not Available	Supported
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Enhanced Cryptographic Provider v1.0	YubiKey 4.3.3	Supported	Not Available	Supported
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_7.1.15	cv act sc/ interface CSP	G&D STARCOS 3.2	Supported	Not Available	Supported
N/A (Buypass BelDu)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	BelDu 6.0.4	Supported	Not Available	Supported
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	IDPrime SIS 4.0.2	Supported	Not Available	Supported
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)	Supported	Supported	Supported
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)	Supported	Supported	Supported

## Fixed Issues

Table 167. Fixed issues

Issue ID	Description
DTOS-18310	64-character WPA or WAP2-PSK Passphrase is not allowed in on Wyse 5070 systems with ThinOS 2303.
DTOS-17928	Static noise during VoIP calls through Nice softphone.
DTOS-17918	VPN Configuration no longer allows /<directory> in Local Admin Policy in ThinOS 2303.
DTOS-17715	Wyse 5470 touchpad stops working in ThinOS 9.3.x.
DTOS-17673	Invalid broker URL message in login screen with ThinOS 2303.
DTOS-17653	Samsung S40UA monitor automatically wakes up from Sleep mode on systems with ThinOS 2208-2303 versions.
DTOS-17580	8.6 Feature Parity - Zebra scanner ds367 does not scan values on OptiPlex 3000 with ThinOS 2208.
DTOS-17366	AVD login uses email address through TITO tap in the Imprivata login screen.
DTOS-17336	Session idle timeout is not working.
DTOS-17334	The middle mouse button (Mouse-3) does not work anymore on Dell MS116p in ThinOS 2303 on OptiPlex 3000 systems.
DTOS-17318	Imprivata Connection Timeout does not work after Subsequent logins in ThinOS 2303.
DTOS-17317	64-character WPA or WAP2-PSK Passphrase is not allowed in on Wyse 5070 systems with ThinOS 2303.
DTOS-17316	If the <b>Save the last domain user</b> option is enabled, it overwrites the username for MFA, even if username was changed.
DTOS-17287	Horizon failed to launch remote desktop applications in ThinOS 2303 with OptiPlex thin clients.
DTOS-17266	Dragon Power Mic USB redirection drops. HD audio and split reconnects slowly.
DTOS-17265	OptiPlex 3000 WiFi latency when using mobile cart in the patient room.
DTOS-17251	Citrix browser-based login expires in 10–15 minutes.
DTOS-17234	Advice needed on how to Schedule Shutdown or Reboot Settings and interactions for ThinOS in Wyse Management Suite.
DTOS-17229	After connection loss, the thin clients lose access to the badge reader until you restart.
DTOS-17201	The card reader does not detect the tap of the card using Imprivata.
DTOS-17199	Disabling or enabling live update does not work in ThinOS 2303 on OptiPlex 3000 systems.
DTOS-17000	VMware session unlock screen displays True SSO user issue in ThinOS 2211.
DTOS-16933	The mouse locks up when two monitors are connected to Belkin KVM.

**Table 167. Fixed issues (continued)**

Issue ID	Description
DTOS-16872	8.6 Feature parity - Touchscreen does not work on OptiPlex 3000 Thin Clients.
DTOS-16731	DNS name resolution does not work.
DTOS-16671	Touchscreen does not work in ThinOS 9 but works in ThinOS 8.
DTOS-16538	When Wyse 5470 is connected to Dell WD195S dock, ThinOS 2211 randomly drops the network connection.
DTOS-16489	The screen stops responding or disconnects from VMware when in use for a long time.
DTOS-16331	Smartcard certificate installation fails on Wyse 5070 systems with ThinOS 2211.
DTOS-16314	The screensaver or lock screen does not engage when the session does not open.
DTOS-16313	In OptiPlex 3000 systems with ThinOS 2303, Blast sends the wrong client keyboard layout 409 to a physical desktop.
DTOS-16276	Manual override of monitor settings does not work when switching groups.
DTOS-16084	Citrix Server IP Address is not shown when hovering over connection icon in ThinOS 2211.
DTOS-16071	Logs are filling up home partitions and not being deleted after clearing logs.
DTOS-16034	In Wyse 5070 systems with ThinOS 2211, the screen saver does not work when the timer is set to a higher value with file server.
DTOS-15907	<b>Gateway Transport failure</b> error with external RD gateway is displayed when bypass for local address is enabled.
DTOS-15684	Authentication failure when thin client is sitting idle.
DTOS-15667	USB Thermocouple measuring device does not redirect in the RDSH or RDP session.
DTOS-15500	The smartcard PIN Prompt is not displayed when the card is inserted in systems with ThinOS 2211.
DTOS-15162	1280x1024 is missing from Direct RDP settings in OptiPlex 3000 with ThinOS 2211.
DTOS-15034	Unable to reset the expired password RDS in ThinOS 2208.
DTOS-14362	Japanese keyboard layout is not properly reflected with Blast and PCoIP in the Horizon virtual machine.
DTOS-14264	8.6 Feature Parity - Zebra scanner ds367 does not scan values on OptiPlex 3000 with ThinOS 2208.
DTOS-13898	HP Pinter redirection issue in Citrix session in systems with ThinOS 9.3.2102.
DTOS-11944	VBrick BCR issue in some video formats.
DTOS-16868	In 3040 systems with ThinOS 9.x, 800 x 600 Resolution does not work properly.

## Security fixes

ThinOS 2306 (9.4.2103) addresses multiple vulnerabilities. For information about the vulnerabilities addressed in this release, see [DSA-2023-247: Dell ThinOS Security Update for Multiple Vulnerabilities](#) at [Security Advisories, Notices and Resources](#).

## Known Issues

**Table 168. Known Issues**

Key	Summary	Workaround
DTOS-18117	After signing off from the PCoIP session, redirected USB devices do not come back to local thin client.	Reboot the thin client.
DTOS-17972	Unable to copy paste from one session to another session in Leostream broker.	There is no workaround in this release.
DTOS-17914	When you stop sharing the screen, the video gets mixed in the meeting call of Microsoft Teams - AVD	There is no workaround in this release.
DTOS-17908	When sharing the screen with dual monitors connected, the screen displays as one screen for other users.	There is no workaround in this release.
DTOS-17714	Session or application cannot be launched. <b>Generic license error</b> message is displayed in the specified RDSH environment.	Specific environment issue.
DTOS-17362	Serial printer does not work properly and cannot print completely. After clicking the test print button once, you must click the button many times to finish the printing.	There is no workaround in this release.
DTOS-16178	When an Olympus Device is redirected into a PCoIP session, sound dictation does not work with Windows Speech Recognition.	There is no workaround in this release.
DTOS-16053	Audio issues when changing the resolution.	There is no workaround in this release.
DTOS-15860	PCoIP USB headset redirection has no audio.	There is no workaround in this release.
DTOS-15778	There is no audio when video is played locally in Horizon PCoIP sessions with Nuance Powermic device.	There is no workaround in this release.
DTOS-15720	Display audio does not work with MST enabled on the monitor.	Turn off MST on monitor.
DTOS-15633	When the PCoIP VDI session is disconnected, the event log displays <b>exited with errno =&gt; SIGABRT</b>	There is no workaround in this release.
DTOS-15036	A black screen is displayed on Horizon Blast VDI session with window mode, when changing the display setting from mirror to span mode.	Do not change display mode.
DTOS-14972	USB Disk displays the wrong storage details in RDP sessions.	There is no workaround in this release.
DTOS-14695	VMware VDI displays a black screen when changing from mirror mode to span mode with two monitors connected.	Do not change display mode.
DTOS-14447	Display flickers when changing display mode from mirror to span mode and span to mirror mode.	There is no workaround in this release.

**Table 168. Known Issues (continued)**

<b>Key</b>	<b>Summary</b>	<b>Workaround</b>
DTOS-14020	After dynamic adjustment rotation, the blast session only shows on main display and not on the dual monitors.	Do not rotate monitor.
DTOS-13858	Integrated camera of Dell P2424HEB (C2424HE) monitor does not work when connecting the Uplink cable to USB 3.2 port.	There is no workaround in this release.
DTOS-11052	When you plug out the analog headset, the integrated microphone on Latitude 3420 does not work for several seconds.	Keep recording when plugging out analog headset.
DTOS-18460	Touchpad does not work after resuming from sleep on Latitude 5440.	There is no workaround in this release.
DTOS-19035	VDI Configuration Editor default value is not correct when you add rows in Wyse Management Suite version 4.1 and ConfigUI version 1.9.986.	Manually select the items from dropdown lists when you add rows in VDI Configuration Editor.

# Cisco Webex Meetings VDI 43.2 and Cisco Webex VDI 43.2 for ThinOS 2303

## Release summary

Patch or add-on releases are created to support the existing platforms or software releases, correct defects, make enhancements, or add new features.

## Current version

Cisco\_Webex\_Meetings\_VDI\_ 43.2.5.22.1.pkg

Cisco\_Webex\_VDI\_ 43.2.0.25640.1.pkg (formerly called Cisco Webex Teams)

## Release date

April 2023

## 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
- OptiPlex 5400 All-in-One
- Latitude 3440
- Latitude 5440
- OptiPlex 7410 AIO

## Important notes

- Upgrade the ThinOS firmware to ThinOS 2303 (9.4.1141) before you install the application packages.
- Cisco Webex Meetings VDI and Cisco Webex VDI is qualified for Citrix VDI on ThinOS 2303 (9.4.1141) with Citrix Workspace app package 23.2.0.10.4.
- Cisco Webex Meetings VDI and Cisco Webex VDI is qualified for VMware Blast VDI on ThinOS 2303 (9.4.1141) with VMware Horizon package 2212.8.8.0.21079016.5.

# Installing the application package


## Download the application package

### Steps


1. Go to [www.dell.com/support](http://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

- 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 ThinOS 9.x 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— **Cisco\_Webex\_Meetings\_VDI\_43.2.5.22.1.pkg** and **Cisco\_Webex\_VDI\_43.2.0.25640.1.pkg** (formerly called **Cisco Webex Teams**) are qualified by Dell Technologies.
- Supported Firmware-ThinOS 2303 (9.4.1141).

### Previous versions

Cisco\_Webex\_Meetings\_VDI\_43.2.1.18.5.pkg

Cisco\_Webex\_VDI\_43.2.0.25211.4.pkg (formerly called Cisco Webex Teams)



# Cisco Webex Meetings VDI updates

Cisco Webex Meetings VDI package version is updated to 43.2.5.22.1.

## Cisco Webex Meetings VDI feature matrix

**Table 169. Cisco Webex Meetings VDI feature matrix**

Scenarios	ThinOS 2303 (9.4.1141)
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
Polls	Supported
Q & A- Participants ask Questions to Host	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 169. Cisco Webex Meetings VDI feature matrix (continued)**

Scenarios	ThinOS 2303 (9.4.1141)
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
Breakout sessions	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported
Make Host or Co-host other Participants	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

- 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.
- When a user is sharing the screen, the video of all users becomes black screen in the Webex meeting call.

## Cisco Webex VDI update

- Cisco Webex VDI package version is updated to 43.2.0.25640.1.
- Supports Virtual Background/ Blur image.

## Cisco Webex VDI feature matrix

**Table 170. Cisco Webex VDI feature matrix**

Scenarios	ThinOS 2303(9.4.1141)
Join meeting	Supported
Audio call	Supported

**Table 170. Cisco Webex VDI feature matrix (continued)**

<b>Scenarios</b>	<b>ThinOS 2303(9.4.1141)</b>
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
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	Supported

# Cisco Limitations

The Microphone will not work for few seconds if the user starts sharing screen.

## New and enhanced features

Cisco Webex Meetings VDI package version is updated to 43.2.5.22.1 Fixed the virtual background/ blur image issue.

## 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 171. Tested environment—General Components**

Component	Version
Dell Wyse Management Suite	WMS 4.0 547 WMS 4.1
Configuration UI package for Dell Wyse Management Suite	WMS 4.0 547: 1.9.728 WMS 4.1: Refer to upcoming WMS 4.1 release
NetScaler	12.1/13.0
StoreFront	1912 LTSR and later

**Table 172. Tested environment—Cisco Webex VDI**

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR CU6	Windows 10	43.2.0.25640.1	43.2.0.24639
	Windows server 2016	43.2.0.25640.1	43.2.0.24639
Citrix Virtual Apps and Desktops 7 2203 LTSR CU2	Windows server 2019	43.2.0.25640.1	43.2.0.24639
Citrix Virtual Apps and Desktops 7 2206			

**Table 173. Tested environment—Cisco Webex VDI**

Horizon VDI	Operating system	Webex VDI	Webex Teams software
Horizon 7.12	Windows 10	43.2.0.25640.1	43.2.0.24639
Horizon 2106	Windows server 2016	43.2.0.25640.1	43.2.0.24639
Horizon 2111	Windows server 2019	43.2.0.25640.1	43.2.0.24639

**Table 174. Citrix Tested environment—Cisco Webex Meetings VDI**

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR CU6	Windows 10	43.2.5.22.1	43.2
	Windows server 2016		
Citrix Virtual Apps and Desktops 7 2203 LTSR CU2	Windows server 2019		
Citrix Virtual Apps and Desktops 7 2206			

**Table 175. Citrix Tested environment—Cisco Webex Meetings VDI**

<b>Horizon VDI</b>	<b>Operating system</b>	<b>Webex Meetings VDI</b>	<b>Webex Meetings software</b>
Horizon 7.12	Windows 10	43.2.5.22.1	43.2
Horizon 2106	Windows server 2016		
Horizon 2111	Windows server 2019		

# 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)**

**i** **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.

**i** **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](http://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.
  - In ThinOS 2211 and previous versions, the thin client cannot download and install the operating system firmware and BIOS firmware until the next reboot.
  - From ThinOS 2303, the operating system firmware and BIOS firmware downloads in the background but cannot complete installation 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 176. 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](http://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](http://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 177. 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

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

**i** **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

**i** **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 178. 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 179. 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

**Table 179. Tested BIOS details (continued)**

Platform name	BIOS version
OptiPlex All-in-One 7410	1.0.1

## Citrix Workspace app feature matrix

**Table 180. 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

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
			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.
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

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2303 with CWA 2302	Limitations
		limitations, see <i>Dell Wyse ThinOS 2303, 2211, 2208, and 2205 Release Notes</i> at <a href="http://www.dell.com/support">www.dell.com/support</a>
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 <i>Dell Wyse ThinOS Administrator's Guide</i> at <a href="http://www.dell.com/support">www.dell.com/support</a> .
Skype for business Optimization pack	Supported	Not supported through proxy server.
Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the <i>Dell Wyse ThinOS Administrator's Guide</i> at <a href="http://www.dell.com/support">www.dell.com/support</a> .
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 <i>Dell Wyse ThinOS Administrator's Guide</i> at <a href="http://www.dell.com/support">www.dell.com/support</a> .
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

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
			configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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.

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
	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	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.

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
	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: <ul style="list-style-type: none"> <li>• Citrix Federated Authentication Service SAML with Microsoft Azure Active Directory</li> <li>• Citrix ADC Native OTP</li> <li>• Citrix ADC MFA with SAML using OKTA as IDP and Citrix FAS for SSO to VDA</li> </ul>
	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.



**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
	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.
	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	

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
	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)	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 <b>Give control</b> 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 <a href="http://www.dell.com/support">www.dell.com/support</a> .
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	For limitations, see the Dell Wyse ThinOS Version 2205 Administrator's Guide at <a href="http://www.dell.com/support">www.dell.com/support</a> .
	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 <i>Dell Wyse ThinOS 2303, 2211, 2208, and 2205 Release Notes</i> at <a href="http://www.dell.com/support">www.dell.com/support</a>
	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

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature	ThinOS 2303 with CWA 2302	Limitations
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)	Supported	For limitations, see <i>Dell Wyse ThinOS 2303, 2211, 2208, and 2205 Release Notes</i> at <a href="http://www.dell.com/support">www.dell.com/support</a>
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.

**Table 180. Citrix Workspace app feature matrix (continued)**

Feature		ThinOS 2303 with CWA 2302	Limitations
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
	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 181. 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

**Table 181. ThinOS AVD Client Feature Matrix (continued)**

Category Supported	Features	ThinOS 2303
	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	Supported
	SmartCard	Not supported
	Imprivata	Supported

## VMware Horizon feature matrix

**Table 182. 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

**Table 182. VMware Horizon feature matrix (continued)**

Feature	ThinOS 2303 with Horizon Client 2212	
	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
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI

**Table 182. VMware Horizon feature matrix (continued)**

Feature	ThinOS 2303 with Horizon Client 2212	
	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. 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

**Table 182. VMware Horizon feature matrix (continued)**

Feature	ThinOS 2303 with Horizon Client 2212	
	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. ThinOS does not support local input methods.
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 182. VMware Horizon feature matrix (continued)**

Feature		ThinOS 2303 with Horizon Client 2212
	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. 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

**Table 182. VMware Horizon feature matrix (continued)**

Feature	ThinOS 2303 with Horizon Client 2212	
	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. 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
	Opsswat agent	Not supported
	Opsswat 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

**Table 182. VMware Horizon feature matrix (continued)**

Feature		ThinOS 2303 with Horizon Client 2212
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
	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. <b>Login Use Smartcard Certificate Only</b> must be disabled in ThinOS.

For detailed information about the VMware Horizon features, see the Horizon documentation at [docs.vmware.com](https://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](https://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 the Adobe Acrobat reader in the Citrix HDX Pro 3D desktop. This issue is also reproduced in the Citrix Workspace App Linux binary.

### Supports multiple audio devices by default

- From ThinOS 2303 and Citrix Workspace App 2302, the 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, the `AudioRedirectionV4=True` parameter has already been configured during Citrix Workspace App 2302 package installation. You need not change the Citrix INI settings in the Citrix configuration editor in Wyse Management Suite or Admin Policy Tool.
- To disable this feature, do the following:
  1. In the 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.

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

**i** **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 the 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 a MultiWindow 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 the 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 the 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 the 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 the 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 the 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 **HDXWebCamDelayTime**.
  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.


- The 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.
- The mouse cursor is displayed as a black block in Adobe Acrobat Reader (32-bit) in the 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 the **Citrix Desktop Viewer** toolbar.
- Audio issues are noticed when using a redirected USB headset in a 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](http://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](http://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](http://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 183. 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.

**Table 183. Troubleshooting errors during Horizon login (continued)**

Error message	Reason	Solution
Connect broker timeout	Cannot reach Horizon server through Proxy.	Check your proxy connection.
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 <b>Continue</b> 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**.
  - In the **Broker Server** field, you can configure the Broker agent server address by adding the URL of the other Broker agent.
  - In the **Auto Connect List** field, you can configure the desktop and applications that must be automatically connected.
  - 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 184. Leostream Feature Matrix**

RDP/ThinOS	Category Supported	Features	ThinOS 2303
RDP feature	Input	Keyboard	Supported
		Mouse	Supported
		Single touch	Supported



**Table 184. Leostream Feature Matrix (continued)**

RDP/ThinOS	Category Supported	Features	ThinOS 2303
	Session	Desktop	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
	Graphics (CODECs)	Video/Audio/Online playback	Supported
		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 185. 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
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\_5.
- Added new features:
  - Watermark
  - Background noise cancellation
- **Limitations:**
  - A shadow of the virtual background is displayed in meetings.
  - When you share your screen during meetings, other participants take longer to see your screen on their systems.

## Cisco Webex VDI update

- Cisco Webex VDI package version is updated to 43.2.0.25211.4.
- Added new features to Webex Teams VDI:
  - Music mode
- **Limitations:**
  - When you enable the virtual background in Webex VDI application, the application stops responding.
  - When sharing your screen, the microphone does not work for some time on network speed.

## Cisco Jabber

- Cisco Jabber (jVDI) version is updated to 14.1.3.307560.10.
- **Limitations:**
  - When optimization is disabled, there is Citrix Jabber audio issues.
  - Bluetooth headset does not work in jVDI. As a workaround, change to **Streaming** profile, but the headset cannot be used for jVDI calls.

## Zoom

Zoom package version is updated to 5.13.0.22460.2.

## RingCentral

RingCentral package version is updated to 23.1.10.5.

## ControlUp

ControlUp package version is 1.0.0.1.33.

## ThinOS enhancements

**Supports Latitude 3440**—The following hardware configurations are supported:

**Table 186. Hardware configurations that are supported for Latitude 3440**

Hardware Type	Hardware
CPU	Intel Celeron 7305

**Table 186. Hardware configurations that are supported for Latitude 3440 (continued)**

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

The following hardware configurations are not supported for Latitude 3440:

**Table 187. 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 188. 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

**Table 188. Hardware configurations that are supported for Latitude 5440 (continued)**

Hardware Type	Hardware
	FHD 300 nit + touch
Smart Card reader slot	Smart Card reader only

The following hardware configurations are not supported for Latitude 5440:

**Table 189. 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
Storage	SED storage

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

**Table 190. 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 191. 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

**Table 191. Hardware configurations that are not supported for OptiPlex All-in-One 7410 (continued)**

Hardware Type	Hardware
Wireless	Realtek RTL8852BE
HDMI in	HDMI in 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.  
**i** **NOTE:** The operating system firmware and BIOS firmware downloads in the background, and the thin client can download them when **Live Update** is disabled. However, the installation cannot be completed until the next reboot.
- 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.

**i** **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.

If you are using the Streaming profile, you cannot record or use the microphone when in session or locally.

**i** **NOTE:** Close the Jabbar application to use Bluetooth headsets.

**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.

- The feature supports papersize management, lossless compression of scanned pages, and color management.
- Various printer drivers and 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 connect to OpenVPN, do the following:
  1. Go to **System Settings > VPN Manager**.
  2. Click **Open VPN**.
  3. Click **+** to add VPN details.
  4. Select the OVPN config file in **APT/WMS > Network Configuration > VPN Settings > VPN > Open VPN config** dropdown list.
  5. Click **OK**.
  6. In the Open VPN tab server list, select **VPN**.
  7. Click **Connect**.

**Fortinet VPN**—Fortinet is supported in ThinOS 2303 and is added in **Open Connect > Protocol**. You cannot edit the server field locally once the server fields are saved.

**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-Stream 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 192. 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-Stream 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.
- If you hot plug monitors when ThinOS is displaying screensaver, the monitors display a black screen.

**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 193. 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 194. Platforms 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 HDMI 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.
- ThinOS only supports one external network port. If there is a network port on the monitor and you connect the monitor to a docking station with type-C cable, the network port on monitor works and the network port on the dock does not work.
- Latitude 5440 does not support hot plugging the docking station. You must power on with the docking station connected.



**Allow server list**—If the Wyse Management Suite server is not in the allow server list and you check 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:

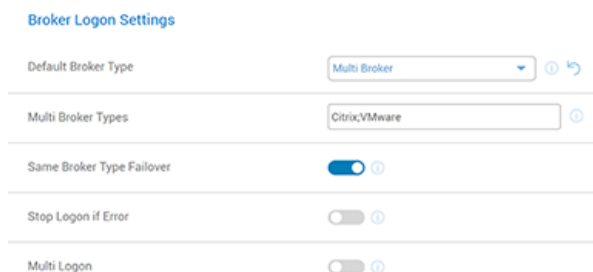
**Table 195. Cipher List and their security status**

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
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

**Table 195. Cipher List and their security status (continued)**

<b>Ciphers</b>	<b>Security Status</b>
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
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.



**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.

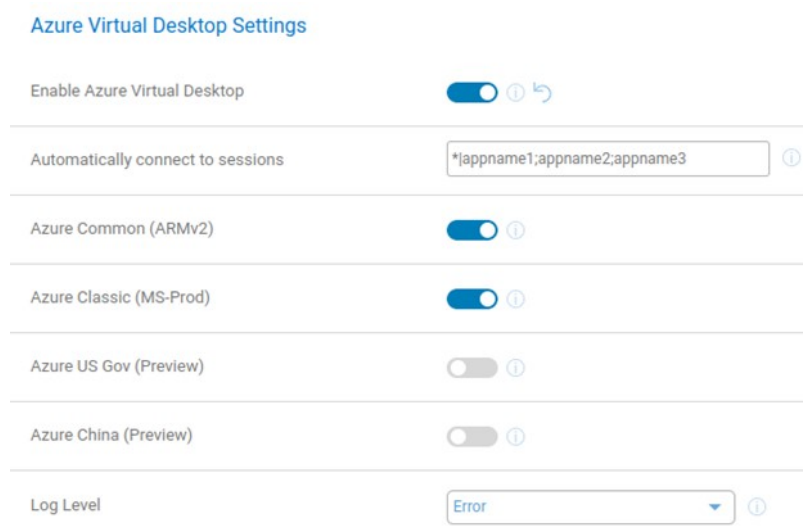
**NOTE:** When the **Multi Logon** policy is enabled, a different Broker agent logon page is displayed in the login window when waiting to enter credentials. When logging in using Multi Farm policy with Multi Logon disabled, only the general ThinOS login window is displayed.

 **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 core dump 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:



**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 196. 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 197. 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 198. 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 199. 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 200. 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 201. 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 202. 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	Windows 10	2.9.500	2.9.500	Skype for Business 2016	Skype for Business 2015

**Table 202. Tested environment—Skype for Business (continued)**

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

**Table 203. 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	Windows 10	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
VMware Horizon 2106	Windows server 2016	5.4, 8.2, 8.4	7.12, 8.2, 8.4	Skype for Business 2016	Skype for Business 2015
VMware Horizon 2111	Windows server 2019	Not tested	Not tested	Not tested	Not tested

**Table 204. 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			
Citrix Virtual Apps and Desktops 7 2203 LTSR (CU2)	Windows server 2019			
	Windows server 2022			
Citrix Virtual Apps and Desktops 7 2212				

**Table 205. Tested environment—JVDI**

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

**Table 206. Tested environment—Zoom**

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

**Table 207. Tested environment—Zoom**

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

**Table 208. 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 209. Tested environment—Cisco Webex Teams**

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

**Table 210. Tested environment—Cisco Webex Teams**

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

**Table 211. Tested environment—Cisco Webex Meetings**

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

**Table 212. Tested environment—Cisco Webex Meetings**

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

**Table 213. Tested environment—RingCentral**

VMware VDI	Operating system	RingCentral Package
Horizon 2111	Windows 10	23.1.10.5



**Table 213. Tested environment—RingCentral (continued)**

VMware VDI	Operating system	RingCentral Package
Horizon View 7.13.2	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 214. 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 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
Dell Laser Wired Mouse - MS3220 - Morty		Supported	Supported	Supported	Not Available

**Table 214. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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
	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)	Supported	Supported	Supported	Not Available

**Table 214. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	- DANAUBC087 - DANAUBC087				
	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
	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

**Table 214. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

<b>Product Category</b>	<b>Peripherals</b>	<b>3040</b>	<b>5070</b>	<b>5470 AIO</b>	<b>5470</b>
	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
	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

**Table 214. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**


Product Category	Peripherals	3040	5070	5470 AIO	5470
	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
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

**Table 214. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)**

Product Category	Peripherals	3040	5070	5470 AIO	5470
	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 215. 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  <b>NOTE:</b> Bluetooth connection is not supported.
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
	Dell Keyboard KB216
Audio Devices	Dell Pro Stereo Headset - UC150 - UC150 - Lemmy - UC150
	Dell Pro Stereo Headset UC350
Storage	Dell USB Slim DVD +/R 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 216. 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

**Table 216. Supported ecosystem peripherals for Latitude 3440 (continued)**

Product Category	Peripherals
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 +/- 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 217. 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
	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 218. 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

**Table 218. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	Dell Slim Conferencing Soundbar - Lizzo - SB522A
	Dell Speakerphone - Mozart - SP3022
	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
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 19 Monitor E1920H - E1920H
	Dell 20 Monitor E2020H - E2020H
	Dell 22 Monitor - E2223HN - E2223HN
	Dell 22 Monitor - P2222H - P2222H
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 24 Monitor - P2422H - P2422H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS



**Table 218. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)**

Product Category	Peripherals
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 Monitor - P2722H - P2722H
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE
	Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
Storage	Dell USB Slim DVD +/- 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 Pro Webcam - Falcon - WB5023
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

# Supported ecosystem peripherals for OptiPlex 5400 All-in-One

**Table 219. 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
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
Audio/Video	Dell Pro Stereo Headset - Cortez - WH3022
Storage	Dell USB Slim DVD +/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 220. 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 +/RW Drive - DW316 - DW316 - Agate - DW316

# Third-party supported peripherals

**Table 221. 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

**Table 221. Third-party supported peripherals (continued)**

Product Category	Peripherals
	Jabra UC SUPREME MS Bluetooth ( link 360 )
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Support USB only, not support Bluetooth)
	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)
	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	ET2201L IntelliTouch ZB (Worldwide) - E382790
	ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473

**Table 221. Third-party supported peripherals (continued)**

Product Category	Peripherals
	PCAP E351600 - 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
	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

**Table 221. Third-party supported peripherals (continued)**

<b>Product Category</b>	<b>Peripherals</b>
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
	Imprivata HDW-IMP-80-MINI
	Imprivata HDW-IMP-82-MINI
	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	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 in VMware PCoIP sessions, add **0x05541001, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.
- If you are using Power Mic 4 in VMware PCoIP sessions, add **0x05540064, NoDriver** in **vUSB Force Redirect**. To add the parameter, go to **APT > Advanced > Peripheral Management > USB Redirection > vUSB Force Redirect > Add Row**.

## Supported smart cards

**Table 222. Supported smart cards**

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 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
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K

**Table 222. Supported smart cards (continued)**

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
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 key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java(aladdin) (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110
Etoken Java(aladdin) (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS
Etoken Java(aladdin) (black USB key)	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	G&D 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	G&D STARCOS 3.2
N/A (Buypass BelDu)	Net iD 6.8.5.20, 2.0.50	Net iD - CSP	BelDu 6.0.4
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.5.20, 2.0.50	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 223. 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.

**Table 223. Fixed issues (continued)**

Issue ID	Description
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 <b>Custom</b> —CIPS-30334.
DTOS-15884	New connections can be added when privilege level is set to <b>None</b> —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	<b>DHCP OT 12</b> hostname is not taken as expected in ThinOS 9—CIPS-30004.
DTOS-15458	The <b>Change password</b> 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 <b>Download ARMv2 feeds failed</b> error message—CIPS-29697.
DTOS-15031	Taskbar covers the bottom of published apps in ThinOS 2208 with dual monitors that are connected in <b>Classic</b> 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.
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	<b>Cannot resolve host name</b> error message is displayed when devices are in <b>Select group</b> 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



**Table 223. Fixed issues (continued)**

Issue ID	Description
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 <b>Custom</b> , 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	<b>Error: The session id is expired, please retry to log in the broker</b> error message is displayed on 5070 devices with ThinOS 9.3—CIPS-29534.
DTOS-14439	When Fast Disconnect option is set to <b>SignOff</b> , 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.
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.

**Table 223. Fixed issues (continued)**

Issue ID	Description
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 224. 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 <b>Browse</b> button to upload a valid application package. For example, <b>Citrix_22.12.0.12_1_signed.pkg</b>	Open the admin policy tool again.
DTOS-15999	Both <b>Cancel</b> and <b>Open</b> button is not displayed in <b>Open Files</b> page when clicking <b>Browse</b> 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.
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	<b>Integrated Webcam FHD</b> is displayed two times in Webex Teams, jVDI, Zoom and Webex meetings in the <b>Devices</b> drop-down list.	No Workaround

**Table 224. Known issues (continued)**

<b>Issue ID</b>	<b>Description</b>	<b>Workaround</b>
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 <b>Portrait</b> 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 <b>Mirror</b> mode to <b>Span</b> 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 <b>Window</b> 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 <b>Streaming</b> and back to <b>UC</b> profile for the device to work.
DTOS-14434	Troubleshooting window is closed when user tries to enable or disable <b>Capture Debug logs</b> 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 <b>Fast Wakeup</b> 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.

## Resources and support

### Accessing documents using the product search

1. Go to [www.dell.com/support](http://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, **OptiPlex 3000 Thin Client**. 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](http://www.dell.com/support).
2. Click **Browse all products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **OptiPlex Thin Client**.
6. Click **OptiPlex 3000 Thin Client**.
7. Click **Select this Product**.
8. Click **Documentation**.

# 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](http://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.