Dell ThinOS 9.x 2402, 2405, 2408 and 2411

Release Notes

January 2025
Rev. A12

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

ThinOS Recovery Firmware 2411.004

Release details

Release date

January 2025

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 Recovery Firmware version 2411.004

Package information

ThinOS_Recovery_Firmware_2411.004.pkg

Supported platform

Table 1. Supported platform

Supported platform
Wyse 5070 Thin Client
Wyse 5470 All-in-One Thin Client
Wyse 5470 Mobile Thin Client
Dell OptiPlex 3000 Thin Client
Dell Latitude 3420
Dell OptiPlex 5400 All-in-One
Dell Latitude 3440
Dell Latitude 5440
Dell Latitude 5450
Dell OptiPlex AIO 7410
Dell OptiPlex AIO 7420

Supported ThinOS versions

Table 2. Supported ThinOS versions

Supported ThinOS versions
ThinOS 2411 (9.5.4070)

Upload and publish the ThinOS recovery firmware package

Prerequisites

- Ensure that you are running ThinOS 2411 (9.5.4070) on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.

Steps

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

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

6. Click **Browse** and select `ThinOS_Recovery_Firmware_2411.004.pkg` to upload.

   ⓘ **NOTE:** Under the **Other** category, ensure that the switch option of **Other** is set to **INSTALL**.

7. Click to expand the **Other** dropdown list and select the uploaded package.
8. Click **Save & Publish**.
   The thin client downloads the package, installs it, and then restarts.

What's new

- When the ThinOS client storage size is less than 32 GB, nothing happens.
- When the ThinOS client has a storage size of 32 GB or larger, pressing **F12** and selecting **Dell ThinOS Recovery** in the boot menu causes the client to format its disk, and reinstall the ThinOS 2411 9.5.4070 OS firmware. This process does not preserve any preinstalled applications.

3

ThinOS 24.12.002 Hotfix

Release details

Release date

January 2025

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 24.12.002

Previous version

ThinOS 2411 (9.5.4070)

Package information

ThinOS_Hotfix_24.12.002.5.pkg

Supported Platforms

Table 3. Supported platforms for ThinOS Hotfix 24.06.001

Supported platforms
Wyse 5070 Thin Client
Wyse 5470 All-in-One Thin Client
Wyse 5470 Mobile Thin Client
Dell OptiPlex 3000 Thin Client
Dell Latitude 3420
Dell OptiPlex 5400 All-in-One
Dell Latitude 3440
Dell Latitude 5440
Dell Latitude 5450
Dell OptiPlex AIO 7410
Dell OptiPlex AIO 7420

Supported ThinOS versions

Table 4. Supported ThinOS versions

Supported ThinOS versions
ThinOS 2411 (9.5.4070)

Upload and publish the ThinOS Hotfix package through Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 2411 (9.5.4070) on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.

Steps

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

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

6. Click **Browse** and select the ThinOS Hotfix package to upload.
7. Ensure the switch option of **Hotfix** is set to **Install** under the category **Dell**.
8. Click to expand the **Hotfix** dropdown list, and select the uploaded package.
9. Click **Save & Publish**.
   The thin client downloads the package, installs it, and then restarts.

What's new

Table 5. What's new in ThinOS Hotfix Patch 24.12.002

Issue	Root cause analysis	Fix details
DTOS-30398—Certificate invalid error after updating the firmware and packages to ThinOS 2411.	Error messages appear when a trusted server's certificate verification fails during a Horizon login, even if the server is trusted.	The issue is fixed with this release.
DTOS-30225—Unexpected behavior when roaming with virtual apps.	Citrix session auto launch does not exclude the session from the ignore list in version 2411REL.	The issue is fixed with this release. Ignore the session auto launch if the session is in the ignore list.

Known Issues

The Horizon Server prefix may display as red, despite a verified and successfully validated certificate by the ThinOS Horizon Client. This issue is limited to the graphical user interface (GUI) and does not affect the functionality of the system, which remains unaffected.

4

ThinOS 2411

Release details

Release date

November 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 2411 (9.5.4070)

Previous version

ThinOS 2408 (9.5.3102)

Firmware upgrade

The following firmware upgrade scenarios are supported:

9.1.3129 or later versions > **ThinOS 2411 (9.5.4070)**

ⓘ **NOTE:**

If the current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2411. You must upgrade to ThinOS 9.1.3129 before upgrading to the latest version of ThinOS 9.x.

To downgrade ThinOS 2411 to a version earlier than 9.1.3129, use the ThinOS Merlin image.

For more information, see the *Dell ThinOS 2402, 2405, 2408 and 2411 Migration Guide* at Support | Dell. For the steps to access documents, see Resources and support.

Important notes

- ThinOS 2411 includes an updated Chrome package that provides the latest security enhancements. For Virtual Desktop Infrastructure (VDI) use cases and general browser use cases, ensure that the Chrome package is updated to the latest version in private distribution. To access the new version of the Chrome package on ThinOS, contact Dell sales or Support | Dell.
- Ensure that the following conditions are met in your OneSign environment before using the Imprivata PIE function:
  - Install the Imprivata ProveID embedded (PIE) agent on the Imprivata appliance.
  - Confirm that the Imprivata ProveID embedded (PIE) agent version is 23.3 or greater.
- Download the latest Imprivata server and PIE agent for ThinOS 2411 from the Imprivata platform. For the latest PIE package deployment, contact Imprivata directly for assistance.

- To further improve the security of ThinOS devices, from 2311, 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**. From 2408, ThinOS is updated to follow the **WMS Security Policy** > **TLS Security Level** (default = 1). If your network environment requires a legacy OpenSSL version, you must change the TLS security level to 0, when updating to 2408 or later version. Otherwise, the device can lose its network. Legacy OpenSSL versions are not supported on future ThinOS versions. If a Legacy OpenSSL version is required, update your environment.
- From ThinOS 2411, the `VMware Horizon Session SDK` package is no longer supported. It is recommended to upgrade ThinOS clients in the environment to the `VMware Horizon Client SDK` package to avoid issues.
- Dell aims to equip ThinOS with the broadest range of virtual computing Broker agent, and protocol capabilities. To periodically update to meet your needs.

From 2024-11-02, `Teradici PCoIP` package and **Teradici PCoIP license entitlement** are no longer included on newly manufactured ThinOS 2408 devices. The following issues are expected:

- Attaching to VMware environments is not impacted. You can continue to use the `VMware Horizon Client SDK` package to attach to VMware Horizon Servers using Blast, PCoIP, or Remote Desktop protocols.
- Attaching to Amazon WorkSpaces environments are limited to WorkSpace Streaming Protocol (WSP). You must use Wyse Management Suite Pro to download the `Teradici PCoIP` package and allocate a ThinOS Activation License if you are using PCoIP protocol connections to Amazon WorkSpace.
- Attaching to Teradici Cloud Access Software (HP Anywhere) and PCoIP Host Card environments are discontinued. You must use Wyse Management Suite Pro to download the `Teradici PCoIP` package and allocate a ThinOS Activation License.
- The ThinOS Activation License is a dual-purpose license that is managed by WMS Pro. It is used for:
  - Enabling virtual connections on devices that are converted from an alternative operating system to ThinOS.
  - Enabling PCoIP entitlement on ThinOS devices, including ThinOS 8.6 devices without PCoIP and all ThinOS client devices manufactured on or after 2024-11-02. It is done when the ThinOS policy managed by WMS is enabled using **Services** > **WDA Settings** > **Enable PCoIP Activation License**.
- To improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are removed in the future release. Some TLS ciphers are not secure and are subject to change in the future release.

Table 6. TLS Cipher list

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Disabled by default in the future release
ECDHE-RSA-AES256-SHA384	Disabled by default in the future release
ECDHE-RSA-AES128-SHA	Removed in future release
ECDHE-RSA-AES256-SHA	Removed in future release
DHE-RSA-AES128-GCM-SHA256	Removed in future release
DHE-RSA-AES256-GCM-SHA384	Removed in future release
DHE-RSA-AES128-SHA256	Removed in future release
DHE-RSA-AES256-SHA256	Removed in future release
DHE-RSA-AES128-SHA	Removed in future release
DHE-RSA-AES256-SHA	Removed in future release
AES128-SHA256	Removed in ThinOS 2303
AES256-SHA256	Removed in ThinOS 2303
AES128-SHA	Removed in ThinOS 2303
AES256-SHA	Removed in ThinOS 2303
AES128-GCM-SHA256	Removed in ThinOS 2303
AES256-GCM-SHA384	Removed in ThinOS 2303
ECDHE-ECDSA-AES128-GCM-SHA256	Secure

Table 6. TLS Cipher list (continued)

Ciphers	Security Status
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Disabled by default in the future release
ECDHE-ECDSA-AES256-SHA384	Disabled by default in the future release
ECDHE-ECDSA-AES128-SHA	Removed in future release
ECDHE-ECDSA-AES256-SHA	Removed in future release
DHE-PSK-AES128-GCM-SHA256	Removed in future release
DHE-PSK-AES256-GCM-SHA256	Removed in future release
DHE-PSK-AES128-CBC-SHA256	Removed in future release
DHE-PSK-AES256-CBC-SHA384	Removed in future release
DHE-PSK-AES128-CBC-SHA	Removed in future release
DHE-PSK-AES256-CBC-SHA	Removed in future release
ECDHE-PSK-AES128-CBC-SHA	Removed in future release
ECDHE-PSK-AES256-CBC-SHA	Removed in future release
ECDHE-PSK-AES128-CBC-SHA256	Disabled by default in the future release
ECDHE-PSK-AES256-CBC-SHA384	Disabled by default in the future release
PSK-AES128-GCM-SHA256	Removed in future release
PSK-AES256-GCM-SHA384	Removed in future release
PSK-AES128-CBC-SHA	Removed in future release
PSK-AES256-CBC-SHA	Removed in future release
PSK-AES128-CBC-SHA256	Removed in future release
PSK-AES256-CBC-SHA384	Removed in future release
RSA-PSK-AES128-GCM-SHA256	Removed in future release
RSA-PSK-AES256-GCM-SHA384	Removed in future release
RSA-PSK-AES128-CBC-SHA	Removed in future release
RSA-PSK-AES256-CBC-SHA	Removed in future release
RSA-PSK-AES128-CBC-SHA256	Removed in future release
RSA-PSK-AES256-CBC-SHA384	Removed in future release
ECDHE-ECDSA-CHACHA20-POLY1305	Removed in future release
ECDHE-RSA-CHACHA20-POLY1305	Removed in future release
DHE-RSA-CHACHA20-POLY1305	Removed in future release
RSA-PSK-CHACHA20-POLY1305	Removed in future release
DHE-PSK-CHACHA20-POLY1305	Removed in future release
ECDHE-PSK-CHACHA20-POLY1305	Removed in future release
PSK-CHACHA20-POLY1305	Removed in future release
SRP-RSA-AES-256-CBC-SHA	Removed in future release
SRP-AES-256-CBC-SHA	Removed in future release
SRP-RSA-AES-128-CBC-SHA	Removed in future release

Table 6. TLS Cipher list (continued)

Ciphers	Security Status
SRP-AES-128-CBC-SHA	Removed in future release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

- There are chances that after the upgrade, the device displays a black screen. Reboot the device to boot it up correctly.
- From ThinOS 2303, the firmware update sequence is changed to **BIOS** > **OS** > **Application**.
- From ThinOS 2303, if the thin client is registered in Wyse Management Suite group 1 and you set the Wyse Management Suite group 2 token in group 1 policy, a dialog box is displayed to change the group. Click **Cancel** to change to group 2 immediately. Click **Restart Now** or wait for the 60-second countdown to finish and then reboot to change to group 2.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you 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 published in the same group, the thin client does not download it.
  - 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 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 (WMS), 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 ThinOS, 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 2411 (9.5.4070) 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 2411 (9.5.4070) 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:** The upgrade can fail sometimes when the event log is fails to install. You can reboot the device and upgrade again.

   ⓘ **NOTE:** Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2411. Ensure to install the latest application packages. Microsoft AVD packages released prior to version 2311, along with the Zoom AVD, Zoom Citrix, and Zoom Horizon packages, are automatically removed and cannot be installed again.

Convert Ubuntu with DCA to ThinOS 2411

Prerequisites

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

Table 7. 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, 2405, 2408 and 2411 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.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS.
- 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, 2405, 2408 and 2411 Migration Guide* at Support | Dell.
- Ensure you have downloaded the Ubuntu to ThinOS 2411 conversion image.
- Extract the Ubuntu to ThinOS 2411 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.3-dtos3-amd64_signed.tar.gz` and ThinOS image `ThinOS_2411_9.5.4070.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_2411_9.5.4070.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:

    - You must connect the power adapter to Ubuntu devices; otherwise, the conversion fails.
    - The ThinOS activation license number for Wyse Management Suite must be greater than the Ubuntu device number. If it is not, you cannot create an advanced policy for conversion.
    - After conversion, ThinOS returns to its factory default status. You must register ThinOS to Wyse Management Suite manually or through DHCP/DNS discovery.
    - After registering the converted ThinOS devices to Wyse Management Suite, the ThinOS activation license will be consumed.
    - If the conversion fails, resolve the issue based on the error log below. Then reschedule the job from **Jobs** > **Schedule APP Policy**. Dell recommends installing the ThinOS ISO image if the conversion fails.

    If the `/usr/dtos` folder exists on the Ubuntu device, use the command **cat /var/log/dtos_dca_installer.log** to retrieve the error log. You can also obtain error messages from the **WMS** job details. Although the error messages may differ, the resolutions remain the same.

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

Table 8. 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 the 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 2411, it is recommended to install the latest application packages mentioned in the below table.

Table 9. ThinOS application package details

ThinOS application package details
Amazon_WorkSpaces_Client_ 24.6.5072.4.pkg
Cisco_Jabber_15.0.0.309289.6.pkg
Cisco_Webex_Meetings_VDI_44.10.1.3.4.pkg
Cisco_Webex_App_VDI_44.10.0.30906.5.pkg
Citrix_Workspace_App_24.8.0.98.67.pkg
Common_Printing_2.0.0.5.pkg
ControlUp_VDI_Agent_2.2.30.pkg
eG_VM_Agent_7.2.10.12.pkg
EPOS_Connect_7.8.1.3.pkg
HID_Fingerprint_Reader_210217.24.pkg
Identity_Automation_QwickAccess_2.1.1.13.pkg
Imprivata_PIE_23.3.0.715913.52.pkg
Jabra_8.5.8.7.pkg
Lakeside_Virtual_Agent_99.0.0.173.12.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.7.0.7.1.pkg
Microsoft_AVD_3.0.2442.pkg
RingCentral_App_VMware_Plugin_24.3.31.2.pkg
Teradici_PCoIP_24.07.3.7.pkg
ThinOS_Telemetry_Dashboard_1.1.0.6.pkg
UXM_Endpoint_Agent_2024.07.11.6.pkg
VMware_Horizon_ClientSDK_2406.8.13.0.33.pkg
Zoom_Universal_6.1.10.25260.3.pkg
ChromeBrowser_130.0.6723.116.1.pkg

Important notes

- After upgrading to ThinOS 2411, 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 2411 includes an updated Chrome package that incorporates the latest security updates. For VDI and browser use cases, ensure you update the Chrome package to the latest version in your private distribution. For access to the new version of the Chrome package on ThinOS, please contact Dell sales or support.

ThinOS build

- ThinOS 9.1.3129 or later versions to ThinOS 2411 (9.5.4070)—`ThinOS_2411_9.5.4070.pkg`
- Ubuntu to ThinOS 2411 conversion build—`ThinOS_2411_9.5.4070_Ubuntu_Conversion.zip`

Tested BIOS versions and BIOS packages

The following table contains the tested BIOS versions and BIOS packages for ThinOS 2411.

Table 10. Tested BIOS versions and BIOS packages

Supported platform	Tested BIOS version	New BIOS package
Wyse 5070 Thin Client	1.33.0	bios-5070_1.33.0.pkg
Wyse 5470 All-in-One Thin Client	1.28.0	bios-5470AIO_1.28.0.pkg
Wyse 5470 Mobile Thin Client	1.27.0	bios-5470_1.27.0.pkg
Dell OptiPlex 3000 Thin Client	1.22.1	bios-Op3000TC_1.22.1.pkg
Dell Latitude 3420	1.36.0	N/A
Dell OptiPlex 5400 All-in-One	1.1.43	bios-OptiPlex5400AIO_1.1.43.pkg
Dell Latitude 3440	1.17.0	bios-Latitude3440_1.17.0.pkg
Dell Latitude 5440	1.18.1	bios-Latitude5440_1.18.1.pkg
Dell Latitude 5450	1.8.0	bios-Latitude5450_1.8.0.pkg
Dell OptiPlex AIO 7410	1.19.0	bios-OptiPlexAIO7410_1.19.0.pkg
Dell OptiPlex AIO 7420	1.9.0	bios-OptiPlexAIO7420_1.9.0.pkg

Wyse Management Suite and Configuration UI packages

- Wyse Management Suite version 4.4
- Configuration UI package 1.10.460

NOTE:

- Use Wyse Management Suite 4.4 or later versions server for the new Wyse Management Suite ThinOS 9.x Policy features.
- Configuration UI package 1.10.460 must be installed separately with the Wyse Management Suite 4.4 server.

Feature Matrices

Citrix Workspace App feature matrix

Table 11. Citrix Workspace App feature matrix

Feature		ThinOS 2411 with CWA 2408	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

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	App Personalization service	Not Supported	Not Supported
Workspace Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	Not Supported	Not Supported
	Citrix Auto updates	Not Supported	Not Supported
	Client App Management	Not Supported	Not Supported
User Interface	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.
	HDX adaptive throughput	Not Supported	Not Supported
	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.

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	File open in Citrix Workspace app	Not Supported	Not supported. No local file explorer on ThinOS.
	Location Based Services (Location available via API-description)	Not Supported	Not Supported
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 (x64 only)	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, 2405, and 2408 Administrator's Guide* at Support | Dell.

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	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, 2405, and 2408 Administrator's Guide* at Support | Dell.
	Unified Communication Cisco Webex Meetings Optimization	Supported	Dell Technologies recommends to wait for 10 seconds 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, 2405, and 2408 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, 2405, and 2408 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, 2405,*

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
			and 2408 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.
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	Not supported	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, 2405, and 2408 Administrator's Guide* atSupport | Dell.

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	Not supported	Not supported
Authentication	Federated Authentication (SAML/Azure AD)	Supported	There are no limitations in this release.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Supported	There are no limitations in this release.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	Not supported	Not supported
	User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	Not supported	Not supported
	ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor authentications are not qualified.
	ADC Full VPN	Not supported	Not supported
	ADC Native OTP	Supported	There are no limitations in this release.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	PingID SAML MFA	Supported	There are no limitations in this release.
	Single Sign on to Citrix Mobile apps	Not supported	Not supported

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not qualified	Not qualified
	Citrix cloud + Azure Active Directory	Not qualified	Not qualified
	Citrix cloud + Active Directory + Token	Not qualified	Not qualified
	Citrix cloud + Citrix Gateway	Not qualified	Not qualified
	Citrix cloud + Okta	Not qualified	Not qualified
	Citrix cloud + SAML 2.0	Not qualified	Not qualified
	Netscaler load balance	Not qualified	Not qualified
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.

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	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	Enhanced virtual desktop screen resizing experience	Supported	There are no limitations in this release.
	Accessibility support for enhanced Desktop Viewer toolbar	Supported	There are no limitations in this release.
	Performance optimization for graphics	Supported	There are no limitations in this release.
	Endpoint Analysis support for multi factor (nFactor) authentication	Not Supported	Not Supported
	Multiple webcam resolutions support	Supported	There are no limitations in this release.
	Improved loading experience for shared user mode	Not Supported	Not Supported
	Support for Optimized Microsoft Teams on ARM64 devices	Not Supported	Not Supported
	Version upgrade for Chromium Embedded Framework 128	Supported	There are no limitations in this release.
	App protection Configure allow list for the apps which use LD_Preload functionalities	Not Supported	Not Supported
	Provision to manage multiple proxy servers	Not Supported	Not Supported
	Support for Cryptography Next Generation smartcards	Not Supported	Not Supported
	Manage settings for user groups using configuration profile	Not Supported	Not Supported
	NFC support for FIDO2 Authentication	Not Supported	Not Supported
	Enhanced Unified Communications SDK API	Not Supported	Not Supported
	Support for WebHID API in UCSDK	Not Supported	Not Supported
	Support integrated windows authentication for browser content redirection	Not Supported	Not Supported
	Support for H.264 and H.265 hardware decoding	Not Supported	Not Supported
	Clipboard Support for HTML formatted text	Not Supported	Not Supported
	Enhanced system logs for browser content redirection	Not Supported	Not Supported

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	Support for authentication using FIDO2 when connecting to cloud stores	Not Supported	Not Supported
	Composite USB device redirection using DDC policies	Not Supported	Not Supported
	Support for multiple passkeys in HDX session	Not Supported	Not Supported
	PDF Universal Printing	Not Supported	Not Supported
	HDX direct	Not Supported	Not Supported
	AI based noise suppression	Not Supported	Not Supported
	Synchronize multiple keyboards at session start	Not Supported	Not Supported
	Enhancement for composite USB auto-redirection	Not Supported	Not Supported
	Loss tolerant mode for audio	Not Qualified	Not Qualified
	Enable Packet Loss Concealment to improve audio performance	Not Supported	Not Supported
	Version upgrade for Chromium Embedded Framework	Not Supported	Not Supported
	Enhancement to multiple monitors	Not Supported	Not Supported
	Support for GTK3	Supported	There are no limitations in this release.
	Availability of Credential Insertion SDK for cloud stores	Not Supported	Not Supported
	Improved UI for error messages	Not Supported	Not Supported
	Send feedback on Citrix Workspace app	Not Supported	Not Supported
	Introduction of a new command in Storebrowse	Not Supported	Not Supported
	Configure UDP port range for Microsoft Teams optimization	Not Supported	Not Supported
	Enhanced Desktop Viewer toolbar	Supported	There are no limitations in this release.
	Customize toolbar	Supported	There are no limitations in this release.
	Sustainability initiative from Citrix Workspace app	Not Supported	Not Supported
	Include system audio while screen sharing	Not Supported	Not Supported

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	App Protection compatibility with HDX optimization for Microsoft Teams	Supported	There are no limitations in this release.
	Fast smart card	Not Supported	Not Supported
	Support for Audio volume synchronization	Supported	There are no limitations in this release.
	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 MJPEG webcams	Not Supported	Not Supported
	Supports system certificate paths for SSL connection	Not Supported	Not Supported
	Enhanced virtual channel SDK	Not Supported	Not Supported
	Support for keyboard shortcut to switch between Full-screen and Window mode	Not Supported	Not Supported
	Policy tampering detection	Not Supported	Not Supported
	Webcam redirection and service continuity support for ARM64 devices	Not Supported	Not Supported
	Enable Packet Loss Concealment to improve audio performance	Not Supported	Not Supported
	Multi-touch support	Not Supported	Not Supported
	HTTPS protocol support for proxy server	Not Supported	Not Supported
	Support for IPv6 UDT with DTLS	Not Supported	Not Supported

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	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, 2405, and 2408 Administrator's Guide* at Support | Dell
	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

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	Microsoft Teams enhancements-Limiting video resolutions	Not Supported	Not Supported
	Microsoft Teams enhancements-Configuring a preferred network interface	Not Supported	Not Supported
	Inactivity Timeout for Citrix Workspace app	Not Supported	Not Supported
	Screen pinning in custom web stores	Not Supported	Not Supported
	Support for 32-bit cursor	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit still exists in Citrix HDX Pro 3D desktop. This issue is also reproduced in **Citrix Workspace App** Linux binary.
	Addition of client-side jitter buffer mechanism	Not Supported	Not Supported
	Background blurring and replacement for Citrix Optimized Teams	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported
	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

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	Provision to disable LaunchDarkly service	Not Supported	Not Supported
	Email-based auto-discovery of store	Not Supported	Not Supported
	Persistent login	Not Supported	Not Supported
	Authentication enhancement for Storebrowse	Not Supported	Not Supported
	Support for EDT IPv6	Not Supported	Not Supported
	Support for TLS protocol version 1.3	Not Supported	Not Supported
	Custom web stores	Not Supported	Not Supported
	Authentication enhancement experimental feature	Not Supported	Not Supported
	Keyboard layout synchronization enhancement	Not Supported	Not Supported
	Multi-window chat and meetings for Microsoft Teams	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
	Request control in Microsoft Teams	Supported	Users on ThinOS client cannot give control to other users. In other words, after the user on the ThinOS client starts sharing screen or content, the option Give control is present in the sharing toolbar, but it does not work when you give control to 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, 2405, and 2408 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.

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	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 (Public Technical Preview)	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	Supported	Refer to the limitations in ThinOS 2411 release note.
	User Interface enhancement	Not Supported	Not Supported
	Pinning multi-monitor screen layout	Not Supported	Not Supported
	Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported
	Multiple audio	Supported	Multiple audio devices feature is not supported by Cisco JVDI. This is Cisco known limitation. To eliminate confusion or mistakes, multiple audio devices feature is dynamically disabled after JVDI package installed, and it is dynamically enabled after JVDI package is uninstalled. Only Citrix VDA 2308 and later versions support 12 audio devices. The previous VDA version still has the 8 audio devices limitation. This is Citrix limitation
	Citrix logging	Supported	There are no limitations in this release.
	Cryptographic update	Not Supported	Not Supported

Table 11. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2411 with CWA 2408	Limitations
	Transparent User Interface (TUI)	Not Supported	Not Supported
	GStreamer 1.x support experimental feature	Supported	There are no limitations in this release.
	App indicator icon	Not Supported	Not Supported
	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.
	Native mode	Supported	There are no limitations in this release.

NOTE: The features and product environments that are marked as not qualified are not tested by Dell Technologies and are found to be working with other users.

ThinOS AVD Client Feature Matrix

Table 12. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 2411
Service	Direct connection to Desktop via RDP	Supported
	Remote Desktop Services broker (Local)	Supported
	Windows Virtual Desktop (Azure)	Supported
	Windows 365	Supported
Session	Desktop	Supported
	Remote App (Integrated)	Supported
	Remote App (Immersive)	Supported
Input	Keyboard	Supported
	Mouse	Supported

Table 12. ThinOS AVD Client Feature Matrix (continued)

Category Supported	Features	ThinOS 2411
	Single Touch	Supported
Audio Visual	Audio in	Supported
	Audio out	Supported
	Camera	Supported
Storage	Folder / Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
Redirections	Printer	Supported
	SmartCard	Supported
	USB (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 play back	Supported
	Compression	Supported
	Optimize for low-speed link	Supported
Graphics (CODECs)	H.264 Hardware Acceleration	Supported
Unified Communications	Microsoft Teams Optimization	Supported
	Zoom Cloud Meeting Optimization	Supported
	Cisco Webex App Optimization	Supported
Authentication	TS Gateway	Supported
	NLA	Supported
	SmartCard	● Microsoft Remote Desktop: Only supports login broker. ● Azure Virtual Desktop: Supports login broker and Single Sign-On (SSO) for AVD sessions.
	FIDO2	Support for FIDO2 Authentication in Azure Virtual Desktop Broker agent
	Imprivata	Supported

VMware Horizon feature matrix

Table 13. VMware Horizon feature matrix

Category	Feature	Horizon Client SDK
Broker Connectivity	SSL certificate verification	Supported

Table 13. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
	Disclaimer dialog	Supported
	UAG compatibility	Supported
	Shortcuts from server	Not Supported
	Preinstall shortcuts from server	Not Supported
	File type association	Not Supported
	Phonehome	Supported
Broker Authentication	Password authentication	Supported
	SAML authentication	Supported
	FIDO2 Authentication	Supported
	Single sign on	Supported
	RSA authentication	Supported
	Integrated RSA SecurID token generator	Not Supported
	Radius - Cisco ACS	Supported
	Radius - SMS Passcode	Supported
	Radius - DUO	Supported
	Radius - OKTA	Supported
	Radius - Microsoft Network Policy	Supported
	Radius - Cisco Identity Services Engine	Supported
	Kiosk mode	Supported
	Remember credentials	Supported
	Log in as current user	Not Supported
	Nested log in as current user	Not Supported
	Log in as current user 1-way trust	Not Supported
	OS biometric authentication	Not Supported
	Windows Hello	Not Supported
	Unauthentication access	Supported
Smartcard	x.509 certificate authentication (Smart Card)	Supported
	CAC support	Supported
	.Net support	Supported
	PIV support	Supported
	Java support	Supported
	Purebred derived credentials	Not Supported
	Device Cert auth with UAG	Supported
Desktop Operations	Reset	Only supported with VDI
	Restart	Only supported with VDI
	Log off	Supported

Table 13. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported
	Multiple connections	Supported
	Multi-broker/multi-site redirection - Universal	Not Supported
	App launch on multiple end points	Supported
	Auto-retry 5+ minutes	Supported
	Blast network recovery	Supported
	Time zone synchronization	Supported
	Jumplist integration (Windows 7- Windows 10)	Not Supported
Client Customization	Command line options	Not Supported
	URI schema	Not Supported
	Launching multiple client instances using URI	Not Supported
	Preference file	Not Supported
	Parameter pass-through to RDSH apps	Not Supported
	Noninteractive mode	Not Supported
	GPO-based customization	Not Supported
Protocols supported	Blast Extreme	Supported
	H.264 - HW decode	Supported
	H.265 - HW decode	Supported
	Blast Codec	Supported
	JPEG/PNG	Supported
	Switch encoder	Supported
	BENIT	Supported
	Blast Extreme Adaptive Transportation	Supported
	RDP 8.x, 10.x	Supported
	PCoIP	Supported
Features/Extensions Monitors/Displays	Dynamic display resizing	Supported
	VDI windowed mode	Supported
	Remote app seamless window	Supported
	Multiple monitor support	Supported
	External monitor support for mobile	Not Supported
	Display pivot for mobile	Not Supported
	Number of displays supported	4
	Maximum resolution	3840x2160
	High DPI scaling	Not Supported
	DPI sync	Not Supported

Table 13. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
	Exclusive mode	Not Supported
	Multiple monitor selections	Supported
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported
	Relative mouse	Only supported with VDI
	External Mouse Support	Supported
	Local buffer text input box	Not Supported
	Keyboard Mapping	Supported
	International Keyboard Support	Supported
	Input Method local/remote switching	Not Supported
	IME Sync	Supported
Clipboard Services	Clipboard Text	Supported
	Clipboard Graphics	Not Supported
	Clipboard memory size configuration	Supported
	Clipboard File/Folder	Not Supported
	Drag and Drop Text	Not Supported
	Drag and Drop Image	Not Supported
	Drag and Drop File/Folder	Not Supported
Connection Management	IPv6 only network support	Supported
	PCoIP IP roaming	Supported
Optimized Device Redirection	Serial (COM) Port Redirection	Supported
	Client Drive Redirection/File Transfer	Not Supported
	Scanner (TWAIN/WIA) Redirection	Supported
	x.509 Certificate (Smart Card/Derived Credentials)	Supported
	Storage Drive Redirection	Not Supported
	Gyro Sensor Redirection	Not Supported
Real-Time Audio-Video	Audio input (microphone)	Supported
	Video input (webcam)	Supported
	Multiple webcams and microphones	Not Supported
	Multiple speakers	Not Supported
USB Redirection	USB redirection	Supported
	Policy: ConnectUSBOnInsert	Supported
	Policy: ConnectUSBOnStartup	Supported
	Connect/Disconnect UI	Not Supported
	USB device filtering (client side)	Supported
	Isochronous Device Support	Only supported with VDI
	Split device support	Supported

Table 13. VMware Horizon feature matrix (continued)

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

Table 13. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
Security	FIPS-140-2 Mode Support	Supported
	Imprivata Integration	Supported
	Opswat agent	Not Supported
	Opswat on-demand agent	Not Supported
	TLS 1.1/1.2	Supported
	Screenshot blocking	Not Supported
	Keylogger blocking	Not Supported
Session Collaboration	Session Collaboration	Supported
	Read-only Collaboration	Supported
Updates	Update notifications	Not Supported
	App Store update	Not Supported
Other	Smart Policies from DEM	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported
	Nested - basic connection	Supported
	DCT Per feature/component collection	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported
	Auth Method - RSA SecurID	Supported
	Auth Method - X.509 Certificate (Smart Card)	Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported
	Auth Method - RADIUS	Supported
	Auth Method - SAML - 3rd Party Identity Provider	Supported

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

Table 14. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix

Feature	ThinOS 2408
Client access restriction	Supported
USB redirection	Not supported
Audio input	Supported
Video input	Supported

Table 14. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix (continued)

Feature	ThinOS 2408
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
Smart card (CAC and PIV readers)	Supported
Certificate for access control	Supported
Encryption at rest	Supported
Client customization	Not supported
YubiKey support	Not supported
Monitor support	Supported (Dual Monitor with 3840x2160 resolution)

What's new

Citrix Workspace App updates

Citrix Workspace App (CWA) package version is updated to 24.8.0.98.67, and the package can install the Citrix Workspace App version 2408 on ThinOS. Citrix HDX RealTime Optimization Pack for Microsoft Skype® for Business (RTOP) within the Citrix Workspace app package 2408 is announced for deprecation. It will be removed in future ThinOS releases.

The following are the updates for Citrix Workspace App:

- Support for service continuity
- Support for audio volume synchronization
- Support for multiple webcam resolutions
- Support for enhanced desktop viewer toolbar
- Support for customization of the toolbar
- Support for keyboard shortcuts for enhanced desktop viewer toolbar
- Support for performance optimization for graphics
- Enhanced Virtual Desktop Screen Resizing Experience
- Enhance Samsung Smartphone with USB Redirection for transferring images

Support for service continuity

This section explains the support for Service Continuity in ThinOS 2411 and Citrix Workspace App 2408.

In **ThinOS 2411** and **Citrix Workspace App 2408**, service continuity is supported. Users can use this feature to access their DaaS applications and desktops during outages. The endpoint device must sustain a network connection to the resource location for this capability to be effective.

Users can access DaaS applications and desktops during outages that affect Citrix Cloud components or operate in public and private clouds. Connections can be made directly to the resource location or through the **Citrix Gateway Service**.

Service continuity uses Workspace connection leases that grant users access to applications and desktops during outages. These leases are long-lived authorization tokens that are securely cached on the endpoint device . When a user signs in to Citrix Workspace, lease files are stored in the user profile for each resource that is published to that user.

Importantly, service continuity allows users to access applications and desktops during an outage, even if they have never launched a particular app or desktop before. Workspace connection lease files are both signed and encrypted, ensuring that they are linked to the user and the specific endpoint device .

When service continuity is enabled, a Workspace connection lease allows users to access applications and desktops for seven days by default. Configuration options exist to extend this access period up to 30 days.

Service Continuity Requirements

- Enable the **Citrix Native mode** using the ThinOS Admin Policy Tool or Wyse Management Suite policy.
- Service continuity is only supported with Citrix Cloud when **Citrix Native mode** is enabled.
- Confirm that Service Continuity is enabled on the Citrix Cloud server side.

Limitations

- Service continuity cannot function if the user signs off from Citrix Cloud using ThinOS or if the endpoint device is restarted.
- Citrix session windows do not display in full screen when reconnecting after a Citrix Cloud server outage.
- Only one ICA session can reconnect after a Citrix Cloud server outage.

Service continuity cannot function if the user signs off from Citrix Cloud using ThinOS or if the endpoint device is restarted.

Support for audio volume synchronization

Audio volume synchronization between VDA and audio devices in ThinOS client.

From ThinOS 2411 and Citrix Workspace App 2408, the Citrix Workspace app supports audio volume synchronization between the VDA and your audio devices. You can adjust the volume using the VDA audio volume slider. The volume reflects the same level on both your device and the VDA. This feature is enabled by default.

To use this feature, ensure you have VDA version 2308 or later.

To disable audio volume synchronization, follow these steps:

1. Open the **Admin Policy Tool** or the **Wyse Management Suite policy settings**.
2. Go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
3. In the **Citrix INI Settings**, click **Add Row**.
4. From the **File** drop-down list, select **module.ini**.
5. From the **Operation** drop-down list, select **Add or Update**.
6. In the **Section** field, enter **ClientAudio**.
7. In the **Key** field, enter **EnableVolumeSync**.
8. In the **Value** field, enter **FALSE**.
9. Click **Save & Publish**.
10. Restart the session for the changes to take effect.

NOTE: Audio volume synchronization does not work when the Cisco Jabber package is installed.

Support for multiple webcam resolutions

High-definition webcam streaming support for all available client-side resolutions in the Citrix Workspace App.

In ThinOS 2411 and Citrix Workspace App 2408, the Citrix Workspace app supports high-definition webcam streaming for all available client-side resolutions. The application on VDA determines the best resolution to capture. If media type negotiation fails, HDX defaults to VGA resolution (640 x 480 resolution). This feature is enabled by default.

To disable this feature, follow these steps:

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

6. In the **Key** field, enter **HDXWebCamEnablePnp**.
7. In the **Value** field, enter **FALSE**.
8. Click **Save & Publish**.
9. Sign out or restart the device for the settings to take effect.

ⓘ **NOTE:** Multiple webcam Resolutions feature does not support the Camera Width, Camera Height, and Camera FPS settings in the Admin Policy Tool or Wyse Management Suite policy. Disable this feature to use the camera settings.

Support for enhanced desktop viewer toolbar

This section describes the enhanced Desktop Viewer toolbar in the Citrix Workspace app.

The enhanced toolbar includes the following options:

- **Show or hide toolbar**: Click this button to show or hide the Desktop Viewer toolbar.
- **Switch desktop**: Click this button to see the available open desktops. Switch to another desktop by clicking the wanted desktop. The selected desktop appears in the front.
- **Ctrl+Alt+Del**: Click this button to access the Ctrl+Alt+Del shortcut.
- **Devices**: Click this button to access the options in the Devices section.
- **Preferences**: Click this button to access the options in the Preferences section.
- **Minimize**: Click this button to minimize the virtual session.
- **Fullscreen** or **Restore**: Click the **Fullscreen** button to expand the desktop session to full screen. Click the **Restore** button to return to the previous window mode.
- **Disconnect / Sign out**: Click this button to sign out or disconnect from a virtual session.

You can float or rotate the toolbar across the screen as per your preference. By default, the new toolbar is available.

Limitation

Citrix Desktop Viewer toolbar position is always reset to the middle of the monitor.

Support for customization of the toolbar

This section describes how to customize the Citrix Workspace app toolbar.

Previously, you could completely disable the Desktop Viewer using Desktop Viewer Toolbar setting in Policy Tool or the Wyse Management Suite policy settings. However, you could not enable or disable specific options on the toolbar.

From ThinOS 2411 and Citrix Workspace App 2408, you can customize the Citrix Workspace app toolbar by adding or removing options.

To hide the Devices option on the toolbar, follow these steps:

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

Support for keyboard shortcuts for enhanced desktop viewer toolbar

This section explains how to use keyboard shortcuts to access the enhanced Desktop Viewer toolbar.

In ThinOS 2411 and Citrix Workspace App 2408, you can access the enhanced Desktop Viewer toolbar using the keyboard on your endpoint devices. This feature allows you to invoke the toolbar, navigate through options, and select required options using keyboard shortcuts.

Use the following keyboard shortcuts to access the toolbar:

- **Ctrl + Shift + t**: Show the toolbar and move focus to the first button.
- **Tab**: Move through the options in the forward direction.
- **Space**: Select a menu.
- **Up and Down arrow keys**: Move across submenus.
- **Enter**: Select a submenu.
- **Esc**: When focused on a submenu, exit the submenu. When focused on the toolbar, remove focus and exit keyboard shortcut mode.

The keyboard shortcuts are enabled by default.

To disable this feature, follow these steps:

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

Support for performance optimization for graphics

This section explains how to enable performance optimization for graphics when using multiple monitors.

Previously using multiple monitors, docking or undocking your primary endpoint machine from a docking station automatically extends the session to the monitors with the updated layout. When you start a session with multiple monitors, the session extends to those monitors as well. If you add or remove monitors, the session adapts to the newly available screens. This feature is disabled by default.

Enabling Performance Optimization

To enable this feature, follow these steps:

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

Using the Automatically Extend Desktop Session

In ThinOS 2411 and Citrix Workspace App 2408, a new UI option, the **Automatically extend desktop session to external monitors** checkbox, is available to enable or disable the monitor **plug and play** feature. By default, the **Automatically extend desktop session to external monitors** checkbox is not selected.

To select this option, follow these steps:

1. Click **Desktop viewer Preferences** > **General**.
2. Select the **Automatically extend desktop session to external monitors** checkbox.
3. Click **OK**. The change takes effect the next time you open the desktop session.

ⓘ **NOTE:** If you disable the feature through **wfclient.ini** per machine, the **Automatically extend desktop session to external monitors** checkbox is not visible.

Limitations

When you enable both the **Automatically extend desktop session to external monitors** and the virtual desktop screen resizing features, the Citrix desktop viewer toolbar does not work correctly.

To use the **Automatically extend desktop session to external monitors** feature, it is recommended to disable the **Virtual desktop screen resizing** feature.

Enhanced Virtual Desktop Screen Resizing Experience

This section describes the features that are related to virtual desktop screen resizing in the Citrix Workspace app.

In ThinOS 2411 and Citrix Workspace App 2408, the Citrix Workspace app ensures a smooth transition when resizing or stretching your virtual desktop screen. It also prevents black screens and flickers during the resizing process. This feature is enabled by default.

Disabling the Feature

To disable this feature, follow these steps:

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

Limitations

When you enable both the **Automatically extend desktop session to external monitors** and the virtual desktop screen resizing features, the Citrix desktop viewer toolbar does not work correctly.

To use the **Automatically extend desktop session to external monitors** feature, it is recommended to disable the virtual desktop screen resizing feature.

Enhance Samsung Smartphone with USB Redirection for transferring images

This section describes how to enable USB redirection for transferring images on Samsung smartphones.

In ThinOS 2411 and Citrix Workspace App 2408, ThinOS enhances the **Transferring images** function for Samsung smartphones.

To enable this feature, follow these steps:

1. Open the Admin Policy Tool or the Wyse Management Suite policy settings.
2. Go to **Advanced VDI Configuration Editor** > **Citrix Configuration Editor**.
3. In the Citrix USB File Settings, click **Add Row**.
4. In the **Key** field, enter **CONNECT**.
5. In the **Value** field, enter **vid=04e8 pid=6865 disableselectconfig=1**.

   ⓘ **NOTE:** Replace the VID and PID in the Value field with the VID and PID of your Android smartphone. The Samsung Galaxy F52 and S21 are qualified with ThinOS 2411.

6. Click **Save & Publish**.
7. Sign out or restart the device for the settings to take effect.

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

Limitation

The **Transferring files** function of Samsung smartphones with USB redirection does not work. This issue also occurs in the Linux Citrix Workspace app binary.

Citrix Workspace App Limitations

This section outlines the limitations of the Citrix Workspace app.

The following limitations apply when using the Citrix Workspace app:

- When you enable **native mode**, the disk drive maps with the map disks option disabled.
- Enabling **native mode** causes Single Desktop User log in to fail.
- **Native mode** does not work with ThinOS 2408 and Citrix Workspace App 2408.
- Sometimes, videos flicker when **BCR** is enabled.
- The **"Open Citrix Workspace Launcher"** dialog cannot be saved during FIDO2 login using CEB with Citrix Workspace App 2408.

The following issues also occur in the Linux Citrix Workspace app binary:

- USB redirection for **"Transferring files"** does not work well with Samsung smartphones.
- Topaz signature pad mapping fails in an ICA session when you unplug and replug the device during a signature.
- Occasionally, USB disk redirection does not work in Citrix when the Desktop Viewer Toolbar is disabled.
- The Microsoft Teams camera preview does not work properly when multiple cameras are connected.

Teradici PCoIP updates

- Teradici version is updated to 24.07.3.7 in ThinOS 2411.

  ⓘ **NOTE:** This package is not available in ThinOS 2408 and earlier versions.

VMware Horizon updates

- The `Horizon Client SDK` package is updated to `VMware_Horizon_ClientSDK_2406.8.13.0.33.pkg`.

Limitations

- When you disconnect a published Horizon PCoIP application, the event log appears after 2 minutes.
- The NumLock/CapLock status changes locally when you launch a Horizon Blast/PCoIP session.
- Horizon Blast and PCoIP sessions may randomly display a black screen when the RingCentral package is installed on ThinOS. To resolve, sign off from the Horizon Broker agent and log in again. If you do not use the RingCentral function, do not install the RingCentral package on ThinOS.

Microsoft RDP and AVD updates

Microsoft AVD package is updated to version 3.0.2442 in ThinOS 2411.

ⓘ **NOTE:**

> - The AVD package for ThinOS 2411 is not compatible with previous ThinOS releases. ThinOS 2411 exclusively supports the AVDpackage that is designed for this version. If you enable the "Use External Engine for WebLogin" option, ensure you use the Chrome Browser package version 130.0.6723.116.1.
> - The ThinOS 2411 AVD WebLogin functionality has been enhanced for improved security, necessitating the use of the updated Chrome package version 130.0.6723.116. For access to the new Chrome package version, contact Dell sales or Support | Dell.

Known issue

- There is a known issue where direct Remote Desktop Protocol (RDP) connections to Windows Server 2008 are unsuccessful.

Support for Single Sign-On with FIDO2

In ThinOS 2411 and Microsoft AVD Package 3.0.2442, users can authenticate using FIDO2 security keys. FIDO2 security keys provide a passwordless login experience for the AVD Broker agent and facilitate single sign-on (SSO) for AVD sessions. It is recommended to enable the Entra single sign-on on their Azure policy for device single sign-on experience.

Support for SmartCard login AVD Broker agent

In ThinOS 2411 and Microsoft AVD package 3.0.2442 you can authenticate using SmartCard to login AVD Broker agent, and launch an AVD session. It is recommended to enable Entra single sign-on on their Azure policy for device single sign-on experience.

To enable SmartCard for login AVD Broker agent, do the following:

1. Open **Wyse Management Suite policy**.
2. Go to **Broker Settings** > **Azure Virtual Desktops Settings**.
3. Enable **Enable Azure Virtual Desktop**.
4. Enable **Use External Engine for WebLogin**.
5. Go to **Browser Settings** > **Chrome Browser Settings**, enable **Enable Browser**.
6. ⓘ **NOTE:** To use Chrome Browser, install the Chrome Browser package first.
7. Click **Save and Publish**.
8. Sign out or restart the device for the settings to take effect.
9. In the **webview login window**, enter the user account, and click **Next**.
10. Do not enter the password, click **Use certificate or smart card** link.
11. Select the user and enter the PIN.

ⓘ **NOTE:** Automatic sign-off from the AVD Broker agent is not supported when the Smart Card is unplugged from ThinOS. Users must manually sign off to end their session.

Support for Cisco Webex App VDI Optimization in AVD and RDP Sessions

In ThinOS 2411, with Microsoft AVD Package 3.0.2442 and the updated Cisco Webex VDI package version 44.10.0.30906.5, the Cisco Webex App VDI Optimization is enabled. This feature is available for both AVD and RDP sessions.

Amazon WorkSpaces update

Amazon WorkSpaces Client package version is updated to 24.6.5072.4 in ThinOS 2411.

ⓘ **NOTE:** This package is not compatible with ThinOS 2408 and earlier versions.

Full Screen Mode Policy

In **WMS** > **Session Settings** > **Global Session Settings**, the Full Screen Mode policy is working for the AWS WSP desktop from ThinOS version 2411. By default, this setting is **Enabled** .

Known Issues

The following known issues are identified:

- If the default login user and password are set, users cannot log in with nondefault credentials when connecting to the Amazon WSP standard Broker agent.
- When the Amazon WSP virtual machine is in a **Stopped** state, the desktop fails to launch on the first login attempt.
- Occasionally, the AWS login window disappears when changing the Remote Connection Settings.

Imprivata OneSign Authentication

Configure Imprivata OneSign Authentication and related settings in ThinOS.

Imprivata PIE Bootstrap Support

The Imprivata PIE bootstrap package version 23.3.0.715913.52 is supported in ThinOS 2411.

- This Imprivata PIE bootstrap package does not include the Imprivata PIE agent.
- After installing the Imprivata PIE bootstrap, ThinOS connects to the OneSign appliance to obtain the Imprivata PIE agent during the first boot.
- Once ThinOS has installed the Imprivata PIE agent using the OneSign appliance, it does not reinstall the same version of the Imprivata PIE agent.
- ThinOS upgrades the Imprivata PIE agent only if a newer version is available on the Imprivata OneSign appliance.
- A message stating **Start Imprivata Bootstrap** is displayed when the PIE application begins to launch. The initial boot takes longer than usual.
- A message stating **Imprivata agent failed to start** is displayed when the PIE agent is not successfully obtained from the Imprivata OneSign appliance.

Preconditions on Imprivata appliance

The Imprivata ProveID Embedded (PIE) agent must be installed on the Imprivata appliance.

The Imprivata PIE agent version must be equal to or greater than 23.3.

Create and configure a system policy for ThinOS:

1. Go to **General tab** > **ProveID Embedded agent version**.
2. Select **When an agent upgrade is available:** Install the upgrade when idle or on reboot. For details, see **Upgrades and Downgrades**.
3. Select a specific version to install from the list. If only one IPM file is uploaded to the appliance, this version is selected by default.
4. Save and assign the system policy to your ThinOS devices.

Configurations in ThinOS

This section provides instructions for configuring ThinOS, including installing the Imprivata PIE bootstrap package and uploading SSL certificates.

- Install the Imprivata PIE bootstrap package. For more information, see Install Imprivata PIE bootstrap package.
- Upload the SSL Certificate. For more information, see Uploading the SSL Certificate.
- Configure the OneSign server, using the ThinOS 9.x policy settings in Wyse Management Suite or the local Admin Policy Tool. Enable the Imprivata ProveID Embedded (PIE) mode through these settings. For more information, see Configure OneSign server.

Install Imprivata PIE bootstrap package

You can install the Imprivata PIE bootstrap package:

- Using Wyse Management Suite: For more information, see **Upload and push ThinOS 9.x application packages using Groups and Configs on Wyse Management Suite** in Dell ThinOS 2402, 2405, and 2408 Administrator's Guide.
- Using Admin Policy Tool: For more information, see **Upload and install ThinOS 9.x application packages using Admin Policy Tool** in Dell ThinOS 2402, 2405, and 2408 Administrator's Guide.

Uploading the SSL Certificate

You can upload the SSL certificate by following any of the two methods:

- Import the OneSign appliance SSL certificate automatically. For more information, see Importing the OneSign appliance SSL certificate automatically.
- Import the OneSign appliance SSL certificate manually. For more information, see Importing the OneSign appliance SSL certificate manually.

Importing the OneSign appliance SSL certificate automatically

This section provides the steps to configure the automatic importing and installation of the OneSign Appliance SSL Certificates for ThinOS devices using the WMS.

Prerequisites

- Create a group in the Wyse Management Suite with a valid group token.
- Register ThinOS devices with the Wyse Management Suite.
- Upload the SSL certificate to **Apps & Data** > **File Repository** > **Inventory**.

Steps

1. Log in to the **Wyse Management Suite**.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies ThinOS 9.x**.
4. The **Configuration Control | ThinOS** window displays.
5. Click the **Advanced** tab.
6. Expand **Privacy & Security**, then click **Certificates**.
7. Click the **Auto Install Certificates** slider to enable automatic installation of certificates on ThinOS.
8. From the **Select Certificates to Upload** drop-down list, select the SSL certificate.
9. Click **Save & Publish**.

Results

The SSL certificate is now installed on your ThinClient.

NOTE: Import the SSL certificate of the Imprivata appliance into ThinOS before you obtain the Imprivata PIE agent from the OneSign appliance during the first boot.

Importing the OneSign appliance SSL certificate manually

This section provides the steps to Import the SSL certificate to your thin client manually.

Prerequisites

Ensure you have the OneSign appliance SSL certificate that is stored on your USB drive.

Steps

1. Connect the USB drive to the thin client.
2. Go to **System Tools** > **Certificates**.
3. From the **Import From** drop-down list, select **USB Storage**.
4. Click **Import**.

5. Browse and select the SSL certificate from the USB drive.
6. Click **OK**.

Results

The SSL certificate is successfully imported to the ThinClient.

ⓘ **NOTE:** Import the SSL certificate of the Imprivata appliance into ThinOS before you obtain the Imprivata PIE agent from the OneSign appliance during the first boot.

Configure OneSign server

Configure the OneSign server using the Admin Policy Tool or Wyse Management Suite.

Prerequisites

Ensure you have access to the Admin Policy Tool or Wyse Management Suite.

About this task

This task enables the Imprivata PIE mode on ThinOS.

Steps

1. Open the **Admin Policy Tool** on your thin client or go to the **ThinOS 9.x policy settings** in **Wyse Management Suite**.
2. In the **Configuration Control** > **ThinOS** window, click the **Advanced** tab.
3. Expand **Login Experience** and select the **3rd Party Authentication** option.
4. From the **Select Authentication Type** drop-down list, choose **Imprivata**.
5. The **Imprivata Settings** window appears.
6. In the **OneSign Server** field, enter the FQDN of the Imprivata OneSign servers.
7. Enable the **ProveID Embedded Mode** on ThinOS by clicking the **Enable ProveID Embedded Mode** slider switch.
8. Click **Save & Publish** to apply the changes.

Results

The OneSign server is configured, and ProveID Embedded mode is enabled on ThinOS.

Known Issues and Limitations for ThinOS 2411

This section outlines the limitations and known issues that are related to the ThinOS 2411 release.

The limitations and known issues are listed as follows:

- Customized SSPR is not supported in ThinOS 2411 release.
- Allow list of local Windows is not supported in ThinOS 2411 release.

ⓘ **NOTE:** Due to this limitation, the **Display Settings** window can only be opened using **Win+P** after the session has started.

Known issue with ThinOS PIE Application:

- ThinOS PIE application gets stuck after RDS session disconnects during fingerprint authentication on Imprivata Agent.

Workaround: It is a random issue. Sign off from the RDS session and reboot ThinOS to recover.

Known cosmetic issue:

- XenApp menu remains on top of the session after login and automatic launch of Citrix session.

It is a UI cosmetic issue. Click the mouse to focus on the Citrix session.

Horizon SAML Authentication in PIE Mode

This document outlines the steps to enable and configure SAML authentication in the Horizon server for PIE mode.

Horizon SAML authentication supports PIE mode. Follow these steps to enable and configure SAML authentication in the Horizon server:

Enable and configure SAML authentication in the Horizon server:

1. Open the **Connection Servers** tab.
2. Click **Edit**.
3. Open the **Authentication** tab.
4. Click the **Manage SAML Authenticators...** button.
5. Click the **Add** button.
6. Add the appliance DNS name to the Metadata URL, using the following format: **https://ApplianceDNS.domain/sso/vmware/idp/SAML2**.
7. Select the **Dynamic** type.
8. Check **Enabled for Connection Server** and accept the certificate.

Configure Horizon VDI and enable SAML authentication from the Imprivata OneSign Server:

1. Open the **Computers** tab for Virtual Desktop.
2. Add the VMware URL to the **VMware Horizon - Desktops** section.
3. Check **Use SAML Authentication**.

ⓘ **NOTE:** You should not configure this feature in ThinOS. Once you complete the server-side configurations, logging into Horizon in ThinOS PIE mode automatically uses SAML authentication.

Identity Automation Update

IDAuto package

IDAuto package is updated to 2.1.1.13

Support for Show Password and PIN

The IDAuto 2.1.1 update introduces the following functionalities:

- Show Password Functionality— Users can now verify the accuracy of their entered password before submission. This feature is available during:
  - User registration
  - Logging into Identity Automation
  - Manual login steps
  - Password reset process
- Show PIN Functionality— Users can also verify their entered PIN for accuracy prior to submission. This feature is available during:
  - User registration
  - Logging into Identity Automation
  - PIN reset process

Cisco updates

Cisco Webex App VDI Update

The following updates are now available:

- The Cisco Webex VDI package version is now 44.10.0.30906.5.
- The update supports Webex App VDI optimization in AVD, RDP, and RDS sessions.

Cisco Webex Meetings VDI Update

The following updates are now available:

- The Cisco Webex Meetings package version is now 44.10.1.3.4.

Cisco Jabber Update

The following updates are now available:

- The Cisco Jabber package version is now 15.0.0.309289.6.

Zoom updates

Zoom package version is updated to Zoom_Universal_6.1.10.25260.3.

New features

- Enhanced Visual Effects and Background Controls.
- Multi-share feature allows you to view the newest shared tab.

RingCentral App VMware plugin update

- Updated the version of the RingCentral App VMware Plugin to 24.3.31.2.
- The update fixes the issue where Horizon VDI sessions stop responding and experience lag while using the RingCentral application.

eG VM Agent

- The eG VM Agent package version is updated to 7.2.10.12 in ThinOS 2411.

Liquidware Stratusphere UX Connector ID Agent update

Liquidware Stratusphere UX Connector ID Agent is updated to version 6.7.0.7.1 in ThinOS 2411.

ControlUp VDI agent updates

- ControlUp VDI Agent package version is updated to 2.2.30 in ThinOS 2411.

Common printing package updates

The common printing package version is updated to Common_Printing_2.0.0.5.

New features

- Support for browser printing using Line Print Terminal (LPT) and Server Message Block (SMB) printing.

ⓘ **NOTE:** Line Printer Daemon (LPD) service printing and network printing using LPD are not supported in this version.

ThinOS updates

Improved DNS IP Version Logic in ThinOS 2411

Starting with ThinOS version 2411, the DNS IP version logic was refined to prioritize an efficient hostname resolution. The following changes were made:

- By default, on a ThinOS client, the DNS server resolves a hostname to both IPv4 and IPv6 addresses. The client prioritizes the IPv4 address over the IPv6 address.

- When the WMS policy **Enable IPv6** option is set to disable within **Network Configuration** > **Common Settings**, the DNS server on the ThinOS client exclusively resolves hostnames to IPv4 addresses. This change takes effect after rebooting the client.
- When the WMS policy **Enable IPv4** option is set to disable in the same settings, the DNS server on the ThinOS client exclusively resolves hostnames to IPv6 addresses. This change takes effect after rebooting the client.
- The WMS policy must be set to update the DNS IP version. Changes made to enable or disable IPv4 or IPv6 through the ThinOS Graphical UI do not affect the DNS IP version.

Support for WMS auto discovery by IPv6 DHCP option

From ThinOS 2411, ThinOS supports WMS auto discovery by IPv6 DHCP option. Below are the IPv6 DHCP option tags for WMS auto discovery.

ⓘ **NOTE:** When there is only IPv6 but no IPv4 in your network, it takes about 5 minutes to wait for IPv4 DHCP time-out. WMS is discovered automatically from IPv6 DHCP. Disable IPv4 in your WMS policy, or after each reboot it takes 5 minutes to wait for IPv4 DHCP time-out.

Table 15. Options table for WMS auto discovery by IPv6 DHCP option

Option Tag	Description
Name—WMS Data Type—String Code—16500 Description—WMS Server FQDN	This tag directs to the Wyse Management Suite server URL. For example, wmsserver.acme.com, where wmsserver.acme.com is the fully qualified domain name of the server hosting the Wyse Management Suite. ⓘ **NOTE:** HTTPS:// is not required in the Wyse Management Suite URL.
Name—WMS Data Type—String Code—20100 Description—Secure WMS Server	This tag directs to the secure Wyse Management Suite server.
Name—CA Validation Data Type—String Code—16700 Description—Certificate Authority Validation	You can enable or disable the CA validation option when you are registering your devices with Wyse Management Suite on private cloud. ● Enter True, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. ● Enter False, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. ⓘ **NOTE:** CA Validation is optional for Wyse Management Suite 2.0 and later versions. However, it is recommended to configure this option tag.
Name—Group Registration Key Data Type—String Code—19900 Description—Group Registration Key	The tag directs the device to retrieve the Group Registration Key for Wyse Management Suite. For example, SCDA-DTos91SalesGroup. ⓘ **NOTE:** Group Token is optional for Wyse Management Suite 2.0 and later versions on private cloud. However, there is a known issue that if you do not provide the group token, the device is not moved to an unmanaged group. Therefore, It is recommended to configure the Group Token key.
Name—Group Registration Key Data Type—String Code—20200	The tag directs the device to retrieve the secure Group Registration Key for Wyse Management Suite.

Table 15. Options table for WMS auto discovery by IPv6 DHCP option (continued)

Option Tag	Description
Description—Secure Group Registration Key	

Support for FIDO2 Security Key Management

ThinOS FIDO2 Security Key Management offers functionalities for changing the FIDO2 Security Key PIN and FIDO2 Security Key Reset. The FIDO2 Security Key Management Icon is accessible from the ThinOS system tray.

When you click the Security Key icon, the following features are available:

- **Create a PIN**
- **Reset Your Security Key**

Create a PIN

To create a PIN, follow these steps:

1. Plug in the FIDO2 Security Key device.
2. Select **Create a PIN** from the Security Key Management menu.
3. A message is displayed: **To continue, insert and touch your security key.**
4. Touch your security key to open the PIN reset window.
5. Input valid PINs to change the PIN.
6. Upon successful PIN change, a message appears: **Your PIN was created.**

Reset Your Security Key

To reset your security key, follow these steps:

1. Select **Reset Your Security Key** from the Security Key Management menu.
2. Plug in the FIDO2 Security Key device.
3. Touch your security key.
4. If prompted with the message **Touch your security key again to confirm reset. All information stored on the security key, including its PIN, will be deleted,** touch your security key again.
5. After the reset, a message will appear: **Your security key has been reset.**

If you receive the message: **Cannot reset this security key. Try resetting the key immediately after inserting it.**, unplug, and replug your security key, then touch it immediately.

New Settings for FIDO2 Security Key Management

A new setting has been added under Peripheral Management for FIDO2 Security Key:

- **Allow Minimize PIN Length**

You can set the allowed minimum PIN length (ranging from 4 to 63) in the FIDO Service Tray.

Support for displaying firmware version of external monitor

Instructions to display the firmware version of an external monitor that is connected to a device.

Procedure

To view the firmware version of an external monitor that is connected to your device, follow these steps:

- Go to the **System Info** section.
- Select **Peripherals**.
- Locate the external monitor in the list.

The firmware version is displayed under the **WMS server console** in the **WMS Devices Details** page.

Bluetooth

Bluetooth headset volume is lower than ThinOS 2408.

WMS ThinOS 9.xPolicy/ThinOS 9 Admin Policy Tool update

ⓘ **NOTE:** Wyse Management Suite 4.4 server is required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

Updated Device Action Post Package Update

Go to **Services** > **WDA Settings**. Select **Shutdown** from the Device Action Post Package Update list when you want to update only the BIOS. The device shuts down after the BIOS update is complete.

Added Allow Minimize PIN Length for FIDO2 Security Key

Go to **Peripheral Management** > **FIDO2 Security Key Settings** page. Set the allowed minimum PIN length (4-63) for your security key in the FIDO Service tray.

Added Show Login Icon on Floatbar/Taskbar

The **Show Login Icon on Floatbar/Taskbar** option is added in **Personalization** > **User Experience Settings**. Enable this option to see the login window icon on the taskbar. Click the icon to minimize the login window. This option requires a reboot to take effect. This feature is disabled by default. It allows users to switch between the browser window and the VDI login window.

Changed Names and Added New Options in Device Driver Page

In **Peripheral Management** > **Device Driver Page**, change the Device Driver row name to **USB Force UHID Driver**. A **Device Name** field is added to improve the user experience for multiple rows.

Added **USB Device Fine Tuning** for special devices like the ZEBRA printer, which may not work directly on ThinOS. You can add a row and input the required information to make these devices work. This feature requires a reboot to take effect.

Added Bookmark Folder Name

The **Bookmark Folder Name** option is added in **Browser Settings** > **Chrome Browser Settings**. Enable the **Enable Managed Bookmarks** option to see the **Bookmark Folder Name** option. You can input a value for the bookmark folder name in the Chrome browser window.

Added Kiosk Window in Lockdown Mode

In **Browser Settings** > **Chrome Browser Settings**, the **Kiosk Window in Lockdown Mode** option is added in the Launch Mode drop-down list.

When you open a Chrome browser session with the **Kiosk Window in Lockdown Mode**, the Chrome browser window remains on top, and the ThinOS taskbar is disabled. This feature allows the users to lock down the device for browser access only.

Added Enable Ctrl+Alt+Del for Shutdown Menu in Lockdown Mode

The **Enable Ctrl+Alt+Del for Shutdown Menu in Lockdown Mode** option is added in **Browser Settings** > **Chrome Browser Settings**. When you open a Chrome browser session with the **Kiosk Window in Lockdown Mode**, you can press Ctrl+Alt+Del to open the Shutdown Menu when this option is enabled.

Added Allow Chrome Package Installation using USB

The **Allow Chrome Package Installation via USB** option is added in **Browser Settings** > **Chrome Browser Privilege**. Enable this option to upload the Chrome Browser package in the ThinOS Admin Policy Tool using USB and install it.

Added Chrome Browser Permission Page

The Chrome Browser Permission page is added in **Browser Settings**. By default, when you want to use the camera or microphone on a website, a window appears with **Block** and **Allow** buttons. You must click the **Allow** button to use the camera or microphone.

You can add rows and input URLs as hostnames in the Camera and Microphone-allowed list. Therefore, you cannot see the permission window when using the camera or microphone on the specified website URLs. This feature enables browser users to access web meetings without allowing camera and microphone permissions each time. A URL is required here, following Google policy practice.

Added Unique Validation for Network Interface Index Option

In **Ethernet Settings** > **802.1X Authentication Settings**, you could previously add multiple rows with the same **Network Interface Index**. Unique validation is now added for the Network Interface Index option, to avoid conflicts.

Added Input Validation for Liquidware URL Option

In **System Settings** > **Device Monitoring**, enable the **Liquidware Stratusphere UX Connector ID Agent** option. In the URL field, you must input the URL with the `http://` or `https://` prefix.

Updated Common Printing Package Category

Moved the Common Printing package from **Firmware** > **Application Package Updates** > **Other** to **Firmware** > **Application Package Updates** > **Third Party**.

Added Cisco Webex App VDI Optimization Option

This option is added in **Session Settings** > **RDP** and **AVD Session Settings** > **UC Virtual Channel Settings**, with the default value set to Enable. When enabled, it allows Webex App VDI optimization in AVD, RDP, and RDS sessions.

Updated Teams Video Acceleration

The default value for Teams Video Acceleration is changed from **Enable** to **Disable**.

Updated Time Zone

The Time Zone for **Europe/Dublin** updates from **UTC+1** to **UTC+0**.

Added The Maximum WMS Request Timeout Option

The **Maximum WMS Request Timeout** option is added to **Services** > **WDA Settings**. You can specify the timeout in milliseconds for WMS requests, with a default value of 3000.

Added WebLogin Timeout

The **WebLogin Timeout** option is added in **Broker Settings** > **Azure Virtual Desktop Settings**. You must enable the **Enable Azure Virtual Desktop** option first for it to appear. By default, it is set to 0 minutes, meaning this feature is disabled and the device follows the Microsoft timeout interval. This entry box accepts values from 0 to 300 minutes.

The Microsoft login page has a timeout interval that is unknown to the device and user before login. The **WebLogin timeout** value is designed to initiate a timeout from the device, allowing the device or user to refresh the page before login. Specify a value in minutes so the device can initiate a timeout with the **OK** button to the login page, or it automatically refreshes in 10 s.

NOTE: The **Enable Azure Virtual Desktop** option must be enabled for the **WebLogin timeout** to appear.

Tested environment and peripheral matrices

General tested environments matrices

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

Table 16. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.4.211
Configuration UI package for Wyse Management Suite	1.10.460
Citrix ADC (formerly NetScaler)	13.0 and later
Storefront	1912 LTSR and later

Table 17. 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 (CU4)	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2402 LTSR	Tested	Tested	Tested	Tested	Tested	Tested

Table 18. Test environment—VMware Horizon View

VMware	Windows 11	Windows 10	Windows Server 2022	Windows Server 2022 APPs	Ubuntu 20.04
VMware Horizon 2312	Tested	Tested	Tested	Tested	Tested
VMware Horizon 2312.1	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2406	Tested	Tested	Tested	Tested	Tested

Table 19. Test environment – VMware Horizon Cloud Next Gen

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

Table 20. 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 21. 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 (MICROSOFT-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 22. Test environment—Windows 365 cloud PC

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

Table 23. Test environment—Amazon WorkSpaces

Protocol	Authentication Method	Windows 2016	Windows 2019	Windows 2022
PCoIP	Standard	Tested	Not tested	Not tested
	MFA	Tested	Not tested	Not tested
WSP	Standard	Tested	Not tested	Not tested
	MFA	Not tested	Not tested	Tested
	SmartCard	Not tested	Tested	Not tested

Table 24. Tested environment—Skype for Business offloading

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 (CU4) • Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10 Windows 11 Windows server 2016 Windows server 2019	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015

Table 25. Tested environment—JVDI

Citrix VDI	Operating system	Cisco Jabber package	JVDI agent	Jabber software
• Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) • Citrix Virtual Apps and Desktops 7 2203 LTSR (CU4)	Windows 10 Windows 11 Windows server 2016 Windows server 2019	15.0.0.309289.6	15.0.0.309289	15.0.0.309289

Table 25. Tested environment—JVDI (continued)

Citrix VDI	Operating system	Cisco Jabber package	JVDI agent	Jabber software
- Citrix Virtual Apps and Desktops 7 2402 LTSR				

Table 26. Tested environment—JVDI

VMware VDI	Operating system	Cisco Jabber package	JVDI agent	Jabber software
- VMware Horizon 2312 - VMware Horizon 2312.1 - VMware Horizon 2406	Windows 10	15.0.0.309289.6	15.0.0.309289	15.0.0.309289
	Windows 11			
	Windows server 2022			

Table 27. 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 (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10	6.1.10.25260.3	6.1.10(25260)
	Windows 11		
	Windows server 2016		
	Windows server 2019		

Table 28. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
- VMware Horizon 2312 - VMware Horizon 2312.1 - VMware Horizon 2406	Windows 10	6.1.10.25260.3	6.1.10(25260)
	Windows server 11		
	Windows server 2022		

Table 29. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	6.1.10.25260.3	6.1.10(25260)
	Windows server 2016		
	Windows server 2019		

Table 30. Tested environment—Cisco Webex App VDI

RDP Protocol VDI	Operating system	Webex App VDI	Webex App VDI software
- Azure Virtual Desktop	Windows 10	44.10.0.30906.5	44.10.0.30906
	Windows 11		

Table 30. Tested environment—Cisco Webex App VDI

Citrix VDI	Operating system	Webex App VDI	Webex App software
- Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6)	Windows 10	44.10.0.30906.5	44.10.0.30906
	Windows 11		

Table 30. Tested environment—Cisco Webex App VDI (continued)

Citrix VDI	Operating system	Webex App VDI	Webex App software
- Citrix Virtual Apps and Desktops 7 2203 LTSR (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 31. Tested environment—Cisco Webex App VDI

VMware VDI	Operating system	Webex App VDI	Webex App software
- VMware Horizon 2312 - VMware Horizon 2312.1 - VMware Horizon 2406	Windows 10	44.10.0.30906.	44.10.0.30906
	Windows 11		
	Windows server 2022		

Table 32. Tested environment—Cisco Webex Meetings VDI

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
- Citrix Virtual Apps and Desktops 7 1912 LTSR (CU6) - Citrix Virtual Apps and Desktops 7 2203 LTSR (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10	44.10.1.3.4	44.10.1.3
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 33. Tested environment—Cisco Webex Meetings VDI

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
- VMware Horizon 2312 - VMware Horizon 2312.1 - VMware Horizon 2406	Windows 10	44.10.1.3.4	44.10.1.3
	Windows 11		
	Windows server 2022		

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

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

Table 34. Supported peripherals for Dell Wyse 5070, 5470, and 5470 AIO

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

Table 34. Supported peripherals for Dell Wyse 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	Dell USB Sound Bar (AC511M)	Supported	Not Available	Supported
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Supported	Supported
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Not Available	Supported
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Not Available	Supported
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Not Available	Supported
	Dell USB Wired Keyboard - KB216	Supported	Supported	Not Available
	Dell USB Wired Optical Mouse - MS116	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Supported	Supported
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link)	Supported	Not Available	Not Available

Table 34. Supported peripherals for Dell Wyse 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	- DANARBC084 - DANARBC084			
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Supported	Not Available	Supported
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI - DBQAUBC064 - DBQAUBC064	Supported	Not Available	Not Available
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Supported	Not Available	Not Available
	Trendnet USB to Serial Converter RS-232	Supported	Supported	Supported
	Dell Adapter - HDMI to DVI - DAUARBN004 - DAUARBN004	Not Available	Not Available	Supported
	Dell Adapter - HDMI to VGA - DAUBNBC084 - DAUBNBC084	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	Supported	Supported
Displays	E1916H	Supported	Supported	Not Available
	E1920H	Supported	Supported	Supported
	E2016H	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported
	E2216H	Supported	Supported	Supported

Table 34. Supported peripherals for Dell Wyse 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	E2216Hv (China only)	Not Available	Not Available	Supported
	E2218HN	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported
	E2318H	Supported	Supported	Supported
	E2318HN	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported
	E2420HS	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported
	E2720HS	Supported	Supported	Supported
	P2016	Supported	Not Available	Not Available
	P2018H	Not Available	Not Available	Supported
	P2217	Supported	Not Available	Not Available
	P2217H	Supported	Not Available	Not Available
	P2219H	Supported	Not Available	Supported
	P2219HC	Supported	Not Available	Supported
	P2317H	Supported	Not Available	Not Available
	P2319H	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Not Available
	P2417H	Supported	Not Available	Not Available
	P2418HT	Supported	Supported	Not Available
	P2418HZ	Supported	Not Available	Not Available
	P2419H	Supported	Supported	Supported
	P2419HC	Supported	Not Available	Supported
	P2421D	Supported	Not Available	Supported
	P2421DC	Supported	Not Available	Supported
	P2719H	Supported	Supported	Supported
	P2719HC	Supported	Not Available	Supported
	P2720D	Supported	Not Available	Supported
	P2720DC	Supported	Not Available	Supported
	P3418HW	Supported	Supported	Not Available
	P4317Q	Supported	Supported	Not Available
	MR2416	Supported	Not Available	Not Available
	U2415	Supported	Supported	Not Available
	U2419H	Supported	Supported	Supported
	U2419HC	Supported	Not Available	Supported
	U2518D	Supported	Supported	Not Available

Table 34. Supported peripherals for Dell Wyse 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	U2520D	Supported	Supported	Supported
	U2718Q (4K)	Supported	Supported	Supported
	U2719D	Supported	Supported	Supported
	U2719DC	Supported	Not Available	Supported
	U2720Q	Supported	Supported	Supported
	U2721DE	Supported	Supported	Supported
	U2421HE	Not Available	Supported	Supported
	U4320Q	Supported	Supported	Supported
	U4919DW	Supported	Not Available	Not Available
Networking	Add On 1000 Base-T SFP transceiver (RJ-45)	Supported	Not Available	Not Available
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Supported
Storage	Dell Portable SSD, USB-C 250GB	Supported	Not Available	Supported
	Dell External Tray Load ODD (DVD Writer)	Supported	Not Available	Supported
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported
	Sun microsystem SCR 3311	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Supported	Not Available	Supported
Printers	Dell Color Printer- C2660dn	Supported	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 35. Supported ecosystem peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio Devices	Dell Pro Stereo Headset - Cortez - WH3022

Table 35. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Soundbar - AE515M - AE515M - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - AC511M - AC511M - Potential M
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P
	Dell Premier Wireless ANC Headset - Blazer - WL7022
	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Slim Conferencing Soundbar - Lizzo - SB522A
	Dell Speakerphone - Mozart - SP3022
	Stereo Headset WH1022 (Presto)
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync - 202652-02 - 202652-02
Input Devices	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Bluetooth connection is not supported)
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_GREY - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_WHITE - MS116 - MS116 - Sapphire
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_Grey - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_WHITE - KB216 - KB216 - Rusty
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819 (Fingerprint reader is not supported)
	Dell Wireless Keyboard and Mouse - Auburn MLK - KM3322W
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726
	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

Table 35. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

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

Table 35. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	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 36. 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 (Supports USB dongle connection and not Bluetooth connection.)
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
Audio/Video	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 37. 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 38. 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 (Supports USB dongle connection and not Bluetooth connection.)
	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 39. 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 40. 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

Table 40. Supported ecosystem peripherals for Latitude 5450 (continued)

Product Category	Peripherals
	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 41. 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 42. 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 43. Third-party supported peripherals

Product Category	Peripherals
Audio Devices	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth （Link 360 is the bluetooth dongle name.）
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Supports USB dongle connection and not Bluetooth connection.)

Table 43. Third-party supported peripherals (continued)

Product Category	Peripherals
	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 supports 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
	Yealink WH66 (Limitation: The **Call** button works well with Skype for Business in Citrix. You can decline calls in Zoom meetings in Citrix, Blast, and RDP sessions. In other scenarios, only audio works and the **Call** button does not work. ⓘ **NOTE:** The **Call** button does not work with Microsoft Teams in Blast after Microsoft Teams is updated to version 2.0.
Input Devices	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
Displays	Elo ET2201L IntelliTouch ZB (Worldwide) - E382790

Table 43. Third-party supported peripherals (continued)

Product Category	Peripherals
	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
	Gemalto IDBridge CT710

Table 43. Third-party supported peripherals (continued)

Product Category	Peripherals
	GemPC Twin
	Gemalto IDBridge CT30 V2
	Gemalto IDBridge CT30 V3
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
	MFR75A Fido-2
	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.
- 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 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.

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 44. Supported smart cards

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2	Supported	Supported	Supported
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c	Supported	Supported	Supported
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8	Supported	Supported	Not Available
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 7.0 (T=0)	Supported	Supported	Not Available
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported

Table 44. 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)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available
A.E.T. Europe B.V. (Integrated Latitude 5450 reader	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	G&D STARCOS 3.0 T=0/1 0V300	Supported	Not Available	Supported

Table 44. 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)
is not 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 issue list

Table 45. Fixed issue list

Key	Summary
DTOS-29541	5070 - Update to 2408 or 2405 is not allowing customer to connect to WMS.
DTOS-29399	Firmwareupdate/downgrade failure when disabling live update with wired 802.1x Auth.
DTOS-29376	Integrated (inbuilt) camera resolution and refresh rate is too low.
DTOS-29367	Azure Conditional Access causes the ThinOS to prompt for RDP login.
DTOS-29186	Thin Clients automatically change to the default group.

Table 45. Fixed issue list (continued)

Key	Summary
DTOS-29066	ThinOS AVD RDP NumLock does not work on login when NLA is off.
DTOS-29000	Unable to launch multiple sessions simultaneously from VMware.
DTOS-28989	Users getting error while connecting to DAAS post ThinOS upgrade when using specific ISP.
DTOS-28822	OPT3K - 2405 - Devices not registering to WMS 4.4 with IPv6.
DTOS-28534	USB Key model Apricorn SecureKey that is not recognized since update to 2405.
DTOS-28046	Azure | Clicking issues from one app to another app in the background or foreground.
DTOS-27814	OptiPlex 3000 - 2405 - Kodak scanner intermittently works.
DTOS-26968	Horizon VDI freezing issue when optimizing the RingCentral application.
DTOS-25585	ThinOS 2311 - OptiPlex 3000 - Cisco USB Roomkit Camera - Video lag, delay.
DTOS-25144	Zebra 411 label printer issue on the backend session of OptiPlex 3000 Thin Client.
DTOS-25071	Inability to use smartcard to sign documents in the AVD session.
DTOS-29447	Unable to get the AWS Workspaces Client to log in fullscreen mode.
DTOS-29792	The medigenic USB Keyboard is not working.
DTOS-22848	USB Smart Touch Display causes reboot.
DTOS-28354	Galaxy S21 not redirecting in Blast.
DTOS-29347	WMS Cloud possible Wave deployment problem.
DTOS-29932	When screen sharing during Microsoft Teams meetings, the mouse cursor is missing.
DTOS-29832	Citrix session launch stops responding when WMS is unresponsive.
DTOS-29642	WiFi captive portal not opening.
DTOS-26915	SCEP enrollment failure.
DTOS-29253	Cert import from USB fails if more than 182 PFX files are on the USB drive.
DTOS-29624	WMS reporting wrong information.
DTOS-29789	RDP connection and network settings disappear when restarting the device.
DTOS-30098	If the DHCP server does not correctly assign the GATEWAY when the IP address has all octets consisting of three digits, issues may arise.
DTOS-30028	Teams ringer issue.
DTOS-29900	Scanner not reattaching to session after thin client/scanner awakens from sleep.

Known Issues

Table 46. Known Issues

Key	Summary	Workaround
DTOS-29589	[Security Key] A proper error message does not appear when attempting to create a security PIN without a Yubico Security Key.	There is no workaround.
DTOS-29696	Bluetooth headset volume is lower than ThinOS 2408.	The max volume level is the same.
DTOS-29883	The Chrome browser session remains available even after locking the terminal.	There is no workaround.
DTOS-29462	Browser session that is configured remains on the screen/VDI menu even after signing off from the Microsoft RDS broker.	There is no workaround.
DTOS-29240	[CWA Native Mode] The Citrix Broker does not sign out from Native mode after the client remains idle for 15–30 minutes.	Use the ThinOSsign-offf menu to sign off from the Citrix broker.
DTOS-29654	ICA desktop stops responding when reloading a BCR video URL 3-4 times.	Close browser of sign off session.
DTOS-29029	The keyboard stops working after refreshing the Chrome browser with the BCR extension enabled.	Switch session to client desktop, then switch back to the session; the keyboard should work.
DTOS-29182	VMware Blast: Encoder settings change is not taking effect on the first attempt.	Sign off from the broker and sign in again.
DTOS-29904	NumLock/CapLock status changes locally when launching a Blast/PCoIP session.	Press the NumLock/CapLock key again to correct the status.
DTOS-30031	When changing the Remote Connection Settings, the AWS login window is lost.	Reboot the thin client.
DTOS-29892	The new Citrix toolbar position cannot be moved or expanded after closing and opening the laptop lid.	See the ThinOS 2411 release note; disable the virtual desktop screen resizing feature.
DTOS-29893	The Citrix session desktop does not display correctly after closing and opening the laptop lid.	See the ThinOS 2411 release note; disable the virtual desktop screen resizing feature.
DTOS-29897	[Bluetooth] Volume increase or decrease not working in UC profile [AirPods].	There is no workaround.

5

ThinOS 2408

Release details

Release date

September 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 2408 (9.5.3102)

Previous version

ThinOS 2405 (9.5.2109)

Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2408 (9.5.3102)**

ⓘ **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2408. You must upgrade to ThinOS 9.1.3129 or later versions before upgrading to the latest version of ThinOS 9.x.

ⓘ **NOTE:** To downgrade ThinOS 2408 to a version earlier than 9.1.3129, use the ThinOS Merlin image.

For more information, see the *Dell ThinOS 2402, 2405, and 2408 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 2311, 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**. The ThinOS 2408 is updated to follow the **WMS Security Policy** > **TLS Security Level** (default = 1). If your network environment requires a legacy OpenSSL version, must change TLS security level to 0, when updating to 2408. Otherwise, device can lose network. Legacy OpenSSL versions are not supported on future ThinOS versions. If a Legacy OpenSSL version is required, update your environment.
- From ThinOS 2408, the `VMware Horizon Session SDK` package is no longer supported. It is recommended to upgrade ThinOS clients in the environment to the `VMware Horizon Client SDK` package to avoid issues.
- Our goal at Dell is to ensure all ThinOS offerings have the broadest range of virtual computing broker and protocol capabilities. To achieve this goal, periodic changes are required to align with your needs. From 2024-11-02, `Teradici`

`PCoIP` package and **Teradici PCoIP license entitlement** are no longer included on newly manufactured ThinOS 2408 devices. The following issues are expected:

  - Attaching to VMware environments is not impacted. You can continue to use the `VMware Horizon Client SDK` package to attach to VMware Horizon Servers using Blast, PCoIP, or Remote Desktop protocols.
  - Attaching to Amazon WorkSpaces environments are limited to WorkSpace Streaming Protocol (WSP). You must use Wyse Management Suite Pro to download the `Teradici PCoIP` package and allocate a ThinOS Activation License if you are using PCoIP protocol connections to Amazon WorkSpace.
  - Attaching to Teradici Cloud Access Software (HP Anywhere) and PCoIP Host Card environments are discontinued. You must use Wyse Management Suite Pro to download the `Teradici PCoIP` package and allocate a ThinOS Activation License.

- The ThinOS Activation License is a dual-purpose license managed by WMS Pro. It is used for:
  - Enabling virtual connections on devices converted from an alternative operating system to ThinOS.
  - Enabling PCoIP entitlement on ThinOS devices, including ThinOS 8.6 devices without PCoIP and all ThinOS client devices manufactured on or after 2024-11-02. This is done when the ThinOS policy managed by WMS is enabled using **Services** > **WDA Settings** > **Enable PCoIP Activation License**.
- To improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are removed in the future release. Some TLS ciphers are not secure and are subject to change in the future release.

Table 47. TLS Cipher list

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Disabled by default in the future release
ECDHE-RSA-AES256-SHA384	Disabled by default in the future release
ECDHE-RSA-AES128-SHA	Removed in future release
ECDHE-RSA-AES256-SHA	Removed in future release
DHE-RSA-AES128-GCM-SHA256	Removed in future release
DHE-RSA-AES256-GCM-SHA384	Removed in future release
DHE-RSA-AES128-SHA256	Removed in future release
DHE-RSA-AES256-SHA256	Removed in future release
DHE-RSA-AES128-SHA	Removed in future release
DHE-RSA-AES256-SHA	Removed in future release
AES128-SHA256	Removed in ThinOS 2303
AES256-SHA256	Removed in ThinOS 2303
AES128-SHA	Removed in ThinOS 2303
AES256-SHA	Removed in ThinOS 2303
AES128-GCM-SHA256	Removed in ThinOS 2303
AES256-GCM-SHA384	Removed in ThinOS 2303
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Disabled by default in the future release
ECDHE-ECDSA-AES256-SHA384	Disabled by default in the future release
ECDHE-ECDSA-AES128-SHA	Removed in future release
ECDHE-ECDSA-AES256-SHA	Removed in future release
DHE-PSK-AES128-GCM-SHA256	Removed in future release
DHE-PSK-AES256-GCM-SHA256	Removed in future release

Table 47. TLS Cipher list (continued)

Ciphers	Security Status
DHE-PSK-AES128-CBC-SHA256	Removed in future release
DHE-PSK-AES256-CBC-SHA384	Removed in future release
DHE-PSK-AES128-CBC-SHA	Removed in future release
DHE-PSK-AES256-CBC-SHA	Removed in future release
ECDHE-PSK-AES128-CBC-SHA	Removed in future release
ECDHE-PSK-AES256-CBC-SHA	Removed in future release
ECDHE-PSK-AES128-CBC-SHA256	Disabled by default in the future release
ECDHE-PSK-AES256-CBC-SHA384	Disabled by default in the future release
PSK-AES128-GCM-SHA256	Removed in future release
PSK-AES256-GCM-SHA384	Removed in future release
PSK-AES128-CBC-SHA	Removed in future release
PSK-AES256-CBC-SHA	Removed in future release
PSK-AES128-CBC-SHA256	Removed in future release
PSK-AES256-CBC-SHA384	Removed in future release
RSA-PSK-AES128-GCM-SHA256	Removed in future release
RSA-PSK-AES256-GCM-SHA384	Removed in future release
RSA-PSK-AES128-CBC-SHA	Removed in future release
RSA-PSK-AES256-CBC-SHA	Removed in future release
RSA-PSK-AES128-CBC-SHA256	Removed in future release
RSA-PSK-AES256-CBC-SHA384	Removed in future release
ECDHE-ECDSA-CHACHA20-POLY1305	Removed in future release
ECDHE-RSA-CHACHA20-POLY1305	Removed in future release
DHE-RSA-CHACHA20-POLY1305	Removed in future release
RSA-PSK-CHACHA20-POLY1305	Removed in future release
DHE-PSK-CHACHA20-POLY1305	Removed in future release
ECDHE-PSK-CHACHA20-POLY1305	Removed in future release
PSK-CHACHA20-POLY1305	Removed in future release
SRP-RSA-AES-256-CBC-SHA	Removed in future release
SRP-AES-256-CBC-SHA	Removed in future release
SRP-RSA-AES-128-CBC-SHA	Removed in future release
SRP-AES-128-CBC-SHA	Removed in future release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

- There are chances that after the upgrade, the device displays a black screen. Reboot the device to boot it up correctly.
- From ThinOS 2303, the firmware update sequence is changed to **BIOS** > **OS** > **Application**.
- From ThinOS 2303, if the thin client is registered in Wyse Management Suite group 1 and you set the Wyse Management Suite group 2 token in group 1 policy, a dialog box is displayed to change the group. Click **Cancel** to change to group 2 immediately. Click **Restart Now** or wait for the 60-second countdown to finish and then reboot to change to group 2.

- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you 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 published in the same group, the thin client does not download it.
  - 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 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 ThinOS, 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 2408 (9.5.3102) 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 2408 (9.5.3102) 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: The upgrade can be failed sometimes when the event log is failed to install. You can reboot the device and upgrade again.

   NOTE: Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2408. Ensure to install the latest application packages.

Convert Ubuntu with DCA to ThinOS 2408

Prerequisites

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

Table 48. 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, 2405, and 2408 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 2408.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2408.
- 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, 2405, and 2408 Migration Guide* at Support | Dell.
- Ensure you have downloaded the Ubuntu to ThinOS 2408 conversion image.
- Extract the Ubuntu to ThinOS 2408 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.3-dtos3-amd64_signed.tar.gz` and ThinOS image `ThinOS_2405_9.5.3102.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_2405_9.5.3102.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 conversion, ThinOS is in the factory default status. ThinOS must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

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

ⓘ **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 49. 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 the 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 2408, it is recommended to install the latest application packages mentioned in the below table.

Table 50. ThinOS application package details

ThinOS application package details
Amazon_WorkSpaces_Client_ 24.0.4707.8.pkg
Cisco_Jabber_14.3.1.308744.9.pkg
Cisco_Webex_Meetings_VDI_44.6.2.3.4.pkg
Cisco_Webex_App_VDI_44.6.0.30048.2.pkg
Citrix_Workspace_App_24.2.0.65.17.pkg
Common_Printing_1.0.0.26.pkg
ControlUp_VDI_Agent_2.2.24.pkg
eG_VM_Agent_7.2.10.9.pkg
EPOS_Connect_7.8.1.3.pkg

Table 50. ThinOS application package details (continued)

ThinOS application package details
HID_Fingerprint_Reader_210217.24.pkg
Identity_Automation_QwickAccess_2.1.0.7.pkg
Imprivata_PIE_7.11.001.0045.48.pkg
Jabra_8.5.8.7.pkg
Lakeside_Virtual_Agent_99.0.0.173.12.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.7.0.3.4.pkg
Microsoft_AVD_2.6.2384.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_24.03.2.10.pkg
ThinOS_Telemetry_Dashboard_1.1.0.6.pkg
UXM_Endpoint_Agent_2024.07.11.6.pkg
VMware_Horizon_ClientSDK_2406.8.13.0.10.pkg
Zoom_Universal_6.0.11.25150.1.pkg

Important notes

- After upgrading to ThinOS 2408, 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 2408 (9.5.3102)—`ThinOS_2408_9.5.3102.pkg`
- Ubuntu to ThinOS 2408 conversion build—`ThinOS_2408_9.5.3102_Ubuntu_Conversion.zip`

Tested BIOS versions and BIOS packages

The following table contains the tested BIOS versions and BIOS packages for ThinOS 2408.

Table 51. Tested BIOS versions and BIOS packages

Supported platform	Tested BIOS version	New BIOS package
Wyse 5070 Thin Client	1.31.0	Not Applicable
Wyse 5470 All-in-One Thin Client	1.26.0	bios-5470AIO_1.26.0.pkg
Wyse 5470 Mobile Thin Client	1.25.0	bios-5470_1.25.0.pkg
Dell OptiPlex 3000 Thin Client	1.20.0	bios-Op3000TC_1.20.0.pkg
Dell Latitude 3420	1.36.0	bios-Latitude_3420_1.36.0.pkg
Dell OptiPlex 5400 All-in-One	1.1.41	bios-OptiPlex5400AIO_1.1.41.pkg
Dell Latitude 3440	1.15.0	bios-Latitude3440_1.15.0.pkg
Dell Latitude 5440	1.16.0	bios-Latitude5440_1.16.0.pkg
Dell Latitude 5450	1.6.0	bios-Latitude5450_1.6.0.pkg
Dell OptiPlex AIO 7410	1.16.0	bios-OptiPlexAIO7410_1.16.0.pkg

Table 51. Tested BIOS versions and BIOS packages (continued)

Supported platform	Tested BIOS version	New BIOS package
Dell OptiPlex AIO 7420	1.6.1	bios-OptiPlexAIO7420_1.6.1.pkg

Wyse Management Suite and Configuration UI packages

- Wyse Management Suite version 4.4
- Configuration UI package 1.10.415

NOTE: Use Wyse Management Suite 4.4 or later versions server for the new Wyse Management Suite ThinOS 9.x Policy features.

NOTE: Configuration UI package 1.10.415 must be installed separately with the Wyse Management Suite 4.4 server.

Feature Matrices

Citrix Workspace App feature matrix

Table 52. Citrix Workspace App feature matrix

Feature		ThinOS 2408 with CWA 2402	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Secure Private Access	Not Supported	Not Supported
	Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Not Supported	Not Supported
	SaaS/Web apps with SSO	Not Supported	Not Supported
	Citrix Mobile Apps	Not Supported	Not Supported
	App Personalization service	Not Supported	Not Supported
Workspace Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	Not Supported	Not Supported
	Citrix Auto updates	Not Supported	Not Supported
	Client App Management	Not Supported	Not Supported
User Interface	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	SDWAN support	Not Supported	Not Supported
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not Supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
	TWAIN 2.0	Not supported	Not supported
HDX Integration	Local App Access	Not Supported	Not Supported
	Multi-touch	Not Supported	Not Supported
	Mobility Pack	Not Supported	Not Supported
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR)

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
			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, 2405, and 2408 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, 2405, and 2408 Administrator's Guide* at Support | Dell.
	Unified Communication Cisco Webex Meetings Optimization	Supported	Dell Technologies recommends to wait for 10 seconds to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
			configured by DHCP Option 252. For more information, see the *Dell ThinOS 2402, 2405, and 2408 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, 2405, and 2408 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, 2405, and 2408 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.
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	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	Not supported	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, 2405, and 2408 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.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Supported	There are no limitations in this release.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	User Cert Auth via NetScaler Gateway (via Browser Only)	Not supported	Not supported
	User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	Not supported	Not supported
	ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor authentications are not qualified.
	ADC Full VPN	Not supported	Not supported
	ADC Native OTP	Supported	There are no limitations in this release.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	PingID SAML MFA	Supported	There are no limitations in this release.
	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 qualified	Not qualified
	Citrix cloud + Active Directory + Token	Not qualified	Not qualified
	Citrix cloud + Citrix Gateway	Not qualified	Not qualified
	Citrix cloud + Okta	Not qualified	Not qualified
	Citrix cloud + SAML 2.0	Not qualified	Not qualified
	Netscaler load balance	Not qualified	Not qualified
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported	There are no limitations in this release.

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session launched (Client Setting in ThinOS)	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard setting in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Synchronize multiple keyboards at session start	Not Supported	Not Supported
	Enhancement for composite USB auto-redirection	Not Supported	Not Supported
	Loss tolerant mode for audio	Not Qualified	Not Qualified
	Enable Packet Loss Concealment to improve audio performance	Not Supported	Not Supported
	Version upgrade for Chromium Embedded Framework	Not Supported	Not Supported
	Enhancement to multiple monitors	Not Supported	Not Supported

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	Support for GTK3	Supported	There are no limitations in this release.
	Availability of Credential Insertion SDK for cloud stores	Not Supported	Not Supported
	Improved UI for error messages	Not Supported	Not Supported
	Send feedback on Citrix Workspace app	Not Supported	Not Supported
	Introduction of a new command in Storebrowse	Not Supported	Not Supported
	Configure UDP port range for Microsoft Teams optimization	Not Supported	Not Supported
	Enhanced Desktop Viewer toolbar	Not Supported	Not Supported
	Customize toolbar	Not Supported	Not Supported
	Sustainability initiative from Citrix Workspace app	Not Supported	Not Supported
	Include system audio while screen sharing	Not Supported	Not Supported
	App Protection compatibility with HDX optimization for Microsoft Teams	Not Supported	Not Supported
	Fast smart card	Not Supported	Not Supported
	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 MJPEG webcams	Not Supported	Not Supported

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	Supports system certificate paths for SSL connection	Not Supported	Not Supported
	Enhanced virtual channel SDK	Not Supported	Not Supported
	Support for keyboard shortcut to switch between Full-screen and Window mode	Not Supported	Not Supported
	Policy tampering detection	Not Supported	Not Supported
	Webcam redirection and service continuity support for ARM64 devices	Not Supported	Not Supported
	Enable Packet Loss Concealment to improve audio performance	Not Supported	Not Supported
	Multi-touch support	Not Supported	Not Supported
	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, 2405, and 2408 Administrator's Guide* at Support | Dell
	Copy and paste files and folders between two virtual desktops	Not Supported	Not Supported

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	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.
	Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	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 users. In other words, after the user on the ThinOS client starts sharing screen or content, the option

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
			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, 2405, and 2408 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 (Public Technical Preview)	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
	Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported

Table 52. Citrix Workspace App feature matrix (continued)

Feature		ThinOS 2408 with CWA 2402	Limitations
	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 support experimental feature	Supported	There are no limitations in this release.
	App indicator icon	Not Supported	Not Supported
	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.
	Native mode	Supported	There are no limitations in this release.

NOTE: The features and product environments that are marked as not qualified are not tested by Dell Technologies and are found to be working with other users.

ThinOS AVD Client Feature Matrix

Table 53. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 2408
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)	Supported
	Remote App (Immersive)	Supported
Input	Keyboard	Supported
	Mouse	Supported
	Single Touch	Supported
Audio Visual	Audio in	Supported
	Audio out	Supported
	Camera	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
Redirections	Printer	Supported
	SmartCard	Supported
	USB (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	Supported
	Zoom Cloud Meeting Optimization	Supported
Authentication	TS Gateway	Supported
	NLA	Supported
	SmartCard	Limited support (Supports Microsoft Remote Desktop Services broker login.)
	Imprivata	Supported

VMware Horizon feature matrix

Table 54. VMware Horizon feature matrix

Category	Feature	Horizon Client SDK
Broker Connectivity	SSL certificate verification	Supported
	Disclaimer dialog	Supported
	UAG compatibility	Supported
	Shortcuts from server	Not Supported
	Pre-install shortcuts from server	Not Supported
	File type association	Not Supported
	Phonehome	Supported
Broker Authentication	Password authentication	Supported
	SAML authentication	Supported
	FIDO2 Authentication	Supported
	Single sign on	Supported
	RSA authentication	Supported
	Integrated RSA SecurID token generator	Not Supported
	Radius - Cisco ACS	Supported
	Radius - SMS Passcode	Supported
	Radius - DUO	Supported
	Radius - OKTA	Supported
	Radius - Microsoft Network Policy	Supported
	Radius - Cisco Identity Services Engine	Supported
	Kiosk mode	Supported
	Remember credentials	Supported
	Log in as current user	Not Supported
	Nested log in as current user	Not Supported
	Log in as current user 1-way trust	Not Supported
	OS biometric authentication	Not Supported
	Windows Hello	Not Supported
	Unauthentication access	Supported
Smartcard	x.509 certificate authentication (Smart Card)	Supported
	CAC support	Supported
	.Net support	Supported
	PIV support	Supported
	Java support	Supported
	Purebred derived credentials	Not Supported
	Device Cert auth with UAG	Supported
Desktop Operations	Reset	Only supported with VDI

Table 54. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
	Restart	Only supported with VDI
	Log off	Supported
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported
	Multiple connections	Supported
	Multi-broker/multi-site redirection - Universal	Not Supported
	App launch on multiple end points	Supported
	Auto-retry 5+ minutes	Supported
	Blast network recovery	Supported
	Time zone synchronization	Supported
	Jumplist integration (Windows 7-Windows 10)	Not Supported
Client Customization	Command line options	Not Supported
	URI schema	Not Supported
	Launching multiple client instances using URI	Not Supported
	Preference file	Not Supported
	Parameter pass-through to RDSH apps	Not Supported
	Non interactive mode	Not Supported
	GPO-based customization	Not Supported
Protocols supported	Blast Extreme	Supported
	H.264 - HW decode	Supported
	H.265 - HW decode	Supported
	Blast Codec	Supported
	JPEG / PNG	Supported
	Switch encoder	Supported
	BENIT	Supported
	Blast Extreme Adaptive Transportation	Supported
	RDP 8.x, 10.x	Supported
	PCoIP	Supported
Features / Extensions Monitors / Displays	Dynamic display resizing	Supported
	VDI windowed mode	Supported
	Remote app seamless window	Supported
	Multiple monitor support	Supported
	External monitor support for mobile	Not Supported
	Display pivot for mobile	Not Supported
	Number of displays supported	4
	Maximum resolution	3840x2160

Table 54. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
	High DPI scaling	Not Supported
	DPI sync	Not Supported
	Exclusive mode	Not Supported
	Multiple monitor selection	Supported
Input Device (Keyboard / Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported
	Relative mouse	Only supported with VDI
	External Mouse Support	Supported
	Local buffer text input box	Not Supported
	Keyboard Mapping	Supported
	International Keyboard Support	Supported
	Input Method local/remote switching	Not Supported
	IME Sync	Supported
Clipboard Services	Clipboard Text	Supported
	Clipboard Graphics	Not Supported
	Clipboard memory size configuration	Supported
	Clipboard File/Folder	Not Supported
	Drag and Drop Text	Not Supported
	Drag and Drop Image	Not Supported
	Drag and Drop File/Folder	Not Supported
Connection Management	IPv6 only network support	Supported
	PCoIP IP roaming	Supported
Optimized Device Redirection	Serial (COM) Port Redirection	Supported
	Client Drive Redirection/File Transfer	Not Supported
	Scanner (TWAIN/WIA) Redirection	Supported
	x.509 Certificate (Smart Card/Derived Credentials)	Supported
	Storage Drive Redirection	Not Supported
	Gyro Sensor Redirection	Not Supported
Real-Time Audio-Video	Audio input (microphone)	Supported
	Video input (webcam)	Supported
	Multiple webcams and microphones	Not Supported
	Multiple speakers	Not Supported
USB Redirection	USB redirection	Supported
	Policy: ConnectUSBOnInsert	Supported
	Policy: ConnectUSBOnStartup	Supported
	Connect/Disconnect UI	Not Supported
	USB device filtering (client side)	Supported

Table 54. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
	Isochronous Device Support	Only supported with VDI
	Split device support	Supported
	Bloomberg Keyboard compatibility	Only supported with VDI
	Smartphone sync	Only supported with VDI
Unified Communications	Skype for business	Not Supported
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Teams	Supported with VDI, RDS Hosted Desktops
	Cisco Webex Meeting	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams HID Headset	Supported with VDI, RDS Hosted Desktops
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops
	HTML5 Redirection	Not Supported
	Directshow Redirection	Not Supported
	URL content redirection	Not Supported
	MMR Multiple Audio Output	Not Supported
	UNC path redirection	Not Supported
	Browser content redirection	Not Supported
Graphics	vDGA	Only supported with VDI
	vSGA	Only supported with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Only supported with VDI
	AMD vGPU	Only supported with VDI
Mobile Support	Client-side soft keyboard	Not Supported
	Client-side soft touchpad	Not Supported
	Full Screen Trackpad	Not Supported
	Gesture Support	Not Supported
	Multi-touch Redirection	Not Supported
	Presentation Mode	Not Supported
	Unity Touch	Not Supported
Printing	VMware Integrated Printing	Supported

Table 54. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Client SDK
	Location Based Printing	Supported
	Native Driver Support	Not Supported
Security	FIPS-140-2 Mode Support	Supported
	Imprivata Integration	Supported
	Opswat agent	Not Supported
	Opswat on-demand agent	Not Supported
	TLS 1.1/1.2	Supported
	Screen shot blocking	Not Supported
	Keylogger blocking	Not Supported
Session Collaboration	Session Collaboration	Supported
	Read-only Collaboration	Supported
Updates	Update notifications	Not Supported
	App Store update	Not Supported
Other	Smart Policies from DEM	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported
	Nested - basic connection	Supported
	DCT Per feature/component collection	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported
	Auth Method - RSA SecurID	Supported
	Auth Method - X.509 Certificate (Smart Card)	Supported
	Auth Method - Device X.509 Certificate and Passthrough	Supported
	Auth Method - RADIUS	Supported
	Auth Method - SAML - 3rd Party Identity Provider	Supported

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

Table 55. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix

Feature	ThinOS 2408
Client access restriction	Supported
USB redirection	Not supported

Table 55. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix (continued)

Feature	ThinOS 2408
Audio input	Supported
Video input	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
Smart card (CAC and PIV readers)	Supported
Certificate for access control	Supported
Encryption at rest	Supported
Client customization	Not supported
YubiKey support	Not supported
Monitor support	Supported (Dual Monitor with 3840x2160 resolution)

What's new

Citrix Workspace App updates

The features of Citrix VDI on ThinOS 2408 are qualified with Citrix Workspace App package 24.2.0.65.17.

The following are the updates for Citrix Workspace App:

- Support Citrix Native Mode
- Support App Protection in Citrix Native Mode
- App Protection compatibility with HDX optimization for Microsoft Teams
- Support Microsoft Teams 2.x Optimization
- Enhance Generic USB redirection

Support Citrix Native Mode

With ThinOS 2408 and Citrix Workspace App 2402, added a support for Citrix Native Mode. Citrix Native mode uses the Citrix Linux binary to launch Citrix sessions, which can improve some Citrix features, like App Protection. But it has some limitations and considerations:

- It is a technical preview feature, not fully tested and may have issues.
- It is not compatible with most WMS settings for ThinOS. Only the settings that change the Citrix configuration INI files or the ThinOS local configuration are supported.

Citrix Native Mode enables you to customize the look and feel of your ThinOS to match the Linux native Citrix Workspace App layout of published applications and desktops. Citrix Native Mode displays both the ThinOS full taskbar and the virtual apps and desktops.

To enable Citrix Native Mode, go to the Admin Policy Tool or the Wyse Management Suite policy settings, enable the **Citrix Native Mode** check box in **Broker Settings** > **Citrix Virtual Apps and Desktops Settings**.

ⓘ **NOTE:** Citrix Native Mode can be enabled or disabled if you have already configured the system mode as Classic or Modern.

ⓘ **NOTE:** Ensure that Citrix Workspace Mode is disabled before enabling Citrix Native Mode.

The following are the important notes for Citrix Native mode:

- Citrix broker login mechanism in Citrix Native Mode is the same as Linux Citrix Workspace App binary.
- Ensure set the Citrix broker address as the full Citrix Storefront URL such as `https://test.storefront.com/citrix/store` if there are more than three stores in your Citrix Storefront server. If only set the Citrix broker address as Citrix Storefront FQDN server name and your Citrix Storefront server has more than three stores, the Citrix broker login gets fail or the client gets stuck during broker login. This is Citrix binary designment.
- The default credentials that are configured from Admin Policy Tool or Wyse Management Suite policy settings are only applicable for login the HTTPS protocol Citrix Storefront server which has enabled the **User name and password** and **HTTP Basic** authentication methods. If you do not setup default user credentials in the Admin Policy Tool or Wyse Management Suite policy settings, the Citrix Workspace login window is displayed on top of the ThinOS login window and ask you for login. For other Storefront and Citrix ADC authentication methods, do not set default credentials in the Admin Policy Tool or Wyse Management Suite policy settings.
- Ensure set correct default credentials in the Admin Policy Tool or Wyse Management Suite policy settings to log in Citrix Storefront server. If you set the wrong default credentials, you get locked when you try to login broker at the first time. This is Citrix binary designment.
- For the Citrix Storefront with smartcard authentication method, do not set default user credentials, otherwise, the smartcard PIN code dialog cannot be displayed.
- For Citrix Storefront SSPR feature, do not set default user credentials for login if you want to use SSPR feature. Citrix Storefront SSPR feature can only work with the Citrix Workspace login window.
- For Citrix ADC (Formally is NetScaler) 2FA or MFA login, Citrix Native Mode only accepts you to enter Citrix Gateway Fully Qualified Domain Name (FQDN) in ThinOS Remote Connection Broker Server address. Ensure to login using Citrix Workspace login window and manually select the correct Citrix store.
- Citrix Native mode supports authentication using FIDO2 with Citrix Enterprise Browser (CEB) when connecting to on-premises stores. To enable FIDO2 authentication for logging in to on-premises stores, do the following:
    1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
    2. In the **Citrix XML Settings**, click **Add Row**.
    3. In the Key field, enter **FIDO2Enabled** .
    4. In the Value field, enter **true** .
    5. Sign out or restart the device for the settings to take effect.
- About LDAP and RSA login
    - If your Citrix ADC gateway is configured like the primary authentication is LDAP and secondary authentication is RADIUS, the Citrix Workspace login window only accepts username without including the domain prefix or postfix. Ensure to input the password in **Passcode** field and input the passcode in **Password** field. This is the same as Linux Citrix Workspace app binary.
    - If your Citrix ADC gateway is configured like the primary authentication is RADIUS and secondary authentication is LDAP, ensure not including domain in the User name field.
- Support log in Citrix Storefront or NetScaler with Citrix Native Mode using anonymous proxy user, you must not set Proxy Application List = RTME in Admin Policy Tool or Wyse Management Suite policy settings.
- It is recommended to log off user from Citrix native mode using ThinOS sign-off menu, not using Citrix Workspace App Sign Out menu.
- Do not set default credentials when you log in Storefront using Anonymous user.

Enable Citrix Native Mode

Prerequisites

In the Citrix Storefront server, do the following:

1. Open **Citrix StoreFront**.
2. Select the store which you want to connect from ThinOS.
3. Click **Manage Authentication Methods**.
4. Ensure that **HTTP Basic** and **User name and password** are enabled, if you login the HTTPS protocol Citrix Storefront server using the default credentials configured from Admin Policy Tool or Wyse Management Suite policy settings.

Steps

1. From the **desktop** menu, click **System Setup** > **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. On the **Broker Setup** tab, select **Citrix Virtual Apps and Desktops** from the **Select Broker Type** drop-down list, and do the following:
   a. Select the **Native Mode** check box if you want to enable the native Citrix Workspace App based layout of published applications and desktops.
   b. In the **Broker Server** field, you can enter the Citrix NetScaler Gateway URL with FQDN server name or StoreFront URL.
   c. Click **OK** to save your settings.

   NOTE: Citrix Native Mode does not support **Auto Connect List**, **Enable automatic reconnection at logon**, and **Enable automatic reconnection** from button menu fields.

Unsupported WMS policy and Citrix Native Mode features

The following are the unsupported Wyse Management Suite policy settings:

- Broker Settings > Global Broker Settings
  - Multi Farm
  - Multi Logon
  - Stop Logon if Error
  - Sequential Domain
  - Multi Broker
  - Same Broker Type Failover
- Broker Settings > Citrix Virtual Apps and Desktop Settings
  - HTTP User Agent
  - Automatically Connect to Sessions
  - Automatically Reconnect from Button
  - Automatically Reconnect At Logon
  - Connection Timeout
  - WebLogin Timeout
  - Use External Engine for WebLogin
  - Login Expire Time
  - Password Expiry Notification
  - NetScaler/ADC Authentication Method
  - NetScaler/ADC Authentication using web-based login
  - CAG Ignore Default Gateway
  - Direct External Connection to the NetScaler/ADC (no beacons being used)
  - Send Domain to the NetScaler/ADC
  - NetScaler/ADC login Timeout
- Session Settings > Global Session Settings
  - Launch Only Once
  - On Desktop
  - Only Show and Launch the On Desktop Session Type
  - Reconnect
  - Disable Reset VM
  - Auto Connect
  - Single Connection
- Session Settings > Citrix Session Settings
  - Cursor Pattern (Deprecated)
  - Password Exprity Notification
  - Show Applications with KEYWORDS (Mandatory)
  - Seamless Window Mode
- Login Experience > Login Settings
  - Connection Manager
  - Login Use Smartcard Certificate Only
- Login Experience > Session Settings

- Login Experience > Smartcard Settings
- Personalization > Shortcut Keys
  - Fast Disconnect Settings
  - Fast Connect Settings

The following are the unsupported features in Citrix Native Mode:

- Citrix cloud login
- Citrix ADC server timeout
- PNAgent server
- Connection manager
- PNMenu icon
- HTTP protocol storefront login
- Logon Citrix Storefront or ADC using user pfx format certificate
- Preferences settings in Citrix native mode menu and Citrix Connection Center.

Limitations for Citrix Native Mode

- NativeAuth is displayed in the last logged in user in Wyse Management Suite if you use Citrix Workspace login window to login Citrix broker in Citrix Native mode. After logging into a VDI Broker with Citrix Workspace login window and locking the ThinOS, you must set a temporary password to unlock the system.
- **FIDO2 CEB** webview login window is displayed behind the ThinOS login window.
- Native mode displays time for around 8 seconds when you log in Citrix Storefront or NetScaler or reboot client then log in broker.
- **Windows** key and **Alt+Tab** shortcuts are not working inside VDA session in native mode.
- Resolution set under **Global Session** settings is not working.
- Disabled Map Clipboard under **Global Session** settings is not working.
- Disabled HDX Multimedia Redirection under **Citrix Session** settings is not working.
- Sometimes, the Citrix desktop viewer toolbar does not respond.
- The account selection window cannot refresh using keyboard up or down arrow when login Citrix broker using native mode.
- Keyboard Function keys **Alt+Tab** and **Fn+Alt+F4** in Citrix are not working. This issue occurs with Dell Pro Wireless Keyboard and Mouse KM5221W.
- Keyboard maximizes or minimizes key is not working in Citrix Native Mode. This issue occurs with Dell Pro Wireless Keyboard and Mouse KM5221W.

Support App Protection in Citrix Native Mode

From ThinOS 2408 and Citrix Workspace App 2402, the Citrix App Protection feature is supported. The App Protection component is in the Citrix Workspace App package. App Protection feature is only applicable for Citrix Native Mode.

This feature restricts the ability of clients to be compromised with keylogging and screen which is capturing malware. In the ThinOS client, you are restricted to install keylogging application. ThinOS also restricts you to capture screenshot through **ThinOS** > **Troubleshooting** > **Export Screenshot**.

ⓘ **NOTE:** There is a restriction to export screenshot from ThinOS if there is an active protected session.

For more information, see Citrix.

App Protection compatibility with HDX optimization for Microsoft Teams

From ThinOS 2408 and Citrix Workspace App 2402, Optimized Microsoft Teams supports screen sharing when the Citrix Workspace app is enabled with App Protection in the Desktop Viewer mode only. When you click Share content in Microsoft Teams, the screen picker provides the following options:

- **Window option to share any open app** - This option is displayed only if the VDA version is 2109 or later.
- Desktop option to share the contents on your VDA desktop.

ⓘ **NOTE:** For the Citrix Workspace app for Linux, the Desktop share option is disabled by default.

To enable the Desktop share option, do the following:

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In the **Citrix 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 **UseGbufferScreenSharing**.
6. In the Value field, enter **1**.
7. Sign out or restart the device for the settings to take effect.

For more information, see Citrix.

Support Microsoft Teams 2.x Optimization

Starting from ThinOS 2408 and Citrix Workspace App 2402, Citrix now supports optimization for Microsoft Teams 2.x. There are two limitations in your Citrix environment with the new Microsoft Teams:

- The new Teams Client does not install or run on Windows Server 2016. Microsoft recommends you to upgrade to Server 2019 or 2022.
- The new Teams Client does not support running as a Published (seamless) application. This is fixed in CVAD 2402 LTSR, CVAD 2203 LTSR CU5, and later.

For more information about the requirements, how to deploy the new Microsoft Teams client, and limitations, see Citrix and Microsoft.

Enhance Generic USB redirection

From ThinOS 2408 and Citrix Workspace App 2402, ThinOS controls the Citrix USB redirection behavior. The latest update in ThinOS now allows USB devices configured for USB redirection to automatically redirect into the VDA (Virtual Desktop Agent) desktop. This feature works whether the USB device is connected before the session starts or after the session is launched.

The following two options in Citrix Workspace under**Preferences** > **Devices tab** are enabled by default and should not be changed:

- When a session starts, connect devices automatically.
- When a new device is connected while a session is running, connect devices automatically.

To configure USB redirection, it is recommended to adjust the relevant Citrix policies as follows:

1. For Citrix Virtual Apps and Desktop 2206 and VDA 2206 and later versions, ensure that the two Citrix policies below are enabled.
   - Set Citrix policy **Allow existing USB devices to be automatically connected** with value **Automatically redirect available USB devices**.
   - Set Citrix policy **Allow newly arrived USB devices to be automatically connected** with value **Automatically redirect available USB devices**.
2. Sign out on the VDA desktop.

Microsoft RDP and AVD updates

Microsoft AVD package is updated to version 2.6.2384 in ThinOS 2408.

Supports FIDO2

From ThinOS 2408 and Microsoft AVD package version 2.6.2384, you can authenticate using FIDO2 security keys which do not require passwords when login AVD broker but does not support login AVD sessions. Open desktop requires user enter credentials again. This behavior improves for single-sign-on experience in next release. To enable FIDO2 authentication for login AVD broker, do the following:

1. Open **Wyse Management Suite policy**.
2. Go to **Broker Settings** > **Azure Virtual Desktops Settings**.
3. Enable **Enable Azure Virtual Desktop**.
4. Enable **Use External Engine for WebLogin**.
5. Go to **Browser Settings** > **Chrome Browser Settings**. Enable **Enable Browser**.

ⓘ **NOTE:** Ensure to install the Chrome Package to use the Chrome Browser.

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 AVD broker.

Supports FIDO2 devices such as Yubikey 5 NFC and Yubikey 5 Ci.

ⓘ **NOTE:** ThinOS only supports the Wyse Management Suite setting **Use External Engine for WebLogin** to enable or disable the FIDO2 authentication.

Teradici PCoIP updates

- Teradici version is updated to 24.03.2.10 in ThinOS 2408.
- For the devices manufactured before 2024-11-01:
  - **Devices with PCoIP enabled**: Retain the ability to use Teradici PCoIP without further action.
  - **Devices without PCoIP enabled**: Require a ThinOS Activation License to enable the Teradici PCoIP function.
- For the devices manufactured after 2024-11-01:
  - Teradici PCoIP is not enabled unless a ThinOS Activation License is installed.

VMware Horizon updates

- The `Horizon Client SDK` package is updated to `VMware_Horizon_ClientSDK_2406.8.13.0.10.pkg`.
- The **Blast** and **PCoIP** icons are updated.
- Added **WebLogin Timeout** setting:
  - Added **WebLogin Timeout** setting in **WMS/APT** > **Broker setting** > **VMware Horizon Setting** page.
  - Added the capability to specify a timeout in minutes for automatically closing the WebLogin page and reconnecting to the broker. Value Range: 0 to 300 minutes, where 0 means the page will never automatically close.
- Updated **WebLogin Use ThinOS Extension** to **WebLogin Use Chrome Browser** in **WMS/APT** > **Broker setting** > **VMware Horizon Setting** page.

  ⓘ **NOTE:** To use this function, the ThinOS chrome browser package must be installed.

- Supports **DPI** scaling in **Blast** and **PCoIP** session. **Blast** and **PCoIP** session enables you to change the DPI scaling of one session property. The range that it supports is from 100% to 300%. The value is stored on Horizon Broker Server. The change in scaling supports two scenarios.
  - Full-screen sessions when the multimonitor option is disabled in WMS settings.
  - Sessions launched in windowed mode.

DPI scaling change does not support application that is published by Horizon broker.

The maximum DPI is limited by the vertical lines of resolution as determined by Microsoft. For more information, see DPI-related APIs and registry settings.

ⓘ **NOTE:** On Blast Session, when Multimedia Redirection (MMR) video is played then the first frame of the video is displayed as black. This is a limitation from Fluendo. The HID button does not function for ending Microsoft Teams calls.

Amazon WorkSpaces Client with WSP updates

Amazon WorkSpaces Client package version is updated to 24.0.4707.8 in ThinOS 2408.

WebLogin use Chrome Browser

WebLogin use ThinOS Extension is changed to **WebLogin use Chrome Browser**.

Imprivata OneSign Authentication

MFR75A FIDO-2 card reader is supported in ThinOS PIW mode.

Cisco updates

Cisco Webex VDI

- The Cisco Webex VDI package version is updated to 44.6.0.30048.2.
- Fixed the VPN or other network configuration which makes the plugin stop responding when you start the plugin.

Cisco Webex Meetings

- The Cisco Webex Meetings package version is updated to 44.6.2.3.4.
- Fixed that the gray screen is displayed on Cisco VDI when the Citrix App protection is enabled.

Cisco Jabber

- The Cisco Jabber package version is updated to 14.3.1.308744.9.
- Fixed the cursor issue during SIP session refresh on the Jabber VDI screen.

Zoom updates

Zoom universal package version 6.0.11.25150.1 is supported as part of ThinOS 2408.

New features

- Added new color themes and visual overhaul in Zoom desktop application.
- Updated the global navigation toolbar. This feature allows you to click any item in the More menu to automatically pin it to the toolbar to keep frequently used products available for quick access. If you attempt to move all product tabs into the More menu, a notification message is displayed that at least one tab must remain active.
- Added a policy to force silent updates for the VDI Plugin.
- Improved the collaboration with Google Drive and Microsoft OneDrive files.
- Updated the icons and meeting visuals.
- Added personalized in-meeting toolbars.
- Updated the Multispeaker video layout.
- You can view the new share tab in the Multi-share tab.

Jabra update

Jabra package version 8.5.8.7 is supported in ThinOS 2408.

EPOS Connect update

EPOS Connect version 7.8.1.3 is supported in ThinOS 2408.

Liquidware Stratusphere UX Connector ID Agent update

Liquidware Stratusphere UX Connector ID Agent version 6.7.0.3.4 is supported in ThinOS 2408.

ControlUp updates

- The ControlUp package version 2.2.24 is supported in ThinOS 2408.
- Fixed Wi-Fi signal strength and operating system version display issues.
- Fixed **ControlUp_Client** Public IP does not display for VMware Session.

UXM Endpoint Agent

- The UXM Endpoint agent package version in ThinOS 2408 is `UXM_Endpoint_Agent_2024.07.11.6.pkg`.
- New features in UXM Endpoint Agent:
  - Added the latest application versions.
  - Added the latest information of machine warranty, model, and manufacturer.

ThinOS updates

Supports P2P connection with IPV6 environment

The remote P2P connection can work in an IPV6 environment.

Improved Boot Wizard screen

Added a new button and layout in the first boot wizard screens. For more information, see the *Dell ThinOS 2402, 2405, and 2408 Administrator's Guide* at Support | Dell.

Updated Dell logo on the ThinOS device

Updated the Dell logo on the ThinOS devices.

Wyse Management Suite and Admin Policy Tool updates

NOTE: Wyse Management Suite 4.4 server along with Configuration UI package 1.10.415 is required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

Updated Password Expiry Notification

Updated the password expiry notification for the Wyse Management Suite.

Added Device Action Post Package Update

- Added **Device Action Post Package Update** under **WDA** settings.
- Go to **Services** > **WDA Settings**, you can select Reboot or Shutdown from the Device Action Post Package Update list.

  NOTE: The option Shutdown cannot be supported when a BIOS update is selected without an OS or application package update.

Changed ThinOS Extension package name

- ThinOS Extension package name is changed to Chrome Browser.
- It is moved from the Dell category to Third Party.

Changed Extension Settings

Changed the Extension Settings to Browser Settings.

Added Chrome Browser Privilege

The Chrome Browser Privilege is added under Browser Settings. The following are the setting scenarios.

- Allow access to the Chrome settings on the device.
  - Chrome Browser settings and Chrome Browser Other Policy pages are displayed on the Admin Policy Tool.
  - You can add a Chrome connection on the device.
- Deny access to the Chrome settings on the device.
  - Chrome Browser settings and Chrome Browser Other Policy pages are not displayed on the Admin Policy Tool.
  - You cannot add a Chrome connection on the device.
- Deny access to the Chrome settings on the device but allow adding a Chrome connection.
  - Chrome Browser settings and Chrome Browser Other Policy pages are not displayed on the Admin Policy Tool.
  - You can add a Chrome connection on the device.

Added new options in Chrome Browser settings

- Enabled the **Save Local Created Sessions** option and the local created Chrome connections is not removed by WMS policy.
- **Auto Update**
  - **Enable auto update from Google**: Only auto update from Google official release site.
  - **Enable update from WMS**: Only update package which is published from WMS policy.
  - **Disable package update**: It does not update the package.
- Input **Browser User-Agent** to modify the HTTP User Agent for Chrome Browser.
- **Browser Idle in Minute** option only works with None broker. Set a value, then after idle time, below are behaviors.
  - If you have defined chrome connections which are set with auto launch on boot, all current Chrome Browser windows are auto closed, the auto launch on boot chrome connections are auto launched
  - If you have not defined chrome connections which are set with auto launch on boot, all current Chrome Browser windows are auto closed, and auto launch one blank chrome connection

Added Use Browser for Captive Portal Detection

1. Added **Use Browser for Captive Portal Detection** in **Network Configuration** > **Wireless Settings**.
2. Enable the **Use Browser for Captive Portal Detection** option. The Captive Portal Detection uses Chrome browser to do web authentication.

   NOTE: You must install the Chrome Browser application package to use this function.

Added Use External Engine for WebLogin

1. Added Use External Engine for WebLogin option in **Broker Settings** > **Azure Virtual Desktop Settings**.
2. Enable Azure Virtual Desktop. The default value is disabled.
3. If you use external engine for Azure web-based login, then you must enable this option and install the Chrome Browser package. Then enable **Enable Browser** option in **WMS Browser Settings** > **Chrome Browser Settings**.

   NOTE: You cannot single sign-on AVD sessions when enable **Use External Engine** for WebLogin

Added AD Group Query timeout

- Added AD Group Query timeout option in **Login Experience** > **Login Settings** > **Default Credentials**.

You must select Authenticate to the domain controller in Login Type, and the default value is 5. It sets a maximum seconds for waiting AD group query reply. Its range is from 0 to 60 seconds.

Added Allow Indirect AD Groups

Added Allow Indirect AD Groups option in **Login Experience** > **Login Settings** > **Default Credentials**.

You must select Authenticate to the domain controller in Login Type, and the default value is Disable.

When enable this option, include all groups which the you are belonged to directly or indirectly when query AD groups.

NOTE: After enabling this, a big latency of the reply from domain controller for AD group query and set a bigger value for AD Group Query Timeout. Only direct groups are queried for when the setting is disabled.

Added WebLogin Timeout setting in VMware Horizon Setting

It specifies a time in minutes to automatically close the WebLogin page and re-connect to the broker. 0 means never and the range is from 0 to 300 minutes.

Change Blast Session Settings to Horizon Session Settings

Changed **Enable Relative Mouse when launching Blast Session** to **Enable Relative Mouse when launching Horizon Session**.

Change PCoIP Session Settings to Teradici PCoIP Session Settings

- Changed **Relative Mouse when launching PCoIP session** to **Enable Relative Mouse when launching Teradici PCoIP session**.
- Changed **PCoIP Connection Settings** to **Teradici PCoIP Connection Settings**.

Change Horizon Blast Configuration Editor to Horizon Configuration Editor

Changed **Horizon Blast Key-Value** to **Horizon Key-Value**.

Added vUSB Device Name to USB Redirection Settings

Added vUSB Device Name for the **VUSB Force Redirection Settings row** and **VUSB Force Local Settings row**.

Added the Maximum Non-Compliant Time to the WDA settings

The default value is 0 (disabled). If the device is non-compliant on the WMS server for longer than this time, then the broker login is blocked.

You must check in the client to the WMS server to make the broker login available.

Added Teams Video Acceleration

Added **Teams Video Acceleration** option in **Session Settings** > **RDP and AVD Session Settings**. The default value is Enable.

If enable Teams video acceleration, then Video Accerlation supported codecs are VP8, VP9, H264 decoder, and H264 encoder.

Added Hide None Secure Message

Added the Hide none secure message setting in **Login Experience** > **Login Settings**. The default setting is disabled. When you enable this setting for HTTP Protocol Broker Server logon, the **Broker connection not secure** warning message is not displayed in ThinOS user login window.

Added Citrix Native Mode

Added the **Citrix Native Mode** setting in **Broker Settings** > **Citrix Virtual Apps and Desktops Settings**. For more information on how to enable Citrix Native Mode, see How to enable Citrix Native Mode. You must sign out or reboot the ThinOS device after enabling or disabling it. This setting enables Citrix Workspace App based layout and features of published apps and desktops. Ensure Citrix Workspace Mode is disabled before enabling Citrix Native Mode. App Protection feature is only applicable for Citrix Native Mode.

Tested environment and peripheral matrices

General tested environments matrices

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

Table 56. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.4
Configuration UI package for Wyse Management Suite	1.10.415
Citrix ADC (formerly NetScaler)	13.0 and later
StoreFront	1912 LTSR and later

Table 57. 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 (CU4)	Tested	Tested	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2402 LTSR	Tested	Tested	Tested	Tested	Tested	Tested

Table 58. Test environment—VMware Horizon View

VMware	Windows 11	Windows 10	Windows Server 2022	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 2312	Tested	Tested	Tested	Tested	Tested
VMware Horizon 2312.1	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2406	Tested	Tested	Tested	Not tested	Not tested

Table 59. Test environment – VMware Horizon Cloud Next Gen

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

Table 60. 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 61. 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 62. Test environment—Windows 365 cloud PC

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

Table 63. Test environment—Amazon WorkSpaces

Protocol	Authentication Method	Windows 2016	Windows 2019	Windows 2022
PCoIP	Standard	Tested	Not tested	Not tested
	MFA	Tested	Not tested	Not tested
WSP	Standard	Tested	Not tested	Not tested
	MFA	Not tested	Not tested	Tested
	SmartCard	Not tested	Tested	Not tested

Table 64. Tested environment—Skype for Business offloading

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 (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
	Windows server 2019				

Table 65. 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 (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10	14.3.1.308744.2	14.3.1.58744	14.3.0.58392
	Windows 11			
	Windows server 2016			
	Windows server 2019			

Table 66. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
- VMware Horizon 2209 - VMware Horizon View 7.13.2	Windows 10	14.3.1.308744.2	14.3.1.58744	14.3.0.58392
	Windows server 2016			
	Windows server 2019			

Table 67. 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 (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10	6.0.10.25100.3	6.0.11(25150)
	Windows 11		
	Windows server 2016		
	Windows server 2019		

Table 68. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
- VMware Horizon 2209 - VMware Horizon View 7.13.2	Windows 10	6.0.10.25100.3	6.0.11(25150)
	Windows server 2016		
	Windows server 2019		

Table 69. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	6.0.10.25100.3	6.0.11(25150)
	Windows server 2016		
	Windows server 2019		

Table 70. 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 (CU4)	Windows 10	44.6.0.30048.1	44.6.0.30048
	Windows 11		
	Windows server 2016		
	Windows server 2019		

Table 70. Tested environment—Cisco Webex Teams (continued)

Citrix VDI	Operating system	Webex App VDI	Webex Teams software
- Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows server 2022		

Table 71. 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	44.6.0.30048.1	44.6.0.30048
	Windows server 2016		
	Windows server 2019		

Table 72. 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 (CU4) - Citrix Virtual Apps and Desktops 7 2402 LTSR	Windows 10	44.6.2.3.1	44.9.0.400
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022		

Table 73. Tested environment—Cisco Webex Meetings

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
- VMware Horizon 7.12 - VMware Horizon 2209	Windows 10	44.6.2.3.1	44.9.0.400
	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 74. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

Product Category	Peripherals	5070	5470 AIO	5470
Audio Devices	Dell Pro Stereo Headset – UC150 – Skype for Business	Supported	Not Available	Supported
	Dell Pro Stereo Headset - Skype for Business - UC350	Supported	Supported	Supported
	Dell Professional Sound Bar (AE515M)	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Supported	Not Available	Supported
	Jabra PRO 935 USB MS Lync Headset	Supported	Not Available	Not Available

Table 74. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	- 935-15-503-185 - 935-15-503-185			
	Dell 2.0 Speaker System - AE215	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Supported	Supported
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Not Available	Supported
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Not Available	Supported
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Not Available	Supported
	Dell USB Wired Keyboard - KB216	Supported	Supported	Not Available
	Dell USB Wired Optical Mouse - MS116	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Supported	Supported
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K)	Supported	Supported	Not Available

Table 74. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	- DANAUBC087 - DANAUBC087			
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Supported	Not Available	Supported
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070	Not Available	Not Available	Supported
	Dell Adapter - USB-C to HDMI - DBQAUBC064 - DBQAUBC064	Supported	Not Available	Not Available
	Dell Adapter - USB-C to VGA - DBQBNBC064 - DBQBNBC064	Supported	Not Available	Not Available
	Trendnet USB to Serial Converter RS-232	Supported	Supported	Supported
	Dell Adapter - HDMI to DVI - DAUARBN004 - DAUARBN004	Not Available	Not Available	Supported
	Dell Adapter - HDMI to VGA - DAUBNBC084 - DAUBNBC084	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	Supported	Supported
Displays	E1916H	Supported	Supported	Not Available
	E1920H	Supported	Supported	Supported
	E2016H	Supported	Supported	Supported
	E2016Hv (China only)	Not Available	Not Available	Supported
	E2020H	Supported	Supported	Supported
	E2216H	Supported	Supported	Supported
	E2216Hv (China only)	Not Available	Not Available	Supported
	E2218HN	Not Available	Supported	Supported
	E2220H	Supported	Supported	Supported

Table 74. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	E2318H	Supported	Supported	Supported
	E2318HN	Supported	Not Available	Not Available
	E2417H	Supported	Supported	Supported
	E2420H	Supported	Supported	Supported
	E2420HS	Supported	Supported	Supported
	E2720H	Supported	Supported	Supported
	E2720HS	Supported	Supported	Supported
	P2016	Supported	Not Available	Not Available
	P2018H	Not Available	Not Available	Supported
	P2217	Supported	Not Available	Not Available
	P2217H	Supported	Not Available	Not Available
	P2219H	Supported	Not Available	Supported
	P2219HC	Supported	Not Available	Supported
	P2317H	Supported	Not Available	Not Available
	P2319H	Supported	Not Available	Supported
	P2415Q	Supported	Supported	Not Available
	P2417H	Supported	Not Available	Not Available
	P2418HT	Supported	Supported	Not Available
	P2418HZ	Supported	Not Available	Not Available
	P2419H	Supported	Supported	Supported
	P2419HC	Supported	Not Available	Supported
	P2421D	Supported	Not Available	Supported
	P2421DC	Supported	Not Available	Supported
	P2719H	Supported	Supported	Supported
	P2719HC	Supported	Not Available	Supported
	P2720D	Supported	Not Available	Supported
	P2720DC	Supported	Not Available	Supported
	P3418HW	Supported	Supported	Not Available
	P4317Q	Supported	Supported	Not Available
	MR2416	Supported	Not Available	Not Available
	U2415	Supported	Supported	Not Available
	U2419H	Supported	Supported	Supported
	U2419HC	Supported	Not Available	Supported
	U2518D	Supported	Supported	Not Available
	U2520D	Supported	Supported	Supported
	U2718Q (4K)	Supported	Supported	Supported
	U2719D	Supported	Supported	Supported

Table 74. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	5070	5470 AIO	5470
	U2719DC	Supported	Not Available	Supported
	U2720Q	Supported	Supported	Supported
	U2721DE	Supported	Supported	Supported
	U2421HE	Not Available	Supported	Supported
	U4320Q	Supported	Supported	Supported
	U4919DW	Supported	Not Available	Not Available
Networking	Add On 1000 Base-T SFP transceiver (RJ-45)	Supported	Not Available	Not Available
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Supported
Storage	Dell Portable SSD, USB-C 250GB	Supported	Not Available	Supported
	Dell External Tray Load ODD (DVD Writer)	Supported	Not Available	Supported
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported
	Sun microsystem SCR 3311	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Supported	Not Available	Supported
Printers	Dell Color Printer- C2660dn	Supported	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 75. 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

Table 75. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P
	Dell Premier Wireless ANC Headset - Blazer - WL7022
	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Slim Conferencing Soundbar - Lizzo - SB522A
	Dell Speakerphone - Mozart - SP3022
	Stereo Headset WH1022 (Presto)
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync - 202652-02 - 202652-02
Input Devices	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Bluetooth connection is not supported)
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_GREY - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_WHITE - MS116 - MS116 - Sapphire
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_Grey - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_WHITE - KB216 - KB216 - Rusty
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819 (Fingerprint reader is not supported)
	Dell Wireless Keyboard and Mouse - Auburn MLK - KM3322W
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726
	Dell Bluetooth Travel Mouse - MS700 - Black
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 19 Monitor E1920H - E1920H
	Dell 20 Monitor E2020H - E2020H
	Dell 22 Monitor - E2223HN - E2223HN
	Dell 22 Monitor - P2222H - P2222H
	Dell 23 Monitor - P2319H - P2319H - P2319H

Table 75. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell 24 Monitor - P2421 - P2421 - P2421
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 24 Monitor - P2422H - P2422H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 Monitor - P2722H - P2722H
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE
	Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
	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

Table 75. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Western Digital My Passport Ultra 1TB, Black - WDBYNN0010BBK-WESN - WDBYNN0010BBK-WESN
Camera	Logitech BRIO 4K Ultra HD Webcam - 960-001105 - 960-001105
	Logitech C525 HD Webcam - 960-000715 - 960-000715
	Logitech C930e HD Webcam - 960-000971 - 960-000971
	Dell Pro Webcam - Falcon - WB5023
	Dell UltraSharp Webcam - Acadia Webcam - WB7022

Supported ecosystem peripherals for Latitude 3420

Table 76. 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 (Supports USB dongle connection and not Bluetooth connection.)
	Dell Pro Wireless Keyboard and Mouse - Tasman (previously Windsor) - KM5221W
Audio/Video	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 77. 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 78. Supported ecosystem peripherals for Latitude 3440

Product Category	Peripherals
Displays	Dell 24 USB-C Hub Monitor - P2422HE
	Dell 27 Monitor - E2723HN

Table 78. Supported ecosystem peripherals for Latitude 3440 (continued)

Product Category	Peripherals
Input Devices	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Supports USB dongle connection and not Bluetooth connection.)
	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 79. 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 80. 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 81. 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 82. 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 83. Third-party supported peripherals

Product Category	Peripherals
Audio Devices	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth （Link 360 is the bluetooth dongle name.）
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Supports USB dongle connection and not Bluetooth connection.)
	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

Table 83. Third-party supported peripherals (continued)

Product Category	Peripherals
	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 supports 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
	Yealink WH66 (Limitation: The **Call** button works well with Skype for Business in Citrix. You can decline calls in Zoom meetings in Citrix, Blast, and RDP sessions. In other scenarios, only audio works and the **Call** button does not work. **NOTE:** The **Call** button does not work with Microsoft Teams in Blast after Microsoft Teams is updated to version 2.0.
Input Devices	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
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

Table 83. Third-party supported peripherals (continued)

Product Category	Peripherals
	Logitech C910 HD Pro Webcam
	Logitech C925e Webcam
	Poly EagleEye Mini webcam
	Logitech BRIO 4K Webcam
	Jabra PanaCast 4K Webcam
Storage	SanDisk cruzer 8 GB
	SanDisk cruzer 16G
	SanDisk USB 3.1 and Type-C 16 GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32 GB
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	IDBridge CT31 PIV
	Gemalto IDBridge CT710
	GemPC Twin
	Gemalto IDBridge CT30 V2
	Gemalto IDBridge CT30 V3
Proximity card readers	RFIDeas RDR-6082AKU
	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80

Table 83. Third-party supported peripherals (continued)

Product Category	Peripherals
	Imprivata HDW-IMP-82
	Imprivata HDW-IMP-82-BLE
	Imprivata HDW-IMP-80-MINI
	Imprivata HDW-IMP-82-MINI
	MFR75A Fido-2
	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.
- 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 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.

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 84. 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 CosmopoIC 64k V5.2	Supported	Supported	Supported
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c	Supported	Supported	Supported
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8	Supported	Supported	Not Available
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 7.0 (T=0)	Supported	Supported	Not Available
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported

Table 84. 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)
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available
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	YubiKey 4.3.3	Supported	Not Available	Supported

Table 84. 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)
		Cryptographic Provider v1.0				
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 85. Fixed issues

Issue ID	Description
DTOS-28545	There is a WMS Events error when changing the device exception policy.
DTOS-28352	SNMP tool runs a command and fails to provide the correct OID value.
DTOS-28349	Cherry MW 8C Ergo and Cherry DW 9500 Slim mouses drag-and-drop function is not working since 2405 version update.
DTOS-28246	The icon of new mail does not display on the **ThinOS VDI** menu bar when you click the new mail button in Outlook which is the RDS remote app and a new mail window is displayed.
DTOS-28245	Azure automatic login behavior is different based on the username.
DTOS-28072	ThinOS taskbar is disappeared when you open and maximize the published applications.
DTOS-27994	Last logged user in **WMS Cloud** is displayed as unknown.
DTOS-27768	The new Microsoft Teams application is failed to connect to calls or meetings in **AVD Session** when Optimization is configured.
DTOS-27726	The VPN client stops responding when an SSL CERT certificate is not present in ThinOS.

Table 85. Fixed issues (continued)

Issue ID	Description
DTOS-27725	A black screen is displayed, and the system screen flickers after ThinOS 2405 update. This issue occurs with Wyse 5470 Mobile Thin Client.
DTOS-27235	USB peripherals randomly stop responding on OptiPlex 3000 Thin Client.
DTOS-27062	**WLANReconnectCount** INI parameter equivalent is removed.
DTOS-27019	AVD is displaying a notification for credentials twice.
DTOS-26988	The last logged in user is displayed as null in the **Postman** tool.
DTOS-26767	Changing device level policy triggers the machine to restart immediately without any notification.
DTOS-26755	Unable to connect to Citrix broker server with **HTTPS protocol URL** after version 2402 upgrade.
DTOS-25910	Unable to connect to direct **RDP session** and failed to query user group from AD server.
DTOS-25667	A **Refresh Token Error** message is displayed in during **AVD session**.
DTOS-25091	**Fujitsu SP-112-N scanner** does not reattach to session after waking up from sleep mode.
DTOS-27832	Unable to log in to Azure with latest 2405 firmware.
DTOS-28189	Unable to connect to VPN with no password provided.
DTOS-28601	Device stops responding or recurring reboot issue after firmware update.
DTOS-28394	**CAPS Lock** & **Yen ¥** keys do not function correctly in the Japanese 109 Keyboard.
DTOS-28279	Login issue when using Horizon Client SDK - VMware UAG 2312 with **SAML Enabled** on Dell OptiPlex 3000 Thin Client
DTOS-28130	All menus are grayed out when you upgrade the device from ThinOS 2402 to ThinOS 2405.

Known Issues

Table 86. Known Issues

Key	Summary	Workaround
DTOS-28039	Able to create two RDP connections with the same name and the same hostname.	Not available.
DTOS-28327	The browser session shortcut does not list while switching system mode from classic to modern, or the opposite way.	Allow access to the Chrome settings on ThinOS device or do not click **Admin Policy** tool and **Save & Publish** button on ThinOS device.
DTOS-28562	USB disk is not detected after signing off from the RDS broker.	Re-plugin the USB disk.
DTOS-28792	**RDS Session** is not launched through Chrome Browser.	Not available.

Table 86. Known Issues (continued)

Key	Summary	Workaround
DTOS-26144	The device is resumed automatically from sleep mode when Bluetooth is connected.	Not available.
DTOS-26301	The device is not performing audio Bluetooth devices scan. Scan duration is short.	Not available.
DTOS-27849	Volume increases or decreases the UI is not working when you connect the Bluetooth Headsets.	Not available.
DTOS-28094	Debug information is not displayed after the successful connection of Open VPN.	Not available.
DTOS-28682	Dell 24 Video Conferencing Monitor - C2423H volume user interface is not synchronizing in Citrix VDI Session.	Adjust audio in **session** and **client** manually.
DTOS-28768	The Dell Latitude 5440 system makes a sound when you connect dual Monitor to the system. This issue occurs with Dell 24 Video Conferencing Monitor - C2423H.	Plug-out and plug-in the cable to the monitor.
DTOS-28338	During **Webex VDI** or **Zoom** calls, the video flickers when the mouse is hovered over the self-video window.	The issue occurs with Dell Latitude 3420 systems with reported configuration only.
DTOS-28554	Duplicate Event logs and duplicate session names are seen under Citrix Toolbar Switch.	Sign out or disconnect the Citrix session.
DTOS-27978	**eG_Device** details are not displayed in eG cloud.	Disable the **eG Agent** in WMS policy and enable again with the correct eG Manager.

6

ThinOS Smartcard Firmware 24.06 for Latitude 5450

Release details

Release date

June 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 Latitude 5450 Smartcard Firmware version 24.06

Package information

Lati5450_SmartCard_FW_24.06.2.pkg

Supported platform

Table 87. Supported platform

Supported platform
Dell Latitude 5450

Supported ThinOS versions

Table 88. Supported ThinOS versions

Supported ThinOS versions
ThinOS 2405 (9.5.2109)
ThinOS 2402 (9.5.1079)

Tested Wyse Management Suite and Configuration UI version

Table 89. Tested Wyse Management Suite and Configuration UI version

Wyse Management Suite version	Configuration UI package version for Wyse Management Suite
4.4	1.10.322

Upload and publish the Smartcard firmware package

Prerequisites

- Ensure that you are running ThinOS 2402 (9.5.1079) or ThinOS 2405 (9.5.2109) on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.

Steps

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

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

6. Click **Browse** and select `Lati5450_SmartCard_FW_24.06.2.pkg` to upload.

   ⓘ **NOTE:** Under the **Other** category, ensure that the switch option of **Other** is set to **INSTALL**.

7. Click to expand the **Other** dropdown list and select the uploaded package.
8. Click **Save & Publish**.
   The thin client downloads the package, installs it, and then restarts.

What's new

After installing this application package, the Latitude 5450 integrated Smartcard reader works.

You must manually reboot your Latitude 5450 device again to ensure that the Smartcard reader works in the following scenarios:

- Installing the application package in ThinOS 2402 and upgrading to ThinOS 2405.
- Installing the application package in ThinOS 2405 and downgrading to ThinOS 2402.

7

ThinOS 24.06.001 Hotfix

Release details

Release date

June 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 24.06.001

Previous version

ThinOS 2405 (9.5.2109)

Package information

ThinOS_Hotfix_24.06.001.1.pkg

Supported Platforms

Table 90. Supported platforms for ThinOS Hotfix 24.06.001

Supported platforms
Wyse 5070 Thin Client
Wyse 5470 All-in-One Thin Client
Wyse 5470 Mobile Thin Client
Dell OptiPlex 3000 Thin Client
Dell Latitude 3420
Dell OptiPlex 5400 All-in-One
Dell Latitude 3440
Dell Latitude 5440
Dell Latitude 5450
Dell OptiPlex AIO 7410
Dell OptiPlex AIO 7420

Supported ThinOS version

ThinOS 2405 (9.5.2109)

Upload and publish the ThinOS Hotfix package through Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 2405 (9.5.2109) on your thin client.
- Create a group in Wyse Management Suite with a group token.
- The thin client must be registered to Wyse Management Suite.

Steps

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

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

6. Click **Browse** and select the ThinOS Hotfix package to upload.
7. Click to expand the **Hotfix** dropdown list, and select the uploaded package.
8. Click **Save & Publish**.
   The thin client downloads the package, installs it, and then restarts.

Important Notes

- Configure this hotfix to the group where the operating system firmware is configured with ThinOS 2405 (9.5.2109).
- When you change the group policy and configure the operating system firmware other than ThinOS 2405 (9.5.2109), remove this hotfix package from the application package policy.
- If you install the hotfix package on a device that is not on ThinOS 2405 (9.5.2109), then update the operating system to ThinOS 2405. Reboot again for the update for the hotfix package to take effect.

What's new

Table 91. What's new in ThinOS Hotfix Patch 24.06.001

Issue	Root cause analysis	Fix details
DTOS-27326—The cloud or on-premises P2P connection cannot be established with a client that is connected through a wireless network only.	A device change in ThinOS 2405 impacted the cloud or on-premises P2P function with the wireless connection.	The issue has been fixed with this release.

8

ThinOS 2405

Release details

Release date

May 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 2405 (9.5.2109)

Previous version

ThinOS 2402

Firmware upgrade

The following firmware upgrade scenarios are supported:

- **9.1.3129 or later versions > ThinOS 2405 (9.5.2109)**

ⓘ **NOTE:** If your current version is earlier than 9.1.3129, you cannot upgrade to ThinOS 2405. 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 2405 to a version earlier than 9.1.3129, you must use ThinOS Merlin image.

For more information, see the *Dell ThinOS 2402 and 2405 Migration Guide* at Support | Dell. For the steps to access documents, see Resources and support.

Important notes

- ThinOS 2405 does not support Wyse 3040 devices.
- To further improve the security of ThinOS devices, from 2311, 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.
- Some features and product environments that are not tested by Dell Technologies are found to be working with other users. These features or product environments have been marked as **Not Qualified**.
- To further improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are going to be removed in the next release. Some TLS ciphers are not secure and are subject to change in the next release.

Table 92. TLS Cipher list

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Disabled by default in the next release
ECDHE-RSA-AES256-SHA384	Disabled by default in the next release
ECDHE-RSA-AES128-SHA	Removed in next release
ECDHE-RSA-AES256-SHA	Removed in next release
DHE-RSA-AES128-GCM-SHA256	Removed in next release
DHE-RSA-AES256-GCM-SHA384	Removed in next release
DHE-RSA-AES128-SHA256	Removed in next release
DHE-RSA-AES256-SHA256	Removed in next release
DHE-RSA-AES128-SHA	Removed in next release
DHE-RSA-AES256-SHA	Removed in next release
AES128-SHA256	Removed in ThinOS 2303
AES256-SHA256	Removed in ThinOS 2303
AES128-SHA	Removed in ThinOS 2303
AES256-SHA	Removed in ThinOS 2303
AES128-GCM-SHA256	Removed in ThinOS 2303
AES256-GCM-SHA384	Removed in ThinOS 2303
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Disabled by default in the next release
ECDHE-ECDSA-AES256-SHA384	Disabled by default in the next release
ECDHE-ECDSA-AES128-SHA	Removed in next release
ECDHE-ECDSA-AES256-SHA	Removed in next release
DHE-PSK-AES128-GCM-SHA256	Removed in next release
DHE-PSK-AES256-GCM-SHA256	Removed in next release
DHE-PSK-AES128-CBC-SHA256	Removed in next release
DHE-PSK-AES256-CBC-SHA384	Removed in next release
DHE-PSK-AES128-CBC-SHA	Removed in next release
DHE-PSK-AES256-CBC-SHA	Removed in next release
ECDHE-PSK-AES128-CBC-SHA	Removed in next release
ECDHE-PSK-AES256-CBC-SHA	Removed in next release
ECDHE-PSK-AES128-CBC-SHA256	Disabled by default in the next release
ECDHE-PSK-AES256-CBC-SHA384	Disabled by default in the next release
PSK-AES128-GCM-SHA256	Removed in next release
PSK-AES256-GCM-SHA384	Removed in next release
PSK-AES128-CBC-SHA	Removed in next release

Table 92. TLS Cipher list (continued)

Ciphers	Security Status
PSK-AES256-CBC-SHA	Removed in next release
PSK-AES128-CBC-SHA256	Removed in next release
PSK-AES256-CBC-SHA384	Removed in next release
RSA-PSK-AES128-GCM-SHA256	Removed in next release
RSA-PSK-AES256-GCM-SHA384	Removed in next release
RSA-PSK-AES128-CBC-SHA	Removed in next release
RSA-PSK-AES256-CBC-SHA	Removed in next release
RSA-PSK-AES128-CBC-SHA256	Removed in next release
RSA-PSK-AES256-CBC-SHA384	Removed in next release
ECDHE-ECDSA-CHACHA20-POLY1305	Removed in next release
ECDHE-RSA-CHACHA20-POLY1305	Removed in next release
DHE-RSA-CHACHA20-POLY1305	Removed in next release
RSA-PSK-CHACHA20-POLY1305	Removed in next release
DHE-PSK-CHACHA20-POLY1305	Removed in next release
ECDHE-PSK-CHACHA20-POLY1305	Removed in next release
PSK-CHACHA20-POLY1305	Removed in next release
SRP-RSA-AES-256-CBC-SHA	Removed in next release
SRP-AES-256-CBC-SHA	Removed in next release
SRP-RSA-AES-128-CBC-SHA	Removed in next release
SRP-AES-128-CBC-SHA	Removed in next release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

- There are chances that after the upgrade, the device displays a black screen. You may reboot the device to boot it up correctly.
- From ThinOS 2303, if the thin client is registered in Wyse Management Suite group 1 and you set the Wyse Management Suite group 2 token in group 1 policy, a dialog box is displayed to change the group. Click **Cancel** to change to group 2 immediately. Click **Restart Now** or wait for the 60-second countdown to finish and then reboot to change to group 2.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. 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 published in the same group, the thin client does not download it.
  - 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 2405 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.

Upcoming changes for ThinOS 2408

The following changes are going to occur as part of the next ThinOS release, which is ThinOS 2408:

- Starting from ThinOS 2405, the VMware Horizon Client SDK package is supported, which is a replacement for the earlier VMware Horizon Session SDK package. FromThinOS 2408, the VMware Horizon Session SDK package is going to be discontinued.
- After the ThinOS 2408 release, you are encouraged to upgrade your ThinOS clients in their environment to the VMware Horizon Client SDK package to avoid issues that prevent future firmware updates.
- Support for the Teradici PCoIP SDK package may be discontinued with ThinOS 2408, as it is under review. The following issues can also be expected:
    - Attaching to VMware environments is not impacted. You can continue to use the VMware Horizon Client SDK ThinOS package to attach to VMware Horizon Servers using Blast, PCoIP, or Remote Desktop protocols.
    - Attaching to Amazon WorkSpaces environments may be limited to WorkSpace Streaming Protocol (WSP) only. If you are using PCoIP protocol connections in Amazon WorkSpaces, it is recommended to transition to WSP environments soon.
    - Attaching to Teradici Cloud Access Software (HP Anywhere) and PCoIP Host Card environments may be discontinued. It is recommended that you contact your local Dell Sales representative for information pertaining to alterative endpoint solutions.

Prerequisites for firmware upgrade

Before you upgrade from ThinOS 9.1.x to ThinOS 2405, 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 2405 (9.5.2109) 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 2405 (9.5.2109) 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: Application packages that are released before ThinOS 2205 are removed automatically after upgrading to ThinOS 2405. Install the latest application packages.

Convert Ubuntu with DCA to ThinOS 2405

Prerequisites

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

Table 93. 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 and 2405 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 2405.
- Wyse Management Suite version 4.0 or later versions must be used to convert to ThinOS 2405.
- 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 and 2405 Migration Guide* at Support | Dell.
- Ensure you have downloaded the Ubuntu to ThinOS 2405 conversion image.
- Extract the Ubuntu to ThinOS 2405 conversion image to get the Conversion Installer file `DTOS_Ubuntu_Installer_1.3-dtos3-amd64_signed.tar.gz` and ThinOS image `ThinOS_2405_9.5.2109.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_2405_9.5.2109.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 is in the factory default status. ThinOS must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.

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

ⓘ **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 94. 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 2405, it is recommended to install the latest application packages from the below table.

Table 95. ThinOS application package details

ThinOS application package details
Amazon_WorkSpaces_Client_ 24.0.4707.6.pkg
Cisco_Jabber_14.3.0.308378.11.pkg
Cisco_Webex_Meetings_VDI_44.2.0.76.2.pkg
Cisco_Webex_App_VDI_44.2.0.28744.1.pkg
Citrix_Workspace_App_24.2.0.65.17.pkg
Common_Printing_1.0.0.26.pkg
ControlUp_VDI_Agent_2.2.13.pkg
eG_VM_Agent_7.2.10.9.pkg
EPOS_Connect_7.7.0.2.pkg

Table 95. ThinOS application package details (continued)

ThinOS application package details
HID_Fingerprint_Reader_210217.24.pkg
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_99.0.0.173.12.pkg
Liquidware_Stratusphere_UX_Connector_ID_Agent_6.7.0.2.2.pkg
Microsoft_AVD_2.5.2334.pkg
RingCentral_App_VMware_Plugin_23.2.20.1.pkg
Teradici_PCoIP_24.03.2.7.pkg
ThinOS_Telemetry_Dashboard_1.1.0.6.pkg
UXM_Endpoint_Agent_2024.04.26.1.pkg
VMware_Horizon_2312.1.8.12.1.5.pkg
VMware_Horizon_ClientSDK_2312.1.8.12.1.12.pkg
Zoom_Universal_5.17.10.24730.2.pkg

Important notes

- After upgrading to ThinOS 2405, 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.
- If you downgrade to previous ThinOS versions, Lakeside Virtual Agent, eG VM Agent, and UXM Endpoint Agent packages are removed automatically.

ThinOS build

- ThinOS 9.1.3129 or later versions to ThinOS 2405 (9.5.2109)—`ThinOS_2405_9.5.2109.pkg`
- Ubuntu to ThinOS 2405 conversion build—`ThinOS_2405_9.5.2109_Ubuntu_Conversion.zip`

Tested BIOS versions and BIOS packages

The following table contains the tested BIOS versions and BIOS packages for ThinOS 2405.

Table 96. Tested BIOS versions and BIOS packages

Supported platform	Tested BIOS version	New BIOS package
Wyse 3040 Thin Client	1.2.5	Not applicable
Wyse 5070 Thin Client	1.31.0	bios-5070_1.31.0.pkg
Wyse 5470 All-in-One Thin Client	1.25.0	bios-5470AIO_1.25.0.pkg
Wyse 5470 Mobile Thin Client	1.24.0	bios-5470_1.24.0.pkg
Dell OptiPlex 3000 Thin Client	1.18.0	bios-Op3000TC_1.18.0.pkg
Dell Latitude 3420	1.35.0	bios-Latitude_3420_1.35.0.pkg
Dell OptiPlex 5400 All-in-One	1.1.38	bios-OptiPlex5400AIO_1.1.38.pkg
Dell Latitude 3440	1.12.0	bios-Latitude3440_1.12.0.pkg

Table 96. Tested BIOS versions and BIOS packages (continued)

Supported platform	Tested BIOS version	New BIOS package
Dell Latitude 5440	1.13.0	bios-Latitude5440_1.13.0.pkg
Dell Latitude 5450	1.3.0	bios-Latitude5450_1.3.0.pkg
Dell OptiPlex AIO 7410	1.13.0	bios-OptiPlexAIO7410_1.13.0.pkg
Dell OptiPlex AIO 7420	1.4.1	bios-OptiPlexAIO7420_1.4.1.pkg

Wyse Management Suite and Configuration UI packages

- Wyse Management Suite version 4.4
- Configuration UI package 1.10.322

NOTE: Use Wyse Management Suite 4.4 server for the new Wyse Management Suite ThinOS 9.x Policy features.

NOTE: Configuration UI package 1.10.322 must be installed separately with Wyse Management Suite 4.4 server.

Feature Matrices

Citrix Workspace App feature matrix

Table 97. Citrix Workspace app feature matrix

Feature		ThinOS 2405 with CWA 2402	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Secure Private Access	Not Supported	Not Supported
	Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Not Supported	Not Supported
	SaaS/Web apps with SSO	Not Supported	Not Supported
	Citrix Mobile Apps	Not Supported	Not Supported
	App Personalization service	Not Supported	Not Supported
Workspace Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	Not Supported	Not Supported
	Citrix Auto updates	Not Supported	Not Supported
	Client App Management	Not Supported	Not Supported

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Not Supported	Not Supported
	HDX adaptive throughput	Not Supported	Not Supported
	SDWAN support	Not Supported	Not Supported
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not Supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	Only FAT32 and NTFS file systems on the USB disk are supported.
	TWAIN 2.0	Not supported	Not supported
HDX Integration	Local App Access	Not Supported	Not Supported
	Multi-touch	Not Supported	Not Supported
	Mobility Pack	Not Supported	Not Supported
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
			recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	File open in Citrix Workspace app	Not Supported	Not supported. No local file explorer on ThinOS.
	Location Based Services (Location available via API-description)	Not Supported	Not Supported
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	There are no limitations in this release.
	Video playback	Supported	There are no limitations in this release.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell ThinOS 2402 and 2405 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 and 2405 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

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
			authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell ThinOS 2402 and 2405 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 and 2405 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 and 2405 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.
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	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 and 2405 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.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Supported	There are no limitations in this release.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	User Cert Auth via NetScaler Gateway (via Browser Only)	Not supported	Not supported
	User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	Not supported	Not supported
	ADC nFactor Authentication	Supported	ThinOS currently supports ADC nFactor authentication such as Azure AD SAML MFA, OKTA SAML MFA, PingID SAML MFA, OTP. Other nFactor authentications are not qualified.
	ADC Full VPN	Not supported	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
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not qualified	Not qualified
	Netscaler load balance	Not supported	Not supported
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported	There are no limitations in this release.

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session launched (Client Setting in ThinOS)	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard setting in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Synchronize multiple keyboards at session start	Not Supported	Not Supported
	Enhancement for composite USB auto-redirection	Not Supported	Not Supported
	Loss tolerant mode for audio	Not Qualified	Not Qualified
	Enable Packet Loss Concealment to improve audio performance	Not Supported	Not Supported
	Version upgrade for Chromium Embedded Framework	Not Supported	Not Supported
	Support for GTK3	Supported	There are no limitations in this release.

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	Availability of Credential Insertion SDK for cloud stores	Not Supported	Not Supported
	Improved UI for error messages	Not Supported	Not Supported
	Send feedback on Citrix Workspace app	Not Supported	Not Supported
	Introduction of a new command in Storebrowse	Not Supported	Not Supported
	Configure UDP port range for Microsoft Teams optimization	Not Supported	Not Supported
	Enhanced Desktop Viewer toolbar	Not Supported	Not Supported
	Customize toolbar	Not Supported	Not Supported
	Sustainability initiative from Citrix Workspace app	Not Supported	Not Supported
	Include system audio while screen sharing	Not Supported	Not Supported
	App Protection compatibility with HDX optimization for Microsoft Teams	Not Supported	Not Supported
	Fast smart card	Not Supported	Not Supported
	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

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	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 and 2405 Administrator's Guide at Support | Dell
	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

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	Microsoft Teams enhancements-Configuring a preferred network interface	Not Supported	Not Supported
	Inactivity Timeout for Citrix Workspace app	Not Supported	Not Supported
	Screen pinning in custom web stores	Not Supported	Not Supported
	Support for 32-bit cursor	Supported	The black box around the cursor issue in Adobe Acrobat reader 32-bit still exists in Citrix HDX Pro 3D desktop. This issue is also reproduced in Citrix Workspace App Linux binary.
	Addition of client-side jitter buffer mechanism	Not Supported	Not Supported
	Background blurring and replacement for Citrix Optimized Teams	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported
	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

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	Email-based auto-discovery of store	Not Supported	Not Supported
	Persistent login	Not Supported	Not Supported
	Authentication enhancement for Storebrowse	Not Supported	Not Supported
	Support for EDT IPv6	Not Supported	Not Supported
	Support for TLS protocol version 1.3	Not Supported	Not Supported
	Custom web stores	Not Supported	Not Supported
	Authentication enhancement experimental feature	Not Supported	Not Supported
	Keyboard layout synchronization enhancement	Not Supported	Not Supported
	Multi-window chat and meetings for Microsoft Teams	Supported	There are no limitations in this release.
	Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
	Request control in Microsoft Teams	Supported	Users on ThinOS client cannot give control to other users. In other words, after the user on the ThinOS client starts sharing screen or content, the option Give control is present in the sharing toolbar, but it does not work when you give control to 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 and 2405 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

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	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
	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

Table 97. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2405 with CWA 2402	Limitations
	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 98. ThinOS AVD Client Feature Matrix

Category Supported	Features	ThinOS 2405
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

Table 98. ThinOS AVD Client Feature Matrix (continued)

Category Supported	Features	ThinOS 2405
	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	Supported
	Zoom Cloud Meeting Optimization	Supported
Authentication	TS Gateway	Supported
	NLA	Supported
	SmartCard	Limited support
	Imprivata	Supported

VMware Horizon feature matrix

Table 99. VMware Horizon session and client package versions

Horizon	Package version
Horizon Session SDK	`VMware_Horizon_2312.1.8.12.1.5.pkg`
Horizon Client SDK	`VMware_Horizon_ClientSDK_2312.1.8.12.1.12.pkg`

Table 100. 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

Table 100. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	SAML authentication	Supported	Supported
	FIDO2 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
	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

Table 100. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	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
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

Table 100. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Relative mouse	Only supported with VDI	Only supported with VDI
	External Mouse Support	Supported	Supported
	Local buffer text input box	Not Supported	Not Supported
	Keyboard Mapping	Supported	Supported
	International Keyboard Support	Supported	Supported
	Input Method local/remote switching	Not Supported	Not Supported
	IME Sync	Supported	Supported
Clipboard Services	Clipboard Text	Supported	Supported
	Clipboard Graphics	Not Supported	Not Supported
	Clipboard memory size configuration	Supported	Supported
	Clipboard File/Folder	Not Supported	Not Supported
	Drag and Drop Text	Not Supported	Not Supported
	Drag and Drop Image	Not Supported	Not Supported
	Drag and Drop File/Folder	Not Supported	Not Supported
Connection Management	IPv6 only network support	Supported	Supported
	PCoIP IP roaming	Supported	Supported
Optimized Device Redirection	Serial (COM) Port Redirection	Supported	Supported
	Client Drive Redirection/File Transfer	Not Supported	Not Supported
	Scanner (TWAIN/WIA) Redirection	Supported	Supported
	x.509 Certificate (Smart Card/Derived Credentials)	Supported	Supported
	Storage Drive Redirection	Not Supported	Not Supported
	Gyro Sensor Redirection	Not Supported	Not Supported
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

Table 100. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	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
	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

Table 100. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	Location Based Printing	Supported	Supported
	Native Driver Support	Not Supported	Not Supported
Security	FIPS-140-2 Mode Support	Supported	Supported
	Imprivata Integration	Supported	Supported
	Opswat agent	Not Supported	Not Supported
	Opswat on-demand agent	Not Supported	Not Supported
	TLS 1.1/1.2	Supported	Supported
	Screen shot blocking	Not Supported	Not Supported
	Keylogger blocking	Not Supported	Not Supported
Session Collaboration	Session Collaboration	Supported	Supported
	Read-only Collaboration	Supported	Supported
Updates	Update notifications	Not Supported	Not Supported
	App Store update	Not Supported	Not Supported
Other	Smart Policies from DEM	Supported	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported	Supported
	Nested - basic connection	Supported	Supported
	DCT Per feature/component collection	Not Supported	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported	Supported
	Auth Method - RSA SecurID	Supported	Supported
	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 101. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix

Feature	ThinOS 2405
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 24.2.0.65.17, and the package can install the Citrix Workspace App version 2402 on ThinOS. From ThinOS 2405, Citrix Workspace Mode can be enabled or disabled if you have already configured the system mode as **Classic** mode or Modern mode. Sign out or restart the device for the settings to take effect.

Enhanced Citrix Workspace Mode

- From ThinOS 2405, Citrix Workspace Mode can be enabled or disabled when you have already configured system mode as **Classic** or **Modern**.
- Sign out or restart the device for the settings to take effect.

Authentication using FIDO2 with Citrix Enterprise Browser (CEB) when connecting to on-premises stores

- From ThinOS 2405 and Citrix Workspace App 2402, administrators can configure the **Citrix Enterprise Browser (CEB) WebLogin Engine** 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 **Use External Engine for WebLogin**.
5. Ensure that **WebLogin Engine** is **CEB**.

   ⓘ **NOTE:** If you choose **CEB**, ThinOS uses Citrix Enterprise Browser (CEB) for WebLogin which is in the Citrix Workspace App package.

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.

ⓘ **NOTE:** An **Open Citrix Workspace Launcher** dialog box is displayed when logging in to the Citrix broker server. Check the **Always allow Broker URL** checkbox to open links of this type in the associated app, and click the **Open Citrix Workspace Launcher** button to trust this dialog box.

Supports gray cursor and deprecated invert cursor

- From ThinOS 2405 and Citrix Workspace App 2402, a gray cursor is used in ICA sessions.
- Inverted cursor is deprecated by Citrix, which means the setting **InvertCursorEnabled=true** or **InvertCursorEnabled=false** in Citrix Configuration Editor is not supported from CWA 2402 version.
- The **Cursor Pattern** setting is deprecated from Citrix Workspace App version 2402. The gray cursor is used, by default, in ICA sessions.

Nitgen Fingkey Hamster III Fingerprint USB device

From ThinOS 2405 and Citrix Workspace App 2402, Nitgen Fingkey Hamster III Fingerprint USB device redirection is supported in Citrix sessions. To enable Nitgen Fingkey Hamster III Fingerprint USB device redirection, do the following:

1. Open Admin Policy Tool or Wyse Management Suite policy.
2. Go to **Peripheral Management > USB Redirection > vUSB Force Redirect** .
3. Click **Add Row**.
4. In the **vUSB Force Redirect** field, enter `0x0a860602`.
5. Go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.
6. In the **Citrix INI Settings**, click **Add Row**.
7. From the **File** drop-down list, select **All_Regions.ini**.
8. From the **Operation** drop-down list, select **Add or Update**.
9. In the **Section** field, enter `Virtual Channels\Generic USB Redirection`.
10. In the **Key** field, enter `MaxUsbdevfsBuffer`.
11. In the **Value** field, enter `262144`.
12. Sign out or restart the device for the settings to take effect.

Citrix Workspace App limitations that also occur in the Linux Citrix Workspace app binary

- On Dell P2724DEB Monitor, the integrated Web camera does not work in Citrix-Zoom VDI Sessions when connected using the USB 2.0 port.
- Sometimes, HDX webcam preview fails for both 32bit and 64bit applications. As a workaround, close and reopen the application that is using the HDX webcam.
- Redirected touch does not work in Windows server operating system desktop in AIO clients.
- When a USB drive is mapped to a Citrix session, copying files takes time.

- When **Desktop Viewer Toolbar** is disabled, Generic USB Redirection does not work in Citrix sessions when the USB device is inserted after session starts. As a workaround, plug in the USB device before the session starts.

Microsoft RDP and AVD updates

Microsoft AVD package is updated to version 2.5.2334 in ThinOS 2405.

Default RDP connection

The default **Enable Default RDP Connection** icon must be enabled in **APT/WMS > Session Settings > RDP and AVD Session Settings** to appear in the session list. Click the default RDP icon, and then enter the host to connect to the RDP session.

ⓘ **NOTE:** The Default RDP Connection settings are temporary in ThinOS. If the sign-off broker or the client is restarted, your Default RDP settings become the default settings.

ⓘ **NOTE:** It is recommended that you use the Microsoft AVD package of ThinOS 2405 with ThinOS 2405 or 2402 firmware.

Teradici PCoIP updates

- Teradici version is updated to 24.03.2.7 in ThinOS 2405.

ⓘ **NOTE:** ThinOS 2405 is the last release that supports the Teradici PCoIP package.

VMware Horizon updates

- The Horizon Session SDK package is updated to `VMware_Horizon_2312.1.8.12.1.5.pkg`.
- The Horizon Client SDK package is updated to `VMware_Horizon_ClientSDK_2312.1.8.12.1.12.pkg`.

New features in ThinOS Horizon

- Added the **Blast codec** option in **Global settings** in the UI and Wyse Management Suite. When only **Blast codec** is enabled, the Blast session runs the Blast codec when possible. If the option is disabled in the configuration, Blast and ThinOS run in H.264 by default.
- Teams video call supports background blur. The current version only supports the default blur effect, while blurring other backgrounds are not supported, which is a VMware Horizon.limitation.

Horizon Client SDK supports FIDO2 authentication as same as Horizon Session SDK in ThinOS 2402

- FIDO2 enrollment and authentication in VMware Workspace One Access and Smartcard authentication in Azure MFA are supported.
- To use this function, the ThinOS Extension application package must be installed.

Amazon WorkSpaces Client with WSP updates

Amazon WorkSpaces Client package version is updated to 24.0.4707.6 in ThinOS 2405.

Cisco updates

Cisco Webex VDI

- The Cisco Webex VDI package version is `Cisco_Webex_App_VDI_44.2.0.28744.1`.
- Vidcast feature
  - You can record video using the camera.
  - You can upload local or USB videos.
  - You can share the recorded or uploaded videos in a meeting.
  - You can share a single video or an entire screen.

Cisco Webex Meetings

- The Cisco Webex Meetings package version is `Cisco_Webex_Meetings_VDI_44.2.0.76.2.pkg`.
- Wording changes to the user interface:
  - **They can join the meeting** to **Guests can join the meeting**.
  - **They wait in the lobby until the host admits them** to **They wait in the lobby until the host admits them**.
  - **They can't join the meeting** to **Guests can't join the meeting**.

Zoom updates

Zoom universal package version 5.17.10.24730.2 is supported as part of ThinOS 2405.

ControlUp updates

- The ControlUp package version is `ControlUp_VDI_Agent_2.2.13.pkg`.
- Fixed Wi-Fi signal strength and operating system version display issues.

Lakeside Virtual Agent updates

- The Lakeside Virtual Agent package version `Lakeside_99.0.0.173.12.pkg` is supported with ThinOS 2405.
- The Lakeside package version that is released with ThinOS 2402 is incompatible in ThinOS 2405.

UXM Endpoint Agent

- The UXM Endpoint agent package version, as part of ThinOS 2405, is `UXM_Endpoint_Agent_2024.04.26.1.pkg`.
- After enabling **UXM Endpoint Agent**, enter the appropriate values in **URL** and **Agent Key** fields for the date to be populated in the UXM site.

eG VM Agent

- The eG VM agent package version, which is released as part of ThinOS 2405, is `eG_VM_Agent_7.2.10.9.pkg`.
- After enabling the eG Agent, enter the appropriate values in the **Dell ThinOS Client Group Name**, **Remote Agent or eG Manager IP / Name**, and **Remote Agent or eG Manager Port** fields for the date to be populated in the eG site.

ThinOS updates

Disabled Sleep and Reset the system options when the updated process is deferred

- If you click **Next Reboot** or schedule the update time to defer the operating system, BIOS, or application installation, **Sleep** is hidden and **Reset the system settings** is disabled in the **Shutdown** window.
- If you click **Next Reboot** to defer the update process, the ThinOS client enters sleep mode using a sleep timer.
- If you schedule the update time to defer the update process, the ThinOS client cannot enter sleep mode using a sleep timer.

Device exception policy takes higher priority than Select Group policy when switching between child groups

- If **Enable Device Exception To Override Select Group Policy** is selected for the parent group on the Wyse Management Suite server, then the **Device Exception policy** takes higher priority than the **Select Group policy** when switching between child groups.

ⓘ **NOTE:** If enabled, the device needs a re-check in for the option to take effect.

Improved the ThinOS activation license error message in the login window

When the mouse hovers over the ThinOS Activation license error message in the login window a dialog box shows more details. The dialog box displays the following:

If your device has replaced the motherboard, please contact Dell service team to update the license. If your device is converted from other OS, please register it to WMS server to apply ThinOS activation license.

Improved the boot speed of ThinOS

From pressing the power button to displaying the ThinOS desktop, ThinOS boot speed is improved with the 2405 version.

Supports Wyse Management Suite server with IPv6

- Wyse Management Suite server 4.4 supports IPv6, and you can register the ThinOS client to the Wyse Management Suite server with IPv6 only.
- If IPv4 is disabled and only IPv6 is enabled in your network, it takes 5 to 10 minutes to register a new ThinOS client to the Wyse Management Suite server for the first time.
- After registration, you can publish the Wyse Management Suite policy to disable IPv4 on the ThinOS client.
- Then, the ThinOS client registers to the Wyse Management Suite server immediately after next reboot.

ⓘ **NOTE:** If IPv4 is disabled on the ThinOS client, the wired and wireless icons on the taskbar do not display the IPv6 address. You also cannot remote shadow (P2P) from the Wyse Management Suite server with IPv6.

Wyse Management Suite and Admin Policy Tool updates

ⓘ **NOTE:** Wyse Management Suite 4.4 server along with Configuration UI package 1.10.322 is required for the updates to Admin Policy Tool and Wyse Management Suite policy settings.

Added Extension Settings

- You must install the ThinOS Extension package on the ThinOS client to use **Extension Settings**. After installation, you can enable the Chrome browser and use it.
- ThinOS Extension application package is provided for private preview and production along with ThinOS 2405. It is recommended that you contact your local Dell Sales representative for access to this private offer with separate documentation.

- Without the ThinOS Extension package installed, the **Extension Settings** are blocked on the device.
- The ThinOS Extension package can only be installed from Wyse Management Suite by an IT administrator.
- The **Chrome Browser Settings** page is added in **Extension Settings**.
- Enable the **Enable Browser** option to use the Chrome browser in theThinOS client.
- You can add the Browser sessions from the ThinOS locally by going to **VDI Menu > Add Connection > Add Browser Connection**.
- If you click **Add Row** to add a browser session:
  - **Launch Show Mode** defines whether the browser session can be automatically launched and whether the browser session must be displayed always or displayed after the login broker.
  - **Launch Mode** sets the browser session window.
  - **Screen ID** defines the screen in which the browser session is going to be launched. Screen 0 is the main screen.
- You can enable **Show Home Button**, and enter the home page URL to see the home icon in the browser. You can select a resolution in the **Window Size for Normal Mode** drop-down list as the browser window resolution. The default resolution is 1024 x 768.
- You can enable the **Enable Download** option to download files in the Chrome browser.
- You can enable the **Enable Printer** option to use the printer with the Chrome browser. The option is under development.
- You can enable the **Enable Persistent User Data** option and log in to the broker with your username, password, and domain name. Then, your browser data is saved. If you disable this option, user data is cleared. Data of only one user is saved.
  - If you log in to the broker with the same username next time, your browser data is kept.
  - If you log in to the broker with a different username next time, the previous user data is cleared, and the current user data is saved.
  - If you disable the option, the user data is cleared automatically.
  - If you enable the **Enable to Clear Persistent User Data** option in the ThinOS local **Troubleshooting** window, the **Clear Browser Data** button is available. Click the button to clear the browser user data.
- You can enable **Enable Default Tabs**. If you enable, add rows for the **Default Tabs** list, and open a browser session, the URLs in the list are automatically launched as tabs in the browser.
- You can enable **Managed Bookmarks** and add rows to see the bookmark list in the browser.
- If you enable **Enable Allowed/Blocked List**, the applicable scenarios are as follows:
  - If you only add rows for **Allowed List**, then you can only access the URLs in the **Allowed List**. The other URLs are blocked.
  - If you only add rows for **Blocked List**, then you cannot access the URLs in the **Blocked List**. You can access all the other URLs.
  - If you add rows for both the **Allowed List** and **Blocked List**, then you cannot access the URLs in the **Blocked List**. You can access all the other URLs. If there is a conflict, **Allowed List** takes priority.
  - If you add one URL in both **Managed Bookmark** and **Blocked List**, then you can still access the URL.
- The **Chrome Browser Other Policy** page is also added in **Extension Settings**, where you can add rows for other Chrome policies.

Noise Cancellation

- Added **Noise Cancellation** in **Peripheral Management > Audio**.
- Enable this option to resolve audio issues with some softphone applications and also display audio issues with OptiPlex 3000 Thin Clients.

Background Color

- Added the **Background Color** option in **Personalization > Desktop > Background Info Settings**.
- You must enable the **Enable Background Info** option first, and then the **Background Color** option is displayed.
- You can set the background color for Background Info.

Background Transparency

- Added the **Background Transparency** option in **Personalization > Desktop > Background Info Settings**.
- You must enable the **Enable Background Info** option first, and then the **Background Transparency** option is displayed.
- You can set the background transparency for the Background Info by entering an integer from 0 to 10, and the background transparency gradually decreases.

Disable On Premise WebSocket Gateway

- Added the **Disable On Premise WebSocket Gateway** option in **Session Settings > RDP and AVD Session Settings**.
- The option is disabled by default.
- If enabled, the WebSocket is not used when connecting to sessions on premises through a gateway.

Enable Default RDP Connection

- Added the **Enable Default RDP Connection** option in **Session Settings > RDP and AVD Session Settings**.
- The option is disabled by default.
- If enabled, the default RDP icon is displayed in the session list.

Updated Granular Control of Background Info

Added **ThinOS Extension** in the **Granular Control of Background Info** list.

SHA384 and SHA512 options in CA Certificate Hash Type

Added new options **SHA384** and **SHA512** in **Privacy & Security > SCEP > SCEP Settings > CA Certificate Hash Type**.

Supports WDA Settings in Select Group policy

You can configure WDA Settings in **Services > WDA Settings** in the Select Group policy.

Allow BlastCodec decoding

- Added the **Allow BlastCodec decoding** option in **Session settings > Blast Session Settings**.
- To keep parity with the previous ThinOS, the default value is enabled.
- You can enable or disable the Blast codec decoding on thin clients with this setting.

Enable IPv4

Added **Enable IPv4** in **Network Configuration > Common Settings** to enable or disable IPv4 on ThinOS clients.

Boot Logo

- Added the **Boot Logo** option in **Personalization > User Experience Settings**.
- You can upload a 24 or 32-bit BMP image and select it as the boot logo. Then, the image replaces the Dell loading logo that is displayed when booting.
- The maximum file size is 5 MB, and the maximum image resolution is 1024x768.

UXM settings

Added **UXM settings** in **System Settings > Device Monitoring**.

eG Agent Configuration Editor settings

- Added **eG Agent Configuration Editor settings** in **System Settings > Device Monitoring**.

Updated the operating system firmware updates UI

- In the previous releases, all the operating system versions are displayed in a drop-down list.
- Now the operating system versions are displayed on the page directly.
- You can ignore the **Order** option as the option is going to be supported in the future only.

New application package categories

- eG VM Agent
- UXM Endpoint Agent

Added Imprivata PIE settings

- General logging level
- Clear logs on startup
- Enable agent auto restart
- Time period for maximum restarts
- Maximum number of restarts
- Enable windows activity logging

Updated wording of WebLogin Use External Engine and WebLogin Use ThinOS Extension

- **WebLogin Use External Engine** is updated to **Use External Engine for WebLogin** in **Broker Settings > Citrix Virtual Apps and Desktops Settings**.
- **WebLogin Use ThinOS Extension** is updated to **WebLogin Engine** in **Broker Settings > Citrix Virtual Apps and Desktops Settings**.

Tested environment and peripheral matrices

General tested environments matrices

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

Table 102. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	WMS 4.4
Configuration UI package for Wyse Management Suite	1.10.322
Citrix ADC (formerly NetScaler)	13.0 and later
StoreFront	1912 LTSR and later

Table 103. 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	Tested	Tested

Table 103. 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 2402 LTSR	Tested	Tested	Tested	Tested	Tested	Tested

Table 104. Test environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2022	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 2312	Tested	Tested	Tested	Tested	Tested
VMware Horizon 2312.1	Tested	Tested	Tested	Tested	Not tested

Table 105. Test environment – VMware Horizon Cloud Next Gen

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

Table 106. 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 107. 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 108. Test environment—Windows 365 cloud PC

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

Table 109. Test environment—Amazon WorkSpaces

Protocol	Authentication Method	Windows 2016	Windows 2019	Windows 2022
PCoIP	Standard	Tested	Not tested	Not tested
	MFA	Tested	Not tested	Not tested
WSP	Standard	Tested	Not tested	Not tested
	MFA	Not tested	Not tested	Tested
	SmartCard	Not tested	Tested	Not tested

Table 110. 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	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
	Windows server 2019				
	Windows server 2022 (Not tested)				

Table 111. 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	14.3.0.308378.11	14.3.0.308378.11	14.3.0.308378.11
	Windows 11			
	Windows server 2016			
	Windows server 2019			
	Windows server 2022 (Not tested)			

Table 112. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
• VMware Horizon 2209 • VMware Horizon View 7.13.2	Windows 10	14.3.0.308378.11	14.3.0.308378.11	14.3.0.308378
	Windows server 2016			
	Windows server 2019			

Table 113. 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	5.17.10.24730.2	5.17.10.24730.2
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 114. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
• VMware Horizon 2209 • VMware Horizon View 7.13.2	Windows 10	5.17.10.24730.2	5.17.10.24730.2
	Windows server 2016		
	Windows server 2019		

Table 115. Tested environment—Zoom

RDP/RDSH/AVD	Operating system	Zoom package	Zoom software
RDSH	Windows 10	5.17.10.24730.2	5.17.10.24730.2
	Windows server 2016		
	Windows server 2019		

Table 116. 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	44.2.0.28744.1	44.2.0.28744.1
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 117. 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	44.2.0.28744.1	44.2.0.28744.1
	Windows server 2016		
	Windows server 2019		

Table 118. 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	44.2.0.76.2	44.2.0.76.2
	Windows 11		
	Windows server 2016		
	Windows server 2019		
	Windows server 2022 (Not tested)		

Table 119. Tested environment—Cisco Webex Meetings

VMWare VDI	Operating system	Webex Meetings VDI	Webex Meetings software
● VMware Horizon 7.12 ● VMware Horizon 2209	Windows 10	44.2.0.76.2	44.2.0.76.2
	Windows server 2016		
	Windows server 2019		

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

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

Table 120. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO

Product Category	Peripherals	3040	5070	5470 AIO	5470
Audio Devices	Dell Pro Stereo Headset – UC150 – Skype for Business	Supported	Supported	Not Available	Supported
	Dell Pro Stereo Headset - Skype for Business - UC350	Supported	Supported	Supported	Supported
	Dell Professional Sound Bar (AE515M)	Supported	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Not Available	Supported	Not Available	Not Available
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Not Available	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Not Available	Supported	Supported
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0	Not Available	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available

Table 120. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell USB Wired Keyboard - KB216	Supported	Supported	Supported	Not Available
	DellUSB Wired Optical Mouse - MS116	Supported	Supported	Supported	Supported
	Dell Premier Wireless Mouse - WM527	Supported	Supported	Not Available	Supported
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white	Not Available	Not Available	Not Available	Not Available
	SEAL SHIELD MEDICAL GRADE OPTICAL (Mouse)	Not Available	Not Available	Not Available	Not Available
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white	Not Available	Not Available	Not Available	Not Available
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white	Not Available	Not Available	Not Available	Not Available
	Dell Wireless Mouse - WM126_BLACK - Rosewood	Not Available	Not Available	Not Available	Not Available
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Not Available	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Not Available	Supported	Not Available	Supported

Table 120. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

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

Table 120. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

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

Table 120. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	U2421HE	Not Available	Not Available	Supported	Supported
	U4320Q	Not Available	Supported	Supported	Supported
	U4919DW	Not Available	Supported	Not Available	Not Available
Networking	Add On 1000 Base-T SFP transceiver (RJ-45)	Not Available	Supported	Not Available	Not Available
Docking station	Dell Dock - WD19-C	Not Available	Not Available	Not Available	Supported
	Dell Thunderbolt Dock - WD19TB (Thunderbolt Display is not supported)	Not Available	Not Available	Not Available	Supported
Storage	Dell Portable SSD, USB-C 250GB	Not Available	Supported	Not Available	Supported
	Dell External Tray Load ODD (DVD Writer)	Not Available	Supported	Not Available	Supported
Smart Card Readers	Dell Smartcard Keyboard - KB813	Supported	Supported	Supported	Supported
	Dell keyboard KB813t	Supported	Supported	Supported	Supported
	Sun microsystem SCR 3311	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal SMART Card Reader - ST-1044U	Not Available	Supported	Not Available	Not Available
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0	Not Available	Supported	Supported	Supported
	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU	Not Available	Supported	Not Available	Supported
Printers	Dell Color Multifunction Printer - E525w	Supported	Not Available	Not Available	Not Available
	Dell Color Printer-C2660dn	Supported	Supported	Not Available	Not Available
	Dell Multifunction Printer - E515dn	Supported	Not Available	Not Available	Not Available

Supported ecosystem peripherals for OptiPlex 3000 Thin Client

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

Table 121. Supported ecosystem peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio Devices	Dell Pro Stereo Headset - Cortez - WH3022
	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Soundbar - AE515M - AE515M - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - AC511M - AC511M - Potential M
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo - MH3021P
	Dell Premier Wireless ANC Headset - Blazer - WL7022
	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Slim Conferencing Soundbar - Lizzo - SB522A
	Dell Speakerphone - Mozart - SP3022
	Stereo Headset WH1022 (Presto)
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync - 202652-02 - 202652-02
Input Devices	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Bluetooth connection is not supported)
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_GREY - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_WHITE - MS116 - MS116 - Sapphire
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_Grey - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_WHITE - KB216 - KB216 - Rusty
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819 (Fingerprint reader is not supported)
	Dell Wireless Keyboard and Mouse - Auburn MLK - KM3322W
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726
	Dell Bluetooth Travel Mouse - MS700 - Black
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 19 Monitor E1920H - E1920H

Table 121. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

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

Table 121. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	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 122. 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 123. 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 124. 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 125. 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 126. 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

Table 126. Supported ecosystem peripherals for Latitude 5450 (continued)

Product Category	Peripherals
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 127. 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 128. 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 129. Third-party supported peripherals

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

Table 129. Third-party supported peripherals (continued)

Product Category	Peripherals
	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
	Yealink WH66 (Limitation: The **Call** button works well with Skype for Business in Citrix and Microsoft Teams in Blast sessions. You can decline calls in Zoom meetings in Citrix, Blast, and RDP sessions. In other scenarios, only audio works and the **Call** button does not work.)
Input Devices	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	Elo ET2201L IntelliTouch ZB (Worldwide) - E382790
	Elo ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473
	Elo PCAP E351600 - ET2202L-2UWA-0-BL-G
Camera	Logitech C920 HD Pro Webcam
	Logitech HD Webcam C525

Table 129. Third-party supported peripherals (continued)

Product Category	Peripherals
	Microsoft LifeCam HD-3000
	Logitech C930e HD Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C910 HD Pro Webcam
	Logitech C925e Webcam
	Poly EagleEye Mini webcam
	Logitech BRIO 4K Webcam
	Jabra PanaCast 4K Webcam
Storage	SanDisk cruzer 8 GB
	SanDisk cruzer 16G
	SanDisk USB 3.1 and Type-C 16 GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32 GB
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	IDBridge CT31 PIV
	Gemalto IDBridge CT30 V2
	Gemalto IDBridge CT30 V3
	Gemalto IDBridge CT710
	GemPC Twin
Proximity card readers	RFIDeas RDR-6082AKU

Table 129. Third-party supported peripherals (continued)

Product Category	Peripherals
	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 130. Supported smart cards

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

Table 130. 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)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available

Table 130. Supported smart cards (continued)

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
A.E.T. Europe B.V. (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 131. Fixed issues

Issue ID	Description
DTOS-26435	The fingerprint reader is duplicating the biometry register.
DTOS-26389	Devices do not get an IP address when first booted after update to ThinOS 2402.

Table 131. Fixed issues (continued)

Issue ID	Description
DTOS-26202	On OptiPlex 3000 devices with ThinOS 2402, Horizon 2309 is disconnected after entering the password to unlock the session.
DTOS-26062	On OptiPlex 3000 devices with ThinOS 2402, the French keyboard layout does not pass through to the Citrix session after firmware upgrade.
DTOS-26061	Using YubiKey MFA authentication, the ICA connection screen remains on top of the login screen.
DTOS-25946	On OptiPlex 3000 devices with ThinOS 2402 and VMware Horizon 8.11 version, the WebEx camera issue is fixed.
DTOS-25945	Horizon Client SDK (.46) does not work with Smartcards when **Require Smartcard** is set to **Yes**.
DTOS-25909	On Wyse 5070 devices with ThinOS 2402, the audio and video does not work when connected through USB-C with a Dell P2724DEB Monitor.
DTOS-25908	On Wyse 5070 devices with ThinOS 2402, the audio playback, audio recording, and videos are not passed through USB-C when connected to Dell P2424HEB monitor.
DTOS-25705	On OptiPlex 3000 devices with ThinOS 2402 and Azure, an error message **Error: Could not add account. Please check your account and try again.** is displayed.
DTOS-25584	On OptiPlex 3000 devices with ThinOS 2402 and AVD, the RDP screen size changes after timeout.
DTOS-25341	The Zoom H5 audio recorder does not redirect into Citrix sessions.
DTOS-25092	On Wyse 5470 devices with ThinOS 2311, you cannot connect to RDP sessions by typing in different host names.
DTOS-24887	The Smartcard fails when the RDP session disconnects or reconnects.
DTOS-24885	In ThinOS 2311, there are local issues with the Dell P3424WEB monitor camera in VDI sessions.
DTOS-24877	Windows 7 session stops responding and cannot close the connection in ThinOS.
DTOS-24722	RDP Session error **Missed heartbeat threshold exceeded** is displayed.
DTOS-24483	G key reset does not work correctly.
DTOS-24359	OptiPlex 3000 devices have performance issues and stop responding in RDP sessions.
DTOS-24255	In ThinOS 2308, the WiFi stops responding or connects late in Citrix VDI sessions when moving between applications.
DTOS-24002	Keyboard layout issues when using P2P Remote shadow protocol.
DTOS-24001	How to redirect USB composite devices like Android Samsung phone and Panasonic Camera with SD card.
DTOS-23828	On Wyse 5070 devices with ThinOS 2308, the WiFi sporadically disconnects in Citrix sessions.

Table 131. Fixed issues (continued)

Issue ID	Description
DTOS-23206	OptiPlex 3000 devices with ThinOS 2308 have intermittent issues with Teams calls, screen sharing, dial tone, and microphone appears muted.
DTOS-22921	On devices with ThinOS 9.4.2103 version and CWA 23.5.0.58.1, there is bad audio quality in the outbound direction from the Softphone.
DTOS-22302	On OptiPlex 3000 devices with ThinOS 2308, WiFi fails to connect to the access points after few attempts.
DTOS-22061	You must limit users to one Blast session at a time.
DTOS-21707	Fujitsu scanners add a horizontal bar on the top and bottom of the document when scanning.
DTOS-21635	Association is rejected when roaming to a new access point.
DTOS-20308	Thin clients sporadically lock when 802.1x Ethernet settings are applied.
DTOS-26728	Wyse Management Suite Group Configurations job stays in the **In-progress** status when both wave policy and Group policy are running simultaneously on a device.
DTOS-26729	Wyse Management Suite download status of applications for Wave Policy is not displayed correctly in Group Configurations jobs.
DTOS-26159	**TCP Keep-Alive ACK** flooding issue on OptiPlex 3000 devices.
DTOS-26376	Unable to unlock a locked client.
DTOS-26801	There are smart card login issues with the client SDK.
DTOS-26581	In ThinOS , 2402 **Other Broker** is missing in **Default Broker Type** in Admin Policy Tool.
DTOS-25251	Windows desktop in VDI sessions cannot be displayed on external monitors when unplugging and replugging the video cable.

Known Issues

Table 132. Known Issues

Key	Summary	Workaround
DTOS-25939	Volume increase or decrease functionality is not working locally in the DellWL5022 headset that is connected using a USB dongle.	Not available.
DTOS-25495	Low Bluetooth audio with AirPods Pro 2 in UC Profile.	Not available.
DTOS-26422	The volume controller user interface does not work locally with the Dell WL5024 headsets.	The function works , but the UI does not reflect the changes. Use the slider to control the volume.
DTOS-25679	Event logs are not getting generated when disconnecting the launched applications.	Not available.

Table 132. Known Issues (continued)

Key	Summary	Workaround
DTOS-26137	In the Amazon WorkSpaces session, the fast disconnect shortcut key is not working.	Not available.
DTOS-25951	There is a UI Issue where you are unable to increase Dell WL5022headset volume in the UI beyond 80%.	Not available.
DTOS-26417	The volume controller user interface does not work locally with the Dell WL7022 headset.	The function works , but the UI does not reflect the changes. Use the slider to control the volume.
DTOS-25900	The automatic connection to multiple applications is not functioning as expected.	Manually launch the application when that application cannot be launched by automatic connections.
DTOS-24739	Citrix INI file permission denied in event log prints.	Reboot the client.
DTOS-26072	After clicking **Sign-off**, a **You have active connections. Are you sure want to continue?** dialog box is displayed even when there are no active application sessions connected.	Click the confirmation **You have active connections. Are you sure want to continue?**, and continue to sign off.
DTOS-27092	Horizon VDI stops responding when using the Ring Central application with Control Up RemoteDX VDI Agent.	Ring Central application works without the Control Up package. Do not use Control Up package with the Ring Central package.
DTOS-26403	VMware Workstation audio does not work after launching multiple VMware Horizon PCoIP sessions.	When playing a video with Window Media Player, use a single PCoIP session.
DTOS-25610	The focus cannot switch from the Citrix desktop to the local ThinOS desktop after connecting a dock.	Switch to Citrix desktop, then switch to ThinOS again.
DTOS-26793	ThinOS Extension Windows key and Ctrl + Tab key combination do not work well inside the VDA desktop. The issue occurs when using FIDO2 to log in to the broker using the ThinOS Chrome browser package.	Not available.
DTOS-26471	When **Force Full Screen** is enabled, failing to launch multiple applications.	Enable **Seamless Window Mode** setting from Wyse Management Suite.
DTOS-25723	The **Device** tab in the Citrix toolbar is not displayed with CWA version 24.2.0.65.9.	Download and install CWA version 24.2.0.65.17.
DTOS-26960	RDP hostname dialog box is displayed after signing off from the VMware broker.	Not available.
DTOS-27326	The P2P connection cannot be established, and the client connects using wireless network only.	Connect the client to a wired network and reboot. Then, the remote shadow with P2P is successful for the first time. After that, the P2P connection can be established wirelessly.

9

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 133. 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 134. 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 135. 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 135. 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 136. 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 137. 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 138. 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 139. 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 140. 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 141. Test environment—Windows 365 cloud PC

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

Table 142. 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	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
	Windows server 2019				
	Windows server 2022 (Not tested)				

Table 143. 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	14.3.0.308378.8	14.3.0.308378	14.3.0.308378
	Windows 11			
	Windows server 2016			
	Windows server 2019			
	Windows server 2022 (Not tested)			

Table 144. Tested environment—JVDI

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

Table 145. 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 146. 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 147. 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 148. 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 149. 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 150. 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)	Windows 10	43.10.2.11.3	43.10.2.11
	Windows 11		
	Windows server 2016		
	Windows server 2019		

Table 150. Tested environment—Cisco Webex Meetings (continued)

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
- Citrix Virtual Apps and Desktops 7 2308	Windows server 2022 (Not tested)		

Table 151. 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		

10

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 2311, 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 152. 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 152. 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 153. 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 154. 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 155. 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

Table 155. ThinOS application package details (continued)

ThinOS application package details
EPOS_Connect_7.7.0.2.pkg
HID_Fingerprint_Reader_210217.24.pkg
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_1.0.0.8.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

- If you have installed `ThinOS_Telemetry_Dashboard 1.0.0.7`, upgrade to version 1.0.0.8 at the earliest.
- **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.
  - From 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 156. Tested BIOS versions and BIOS packages

Supported platform	Tested BIOS version	New BIOS package
Wyse 3040 Thin Client	1.2.5	Not applicable
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 157. 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

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	App Personalization service	Not Supported	Not Supported
Workspace Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	Global App Config service (Workspace)	Not Supported	Not Supported
	Global App Config service (StoreFront)	Not Supported	Not Supported
	App Store Updates	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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Bi-directional Content redirection	Not Supported	Not Supported
	URL redirection	Not Supported	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	File open in Citrix Workspace app	Not Supported	Not supported. No local file explorer on ThinOS.
	Location Based Services (Location available via API-description)	Not Supported	Not Supported
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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	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 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

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Desktop Composition redirection	Not supported	Not supported
Authentication	Federated Authentication (SAML/Azure AD)	Supported	There are no limitations in this release.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Supported	There are no limitations in this release.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	Not supported	Not supported
	User Cert Auth via Gateway (via native Workspace app)	Not supported	Not supported
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	Not supported	Not supported
	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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Netscaler + RSA	Not qualified	Not qualified
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not qualified	Not qualified
	Netscaler load balance	Not supported	Not supported
Input experience	Keyboard layout sync - client to VDA (Windows VDA)	Supported	There are no limitations in this release.
	Keyboard layout sync - client to VDA (Linux VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Windows VDA)	Not Supported	Not Supported
	Keyboard layout sync - VDA to client (Linux VDA)	Not Supported	Not Supported
	Unicode keyboard layout mapping	Supported	There are no limitations in this release.
	Keyboard input mode - unicode	Supported	There are no limitations in this release.
	Keyboard input mode - scancode	Supported	There are no limitations in this release.
	Server IME	Supported	There are no limitations in this release.
	Generic client IME (CTXIME) for CJK IMEs	Not Supported	Not Supported
	Command line interface	Not Supported	Not Supported
	Keyboard sync setting UI and configurations	Not Supported	Not Supported
	Input mode setting UI and configurations	Not Supported	Not Supported
	Language bar setting UI and configurations	Not Supported	Not Supported
	Dynamic Sync setting in ThinOS	Supported	There are no limitations in this release.
	Keyboard sync only during session launched (Client Setting in ThinOS)	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard setting in ThinOS	Supported	There are no limitations in this release.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
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
	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	Supported	For information about limitations, see the

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	connecting to on-premises stores		Dell ThinOS 2402 Administrator's Guide at Support | Dell
	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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Microsoft Teams enhancements: WebRTC SDK upgrade	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: App sharing enabled	Supported	There are no limitations in this release.
	Microsoft Teams enhancements: Enhancements to high DPI support	Not Supported	Not Supported
	Support for extended keyboard layouts	Supported	There are no limitations in this release.
	Keyboard input mode enhancements	Not Supported	Not Supported
	Support for authentication using FIDO2 in HDX session	Supported	There are no limitations in this release.
	Support for secondary ringer	Supported	There are no limitations in this release.
	Improved audio echo cancellation support	Not Supported	Not Supported
	Composite USB device redirection	Not Supported	Not Supported
	Support for DPI matching	Not Supported	Not Supported
	Enhancement to improve audio quality	Not Supported	Not Supported
	Provision to disable LaunchDarkly service	Not Supported	Not Supported
	Email-based auto-discovery of store	Not Supported	Not Supported
	Persistent login	Not Supported	Not Supported
	Authentication enhancement for Storebrowse	Not Supported	Not Supported
	Support for EDT IPv6	Not Supported	Not Supported
	Support for TLS protocol version 1.3	Not Supported	Not Supported
	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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Dynamic e911 in Microsoft Teams	Supported	There are no limitations in this release.
	Request control in Microsoft Teams	Supported	Users on ThinOS client cannot give control to other users. In other words, after the user on the ThinOS client starts sharing screen or content, the option Give control is present in the sharing toolbar, but it does not work when you give control to other participant. This is a Microsoft limitation.
	Support for cursor color inverting	Supported	Invert cursor does not work in Citrix VDA 2212, VDA 2203 CU2, VDA2303 Windows 10 and Windows 2019 desktop. This issue also occurs in Citrix Workspace app Linux binary.
	Microsoft Teams enhancement to echo cancellation	Supported	For limitations, see the Dell 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

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	User Interface enhancement	Not Supported	Not Supported
	Pinning multi-monitor screen layout	Not Supported	Not Supported
	Authentication enhancement is available only in cloud deployments	Not Supported	Not Supported
	Multiple audio	Supported	Multiple audio devices feature is not supported by Cisco JVDI. This is Cisco known limitation. To eliminate confusion or mistakes, multiple audio devices feature is dynamically disabled after JVDI package installed, and it is dynamically enabled after JVDI package is uninstalled. Only Citrix VDA 2308 and later versions support 12 audio devices. The previous VDA version still has the 8 audio devices limitation. This is Citrix limitation
	Citrix logging	Supported	There are no limitations in this release.
	Cryptographic update	Not Supported	Not Supported
	Transparent user interface (TUI)	Not Supported	Not Supported
	GStreamer 1.x supportexperimental feature	Supported	There are no limitations in this release.
	App indicator icon	Not Supported	Not Supported
	Latest webkit support	Supported	There are no limitations in this release.
	Bloomberg audio redirection	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support	Supported	There are no limitations in this release.
	Multiple monitors improvement	Not Supported	Not Supported
	Error messages improvement	Not Supported	Not Supported
	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.

Table 157. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 2402 with CWA 2311	Limitations
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

ThinOS AVD Client Feature Matrix

Table 158. 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

Table 158. ThinOS AVD Client Feature Matrix (continued)

Category Supported	Features	ThinOS 2402
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 159. 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 160. 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
	FIDO2 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

Table 160. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
	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
	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

Table 160. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
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
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

Table 160. VMware Horizon feature matrix (continued)

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

Table 160. VMware Horizon feature matrix (continued)

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

Table 160. VMware Horizon feature matrix (continued)

Category	Feature	Horizon Session SDK	Horizon Client SDK
Other	Smart Policies from DEM	Supported	Supported
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI (Only basic connection is tested)	Supported with VDI (Only basic connection is tested)
	Workspace ONE mode	Supported	Supported
	Nested - basic connection	Supported	Supported
	DCT Per feature/component collection	Not Supported	Not Supported
	Displayed Names for Real-Time Audio-Video Devices	Supported	Supported
	Touchscreen Functionality in Remote Sessions and Client User Interface	Supported with VDI	Supported with VDI
Unified Access Gateway	Auth Method - Password	Supported	Supported
	Auth Method - RSA SecurID	Supported	Supported
	Auth Method - X.509 Certificate (Smart Card)	Supported	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 161. 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

Table 161. ThinOS Amazon WorkSpaces Client with WorkSpaces Streaming Protocol (WSP) feature matrix (continued)

Feature	ThinOS version 9.5.1079
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 162. 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 163. Display shortcut key options

Option	Default Value
Increase brightness key	F7

Table 163. Display shortcut key options (continued)

Option	Default Value
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 164. 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 165. 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 166. 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 167. 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

Table 167. Test environment—VMware Horizon (continued)

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2016 APPs	Windows Server 2019 APPs	Windows Server 2202 APPs	Ubuntu 20.04
VMware Horizon 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 168. 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 169. Test environment – VMware Horizon Cloud version 2

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

Table 170. 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 171. 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 172. Test environment—Windows 365 cloud PC

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

Table 173. 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)	Windows 10	2.9.700	2.9.700	Skype for Business 2016	Skype for Business 2015
	Windows 11				
	Windows server 2016				
	Windows server 2019				

Table 173. Tested environment—Skype for Business (continued)

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
● Citrix Virtual Apps and Desktops 7 2308	Windows server 2022 (Not tested)				

Table 174. 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	14.3.0.308378.8	14.3.0.308378	14.3.0.308378
	Windows 11			
	Windows server 2016			
	Windows server 2019			
	Windows server 2022 (Not tested)			

Table 175. Tested environment—JVDI

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

Table 176. 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 177. 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 178. 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 179. 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 180. 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 181. 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		
	Windows server 2022 (Not tested)		

Table 182. 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 183. 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

Table 183. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Professional Sound Bar (AE515M)	Supported	Supported	Not Available	Supported
	Dell USB Sound Bar (AC511M)	Not Available	Supported	Not Available	Not Available
	Jabra PRO 935 USB MS Lync Headset - 935-15-503-185 - 935-15-503-185	Not Available	Supported	Not Available	Not Available
	Dell 2.0 Speaker System - AE215	Not Available	Not Available	Supported	Supported
	Dell Wired 2.1 Speaker System - AE415	Not Available	Not Available	Supported	Supported
	Jabra Evolve 65 MS Stereo - Headset	Not Available	Not Available	Supported	Supported
	Jabra Engage 65 Stereo Headset	Not Available	Not Available	Supported	Supported
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0	Not Available	Not Available	Supported	Supported
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync	Not Available	Not Available	Supported	Supported
Input Devices	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse - Naruto	Supported	Supported	Supported	Supported
	Dell Laser Wired Mouse - MS3220 - Morty	Supported	Supported	Supported	Not Available
	Dell Mobile Pro Wireless Mice - MS5120W - Splinter	Supported	Supported	Not Available	Not Available
	Dell Mobile Wireless Mouse - MS3320W - Dawson	Supported	Supported	Not Available	Not Available
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W	Supported	Supported	Not Available	Supported
	Dell Multi-Device Wireless Mouse - MS5320W - Comet	Supported	Supported	Not Available	Not Available
	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

Table 183. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

Product Category	Peripherals	3040	5070	5470 AIO	5470
	Dell Wireless Keyboard and Mouse - KM636	Supported	Supported	Supported	Supported
	Dell Wireless Mouse - WM326	Not Available	Not Available	Supported	Supported
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white	Not Available	Not Available	Not Available	Not Available
	SEAL SHIELD MEDICAL GRADE OPTICAL (Mouse)	Not Available	Not Available	Not Available	Not Available
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white	Not Available	Not Available	Not Available	Not Available
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white	Not Available	Not Available	Not Available	Not Available
	Dell Wireless Mouse - WM126_BLACK - Rosewood	Not Available	Not Available	Not Available	Not Available
Adapters and Cables	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084 - DANARBC084	Supported	Supported	Not Available	Not Available
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087 - DANAUBC087	Supported	Supported	Supported	Not Available
	Dell Adapter - DisplayPort to VGA - DANBNBC084 - DANBNBC084	Supported	Supported	Not Available	Not Available
	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter	Not Available	Supported	Supported	Supported
	Dell Adapter - USB-C to DisplayPort - DBQANBC067 - DBQANBC067	Not Available	Supported	Not Available	Supported
	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

Table 183. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

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

Table 183. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

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

Table 183. Supported peripherals for Dell Wyse 3040, 5070, 5470, and 5470 AIO (continued)

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

Supported ecosystem peripherals for OptiPlex 3000 Thin Client

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

Table 184. 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

Table 184. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell Premier Wireless ANC Headset - Blazer - WL7022
	Dell Pro Wireless Headset - Daybreak - WL5022
	Dell Slim Conferencing Soundbar - Lizzo - SB522A
	Dell Speakerphone - Mozart - SP3022
	Stereo Headset WH1022 (Presto)
	Jabra Engage 65 MS Wireless Headset - 9559-553-125 Dell part #: AA143343 - 9559-553-125 Dell part #: AA143343
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309 - 6599-823-309
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync - 202652-02 - 202652-02
Input Devices	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty - MS3220
	Dell Business Multimedia Keyboard - KB522 - KB522 - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson - MS3320W (Bluetooth connection is not supported)
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - MS5320W - Comet
	Dell Optical Mouse - MS116_BLACK - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_GREY - MS116 - MS116 - Sapphire
	Dell Optical Mouse - MS116_WHITE - MS116 - MS116 - Sapphire
	Dell KB813 Smartcard Keyboard - KB813 - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter - MS5120W
	Dell Multimedia Keyboard - KB216_BLACK - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_Grey - KB216 - KB216 - Rusty
	Dell Multimedia Keyboard - KB216_WHITE - KB216 - KB216 - Rusty
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine - MS819 (Fingerprint reader is not supported)
	Dell Wireless Keyboard and Mouse - Auburn MLK - KM3322W
	Newmen 100 KM-101 Keyboard/Mouse Combo - Dell China sku A8818726 - Dell China sku A8818726
	Dell Bluetooth Travel Mouse - MS700 - Black
Displays	Dell 17 Monitor - E1715S - E1715S - E1715S
	Dell 19 Monitor - P1917S - P1917S - P1917S
	Dell 19 Monitor E1920H - E1920H
	Dell 20 Monitor E2020H - E2020H
	Dell 22 Monitor - E2223HN - E2223HN
	Dell 22 Monitor - P2222H - P2222H
	Dell 23 Monitor - P2319H - P2319H - P2319H
	Dell 24 Monitor - P2421 - P2421 - P2421

Table 184. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell 24 Monitor - P2421D - P2421D - P2421D
	Dell 24 Monitor - P2422H - P2422H
	Dell 24 Monitor E2420H - E2420H
	Dell 24 Monitor E2420HS - E2420HS
	Dell 24 Touch Monitor - P2418HT - P2418HT - P2418HT
	Dell 24 USB-C Hub Monitor - P2422HE - P2422HE
	Dell 24 USB-C Monitor - P2421DC - P2421DC - P2421DC
	Dell 27 4K USB-C Monitor - P2721Q - P2721Q
	Dell 27 Monitor - P2720D - P2720D
	Dell 27 Monitor - P2722H - P2722H
	Dell 27 Monitor E2720H - E2720H
	Dell 27 Monitor E2720HS - E2720HS
	Dell 27 USB-C Hub Monitor - P2722HE - P2722HE
	Dell 27 USB-C Monitor - P2720DC - P2720DC
	Dell 32 USB-C Monitor - P3221D - P3221D
	Dell 34 Curved USB-C Monitor - P3421W - P3421W
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE - C2422HE
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE - C2722DE
	Dell Collaboration 32 Monitor - U3223QZ - U3223QZ
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE - C3422WE
	Dell UltraSharp 24 Hub Monitor U2421E - U2421E
	Dell UltraSharp 24 Monitor - U2422H - U2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE - U2422HE
	Dell UltraSharp 25 USB-C Monitor - U2520D - U2520D
	Dell UltraSharp 27 4K USB-C HUB Monitor - U2723QE - U2723QE
	Dell UltraSharp 27 4K USB-C Monitor - U2720Q - U2720Q
	Dell UltraSharp 27 Monitor - U2722D - U2722D
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE - U2722DE
	Dell UltraSharp 30 USB-C HUB Monitor - U3023E - U3023E
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q - U3219Q
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE - U3421WE
	Dell UltraSharp 38 Curved USB-C HUB Monitor - U3821DW - U3821DW
	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

Table 184. Supported ecosystem peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
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 185. 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 186. 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 187. 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)

Table 187. Supported ecosystem peripherals for Latitude 3440 (continued)

Product Category	Peripherals
	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 188. 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 189. 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 190. 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 191. 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 192. Third-party supported peripherals

Product Category	Peripherals
Audio Devices	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth （link 360）
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (Support USB only, not support Bluetooth)
	Plantronics AB J7 PLT
	Plantronics Blackwire C5210
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Calisto P820-M
	Plantronics Voyager 6200 UC
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER SC 660 USB ML
	SENNHEISER USB SC230

Table 192. Third-party supported peripherals (continued)

Product Category	Peripherals
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SP 10 ML Speakerphone for Lync
	Sennheiser SDW 5 BS-EU
	Logitech S-150
	POLYCOM Deskphone CX300
	PHILIPS - analog
	Logitech h150 - analog
	LFH3610/00 SPEECH MIKE PREMIUM (only support redirect)
	Nuance PowerMic II (Recommend redirecting whole device)
	Olympus RecMic DR-2200 (Recommend redirecting whole device)
	Apple AirPods (2nd generation)
	Apple AirPods (3rd generation)
	Apple AirPods Pro (1st generation)
	Jabra elite 3
Input Devices	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	SpaceNavigator 3D Space Mouse
	SpaceMouse Pro
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Displays	Elo ET2201L IntelliTouch ZB (Worldwide) - E382790
	Elo ET1717L AccuTouch ZB Black Anti-glare (Worldwide) - E649473
	Elo PCAP E351600 - ET2202L-2UWA-0-BL-G
Camera	Logitech C920 HD Pro Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Logitech C930e HD Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C910 HD Pro Webcam
	Logitech C925e Webcam
	Poly EagleEye Mini webcam
	Logitech BRIO 4K Webcam
	Jabra PanaCast 4K Webcam
Storage	SanDisk cruzer 8 GB

Table 192. Third-party supported peripherals (continued)

Product Category	Peripherals
	SanDisk cruzer 16G
	SanDisk USB 3.1 and Type-C 16 GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32 GB
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Samsung portable DVD Writer SE-208
Signature Tablet	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	IDBridge CT31 PIV
	Gemalto IDBridge 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

Table 192. Third-party supported peripherals (continued)

Product Category	Peripherals
	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 193. Supported smart cards

Smart Card info from ThinOS event log	Smart Card Middleware in VDI	Provider (CSP)	Card type	Citrix	VMware (works for Blast and PCoIP, not RDP)	RDS (works for broker login, and not in sessions)
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2	Supported	Supported	Supported
ActivIdentity V1	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c	Supported	Supported	Supported
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 3.2	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5	Supported	Supported	Not Available
ActivIdentity v2 card	ActivClient 7.4	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8	Supported	Supported	Not Available
ActivIdentity crescendo card	ActivClient 7.4	ActivClient Cryptographic Service Provider	G&D SCE 7.0 (T=0)	Supported	Supported	Not Available
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840	Supported	Not Available	Supported
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B	Supported	Not Available	Supported
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K	Supported	Supported	Supported
ID Prime MD v 4.1.3	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire	Supported	Supported	Supported
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS	Supported	Supported	Supported

Table 193. 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)
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B	Supported	Supported	Supported
ID Prime MD v 4.5.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 930 FIPS L2	Supported	Supported	Supported
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940	Supported	Supported	Supported
Etoken Java	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS	Supported	Supported	Supported
Etoken Java (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC	Supported	Supported	Not Available
ID Prime MD v 4.5.0.F (black USB key)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110+ FIPS L2	Supported	Supported	Supported
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)	Supported	Supported	Not Available
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	YubiKey 4.3.3	Supported	Not Available	Supported

Table 193. 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)
		Cryptographic Provider v1.0				
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 194. Fixed issues

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

Table 194. Fixed issues (continued)

Issue ID	Description
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.
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.

Table 194. Fixed issues (continued)

Issue ID	Description
DTOS-23424	WPA Enterprise credentials are displayed on booting.

Security fixes

ThinOS Telemetry Dashboard version 1.0.0.8 addresses one vulnerability. For information about the vulnerability addressed in this package, see **DSA-2024-170: Dell ThinOS Security Update for Vulnerability** at Security Advisories, Notices and Resources.

Known Issues

Table 195. 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 the Dell WD19 dock, 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 volume in the session, the audio volume does not increase.	Adjust volume in the graphical UI.
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.

Table 195. Known Issues (continued)

Key	Summary	Workaround
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.

11

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 **Wyse Software**.
6. Click **Wyse ThinOS** .
7. Click **Select this Product**.
8. Click **Documentation**.

12

Contacting Dell

Prerequisites

If you do not have an active Internet connection, you can find contact information about 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, follow the steps.

Steps

1. Go to Support | Dell.
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.