Dell ThinOS 2402

Release Notes

April 2024
Rev. A04

Notes, cautions, and warnings

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

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

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

Contents

1

Overview

Dell 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.

2

Security package for ThinOS 2402

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.

Release Package Information

Security_Addon_2402.1.1.pkg

ThinOS BIOS version details

The following table contains the tested BIOS versions details for ThinOS 2402.

Table 1. ThinOS BIOS version details

Supported platform	Tested 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
Dell OptiPlex 3000 Thin Client	1.15.0
Dell Latitude 3420	1.33.0
Dell OptiPlex 5400 All-in-One	1.1.36
Dell Latitude 3440	1.9.1
Dell Latitude 5440	1.10.0
Dell Latitude 5450	1.0.2
Dell OptiPlex AIO 7410	1.11.0
Dell OptiPlex AIO 7420	1.0.0

Upload and publish the security add-on package

Prerequisites

- 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 `Security_Addon_2402.1.1.pkg` to upload.

   NOTE: Under the Dell category, ensure that the switch option of **Security Addon** is set to **INSTALL**.

7. Click to expand the **Security Addon** dropdown list and select the uploaded package.
8. Click **Save & Publish**.
   The thin client downloads the package, installs it, and then restarts. The Common Vulnerabilities and Exposures (CVE) fix is installed.

Important notes

- The `Security_Addon_2402.1.1.pkg` is only for ThinOS 2402 (9.5.1079). All future ThinOS releases include this fix, and installing the stand-alone package is not required.
- If you uninstall `Security_Addon_2402.1.1.pkg`, the fix is removed.
- If you upgrade from ThinOS 2402 (9.5.1079) and `Security_Addon_2402.1.1.pkg` to the next ThinOS release, the package is removed automatically.

What's new

Security vulnerability updates

- Upgraded libexpat from 2.5.0 to 2.6.0 (CVE-2023-52425).
- Updated libxml2 2.10.4 (CVE-2024-25062).

General tested environments matrices

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

Table 2. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.3
Configuration UI package for Wyse Management Suite	1.10.275
Citrix ADC (formerly NetScaler)	13.0
StoreFront	1912 LTSR and later

Table 3. 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

Table 3. Test environment—Citrix (continued)

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 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 4. 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
VMware Horizon 2309	Tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Tested

Table 5. 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 6. Test environment – VMware Horizon Cloud version 2

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

Table 7. 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 8. 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 9. Test environment—Windows 365 cloud PC

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

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

Table 11. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10 Windows 11 Windows server 2016 Windows server 2019 Windows server 2022 (Not tested)	14.3.0.308378.8	14.3.0.308378	14.3.0.308378

Table 12. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10 Windows server 2016 Windows server 2019	14.3.0.308378.8	14.3.0.308378	14.3.0.308378

Table 13. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10	5.16.10.24420.6	5.16.10 (24420)
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 14. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	5.16.10.24420.6	5.16.10 (24420)
	Windows server 2016		
	Windows server 2019		

Table 15. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.16.10.24420.6	5.16.10 (24420)
	Windows server 2016		
	Windows server 2019		

Table 16. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex App VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10	43.10.0.27605.4	43.10.0.27605
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 17. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	43.10.0.27605.4	43.10.0.27605
	Windows server 2016		
	Windows server 2019		

Table 18. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10	43.10.2.11.3	43.10.2.11
	Windows 11		
	Windows server 2016		
	Windows server 2019		

Table 18. Tested environment—Cisco Webex Meetings (continued)

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
	Windows server 2022 (Not tested)		

Table 19. Tested environment—Cisco Webex Meetings

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2209	Windows 10	43.10.2.11.3	43.10.2.11
	Windows server 2016		
	Windows server 2019		

3

ThinOS 2402

Release details

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

ThinOS 2402

Previous version

ThinOS 2311 (9.4.4123)

Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2402 (9.5.1079)**

NOTE: If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2402. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.

NOTE: If you want to downgrade ThinOS 2402 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell ThinOS 2402 Migration Guide* at Support | Dell. For the steps to access documents, see Resources and support.

Important notes

- To further improve the security of ThinOS devices, from 2402, ThinOS uses OpenSSL version 3.0 with default TLS security level **1**. If your environment requires a legacy OpenSSL version (like an 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.
- ThinOS 2402 is the last quarterly major release for Wyse 3040. For the future ThinOS releases, hotfix and components updates are going to be provided for any required updates.
- 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 a Wyse 3040 device 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, 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 20. TLS Cipher list

Ciphers	Security Status	Removal or change in next release
ECDHE-RSA-AES128-GCM-SHA256	Secure	Not applicable
ECDHE-RSA-AES256-GCM-SHA384	Secure	Not applicable
ECDHE-RSA-AES128-SHA256	Not secure	Subject to change in the next release.
ECDHE-RSA-AES256-SHA384	Not secure	Subject to change in the next release.
ECDHE-RSA-AES128-SHA	Not secure	Subject to removal in the next release.
ECDHE-RSA-AES256-SHA	Not secure	Subject to removal in the next release.
DHE-RSA-AES128-GCM-SHA256	Not secure	Subject to removal in the next release.
DHE-RSA-AES256-GCM-SHA384	Not secure	Subject to removal in the next release.
DHE-RSA-AES128-SHA256	Not secure	Subject to removal in the next release.
DHE-RSA-AES256-SHA256	Not secure	Subject to removal in the next release.
DHE-RSA-AES128-SHA	Not secure	Subject to removal in the next release.
DHE-RSA-AES256-SHA	Not secure	Subject to removal in the next release.
AES128-SHA256	Removed in ThinOS 2303	Not applicable
AES256-SHA256	Removed in ThinOS 2303	Not applicable
AES128-SHA	Removed in ThinOS 2303	Not applicable
AES256-SHA	Removed in ThinOS 2303	Not applicable
AES128-GCM-SHA256	Removed in ThinOS 2303	Not applicable
AES256-GCM-SHA384	Removed in ThinOS 2303	Not applicable
ECDHE-ECDSA-AES128-GCM-SHA256	Secure	Not applicable
ECDHE-ECDSA-AES256-GCM-SHA384	Secure	Not applicable
ECDHE-ECDSA-AES128-SHA256	Not secure	Subject to change in the next release.
ECDHE-ECDSA-AES256-SHA384	Not secure	Subject to change in the next release.
ECDHE-ECDSA-AES128-SHA	Not secure	Subject to removal in the next release.
ECDHE-ECDSA-AES256-SHA	Not secure	Subject to removal in the next release.
DHE-PSK-AES128-GCM-SHA256	Not secure	Subject to removal in the next release.
DHE-PSK-AES256-GCM-SHA256	Not secure	Subject to removal in the next release.
DHE-PSK-AES128-CBC-SHA256	Not secure	Subject to removal in the next release.
DHE-PSK-AES256-CBC-SHA384	Not secure	Subject to removal in the next release.
DHE-PSK-AES128-CBC-SHA	Not secure	Subject to removal in the next release.
DHE-PSK-AES256-CBC-SHA	Not secure	Subject to removal in the next release.
ECDHE-PSK-AES128-CBC-SHA	Not secure	Subject to removal in the next release.
ECDHE-PSK-AES256-CBC-SHA	Not secure	Subject to removal in the next release.

Table 20. TLS Cipher list (continued)

Ciphers	Security Status	Removal or change in next release
ECDHE-PSK-AES128-CBC-SHA256	Not secure	Subject to change in the next release.
ECDHE-PSK-AES256-CBC-SHA384	Not secure	Subject to change in the next release.
PSK-AES128-GCM-SHA256	Not secure	Subject to removal in the next release.
PSK-AES256-GCM-SHA384	Not secure	Subject to removal in the next release.
PSK-AES128-CBC-SHA	Not secure	Subject to removal in the next release.
PSK-AES256-CBC-SHA	Not secure	Subject to removal in the next release.
PSK-AES128-CBC-SHA256	Not secure	Subject to removal in the next release.
PSK-AES256-CBC-SHA384	Not secure	Subject to removal in the next release.
RSA-PSK-AES128-GCM-SHA256	Not secure	Subject to removal in the next release.
RSA-PSK-AES256-GCM-SHA384	Not secure	Subject to removal in the next release.
RSA-PSK-AES128-CBC-SHA	Not secure	Subject to removal in the next release.
RSA-PSK-AES256-CBC-SHA	Not secure	Subject to removal in the next release.
RSA-PSK-AES128-CBC-SHA256	Not secure	Subject to removal in the next release.
RSA-PSK-AES256-CBC-SHA384	Not secure	Subject to removal in the next release.
ECDHE-ECDSA-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
ECDHE-RSA-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
DHE-RSA-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
RSA-PSK-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
DHE-PSK-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
ECDHE-PSK-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
PSK-CHACHA20-POLY1305	Not secure	Subject to removal in the next release.
SRP-RSA-AES-256-CBC-SHA	Not secure	Subject to removal in the next release.
SRP-AES-256-CBC-SHA	Not secure	Subject to removal in the next release.
SRP-RSA-AES-128-CBC-SHA	Not secure	Subject to removal in the next release.
SRP-AES-128-CBC-SHA	Not secure	Subject to removal in the next release.
TLS_AES_128_GCM_SHA256	Secure	Not applicable
TLS_AES_256_GCM_SHA384	Secure	Not applicable
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure	Not applicable

- 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 displayed again.
  - If the new firmware or application is downloaded in the same group, a notification is not displayed.
  - The shutdown window asks to **Update and shut down** or **Update and restart** with a yellow dot on their respective icons. ThinOS updates first before shutting down or restarting.
- 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 2402 (9.5.1079) 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.
- Ensure that you have downloaded the ThinOS 2402 (9.5.1079) operating system 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 2402. Install the latest application packages.

Convert Ubuntu with DCA to ThinOS 2402

Prerequisites

Ensure that DCA-Enabler is installed on your Ubuntu devices according to the below table:

Table 21. 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
Latitude 5450	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

For details on how to install and upgrade DCA-Enabler in the Ubuntu operating system, see *Dell ThinOS 2402 Migration Guide* at Support | Dell.

- 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 2402.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2402.
- 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 2402 Migration Guide* at Support | Dell.
- Ensure you have downloaded the Ubuntu to ThinOS 2402 conversion image.
- Extract the Ubuntu to ThinOS 2402 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.3-dtos3-amd64_signed.tar.gz` and ThinOS image `ThinOS_2402_9.5.1079.pkg`.

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_9.5.1079.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 2402 is in the factory default status. ThinOS 2402 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 22. 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, build, and BIOS packages details

For ThinOS 2402, it is recommended to install the latest application packages from the below table.

Table 23. ThinOS application package details

ThinOS application package details
Amazon_WorkSpaces_Client_24.0.4697.3.pkg
Cisco_Jabber_14.3.0.308378.8.pkg
Cisco_Webex_Meetings_VDI_43.10.2.11.3.pkg
Cisco_Webex_App_VDI_43.10.0.27605.4.pkg
Citrix_Workspace_App_23.11.0.82.6.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

Table 23. ThinOS application package details (continued)

ThinOS application package details
Identity_Automation_QwickAccess_2.1.0.7.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.5.6.pkg
Lakeside_Virtual_Agent_99.0.0.173.7.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.6.2.5.10.pkg
Microsoft_AVD_2.4.2282.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_23.06.2.18.pkg
ThinOS_Telemetry_Dashboard_1.0.0.7.pkg
VMware_Horizon_2309.8.11.0.22660930.37.pkg
VMware_Horizon_ClientSDK_2309.8.11.0.22660930.46.pkg
Zoom_Universal_5.16.10.24420.6.pkg

Important notes

- **VMware**
  - From 2024, VMware does not support VMware Horizon Session SDK., which is the SDK in use for the VMware Horizon Client for ThinOS package.
  - With ThinOS 2306, both VMware Horizon Session SDK and the new VMware Horizon Client SDK-based package versions of VMware Horizon Client for ThinOS are released.
  - From ThinOS 2408 onwards, only VMware Horizon Client SDK-based version of the Horizon Client for ThinOS package is provided.
  - Ensure that you upgrade your environment to the VMware Horizon Client SDK-based version of the VMware Horizon Client for ThinOS.
  - To ensure that the upgrade is complete, verify the package name—`VMware_Horizon_ClientSDK_2309.8.11.0.22660930.46.pkg`
- **Zoom**
  - From ThinOS 2402, **Zoom_Citrix**, **Zoom_Horizon**, or **Zoom_AVD** packages are not released.
  - Instead, one **Zoom_Universal** package is released that can be used with all three VDI environments.
  - There is no difference in functionality and features.
- After upgrading to ThinOS 2402, all application packages that are released before 2205, Microsoft AVD package that is released before 2311, Zoom AVD, Zoom Citrix, and Zoom Horizon packages are removed automatically and cannot be installed again. You must install the latest application packages.

ThinOS build

- ThinOS 9.1.3129 or later versions to ThinOS 2402 (9.5.1079)—`ThinOS_2402_9.5.1079.pkg`
- Ubuntu to ThinOS 2402 conversion build—`ThinOS_2402_9.5.1079_Ubuntu_Conversion.zip`

Tested BIOS versions and BIOS packages

The following table contains the tested BIOS versions and BIOS packages for ThinOS 2402.

Table 24. Tested BIOS versions and BIOS packages

Supported platform	Tested BIOS version	New BIOS package
Wyse 3040 Thin Client	1.2.5	Not applicable

Table 24. Tested BIOS versions and BIOS packages (continued)

Supported platform	Tested BIOS version	New BIOS package
Wyse 5070 Thin Client	1.26.0	Not applicable
Wyse 5470 All-in-One Thin Client	1.22.0	Not applicable
Wyse 5470 Mobile Thin Client	1.21.0	Not applicable
Dell OptiPlex 3000 Thin Client	1.15.0	bios-Op3000TC_1.15.0.pkg
Dell Latitude 3420	1.33.0	bios-Latitude_3420_1.33.0.pkg
Dell OptiPlex 5400 All-in-One	1.1.36	bios-OptiPlex5400AIO_1.1.36.pkg
Dell Latitude 3440	1.9.1	bios-Latitude3440_1.9.1.pkg
Dell Latitude 5440	1.10.0	bios-Latitude5440_1.10.0.pkg
Dell Latitude 5450	1.0.2	Not applicable
Dell OptiPlex AIO 7410	1.11.0	bios-OptiPlexAIO7410_1.11.0.pkg
Dell OptiPlex AIO 7420	1.0.0	Not applicable

Wyse Management Suite and Configuration UI packages

- Wyse Management Suite version 4.3
- Configuration UI package 1.10.275

NOTE: Use Wyse Management Suite 4.3 server for the new Wyse Management Suite ThinOS 9.x Policy features.

NOTE: Configuration UI package 1.10.275 is embedded with Wyse Management Suite 4.3 server.

Feature Matrices

Citrix Workspace App feature matrix

Table 25. Citrix Workspace app feature matrix

Feature		ThinOS 2402 with CWA 2311	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.

Table 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	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.
	EUEM Experience Matrix	Supported	There are no limitations in this release.

Table 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	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 ThinOS 2402 Administrator's Guide at Support | Dell.
	Skype for business Optimization pack	Supported	Not support through proxy server
	Cisco Jabber Unified Communications Optimization	Supported	For more information, see the Dell ThinOS 2402

Table 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
			Administrator's Guide at Support | Dell.
	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 ThinOS 2402 Administrator's Guide at Support | Dell.
	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 ThinOS 2402 Administrator's Guide at Support | Dell
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization using 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 ThinOS 2402 Administrator's Guide at Support | Dell
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.

Table 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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 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 ThinOS 2402 Administrator's Guide atSupport | Dell.
	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 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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	EPA scan is not supported in ThinOS.
	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 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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	App Protection compatibility with HDX optimization for Microsoft Teams	Not Supported	Not Supported
	Fast smart card	Not Supported	Not Supported

Table 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Support for Audio volume synchronization	Not Supported	Not Supported
	Improve audio performance during audio loss	Not Supported	Not Supported
	Loss tolerant mode for audio	Not Supported	Not Supported
	Collecting user activity logs	Not Supported	Not Supported
	Addition of a new library	Not Supported	Not Supported
	Improved loading experience for shared user mode	Not Supported	Not Supported
	Enhancement to Storebrowse commands	Not Supported	Not Supported
	Multimedia redirection support for ARM64 devices	Not Supported	Not Supported
	Version upgrade for Chromium Embedded Framework	Supported	There are no limitations in this release.
	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	Supported	For information about limitations, see the Dell ThinOS 2402 Administrator's Guide at Support | Dell

Table 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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 ThinOS 2402 Administrator's Guide at Support | Dell
	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	Supported	There are no limitations in this release.
	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 25. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	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. 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
	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 26. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 2402
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
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 27. VMware Horizon session and client package versions

Horizon	Package version
Horizon Session SDK	VMware_Horizon_2309.8.11.0.22660930.37.pkg
Horizon Client SDK	VMware_Horizon_ClientSDK_2309.8.11.0.22660930.46.pkg

Table 28. 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	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	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	Supported

Table 28. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	CAC support	Supported	Supported
	.Net support	Supported	Supported
	PIV support	Supported	Supported
	Java support	Supported	Supported
	Purebred derived credentials	Not Supported	Not Supported
	Device Cert auth with UAG	Supported	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	Supported
	PCoIP	Supported	Supported

Table 28. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
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
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

Table 28. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	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 Clould 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

Table 28. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	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)
	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

Table 28. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	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	Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported	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.

ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix

Table 29. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix

Feature	ThinOS version 9.5.1079
Client access restriction	Supported
USB redirection	Not supported
Audio input	Supported
Video input	Not supported
Storage redirection	Not supported
Local printer redirection	Not supported
Clipboard redirection	Supported
Active directory authentication	Supported
SAML 2.0	Not supported
Certificate-based Authentication	Supported
Multi-factor authentication (MFA)	Supported
Smartcards (CAC and PIV readers)	Supported
Certificate for access control	Supported
Encryption at rest	Supported
Client customization	Not supported
YubiKey	Not supported
Monitor	Supported (Dual Monitor with 3840x2160 resolution)

What's new

Citrix Workspace app updates

Citrix Workspace App (CWA) package version is updated to 23.11.0.82.6 , and the package can install the Citrix Workspace App version 2311 on ThinOS.

Authentication using FIDO2 when connecting to on-premises stores

- From ThinOS 2402 and Citrix Workspace App 2311, you can authenticate using FIDO2 security keys, which do not require passwords, when signing in to on-premises stores.
- Citrix Workspace app uses the **ThinOS Extension** as the default browser for FIDO2 authentication in ThinOS.

  NOTE: In ThinOS 2311, **Citrix CEB** was the default option. In ThinOS 2402 the **Citrix CEB** option is deprecated due to a security concern, so **ThinOS Extension** is the only viable option.
- Administrators can configure the **ThinOS Extension** using Admin Policy Tool or Wyse Management Suite policy settings to authenticate to CWA.
- To enable FIDO2 authentication for logging in to on-premises stores, do the following:
  1. Open Admin Policy Tool or Wyse Management Suite policy.
  2. Go to **Broker Settings > Citrix Virtual Apps and Desktops Settings**.
  3. Set **Broker server address** to the address that has enabled FIDO2 authentication method.

     NOTE: FIDO2 Security Key to log in to Citrix ADC with OKTA SAML MFA and FIDO2 Security Key to log in to Citrix ADC with Azure AD MFA are two test environments that can be used in ThinOS.
  4. Enable **WebLogin Use External Engine**.
  5. Ensure that **WebLogin Use ThinOS Extension** is **ThinOS Extension**. **ThinOS Extension** is the only supported extension and is the default value.

     NOTE: To use **ThinOS Extension**, install the ThinOS Extension application package and enable the policy.

     NOTE: Do not use the Citrix Enterprise Browser (CEB).
  6. Click **Save & Publish**.
  7. Sign out or restart the device for the settings to take effect.
  8. In the webview login window, enter the PIN code of the Yubikey device.
  9. Touch the Yubikey device to log in to the Citrix broker server.
- Supported FIDO2 devices:
  - Yubikey 5 NFC
  - Yubikey 5 Ci

  NOTE: ThinOS ignores the Citrix file **AuthManConfig.xml** to configure the FIDO2 authentication. ThinOS only supports the Wyse Management Suite setting **WebLogin Use External Engine** to enable or disable the FIDO2 authentication.
- Limitations:
  - You cannot lock or unlock the terminal using FIDO2; you can only set a temporary password.
  - Due to the current ThinOS FIDO2 design, you cannot remain signed in when logging in to Microsoft Azure webview.
  - A **Connecting session xxx** dialog box is always on top of the NetScaler timeout user login window. You can ignore the dialog box, and continue to log in using FIDO2. Then, the connecting session is launched automatically.
  - Only a security key sign-in option is supported in ThinOS to log in to Citrix ADC using FIDO2 authentication.

Fixed stretched video images issue in an optimized Microsoft Teams video call

The issue that a video image may be stretched in an optimized Microsoft Teams video call is fixed in Citrix Workspace App 2311. To enable this fix, 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 JSON Settings**, click **Add Row**.
3. From the **File** drop-down list, select **hdx_rtc_engine/config.json**.
4. From the **Operation** drop-down list, select **Add or Update**.

5. In the **Key** field, enter **`AdaptResolutionAllowCroppingVideo`**.
6. In the **Value** field, enter **`1`**.
7. Sign out or restart the device for the settings to take effect.

Android smartphone USB redirection through Citrix Configuration Editor

From ThinOS 2402 and Citrix Workspace App 2311, you can configure the Android smartphone device redirection using **Citrix USB File Settings** in Citrix Configuration Editor. To redirect the Android smartphone into an ICA session, do the following:

1. In the **Key** field, enter **CONNECT**.
2. In the **Value** field, enter **`vid=04e8 pid=6860 split=01 intf=00`**.

   NOTE: The VID PID in the **Value** field must be replaced by the VID PID of your Android smartphone. Samsung Galaxy SM-E5260 phone is qualified with ThinOS 2402.

If you have already configured **Citrix USB File Settings** to redirect the device, do not configure **USB Redirection** in **Peripheral Management > USB Redirection > vUSB Force Redirect**.

Citrix log enhancement

- From ThinOS 2402 and Citrix Workspace App 2311, the Citrix log path is changed from `/var/log/citrix` to `/compat/linux/var/log/citrix`.
- Citrix log can be enabled through the **Log Level** setting in **Session Settings > Citrix Session Settings** inside Wyse Management Suite.

Citrix Keyboard Layout mode enhancement

- From ThinOS 2402 and Citrix Workspace App 2311, the Citrix VDI Configuration Editor is not required to configure the Citrix keyboard Server default mode and Dynamic Sync mode.
- All the Citrix keyboard layout modes can be configured through the **Keyboard Layout Mode** setting in **Session Settings > Citrix Session Settings**.

Citrix Workspace App limitations

- Android smartphone USB redirection is not supported by Samsung S23 and S24 as the phones are not detected by ThinOS.
- The **High DPI** feature in **Citrix Desktop Viewer toolbar > Preferences > General** is not supported.
- The following issues also occur in the Citrix Workspace App Linux binary:
  - The Citrix toolbar appears on the topmost monitor irrespective of the primary monitor.
  - Desko scanner does not work in Citrix VDI sessions.

Microsoft RDP and AVD updates

Microsoft AVD package is updated to version 2.4.2282 in ThinOS 2402.

RDP and AVD known issue

- The Microsoft AVD package of ThinOS 2402 is not supported in the previous ThinOS release.
- You must install both ThinOS 2402 and Microsoft AVD package simultaneously.
- If you want to install the Microsoft AVD 2.3.2266 package, upgrade to ThinOS 2311.
- Due to hardware limitations, the camera through USB redirection is only works on Latitude and OptiPlex All-in-One series.

Teradici PCoIP updates

- Teradici version is updated to 23.06.2.18 in ThinOS 2402.
- The Teradici PCoIP package version 23.06.2.18 cannot be installed to the previous ThinOS release.
- The latest PCoIP package version 23.06.2.18 must be installed for PCoIP sessions on ThinOS 2402.

VMware Horizon updates

- The Horizon Session SDK package is updated to `VMware_Horizon_2309.8.11.0.22660930.37.pkg`.
- The Horizon Client SDK package is updated to `VMware_Horizon_ClientSDK_2309.8.11.0.22660930.46.pkg`.
- The new features of Horizon Client SDK are as follows:

Supports RDP protocol

- RDP sessions can be displayed and launched in Horizon Broker.
- The Microsoft AVD package is required for the RDP feature.

Supports Horizon HTTPs secure tunnel

- Horizon HTTPs Secure Tunnel can be configured in Horizon Connection Server.
- ThinOS Horizon Client SDK supports Horizon broker connection when **Secure Tunnel** is enabled in the server.
- ThinOS also supports the **Enable Credential Security Service Provider** setting to log in through a secure tunnel.

Supports device certificate authentication in Horizon UAG

- Device certificate authentication is supported in ThinOS Horizon Client SDK 2309.
- The feature is functional when the **Login Use Smartcard Certificate Only** setting in Wyse Management Suite or Admin Policy Tool is disabled.

NOTE: The device certificate must be imported after ThinOS Horizon Client package installation.

Supports Horizon Cloud Next Gen

- Horizon Cloud Next Gen is the latest generation of Horizon Cloud and is supported with the ThinOS Horizon Client SDK package.
- You can configure Horizon Cloud Next Gen by doing the following:
  1. Go to **Remote Connections > Broker Setup > VMware Horizon > Broker Server**.
  2. Initialize the Horizon broker connection from the ThinOS login window.

     The Horizon Cloud web page opens.
  3. Enter **Use Company Domain**.
  4. Click **Continue**.
  5. Enter the username and password.

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

FIDO2 enrollment and authentication in VMware Workspace One Access and Smartcard authentication in Azure MFA are supported in Horizon Session SDK

- To use this function, the ThinOS Extension application package must be installed.
- To enable the function, follow these steps:
  1. Go to **VMware Horizon Settings** in Wyse Management Suite or Admin Policy Tool.
  2. Enable **WebLogin Use ThinOS Extension**.
  3. Enable **Enable Extension Policy** in **Extension Settings**.
- **Known issues and limitations**
  - The lock terminal triggers a temporary password configuration as the local user data is not saved when using the ThinOS extension.
  - Only the Horizon Session SDK package supports this function. Horizon Client SDK does not support it.
  - When the ThinOS extension is enabled, Horizon Cloud Next Gen is not connected. As a workaround, disable **Weblogin use ThinOS Extension**.

Known Issues

- **Disabling Zoom optimized mode is not supported**—In **WMS Advanced > Session Settings > Blast Session Settings**, if **Zoom Meeting Optimized** is disabled, Zoom still runs in Optimized mode in Blast sessions.
- You can plug-in your Smart Card before logging in to ThinOS Horizon broker when the **Smartcard required** option is enabled in the Horizon server.

Amazon WorkSpaces Client with WSP updates

- ThinOS supports Amazon WorkSpaces Client Mode with this ThinOS release.
- The supported Amazon WorkSpaces client version is 24.0.4697.
- The ThinOS Amazon WorkSpaces Client package version is 24.0.4697.3.
- Amazon WorkSpaces desktop with WSP protocol is supported in the session that is launched from Amazon WorkSpaces Client Mode.
- ThinOS Amazon WorkSpaces Client Mode supports password, MFA, and smart card authentications. The ThinOS Extension package is required when using smart card authentication.

New settings for Amazon WorkSpaces Client with WSP

- **Enable Amazon WorkSpaces Client Mode**—The setting enables the Amazon WorkSpaces client to log in to Amazon WorkSpaces and launch a WSP session.
- **WebLogin use ThinOS Extension**—The setting must be enabled to use the smart card authentication.

Configuring Amazon WorkSpaces Client with WSP

You can configure using Wyse Management Suite or ThinOS Admin Policy Tool by following these steps:

1. Open Wyse Management Suite or ThinOS Admin Policy Tool.
2. Go to **Broker Settings > Amazon WorkSpaces Settings**.
3. Enable the **Connect via Registration Code** option.
4. Enable the **Enable Amazon WorkSpaces Client Mode** option.
5. If you want to use smartcard authentication, enable the **WebLogin use ThinOS Extension** setting.

You can configure locally in ThinOS by following these steps:

1. Go to **ThinOS Settings > Remote Connections**.
2. Select **Amazon WorkSpaces** broker type.
3. Select the **Enable Amazon WorkSpaces Client mode** checkbox.
4. If you want to use smartcard authentication, select the **WebLogin use ThinOS Extension** checkbox.

Limitations and known issues

- The camera in ThinOS is not detected on the Amazon WorkSpaces Client with WSP desktop.
- The Amazon WorkSpaces Client with WSP desktop is not in the ThinOS session list when logging in using the **Modern** mode.
- The Amazon WorkSpaces page icon and WSP desktop in the ThinOS taskbar is not shown as an Amazon icon.
- After restarting the terminal, the **username** field in the **AWS Apps Authentication** page displays the username from the previous session.
- After reconnecting the network and clicking **Try Again** in the Amazon WorkSpaces page, you have to reenter the registration code.
- The icons for the minimize and close buttons in the Amazon WorkSpaces page are not shown in the upper-right corner.
- Sometimes, the local ThinOS computer stops responding during WSP login or after restarting the computer.
- There is an issue with the graphics when using Amazon WSP desktop in Latitude 5450.
- Sometimes the Electron window is shown during the Amazon WSP broker login.
- The **Move** and **Resize** buttons, which are accessed by right clicking the WSP desktop taskbar, are not working.
- If you sign off from the WSP broker before the **Connect to AWS session** window is displayed, the signoff fails and the shutdown menu is unresponsive.
- If you plug-in the smartcard after the **Amazon Web Services** window is displayed, the smartcard is not detected.

- The WSP desktop is automatically disconnected when the **Lock the desktop with Smartcard authentication** is enabled.
- In some dual-monitor layouts, the Amazon WorkSpaces login page is not displayed on the home screen.
- If you use the Amazon WSP desktop in full-screen mode with two connected monitors, a second Amazon WorkSpaces desktop icon is shown in the taskbar.
- After switching to ThinOS desktop using Ctrl + Alt + Down, the keyboard in Amazon WorkSpaces desktop does not work.
- The local ThinOS keyboard does not work when the WSP desktop is in full-screen mode.

Identity Automation updates

Identity Automation Package version is updated to 2.1.0.7.

NOTE: The broker server must be in the same domain as the Identity Automation server.

Supports Self-Service Password Reset (SSPR)

You can reset the password yourself by answering questions. Ensure that the Lynx server version is 1.7.1.x, and the Identity Automation package version is 2.1 or later.

After enrolling yourself to the SSPR feature of your card, follow these steps to reset your password:

1. Select **Sign-on without a badge**.
2. Click **Forgot your password**.
3. Enter your username.
4. Enter your new password after answering the questions correctly.

NOTE: After resetting the password once, if you try to tap the card to log in again, Identity automation may ask you to enter the password even if the Lynx server setting is set to authenticate using PIN.

Imprivata OneSign Authentication updates

Supports display setting window

The display setting window can be opened in Imprivata PIE mode by using the Windows key and the letter P combination (Win + P).

NOTE: The display setting window icon is shown in the Imprivata taskbar after logging in to the XenApp broker.

Zoom updates

- Zoom package is updated to the Zoom universal package version 5.16.10.24420.5.
- The package is common for all three brokers—Citrix, Horizon, Microsoft AVD.
- In ThinOS 2402, only Zoom Universal Package is supported.
- The Zoom universal package is supported in old releases of ThinOS, but the admin must uninstall the old Zoom package.

New features

- Sign-in and switch between accounts.
- Quickly create Zoom meetings in Teams chat.
- Disable Zoom notes for meetings.

Lakeside Virtual Agent updates

- The Lakeside Virtual Agent package version 99.0.0.173.7 is supported with ThinOS 2402.
- A virtual machine running the Lakeside SysTrack agent is required, which is downloadable from your Lakeside cloud tenant.
- **Prerequisites to install Lakeside Virtual Agent:**

- The time zone must match with the client and VDA sessions.

- To check the performance of the client, install the Lakeside virtual agent using Wyse Management Suite.

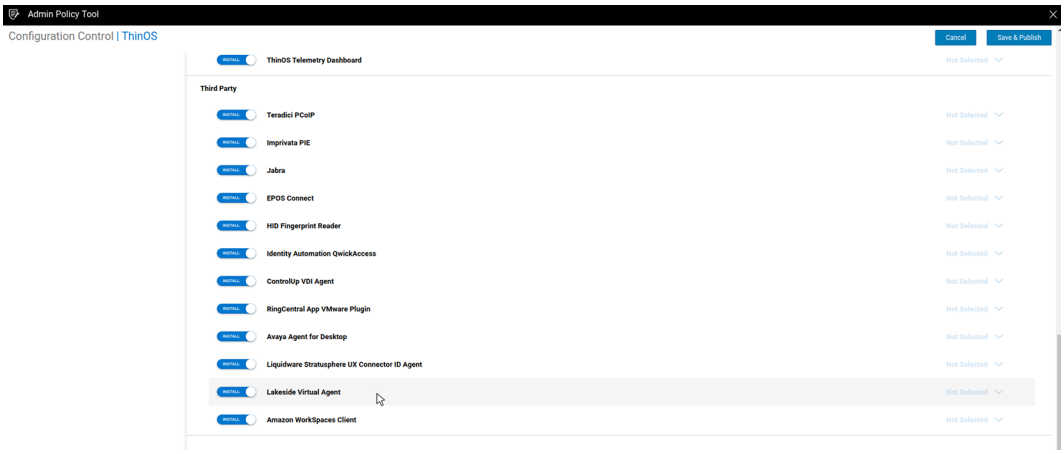

Figure 1. Lakeside virtual agent in Configuration Control

Figure 2. Lakeside Virtual Agent Dashboard

ThinOS updates

Improved the ThinOS graphical UI experience

- Changed the **OK** button to **Save** button on most of the windows.
- Switched the position of **Save** button and **Cancel** button.
- Updated the **Save** and **WiFi** icons.
- You can resize the **System Information** window to check more event logs.

NOTE: The **Cancel** button icon and **Save** button icon are present in modern mode only. Classic mode does not have the icons.

Improved Wyse 5070 and 5470 Thin Client BIOS update process

- If you are updating the devices through a BIOS update policy from Wyse Management Suite, the BIOS update process has been improved.
- If a monitor is not connected to Wyse 5070, the BIOS update fails by design. After the monitor is connected, the BIOS update resumes and goes to the BIOS update screen immediately.

- If a power adapter is not connected on the Wyse 5470, the BIOS update fails. After the power adapter is connected, you must reboot to trigger the BIOS update again.

Updated the shutdown window to display the defer update status

If you click **Next Reboot** or schedule the update time to defer the operating system, BIOS, or application installation, the shutdown window asks to **Update and shut down** or **Update and restart** with a yellow dot on their respective icons. ThinOS updates first before shutting down or restarting.

NOTE: If you press the power button to shutdown, ThinOS shuts down and updates when you turn on the next time.

Improved the operating system, BIOS, and application update process with select group

- In previous ThinOS versions, if there is a policy change with a new operating system, BIOS, and applications in a select group, you must reboot the ThinOS device to download the new operating system, BIOS, and applications to install.
- From ThinOS 2402, if there is a policy change with a new operating system, BIOS, and applications in the parent select group, or a registered child select group, the device downloads the new operating system, BIOS, and applications and installs immediately.
- For example, the ThinOS device is registered to the Wyse Management Suite child1 select group.
  - If there is a policy change with the new operating system, BIOS, and applications in the parent select group, the device downloads and installs immediately.
  - If there is a policy change with the new operating system, BIOS, and applications in the child1 select group, the device downloads and install immediately.
  - If there is a policy change with the new operating system, BIOS, and applications in other child select groups, the device does not download.

Dell ThinOS Recovery boot option in BIOS

- From ThinOS 2402, a new BIOS boot option **DellThinOS Recovery** is added in devices from the factory or installed through an ISO image.
- When you boot using this option, the devices are reset to their factory installed or ISO image-installed status.
- **Important Notes**
  - If you update your old devices to ThinOS 2402 using Wyse Management Suite, you cannot view the Dell ThinOS Recovery boot option.
  - If the device size is less than 32 GB, the Dell ThinOS Recovery boot option is not created.

Updated the Enable Schedule Update policy process in Wyse Management Suite and Admin Policy Tool

- At the scheduled update time, there is a 120-second countdown window that is displayed.
- You can schedule a new time for the update within 24 hours from the time you made the first schedule update change.

NOTE: If you have scheduled an update time and restart or shutdown the device, then the device updates immediately, even when not at the scheduled update time. After an update, the device restarts or shuts down.

New Save & Reboot button in the local Display settings

- A new **Save & Reboot** button is added that can apply resolution, rotation, and other display changes.
- After the changes are applied, the device restarts.
- To view the button and use the feature, follow these steps:
  1. Open the **Display** menu.
  2. Change the resolution or rotation.
  3. Click **Test**.
  4. Click **Save & Reboot** to apply the changes and restart your device.

Enable Rollback to Last Known Good Status

- The option is in the **Troubleshooting** section in the **General** tab in Wyse Management Suite and Admin Policy Tool.
- **Enable Rollback to Last Known Good Status** is not available by default.
- If you want to use it, you must enable the **Enable Rollback to Last Known Good Status** in **WMS/APT > Troubleshooting Settings > Troubleshooting Settings**.
- If you click the button and confirm, the operating system version, applications, and settings of the client rolls back to the previous operating system configuration.
- **Important Notes**
  - The option can only be enabled on ThinOS devices with 64 GB storage or more.
  - When rolling back to the previous version, ThinOS retains the Wyse Management Suite settings. If there are no changes to the Wyse Management Suite group settings, ThinOS does not download any configurations from the Wyse Management Suite group.

    After clicking the **Enable Rollback to Last Known Good Status** button, ThinOS successfully rolls back and there is no change to the operating system version, the **Enable Rollback to Last Known Good Status** feature cannot work.

    The **Enable Rollback to Last Known Good Status** feature works in ThinOS 2402 and later versions.

Added Create QR Code and Scan QR Code in Central Configuration

To use the features, do the following:

1. Go to **Central Configuration**.
2. Enter the valid group registration key and Wyse Management Suite server URL.
3. Click **Create QR Code** button, and a QR code is created.
4. Export the QR code to a USB drive and print it, or save it to another device.
5. Click **Scan QR code** on any other ThinOS device with an integrated camera or external camera to automatically register to the Wyse Management Suite configuration.

NOTE: The QR code is valid for 7 days. **Scan QR Code** is only available when the camera is connected. If multiple cameras are connected, ThinOS automatically selects a camera to scan.

Added QR Code Scan page in the Out of Box Experience (OOBE)

- To see the **QR Code Scan** page, reset the client to factory default status.
- If the device has an integrated camera or an external camera, then you can see the **QR Code Scan** page in the OOBE.
- You can scan the QR code to automatically register to the Wyse Management Suite configuration.
- If scanning the QR code is not required, click the **Next** icon to go to the next page.

Supports new WiFi 6E regions

Mexico and Thailand WiFi 6E regions are supported with ThinOS 2402.

Wyse Management Suite and Admin Policy Tool updates

NOTE: Wyse Management Suite 4.3 server is required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

Log Level in Citrix Session Settings

- Added **Log Level** setting in **Session Settings > Citrix Session Settings**.
- The setting allows you to enable Citrix log with the below levels:
  - Disabled
  - Verbose
  - Information

  - Warnings
  - Errors
  - Fatal Errors
- You must relaunch the Citrix session to make the **Log Level** setting take effect.
- The inherited log level cannot be configured through Wyse Management Suite policy.
- If you use the **Citrix Log Preferences** window to set the level, do not change the other fields of the Citrix log in the **Citrix Log Preferences** window. ThinOS supports changing the log level in Wyse Management Suite or **Citrix Log Preferences** only.

Device Driver

- Added the **Device Driver** option in **Peripheral Management**.
- With the feature, enter the USB device VID PID to force the USB device to use UHID driver.
- The option is for special USB devices that do not work well by default.

Show Admin and Shutdown Button

- Added **Show Admin** and **Shutdown** Button in **Lock Terminal** in **Login Experience > Login Settings > Login Experience**.
- If enabled, the **Admin** and **Shutdown** button is displayed in the login window.

NOTE: The policy only works when logging in using **Modern** mode.

Enable eMMC Disk Lifetime

- Added **Enable eMMC Disk Lifetime** in **Services > WDA Settings**.
- If enabled, the device reports the eMMC Disk Lifetime information to the Wyse Management Suite server; you can check the information from the **System Info** tab.

Screen Refresh Rate(Hz)

- Added **Screen Refresh Rate(Hz)** in **Peripheral Management > Monitor**.
- You can adjust the screen refresh rate with the option.

New application package categories

- Added the following application package categories:
  - Zoom Universal
  - ThinOS Telemetry Dashboard
  - Lakeside Virtual Agent
  - Amazon WorkSpaces Client
- From ThinOS 2402, ThinOS only supports Zoom Universal package and does not support Zoom Citrix, Zoom Horizon, Zoom AVD packages.
- You cannot install the previous Zoom Citrix, Zoom Horizon, and Zoom AVD packages and when the Zoom Universal package is installed, the packages are automatically uninstalled.

ThinOS Telemetry Dashboard

- Added **Telemetry Dashboard** in **System Settings > Device Monitoring**.
- If enabled, **Telemetry Dashboard** button in **Troubleshooting** window is available on the ThinOS client.
- You can click the button to open the dashboard and check device information and monitor the hardware usage.
- The **Update Interval In Seconds** option can be used to set hardware usage monitor interval.
- **Limitation**: RDP direct connection, VMware RDP connection, and Amazon WorkSpaces Client WSP connection are not shown in **Telemetry Dashboard**.

New BIOS pages

Added new BIOS pages for Dell Latitude 5450.

Enable Webcam Audio

- Added **Enable Webcam Audio** in **Peripheral Management > Audio**.
- The option enables or disables the USB webcam microphone and requires a restart to take effect.

ThinOS customized downloads feeds

- Added the **ThinOS customized downloads feeds** option in **Broker Settings > Azure Virtual Desktop Settings**, which is enabled by default.
- If enabled, ThinOS uses the ThinOS customized API to download Azure Virtual Desktop feeds,
- If disabled, ThinOS uses the Microsoft API to download Azure Virtual Desktop feeds.

Enable Rollback to Last Known Good Status

- Added the **Enable Rollback to Last Known Good Status** option in **Services > Troubleshooting Settings > Troubleshooting Settings**, which is disabled by default.
- If enabled, the **Enable Rollback to Last Known Status** button is displayed in the **General** tab in the **Troubleshooting** window.

Enable Logs Preserved at Reboot

- Added the **Enable Logs Preserved at Reboot** option in **Services > Troubleshooting Settings > Log Settings**, which is disabled by default.
- To help improve the disk lifetime for small storage devices like Wyse 3040 thin clients with 8 GB, from ThinOS 2311 all logs were moved from disk to RAM. The **Enable Logs Preserved at Reboot** option can be enabled to move logs that are saved from RAM to disk during a normal restart or shutdown. The logs in RAM are cleared on reboot.
- If enabled, the logs are zipped and transferred from RAM disk to the local disk before restart or shutdown.
- The logs that are zipped are saved as `/var/logs`.

NOTE: Up to three .zip file logs can be saved. When the fourth file is generated, the first file is deleted and the fourth file is saved as the third file.

Persistent Logs on Disk

- Added the **Persistent Logs on Disk** option in **Services > Troubleshooting Settings > Log Settings**, which is disabled by default.
- To help improve disk lifetime for small storage devices like Wyse 3040 thin clients with 8 GB, from ThinOS 2311, all logs were moved from disk to RAM. **Persistent Logs on Disk** can be enabled to put logs on the disk. The logs are not lost due to abnormal reboots or shutdowns, including pressing the power button to shut down.
- If enabled, a dialog box is displayed in the right-bottom corner for a manual reboot to start logging on the disk.
- If disabled, a dialog box is displayed in the right-bottom corner for a manual reboot to stop logging on the disk.
- When the device boots up, the device self-checks if the logs are written to disk. If yes, a dialog box is displayed in the right-bottom corner.

Auto Disable Persistent Logs on Disk

- Added the **Auto Disable Persistent Logs on Disk** option in **Services > Troubleshooting Settings > Log Settings**, which is not enabled by default .
- You must select the **Persistent Logs on Disk**, and then the **Auto Disable Persistent Logs on Disk** option is displayed.
- The option is provided to set a stop date for the **Persistent Logs on Disk** option. For small storage device like Wyse 3040 thin clients with 8 GB, reducing the logs on the disk can help improve disk lifetime.

- If you enter a valid date, which is no more than 7 days from the date of enablement, the device checks on every boot against the stop date and stops persistent logging on the disk.
- If the entered date is invalid or exceeds 7 days from the date of enablement, the device calculates the stop date as 7 days from the date of enablement . The device also checks on every boot against the stop date and stops persistent logging on the disk.
- Before the stop date, the admin can set a new date for the device to recalculate the stop date, which does not require a manual reboot.
- On the calculated stop date, if the device does not reboot, the device continues to log on to the disk until the next reboot.

NOTE: After enabling the **Persistent Logs on Disk** option, the valid date should be within 7 days.

Options for Audio Shortcut key

- Added some options in **Personalization > Shortcut Keys > Audio Shortcut key**.
- If the **Enable Audio Shortcut Key** option is enabled, the following options are displayed:

Table 30. Audio shortcut key options

Option	Default Value
Increase volume key	F3
Decrease volume key	F2
Shortcut key with Ctrl	Disabled
Shortcut key with Alt	Disabled

- **Known Issue**: Long-pressing the shortcut keys do not work for the Audio Shortcut key.

Options for Display Shortcut key

- Added some options in **Personalization > Shortcut Keys > Display Shortcut key**.
- **Known Issue:** Long pressing the shortcut keys do not work for **Display Shortcut key**.
- If the **Enable Display Shortcut key** option is enabled, the following options are displayed:

Table 31. Display shortcut key options

Option	Default Value
Increase brightness key	F7
Decrease brightness key	F6
Shortcut key with Ctrl	Disabled
Shortcut key with Alt	Disabled

NOTE: The brightness adjustments are supported only in ThinOS All-in-One devices.

Options for Background Info Settings

- Added some options in **Personalization > Desktop > Background Info Settings**.
- If the **Enable Background Info** option is enabled, the following options are displayed:

Table 32. Enable Background Info options

Option	Default Value
Background Info font size	14
Background Info font color	White

- In **Background Info Custom Settings**, if you click **Add Row** and enter the characters that you want to display, the characters are displayed below the watermark.

NOTE: If the corresponding application is not installed in ThinOS, even if the application is selected in **Granular Control** of the **Background Info** list, the application information is not displayed in the watermark.

WebLogin Use ThinOS Extension for Horizon FIDO2 authentication

- FIDO2 enrollment and authentication are supported in Horizon Workspace One mode.
- The setting requires installation of the ThinOS Extension application package.
- Install the ThinOS Extension application package and then enable the policy for the web login function.

Enable Remote Shadow Watermark and Specify watermark Message

- Added **Enable Remote Shadow Watermark** and **Specify Watermark Message** in **Services > Remote Shadow Settings**
- If **Enable Remote Shadow Watermark** option is enabled, you can see a red frame border for the shared screen and a default watermark message **username@IP** on the shared screen.
- The **Remote Shadow Password** field supports a minimum of eight characters in **Services > Remote Shadow Settings**.

Updated WebLogin Use External Engine and WebLogin Use ThinOS Extension settings

- The **WebLogin Use External Browser** setting name is changed to **WebLogin Use External Engine** in **Broker Settings > Citrix Virtual Apps and Desktops Settings**.
- Enable the **WebLogin Use External Engine** setting to use the external engine for Citrix web-based login.

  The **External Browser Type** setting name is changed to **WebLogin Use ThinOS Extension** in **Broker Settings > Citrix Virtual Apps and Desktops Settings**.

  ThinOS Extension is the only extension that is supported and is the default value in the **WebLogin Use ThinOS Extension** setting.

Updated Terminal Name option disallows characters

In **System Settings > Device Settings**, the **Terminal name** field does not allow ` ' ! characters for security reasons.

Tested environment and peripheral matrices

General tested environments matrices

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

Table 33. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.3
Configuration UI package for Wyse Management Suite	1.10.275
Citrix ADC (formerly NetScaler)	13.0
StoreFront	1912 LTSR and later

Table 34. 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 35. 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
VMware Horizon 2309	Tested	Tested	Not tested	Not tested	Tested	Not tested	Not tested	Tested	Tested

Table 36. 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 37. Test environment – VMware Horizon Cloud version 2

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

Table 38. 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 39. 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 40. Test environment—Windows 365 cloud PC

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

Table 41. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10 Windows 11 Windows server 2016 Windows server 2019 Windows server 2022 (Not tested)	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015

Table 42. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10 Windows 11 Windows server 2016 Windows server 2019 Windows server 2022 (Not tested)	14.3.0.308378.8	14.3.0.308378	14.3.0.308378

Table 43. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10 Windows server 2016 Windows server 2019	14.3.0.308378.8	14.3.0.308378	14.3.0.308378

Table 44. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10	5.16.10.24420.6	5.16.10 (24420)
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 45. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	5.16.10.24420.6	5.16.10 (24420)
	Windows server 2016		
	Windows server 2019		

Table 46. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.16.10.24420.6	5.16.10 (24420)
	Windows server 2016		
	Windows server 2019		

Table 47. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex App VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) Citrix Virtual Apps and Desktops 7 2203 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10	43.10.0.27605.4	43.10.0.27605
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 48. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 2209 VMware Horizon View 7.13.2	Windows 10	43.10.0.27605.4	43.10.0.27605
	Windows server 2016		
	Windows server 2019		

Table 49. 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 (CU3) Citrix Virtual Apps and Desktops 7 2308	Windows 10	43.10.2.11.3	43.10.2.11
	Windows 11		
	Windows server 2016		
	Windows server 2019		

Table 49. Tested environment—Cisco Webex Meetings (continued)

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
	Windows server 2022 (Not tested)		

Table 50. Tested environment—Cisco Webex Meetings

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2209	Windows 10	43.10.2.11.3	43.10.2.11
	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 51. 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

Table 51. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	DellUSB Wired Optical Mouse - MS116	Supported	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported
	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	Supported	Supported	Not Available	Not Available

Table 51. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	(Single Link) - DANARBC084 - DANARBC084				
	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

Table 51. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	E2016H	Supported	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported	Supported
	E2216H	Not Available	Supported	Supported	Supported
	E2216Hv (China only)	Not Available	Not Available	Not Available	Supported
	E2218HN	Supported	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported	Supported
	E2318H	Supported	Supported	Supported	Supported
	E2318HN	Not Available	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported	Supported
	E2420HS	Not Available	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported	Supported
	E2720HS	Not Available	Supported	Supported	Supported
	P2016	Not Available	Supported	Not Available	Not Available
	P1917S	Supported	Supported	Not Available	Not Available
	P2017H	Supported	Not Available	Not Available	Not Available
	P2018H	Not Available	Not Available	Not Available	Supported
	P2217	Supported	Supported	Not Available	Not Available
	P2217H	Supported	Supported	Not Available	Not Available
	P2219H	Supported	Supported	Not Available	Supported
	P2219HC	Supported	Supported	Not Available	Supported
	P2317H	Supported	Supported	Not Available	Not Available
	P2319H	Not Available	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Supported	Not Available
	P2417H	Supported	Supported	Not Available	Not Available
	P2418D	Supported	Not Available	Not Available	Not Available
	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

Table 51. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

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

Table 51. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	USB - English - US - black - TAA Compliant - JK-A0104EU				
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 52. 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 52. 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 52. 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 +/û RW Drive - DW316 - DW316 - Agate - DW316
	Apricorn 1TB Aegis Padlock 256-bit AES Encrypted Hard Drive
	Western Digital My Passport Ultra 1TB , Black - WDBYNN0010BBK-WESN - WDBYNN0010BBK-WESN
Camera	Logitech BRIO 4K Ultra HD Webcam - 960-001105 - 960-001105
	Logitech C525 HD Webcam - 960-000715 - 960-000715
	Logitech C930e HD Webcam - 960-000971 - 960-000971
	Dell Pro Webcam - Falcon - WB5023
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

Supported ecosystem peripherals for Latitude 3420

Table 53. Supported ecosystem peripherals for Latitude 3420

Product Category	Peripherals
Displays	Dell 24 Monitor E2420HS - E2420HS
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W **NOTE:** Bluetooth connection is not supported.
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
Audio Devices	Dell Pro Stereo Headset - UC150 - UC150 - Lemmy - UC150
Docking 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 54. 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 55. 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 56. 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 Latitude 5450

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

Table 57. Supported ecosystem peripherals for Latitude 5450

Product Category	Peripherals
Monitors	Dell 27 USB-C HUB Monitor - P2723DE
	Dell Collaboration 24 Monitor - C2423H
Input Devices	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
Audio/Video	Dell Speakerphone - Mozart - SP3022
	Dell Pro Webcam - Falcon - WB5023
Docking station	Dell Thunderbolt 4 Dock - WD22TB4 - Salomon TBT MLK - WD22TB4
Cables, Dongles, Adapters	Dell 6-in-1 USB-C Multiport Adapter - DA305
	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 58. 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 59. 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 60. Third-party supported peripherals

Product Category	Peripherals
Audio Devices	Jabra GN2000
	Jabra PRO 9450

Table 60. 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 60. Third-party supported peripherals (continued)

Product Category	Peripherals
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 60. 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
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 61. 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 61. 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)
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 Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported
ID Prime MD v 4.3.5	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authenticatio n Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authenticatio n 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 Authenticatio n Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported

Table 61. 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. (Integrated Latitude 5450 reader is not supported)	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 and Known issues

Fixed issues

Table 62. Fixed issues

Issue ID	Description
DTOS-24310	Wake-on-LAN does not work in certain scenarios in ThinOS 9.

Table 62. Fixed issues (continued)

Issue ID	Description
DTOS-23965	The time that is displayed in the client shifts around five s per day.
DTOS-23814	Ctrl+Alt +Del + Win L key combination does not work as expected when configured locally.
DTOS-23314	The desko scanner does not work in AVD sessions.
DTOS-23014	A blank window is displayed for the captive portal when attempting to connect to a wireless network.
DTOS-23011	On Wyse 5070 computers with ThinOS 2311, the screen saver stops working when a legal notice is set.
DTOS-22919	In ThinOS 2311, the RDP session stops responding when a window is resized over a screen border.
DTOS-22886	On OptiPlex 3000 computers with ThinOS 2308, pressing the period key displays a comma instead in Azure sessions with Brazilian keyboard.
DTOS-22843	The Citrix domain value does not work when using the keyboard to cycle through the domain list.
DTOS-22841	The idle timer does not work when Nuance Power Mic 4 is connected.
DTOS-22609	On OptiPlex 3000 computers with ThinOS, the upgrade causes the group to change to selection group.
DTOS-22600	The RDP credential prompt appears in the second monitor.
DTOS-22451	The SCEP certificate automatic renewal fails in Wyse Management Suite Pro.
DTOS-22349	Wyse 5470 touchpad stops working.
DTOS-22224	Request for shutdown option is displayed in the ThinOS Login screen.
DTOS-22129	Keyboard 10 key not working at ThinOS Login Screen
DTOS-22019	Issues with Horizon SDK 2306.8.10.0.21964631.6 package version with SAML authentication
DTOS-21900	ABB 800xa 24/7 RDP usage led to long delays, latency, and video issues.
DTOS-21899	Delayed update for computers in a Wyse Management Suite group.
DTOS-21783	Unable to use the middle scroll wheel button of the Dell MS116 mouse in VDI sessions.
DTOS-21737	Dell Speakerphone - SP3022 mute function does not work consistently in Zoom sessions.
DTOS-21470	OptiPlex 3000 computers had performance and computer not responding issues in RDP sessions.
DTOS-21015	On Wyse 3040 computers, after SmartCard was mapped the computer stopped responding and exited on signal 11 in AVD (RDSH) sessions.
DTOS-20349	In OptiPlex 3000 computers with ThinOS 2306 and AVD package version 2.1.2164, some AVD sessions stopped responding.

Table 62. Fixed issues (continued)

Issue ID	Description
DTOS-20016	Keyboard audio keys do not work in unified applications in AVD sessions.
DTOS-19194	Smart card mapping does not work.
DTOS-18344	After the Wyse 5470 All-in-One is in an idle state overnight, a black screen is displayed.
DTOS-23938	Audio volume is observed at a lower volume until the audio menu in ThinOS is opened.
DTOS-23209	After upgrading to the latest ThinOS 2303 version, a VMware disk error message is displayed.
DTOS-21788	Nitgen Biometric card reader shows dual thumbprint in VDI sessions in ThinOS 9.
DTOS-23324	In ThinOS 2311, some devices have a smaller home partition after restarting the device.
DTOS-24626	Weston signal 11 issue in ThinOS 2311.
DTOS-20017	In OptiPlex computers with ThinOS 2303 and 2306, the USB devices lose connection.
DTOS-24670	A Black screen is displayed, and the device stops responding with a Weston Signal 11 error on Wyse OptiPlex 3000 Thin Client.
DTOS-23424	WPA Enterprise credentials are displayed on booting.

Known Issues

Table 63. Known Issues

Key	Summary	Workaround
DTOS-23132	Incorrect resolution after reconnecting the second monitor.	Reconnect the first monitor and do not reconnect the second monitor.
DTOS-23261	After creating an RDP connection, no error message is displayed when clicking **Connect**.	Give a valid IP to connect to RDP.
DTOS-23162	When restarting the thin client with WyreStrom Focus 210 USB Camera connected, the thin client stops responding for some time.	Remove the camera and restart the thin client.
DTOS-23169	The Bluetooth tab is disabled when rebooting the client with WyreStorm FOCUS 210 USB camera.	Remove the camera and restart the thin client.
DTOS-23888	Dell Premier ANC Wireless Headset - WL7022 has audio issues in VDI sessions.	Not available.
DTOS-23949	When the client is connected to Dell WD19 dock, ENET1 speed is set to 100FX, and you hot plug the network cable on Dell WD19, the network port on WD19 cannot be detected.	Hot plug Dell WD19 and do not hot plug the network cable.
DTOS-23530	When the Dell Wired Headset - WH3024 is mapped in session, the audio volume range does not work properly. For example, when you try to increase	Adjust volume in the graphical UI.

Table 63. Known Issues (continued)

Key	Summary	Workaround
	volume in the session, the audio volume does not increase.	
DTOS-22936	Jabra Elite 3 has disconnection and auto connection delays.	Not available.
DTOS-24584	Jabra PanaCast camera does not work during Teams video calls in the Blast session.	Use theUSB 2.0 port.
DTOS-22780	The camera in ThinOS is not detected in the WSP desktop.	Not available.
DTOS-23128	Packages download in service mode.	Not available.
DTOS-23869	The Windows taskbar remains on theThinOS taskbar when connecting or disconnecting the Citrix VDI desktop.	Sign off from the broker and log in again.
DTOS-24081	After waking up from sleep mode, the keyboard does not automatically connect.	Press any key on the keyboard.
DTOS-22692	The minimize and close button icons are not shown in the upper-right corner of the Amazon WorkSpaces page.	Not available.
DTOS-23807	The integrated camera on Dell 34 Curved Video Conferencing Monitor - P3424WEB does not work.	Use the USB 2.0 port on the client.
DTOS-23319	The webcam on Dell 24 Video Conferencing Monitor - P2424HEB does not work.	Use the USB 2.0 port on the client.
DTOS-21319	The Teams transfer window appears behind the video frame with the VMware Client SDK package installed.	Not available.
DTOS-21731	Switching off Jabra panacast 20 cameras causes the client to stop responding after the first attempt.	Plug out and plug in the device.
DTOS-22261	After connecting the uplink cable to Latitude 5440, the client cannot increase or decrease the volume using the Dell C2423H Monitor touch button when connected to two monitors.	Do not connect the uplink cable for two monitors.

4

Resources and support

Accessing documents using the product search

1. Go to Support | Dell.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, **`OptiPlex 7410 All-In-One`** or **`Latitude 3440 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 Support | Dell.
2. Click **Browse all products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **OptiPlex Thin Client**.
6. Click **OptiPlex 7410 All-In-One** or **Latitude 3440 Client** .
7. Click **Select this Product**.
8. Click **Documentation**.

5

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 Dell 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.