Dell Wyse ThinOS

Version 9.1.4097, 9.1.4234, 9.1.5067, and 9.1.6108

Operating System Release Notes

April 2022
Rev. A11

Notes, cautions, and warnings

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

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

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

Contents

1

Overview

Dell Wyse ThinOS software is designed to run on a broad array of Dell Wyse hardware platforms. New releases are created to support new hardware platforms, correct defects, make enhancements, or add new features. These releases are tested and supported on current, actively shipping hardware platforms, and those hardware platforms that are within their first year after their official End of Life date.

2

Version matrix

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

Table 1. ThinOS firmware version matrix

Release version	Release date	Supported platforms	Release Notes
ThinOS 9.1.6108	February 2022	- Wyse 3040 Thin Client - Wyse 5070 Thin Client - Wyse 5470 Thin Client - Wyse 5470 All-in-One Thin Client - OptiPlex 3000 Thin Client	Release version ThinOS 9.1.6108
ThinOS 9.1.5067	December 2021	- Wyse 3040 Thin Client - Wyse 5070 Thin Client - Wyse 5470 Thin Client - Wyse 5470 All-in-One Thin Client	Release version ThinOS 9.1.5067
ThinOS 9.1.4234	October 2021	- Wyse 3040 Thin Client - Wyse 5070 Thin Client - Wyse 5470 Thin Client - Wyse 5470 All-in-One Thin Client	Release version ThinOS 9.1.4234

Table 2. ThinOS application package version matrix

Application package versions	Release date	Supported platforms	Release Notes
- Citrix_Workspace_App_21.12.0.18_2 .pkg - VMware_Horizon_2111.8.4.0.18957622_3.pkg - Cisco_WebEx_Meetings_VDI_41.12.6.12_1.pkg - Cisco_WebEx_VDI_41.12.0.20899_1.pkg (formerly called Cisco WebEx Teams) - Zoom_Citrix_5.8.4.21112_1.pkg - Zoom_Horizon_5.8.4.21112_1.pkg	January 2022	- Wyse 3040 Thin Client - Wyse 5070 Thin Client - Wyse 5470 Thin Client - Wyse 5470 All-in-One Thin Client	Citrix Workspace app 2112, VMware Horizon 2111, Cisco WebEx Meetings VDI 41.12, Cisco WebEx VDI 41.12, and Zoom 5.8.4 packages for ThinOS
- Citrix_Workspace_App_21.9.0.25_1 .pkg - Cisco_WebEx_Meetings_VDI_41.10.3.19_1.pkg - Cisco_WebEx_VDI_41.10.0.20213_1.pkg (formerly Cisco WebEx Teams) - HID_Fingerprint_Reader_210217_11.pkg	November 2021	- Wyse 3040 Thin Client - Wyse 5070 Thin Client - Wyse 5470 Thin Client - Wyse 5470 All-in-One Thin Client	Cisco WebEx Meetings 41.10, Cisco WebEx VDI 41.10, Citrix Workspace app 2109, and HID fingerprint reader 210217_11 packages for ThinOS

3

ThinOS 9.1.6108

Release date

February 2022

Release summary

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

Previous versions

Dell Wyse 3040, 5070, 5470, and 5470 All-in-One thin clients—ThinOS 9.1.5067

OptiPlex 3000 Thin Client—ThinOS 9.1.4097

Firmware upgrade

The following firmware upgrade scenarios are supported:

- ThinOS 8.6_807 > ThinOS 9.1.6108
- ThinOS 9.1.3129 or later versions > ThinOS 9.1.6108

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

ⓘ **NOTE:** On thin clients that run ThinOS versions earlier than ThinOS 9.1.6018, you must upgrade the OS image first, and then upgrade the BIOS after the OS image is successfully upgraded. Do not upgrade the BIOS and the OS image together. If you upgrade the BIOS and the OS image together, the BIOS upgrade is ignored, and you cannot upgrade the BIOS to the ignored version anymore. You must upgrade the BIOS to another version.

For more information, see the *Dell Wyse ThinOS Version 9.1.4234, 9.1.5067, and 9.1.6108 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

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

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

    - When you change the Wyse Management Suite group.
- When you set a new firmware or an application package in Wyse Management Suite group 2 and then change the device from group 1 to group 2 before upgrading, the following two notifications are displayed:
    - **Wyse Management Suite server or group is changed. System is going to reboot to load full configuration. Press cancel in 60 seconds to prevent reboot**.
    - **A new firmware or application is available, do you want to upgrade now or defer to the next reboot? The changes will automatically be applied in 120 seconds.**

  On ThinOS 9.1.5067 and earlier versions, if you do not select an option, the thin client reboots after 60 seconds. After the reboot, the new application or firmware is installed and the thin client reboots again. The thin client will be in group 2 after the reboot.

  From ThinOS 9.1.6108, a notification for new firmware or application is displayed first. If you do not select an option, the thin client downloads and installs the new application or firmware, and reboots. If you select **Next Reboot**, then the thin client prompts the WMS server or group change notification.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
    - Displays a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
    - Not display any notification if the new firmware or application is downloaded in the same group, from ThinOS 9.1.6108.
    - Installs the firmware or package after a reboot.

Prerequisites for firmware upgrade

- Update the BIOS version of Wyse 5070 Thin Client to 1.3.1 or later before upgrading to ThinOS 9.1.6108. If you upgrade to ThinOS 9.1.6108 with earlier BIOS version and then upgrade the BIOS version to 1.3.1 or later, the device may fail to boot. If there is a boot failure, check if the PTT option is available under security in BIOS Setup. For Wyse 5070 Thin Clients with firmware TPM configuration, the PTT option is available after updating BIOS to 1.3.1 or later versions. You must disable the option and boot into ThinOS if you fail to boot after upgrade BIOS. For latest BIOS versions, see Tested BIOS version for ThinOS 9.1.6108.
- Before you migrate from ThinOS 8.6_807 to ThinOS 9.1.6108 or upgrade from ThinOS 9.x to 9.1.6108, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the Wakeup On LAN command through Wyse Management Suite before using any real-time commands. To use the Wakeup On LAN command, ensure that the Wakeup On LAN option is enabled in BIOS.

Upgrade from ThinOS 8.6 to ThinOS 9.1.6108 using Wyse Management Suite

If you are running any ThinOS 8.6 version, you must first install the ThinOS 8.6_807 image with the latest BIOS version, and then upgrade to ThinOS 9.1.6108. For the latest BIOS versions, see the *Dell Wyse ThinOS Version 8.6_807 Release Notes* at www.dell.com/support.

The device reboots after the ThinOS image is downloaded. Once the upgrade completes, the device is automatically registered to Wyse Management Suite. Dell Technologies recommends you to back up your device settings before you initiate the upgrade process. All device settings are erased after you upgrade from ThinOS 8.6 except the following settings:

- **Wyse Management Suite group token and server settings**
- **Static DNS**
- **Certificates**
- **IEEE802.1x wired authentication settings**
- **Wireless connections**—The WEP/Sharekey security type is changed to **Open** as they are not supported in ThinOS 9.1
- **Proxy settings**

ⓘ **NOTE:** For more information about how to install the ThinOS 9.1.6108 image, see the *Dell Wyse ThinOS Version 9.1.4234, 9.1.5067, and 9.1.6108 Migration Guide* at www.dell.com/support.

Upgrade from ThinOS 9.1.x to ThinOS 9.1.6108 using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on you thin client.
- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.
- Download the ThinOS 9.1.6108 (DTOS_9.1.6108.pkg) firmware to upgrade.

Steps

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

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

5. Click **Browse** and select the **ThinOS 9.1.6108** firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.

   The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

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

Compatibility

ThinOS application package details

- Cisco_Jabber_14.0.3.306553.1.pkg
- Cisco_WebEx_Meetings_VDI_41.12.6.12.1.pkg
- Cisco_WebEx_VDI_41.12.0.20899.1.pkg (formerly called Cisco WebEx Teams)
- Citrix_Workspace_App_21.12.0.18.3.pkg
- EPOS_Connect_7.0.0.19336.1.pkg
- HID_Fingerprint_Reader_210217.13.pkg
- Jabra_8.5.1.12.pkg
- Microsoft_AVD_1.6.1402.pkg
- Teradici_PCoIP_21.03.1.26.pkg
- VMware_Horizon_2111.8.4.0.18957622.6.pkg
- Zoom_Citrix_5.8.4.21112.1.pkg
- Zoom_Horizon_5.8.4.21112.1.pkg
- Imprivata_PIE_7.7.000.0007.1134.pkg
- Identity_Automation_QwickAccess_2.0.0.3.3.pkg

Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 3.6.241
- Configuration UI package 1.5 324

ThinOS build details

- ThinOS 9.1.3129 or later versions to ThinOS 9.1.6108—**DTOS_9.1.6108.pkg**.

- ThinOS 8.6_807 to ThinOS 9.1.6108 conversion builds:
  - **A10Q_wnos**—Wyse 3040 Thin Client
  - **PA10Q_wnos**—Wyse 3040 Thin Client with PCoIP
  - **X10_wnos**—Wyse 5070 Thin Client, Wyse 5470 Thin Client, and Wyse 5470 All-in-One Thin Client
  - **PX10_wnos**—Wyse 5070 Thin Client with PCoIP, Wyse 5470 Thin Client with PCoIP, and Wyse 5470 All-in-One Thin Client with PCoIP

BIOS packages

Table 3. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.15.1.pkg
Wyse 5470 Thin Client	bios-5470_1.12.0.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.13.0.pkg

Table 4. BIOS package—OptiPlex 3000 Thin Client

Platform model	Package filename
OptiPlex 3000 Thin Client	Bios-OP3000TC_1.0.2.pkg

Tested BIOS version for ThinOS 9.1.6108

Table 5. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.15.1
Wyse 5470 All-in-One Thin Client	1.13.0
Wyse 5470 Thin Client	1.12.0

Table 6. Tested BIOS details—OptiPlex 3000 Thin Client

Platform name	BIOS version
OptiPlex 3000 Thin Client	1.0.2

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

Citrix Workspace app feature matrix

Table 7. Citrix Workspace app feature matrix

Feature		ThinOS 9.1.6108	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	There are no limitations in this release.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	This feature is only supported with Citrix Workspace app 2109 in this release. Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. This is Citrix binary design. Citrix Workspace app 2112 only supports built-in camera. External cameras does not work. The issue is also observed in Linux binary.
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Version 9.1.6108 Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Version 9.1.6108 Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.6108 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco WebEx Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebExTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 9.1.6108 Administrator's Guide at www.dell.com/support.

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 9.1.6108 Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Version 9.1.6108 Administrator's Guide at www.dell.com/support.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Active Directory	Supported	There are no limitations in this release.
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
New features listed in Citrix Workspace app release notes but not in feature matrix	Dynamic e911 in Microsoft Teams (CWA2112)	Not Supported	Not Supported
	Request control in Microsoft Teams (CWA2112)	Not Supported	Not supported
	Support for cursor color inverting (CWA2112)	Supported	There are no limitations in this release.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	There are no limitations in this release.
	Enhancement on smart card support (CWA2112)	Supported	There are no limitations in this release.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Not supported	Not supported
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported

Table 7. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.6108	Limitations
	App Protection (CWA2101, CWA2106, CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio (CWA2012, CWA2010, and CWA2112)	Not supported	Not supported
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

VMware Horizon feature matrix

Table 8. VMware Horizon feature matrix

Feature		ThinOS 9.1.6108
Broker Connectivity	SSL certificate verification	Supported only with VDI
	Disclaimer dialog	Supported with VDI, RDS Hosted Desktops and Apps
	UAG compatibility	Supported with VDI, RDS Hosted Desktops and Apps

Table 8. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.6108
	Shortcuts from server	Not supported
	Pre-install shortcuts from server	Not supported
	File type association	Not supported
	Phone home	Supported with VDI, RDS Hosted Desktops and Apps
Broker Authentication	Password authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Single sign on	Supported with VDI, RDS Hosted Desktops and Apps
	RSA authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Integrated RSA SecurID token generator	Not supported
	Kiosk mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remember credentials	Not supported
	Log in as current user	Not supported
	Nested log in as current user	Not supported
	Log in as current user 1-way trust	Not supported
	OS biometric authentication	Not supported
	Un-authentication access	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Cisco ACS	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – SMS Passcode	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - DUO	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Microsoft Network Policy	Supported with VDI, RDS Hosted Desktops and Apps
Smart card	x.509 certificate authentication (Smart Card)	Supported with VDI, RDS Hosted Desktops and Apps
	CAC support	Supported with VDI, RDS Hosted Desktops and Apps
	.Net support	Supported with VDI, RDS Hosted Desktops and Apps
	PIV support	Supported with VDI, RDS Hosted Desktops and Apps
	Java support	Not supported
	Purebred derived credentials	Not supported
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI
	Restart	Supported only with VDI

Table 8. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.6108
	Log off	Supported with VDI, RDS Hosted Desktops and Apps
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple connections	Supported with VDI, RDS Hosted Desktops and Apps
	Multi-broker/multi-site redirection - Universal	Not supported
	App launch on multiple end points	Supported with VDI, RDS Hosted Desktops and Apps
	Auto-retry 5+ minutes	Supported with VDI, RDS Hosted Desktops and Apps
	Blast network recovery	Supported with VDI, RDS Hosted Desktops and Apps
	Time zone synchronization	Supported with VDI, RDS Hosted Desktops and Apps
	Jumplist integration (Windows 7-Windows 10)	Not supported
Client Customization	Command line options	Not supported
	URI schema	Not supported
	Launching multiple client instances using URI	Not supported
	Preference file	Not supported
	Parameter pass-through to RDSH apps	Not supported
	Non interactive mode	Not supported
	GPO-based customization	Not supported
Protocols Supported with VDI, RDS Hosted Desktops and Apps	Blast Extreme	Supported with VDI, RDS Hosted Desktops and Apps
	H.264 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	H.265 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps—Except OptiPlex 3000 Thin Client.
	Blast Codec	Supported with VDI, RDS Hosted Desktops and Apps
	JPEG/PNG	Supported with VDI, RDS Hosted Desktops and Apps
	Switch encoder	Supported with VDI, RDS Hosted Desktops and Apps
	BENIT	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Extreme Adaptive Transportation	Supported with VDI, RDS Hosted Desktops and Apps
	RDP 8.x, 10.x	Supported with VDI, RDS Hosted Desktops and Apps

Table 8. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.6108
	PCoIP	Supported with VDI, RDS Hosted Desktops and Apps
Features/Extensions Monitors/ Displays	Dynamic display resizing	Supported with VDI, RDS Hosted Desktops and Apps
	VDI windowed mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remote app seamless window	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple monitor support	Supported with VDI, RDS Hosted Desktops and Apps
	External monitor support for mobile	Not supported
	Display pivot for mobile	Not supported
	Number of displays Supported with VDI, RDS Hosted Desktops and Apps	4
	Maximum resolution	3840x2160
	High DPI scaling	Supported only with VDI
	DPI sync	Supported with VDI, RDS Hosted Desktops and Apps
	Exclusive mode	Not supported
	Multiple monitor selection	Supported with VDI, RDS Hosted Desktops and Apps
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported with VDI, RDS Hosted Desktops and Apps
	Relative mouse	Supported only with VDI
	External Mouse Support	Supported with VDI, RDS Hosted Desktops and Apps
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported with VDI, RDS Hosted Desktops and Apps
	International Keyboard Support	Supported with VDI, RDS Hosted Desktops and Apps
	Input Method local/remote switching	Not supported
	IME Sync	Supported with VDI, RDS Hosted Desktops and Apps
Clipboard Services	Clipboard Text	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard Graphics	Not supported
	Clipboard memory size configuration	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard File/Folder	Not supported
	Drag and Drop Text	Not supported
	Drag and Drop Image	Not supported
	Drag and Drop File/Folder	Not supported

Table 8. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.6108
Connection Management	IPv6 only network support	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP IP roaming	Supported with VDI, RDS Hosted Desktops and Apps
Optimized Device Redirection	Serial (COM) Port Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Client Drive Redirection/File Transfer	Not supported
	Scanner (TWAIN/WIA) Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	x.509 Certificate (Smart Card/ Derived Credentials)	Supported with VDI, RDS Hosted Desktops and Apps
	Gyro Sensor Redirection	Not supported
Real-Time Audio-Video	Audio in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Video in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple webcams	Not supported
	Multiple speakers	Not supported
USB Redirection	USB redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnInsert	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnStartup	Supported with VDI, RDS Hosted Desktops and Apps
	Connect/Disconnect UI	Not supported
	USB device filtering (client side)	Supported with VDI, RDS Hosted Desktops and Apps
	Isochronous Device Support	Supported only with VDI
	Split device support	Supported with VDI, RDS Hosted Desktops and Apps
	Bloomberg Keyboard compatibility	Supported only with VDI
	Smartphone sync	Supported only with VDI
Unified Communications	Skype for business	Supported with VDI, RDS Hosted Desktops and Apps
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Teams	Supported with VDI, RDS Hosted Desktops
	Cisco WebEx Meetings	Supported with VDI, RDS Hosted Desktops
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops and Apps
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops and Apps
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops

Table 8. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.6108
	HTML5 Redirection	Not supported
	Directshow Redirection	Not supported
	URL content redirection	Not supported
	MMR Multiple Audio Output	Not supported
	Browser content redirection	Not supported
Graphics	vDGA	Supported only with VDI
	vSGA	Supported only with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops
	Intel vDGA	Supported only with VDI
	AMD vGPU	Supported only with VDI
Mobile Support	Client-side soft keyboard	Not supported
	Client-side soft touchpad	Not supported
	Full Screen Trackpad	Not supported
	Gesture Support	Not supported
	Multi-touch Redirection	Not supported
	Presentation Mode	Not supported
	Unity Touch	Not supported
Printing	VMware Integrated Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Location Based Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Native Driver Support	Not supported
Security	FIPS-140-2 Mode Support	Supported with VDI, RDS Hosted Desktops and Apps
	Imprivata Integration	Supported with VDI, RDS Hosted Desktops and Apps
	Opswat agent	Not supported
	Opswat on-demand agent	Not supported
	TLS 1.1/1.2	Supported with VDI, RDS Hosted Desktops and Apps
	Screen shot blocking	Not supported
	Keylogger blocking	Not supported
Session Collaboration	Session Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
	Read-only Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
Update	Update notifications	Not supported
	App Store update	Not supported
Other	Smart Policies from DEM	Supported with VDI, RDS Hosted Desktops and Apps

Table 8. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.6108
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI—Only basic connection is tested
	Workspace ONE mode	Supported with VDI, RDS Hosted Desktops and Apps
	Nested - basic connection	Supported with VDI, RDS Hosted Desktops and Apps
	DCT Per feature/component collection	Not supported

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

New and enhanced features

Citrix Workspace app updates

- **Plug-and-play functionality for smart card reader enhancement**—ThinOS does not allow to disable smart card plug-and-play through Citrix Configuration Editor by modifying DriverName parameter due to ThinOS security concern. Hence, plug-and-play functionality for smart card reader is always enabled from this release.
- **Webcam redirection (HDX RealTime Webcam Video Compression) for 32-bit apps enhancement**—Only 32-bit apps on the virtual desktop with HDX RealTime Webcam Video Compression are supported by ThinOS. Dell Technologies only qualified this feature using Citrix Workspace App 2109 package. With this feature, you can customize the camera resolution and frames per second from **System Setup** > **Peripherals** > **Camera**. You can also customize this feature using Admin Policy Tool or Wyse Management Suite policy settings. HDX RealTime Webcam Video Compression is compatible with most unified communications clients. The feature has been tested for compatibility with Cisco Webex Meetings, Cisco Webex Teams, Cisco Jabber, Microsoft Teams, Skype for Business 365, and Zoom. You can use a 32-bit browser such as Google Chrome or Mozilla Firefox to verify the webcam redirection online. External USB cameras or the integrated camera can be used with HDX RealTime Webcam Video Compression. Webcam bandwidth consumption can vary with webcam models. Different webcams offer different frame rates and resolution. Dell Technologies used the following webcams for initial feature validation:
  - Microsoft LifeCam HD-3000—Highest supported resolution with HDX RealTime Webcam Video Compression is 1920x800.
  - Logitech C920, C922, C930e—Highest supported resolution with HDX RealTime Webcam Video Compression is 1600x896.
  - Wyse 5470 and 5470 All-in-One thin clients with built-in camera.

  For the steps to configure camera settings, see *Dell Wyse ThinOS 9.1.4234, 9.1.5067, and 9.1.6108 Administrator's Guide* at www.dell.com/support.

  HDX RealTime Webcam Video Compression limitations

  - Camera with hardware encoding is not supported in ThinOS.
  - Since x264 library is not integrated into ThinOS, 64-bit apps with HDX RealTime Webcam Video Compression are not supported by Citrix Workspace App. Hence, only 32-bit apps with HDX RealTime Webcam Video Compression are supported in ThinOS.
  - Citrix Workspace App 2112 with HDX RealTime Webcam Video Compression works only with built-in camera. The issue is also reproduced in Linux Citrix Workspace app binary. Hence, from this ThinOS release, HDX RealTime Webcam Video Compression is only supported with Citrix Workspace app 2109.
  - Sometimes, the updated Camera Width, Camera Height and Camera FPS settings does not sync from Wyse Management Suite to the thin client. You must reboot the client for the changes to take effect.
  - HDX RealTime Webcam Video Compression in ThinOS supports only one webcam at a time. Citrix Workspace Linux binary can update the default webcam by modifying **HDXWebCamDevice** in `$HOME/.ICAClient/wfclient.ini` configuration file. For example, add **`HDXWebCamDevice=/dev/video2`** to set the webcam mapped to */dev/video2* in a system. However, ThinOS does not allow to input the value `/dev/video2` in VDI Configuration Editor due to security reasons.
  - If client camera is set to 2304x1296 or 2304x1536 video resolution, the HDX webcam redirection cannot be previewed in the session. This limitation is reproduced in CWA 2109 Linux binary as well.

    - If client camera is set to 1920x1080 video resolution, the HDX webcam redirection falls back to 325x288 video resolution in the session. This limitation is reproduced in CWA 2109 Linux binary as well.
    - HDX webcam camera sometimes does not work on WebEx Meeting call. This limitation is reproduced in CWA 2109 Linux binary as well.
    - Zoom application video preview sometimes fails when you use Citrix HDX Webcam. This limitation is reproduced in CWA 2109 Linux binary as well.
    - WebEx application video fails to preview when you use Citrix HDX Webcam. This limitation is reproduced in CWA 2109 Linux binary as well.
    - External USB camera does not work with Citrix HDX Webcam in Citrix Workspace app 2112. Only the built-in camera works. This limitation is reproduced in CWA 2109 Linux binary as well.

- **Citrix Workspace app fixed issues**
    - Resolved the issue where the cursor color inverting feature does not work after you upgrade or downgrade the Citrix Workspace app package.
    - Resolved the issue where DriverName in smartcard settings under module.ini is changed from VDSCARDV2.DLL to VDSCARD.DLL.
- **Citrix Workspace app limitations**
    - Graphics issue while using YouTube with Browser Content Redirection (BCR) enabled.
    - Zoom optimization does not support proxy using nonanonymous authentication.
    - Mouse cursor displays a black block in Citrix HDX 3D desktop.
    - Jabra Evolve 75, Jabra Engage 75, and Jabra PRO 9450 headsets do not support answering and disconnecting calls using headset buttons for RTME, Cisco JVDI, Zoom, Cisco WebEx teams VDI, Cisco WebEx Meeting VDI, and Microsoft Teams. Jabra Engage 75 headset supports RTME.
    - Zoom window displays a shadow when you share screen.

Unified communication updates

Cisco Jabber application package is updated to version 14.0.3.406553.1.

NOTE: Answering and disconnecting calls using headset buttons is not supported in Cisco JVDI, Zoom, Cisco WebEx teams VDI, Cisco WebEx Meeting VDI, and Microsoft Teams.

ThinOS enhancements

- You can register devices with the Wyse Management Suite using DHCP scope options 201 and 202.
- The following are the updates in the download and installation process of firmware, BIOS, and application packages files:
    - The pop-up window for new firmware or application package is prompted before downloading the file. After you click **Install Now**, the download is initiated.
    - Once a file is downloaded, it gets installed before the next file is downloaded. After the installation of the downloaded file is finished, the next download is initiated.
    - OS image is downloaded and installed first. The client reboots after the image is installed. After the reboot, the download and installation of other packages are initiated.
- If you set a new firmware or an application package to update from group 2 when your device is in Wyse Management Suite group 1, and then change the device from group 1 to group 2, the notification window that is displayed to initiate the new firmware or application package upgrade is prompted first. After you click the **Next Reboot** button, the notification window of WMS server or group change is displayed.
- If you change the **Wyse Management Suite** server or group in **Central Configuration** when there is a notification window with a new available firmware or application package upgrade, a pop-up window is displayed to notify that the upgrade will be terminated.
- Added new wireless security type WPA3 Personal and Opportunistic Wireless Encryption (OWE).
    - Wyse 3040 Thin Client does not support WPA3 Personal and OWE.
    - Wyse 5070, 5470, 5470 All-in-One thin clients, and OptiPlex 3000 Thin Client with wireless chipset 9560 do not support OWE.
    - OptiPlex 3000 Thin Client with wireless chipset AX210 supports both WPA3 Personal and OWE with WIFI 6/6e.

  NOTE: If you disable **11n** from **Wyse Management Suite** policy settings or **Admin Policy Tool**, WPA3 Personal does not work with some wireless routers.
- Added the Energy Star logo to the System Information window of OptiPlex 3000 Thin Clients.

  NOTE: The logo is present only in factory shipped OptiPlex 3000 thin clients.

- Updated the battery icons that are displayed on Wyse 5470 Thin Client.
- When the manual override option is enabled, the audio devices that are manually selected in the **Peripherals** > **Audio** tab take priority. Audio devices remain selected after you reboot the device.
- Supports configuring proxy for Secure MQTT using PAC/WPAD settings.
- Added **Pulse secure and Global Protect** in the VPN Protocol list. The default value is **Cisco AnyConnect**. You can connect to VPN with Cisco Anyconnect, Pulse secure, or Global Protect.
- Added camera control options such as resolution and FPS. The feature currently works in Citrix only. For more information, see Citrix Workspace app updates.

For more information about the updates, see the *Dell Wyse ThinOS 9.1.4234, 9.1.5067, and 9.1.6108 Administrator's Guide* and *Dell Wyse ThinOS 9.1.4234, 9.1.5067, and 9.1.6108 Migration Guide* at www.dell.com/support .

Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **On Desktop**—Added **On Desktop** option in **Session Settings** > **Global Session Settings**. If you select **On desktop = Specified Applications/Desktops**, you can specify the applications or desktops list in the **Specified Applications/Desktops List** to be displayed on desktop. The option works only when you log in with classic mode or modern mode.
- **Map Disks**—Changed the default value of **Map Disks** option in **Session Settings** > **Global Session Settings** to enabled.
- **Show Password for Login Window**—Added **Show Password for Login Window** option in **Login Experience** > **Login Settings**. If you enable this option, an eye symbol is displayed in the password, passcode, or PIN field on the login window. Clicking the eye symbol displays the characters that you have entered in the password, passcode, or PIN field.

  ⓘ **NOTE:** To use this option, ensure that there is no default password set. The option is not available on the login screen of web view windows such as Citrix Azure AD login window or Citrix OTP login window. The option is also not available on second passcode windows such as Citrix SMS passcode or Citrix OKTA passcode.
- **Analog Audio Jack pop-up**—Added **Analog Audio Jack pop-up** option in **Peripheral Management** > **Audio** to enable or disable the pop-up that is displayed when you plug in analog headsets.
- **SmartCard Certificate Show Common Name**—Added **SmartCard Certificate Show Common Name** in **Login Experience** > **SmartCard Settings** to display the common certificate name as the username when you use a smart card to log in.
- **Admin User Password**—Changed the minimum required length of **Admin User Password** from 8 characters to 9 in **Privacy & Security** > **Account Privileges**.
- **System Information**—Added **System Information** in **Privacy & Security** > **Account Privileges** to enable or disable the account privilege of having system information window.
- **Security Type**—Added **WPA3 Personal** and **Opportunistic Wireless Encryption** under the **Security Type** drop-down list in **Network Configuration** > **Wireless Settings**.
- **Current BIOS Admin Password**—Added **Current BIOS Admin Password** in the **BIOS** pages of all platforms.

  ⓘ **NOTE:** If you have not synced the BIOS password in the **Wyse Management Suite** server, you can enter the current BIOS password in this field to publish the BIOS settings. If you have synced the BIOS password in the Wyse Management Suite server, this field is ignored.

  ⓘ **NOTE:** If you enable **Set Admin Password**, set new BIOS password and then reboot, the new BIOS password is synced to WMS server automatically. If you first enable **Set Admin Password**, set the new BIOS password, and then disable **Set Admin Password**, the BIOS password is cleared to empty. On the thin client, the **Current BIOS Admin Password** option is always blank, and **Set Admin Password** option is always disabled. These options do not have any impact on the functionality.
- **Playing video**—Added the option to add a video in **Personalization** > **Screen Saver** > **Screen Saver Type**. Click **Browse** to upload a video file. The maximum file size that is allowed is 100 MB.
- **Brightness**—Added **Brightness** option in **Peripheral Management** > **Monitor** > **Monitor Settings** for adjusting the brightness of the built-in display. The option is only applicable on Wyse 5470 and Wyse 5470 All-in-One thin clients. The option is not available on external monitors.
- **Main Screen**—Removed **Main Screen** from **Peripheral Management** > **Monitor** > **Monitor Settings** > **MultiHead Monitor** > **Mirror Mode**. **Main Screen** is only available under Span mode.
- **Enable the Intel's special GPU buffer format for Dual GPU (5070 Extended only)**—Enabled the option in **Peripheral Management** > **Monitor** > **Monitor Settings**.

  ⓘ **NOTE:** If you face issues with the mouse cursor speed, disable this option to improve the performance.
- **MultiHead Monitor**—Added **Monitor Resolution** and **Monitor Rotation**options in **Peripheral Management** > **Monitor** > **Monitor Settings** to support configuring display resolution and rotation in mirror mode with multihead monitor enabled.

- **Default Printer**—The default printer list in **Peripheral Management** > **Printers** > **Printer Settings** only supports LPD1-LPD19.
- **LPD Printer**—The LPD printer list in **Peripheral Management** > **Printers** > **Printer Settings** only supports LPD1-LPD19.
- **Enable Show Group Key**—Added the option **Enable Show Group Key** in **Services** > **WDA Settings** to enable an eye symbol that you can click to display the WMS group registration key.
- **Key Length**—Changed the default value for **Key Length** in **Privacy & Security** > **SCEP** > **SCEP Settings** to 4096 from 2048.
- **Manual Override**—Added **Manual Override** option in **Region & Language Settings** > **TimeServer Settings**. If you enable this option, changes made to the **TimeServer Settings** in the ThinOS local UI takes priority. The default value is disabled.
- **Optimize for CPU**—Added **Optimize for CPU** option in **Peripheral Management** > **Camera**. The option is enabled by default. The recommended settings for camera format, resolution and FPS are automatically set. The default settings are **`format=RAW`**, **`resolution=320X240`** and **`FPS=10`**. You can customize **Camera Format**, **Camera Width**, **Camera Height**, and **Camera FPS** settings after disabling this option. Before you configure the camera settings, ensure that the camera supports the specified resolution and FPS. Increasing the resolution and FPS impacts the performance. The default camera device in the Admin Policy Tool or Wyse Management Suite policy settings is not supported in this release.
- **Authority URL** and **Authority Endpoint**—Changed the **Authority URL** and **Authority Endpoint** options in **Broker Settings** > **Azure Virtual Desktop Settings**to read only.
- Updated the VDI configuration editor settings that cannot be modified. For more information, see the *VDI Configuration Editor* section in the latest *Dell Wyse ThinOS 9.1.4234, 9.1.5067, and 9.1.6108 Administrator's Guide* at www.dell.com/support.
- Updated the ThinOS 9.x policy settings for OptiPlex 3000 Thin Client.
  - Removed the **Business Hours** option.
  - Changed the option **Disabling Push Notification** to **Ignore MQTT**.
- **Terminal Name**—If the default value has been changed, the value of **Terminal Name** does not change when you set **`$TN`** in the policy or change the group of **Wyse Management Suite** server.
  - To change the terminal name—Insert a different name in the policy and send a new name using **Change Host Name** command from Wyse Management Suite.
  - To reset to the default value—Insert a special string **`-default-`** in the policy to reset to default value and then reset the system settings to factory default in the ThinOS local client.

VMware Horizon update

VMware Horizon RSA login enhancement—Added RSA logo to the Horizon RSA login window to emphasize the **RSA passcode** input field.

VMware Horizon Blast limitations

- Multimedia Redirection—There can be performance issues on videos that are played using Multimedia Redirection in VMware Horizon Blast. The issue is observed when you install both VMware Horizon and Windows Virtual Desktop packages together. As a workaround, uninstall the Azure Virtual Desktop (Microsoft AVD) package. For information about how to delete the package, see the *Dell Wyse ThinOS 9.1.4234, 9.1.5067, and 9.1.6108 Administrator's Guide* at www.dell.com/support.
- Cisco JVDI—Sometimes JVDI fails to register. This issue is a ThinOS issue. On VMware Ubuntu Linux client, JVDI can be registered manually. But, as a workaround for this issue, do not register JVDI manually. JVDI registers automatically if you wait for 5-10 m. However, if you register manually, JVDI may not get registered and it cannot be used.
- HEVC on OptiPlex 3000 Thin Client—OptiPlex 3000 Thin Client does not support HEVC.
- If an error message that states **Zoom Plugin is missing some components. Please reinstall the plugin to restore it** is displayed when you connect to a Zoom call, remove all the application packages from the client, and reinstall them.

Supported peripherals

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

Table 9. Supported peripherals

Product Category	Peripherals
Adapters and cables	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter
	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087
	Dell Adapter - DisplayPort to VGA - DANBNBC084
	Dell Adapter - HDMI to DVI - DAUARBN004
	Dell Adapter - HDMI to VGA - DAUBNBC084
	Dell Adapter - USB-C to DisplayPort - DBQANBC067
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter
	Dell Adapter - USB-C to HDMI - DBQAUBC064
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070
	Dell Adapter - USB-C to VGA - DBQBNBC064
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232
	Trendnet USB to Serial Converter RS-232
Audio devices	Dell 2.0 Speaker System - AE215
	Dell Pro Stereo Headset - Skype for Business - UC350
	Dell Pro Stereo Headset - UC150 - Skype for Business
	Dell Professional Sound Bar (AE515M)
	Dell USB Sound Bar (AC511M)
	Dell Wired 2.1 Speaker System - AE415
	Jabra BIZ 2400 Duo USB MS
	Jabra EVOLVE UC VOICE 750
	Jabra Engage 65 Stereo Headset
	Jabra Evolve 65 MS Stereo - Headset
	Jabra Evolve 75
	Jabra Engage 75
	Jabra GN2000
	Jabra PRO 935 USB Microsoft Lync Headset - 935-15-503-185
	Jabra Pro 9450
	Jabra Speak 510 MS Bluetooth
	Jabra UC SUPREME MS Bluetooth (link 360)
	LFH3610/00 Speechmike Premium—Only supports redirect
	Logitech S-150
	Logitech h150 - analog
	Nuance PowerMic II—supports to redirect whole device
	Olympus RecMic DR-2200—supports to redirect whole device
	PHILIPS - analog
	POLYCOM Deskphone CX300

Table 9. Supported peripherals (continued)

Product Category	Peripherals
	Plantronics AB J7 PLT
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Blackwire 5220 Series
	Plantronics Blackwire C5210
	Plantronics Calisto P820-M
	Plantronics SAVI W740/Savi W745—supports USB only and does not support bluetooth
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0
	Plantronics Voyager 6200 UC
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync
	EPOS | SENNHEISER D 10 USB ML-US Wireless DECT Headset
	EPOS | SENNHEISER SC 40 USB MS
	EPOS | SENNHEISER SC 660 USB ML
	EPOS | SENNHEISER SDW 5 BS-EU
	EPOS | SENNHEISER SP 10 ML Speakerphone for Lync
	EPOS | SENNHEISER USB SC230
Camera	Dell Utra WB7022
	Jabra PanaCast 4K Webcam
	Logitech BRIO 4K Webcam
	Logitech C910 HD Pro Webcam
	Logitech C920 HD Pro Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C925e Webcam
	Logitech C930e HD Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Poly EagleEye Mini webcam
Displays	C2422HE
	C2722DE
	C3422WE
	E1916H
	E1920H
	E2016H
	E2016Hv—China only
	E2020H
	E2216H
	E2216Hv—China only
	E2218HN

Table 9. Supported peripherals (continued)

Product Category	Peripherals
	E2220H
	E2318H
	E2318HN
	E2417H
	E2420H
	E2420HS
	E2720H
	E2720HS
	MR2416
	P1917S
	P2016
	P2017H
	P2018H
	P2217
	P2217H
	P2219H
	P2219HC
	P2317H
	P2319H
	P2415Q (3840 x 2160)
	P2417H
	P2418D
	P2418HT
	P2418HZ
	P2419H
	P2419HC
	P2421D
	P2421DC
	P2715Q (3840 x 2160)
	P2719H (1920 x 1080)
	P2719HC
	P2720D
	P2720DC
	P3418HW
	P4317Q
	S2719HS (1920 x 1080)
	S2817Q (3840x2160)

Table 9. Supported peripherals (continued)

Product Category	Peripherals
	U2415
	U2419H
	U2419HC
	U2421HE
	U2518D
	U2520D
	U2713HM (2560 x 1440)
	U2718Q (4K) (3840 x 2160)
	U2719D (1920 x 1080)
	U2719DC
	U2720Q
	U2721DE
	U3219Q (3840 x 2160)—No support for Type C to HDMI convertor
	U3419W (3440 x 1440)
	U4320Q
	U4919DW
Docking station	Dell Dock - WD19-C
	Dell Thunderbolt Dock - WD19TB—Thunderbolt Display is not supported
Fingerprint readers	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader
	Imprivata HDW-IMP-1C
	KSI-1700-SX Keyboard
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR—BLEdongle
Input devices (Keyboard and Mouse)	Bloomberg Keyboard STB 100
	Dell Keyboard KB212-B
	Dell Keyboard KB216p
	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse
	Dell Laser Wired Mouse - MS3220
	Dell Mobile Pro Wireless Mice - MS5120W
	Dell Mobile Wireless Mouse - MS3320W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W
	Dell Multi-Device Wireless Mouse - MS5320W
	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123

Table 9. Supported peripherals (continued)

Product Category	Peripherals
	Dell Premier Wireless Mouse - WM527
	Dell USB Wired Keyboard - KB216
	Dell USB Wired Optical Mouse - MS116
	Dell Wireless Keyboard and Mouse - KM636
	Dell Wireless Keyboard/mouse KM632
	Dell Wireless Mouse - WM126 - black
	Dell Wireless Mouse - WM326
	Dell wireless Keyboard/mouse KM714
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white
	Microsoft Arc Touch Mouse 1428
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth
	Seal Shield Medical Grade Optical Mouse
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white
	SpaceMouse Pro
	SpaceNavigator 3D Space Mouse
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Others	Intuos Pro Wacom
	Wacom One
Printers	Brother DCP-7190DW—works on ICA only and not Blast
	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer
	Dell B2360d Laser Printer
	Dell B2360dn Laser Printer
	Dell Color Multifunction Printer - E525w
	Dell Color Printer- C2660dn
	Dell Multifunction Printer - E515dn
	HP Color LaserJet CM1312MFP—tested on Blast
	HP LaserJet P2055d
	HP M403D— works on ICA only and not Blast
	Lexmark X864de- tested on LPD only
Proximity card readers	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80
	Imprivata HDW-IMP-82
	KSI-1700-SX Keyboard

Table 9. Supported peripherals (continued)

Product Category	Peripherals
	OMNIKEY 5025CL
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM
	OMNIKEY 5325 CL
	OMNIKEY 5326 DFR
	RFIDeas RDR-6082AKU
Signature tablets	TOPAZ Signature Tablet T-LBK462-B8B-R
	Wacom Signature Tablet STU-500B
	Wacom Signature Tablet STU-520A
	Wacom Signature Tablet STU-530
	Wacom Signature Tablet STU-430/G
Smart card readers	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU-
	Cherry SmartTerminal SMART Card Reader - ST-1044U
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0
	Cherry keyboard KC 1000 SC with smart card
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Dell Keyboard SK-3205 with smart card reader
	Dell keyboard KB813 with smart card reader
	Dell keyboard KB813t with smart card reader
	GemPC Twin
	Gemalto IDBridge CT710
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	IDBridge CT31 PIV
	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	SmartOS powered SCR3310
	SmartOS powered SCR335
	Sun microsystem SCR 3311
Storage	Bano type-c 16B
	Dell External Tray Load ODD (Agate)—DVD Writer
	Dell Portable SSD, USB-C 250 GB
	Kingston DT microDuo 3C 32 GB
	Kingston DTM30 32 GB
	Kingston DataTraveler G3 8 GB
	Samsung portable DVD Writer SE-208

Table 9. Supported peripherals (continued)

Product Category	Peripherals
	SanDisk Cruzer 16 GB
	SanDisk Cruzer 8 GB
	SanDisk USB 3.1 and Type-C 16 GB
	SanDisk Ultra Fit 32 GB
Teradici remote cards	Teradici host card 2220
	Teradici host card 2240

Supported peripherals for OptiPlex 3000 Thin Client

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

Table 10. Supported peripherals for OptiPlex 3000 Thin Client

Product Category	Peripherals
Audio and Video	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Headset - Cortez - WH3022.
	Logitech BRIO 4K Ultra HD Webcam - 960-001105
	Logitech C525 HD Webcam - 960-000715
	Logitech C930e HD Webcam - 960-000971
	Dell Pro Stereo Soundbar - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - Potential M
	Jabra Engage 65 MS Wireless Headset - 9559-553-125
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo
Displays	Dell UltraSharp 24 Monitor - U2422H
	Dell 24 Monitor - P2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE
	Dell 24 USB-C Hub Monitor - P2422HE
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE
	Dell 27 USB-C Hub Monitor - P2722HE
	Dell UltraSharp 27 Monitor - U2722D
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE
	Dell 27 Monitor - P2722H
	Dell 22 Monitor - P2222H
	Dell 24 Monitor - P2421
	Dell 24 Monitor - P2421D
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE

Table 10. Supported peripherals for OptiPlex 3000 Thin Client (continued)

Product Category	Peripherals
	Dell 20 Monitor E2020H
	Dell 27 Monitor - P2720D
	Dell UltraSharp 25 USB-C Monitor - U2520D
	Dell 24 Monitor E2420HS
	Dell 27 Monitor - P2720D
	Dell 23 Monitor - P2319H
	Dell 27 Monitor E2720HS
	Dell 27 Monitor E2720H
	Dell 24 Touch Monitor - P2418HT
	Dell 19 Monitor E1920H
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q
	Dell 24 Monitor E2420H
Input devices (Keyboard and Mouse)	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - Comet
	Dell Multimedia Keyboard - KB216_BLACK - Rusty
	Dell Optical Mouse - MS116_BLACK - Sapphire
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine
	Dell KB813 Smartcard Keyboard - KB813- Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter
	Dell Business Multimedia Keyboard - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty
Storage	Dell USB Slim DVD +/û RW Drive - DW316 - Agate

Tested environments matrix

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

Table 11. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.6
Configuration UI package for Wyse Management Suite	1.5 324
Imprivata OneSign	7.7.000.10
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 12. Test environment—Citrix

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

Table 13. Tested environment—VMware Horizon

VMware	Windows 11	Windows 10	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs	Ubuntu 20.04
VMware Horizon 7.12	Not tested	Tested	Tested	Not tested	Tested	Not tested	Not tested
VMware Horizon 7.13	Not tested	Tested	Not tested	Tested	Not tested	Not tested	Not tested
VMware Horizon 2106	Not tested	Tested	Tested	Tested	Tested	Tested	Not tested
VMware Horizon 2111	Tested	Tested	Tested	Tested	Tested	Tested	Tested—Only basic connection is tested on Ubuntu 20.04

Table 14. Test environment—Microsoft RDP

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

Table 15. Test environment—AVD

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

Table 16. Tested environment—Skype for Business

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

Table 17. Tested environment—Skype for Business

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

Table 18. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	14.0.3.306553.1	14.0.3	14.0.3
	Windows server 2016			
	Windows server 2019			

Table 19. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	14.0.3	14.0.3	14.0.3
	Windows server 2016	14.0.3	14.0.3	14.0.3
	Windows server 2019	Not tested	Not tested	Not tested

Table 20. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	5.8.4.21112.1	5.8.4 (21112)
	Windows server 2016		
	Windows server 2019		

Table 21. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106	Windows 10	5.8.4.21112	5.8.4 (21112)
	Windows server 2016	5.8.4.21112	5.8.4 (21112)
	Windows server 2019	Not tested	Not tested

Table 22. Tested environment—Cisco Webex VDI

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	41.12.0.20899.1	41.12.0.20899
	Windows server 2016		
	Windows server 2019		

Table 23. Tested environment—Cisco Webex VDI

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	41.12.0.20899	41.12.0.20899
	Windows server 2016	41.12.0.20899	41.12.0.20899
	Windows server 2019	Not tested	Not tested

Table 24. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	41.12.6.12.1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.12 to 42.4.
	Windows server 2016		
	Windows server 2019		

Table 25. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106	Windows 10	41.12.6.12.1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.12 to 42.4. Webex Meeting does not work well with Horizon 2111. This is a Cisco limitation.
	Windows server 2016		
	Windows server 2019		

Supported smart cards

Table 26. Supported smart cards

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	G&D SCE 3.2
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Giesecke and Devrient SmartCafe Expert 7.0 (T=0)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840
ID Prime MD v 4.0.2 (Gemalto 840)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K

Table 26. Supported smart cards (continued)

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

Fixed issues

Table 27. Fixed issues

Issue ID	Description
DTOS-7069	**Dutch (Belgian)** and **French (Belgium)** keyboard layouts are not available in ThinOS 9.x—CIPS-25488.
DTOS-7066	When using Classic desktop mode with 9.1.5067, RDP icons do not show up on the desktop—CIPS-25380.

Table 27. Fixed issues (continued)

Issue ID	Description
DTOS-7010	After upgrading from ThinOS 9.1.3129 to 9.1.5067, the UI displays **Apps** even after configuring **Desktop only** —CIPS-25461.
DTOS-6996	Unable to get full screen for direct RDP connection that is configured using Admin Policy Tool—CIPS-25272.
DTOS-6993	ThinOS stops responding when you plug in analog head set after selecting the local language as German—CIPS-25367.
DTOS-6976	Enter key on the Num pad is not working—CIPS-25373.
DTOS-6969	Performance issues are observed in ThinOS when connected to Nexan Switch—CIPS-25423
DTOS-6967	Screen turns off when 3.5 MM Audio jack is connected in 5070 device—CIPS-25421.
DTOS-6819	Resolution changes and device lose focus while working in Citrix session on ThinOS 9.x—CIPS-25176.
DTOS-6759	Wireless configuration issues are observed when a comma is used in the password.
DTOS-6453	Sometimes an error message that states **hostname not resolved, DNS error** is displayed on the client.—CIPS-25154/CIPS-25184.
DTOS-6437	PowerMic 3 causes USB enumeration issues when it is not plugged in before BLAST session starts, or when it is disconnected and connected back in while a BLAST session is active—CIPS-25190.
DTOS-6347	Boot partition error is displayed while upgrading from ThinOS 9.1.3131 or 9.1.3129 to ThinOS 9.1.4234 firmware —CIPS-25043.
DTOS-6293	Fails to install Citrix application packages after upgrading to ThinOS 9.1.3129 or 4234 from ThinOS 8.6 using Wyse Management Suite—CIPS-24920.
DTOS-6279	Thin clients lose terminal name when moving to different group while upgrading from ThinOS 8.6 to 9.1.3129 or 4234 using Wyse Management Suite 3.5—CIPS-24926.
DTOS-5821	Unable to import password protected pfx certificate—CIPS-24582.
DTOS-5804	SIPR tokens stopped working after upgrading to ThinOS 9.1—CIPS-23733.
DTOS-5667	Slow virtual channel error in Webex VDI plugin on ThinOS 9.1—CIPS-24767.
DTOS-5627	VDI getting disconnected while using Single Access point—CIPS-24686.
DTOS-5596	Thin clients lose terminal name after upgrading to ThinOS 9.1.4234—CIPS-24542, Case 126661742.
DTOS-5586	Option to disable analog audio jack pop-up is not available on ThinOS 9.X—CIPS-24698.
DTOS-5569	Mouse wheel scrolls are too fast after upgrading to ThinOS 9.1.4234—CIPS-24555.
DTOS-5562	Device loses Wyse Management Suite cache configuration if Wyse Management Suite connection fails in ThinOS 9.x firmware—CIPS-24609.
DTOS-5541	No option to disable the **System Information** window—CIPS-24527.
DTOS-5521	Packages are downloaded twice when updating a Firmware—CIPS-24598.
DTOS-5462	If the user press key combinations **Ctrl + Alt ...** during Windows-session (BLAST), the focus changes from session to ThinOS—CIPS-24465.
DTOS-5413	Unbale to publish selected Citrix apps and VDI on ThinOS 9.1 similar to 8.X—CIPS-24523.
DTOS-5352	Floatbar does not go away after the session launches—CIPS-24424.
DTOS-5328	USB headset Hot Plug issue in RDS connection—CIPS-24383.
DTOS-5327	Cannot provide current BIOS password using policy settings instead of doing a BIOS sync—CIPS-23757.
DTOS-5204	Unable to use variables in hostname field of a Direct RDP connection in ThinOS 9.1—CIPS-24172.
DTOS-5086	E-signature dongle fails on ThinOs 9.1.x—CIPS-23921.
DTOS-5051	The mouse cursor lags when connected to AMD GPU DP mini port—CIPS-23947.
DTOS-5049	Unable to type the password in the password field while unlocking the client—CIPS-23870

Table 27. Fixed issues (continued)

Issue ID	Description
DTOS-4947	Microsoft HD-3000 webcam LED is always on—CIPS-23815.
DTOS-4909	Manual Override option for audio devices is not available in ThinOS 9.1—CIPS-23753.

Known issues

Table 28. Known issues

Issue ID	Description	Workaround
DTOS-5726	VNC settings timeout type and the timeout policy do not show the expected values when launching a VNC client.	There is no workaround in this release.
DTOS-6426	There is no audio on the videos played using Multimedia redirection. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Go to **Peripherals** > **Audio** on the client and click **OK**. The audio resumes playing.
DTOS-5761	Webcam redirection on 32-bit applications does not work with 1280x720p video resolution. **gs_read1.0 CPU** usage displays 100%, and the client stops responding after about 10 minutes.	Reduce the webcam resolution to 320p or 480p from ThinOS **Peripherals** > **Camera**.
DTOS-6386	During a Citrix session, if you enable multiple audio and open the **Recording** tab from the **Sound** window, the session gets disconnected. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Do not open **Sound** > **Recording**. You cannot switch the recording device in Windows Sound settings.
DTOS-6920	The client does not download package files from Wyse Management Suite. The client does not retry the download either. **Error 7700, 115** is displayed in the event log.	Check in Wyse Management Suite again manually or reboot the client.
DTOS-7008	During a VDI session, Citrix HDX audio volume bar gets adjusted when using the volume control buttons on the keyboard. The issue is observed on Wyse 5470 All-in-One thin clients.	If **Enable volume control for client volume** is added as part of Admin Policy Tool, the user does not have to adjust volume in the VDI session.
DTOS-7108	If you set **Close lid action on battery power** to shut down device when you have an external monitor connected to the thin client, the external screen stays lit. The issue is observed on Wyse 5470 thin clients.	There is no workaround in this release.
DTOS-6958	An error message that states **Unable to connect you to your desktop. Try again or contact your administrator for assistance** is displayed on the PIE login window after signing off from a VDI session. The issue is observed on Imprivata version 7.7.1134.	Ignore this error message. It does not impact Imprivata OneSign server connection.
DTOS-7414	Skype for Business calls with 32-bit Skype for Business application, without using RTME, has an audio and video lag of 4-5 s. The issue is observed on Wyse 3040 thin clients.	Use RTME for Skype for Business calls.
DTOS-7385	Audio is sometimes noisy and not audible on Zoom meetings while using 32-bit Zoom VDI application and Citrix HDX Webcam. The issue is observed on Wyse 5470 All-in-One thin clients.	Do Zoom meeting with optimization enabled.
DTOS-7092	Imprivata does NOT work in PCoIP session. The issue is observed on clients with Horizon version 2111 and Imprivata 7.7.	Do not use Horizon 2111 environment. Use Blast protocol.
DTOS-6837	JVDI cannot register with VMware Blast.	Do not register manually. Wait about 5-10 m, JVDI will register automatically.
DTOS-7038	Citrix broker connections display an error that states **An unknown login error occurred** when setting broker timeout as 5 seconds.	Use the default settings for **Advanced** > **Broker Session**

Table 28. Known issues (continued)

Issue ID	Description	Workaround
		> **Citrix Broker Settings** > **Timeout**.
DTOS-6741	The default audio input and output device does not change when you change the default audio device from the application in a session. The default device that is selected on the client is used for audio input and output. The issue occurs when multiple audio is enabled. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Disable multiple audio.
DTOS-7257	**OK** button under the properties window does not work in Citrix ICA session.	There is no workaround in this release.
DTOS-7400	Camera settings for Logitech webcam models do not display any resolution and frames per second.	The issue is observed only on secondary cameras. Use the primary camera
DTOS-7380	Horizon Universal Broker cannot be connected.	Universal Broker is not supported in this release.
DTOS-7403	Customizing the supported FPS for HDX webcam is not supported when using HDX webcam technology.	There is no workaround in this release.
DTOS-7185	No default camera option in Admin Policy Tool.	This feature is not supported in this release.
DTOS-7064	After disabling network proxy in Wyse Management Suite policy settings, Admin Policy Tool still displays the default settings. Wyse Management Suite settings are not synced with Admin Policy Tool.	There is no workaround in this release.
DTOS-6894	Network speed is slow when you connect the network cable to monitor for PCR. The issue is observed on Wyse 5470 thin client.	There is no workaround in this release.
DTOS-7313	Jabra Evolve 75 headset that is mapped to a Citrix session desktop keeps showing **Connected** and **Not Connected** status repeatedly.	Do not use Jabra Evolve 75 headset.
DTOS-7405	Camera settings does not update automatically when you disconnect and plug back in external camera. The issue is observed on Wyse 5470 thin clients.	Close the camera settings and reopen.
DTOS-7417	After disabling WMS, it still checks the Group registration code on ThinOS UI. The issue is observed on Wyse 5470 thin clients.	Do not disable WMS when group key is empty.
DTOS-6998	The external camera with HDX webcam redirection in 32-bit applications does not work on Wyse 5470 All-in-One thin clients. On Wyse 5070 thin clients, second camera does not work.	Use only the built-in camera on Wyse 5470 and 5470 All-in-One thin clients. Connect only one camera to Wyse 3040, 5070 or OptiPlex 3000 thin clients.
DTOS-7449	Smartcard fails to log in Citrix broker after disconnecting or reconnecting ICA session multiple times.	Remove and replugin smartcard.
DTOS-7472	Sometimes the camera settings do not sync from Wyse Management Suite to **wfclient.ini**.	Reboot the client.
DTOS-5356	High **CPU usage** is observed with Zoom call optimization.	The issue is due to a Zoom limitation. For more information, see https://support.zoom.us/hc/en-us/articles/201362023-Zoom-system-requirements-Windows-macOS-Linux.
DTOS-7160	HEVC does not work with VMware Blast. The issue is observed on OptiPlex 3000 Thin Client.	There is no workaround in this release.
DTOS-7190	When you restart the client after connecting a Bluetooth device, the Bluetooth device gets connected automatically after the restart, but the connection status is displayed incorrectly. The issue is observed on OptiPlex 3000 Thin Client.	Reconnect the Bluetooth device.

Table 28. Known issues (continued)

Issue ID	Description	Workaround
DTOS-7077	Updated Static IP address is not reflecting in Systray after changing the static IP. The issue is observed on OptiPlex 3000 Thin Client.	There is no workaround in this release.
DTOS-8143	Zoom Horizon VDI package does not work in a session—**CIPS-26069**.	For the Zoom Horizon VDI package to work in a session, it must be uninstalled and reinstalled.

4

ThinOS 9.1.5067

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 date

December 2021

Previous version

ThinOS 9.1.4234

Firmware upgrade

The following firmware upgrade scenarios are supported:

- ThinOS 8.6_807 > ThinOS 9.1.5067
- ThinOS 9.1.3129 or 9.1.4234 > ThinOS 9.1.5067

NOTE: If you are using earlier versions of ThinOS 8.6, you must first upgrade to ThinOS 8.6_807 and apply the latest BIOS updates before upgrading to ThinOS 9.1.5067. If you are using earlier versions of ThinOS 9.x, you must first upgrade to ThinOS 9.1.3129 or later versions before upgrading to ThinOS 9.1.5067.

For more information, see the *Dell Wyse ThinOS Version 9.1.4234 and 9.1.5067 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

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

  NOTE: Dell Technologies recommends that you set a new ThinOS application package or a ThinOS firmware package in Group 1, so that thin client installs the package, and automatically reboots, and changes to Group 2.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.
- When you set a new firmware or an application package in Wyse Management Suite group 2 and then change the device from group 1 to group 2 before upgrading, the following two notifications are displayed:
  - **Wyse Management Suite server or group is changed. System is going to reboot to load full configuration. Press cancel in 60 seconds to prevent reboot**.

    - **A new firmware or application is available, do you want to upgrade now or defer to the next reboot? The changes will automatically be applied in 120 seconds.**

    If you do not select an option, the thin client reboots after 60 seconds. After the reboot, the new application or firmware is installed and the thin client reboots again. The thin client will be in group 2 after the reboot.

- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
    - Displays a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
    - Not display any notification if the new firmware or application is downloaded in the same group.
    - Installs the firmware or package after a reboot.

Prerequisites for firmware upgrade

- Update the BIOS version of Wyse 5070 Thin Client to 1.3.1 or later before upgrading to ThinOS 9.1.5067. If you upgrade to ThinOS 9.1.5067 with earlier BIOS version and then upgrade the BIOS version to 1.3.1 or later, the device may fail to boot. If there is a boot failure, check if the PTT option is available under security in BIOS Setup. For Wyse 5070 Thin Clients with firmware TPM configuration, the PTT option is available after updating BIOS to 1.3.1 or later versions. You must disable the option and boot into ThinOS if you fail to boot after upgrade BIOS. For latest BIOS versions, see Tested BIOS version for ThinOS 9.1.5067.
- Before you migrate from ThinOS 8.6_807 to ThinOS 9.1.5067 or upgrade from ThinOS 9.x to 9.1.5067, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the Wakeup On LAN command through Wyse Management Suite before using any real-time commands. To use the Wakeup On LAN command, ensure that the Wakeup On LAN option is enabled in BIOS.

Upgrade from ThinOS 9.1.x to ThinOS 9.1.5067 using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.1.3129 or later version on you thin client.
- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.
- Download the ThinOS 9.1.5067 (DTOS_9.1.5067.pkg) firmware to upgrade.

Steps

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

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

5. Click **Browse** and select the **ThinOS 9.1.5067** firmware to upload.
6. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
7. Click **Save & Publish**.
    The thin client downloads the firmware to install and restarts. The firmware version is upgraded.

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

Upgrade from ThinOS 8.6 to ThinOS 9.1.5067 using Wyse Management Suite

If you are running any ThinOS 8.6 version, you must first install the ThinOS 8.6_807 image with the latest BIOS version, and then upgrade to ThinOS 9.1.5067. For the latest BIOS versions, see the *Dell Wyse ThinOS Version 8.6_807 Release Notes* at www.dell.com/support.

The device reboots after the ThinOS image is downloaded. Once the upgrade completes, the device is automatically registered to Wyse Management Suite. Dell Technologies recommends you to back up your device settings before you initiate the upgrade process. All device settings are erased after you upgrade from ThinOS 8.6 except the following settings:

- **Wyse Management Suite group token and server settings**
- **Static DNS**
- **Certificates**
- **IEEE802.1x wired authentication settings**
- **Wireless connections**—The WEP/Sharekey security type is changed to **Open** as they are not supported in ThinOS 9.1
- **Proxy settings**

NOTE: For more information about how to install the ThinOS 9.1.5067 image, see the *Dell Wyse ThinOS Version 9.1.4234 and 9.1.5067 Migration Guide* at www.dell.com/support.

Compatibility

ThinOS application package details

- Cisco_Jabber_14.0.2.306216_3.pkg
- Cisco_WebEx_Meetings_VDI_41.10.3.19_2.pkg
- Cisco_WebEx_VDI_41.10.0.20213_4.pkg (formerly called Cisco WebEx Teams)
- Citrix_Workspace_App_21.9.0.25_6.pkg
- EPOS_Connect_7.0.0.19336_1.pkg
- HID_Fingerprint_Reader_210217_13.pkg
- Jabra_8.5.1_12.pkg
- Microsoft_AVD_1.5_1325.pkg
- Teradici_PCoIP_21.03.1_21.pkg
- VMware_Horizon_2106.8.3.0.18251983_9.pkg
- Zoom_Citrix_5.8.0.20927_8.pkg
- Zoom_Horizon_5.8.0.20927_8.pkg
- Imprivata_PIE_7.6.000.0005_1124.pkg
- Identity_Automation_QwickAccess_2.0.0.3.3.pkg

Wyse Management Suite and Configuration UI package

- Wyse Management Suite version 3.5
- Configuration UI package 1.5 300

ThinOS build details

- ThinOS 9.1.3129 or 9.1.4234 to ThinOS 9.1.5067—**DTOS_9.1.5067.pkg**.
- ThinOS 8.6_807 to ThinOS 9.1.5067 conversion builds:
  - **A10Q_wnos**—Wyse 3040 Thin Client
  - **PA10Q_wnos**—Wyse 3040 Thin Client with PCoIP
  - **X10_wnos**—Wyse 5070 Thin Client, Wyse 5470 Thin Client, and Wyse 5470 All-in-One Thin Client
  - **PX10_wnos**—Wyse 5070 Thin Client with PCoIP, Wyse 5470 Thin Client with PCoIP, and Wyse 5470 All-in-One Thin Client with PCoIP

BIOS packages

Table 29. BIOS package

Platform model	Package filename
Wyse 5070 Thin Client	bios-5070_1.13.1.pkg

Table 29. BIOS package (continued)

Platform model	Package filename
Wyse 5470 Thin Client	bios-5470_1.10.1.pkg
Wyse 5470 All-in-One Thin Client	bios-5470AIO_1.10.1.pkg

Tested BIOS version for ThinOS 9.1.5067

Table 30. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Thin Client	1.13.1
Wyse 5470 All-in-One Thin Client	1.10.1
Wyse 5470 Thin Client	1.10.1

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

New and enhanced features

Citrix Workspace app updates

- **Exporting Citrix Workspace app logs**—Citrix Workspace app logs can only be exported from **Troubleshooting** > **General** > **Export Logs** on the ThinOS device.

  For more information about how to export Citrix Workspace app logs, see the *Dell Wyse ThinOS 9.1.4234 and 9.1.5067 Administrator's Guide* at www.dell.com/support.

- **Keyboard Layout Server Default Mode enhancement**—From Citrix Workspace App 2109 and ThinOS 9.1.5067 onwards, only the Server Default mode uses the **Scancode**. Other Keyboard layout modes such as Specific Keyboard, Client Setting, and Dynamic Sync use the default Unicode. There are no changes to the other keyboard layout modes in Citrix Workspace App 2109.

  To configure, do the following:

  1. Set the Keyboard Layout Mode to Server Default using Admin Policy Tool or Wyse Management Suite.
  2. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced tab** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
  3. In the Citrix INI settings section, 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 `KeyboardEventMode`.
  8. In the **Value** field, enter `Scancode`.
  9. Sign out or restart the device for settings to take effect.

     NOTE: If you want to change the Server Default mode to other keyboard layout modes, you must remove the `KeyboardEventMode` with `Scancode` setting from **Citrix Configuration Editor**.

  For more information about how to configure the VDI Configuration Editor, see the *Dell Wyse ThinOS 9.1.4234 and 9.1.5067 Administrator's Guide* at www.dell.com/support.

- **Citrix VDA policy setting update**—In Citrix VDA 2109 and later versions, the Citrix VDA policy setting **Virtual channel allow list** is enabled by default. As a result, the non-Citrix virtual channels, such as Zoom, WebEx VDI, WebEx Meetings VDI, JVDI, Imprivata OneSign and HID do not work. You can disable the setting, or find the name of the third-party virtual channel and add it to the virtual channel allow list. For more information, see the *Citrix documentation* at docs.citrix.com.

Limitations

- After you enable the Citrix Workspace app log feature and join the Microsoft Teams meeting, the ICA session stops responding for a few seconds.
- Citrix session gets disconnected if Adaptive Audio is enabled when you connect to a VDI desktop that runs on Citrix VDA 2109. You must disable Adaptive Audio function to connect to Citrix VDA 2109 desktop. This issue is observed in Linux Citrix Workspace app binary.
  - If you are using Desktop Delivery Controller (DDC) version 2109, you can find the Adaptive Audio policy, and disable it using the policy settings.
  - If you are using DDC version 1912, change the registry value of REG_DWORD EnableAdaptiveAudio to 0 in the following registry paths:
    - **`Desktop VDA (Windows 10)—HKLM\Software\Citrix\Audio`**
    - **`Server VDA (Server 2016\2019)—HKLM\Software\WOW6432Node\Citrix\Audio`**
- The video resolution may be downgraded when you close and replay the Multimedia redirection (MMR) enabled video. This is observed when the thin client is connected to a VPN.
- If you are using a low-bandwidth network connection, the 1080p MMR video stops playing with no audio output. This is observed in a Citrix ICA session.
- Battery status does not appear on the session desktop when you launch a session on Wyse 5470 Thin Client. This issue is resolved in Citrix Workspace app 2111.
- The published Skype For Business application cannot connect to RTME.
- During a Microsoft Teams meeting, echo is observed when you disconnect a headset from the device.
- Audio noise is observed when recording voice with an analog or USB headset in the VDI session. This issue is observed on Wyse 5070 Thin Client.
- Microsoft Teams share screen function is disabled automatically when you switch the mouse to the client during the Teams call.
- The Citrix desktop screen does not display correctly when the Citrix policy **Use video codec for compression** is configured for the entire screen.
- The server VDA desktop stops responding when you are using a smart card to reconnect the session.
- Bluetooth device cannot be detected in the JVDI device list.
- If you open the camera in a session desktop, you cannot use the camera for other applications. You must log out of the account and log in back to the desktop.
- Sometimes, Microsoft teams audio and camera change to None on the Settings Devices list.

Azure Virtual Desktop updates

- Windows Virtual Desktop (WVD) is renamed to Azure Virtual Desktop (AVD).
- Supports camera redirection in an RDP session. Connect your camera to the thin client and launch the RDP session. The camera is redirected automatically.

  NOTE: The direct show application feature does not work properly when using the camera redirection in an RDP session.

For more information, see the *Dell Wyse ThinOS Version 9.1.4234 and 9.1.5067 Administrator's Guide* at www.dell.com/support.

VMware Horizon Blast limitations

- **Headset Redirection**—Dell sound bar SP3022/SB522A USB redirection is not supported on ThinOS. The Blast session stops responding when you use this device. This is a VMware limitation.
- **Session audio**—Sometimes the session has no audio output when you hot plug a headset. As a workaround, you must switch the audio from the ThinOS local system to HD audio and then switch back to Headset.
- **CPU performance**—If you do not sign off from the broker but only disconnects the blast session multiple times, there are a lot of mks processes in the system. This is a VMware limitation.
- **Webex VDI**—Sometimes Webex VDI is not optimized in a Horizon session, As a workaround, you must reboot the device and relaunch the Webex VDI application.

VDI Configuration Editor

ThinOS enables the IT administrator to configure the VDI-related settings by dynamically modifying the VDI configuration files of your ThinOS device. You can configure the Citrix settings, Horizon Blast settings, and Zoom plug-in settings either using Admin Policy Tool or Wyse Management Suite.

To use the VDI settings feature, you must first upgrade to Wyse Management Suite v3.5.866 using the Configuration UI package v1.5 300 or later. If you are using Wyse Management Suite public cloud, the Configuration UI package is updated automatically by Dell.

ⓘ **NOTE:** Ensure that you read the disclaimer that is highlighted on the VDI Configuration Editor page before configuring the options. Improper configuration may lead to VDI applications not work properly. You must also read the Citrix, VMware, and Zoom official documentation from their respective websites to set the relevant VDI settings. All settings are case-sensitive.

To access the configuration page, go to **Advanced** > **VDI Configuration Editor** on Wyse Management Suite policy settings or Admin Policy Tool. For more information about how to configure the VDI dynamic settings, see the *Dell Wyse ThinOS 9.1.4097, 9.1.4234, 9.1.5067, and 9.1.6108 Administrator's Guide* at www.dell.com/support.

ⓘ **NOTE:** VDI settings will dynamically write into the VDI configuration files of the device. For settings to take effect, you must log out and log in to the broker again, or configure the settings before logging into the broker.

Citrix Configuration Editor

Citrix VDI settings

ⓘ **NOTE:** Ensure that you read the disclaimer that is highlighted on the VDI Configuration Editor page before configuring the options. Improper configuration may lead to VDI applications not work properly. You must also read the Citrix official documentation from docs.citrix.com to set the VDI settings. All settings are case-sensitive.

Citrix settings are classified by VDI application and configuration type. The following Citrix VDI settings are supported:

- Citrix INI settings
- Citrix XML settings
- Citrix JSON settings
- Citrix Keyboard layout settings

To update the file settings for Citrix VDI, see the Citrix Workspace app documentation at docs.citrix.com.

The following are the supported configuration file paths for Citrix Workspace app:

- /opt/Citrix/ICAClient/config/All_Regions.ini
- /opt/Citrix/ICAClient/module.ini
- ~/.ICAClient/wfclient.ini
- /opt/Citrix/ICAClient/config/wfclient.template
- /opt/Citrix/ICAClient/config/AuthManConfig.xml
- /opt/Citrix/ICAClient/config/kbdlayoutmap.tbl
- /var/.config/citrix/hdx_rtc_engine/config.json
- ~/.ICAClient/appsrv.ini

Citrix INI settings allow you to enable or disable the Unified Communication Optimization when UC packages are installed on ThinOS. The following UC configurations are qualified by Dell Technologies:

Table 31. Enable or disable UC plug-in settings

UC Plug-ins	Enable UC Plug-in using VDI settings	Disable UC Plug-in using VDI settings	Details
Zoom Citrix	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: ZoomMedia Value: On	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: ZoomMedia Value: Off	Change the values On/Off in module.ini to enable or disable the UC plug-in. Plug-in switch string is located in the section [ICA 3.0].

Table 31. Enable or disable UC plug-in settings (continued)

UC Plug-ins	Enable UC Plug-in using VDI settings	Disable UC Plug-in using VDI settings	Details
	These settings enable the Zoom optimization with ZoomMedia=On in module.ini. These are the default settings after you install the UC package.	These settings disable the Zoom optimization with ZoomMedia=Off in module.ini.	
Cisco WebEx VDI	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: CiscoTeamsVirtualChannel Value: On These settings enable Cisco WebEx VDI optimization with CiscoTeamsVirtualChannel=On in module.ini. These are the default settings after you install the UC package.	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: CiscoTeamsVirtualChannel Value: Off These settings disable Cisco WebEx VDI optimization with CiscoTeamsVirtualChannel= Off in module.ini.	Change the values On/Off in module.ini to enable or disable the UC plug-in. Plug-in switch string is located in the section [ICA 3.0].
Cisco WebEx MeetingsVDI	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: CiscoMeetingsVirtualChannel Value: On These settings enable Cisco WebEx Meetings VDI optimization with CiscoMeetingsVirtualChannel=On in module.ini. These are the default settings after you install the UC package.	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: CiscoMeetingsVirtualChannel Value: Off These settings disable Cisco WebEx Meetings VDI optimization with CiscoMeetingsVirtualChannel =Off in module.ini.	Change the values On/Off in module.ini to enable or disable the UC plug-in. Plug-in switch string is located in the section [ICA 3.0].
Cisco Jabber	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: CiscoVirtualChannel Value: On These settings enable Cisco JVDI optimization with CiscoVirtualChannel=On in module.ini. These are the default settings after you install the UC package.	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: CiscoVirtualChannel Value: Off These settings disable Cisco JVDI optimization with CiscoVirtualChannel=Off in module.ini.	Change the values On/Off in module.ini to enable or disable the UC plug-in. Plug-in switch string is located in the section [ICA 3.0].
Microsoft Teams	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: VDWEBRTC Value: On These settings enable Microsoft Teams optimization with VDWEBRTC =On in module.ini. These are the default settings after you install the UC package.	File: module.ini Operation: Add or Update Section: ICA 3.0 Key: VDWEBRTC Value: Off These settings disable Microsoft Teams optimization with VDWEBRTC=Off in module.ini.	Change the values On/Off in module.ini to enable or disable the UC plug-in. Plug-in switch string is located in the section [ICA 3.0].
RTME	File: module.ini Operation: Add or Update	File: module.ini Operation: Add or Update	Change the values On/Off in module.ini to enable or disable the UC plug-in.

Table 31. Enable or disable UC plug-in settings (continued)

UC Plug-ins	Enable UC Plug-in using VDI settings	Disable UC Plug-in using VDI settings	Details
	Section: ICA 3.0 Key: HDXRTME Value: On These settings enable Skype for business optimization with HDXRTME =On in module.ini. These are the default settings after you install the UC package.	Section: ICA 3.0 Key: HDXRTME Value: Off These settings disable Skype for business optimization with HDXRTME =Off in module.ini	Plug-in switch string is located in the section [ICA 3.0].

Horizon Blast Configuration Editor

> **NOTE:** Ensure that you read the disclaimer that is highlighted on the VDI Configuration Editor page before configuring the options. Improper configuration may lead to VDI applications not work properly. You must also read the VMware official documentation at docs.vmware.com to set the VDI settings. All settings are case-sensitive. If a setting is defined in multiple locations, to know the value that must be used, see the VMware documentation.

The following are the supported configuration file paths for Horizon Blast Client:

- ~/.vmware/config
- ~/.vmware/view-preferences
- /etc/vmware/config
- /etc/vmware/view-default-config

Enable USB trace log—If you face any issues that are related to the USB device, you can enable the USB trace log for debugging purposes. Use the following setting in the `~/.vmware/config` configuration file:

```
 view-usbd.logLevel = "trace"
log.logMinLevel = 140
loglevel.user.usb = 10
```

Numeric keypad numlock——If you face any issue that is related to the numlock key of the USB numeric keypad, you can use the following setting in the `~/.vmware/config` configuration file to resolve the issue:

```
 mks.keyboard.suppressNumlocks = "TRUE"
mks.keyboard.enableHotkeyNumlockBinding = "TRUE"
```

Zoom Plugin Configuration Editor

> **NOTE:** Ensure that you read the disclaimer that is highlighted on the VDI Configuration Editor page before configuring the options. Improper configuration may lead to VDI applications not work properly. You must also read the Zoom official documentation at support.zoom.us to set the VDI settings. All settings are case-sensitive. To update the file settings under Zoom INI, refer to the Cisco document at Configuring the Zoom VDI Linux plugin with ZoomMedia.ini - Zoom Support.

The following are the supported configuration file paths for Zoom plug-ins:

- Zoom Citrix— `~/.ICAClient/config/ZoomMedia.ini`
- Zoom Horizon— `~/.vmware/ZoomMediaVmware.ini`

Important notes

Using the VDI configuration files, you cannot modify the following ThinOS settings that are included in Admin Policy Tool or Wyse Management Suite policy settings. A warning message is displayed when you modify the settings using VDI Configuration Editor.

Table 32. ThinOS settings - Not allowed to be modified

VDI/UC	Configuration files	Deny list
Citrix Workspace app	/opt/Citrix/ICAClient/usb.conf	All
	/opt/Citrix/ICAClient/config/All_Regions.ini	[Virtual Channels\Serial Port\Device] LastComPortNum=8 ComPort1= ComPort2= ComPort3= ComPort4= ComPort5= ComPort6= ComPort7= ComPort8=
	/opt/Citrix/ICAClient/config/module.ini	[ICA 3.0] KeyboardSync=
	~/.ICAClient/wfclient.ini	[WFClient] Version= KeyboardLayout= KeyboardMappingFile= KeyboardDescription= KeyboardType= CDMAllowed= DrivePath* DriveEnabled* DriveReadAccess* DriveWriteAccess* CursorStipple= TransportReconnectEnabled= ClientPrinterList=

	/var/.config/citrix/hdx_rtc_engine/config.json	{
		"ProxyHostname": "xxxx",
		"ProxyPort": xx
		}

	~/.ICAClient/appsrv.ini	[WFClient] COMAllowed=
VMware Horizon	~/.vmware/config	viewusb.AllowAutoDeviceSplitting= viewusb.SplitExcludeVidPid= viewusb.SplitVidPid= viewusb.ExcludeVidPid= viewusb.IncludeVidPid= viewusb.IncludeFamily=

Table 32. ThinOS settings - Not allowed to be modified (continued)

VDI/UC	Configuration files	Deny list
		viewusb.ExcludeFamily= mks.enableFIPSMode= usb.enableFIPSMode= viewusb.ExcludeAllDevices=
Zoom Citrix	~/.ICAClient/config/ZoomMedia.ini	[PROXY] proxyType= httpProxyHost= httpProxyPort= httpsProxyHost= httpsProxyPort=
Zoom Horizon	~/.vmware/ZoomMediaVmware.ini	[PROXY] proxyType= httpProxyHost= httpProxyPort= httpsProxyHost= httpsProxyPort=

Wyse Management Suite policy settings and Admin Policy Tool updates

- Added the **Manual override** option for selected settings. When the manual override feature is enabled, and the user performs the required action on the ThinOS local device, the configured policies from Wyse Management Suite for these settings are not applied to the ThinOS device.

Table 33. Manual override support matrix

Settings	Action to be performed on the ThinOS local device	Default value
DHCP Settings	Click the OK button in the Network Setup window	Disabled
DNS Settings	Click the OK button in the Network Setup window	Disabled
Proxy Settings	Click the OK button in the Network Setup window	Disabled
Ethernet Settings	Click the OK button in the Network Setup window	Disabled
Wireless Settings	Click the OK button in the Network Setup window	Disabled
VPN Settings	Add a new VPN, edit a VPN or remove a VPN	Disabled
Printers	Click the OK button in the Printer Setup window	Disabled
Audio[1]	Change the audio configuration	Disabled
Mouse*	Click the OK button in the Peripherals window	Enabled
Keyboard*	Click the OK button in the Peripherals window	Enabled

Table 33. Manual override support matrix (continued)

Settings	Action to be performed on the ThinOS local device	Default value
Touch pad*	Click the OK button in the Peripherals window	Enabled
Monitor*	Click the Test button and then click OK in the Display Setup window	Disabled
Region & Language - Region Settings	Change region configuration and click OK button	Disabled
Region & Language - Language Settings	Change language configuration and click OK button	Disabled

*The manual override option is available for these settings in the previous ThinOS release.

[1]After the device reboot, the USB audio is set as priority regardless of the Manual Override settings. This is a known issue.

- Added the **Camera** option in **Peripheral Management**. When you disable this option and connect the camera to the device, the device list in the Peripherals window shows empty data. The display resolution list on the device only shows resolutions from the DDC table.
- Changed the **Mute** option in **Peripheral Management** > **Audio** to a drop-down list. Use this option to control the playback audio and system beep separately.

Table 34. Audio options

Value	Playback audio	System beep
Unmute	unmute	unmute
Audio mute, beep mute	mute	mute
Audio unmute, beep mute	unmute	mute

- Added the **Resolutions From DDC Table Only** option under **Peripheral Management** > **Monitor**. When enabled, the display resolution list on the device only shows resolutions from the DDC table.
- Added the **Ignore Server Certificate Check** option under **Privacy & Security** > **SCEP**.

  This option is disabled by default. You must install a CA certificate first and then request a SCEP certificate by using the administrator URL. When using the administrator URL, you must FQDN with prefix HTTPS. Do not use the IP address in the URL.

  If this option is enabled, there is no need to install the CA certificate on the client. You can directly request for a SCEP certificate by using the administrator URL with prefix HTTPS.

  NOTE: If you are using earlier versions of ThinOS and if you have used the IP address in the administrator URL with the Ignore Server Certificate Check option disabled, you must change the URL to FQDN. If the Ignore Server Certificate Check option is enabled, there is no need to change the IP address in the administrator URL.
- The application name WVD is changed to AVD in the **Proxy Application** List field under **Network Configuration** > **Proxy Settings**.

  NOTE: If you have already configured WVD as the application name, the proxy functionality still works.
- Added the option **Show Applications with KEYWORDS:Mandatory** under **Session Settings** > **Citrix Session Settings**. When this option is enabled and you log in with classic mode or modern mode, only the applications that are configured with KEYWORDS:Mandatory are displayed on the ThinOS desktop.
- Added the **Login Expire Time** option under **Broker Settings** > **Citrix Virtual Apps and Desktops Settings**. Use this option to set a timer after you log in to a Citrix session. After the countdown timer expires, you must enter the user credentials again to launch any new desktop or application. After you enter the credentials, the countdown timer starts again. Desktop or applications that you launch before the expiry of the countdown timer remains open and are not affected by this setting.
- The **On Desktop=None** option under **Session Settings** > **Global Session Settings** is not applicable to Modern desktop.
- Values of Keyboard Layout and Screen Saver Timeout from the client are displayed under System Information on the **Devices Details** page on Wyse Management Suite.

ThinOS enhancements

- Supports device registration to Wyse Management Suite using secure DNS record fields.
  - You can register ThinOS-based devices to Wyse Management Suite 3.5 or later versions by using secure DNS record fields.
  - If you have not registered your ThinOS client to Wyse Management Suite and if you have set the DNS server with records, the device will automatically register to Wyse Management Suite.

    NOTE: If both secure DNS records and legacy DNS records are set in the DNS server, the secure DNS records take priority.
- Registering devices to Wyse Management Suite using secure DHCP scope options 201 and 202 is not supported.
- Supports NTFS USB drive mapping.
  - You can import files or export logs to a USB drive with NTFS format from ThinOS local UI.
  - You can map the USB drive with NTFS format to a Citrix or RDP session.
- Supports multiple DNS domain suffixes. Each value must be separated by a semicolon (;).
- Ability to save a new password specified in the prompt window when the current WPA & WPA2 personal wireless connection password is incorrect.
- Supports authentication to domain controller (NTLM) using the None broker. To set the Authentication to domain controller option, go to **Login Experience** > **Login Settings** > **Login Type** on Wyse Management Suite policy settings or Admin Policy Tool.

  If you set the Broker type as None with authentication to domain controller selected, a login window is displayed after you restart the system. Only users in the Active Directory group that are set in Wyse Management Suite can log in to the device. Any policy that is configured in the user policy group is applied to ThinOS.
- Displays a message on the First Boot Wizard screen when you reset the device to factory default settings without a network connection.
- The application name WVD is changed to AVD for the **Apply proxy server on** field.
- Supports the display resolution of about 16000 pixels for a single window in a multidisplay setup. Do not exceed this resolution.

For more information about the updates, see the *Dell Wyse ThinOS Version 9.1.4234 and 9.1.5067 Administrator's Guide* at www.dell.com/support.

Supported peripherals

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

Table 35. Supported peripherals

Product Category	Peripherals
Adapters and cables	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter
	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087
	Dell Adapter - DisplayPort to VGA - DANBNBC084
	Dell Adapter - HDMI to DVI - DAUARBN004
	Dell Adapter - HDMI to VGA - DAUBNBC084
	Dell Adapter - USB-C to DisplayPort - DBQANBC067
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter
	Dell Adapter - USB-C to HDMI - DBQAUBC064
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070
	Dell Adapter - USB-C to VGA - DBQBNBC064
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232

Table 35. Supported peripherals (continued)

Product Category	Peripherals
	Trendnet USB to Serial Converter RS-232
Audio devices	Dell 2.0 Speaker System - AE215
	Dell Pro Stereo Headset - Skype for Business - UC350
	Dell Pro Stereo Headset - UC150 - Skype for Business
	Dell Professional Sound Bar (AE515M)
	Dell USB Sound Bar (AC511M)
	Dell Wired 2.1 Speaker System - AE415
	Jabra BIZ 2400 Duo USB MS
	Jabra EVOLVE UC VOICE 750
	Jabra Engage 65 Stereo Headset
	Jabra Evolve 65 MS Stereo - Headset
	Jabra Evolve 75
	Jabra Engage 75
	Jabra GN2000
	Jabra PRO 935 USB Microsoft Lync Headset - 935-15-503-185
	Jabra Pro 9450
	Jabra Speak 510 MS Bluetooth
	Jabra UC SUPREME MS Bluetooth (link 360)
	LFH3610/00 Speechmike Premium—Only supports redirect
	Logitech S-150
	Logitech h150 - analog
	Nuance PowerMic II—supports to redirect whole device
	PHILIPS - analog
	POLYCOM Deskphone CX300
	Plantronics AB J7 PLT
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Blackwire 5220 Series
	Plantronics Blackwire C5210
	Plantronics Calisto P820-M
	Plantronics SAVI W740/Savi W745—supports USB only and does not support bluetooth
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0
	Plantronics Voyager 6200 UC
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SC 660 USB ML
	SENNHEISER SDW 5 BS-EU

Table 35. Supported peripherals (continued)

Product Category	Peripherals
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER USB SC230
Camera	Jabra PanaCast 4K Webcam
	Logitech BRIO 4K Webcam
	Logitech C910 HD Pro Webcam
	Logitech C920 HD Pro Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C925e Webcam
	Logitech C930e HD Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Poly EagleEye Mini webcam
Displays	C2422HE
	C2722DE
	C3422WE
	E1916H
	E1920H
	E2016H
	E2016Hv—China only
	E2020H
	E2216H
	E2216Hv—China only
	E2218HN
	E2220H
	E2318H
	E2318HN
	E2417H
	E2420H
	E2420HS
	E2720H
	E2720HS
	MR2416
	P1917S
	P2016
	P2017H
	P2018H
	P2217

Table 35. Supported peripherals (continued)

Product Category	Peripherals
	P2217H
	P2219H
	P2219HC
	P2317H
	P2319H
	P2415Q (3840 x 2160)
	P2417H
	P2418D
	P2418HT
	P2418HZ
	P2419H
	P2419HC
	P2421D
	P2421DC
	P2715Q (3840 x 2160)
	P2719H (1920 x 1080)
	P2719HC
	P2720D
	P2720DC
	P3418HW
	P4317Q
	S2719HS (1920 x 1080)
	S2817Q (3840x2160)
	U2415
	U2419H
	U2419HC
	U2421HE
	U2518D
	U2520D
	U2713HM (2560 x 1440)
	U2718Q (4K) (3840 x 2160)
	U2719D (1920 x 1080)
	U2719DC
	U2720Q
	U2721DE
	U3219Q (3840 x 2160)—No support for Type C to HDMI convertor
	U3419W (3440 x 1440)

Table 35. Supported peripherals (continued)

Product Category	Peripherals
	U4320Q
	U4919DW
Docking station	Dell Dock - WD19-C
	Dell Thunderbolt Dock - WD19TB—Thunderbolt Display is not supported
Fingerprint readers	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader
	Imprivata HDW-IMP-1C
	KSI-1700-SX Keyboard
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR—BLEdongle
Input devices (Keyboard and Mouse)	Bloomberg Keyboard STB 100
	Dell Keyboard KB212-B
	Dell Keyboard KB216p
	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse
	Dell Laser Wired Mouse - MS3220
	Dell Mobile Pro Wireless Mice - MS5120W
	Dell Mobile Wireless Mouse - MS3320W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W
	Dell Multi-Device Wireless Mouse - MS5320W
	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123
	Dell Premier Wireless Mouse - WM527
	Dell USB Wired Keyboard - KB216
	Dell USB Wired Optical Mouse - MS116
	Dell Wireless Keyboard and Mouse - KM636
	Dell Wireless Keyboard/mouse KM632
	Dell Wireless Mouse - WM126 - black
	Dell Wireless Mouse - WM326
	Dell wireless Keyboard/mouse KM714
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white
	Microsoft Arc Touch Mouse 1428
	Microsoft Ergonomic Keyboard
	Rapoo E6100, Bluetooth

Table 35. Supported peripherals (continued)

Product Category	Peripherals
	Seal Shield Medical Grade Optical Mouse
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white
	SpaceMouse Pro
	SpaceNavigator 3D Space Mouse
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Others	Intuos Pro Wacom
Printers	Brother DCP-7190DW—works on ICA only and not Blast
	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer
	Dell B2360d Laser Printer
	Dell B2360dn Laser Printer
	Dell Color Multifunction Printer - E525w
	Dell Color Printer- C2660dn
	Dell Multifunction Printer - E515dn
	HP Color LaserJet CM1312MFP—tested on Blast
	HP LaserJet P2055d
	HP M403D— works on ICA only and not Blast
	Lexmark X864de- tested on LPD only
Proximity card readers	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	Imprivata HDW-IMP-80
	Imprivata HDW-IMP-82
	KSI-1700-SX Keyboard
	OMNIKEY 5025CL
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM
	OMNIKEY 5325 CL
	OMNIKEY 5326 DFR
	RFIDeas RDR-6082AKU
Smart card readers	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU-
	Cherry SmartTerminal SMART Card Reader - ST-1044U
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0
	Cherry keyboard KC 1000 SC with smart card
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Dell Keyboard SK-3205 with smart card reader
	Dell keyboard KB813 with smart card reader

Table 35. Supported peripherals (continued)

Product Category	Peripherals
	Dell keyboard KB813t with smart card reader
	GemPC Twin
	Gemalto IDBridge CT710
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	IDBridge CT31 PIV
	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	SmartOS powered SCR3310
	SmartOS powered SCR335
	Sun microsystem SCR 3311
Storage	Bano type-c 16B
	Dell External Tray Load ODD (Agate)—DVD Writer
	Dell Portable SSD, USB-C 250 GB
	Kingston DT microDuo 3C 32 GB
	Kingston DTM30 32 GB
	Kingston DataTraveler G3 8 GB
	Samsung portable DVD Writer SE-208
	SanDisk Cruzer 16 GB
	SanDisk Cruzer 8 GB
	SanDisk USB 3.1 and Type-C 16 GB
	SanDisk Ultra Fit 32 GB
Teradici remote cards	Teradici host card 2220
	Teradici host card 2240

Tested environments matrix

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

Table 36. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.5
Configuration UI package for Wyse Management Suite	1.5 296
Imprivata OneSign	7.6.001.17
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 37. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2109	Tested	Tested	Tested	Tested

Table 38. Tested environment—VMware Horizon

VMware	Windows 10	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs
VMware Horizon 7.12	Tested	Not tested	Tested	Not tested	Tested	Not tested
VMware Horizon 2103	Tested	Not applicable	Tested	Tested	Tested	Tested
VMware Horizon 2106	Tested	Not applicable	Tested	Tested	Tested	Tested

Table 39. Test environment—Microsoft RDP

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

Table 40. Test environment—AVD

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

Table 41. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	2.9.400	2.9.400	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				

Table 42. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	5.4, 8.2	7.12, 8.2	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2	7.12, 8.2	Skype for Business 2016	Skype for Business 2015

Table 42. Tested environment—Skype for Business (continued)

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 2106	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 43. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	14.0.2	14.0.2	14.0.2
	Windows server 2016			
	Windows server 2019			

Table 44. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	14.0.2	14.0.2	14.0.2
	Windows server 2016	14.0.2	14.0.2	14.0.2
	Windows server 2019	Not tested	Not tested	Not tested

Table 45. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom client for VDI software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	5.8.0.20927	5.8.0 (20927)
	Windows server 2016		
	Windows server 2019		

Table 46. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106	Windows 10	5.8.0.20927	5.8.0 (20927)
	Windows server 2016	5.8.0.20927	5.8.0 (20927)
	Windows server 2019	Not tested	Not tested

Table 47. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	41.10.0.20213	41.10.0.20213
	Windows server 2016		
	Windows server 2019		

Table 48. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106	Windows 10	41.10.0.20213	41.10.0.20213
	Windows server 2016	41.10.0.20213	41.10.0.20213
	Windows server 2019	Not tested	Not tested

Table 49. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	41.10.3.19	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.10 to 42.2.
	Windows server 2016		
	Windows server 2019		

Table 50. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106	Windows 10	41.10.3.19	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.10 to 42.2.
	Windows server 2016		
	Windows server 2019		

Supported smart cards

Table 51. Supported smart cards

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	G&D SCE 3.2
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Giesecke and Devrient SmartCafe Expert 7.0 (T=0)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840
ID Prime MD v 4.0.2 (Gemalto 840)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K
ID Prime MD v 4.1.3 (Gemalto 3811)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940

Table 51. Supported smart cards (continued)

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

Fixed issues

Table 52. Fixed issues

Issue ID	Description
DTOS-5635	CIPS-24716 - Wireless reconnection issue in ThinOS 9.x firmware.
DTOS-5632	(Citrix number 80858789) CIPS-24715 - Keyboard layout issue in the Citrix VDI session when using CWA 21.9.
DTOS-5563	CIPS-24634 - Screensaver timeout from the device is not passing to the Wyse Management Suite server.
DTOS-5444	CIPS-24501 - Case 126090009 - An error is observed during Azure SAML2 authentication.
DTOS-5277	CIPS-23802 - On Wyse 3040 Thin Client, 49 percent of ping packets are lost when disabling the power-saving mode.
DTOS-5266	CIPS-24313 - Cursor focus is lost when the cursor reaches the window side on a Modern view desktop.
DTOS-5223	CIPS-24258 - Smart card details are retained on the screen even when it is removed.
DTOS-5221	CIPS-24257 - Window focus is lost when logging into the thin client.

Table 52. Fixed issues (continued)

Issue ID	Description
DTOS-5195	CIPS-23664 - Case 119577083 - Workspace ONE displays an error stating that the Horizon client is not installed.
DTOS-5185	CIPS-24015 - Microphone does not work after unplugging a 3.5 mm analog headset.
DTOS-5178	CIPS-23665 - Citrix apps or desktops are not displayed.
DTOS-5170	CIPS-24150 - Time on the local client is not synchronized with the time server.
DTOS-5082	CIPS-23857 - Power and Sleep tab appears for a few seconds on the Wyse 3040 Thin Client.
DTOS-5050	CIPS-23658 - Admin Mode does not work with the Imprivata classic mode when using the ThinOS classic desktop.
DTOS-5029	CIPS-23985 - An issue is observed when pulling Citrix Workspace app logs from the thin client.
DTOS-5028	CIPS-23772 - NHS USB redirect Olympus speech microphone fails after a VDI session is closed on the Wyse 3040 Thin Client.
DTOS-4976	CIPS-23836 - After the device resumes from sleep or hibernate, the smart card reader and the RSA token do not work.
DTOS-4956	CIPS-23835 - Closing or opening the lid causes Wyse 5470 Thin Client to reboot.
DTOS-4944	CIPS-22805 - Distorted display and a slow cursor movement are observed on screens that are connected to the external graphics card on Wyse 5070 Thin Client.
DTOS-4868	When you set the **Close Lid Action When Plugged in** to **Turn off the built-in display**, closing or opening the lid results in a system reboot. This is observed on the Wyse 5470 Thin Client.
DTOS-4812	CIPS-23708 - On the Wyse 5070 and Wyse 5470 Thin Clients, the $ sign does not work when using a French Keyboard Layout in a VNC session.
DTOS-4810	CIPS-23591 - Wyse Management Suite policy for the time server information does not work.
DTOS-4808	CIPS-23416 | Numeric keypad numlock issue is observed.
DTOS-4764	CIPS-23456 - On the Wyse 5470 PCoIP thin client, the mouse position is incorrect when using an external monitor as a main display.
DTOS-4762	CIPS-23624 | The PCoIP session stops responding.
DTOS-4747	CIPS-23208 | The DDC Table option is missing from ThinOS 9.x.
DTOS-4684	CIPS-23381 - On the Wyse 3040 Thin Client, the application resets to the primary display in a VMware RDS session.
DTOS-4527	CIPS-23409 - Communication with the time server is overloaded.
DTOS-4465	CIPS-23331 - The device restarts when the terminal is locked in a Zoom session.
DTOS-4464	CIPS-23329 - On the Wyse 5070 Thin Client, you cannot log in to the WVD desktop while connecting through ARMv2.
DTOS-4463	CIPS-23286 - On the Wyse 5070 Thin Client, you cannot disable the web cam completely.
DTOS-4325	On the Wyse 3040 Thin Client, an undefined error is displayed when you start a session.
DTOS-4240	CIPS-23161 - On the Wyse 3040 Thin Client, an incorrect session sign-off or application remains open in the remote session.
DTOS-4564	CIPS-22681 - Manual override is missing for audio, time zone, network, printer, and language.
DTOS-5478	A close battery low message is displayed when the power adapter is connected.
DTOS-4765	CIPS-23158 - The Domain drop-down list on the login screen is small.
DTOS-4711	CIPS-22283 - The 8.6 INI expire time feature is missing in Wyse Management Suite policy settings for ThinOS 9.x.

Table 52. Fixed issues (continued)

Issue ID	Description
DTOS-4710	(Citrix number 80383486, Citrix number 80444553) CIPS-20734 - ThinOS ignores the session reliability timeout setting.

Known issues

Table 53. Known issues

Issue ID	Description	Workaround
DTOS-5789	The Zoom configuration file ZoomMediaVmware.ini is unavailable even though the zoom package is installed on the client.	Reinstall the Zoom package.
DTOS-5760	PIE stops responding after you move the window in a Citrix session.	Force restart the device.
DTOS-5630	ThinOS user interface cannot be opened after you switch select groups more than three times.	Force restart the device.
DTOS-5626	The sign-on password in the Remote Connections window is automatically changed to a long string of characters when you switch between broker URLs.	Type the correct password again on the General Options tab.
DTOS-5618	Thin client stops responding for two to three seconds when you launch the ICA session or start the UC application in the ICA session.	Wait until the device is active.
DTOS-5609	ThinOS local user interface stops responding. The USB disk does not work in Troubleshooting. Peripherals and Shutdown menu cannot be opened.	Force restart the device.
DTOS-5606	Session cannot be connected at the first time.	Reconnect the session again.
DTOS-5598	After hot-plugging a headset, the audio device does not synchronize as a local device in the Blast session.	Switch the ThinOS local system audio setting to HD audio and then switch back to Headset.
DTOS-5592	System stops responding when you hot plug a USB disk.	Force restart the thin client.
DTOS-5582	When you convert ThinOS 8.6 to 9.1.5043, the Wyse Management Suite information is unavailable and a blue screen is displayed.	Restart the device. The Wyse Management Suite information is restored.
DTOS-5558	In a Citrix session, an error message may be displayed when you log in and launch a desktop or a published application.	There is no workaround in this release.
DTOS-5454	In a Citrix session, the desktop stops responding when you disconnect or sign out.	Sign off from the broker server.
DTOS-5408	When you plug out a smart card or a smart card reader, the VMware Horizon broker is signed out but the blast session is not closed.	Restart the device.
DTOS-5343	The sign-in broker window stops responding after the device resumes from sleep mode.	Force restart the thin client.
DTOS-5199	If the network signal is weak and you connect to the PSK wireless connection, the credential window is displayed.	Click the Cancel button in the credential window, and manually connect to the wireless connection again.
DTOS-4926	When using Imprivata PIE, the FP/Proxy authentications do not work when you perform multiple FP enrollments in short time.	Close the VDI session or restart the device.
DTOS-5823	The name of AVD package still shows as WVD on the event log tab.	There is no workaround in this release.
DTOS-5814	The device cannot work with secure DHCP.	Use the secure DNS record.

Table 53. Known issues (continued)

Issue ID	Description	Workaround
DTOS-5813	When the smart card server is timed out and you launch a session, the select store window is displayed.	Select the store again to log in.
DTOS-5810	[3040]When you remove the current connected wireless SSID and add another PSK SSID with a wrong password, many low signal logs are generated.	There is no workaround in this release and no impact to the functionality.
DTOS-5796	When you save settings from Admin Policy Tool, a print event log **Left Admin Mode** is generated.	There is no workaround in this release and no impact to the functionality.
DTOS-5793	When you do not specify any strings in the Group Registration key box and click the Validate Key button, a message stating **Checked into WMS Server** is displayed.	There is no workaround in this release.
DTOS-5762	After you redirect a USB disk to a PIE Citrix session and exit PIE, the disk is not recognized by the local device.	Connect the USB disk again.
DTOS-5761	Web cam redirection with 1280x720p video resolution for a 32-bit application does not work.	Disconnect the camera and reconnect it.
DTOS-5740	When you maximize a seamless application on the second display with a different resolution, the application resolution remains same as the main screen.	There is no workaround in this release.
DTOS-5726	The client behavior is not same as the VNC settings timeout type and the timeout policy.	There is no workaround in this release.
DTOS-5683	The device cannot be restarted when the Idle Time and the Schedule Reboot Time are same.	There is no workaround in this release.
DTOS-5681	There is no prompt for clicking the Force Coredump button.	There is no workaround in this release.
DTOS-5665	In VDI settings, if the setting is a number, the string does not get changed.	Remove the setting and add again, or add a new setting.
DTOS-5640	Unable to use the keyboard and cursor when you unlock the terminal.	Restart the device.
DTOS-5608	The USB drive kernel connected to the device stops responding when launching a session multiple times.	Remove and reconnect the smart card.
DTOS-5537	Desktop Viewer or Toolbar blocks do not work.	Click the session power icon, and select Disconnect. The session desktop gets disconnected.
DTOS-5213	The printer class is not automatically configured for a USB printer.	There is no workaround in this release.
DTOS-5639	CPU utilization reaches 100 percent during a Webex Teams VDI call.	There is no workaround in this release.
DTOS-5617	The Teradici Cloud Access Login page keeps checking and does not give an option to add username and password.	There is no workaround in this release.
DTOS-5614	When you specify the printer information in a group on Wyse Management Suite, the corresponding details appear on the printer setup page of a different group.	There is no workaround in this release.
DTOS-5583	USB scanner or printer is not listed in system log.	There is no workaround in this release.
DTOS-5553	USB redirecting and mapping do not work in a Citrix session.	There is no workaround in this release.
DTOS-5552	C6404322: Rows cannot be removed in Admin Policy Tool after clearing and disabling printers in the printer setup window.	There is no workaround in this release.

Table 53. Known issues (continued)

Issue ID	Description	Workaround
DTOS-5551	C6404310: Unable to add the LPD printer rows in the Admin Policy Tool.	There is no workaround in this release.
DTOS-5515	When you maximize the Skype video window and you move the mouse, the screen flashes.	Do not set maximize mode.
DTOS-5513	In a Citrix session, you cannot resolve the hostname error when the broker is set for smart card authentication only.	There is no workaround in this release.
DTOS-5411	DHCP option 182 (domain list) does not work with DHCP options for Wyse Management Suite.	Set the domain list from Wyse Management Suite.
DTOS-5405	Cursor appeared differently after you enable or disable the relative mouse in a PCoIP session .	Relaunch the PCoIP session.
DTOS-5359	When you play a YouTube video with BCR enabled, the BCR content blinks and a graphic-related issue is observed.	Reduce the video resolution to lower than 1080p.
DTOS-5356	High CPU usage is observed with Zoom call optimization.	There is no workaround in this release.
DTOS-5351	VPN cannot be autoreconnected when ThinOS resumes from sleep mode.	Manually reconnect or restart the device.
DTOS-5218	ThinOS stops responding, and the device restarts when you attempt to update the EPOS SP30 firmware.	There is no workaround in this release.
DTOS-5132	You cannot connect to all applications available in the auto-Connect List when the published applications are in the logged off status.	Need connect these apps by manual click.
DTOS-5058	The smart card cannot be detected by the device when you quickly reconnect the smart card,	Plug out the smart card and wait for more than 10 seconds before plugging in the smart card again.
DTOS-5000	The broker login window is displayed on top of the Admin Policy tool screen when an application is getting installed.	There is no workaround in this release.
DTOS-4996	The Printer Open Failed error is not displayed when you disconnect the printer and click the Test Print button.	There is no workaround in this release.
DTOS-8011	The thin client does not get locked automatically after leaving the thin client unattended for 10 minutes.	After the thin client is checked in to the WMS server, you must change the **Screen Saver Settings** under **Personalization** > **Screen Saver** to make the lock terminal work. Do not use the default screen saver settings.
BITS477310	When you change the monitor's USB-C prioritization setting from High Data Speed to High Resolution, a black screen is displayed with a No USB-C Signal found message. Affected displays are U3023E, U4320Q , U2520D , U2421HF, U2721DE, U2421E, U2422H, U2422HE, U2722D, U2722DE , P3222QE, U3023E, U3223E, U3222QE, U2723QE, P3222QE, and C2722DE. This issue is observed on the Wyse 5070 and Wyse 5470 Thin Client.	Force restart the device.

5

ThinOS 9.1.4234

Release date

October 2021

Downgrading the ThinOS firmware

If you are downgrading ThinOS 9.1.4234 to ThinOS 8.6, ThinOS 9.0, or ThinOS 9.1 versions that are older than 9.1.3129, you must use the Dell Wyse USB Imaging Tool to install the ThinOS 8.x or 9.x Merlin image that is posted to www.dell.com/support. Before you downgrade, ensure that you disable the secure boot option. If you want to downgrade to ThinOS 9.0, you must also clear Trusted Platform Module (TPM) or Platform Trust Technology (PTT) in BIOS. Else, ThinOS resets to factory settings after each reboot. You can downgrade from ThinOS 9.1.4234 to ThinOS 9.1.3129 using Wyse Management Suite.

Firmware upgrade

The following firmware upgrade scenarios are supported:

- ThinOS 8.6_807 > ThinOS 9.1.4234
- ThinOS 9.1.3129 > ThinOS 9.1.4234

NOTE: If you are using earlier versions of ThinOS 8.6, you must first upgrade to ThinOS 8.6_807 and apply the latest BIOS updates before upgrading to ThinOS 9.1.4234. If you are using ThinOS 9.0, or any version of ThinOS 9.1 that is older than 9.1.3129, you must first upgrade to ThinOS 9.1.3129 before upgrading to ThinOS 9.1.4234.

For more information, see the *Dell Wyse ThinOS Version 9.1.4234 Migration Guide* at www.dell.com/support. For the steps to access documents, see Resources and support.

Important notes

- In Wyse Management Suite 3.5, the device group key is case sensitive. If the existing ThinOS 8.6 device uses a group key with a different case on the previous version of Wyse Management Suite server, the client cannot check in to the Wyse Management Suite server after you upgrade the server to Wyse Management Suite 3.5 and the device to ThinOS 9.1. For more information, see the *Dell Wyse Management Suite 3.5 Release Notes* and *Dell Wyse Management Suite 3.5 Administrator's Guide* at www.dell.com/support.
- Installation can fail even though the image download is complete. This issue is observed when the package settings are changed in the device group before the device is checked in to Wyse Management Suite from shutdown state.
- There are chances that after the upgrade the device displays a black screen. You may reboot the device to boot it up correctly.
- If the thin client is registered in Wyse Management Suite group 1 and you set Wyse Management Suite group 2 token in group 1 policy, then the group 2 token is applied on GUI but the thin client will still be in group 1. You must reboot the thin client to change the thin client to Wyse Management Suite group 2.

  NOTE: Dell Technologies recommends that you set a new 9.1.4234 application package or a 9.1.4234 OS firmware package in Group 1, so that thin client installs the package, and automatically reboots, and changes to Group 2.
- If the **Live Update** option is disabled, the thin client cannot download and install any firmware or package until the next reboot. However, the firmware or packages are downloaded in the following scenarios even when the **Live Update** option is disabled:
  - When you register the thin client to Wyse Management Suite manually.
  - When you power on the thin client from a power off state.
  - When you change the Wyse Management Suite group.

- When you set a new firmware or an application package in Wyse Management Suite group 2 and then change the device from group 1 to group 2 before upgrading, the following two notifications are displayed:
  - **Wyse Management Suite server or group is changed. System is going to reboot to load full configuration. Press cancel in 60 seconds to prevent reboot**.
  - **A new firmware or application is available, do you want to upgrade now or defer to the next reboot? The changes will automatically be applied in 120 seconds.**

  If you do not select an option, the thin client reboots after 60 seconds. After the reboot, the new application or firmware is installed and the thin client reboots again. The thin client will be in group 2 after the reboot.
- When a new firmware or an application notification is displayed on your thin client, clicking **Next Reboot** will:
  - Displays a notification if you have changed the Wyse Management Suite group and if the files are downloaded from the new group.
  - Not display any notification if the new firmware or application is downloaded in the same group.
  - Installs the firmware or package after a reboot.
- ThinOS 9.1.4234 does not apply OS firmware application package and BIOS firmware in child **Select** group.

Prerequisites for firmware upgrade

- Update the BIOS version of Wyse 5070 Thin Client to 1.3.1 or later before upgrading to ThinOS 9.1.4234. If you upgrade to ThinOS 9.1.4234 with earlier BIOS version and then upgrade the BIOS version to 1.3.1 or later, the device may fail to boot. For latest BIOS versions, see Tested BIOS version for ThinOS 9.1.4234.
- Before you migrate from ThinOS 8.6_807 to ThinOS 9.1.4234 or upgrade from ThinOS 9.1.3129 to 9.1.4234, power on the system and disable the sleep mode. If the system has entered the sleep mode, you must send the WOL command through Wyse Management Suite before using any real-time commands. To use the WOL command, ensure that the Wake-On-LAN (WOL) option is enabled in BIOS.

Upgrade from ThinOS 8.6 to ThinOS 9.1.4234 using Wyse Management Suite

If you are running any ThinOS 8.6 version, you must first install the ThinOS 8.6_807 image with the latest BIOS version, and then upgrade to ThinOS 9.1.4234. For the latest BIOS versions, see Tested BIOS version for ThinOS 9.1.4234.

The device reboots after the ThinOS image is downloaded. Once the upgrade completes, the device is automatically registered to Wyse Management Suite. Dell Technologies recommends you to back up your device settings before you initiate the upgrade process. All device settings are erased after you upgrade from ThinOS 8.6 except the following settings:

- **Wyse Management Suite group token and server settings**
- **Static DNS**
- **Certificates**
- **IEEE802.1x wired authentication settings**
- **Wireless connections**—The WEP/Sharekey security type is changed to **Open** as they are not supported in ThinOS 9.1.4234
- **Proxy settings**

ⓘ **NOTE:** For more information about how to install the ThinOS 9.1.4234 image, see the *Dell Wyse ThinOS Version 9.1.4234 Migration Guide* at www.dell.com/support.

Upgrade from ThinOS 9.1.3129 to ThinOS 9.1.4234 using Wyse Management Suite

Prerequisites

- If you are using ThinOS version 9.0, upgrade to ThinOS 9.1.3129.
- If you are using a ThinOS 9.1 version that is older than 9.1.3129, upgrade to ThinOS 9.1.3129.
- The thin client must be registered to Wyse Management Suite.
- Download the ThinOS 9.1.4234 (DTOS_9.1.4234.pkg) firmware to upgrade.

Steps

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

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

5. Click **Browse** and select the **ThinOS 9.1.4234 OS** 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.

Important notes for upgrading from ThinOS 9.1.3129 to ThinOS 9.1.4234

- There are chances that the upgrade might fail with event log stating **Failed to install.** In such an event, you may reboot the device and upgrade again.
- After you upgrade, if Zoom is not launching or Zoom optimization is not working in Blast or Citrix session, remove the zoom package and reinstall it.

Compatibility

ThinOS build details

- ThinOS 9.1.3129 to ThinOS 9.1.4234—**DTOS_9.1.4234.pkg**.
- ThinOS 8.6_807 to ThinOS 9.1 conversion builds:
  - **A10Q_wnos**—Wyse 3040 Thin Client
  - **PA10Q_wnos**—Wyse 3040 Thin Client with PCoIP
  - **X10_wnos**—Wyse 5070 Thin Client, Wyse 5470 Thin Client, and Wyse 5470 All-in-One Thin Client
  - **PX10_wnos**—Wyse 5070 Thin Client with PCoIP, Wyse 5470 Thin Client with PCoIP, and Wyse 5470 All-in-One Thin Client with PCoIP

ThinOS application package details

- Cisco_Jabber_14.0.1.305989_3.pkg
- Cisco_WebEx_Meetings_VDI_41.6.1.10_2.pkg
- Cisco_WebEx_VDI_41.6.1.19187_1.pkg (formerly called Cisco WebEx Teams)
- Citrix_Workspace_App_21.6.0.28_10.pkg
- EPOS_Connect_6.1.0.19549_20.pkg
- HID_Fingerprint_Reader_210217_10.pkg
- Jabra_7.2.0_10.pkg
- Microsoft_WVD_1.3_1229.pkg
- Teradici_PCoIP_21.03.1_17.pkg
- VMware_Horizon_2106.8.3.0.18251983_5.pkg
- Zoom_Citrix_5.7.6.20822_2.pkg
- Zoom_Horizon_5.7.6.20822_2.pkg
- Imprivata_PIE_7.5_1113.pkg
- Identity_Automation_QwickAccess_2.0.0.3_3.pkg

Previous version

ThinOS 9.1.3129

Tested BIOS version for ThinOS 9.1.4234

Table 54. Tested BIOS details

Platform name	BIOS version
Wyse 3040 Thin Client	1.2.5
Wyse 5070 Economy Thin Client	1.12.0
Wyse 5070 Standard Thin Client	1.12.0
Wyse 5070 Extended Thin Client	1.12.0
Wyse 5470 All-in-One Thin Client	1.9.0
Wyse 5470 Mobile Thin Client	1.9.0

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

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

Citrix Workspace app feature matrix

Table 55. Citrix Workspace app feature matrix

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires to launch client browser through Local app access policy (which is not supported in Linux client), to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Limited support	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	There are no limitations in this release.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 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.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. This is Citrix binary design.
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Do not hot plug headset or the camera during a meeting, or a call. Do not switch the camera during a meeting. It causes the audio and video reception to be inconsistent. Restart Microsoft Teams to resolve this issue. This is also Citrix binary issue. Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For more information, see the Dell Wyse ThinOS Version 9.1.4234

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
			Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Teams Offloading (tVDI)	Supported	Supports Webex Teams optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by APT/ Wyse Management Suite. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Offloading (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported (not with NetScaler Gateway)	Limited support—Not supported with Citrix ADC (formerly NetScaler) due to Citrix's limitation.

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
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	There are no limitations in this release.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
			Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1.4234 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace App release note but not in feature matrix	Battery status indicator (CWA2106)	Supported	There are no limitations in this release.
	Service continuity (Technical Preview) (CWA2104, CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio (CWA2012 and CWA2010)	Not supported	Not supported
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported

Table 55. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234	ThinOS 9.1.4234 limitations
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

VMware Horizon feature matrix

Table 56. VMware Horizon feature matrix

Feature		ThinOS 9.1.4234
Broker Connectivity	SSL certificate verification	Supported with VDI, RDS Hosted Desktops and Apps
	Disclaimer dialog	Supported with VDI, RDS Hosted Desktops and Apps
	UAG compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Shortcuts from server	Not supported
	Pre-install shortcuts from server	Not supported
	File type association	Not supported
	Phone home	Supported with VDI, RDS Hosted Desktops and Apps
Broker Authentication	Password authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Single sign on	Supported with VDI, RDS Hosted Desktops and Apps
	RSA authentication	Supported with VDI, RDS Hosted Desktops and Apps

Table 56. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4234
	Integrated RSA SecurID token generator	Not supported
	Kiosk mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remember credentials	Not supported
	Log in as current user	Not supported
	Nested log in as current user	Not supported
	Log in as current user 1-way trust	Not supported
	OS biometric authentication	Not supported
	Un-authentication access	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Cisco ACS	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – SMS Passcode	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - DUO	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Microsoft Network Policy	Supported with VDI, RDS Hosted Desktops and Apps
Smart card	x.509 certificate authentication (Smart Card)	Supported with VDI, RDS Hosted Desktops and Apps
	CAC support	Supported with VDI, RDS Hosted Desktops and Apps
	.Net support	Supported with VDI, RDS Hosted Desktops and Apps
	PIV support	Supported with VDI, RDS Hosted Desktops and Apps
	Java support	Not supported
	Purebred derived credentials	Not supported
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI
	Restart	Supported only with VDI
	Log off	Supported with VDI, RDS Hosted Desktops and Apps
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple connections	Supported with VDI, RDS Hosted Desktops and Apps
	Multi-broker/multi-site redirection - Universal	Supported with VDI, RDS Hosted Desktops and Apps
	App launch on multiple end points	Supported with VDI, RDS Hosted Desktops and Apps
	Auto-retry 5+ minutes	Supported with VDI, RDS Hosted Desktops and Apps

Table 56. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4234
	Blast network recovery	Supported with VDI, RDS Hosted Desktops and Apps
	Time zone synchronization	Supported with VDI, RDS Hosted Desktops and Apps
	Jumplist integration (Windows 7- Windows 10)	Not supported
Client Customization	Command line options	Not supported
	URI schema	Not supported
	Launching multiple client instances using URI	Not supported
	Preference file	Not supported
	Parameter pass-through to RDSH apps	Not supported
	Non interactive mode	Not supported
	GPO-based customization	Not supported
Protocols Supported with VDI, RDS Hosted Desktops and Apps	Blast Extreme	Supported with VDI, RDS Hosted Desktops and Apps
	H.264 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	H.265 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Codec	Supported with VDI, RDS Hosted Desktops and Apps
	JPEG/PNG	Supported with VDI, RDS Hosted Desktops and Apps
	Switch encoder	Supported with VDI, RDS Hosted Desktops and Apps
	BENIT	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Extreme Adaptive Transportation	Supported with VDI, RDS Hosted Desktops and Apps
	RDP 8.x, 10.x	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP	Supported with VDI, RDS Hosted Desktops and Apps
Features/Extensions Monitors/ Displays	Dynamic display resizing	Supported with VDI, RDS Hosted Desktops and Apps
	VDI windowed mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remote app seamless window	Not supported
	Multiple monitor support	Supported with VDI, RDS Hosted Desktops and Apps
	External monitor support for mobile	Not supported
	Display pivot for mobile	Not supported

Table 56. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4234
	Number of displays Supported with VDI, RDS Hosted Desktops and Apps	4
	Maximum resolution	3840x2160
	High DPI scaling	Supported only with VDI
	DPI sync	Supported with VDI, RDS Hosted Desktops and Apps
	Exclusive mode	Not supported
	Multiple monitor selection	Supported with VDI, RDS Hosted Desktops and Apps
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported with VDI, RDS Hosted Desktops and Apps
	Relative mouse	Supported only with VDI
	External Mouse Support	Supported with VDI, RDS Hosted Desktops and Apps
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported with VDI, RDS Hosted Desktops and Apps
	International Keyboard Support	Supported with VDI, RDS Hosted Desktops and Apps
	Input Method local/remote switching	Not supported
	IME Sync	Supported with VDI, RDS Hosted Desktops and Apps
Clipboard Services	Clipboard Text	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard Graphics	Not supported
	Clipboard memory size configuration	Supported with VDI, RDS Hosted Desktops and Apps
	Drag and Drop Text	Not supported
	Drag and Drop Image	Not supported
	Drag and Drop File/Folder	Not supported
Connection Management	IPv6 only network support	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP IP roaming	Supported with VDI, RDS Hosted Desktops and Apps
Optimized Device Redirection	Serial (COM) Port Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Client Drive Redirection/File Transfer	Not supported
	Scanner (TWAIN/WIA) Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	x.509 Certificate (Smart Card/ Derived Credentials)	Supported with VDI, RDS Hosted Desktops and Apps
	Gyro Sensor Redirection	Not supported

Table 56. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4234
Real-Time Audio-Video	Audio in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Video in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple webcams	Not supported
	Multiple speakers	Not supported
USB Redirection	USB redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnInsert	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnStartup	Supported with VDI, RDS Hosted Desktops and Apps
	Connect/Disconnect UI	Not supported
	USB device filtering (client side)	Supported with VDI, RDS Hosted Desktops and Apps
	Isochronous Device Support	Supported only with VDI
	Split device support	Supported only with VDI
	Bloomberg Keyboard compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Smartphone sync	Supported only with VDI
Unified Communications	Skype for business	Supported with VDI, RDS Hosted Desktops and Apps
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops and Apps
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops and Apps
	Cisco WebEx Teams	Supported with VDI, RDS Hosted Desktops and Apps
	Cisco WebEx Meetings	Not supported
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops and Apps
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops and Apps
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops and Apps
	HTML5 Redirection	Not supported
	Directshow Redirection	Not supported
	URL content redirection	Not supported
	Browser content redirection	Not supported
Graphics	vDGA	Supported only with VDI
	vSGA	Supported only with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops and Apps

Table 56. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4234
	Intel vDGA	Supported only with VDI
	AMD vGPU	Supported only with VDI
Mobile Support	Client-side soft keyboard	Not supported
	Client-side soft touchpad	Not supported
	Full Screen Trackpad	Not supported
	Gesture Support	Not supported
	Multi-touch Redirection	Not supported
	Presentation Mode	Not supported
	Unity Touch	Not supported
Printing	VMware Integrated Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Location Based Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Native Driver Support	Not supported
Security	FIPS-140-2 Mode Support	Supported with VDI, RDS Hosted Desktops and Apps
	Imprivata Integration	Supported with VDI, RDS Hosted Desktops and Apps
	Opswat agent	Not supported
	Opswat on-demand agent	Not supported
	TLS 1.1/1.2	Supported with VDI, RDS Hosted Desktops and Apps
Session Collaboration	Session Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
	Read-only Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
Update	Update notifications	Not supported
	App Store update	Not supported
Other	Smart Policies from DEM	Supported with VDI, RDS Hosted Desktops and Apps
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI, RDS Hosted Desktops and Apps
	Workspace ONE mode	Supported with VDI, RDS Hosted Desktops and Apps
	Nested - basic connection	Supported with VDI, RDS Hosted Desktops and Apps

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

Windows Virtual Desktop and RDP feature comparison matrix

Table 57. Windows Virtual Desktop and RDP feature comparison matrix

Category Supported	Features	ThinOS 9.1.4234
Service	Direct connection to Desktop via RDP	Supported
	Microsoft 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
	Multi-touch	Not supported
Audio Visual	Audio in	Supported
	Audio out	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
	Clipboard (file)	Not supported
Redirections	Printer	Supported
	Serial Port	Not supported
	SmartCard	Not supported
	USB (General)	Not supported
Session Experience	Dynamic Resolution	Supported
	Start Command	Supported
	Desktop Experience	Not supported
	Desktop Scale Factor	Supported
	Multi-Monitor (All)	Supported
	Restricted full screen session	Supported
	Keyboard Layout Mapping	Not supported
	Time Zone Mapping	Supported
	RemoteFX	Not supported
	Video/Audio/Online playback	Supported
	Compression	Supported
	Optimize for low speed link	Supported
Graphics (CODECs)	H.264 Support	Supported
	H.264 AVC-444	Not supported
	TSMM (MMR)	Not supported

Table 57. Windows Virtual Desktop and RDP feature comparison matrix (continued)

Category Supported	Features	ThinOS 9.1.4234
	VOR	Not supported
Authentication	TS Gateway Supported	Supported
	- TSGW II	Not supported
	- TSGW III	Not supported
	- TSGW WebSocket	Not supported
	- TSGW + UDP	Not supported
	NLA	Supported
	SmartCard	Not supported
	Imprivata	Supported

New and enhanced features

Citrix Workspace app updates

- Browser content redirection (BCR) enhancements—BCR with Chromium Embedded Framework (CEF) is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
- Zoom optimization enhancements—Added the HTTP proxy support for anonymous authentication in Zoom optimization. Configure HTTP Proxy server and Proxy Application List as **ZOOM** in Admin Policy Tool or Wyse Management Suite to make Zoom optimization function through the proxy server. The following are the Zoom limitations:
  - HTTPS proxy server is not supported for Zoom optimization in ThinOS.
  - HTTP proxy server with nonanonymous authentication is not supported in ThinOS.
- NetScaler/ADC enhancements—Added NetScaler/ADC Authentication Method. Dell Technologies recommends that you configure the **NetScaler/ADC Authentication Method with RSA+LDAP** either from the **Wyse Management Suite** policy or the **Admin Policy tool** for users who want to use Citrix ADC authentication methods, such as RSA+LDAP with MFA. This setting is supported from Wyse Management Suite 3.5 and later versions.

For more information, see the *Dell Wyse ThinOS 9.1.4234 Administrator's Guide* at www.dell.com/support.

VMware Horizon Blast updates

Smartphone sync

You can sync your iPhone or Android smartphone into a Blast session.

NOTE: Among the Android smartphones, only Huawei phones are tested.

For more information, see the *Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide* at www.dell.com/support.

Bloomberg keyboard STB 100 mapping

You can connect the keyboard using either single or dual USB cables. No setting changes or redirection is required. All the function keys work without any redirection. For steps to disable redirection, see the *Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide* at www.dell.com/support.

High Efficiency Video Coding (HEVC) or H.265

In ThinOS 9.1.4234, VMware Blast Extreme supports High Efficiency Video Coding (HEVC). HEVC is also known as H.265. This feature is disabled by default. To use this feature, select the **Allow High Efficiency Video Decoding (HEVC)** check box from

Connection Manager > **Global Connection Settings** > **Horizon**. You can go to the VMware Horizon Performance tracker and see **Encoder Name** to verify whether HEVC is working. If the name contains HEVC, the feature is working. HEVC in Blast Extreme requires both the ESXi hosts that support the virtual desktops, and RDSH servers to have NVIDIA Tesla or newer graphics cards to offload the encoding. HEVC does not work with only ESXi CPU encoding. If there are no supported graphics cards present, the H.264 or JPEG/PNG encoding is used. For more information, see the *VMware Blast Extreme Optimization Guide* at techzone.vmware.com.

NOTE: HEVC requires hardware support including the graphics card, on both the client and the agent side. If either the client or the agent cannot support HEVC, the session falls back to H.264.

Limitations

- If you launch a session that has been launched from another device, the HEVC feature does not work. The server uses H.264 in this scenario. To use HEVC, sign off other sessions before connecting to the session from the ThinOS client.
- You must upgrade Wyse Management Suite to version 3.5 or later to support the HEVC feature.

Microsoft Teams optimization

VMware Horizon 2106 for the client side includes Microsoft Teams media optimization by default. Media optimization for Microsoft Teams that is installed by default in Horizon Agent, is controlled by a group policy object (GPO). GPO is not enabled by default. You can enable the optimization by using a Group Policy Editor.

For the steps on enabling the optimization using a Group Policy Editor, see the *Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide* at www.dell.com/support.

NOTE: Install the Horizon Agent before you install Microsoft Teams.

To check whether Microsoft Teams is launched in optimized mode, click the three dots next to your profile picture, and go to **About** > **Version**. A banner that says **VMware Media Optimized** is displayed, indicating that Microsoft Teams has launched in optimized mode. Alternatively, you can click the three dots next to your profile picture, and go to **Settings** > **Devices** > **Audio devices.** . Check whether the local headset names are displayed in the **Speakers** and **Microphone** drop-down lists, instead of **Virtual DevTap** or **VDI**.

NOTE: This feature is not supported on Wyse 3040 Thin Client.

Microsoft Teams optimization feature matrix

Table 58. Microsoft Teams optimization feature matrix

Scenario	ThinOS 9.1.4234
Long audio call	Supported
Call—Make an audio call	Supported
Call—Answer an audio call	Supported
Call—Make a video call	Supported
Call—Answer a video call	Supported
Call—Turn the camera on or off	Supported
Call—Enter or exit full screen	Supported
Call—Hold or resume a call	Supported
Call—End call	Supported
Call—Mute or unmute audio	Supported
Call—Transfer	Supported
Call—Consult then transfer	Supported
Call—Keypad	Not tested
Call—Start or stop recording	Supported—You can use this feature in group calls and meetings.

Table 58. Microsoft Teams optimization feature matrix (continued)

Scenario	ThinOS 9.1.4234
Call—Turn off or turn on incoming video	Supported
Call—Group video call	Supported
Call—Group audio call	Supported
Call—Invite someone during a call	Supported
Meeting	Supported
Share screen—Desktop	Supported
Share screen—PowerPoint	Supported
Chat	Supported
Audio or video call in VDI server desktop	Supported
Audio or video call in published Microsoft Teams application	Not tested
Devices—Plug in or disconnect the headset	Supported—Dell Technologies recommends to not plug in or disconnect headsets during a call.
Devices—Switch headset	Supported—Dell Technologies recommends to not switch headsets during a call.
Devices—Plug in or disconnect the camera	Supported—Dell Technologies recommends to not plug in or disconnect camera during a call.
Devices—Switch camera	Supported—Dell Technologies recommends to not switch the camera during a call.
Headset buttons—Answer/Mute/End Call	Not supported

Microsoft Teams optimization limitations and known issues

- Depending on your network bandwidth latency, the audio quality may fluctuate. To avoid this issue, ensure that your network bandwidth is adequate for audio or video call. Dell Technologies recommends 200 KBps or higher network speed for a single client.
- Audio is still played through the first headset when you switch to the second headset during the call. This issue is observed when you have installed the JVDI package on the thin client. Workaround is that if you are using Microsoft Teams (or Zoom), do not install the Cisco JVDI package. This issue is due to Cisco limitation.
- When using a headset, you cannot answer or end the call through headset buttons. This issue is due to a limitation of Microsoft Teams.
- Sharing screen when Microsoft Teams is published as an application is not supported. This issue is due to a limitation of VMware Horizon.
- There maybe inconsistency on how the video is displayed during video calls. The issue fixes by itself after 5 minutes.
- Microsoft Teams optimization is not supported through proxy.
- Audio may be inconsistent during video calls. Try the following:
  - Sometimes audio is distorted during a call. Workaround is to change the headset.
  - Sometimes there can be network issues. Ensure that your network bandwidth is adequate for audio and video calls. Dell Technologies recommends 200 KBps or higher network speed for a single client.

Zoom optimization enhancements

Added the HTTP proxy support for anonymous authentication in Zoom optimization. Configure HTTP Proxy server and Proxy Application List as **ZOOM** in Admin Policy Tool or Wyse Management Suite to make Zoom optimization function through the proxy server. The following are the Zoom limitations:

- HTTPS proxy server is not supported for Zoom optimization in ThinOS.
- HTTP proxy server with nonanonymous authentication is not supported in ThinOS.

Teradici PCoIP update

Updated the Teradici PCoIP package version to 21.03.1_17. No new features are added.

Windows Virtual Desktop update

RDP session supports LPT, LPD and SMB printers from Windows Virtual Desktop version 1.3_1229. RDP protocol supports standard printers.

For more information, see the *Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide* at www.dell.com/support.

Unified Communications optimization packages update

- Updated Cisco Webex VDI to version 41.6.1.19187_1.
- Updated Cisco Jabber to version 14.0.1.305989_3.
- Updated Zoom to version 5.7.6.20822_2.

ⓘ **NOTE:** For known issues on Wyse 3040 Thin Clients while using Unified Communications optimization packages, see the *Citrix Unified Communications support on Wyse 3040 Thin Clients* section in *Dell Wyse ThinOS 9.1.4234 Administrator's Guide* at www.dell.com/support.

Authentication updates

Identity automation updates

Identity Automation QwickAccess package is updated to 2.0.0.3. The following are the enhancements:

- Identity Automation QwickAccess supports Citrix Broker agent and supports user binding card in same domain with Citrix Broker agent. Users in different domains are not supported and not recommended.
- API key is treated as password in Wyse Management Suite policy settings, Admin Policy Tool, and ThinOS local user interface. It is not displayed in plain text.
- Identity Automation QwickAccess is verified based on Identity server version 1.6.0.1.
- PIN reset is removed in this release.

Identity Automation feature matrix

Table 59. Identity Automation feature matrix

Identity Automation Feature		ThinOS 9.1.4234
Broker Type	Authenticate to Citrix Virtual Apps and Desktops	Supported
	Authenticate to VMware Horizon broker	Not supported
	Authenticate to Microsoft Remote Desktop Services	Not supported
Proxy Card	New card enroll	Supported
	Authenticate with proximity card and password	Supported
	Authenticate with proximity card and PIN	Supported
	Authenticate with password	Supported
SSPR	Seamless change password support	Not supported
	Self-service password reset	Not supported

Table 59. Identity Automation feature matrix (continued)

Identity Automation Feature		ThinOS 9.1.4234
	Self-service PIN reset	Not supported
Lock/Unlock	Lock/Unlock the terminal by tapping a proximity card	Supported
	Convenient tap-over functionality	Supported
IA server settings	Settings for authenticate card frequency	Supported
	Settings for authenticate card method (PIN or password)	Supported
	Settings for incorrect PIN time	Supported
	Settings for PIN length requirement	Supported
	Settings for PIN reset	Not supported

Imprivata PIE limitation

Third-party self-service password reset function is not supported in this release.

ThinOS updates

- Secure Boot—If **Secure Boot** is disabled, and the BIOS password is set as the default value or if there is no BIOS password, the prompt window to reboot the system and enable **Secure Boot** is not displayed from this release onwards. **Secure Boot** is enabled after the next reboot.
- Net iD smart card firmware—Updated the Net iD smart card firmware version to 6.8.3.21.
- From ThinOS 9.1.4234 onwards, you can enable or disable IPv6 from **Advanced** > **Network Configuration** > **Common Settings** > **Enable IPv6** in Wyse Management Suite policy settings or the Admin Policy Tool. IPv6 is enabled by default for both wired and wireless networks.
- The window that is displayed when you change a group in Wyse Management Suite is changed.
- The window that is displayed when you update packages and the operating system firmware is changed.
- The **HTTP/HTTPS** proxy default port is changed from 808 to 8080.

For more information about the updates, see the *Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide* at www.dell.com/support.

Display audio limitations

Display audio using converter is not supported on all platforms.

- **Wyse 5070 Thin Client**—Only DP1 and DP2 ports support display audio.
- **Wyse 5470 Thin Client**—When two monitors that support display audio are connected to Dell WD19 docking station, the **HDMI/DP** audio option disappears if you remove one of the monitors.
- **Wyse 3040 Thin Client**
    - Setting the display resolution higher than 1920x1080 results in a black screen.
    - By default the display audio is disabled. You must enable the display audio in Wyse Management Suite and reboot the client.
    - Display audio does not update real time. If you change the monitor or the DP port, you must reboot the client to update the display audio option.
    - Wyse 3040 Thin Client supports only one display audio. If one DP port is working with display audio, then the other DP port does not work with display audio.

Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **VNCD Server**—Added input validation for the VNCD Server field in **Services** > **VNC Service**. You can only enter values in the format of IP addresses.
- **Disable Shutdown**—Added **Disable Shutdown** option in **Login Experience** > **Login Settings**. This option disables the **Shutdown** option in the ThinOS **Shutdown** window, and also disables the physical shutdown button on the thin client.
- **Reboot on monitor connection**—Changed the default value of **Reboot on monitor connection** option under **Enable ProveID Embedded Mode** in **Login Experience** > **3rd Party Authentication** > **Imprivata** to disabled.
- **API Key**—Changed the **API Key** field option in **Login Experience** > **Login Settings** > **Identity Automation** > **Identity Automation** to password type to hide the input values.
- **Enable IPv6**—Added the option **Enable IPv6** in **Network Configuration** > **Common Settings** to enable or disable IPv6.
- **Scheduled Reboot** and **Shutdown Settings**—Added time format validation for the following fields under **System Settings** > **Scheduled Reboot Settings** and **Scheduled Shutdown Settings**:
  - **Scheduled Reboot Settings** > **Scheduled Reboot Time**
  - **Scheduled Reboot Settings** > **Reboot after Idle Time**
  - **Scheduled Shutdown Settings** > **Scheduled Shutdown Time**
  - **Scheduled Shutdown Settings** > **Shutdown after Idle Time**

  NOTE: If you change the time zone on the local client, the **Scheduled Reboot settings** and **Scheduled Shutdown settings** takes effect only after a reboot.
- **Granular Control of Peripherals**—Added **Granular Control of Peripherals** in **Privacy & Security** > **Account Privileges** to make the selected tabs visible in the **Peripherals** window. To see this option, you must set the privilege level as **Customize** and enable **Peripherals**.

  NOTE: If no tabs are selected, all tabs will be visible in the **Peripherals** window by default.
- **DHCP**—Updated the **DHCP** option in **Privacy & Security** > **Account Privileges**. The setting is enabled by default. To see this option, you must set the privilege level as **Customize** and enable **Network Setup**.
- **Allow High Efficiency Video Decoding**—Added **Allow High Efficiency Video Decoding** option in **Session Settings** > **Blast Session Settings** to enable or disable High Efficiency Video Decoding for Blast.
- **On Desktop**—Moved **On Desktop** option from **Session Settings** > **Citrix Session Settings** to **Session Settings** > **Global Session Settings**.

For more information about the updates, see the *Dell Wyse ThinOS 9.1.4234 Administrator's Guide* at www.dell.com/support.

Tested environments matrix

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

Table 60. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.5/3.3.1
Imprivata OneSign	7.5.000.9
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 61. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2103	Tested	Tested	Tested	Tested

Table 62. Tested environment—VMware Horizon

VMware	Windows 10	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs
VMware Horizon 7.12	Tested	Not tested	Tested	Tested	Tested	Tested
VMware Horizon 2103	Tested	Not applicable	Tested	Tested	Tested	Tested
VMware Horizon 2106	Tested	Not applicable	Tested	Tested	Tested	Tested

Table 63. Test environment—Microsoft RDP

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

Table 64. Test environment—WVD

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

Table 65. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	2.9.300	2.9.300	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				

Table 66. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	5.4, 8.2	7.12, 8.2	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2	7.12, 8.2	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 67. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	14.0.1	14.0.1	14.0.1
	Windows server 2016			
	Windows server 2019			

Table 68. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	14.0.1	14.0.1	14.0.1
	Windows server 2016	14.0.1	14.0.1	14.0.1
	Windows server 2019	Not tested	Not tested	Not tested

Table 69. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	5.7.6.20822	5.7.6.20822
	Windows server 2016		
	Windows server 2019		

Table 70. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	5.7.6.20822	5.7.6.20822
	Windows server 2016	5.7.6.20822	5.7.6.20822
	Windows server 2019	Not tested	Not tested

Table 71. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	41.6.1.19187	41.6.1.19162
	Windows server 2016		
	Windows server 2019		

Table 72. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	41.6.1.19187	41.6.0.19162
	Windows server 2016	41.6.1.19187	41.6.0.19162
	Windows server 2019	Not tested	Not tested

Table 73. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	41.6.1.10.2	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.6 to 41.10.
	Windows server 2016		
	Windows server 2019		

Supported peripherals

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

Table 74. Supported peripherals

Product Category	Peripherals
Adapters and cables	C2G - USB 2.0 A (Male) to DB9 (Serial) (Male) Adapter
	Dell Adapter - DisplayPort to DVI (Single Link) - DANARBC084
	Dell Adapter - DisplayPort to HDMI 2.0 (4K) - DANAUBC087
	Dell Adapter - DisplayPort to VGA - DANBNBC084
	Dell Adapter - HDMI to DVI - DAUARBN004
	Dell Adapter - HDMI to VGA - DAUBNBC084
	Dell Adapter - USB-C to DisplayPort - DBQANBC067
	Dell Adapter - USB-C to Dual USB-A with Power Pass-Through - DBQ2BJBC070 - Combo Adapter
	Dell Adapter - USB-C to HDMI - DBQAUBC064
	Dell Adapter - USB-C to HDMI/DP - DBQAUANBC070
	Dell Adapter - USB-C to VGA - DBQBNBC064
	StarTech.com 1 Port USB to RS232 DB9 Serial Adapter Cable - Serial adapter - USB 2.0 - RS-232
	Trendnet USB to Serial Converter RS-232
Audio devices	Dell 2.0 Speaker System - AE215
	Dell Pro Stereo Headset - Skype for Business - UC350
	Dell Pro Stereo Headset - UC150 - Skype for Business
	Dell Professional Sound Bar (AE515M)
	Dell USB Sound Bar (AC511M)
	Dell Wired 2.1 Speaker System - AE415
	Jabra BIZ 2400 Duo USB MS
	Jabra EVOLVE UC VOICE 750
	Jabra Engage 65 Stereo Headset
	Jabra Evolve 65 MS Stereo - Headset
	Jabra Evolve 75
	Jabra GN2000
	Jabra PRO 935 USB Microsoft Lync Headset - 935-15-503-185
	Jabra Pro 9450
	Jabra Speak 510 MS Bluetooth
	Jabra UC SUPREME MS Bluetooth (link 360)
	LFH3610/00 Speechmike Premium—Only supports redirect
	Logitech S-150
	Logitech h150 - analog
	Nuance PowerMic II—supports to redirect whole device
	PHILIPS - analog

Table 74. Supported peripherals (continued)

Product Category	Peripherals
	POLYCOM Deskphone CX300
	Plantronics AB J7 PLT
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Blackwire 5220 Series
	Plantronics Blackwire C5210
	Plantronics Calisto P820-M
	Plantronics SAVI W740/Savi W745—supports USB only and does not support bluetooth
	Plantronics Savi W440M-400 Series convertible wireless headset - DECT 6.0
	Plantronics Voyager 6200 UC
	Plantronics Voyager Focus UC B825-M headset for Microsoft Lync
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SC 660 USB ML
	SENNHEISER SDW 5 BS-EU
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER USB SC230
Camera	Jabra PanaCast 4K Webcam
	Logitech BRIO 4K Webcam
	Logitech C910 HD Pro Webcam
	Logitech C920 HD Pro Webcam
	Logitech C922 Pro Stream Webcam
	Logitech C925e Webcam
	Logitech C930e HD Webcam
	Logitech HD Webcam C525
	Microsoft LifeCam HD-3000
	Poly EagleEye Mini webcam
Displays	C2422HE
	C2722DE
	C3422WE
	E1916H
	E1920H
	E2016H
	E2016Hv—China only
	E2020H
	E2216H
	E2216Hv—China only
	E2218HN

Table 74. Supported peripherals (continued)

Product Category	Peripherals
	E2220H
	E2318H
	E2318HN
	E2417H
	E2420H
	E2420HS
	E2720H
	E2720HS
	MR2416
	P1917S
	P2016
	P2017H
	P2018H
	P2217
	P2217H
	P2219H
	P2219HC
	P2317H
	P2319H
	P2415Q (3840 x 2160)
	P2417H
	P2418D
	P2418HT
	P2418HZ
	P2419H
	P2419HC
	P2421D
	P2421DC
	P2715Q (3840 x 2160)
	P2719H (1920 x 1080)
	P2719HC
	P2720D
	P2720DC
	P3418HW
	P4317Q
	S2719HS (1920 x 1080)
	S2817Q (3840x2160)

Table 74. Supported peripherals (continued)

Product Category	Peripherals
	U2415
	U2419H
	U2419HC
	U2421HE
	U2518D
	U2520D
	U2713HM (2560 x 1440)
	U2718Q (4K) (3840 x 2160)
	U2719D (1920 x 1080)
	U2719DC
	U2720Q
	U2721DE
	U3219Q (3840 x 2160)
	U3419W (3440 x 1440)
	U4320Q
	U4919DW
Docking station	Dell Dock - WD19-C
	Dell Thunderbolt Dock - WD19TB—Thunderbolt Display is not supported
Fingerprint readers	HID EikonTouch 4300 Fingerprint Reader
	HID EikonTouch M211 Fingerprint Reader
	HID EikonTouch TC510 Fingerprint Reader
	HID EikonTouch TC710 Fingerprint Reader
	HID EikonTouch V311 Fingerprint Reader
	Imprivata HDW-IMP-1C
	KSI-1700-SX Keyboard
Hands-Free Authentication (HFA)	BLED112HDW-IMP-IIUR—BLEdongle
Input devices (Keyboard and Mouse)	Bloomberg Keyboard STB 100
	Dell Keyboard KB212-B
	Dell Keyboard KB216p
	Dell Laser Scroll USB 6-Buttons Silver and Black Mouse
	Dell Laser Wired Mouse - MS3220
	Dell Mobile Pro Wireless Mice - MS5120W
	Dell Mobile Wireless Mouse - MS3320W
	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W
	Dell Multi-Device Wireless Mouse - MS5320W
	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123

Table 74. Supported peripherals (continued)

Product Category	Peripherals
	Dell Premier Wireless Mouse - WM527
	Dell USB Wired Keyboard - KB216
	Dell USB Wired Optical Mouse - MS116
	Dell Wireless Keyboard and Mouse - KM636
	Dell Wireless Keyboard/mouse KM632
	Dell Wireless Mouse - WM126 - black
	Dell Wireless Mouse - WM326
	Dell wireless Keyboard/mouse KM714
	Man & Machine C Mouse - Mouse - right and left-handed - optical - 2 buttons - wired - USB - white
	Man & Machine Its Cool Flat - Keyboard - USB - UK layout - white
	Microsoft Arc Touch Mouse 1428
	Microsoft Ergonomic Keyboard
	Rapoo E6100, bluetooth
	Seal Shield Medical Grade Optical Mouse
	Seal Shield Silver Seal Waterproof-Keyboard-USB-US-waterproof-white
	SpaceMouse Pro
	SpaceNavigator 3D Space Mouse
Networking	Add On 1000 Base-T SFP transceiver—RJ-45
Others	Intuos Pro Wacom
Printers	Brother DCP-7190DW—works on ICA only and not Blast
	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer
	Dell B2360d Laser Printer
	Dell B2360dn Laser Printer
	Dell Color Multifunction Printer - E525w
	Dell Color Printer- C2660dn
	Dell Multifunction Printer - E515dn
	HP Color LaserJet CM1312MFP—tested on Blast
	HP LaserJet P2055d
	HP M403D— works on ICA only and not Blast
	Lexmark X864de- tested on LPD only
Proximity card readers	Imprivata HDW-IMP-60
	Imprivata HDW-IMP-75
	KSI-1700-SX Keyboard
	OMNIKEY 5025CL
	OMNIKEY 5321 V2
	OMNIKEY 5321 V2 CL SAM

Table 74. Supported peripherals (continued)

Product Category	Peripherals
	OMNIKEY 5325 CL
	OMNIKEY 5326 DFR
	RFIDeas RDR-6082AKU
Smart card readers	CHERRY KC 1000 SC - Keyboard - with Smart Card reader - USB - English - US - black - TAA Compliant - JK-A0104EU-
	Cherry SmartTerminal SMART Card Reader - ST-1044U
	Cherry SmartTerminal ST-1144 SMART Card Reader - USB 2.0
	Cherry keyboard KC 1000 SC with smart card
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Dell Keyboard SK-3205 with Smartcard reader
	Dell keyboard KB813 with Smartcard reader
	Dell keyboard KB813t with Smartcard reader
	GemPC Twin
	Gemalto IDBridge CT710
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	IDBridge CT31 PIV
	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121
	SmartOS powered SCR3310
	SmartOS powered SCR335
	Sun microsystem SCR 3311
Storage	Bano type-c 16B
	Dell External Tray Load ODD (Agate)—DVD Writer
	Dell Portable SSD, USB-C 250 GB
	Kingston DT microDuo 3C 32 GB
	Kingston DTM30 32 GB
	Kingston DataTraveler G3 8 GB
	Samsung portable DVD Writer SE-208
	SanDisk Cruzer 16 GB
	SanDisk Cruzer 8 GB
	SanDisk USB 3.1 and Type-C 16 GB
	SanDisk Ultra Fit 32 GB
Teradici remote cards	Teradici host card 2220
	Teradici host card 2240

Supported smart cards

Table 75. Supported smart cards

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	G&D SCE 3.2
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Giesecke and Devrient SmartCafe Expert 7.0 (T=0)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840
ID Prime MD v 4.0.2 (Gemalto 840)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K
ID Prime MD v 4.1.3 (Gemalto 3811)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940
Etoken Java (aladdin)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.0 T=0/1 0V300

Table 75. Supported smart cards (continued)

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_6.1.6	cv act sc/interface CSP	Giesecke & Devrient StarCos 3.2
N/A (Buypass BelDu)	Net iD 6.8.3.21, 2.0.48	Net iD - CSP	BelDu 6.0.4
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.3.21, 2.0.48	Net iD - CSP	IDPrime SIS 4.0.2
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)

Fixed issues

Table 76. Fixed issues

Issue ID	Description
DTOS-4911	Camera is not detected when installed with Zoom VDI Client app on virtual desktop. The issue is observed on Wyse 5470 All-in-One Thin Client with ThinOS 9.1.3192—**CIPS-23520**.
DTOS-4743	Double entry of the device in the Wyse Management Suite group list drop-down—**CIPS-23147**.
DTOS-4687	RDP uses a TS Gateway after the TS gateway is disabled in the Wyse Management Suite. The issue is observed on Wyse 3040 Thin Client with ThinOS 9.1.3112—**CIPS-23471**.
DTOS-4514	Pressing **Enter** unlocks the VDI session, after you lock the terminal. The issue is observed on Wyse 5470 Thin Client with ThinOS 9.1.3112—**CIPS-22939**.
DTOS-4481	It takes 10 seconds or more to authenticate using smartcards. The issue is observed on Wyse 5070 Thin Client—**CIPS-23343**.
DTOS-4409	Omni Key 3021 card reader does not redirect to VMware session on ThinOS 9.x—**CIPS-23202**.
DTOS-4403	Unable to log in to Horizon with UAG. The issue is observed on Wyse 5070 Thin Client with ThinOS 9.1.3112—**CIPS-23210**.
DTOS-4375	OmniKey 3121 smart card reader fails to redirect in View Blast and PCoIP sessions—**CIPS-23203**.
DTOS-4362	No pin prompt for smart cards after firmware update—**CIPS-23076. Case 112855083.**
DTOS-4358	Fails to launch Citrix application when RSA (2FA) is included—**CIPS-23247**.
DTOS-4352	Smart card login does not work on ThinOS 9.1.3112—**CIPS-23043**.
DTOS-4326	Wyse 5470 Thin Client crashes when connected to home broadband routers—**CIPS-23148**.
DTOS-4314	Horizon View fails to log in when the user password contains special characters **"**, **<**, or **>**—**CIPS-23125**.
DTOS-4313	Unable to log in to Horizon when password contains the special character **>**. The issue is observed on Wyse 3040 Thin Client with ThinOS 9.1.3112—**CIPS-23138**.

Table 76. Fixed issues (continued)

Issue ID	Description
DTOS-4310	Jabber microphone does not work consistently—**CIPS-23105**.
DTOS-4209	`$TN` does not translate the terminal name when it is defined in the RDP Direct Connection username field in Wyse management Suite—**CIPS-23016, Case 118991265**.
DTOS-4139	Some keys do not work when you use a Japanese keyboard with PCoIP—**CIPS-22956**.
DTOS-4006	Unable to authenticate when connecting internally with no UAG using smart card. The issue is observed on Wyse 5470 Thin Client with ThinOS 9.1.3112—**CIPS-22826**.
DTOS-3979	An error occurs when configuring 2 broker URLs. Failover setting does not work in ThinOS 9.x—**CIPS-22680**.
DTOS-3954	On ThinOS 9.1.3112, after the Wyse authentication, the storefront portal is not on the main screen, but split into 2 screens—**CIPS-22806**.
DTOS-3953	Inconsistent display and slow cursor movement is observed on monitors that are connected to external graphics cards. The issue is observed on Wyse 5070 Thin Client with ThinOS 9.1.3112—**CIPS-22805**.
DTOS-3950	Amazon Web Services session drops unexpectedly while usingMicrosoft Office apps—**CIPS-22418**.
DTOS-3909/DTOS-3530	SCEP auto enrollment does not work in ThinOS 9.x—**CIPS-22725, CIPS-21937**.
DTOS-3890	Idle Timeout does not work in PCoIP and Blast sessions when the value is set to 0. The issue is observed in ThinOS 9.1.2101.
DTOS-3748	Unable to launch PCoIP desktops in ThinOS 9.1.2101—**CIPS-21360**.
DTOS-3506	Unable to authenticate and log in to HealthCast, using Qwikaccess. The issue is observed on Wyse 3040 Thin Client with ThinOS 9.1.2101—**CIPS-22323**.
DTOS-3482	VNC fails to connect if the device is idle for too long. The issue is observed on Wyse 5070 Thin Client with ThinOS 9.1.2101—**CIPS-22070**.
DTOS-3466	Elo Touch Solution 10,1" 1002L does not work with ThinOS 9.1.2101. The issue is observed on Wyse 5070 Thin Client with ThinOS 9.1.2101—**CIPS-22302**.
DTOS-3441	There is a 30-60 seconds delay while connecting a Bluetooth mouse to ThinOS—**CIPS-22239**.
DTOS-3381	Key commands do not work as expected in a Windows Virtual Desktop RDS session. The issue is observed on Wyse 5070 Thin Client with ThinOS 9.1.2101—**CIPS-21920**.
DTOS-3359	Citrix broker failover does not work as expected in ThinOS 9—**CIPS-22156**.
DTOS-3326	SIPR tokens stopped working after upgrading to ThinOS 9.1.2101—**CIPS-22144**.
DTOS-3325	Graphics issue is observed on a Dell E2020H monitor that is connected to a DP1 port. The issue is observed on Wyse 3040 Thin Client with ThinOS 9.1.2101—**CIPS-22165**.
DTOS-3292	Ingenico Lane 3000 has redirection issues in VMware session. The issue is observed in ThinOS 9.1.2101—**VMware #SR21233499906, CIPS-22123**.
DTOS-3286	Ingenico card reader does not redirect in VMware View session—**CIPS-21751**.
DTOS-3242	**Disable Terminal Shutdown** option is not available in ThinOS 9—**CIPS-22024**.
DTOS-3241	**On Desktop** is missing from **Global Session Settings** for ThinOS 9. The option is available as **Display on Desktop** in Wyse Management Suite when configuring ThinOS 8.6 devices.
DTOS-3207	The option to disable lock and shutdown for users is not available—**CIPS-21755**.
DTOS-3175	Imprivata 2FA authentication issues are observed on devices that run ThinOS 9.1.2101—**CIPS-21819**.
DTOS-2995	Password input issue on Citrix session. Sometimes, when a correct password is entered after entering a wrong password, the device fails to log in—**CIPS-21740**.

Table 76. Fixed issues (continued)

Issue ID	Description
DTOS-2891	Smart card authentication fails on SIPR network but works on NIPR network. The issue is observed on Wyse 5070 Thin Client with ThinOS 9.1.2101—**CIPS-21612**.
DTOS-2772	Client loses connection on wireless roaming. The issue is observed on Wyse 3040 Thin Client with ThinOS 9.1.2101.
DTOS-2739	Updating the BIOS to version 1.2.5 on Wyse 3040 Thin Client can sometimes cause an error that states **Fatal Error: System is tampered, and will be restored**—**CIPS-21185**.
DTOS-2242	Granular control of peripherals is not available in 9.1.
DTOS-1985	Wyse 3040 Thin Client reboots when you touch the screen. The issue is observed on Faytech touch displays—**CIPS-20280**.
DTOS-1696	Letters **¥** and \ cannot be used on Japanese keyboard layout.

Known issues

Table 77. Known issues

Issue ID	Description	Workaround
DTOS-4898	The Bluetooth mouse name is not displayed properly in the Bluetooth scan window.	There is no workaround in this release.
DTOS-4893	**Enable LPD service for the printer** option does not work on ThinOS 9.1.4234 but works on ThinOS 8.x.	There is no workaround in this release.
DTOS-4884	Some application icons are not displayed on the desktop when logged into classic mode using VPN.	Use connection manager to get the full application list.
DTOS-4804	The selected default printer in the local client does not take effect in a broker connection.	There is no workaround in this release.
DTOS-4740	Pid information is not captured in the event log when you disconnect an HID 4500 device.	There is no impact on the functionality.
DTOS-4713	The RDP connection waiting prompt box overlaps the window to enter credentials.	There is no workaround in this release.
DTOS-4696	Default Printer drop-down list value is **Unselected** in the Admin Policy Tool. The issue is observed on Wyse 5070 Thin Client.	There is no workaround in this release.
DTOS-4683	An incorrect tip is displayed when you click the **Picture Shown Time** field under **Advanced** > **Personalization** > **Screen Saver** > **Screen Saver Type** > **Showing Pictures** in Admin Policy Tool or the Wyse Management Suite Policy settings.	There is no workaround in this release.
DTOS-4654	USB headset and Bluetooth headset names are displayed as same under **Peripherals** > **Audio**.	There is no workaround in this release.
DTOS-4554	When you connect a monitor to the client using a Type-C to HDMI connector, the monitor displays a black screen. The issue is observed on Wyse 5470 Thin Client.	There is no workaround in this release.
DTOS-4505	A blue screen is displayed for more than 15 seconds after restarting the device from PIE login window. The issue is observed on Wyse 5470 All-in-One Thin Client with PIE version 7.5.	There is no workaround in this release.
DTOS-4479	The PCoIP session is displayed on the system tray for a while after you sign out from account successfully.	There is no workaround in this release.

Table 77. Known issues (continued)

Issue ID	Description	Workaround
	The issue is observed on Horizon Broker server version 10.151.135.22.	
DTOS-4349	It takes approximately 2 minutes to start printing when you click the **Test Print** button. The issue is observed on Wyse 5070 Thin Client.	There is no workaround in this release.
DTOS-4340	After you enable customized login from **Advanced** > **Broker Settings** > **Amazon WorkSpaces Settings**, if you press **ESC** button twice when you start the broker sign-on window, only Amazon WorkSpaces logo is displayed on the customized login page. Username and password text fields are not displayed.	There is no workaround in this release.
DTOS-4319	Cursor disappears after you enable or disable the relative mouse option in PCoIP session.	There is no workaround in this release.
DTOS-4191	When you export Citrix logs to a USB drive, the name of the Citrix log file is **citrixlog.zip**.	There is no impact on the functionality.
DTOS-4188	The **Test Print** button must be clicked multiple times for the serial printer to print the results. The issue is observed on Wyse 5070 Thin Client.	There is no workaround in this release.
DTOS-4126	**Device Error = -1** is displayed after you wake the client from sleep mode.	Close the error window. There is no impact on the functionality.
DTOS-3888	When you set the resolution to 1920x1080 after connecting a monitor that supports a resolution larger than 1920x1080, the resolution is changed to 1680x1050 or 1600x900. The issue is observed when you power off the monitor and power it back on.	Set the resolution manually.
DTOS-3803	When **Citrix Workspace mode** is enabled and **HTTP User Agent** option is set, you cannot log in to Citrix server.	Disable **Citrix Workspace mode**.
DTOS-2754	An incorrect error message is displayed when launch a desktop or app that is under maintenance mode. The issue is observed on Citrix Workspace app version 21.4.0.11.1.	There is no workaround in this release.
DTOS-4870	An incorrect message is displayed when you launch a desktop VDA that is launched on another device. The issue is observed on Citrix Workspace app version 21.6.0.28.7.	There is no workaround in this release.
DTOS-4944	Inconsistent display and slow cursor movement is observed on monitors that are connected to external AMD graphics cards. The issue is observed on Wyse 5070 Thin Client.	Do not connect monitors to AMD graphics cards.
DTOS-5106	Sometimes the Zoom VDI in Citrix session does not work and you cannot start or join a meeting, after you upgrade the Citrix Workspace app package.	Uninstall the Zoom Citrix package and reinstall it.
DTOS-5107	Sometimes the Zoom VDI in Citrix does not launch in optimized mode, after you upgrade the Citrix Workspace app package.	Uninstall the Zoom Citrix package and reinstall it.
DTOS-5334	HID fingerprint reader does not work after you upgrade the HID package.	Disable the **Enable HID Fingerprint Reader** option from **Advanced** > **Session Settings** > **Global Session Settings** in the **Admin Policy Tool** or **Wyse Management Suite** policy settings, and save the setting changes. Enable the **Enable HID Fingerprint Reader** option again, before you log in to the Citrix server.

6

ThinOS 9.1.4097

Release date

March 2022

Compatibility

ThinOS build details

DTOS_9.1.4097.pkg—OptiPlex 3000 Thin Client

ThinOS application package details

- Cisco_Jabber_14.0.1.305989_2.pkg
- Cisco_WebEx_Meetings_VDI_41.6.1.10_2.pkg
- Cisco_WebEx_VDI_41.6.1.19187_1.pkg (formerly called Cisco WebEx Teams)
- Citrix_Workspace_App_21.6.0.28_2.pkg
- EPOS_Connect_6.1.0.19549_20.pkg
- HID_Fingerprint_Reader_210217_10.pkg
- Jabra_7.2.0_10.pkg
- Microsoft_WVD_1.3_1196.pkg
- Teradici_PCoIP_21.03.1_10.pkg
- VMware_Horizon_2106.8.3.0.18251983_6.pkg
- Zoom_Citrix_5.7.6.20822 _1.pkg
- Zoom_Horizon_5.7.6.20822_1.pkg
- Identity_Automation_QwickAccess_2.0.0_3.pkg

Tested BIOS version for ThinOS 9.1.4097

Table 78. Tested BIOS details

Platform name	BIOS version
OptiPlex 3000 Thin Client	1.0.0

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

Citrix Workspace app feature matrix

Table 79. Citrix Workspace app feature matrix

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
			not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires to 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.

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Limited support	Only supports WebKitGTK+, does not support CEF. BCR with CEF. Some of the QUMU videos fail to playback when Browser Content Redirection (BCR) is enabled. YouTube videos of 1080p fails to playback. This is a Citrix binary known issue.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	There are no limitations in this release.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. This is Citrix binary design.
	Video playback	Supported	There are no limitations in this release.

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Do not hot plug headset or the camera during a meeting, or a call. Do not switch the camera during a meeting. It causes the audio and video reception to be inconsistent. Restart Microsoft Teams to resolve this issue. This is also Citrix binary issue. Supports Microsoft Teams optimization through proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For more information, see the Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Zoom optimization via proxy server with anonymous authentication is not supported. For more information, see the Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Teams Offloading (tVDI)	Supported	Supports Webex Teams optimization mode through proxy server which is configured in ThinOS Network Proxy by APT/ Wyse Management Suite. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS 9.1.4097, , 9.1.4234, and later versions

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
			Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Offloading (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	Some of QUMU videos do not playback when BCR is enabled.
	UDP Audio	Supported (not with NetScaler Gateway)	Limited support—Not supported with Citrix ADC (formerly NetScaler) due to Citrix's limitation.
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	There are no limitations in this release.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	Not supported
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.

Table 79. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4097 + Citrix Workspace app 2106	ThinOS 9.1.4097 limitations
New features listed in Citrix Workspace App release note but not in feature matrix	Battery status indicator (CWA2106)	Supported	There are no limitations in this release.
	Service continuity (Technical Preview) (CWA2104, CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio (CWA2012 and CWA2010)	Not supported	Not supported
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

VMware Horizon feature matrix

Table 80. VMware Horizon feature matrix

Feature		ThinOS 9.1.4097
Broker Connectivity	SSL certificate verification	Supported with VDI, RDS Hosted Desktops and Apps
	Disclaimer dialog	Supported with VDI, RDS Hosted Desktops and Apps
	UAG compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Shortcuts from server	Not supported
	Pre-install shortcuts from server	Not supported
	File type association	Not supported
	Phone home	Supported with VDI, RDS Hosted Desktops and Apps
Broker Authentication	Password authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Single sign on	Supported with VDI, RDS Hosted Desktops and Apps
	RSA authentication	Supported with VDI, RDS Hosted Desktops and Apps
	Integrated RSA SecurID token generator	Not supported
	Kiosk mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remember credentials	Not supported
	Log in as current user	Not supported
	Nested log in as current user	Not supported
	Log in as current user 1-way trust	Not supported
	OS biometric authentication	Not supported
	Un-authentication access	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Cisco ACS	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – SMS Passcode	Supported with VDI, RDS Hosted Desktops and Apps
	Radius - DUO	Supported with VDI, RDS Hosted Desktops and Apps
	Radius – Microsoft Network Policy	Supported with VDI, RDS Hosted Desktops and Apps
Smart card	x.509 certificate authentication (Smart Card)	Supported with VDI, RDS Hosted Desktops and Apps
	CAC support	Supported with VDI, RDS Hosted Desktops and Apps
	.Net support	Supported with VDI, RDS Hosted Desktops and Apps

Table 80. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4097
	PIV support	Supported with VDI, RDS Hosted Desktops and Apps
	Java support	Not supported
	Purebred derived credentials	Not supported
	Device Cert auth with UAG	Not supported
Desktop Operations	Reset	Supported only with VDI
	Restart	Supported only with VDI
	Log off	Supported with VDI, RDS Hosted Desktops and Apps
Session Management (Blast Extreme & PCoIP)	Switch desktops	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple connections	Supported with VDI, RDS Hosted Desktops and Apps
	Multi-broker/multi-site redirection - Universal	Supported with VDI, RDS Hosted Desktops and Apps
	App launch on multiple end points	Supported with VDI, RDS Hosted Desktops and Apps
	Auto-retry 5+ minutes	Supported with VDI, RDS Hosted Desktops and Apps
	Blast network recovery	Supported with VDI, RDS Hosted Desktops and Apps
	Time zone synchronization	Supported with VDI, RDS Hosted Desktops and Apps
	Jumplist integration (Windows 7-Windows 10)	Not supported
Client Customization	Command line options	Not supported
	URI schema	Not supported
	Launching multiple client instances using URI	Not supported
	Preference file	Not supported
	Parameter pass-through to RDSH apps	Not supported
	Non interactive mode	Not supported
	GPO-based customization	Not supported
Protocols Supported with VDI, RDS Hosted Desktops and Apps	Blast Extreme	Supported with VDI, RDS Hosted Desktops and Apps
	H.264 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	H.265 - HW decode	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Codec	Supported with VDI, RDS Hosted Desktops and Apps
	JPEG/PNG	Supported with VDI, RDS Hosted Desktops and Apps

Table 80. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4097
	Switch encoder	Supported with VDI, RDS Hosted Desktops and Apps
	BENIT	Supported with VDI, RDS Hosted Desktops and Apps
	Blast Extreme Adaptive Transportation	Supported with VDI, RDS Hosted Desktops and Apps
	RDP 8.x, 10.x	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP	Supported with VDI, RDS Hosted Desktops and Apps
Features/Extensions Monitors/ Displays	Dynamic display resizing	Supported with VDI, RDS Hosted Desktops and Apps
	VDI windowed mode	Supported with VDI, RDS Hosted Desktops and Apps
	Remote app seamless window	Not supported
	Multiple monitor support	Supported with VDI, RDS Hosted Desktops and Apps
	External monitor support for mobile	Not supported
	Display pivot for mobile	Not supported
	Number of displays Supported with VDI, RDS Hosted Desktops and Apps	4
	Maximum resolution	3840x2160
	High DPI scaling	Supported only with VDI
	DPI sync	Supported with VDI, RDS Hosted Desktops and Apps
	Exclusive mode	Not supported
	Multiple monitor selection	Supported with VDI, RDS Hosted Desktops and Apps
Input Device (Keyboard/Mouse)	Language localization (EN, FR, DE, JP, KO, ES, CH)	Supported with VDI, RDS Hosted Desktops and Apps
	Relative mouse	Supported only with VDI
	External Mouse Support	Supported with VDI, RDS Hosted Desktops and Apps
	Local buffer text input box	Not supported
	Keyboard Mapping	Supported with VDI, RDS Hosted Desktops and Apps
	International Keyboard Support	Supported with VDI, RDS Hosted Desktops and Apps
	Input Method local/remote switching	Not supported
	IME Sync	Supported with VDI, RDS Hosted Desktops and Apps
Clipboard Services	Clipboard Text	Supported with VDI, RDS Hosted Desktops and Apps
	Clipboard Graphics	Not supported

Table 80. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4097
	Clipboard memory size configuration	Supported with VDI, RDS Hosted Desktops and Apps
	Drag and Drop Text	Not supported
	Drag and Drop Image	Not supported
	Drag and Drop File/Folder	Not supported
Connection Management	IPv6 only network support	Supported with VDI, RDS Hosted Desktops and Apps
	PCoIP IP roaming	Supported with VDI, RDS Hosted Desktops and Apps
Optimized Device Redirection	Serial (COM) Port Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Client Drive Redirection/File Transfer	Not supported
	Scanner (TWAIN/WIA) Redirection	Supported with VDI, RDS Hosted Desktops and Apps
	x.509 Certificate (Smart Card/ Derived Credentials)	Supported with VDI, RDS Hosted Desktops and Apps
	Gyro Sensor Redirection	Not supported
Real-Time Audio-Video	Audio in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Video in (input)	Supported with VDI, RDS Hosted Desktops and Apps
	Multiple webcams	Not supported
	Multiple speakers	Not supported
USB Redirection	USB redirection	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnInsert	Supported with VDI, RDS Hosted Desktops and Apps
	Policy: ConnectUSBOnStartup	Supported with VDI, RDS Hosted Desktops and Apps
	Connect/Disconnect UI	Not supported
	USB device filtering (client side)	Supported with VDI, RDS Hosted Desktops and Apps
	Isochronous Device Support	Supported only with VDI
	Split device support	Supported only with VDI
	Bloomberg Keyboard compatibility	Supported with VDI, RDS Hosted Desktops and Apps
	Smartphone sync	Supported only with VDI
Unified Communications	Skype for business	Supported with VDI, RDS Hosted Desktops and Apps
	Zoom Cloud Meetings	Supported with VDI, RDS Hosted Desktops and Apps
	Cisco Jabber Softphone	Supported with VDI, RDS Hosted Desktops and Apps

Table 80. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4097
	Cisco WebEx Teams	Supported with VDI, RDS Hosted Desktops and Apps
	Cisco WebEx Meetings	Not supported
	Microsoft Teams RTAV	Supported with VDI, RDS Hosted Desktops and Apps
	Microsoft Teams offload	Supported with VDI, RDS Hosted Desktops and Apps
Multimedia Support	Multimedia Redirection (MMR)	Supported with VDI, RDS Hosted Desktops and Apps
	HTML5 Redirection	Not supported
	Directshow Redirection	Not supported
	URL content redirection	Not supported
	Browser content redirection	Not supported
Graphics	vDGA	Supported only with VDI
	vSGA	Supported only with VDI
	NVIDIA GRID VGPU	Supported with VDI, RDS Hosted Desktops and Apps
	Intel vDGA	Supported only with VDI
	AMD vGPU	Supported only with VDI
Mobile Support	Client-side soft keyboard	Not supported
	Client-side soft touchpad	Not supported
	Full Screen Trackpad	Not supported
	Gesture Support	Not supported
	Multi-touch Redirection	Not supported
	Presentation Mode	Not supported
	Unity Touch	Not supported
Printing	VMware Integrated Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Location Based Printing	Supported with VDI, RDS Hosted Desktops and Apps
	Native Driver Support	Not supported
Security	FIPS-140-2 Mode Support	Supported with VDI, RDS Hosted Desktops and Apps
	Imprivata Integration	Supported with VDI, RDS Hosted Desktops and Apps
	Opswat agent	Not supported
	Opswat on-demand agent	Not supported
	TLS 1.1/1.2	Supported with VDI, RDS Hosted Desktops and Apps
Session Collaboration	Session Collaboration	Supported with VDI, RDS Hosted Desktops and Apps

Table 80. VMware Horizon feature matrix (continued)

Feature		ThinOS 9.1.4097
	Read-only Collaboration	Supported with VDI, RDS Hosted Desktops and Apps
Update	Update notifications	Not supported
	App Store update	Not supported
Other	Smart Policies from DEM	Supported with VDI, RDS Hosted Desktops and Apps
	Access to Linux Desktop - Blast Protocol Only	Supported with VDI, RDS Hosted Desktops and Apps
	Workspace ONE mode	Supported with VDI, RDS Hosted Desktops and Apps
	Nested - basic connection	Supported with VDI, RDS Hosted Desktops and Apps

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

Windows Virtual Desktop and RDP feature comparison matrix

Table 81. Windows Virtual Desktop and RDP feature comparison matrix

Category Supported	Features	ThinOS 9.1.4097
Service	Direct connection to Desktop via RDP	Supported
	Microsoft 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
	Multi-touch	Not supported
Audio Visual	Audio in	Supported
	Audio out	Supported
Storage	Folder/Drive Redirection	Supported
Clipboard	Clipboard (text)	Supported
	Clipboard (object)	Supported
	Clipboard (file)	Not supported
Redirections	Printer	Supported
	Serial Port	Not supported
	SmartCard	Not supported
	USB (General)	Not supported
Session Experience	Dynamic Resolution	Supported

Table 81. Windows Virtual Desktop and RDP feature comparison matrix (continued)

Category Supported	Features	ThinOS 9.1.4097
	Start Command	Supported
	Desktop Experience	Not supported
	Desktop Scale Factor	Supported
	Multi-Monitor (All)	Supported
	Restricted full screen session	Supported
	Keyboard Layout Mapping	Not supported
	Time Zone Mapping	Supported
	RemoteFX	Not supported
	Video/Audio/Online playback	Supported
	Compression	Supported
	Optimize for low speed link	Supported
Graphics (CODECs)	H.264 Support	Supported
	H.264 AVC-444	Not supported
	TSMM (MMR)	Not supported
	VOR	Not supported
Authentication	TS Gateway Supported	Supported
	- TSGW II	Not supported
	- TSGW III	Not supported
	- TSGW WebSocket	Not supported
	- TSGW + UDP	Not supported
	NLA	Supported
	SmartCard	Not supported
	Imprivata	Supported

New and enhanced features

Wireless chipset support and limitation for OptiPlex 3000 Thin Client

Intel WiFi 6E AX210 and Intel 9560 are the two wireless chipsets that are supported on OptiPlex 3000 Thin Client. All wireless and Bluetooth software features remain the same. ThinOS 9.1.4097 does not support WiFi 6/6E.

VMware Horizon Blast updates

Bloomberg keyboard STB 100 mapping

You can connect the keyboard using either single or dual USB cables. No setting changes or redirection is required. All the function keys work without any redirection. For steps to disable redirection, see the *Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide* at www.dell.com/support.

Microsoft Teams optimization

VMware Horizon 2106 package for the client side includes Microsoft Teams media optimization by default. Media optimization for Microsoft Teams that is installed by default in Horizon Agent, is controlled by a group policy object (GPO). GPO is not enabled by default. You can enable the optimization by using a Group Policy Editor.

For the steps on enabling the optimization using a Group Policy Editor, see the *Dell Wyse ThinOS 9.1.4097, , 9.1.4234, and later versions Administrator's Guide* at www.dell.com/support.

NOTE: Install the Horizon Agent before you install Microsoft Teams.

To check whether Microsoft Teams is launched in optimized mode, click the three dots next to your profile picture, and go to **About** > **Version**. A banner that says **VMware Media Optimized** is displayed, indicating that Microsoft Teams has launched in optimized mode. Alternatively, you can click the three dots next to your profile picture, and go to **Settings** > **Devices** > **Audio devices.** . Check whether the local headset names are displayed in the **Speakers** and **Microphone** drop-down lists, instead of **Virtual DevTap** or **VDI**.

Microsoft Teams optimization feature matrix

Table 82. Microsoft Teams optimization feature matrix

Scenario	ThinOS
Long audio call	Supported
Call—Make an audio call	Supported
Call—Answer an audio call	Supported
Call—Make a video call	Supported
Call—Answer a video call	Supported
Call—Turn the camera on or off	Supported
Call—Enter or exit full screen	Supported
Call—Hold or resume a call	Supported
Call—End call	Supported
Call—Mute or unmute audio	Supported
Call—Transfer	Not supported
Call—Consult then transfer	Not tested
Call—Keypad	Not tested
Call—Start or stop recording	Not tested
Call—Turn off or turn on incoming video	Supported
Call—Group video call	Supported
Call—Group audio call	Supported
Call—Invite someone during a call	Supported
Meeting	Supported
Share screen—Desktop	Supported
Share screen—PowerPoint	Supported
Chat	Supported
Audio or video call in VDI server desktop	Supported
Audio or video call in published Microsoft Teams application	Not tested
Devices—Plug in or disconnect the headset	Supported—Dell Technologies recommends to not plug in or disconnect headsets during a call.

Table 82. Microsoft Teams optimization feature matrix (continued)

Scenario	ThinOS
Devices—Switch headset	Supported—Dell Technologies recommends to not switch headsets during a call.
Devices—Plug in or disconnect the camera	Supported—Dell Technologies recommends to not plug in or disconnect camera during a call.
Devices—Switch camera	Not supported
Headset buttons—Answer/Mute/End Call	Not supported

Microsoft Teams optimization limitations and known issues

- Depending on your network bandwidth latency, the audio quality may fluctuate. To avoid this issue, ensure that your network bandwidth is adequate for audio or video call. Dell Technologies recommends 200 KBps or higher network speed for a single client.
- Audio is still played through the first headset when you switch to the second headset during the call. This issue is observed when you have installed the JVDI package on the thin client. Workaround is that if you are using Microsoft Teams (or Zoom), do not install the Cisco JVDI package. This issue is due to Cisco limitation.
- When using a headset, you cannot answer or end the call through headset buttons. This issue is due to a limitation of Microsoft Teams.
- Sharing screen when Microsoft Teams is published as an application is not supported. This issue is due to a limitation of VMware Horizon.
- There maybe inconsistency on how the video is displayed during video calls. The issue fixes by itself after 5 minutes.
- Audio may be inconsistent during video calls. Try the following:
  - Sometimes audio is distorted during a call. Workaround is to change the headset.
  - Sometimes there can be network issues. Ensure that your network bandwidth is adequate for audio and video calls. Dell Technologies recommends 200 KBps or higher network speed for a single client.

Teradici PCoIP update

Updated the Teradici PCoIP package version to 21.03.1_10. No new features are added.

Microsoft Windows Virtual Desktop update

The following peripherals are supported from Microsoft Windows Virtual Desktop version 1.3_1196:

- Camera—Connect the camera to client, and then launch the RDP session. You must disable the Remote Gateway option for the camera to work.
- Printer—RDP session supports LPT, LPD and SMB printers.

  NOTE: RDP protocol supports standard printer.

For more information, see the *Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide* at www.dell.com/support.

Unified Communications optimization packages update

- Updated Cisco Webex Meetings VDI to version 41.6.1.10.2.
- Updated Cisco Webex VDI to version 41.6.1.19187.1.
- Updated Cisco Jabber to version 14.0.1.305989.2.
- Updated Zoom to version 5.7.6.20822.1.

Identity automation updates

Identity Automation QwickAccess package is updated to 2.0.0.3. The following are the enhancements:

- Identity Automation QwickAccess supports Citrix Broker agent and supports user binding card in same domain with Citrix Broker agent. Users in different domains are not supported and not recommended.
- API key is treated as password in Wyse Management Suite policy settings, Admin Policy Tool, and ThinOS local user interface. It is not displayed in plain text.
- Identity Automation QwickAccess is verified based on Identity server version 1.6.0.1.
- PIN reset is removed in this release.

Imprivata PIE limitation

Imprivata PIE is not supported in this release.

ThinOS updates

- From ThinOS 9.1.4097 onwards, you can enable or disable IPv6 from **Advanced** > **Network Configuration** > **Common Settings** > **Enable IPv6** in Wyse Management Suite policy settings or the Admin Policy Tool. IPv6 is enabled by default for both wired and wireless networks.
- The window that is displayed when you change a group in Wyse Management Suite is changed.
- The window that is displayed when you update packages and the operating system firmware is changed.
- The **HTTP/HTTPS** proxy default port is changed from 808 to 8080.

For more information about the updates, see the *Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide* at www.dell.com/support.

Updates to Admin Policy Tool and Wyse Management Suite policy settings

- **Disabling Push Notification**—**Ignore MQTT** in **Services** > **WDA Settings** is changed to **Disabling Push Notification**.
- **VNCD Server**—Added input validation for the VNCD Server field in **Services** > **VNC Service**. You can only enter values in the format of IP addresses.
- **Disable Shutdown**—Added **Disable Shutdown** option in **Login Experience** > **Login Settings**. This option disables the **Shutdown** option in the ThinOS **Shutdown** window, and also disables the physical shutdown button on the thin client.
- **Login Expire Time**—Added **Login Expire Time** option in **Login Experience** > **Login Settings**. Using this option, you can set a countdown after you log in. After the countdown expires, to launch any new desktop or application, you must enter the user password. After you enter the password, the countdown starts again. Desktop or applications that you launch before the expiry of the countdown remains open and are not affected. To disable the countdown, set the value to **0**.

  NOTE: Configuration of this setting is not supported in this release.
- **Reboot on monitor connection**—Changed the default value of **Reboot on monitor connection** option under **Enable ProveID Embedded Mode** in **Login Experience** > **3rd Party Authentication** > **Imprivata** to disabled.
- **API Key**—Changed the **API Key** field option in **Login Experience** > **Login Settings** > **Identity Automation** > **Identity Automation** to password type to hide the input values.
- **Enable IPv6**—Added the option **Enable IPv6** in **Network Configuration** > **Common Settings** to enable or disable IPv6.
- **Scheduled Reboot** and **Shutdown Settings**—Added time format validation for the following fields under **System Settings** > **Scheduled Reboot Settings** and **Scheduled Shutdown Settings**:
  - **Scheduled Reboot Settings** > **Scheduled Reboot Time**
  - **Scheduled Reboot Settings** > **Reboot after Idle Time**
  - **Scheduled Shutdown Settings** > **Scheduled Shutdown Time**
  - **Scheduled Shutdown Settings** > **Shutdown after Idle Time**

  NOTE: If you change the time zone on the local client, the **Scheduled Reboot settings** and **Scheduled Shutdown settings** takes effect only after a reboot.
- **Granular Control of Peripherals**—Added **Granular Control of Peripherals** in **Privacy & Security** > **Account Privileges** to make the selected tabs visible in the **Peripherals** window. To see this option, you must set the privilege level as **Customize** and enable **Peripherals**.
- **DHCP**—Updated the **DHCP** option in **Privacy & Security** > **Account Privileges**. The setting is enabled by default. To see this option, you must set the privilege level as **Customize** and enable **Network Setup**.
- **Allow High Efficiency Video Decoding**—Added **Allow High Efficiency Video Decoding** option in **Session Settings** > **Blast Session Settings**.

ⓘ **NOTE:** OptiPlex 3000 Thin Client does not support this feature.

- **On Desktop**—Moved **On Desktop** option from **Session Settings** > **Citrix Session Settings** to **Session Settings** > **Global Session Settings**.
- **Business Hour Settings**—Added **Business Hour Settings** under **Services** > **WDA Settings**. Administrators can now enable or disable session reporting and enable configure devices to do session reporting outside of business hours. Administrators can also enable configure devices to apply configurations outside of business hours.

  ⓘ **NOTE:** Configuration of this setting is not supported in this release.

For more information about the updates, see the *Dell Wyse ThinOS 9.1.4097, 9.1.4234, and later versions Administrator's Guide* at www.dell.com/support.

Tested environments matrix

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

Table 83. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.5/3.3.1
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 84. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops/Citrix Virtual Apps 7.15 LTSR Cumulative Update 5 (CU5)	Tested	Tested	Not tested	Tested
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2103	Tested	Tested	Tested	Tested

Table 85. Tested environment—VMware Horizon

VMware	Windows 10	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2016 APPs	Windows Server 2019 APPs
VMware Horizon 7.12	Tested	Not tested	Tested	Tested	Tested	Tested
VMware Horizon 2006	Tested	Not applicable	Not tested	Tested	Not tested	Tested
VMware Horizon 2103	Tested	Not applicable	Tested	Tested	Tested	Tested

Table 86. Test environment—Microsoft RDP

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

Table 87. Test environment—WVD

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

Table 88. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	2.9.300	2.9.300	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				

Table 89. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business Client	Skype for Business Agent	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	5.4, 8.2	7.12, 8.2	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	5.4, 8.2	7.12, 8.2	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested	Not tested	Not tested

Table 90. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	14.0.1	14.0.1	14.0.1
	Windows server 2016			
	Windows server 2019			

Table 91. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	14.0.1	14.0.1	14.0.1
	Windows server 2016	14.0.1	14.0.1	14.0.1
	Windows server 2019	Not tested	Not tested	Not tested

Table 92. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	5.7.6.20822	5.7.6
	Windows server 2016		
	Windows server 2019		

Table 93. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	5.7.6.20822	5.7.6
	Windows server 2016	5.7.6.20822	5.7.6
	Windows server 2019	Not tested	Not tested

Table 94. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	41.6.1.19187	41.6.1.19162
	Windows server 2016		
	Windows server 2019		

Table 95. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2103	Windows 10	41.6.1.19187	41.6.0.19162
	Windows server 2016	41.6.1.19187	41.6.0.19162
	Windows server 2019	Not tested	Not tested

Table 96. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2103	Windows 10	41.6.1.10.2	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.6 to 41.10.
	Windows server 2016		
	Windows server 2019		

Supported peripherals

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

Table 97. Supported peripherals

Product category	Peripherals
Audio devices	Dell Slim Soundbar - Ariana - SB521A
	Dell Pro Stereo Headset - Cortez - WH3022.
	Dell Pro Stereo Soundbar - AE515M - Nirvana M
	Dell Stereo Soundbar - AC511M - Potential M
	Jabra Engage 65 MS Wireless Headset - 9559-553-125
	Jabra Evolve 65 MS Stereo - Headset - 6599-823-309
	Dell Mobile Adapter Speakerphone - MH3021P - Apollo
	Dell Pro Stereo Headset UC350
	Jabra GN2000
	Jabra PRO 9450
	Jabra Speak 510 MS, Bluetooth

Table 97. Supported peripherals (continued)

Product category	Peripherals
	Jabra BIZ 2400 Duo USB MS
	Jabra Evolve 75
	Jabra UC SUPREME MS Bluetooth (link 360)
	Jabra EVOLVE UC VOICE 750
	Plantronics SAVI W740/Savi W745 (supportd USB only, does not support Bluetooth)
	Plantronics Blackwire 5220 Series
	Plantronics AB J7 PLT
	Plantronics Blackwire C5210
	Plantronics BLACKWIRE C710, Bluetooth
	Plantronics Calisto P820-M
	Plantronics Voyager 6200 UC
	SENNHEISER SP 10 ML Speakerphone for Lync
	SENNHEISER SC 660 USB ML
	SENNHEISER USB SC230
	SENNHEISER D 10 USB ML-US Wireless DECT Headset
	SENNHEISER SC 40 USB MS
	SENNHEISER SP 10 ML Speakerphone for Lync
	Sennheiser SDW 5 BS-EU
	Logitech S-150
	POLYCOM Deskphone CX300
	PHILIPS - analog
	Logitech h150 - analog
	LFH3610/00 SPEECHMIKE PREMIUM (only support redirect)
	Nuance PowerMic II (suggest to redirect whole device)
Camera	Logitech BRIO 4K Ultra HD Webcam - 960-001105
	Logitech C525 HD Webcam - 960-000715
	Logitech C930e HD Webcam - 960-000971
	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

Table 97. Supported peripherals (continued)

Product category	Peripherals
Displays	Dell UltraSharp 24 Monitor - U2422H
	Dell 24 Monitor - P2422H
	Dell UltraSharp 24 USB-C HUB Monitor - U2422HE
	Dell Collaboration 24 USB-C Hub Monitor - C2422HE
	Dell 24 USB-C Hub Monitor - P2422HE
	Dell Collaboration 34 USB-C Hub Monitor - C3422WE
	Dell UltraSharp 27 USB-C HUB Monitor - U2722DE
	Dell 27 USB-C Hub Monitor - P2722HE
	Dell UltraSharp 27 Monitor - U2722D
	Dell Collaboration 27 USB-C Hub Monitor - C2722DE
	Dell 27 Monitor - P2722H
	Dell 22 Monitor - P2222H
	Dell 24 Monitor - P2421
	Dell 24 Monitor - P2421D
	Dell UltraSharp 34 Curved USB-C HUB Monitor - U3421WE
	Dell 20 Monitor E2020H
	Dell 27 Monitor - P2720D
	Dell UltraSharp 25 USB-C Monitor - U2520D
	Dell 24 Monitor E2420HS
	Dell 27 Monitor - P2720D - P2720DC
	Dell 23 Monitor - P2319H
	Dell 27 Monitor E2720HS - E2720H
	Dell 27 Monitor E2720H - E2720HS
	Dell 24 Touch Monitor - P2418HT
	Dell 19 Monitor E1920H
	Dell UltraSharp 32 4K USB-C Monitor - U3219Q
	Dell 24 Monitor E2420H
	Dell U2718Q (3840x2160)
	Dell U2719D (1920x1080)
	Dell P2719H (1920*1080)
	Dell P2715Q (3840x2160)
	Dell S2719HS (1920x1080)
	Dell S2817Q (3840x2160)
	Dell U2713HM (2560x1440)
	Dell U2718Q (3840x2160)
	Dell P2418HZ
	Dell U3219Q (3840x2160)

Table 97. Supported peripherals (continued)

Product category	Peripherals
	Dell U3419W (3440 x1440)
	Dell P2415Q (3840X2160)
External Data Storage	Dell USB Slim DVD +/û RW Drive - DW316 - Agate
Input devices (Keyboard and Mouse)	Dell Multi-Device Wireless Keyboard and Mouse Combo - KM7120W - Felix
	Dell Multi-Device Wireless Mouse - MS5320W - Comet
	Dell Multimedia Keyboard - KB216_BLACK - Rusty
	Dell Optical Mouse - MS116_BLACK - Sapphire
	Dell Wired Mouse with Fingerprint Reader - MS819 - Ultramarine
	Dell KB813 Smartcard Keyboard - KB813 - Cardinal
	Dell Mobile Pro Wireless Mice - MS5120W_Black - Splinter
	Dell Business Multimedia Keyboard - KB522 - Scarlet
	Dell Mobile Wireless Mouse - MS3320W_Black - Dawson
	Dell Premier Multi-Device Wireless Keyboard and Mouse - Acadia IO - KM7321W
	Dell Pro Wireless Keyboard and Mouse - Tasman (previous Windsor) - KM5221W
	Dell Laser Wired Mouse - MS3220_Black - Morty
	Dell Optical Wireless Mouse - WM122
	Dell Optical Wireless Mouse - WM123
	Dell Keyboard KB216p
	DELL wireless Keyboard/mouse KM632
	DELL wireless Keyboard/mouse KM714
	Dell Keyboard KB212-B
	Bloomberg Keyboard STB 100
	Microsoft Arc Touch Mouse 1428
	Microsoft Ergonomic Keyboard
	Rapoo E6100, bluetooth
Other	Intuos Pro wacom
Printers	Dell B1165nfw Mono Multifunction Printer
	Dell B1265dnf Multifunction Laser Printer
	Dell B2360d Laser Printer
	HP M403D
	Brother DCP-7190DW
	Dell B2360dn Laser Printer
	Lexmark X864de
	HP LaserJet P2055d
	HP Color LaserJet CM1312MFP
Smart card readers	OMNIKEY HID 3021
	OMNIKEY OK CardMan3121

Table 97. Supported peripherals (continued)

Product category	Peripherals
	HID OMNIKEY 5125
	HID OMNIKEY 5421
	SmartOS powered SCR335
	SmartOS powered SCR3310
	Cherry keyboard RS 6600 with smart card
	Cherry keyboard RS 6700 with smart card
	Cherry keyboard KC 1000 SC with smart card
	Dell keyboard KB813 (Smartcard reader)
	Dell Keyboard SK-3205 (Smartcard reader)
	IDBridge CT31 PIV
	Gemalto IDBridge CT710
	GemPC Twin
Storage	Sandisk cruzer 8 GB
	SanDisk cruzer 16G
	SanDisk USB3.1 and Type-C 16GB
	Kingston DTM30 32GB
	Kingston DT microDuo 3C 32GB
	Kingston DataTraveler G3 8 GB
	Bano type-c 16B
	SanDisk Ultra Fit 32G
	Dell External Tray Load ODD (Agate) (DVD Writer)
	Samsung portable DVD Writer SE-208
Teradici remote cards Teradici remote cards	Teradici host card 2220
	Teradici host card 2240

Supported smart cards

Table 98. Supported smart cards

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Oberthur CosmopolC 64k V5.2
ActivIdentity V1	ActivClient 7.1	ActivClient Cryptographic Service Provider	Gemalto Cyberflex Access 64K V2c
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Gemalto TOPDLGX4
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	G&D SCE 3.2

Table 98. Supported smart cards (continued)

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur IDOne 5.5
ActivIdentity v2 card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Oberthur Cosmo V8
ActivIdentity crescendo card	ActiveClient 7.2	ActivClient Cryptographic Service Provider	Giesecke and Devrient SmartCafe Expert 7.0 (T=0)
ID Prime MD v 4.0.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840
ID Prime MD v 4.0.2 (Gemalto 840)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 840 B
ID Prime MD v 4.1.0	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3810 MIFARE 1K
ID Prime MD v 4.1.3 (Gemalto 3811)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 3811 Mifare-Desfire
ID Prime MD v 4.1.1	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS
ID Prime MD v 4.3.5	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 830-FIPS Rev B
ID Prime MD v 4.4.2	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDPrime MD 940
Etoken Java (aladdin)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	IDCore30B eToken 1.7.7
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 510x
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 FIPS
Etoken Java (aladdin) (black USB drive)	Safenet Authentication Client 10.8	eToken Base Cryptographic Provider	SafeNet eToken 5110 CC
SafeNet High Assurance Applets Card	SafeNet High Assurance Client 2.12	SafeNet Smart Card Key Storage Provider	SC650 (SafeNet SC650 4.1t)
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.0 T=0/1 0V300
A.E.T. Europe B.V.	SafeSign-Identity-Client-3.0.76	SafeSign Standard Cryptographic Service Provider	Giesecke & Devrient StarCos 3.2
PIV (Yubico) (black USB drive)	YubiKey PIV Manager	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
PIV (Yubico Neo) (black USB drive)	Yubikey Manager v 1.1.4	Microsoft Base Smart Card Crypto Provider	YubiKey 4.3.3
cv cryptovision gmbh (c) v1.0ns	cv_act_scinterface_6.1.6	cv act sc/interface CSP	Giesecke & Devrient StarCos 3.2
N/A (Buypass BelDu)	Net iD 6.8.1.31, 2.0.44	Net iD - CSP	BelDu 6.0.4
N/A (GEMALTO IDPrime SIS)	Net iD 6.8.1.31, 2.0.44	Net iD - CSP	IDPrime SIS 4.0.2

Table 98. Supported smart cards (continued)

Smart Card information from the ThinOS event log	Driver	Provider (CSP)	Card type
Rutoken ECP 2.0 (2100)	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken ECP 2.0 (2100)
Rutoken 2151	Rutoken Drivers 4.6.3.0	Aktiv ruToken CSP v1.0	Rutoken (2151)

Known issues

Table 99. Known issues

Issue ID	Description	Workaround
DTOS-3450	WiFi6 is not supported on OptiPlex 3000 Thin Clients that run ThinOS 9.1.4097.	There is a no workaround in this release.
DTOS-4339	Bluetooth headset that is connected to the thin client produces a static noise, and the audio is intermittent.	There is a no workaround in this release.
DTOS-4322	When you push BIOS settings using Wyse Management Suite, if you are setting a new password, the password must be pushed first. You cannot push other setting changes along with a new password.	Workaround is to sync BIOS password in the Wyse Management Suite server.
DTOS-4280	After you resume from S3 sleep state, Bluetooth headset that is connected to the thin client shows connected but does not play audio.	Reconnect the Bluetooth headset.
DTOS-4251	If you disconnect the USB Type-C cable, and reconnect it after 30s, the monitor shows a black screen.	Power off and power on the monitor.
DTOS-4122	Bluetooth mouse cursor does not move smoothly.	Do not connect Bluetooth mouse and Bluetooth headset together.
DTOS-4383	Mouse and keyboard do not work for 2 minutes, if you reboot the client with a 3D mouse connected.	There is a no workaround in this release.

Citrix Workspace app 2112, VMware Horizon 2111, Cisco WebEx Meetings VDI 41.12, Cisco WebEx VDI 41.12, and Zoom 5.8.4 application packages for ThinOS

Release summary

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

Current versions

Citrix_Workspace_App_21.12.0.18_2.pkg

VMware_Horizon_2111.8.4.0.18957622_3.pkg

Cisco_WebEx_Meetings_VDI_41.12.6.12_1.pkg

Cisco_WebEx_VDI_41.12.0.20899_1.pkg (formerly Cisco WebEx Teams)

Zoom_Citrix_5.8.4.21112_1.pkg

Zoom_Horizon_5.8.4.21112_1.pkg

Release date

January 2022

Supported platforms

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client

Important notes

- Upgrade the ThinOS firmware to 9.1.5067 before you install the application packages.
- Cisco WebEx Meetings VDI, Cisco WebEx VDI, and Zoom VDI are qualified for Citrix VDI on ThinOS 9.1.5067 with Citrix Workspace app package Citrix_Workspace_App_21.12.0.18_2.pkg.
- Cisco WebEx Meetings VDI, Cisco WebEx VDI, and Zoom VDI are qualified for VMware Blast VDI on ThinOS 9.1.5067 with VMware Horizon package VMware_Horizon_2111.8.4.0.18957622_3.pkg.

Installing the application package

Download the application packages

Steps

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

Install the application package using Wyse Management Suite

Prerequisites

- Upgrade the ThinOS firmware to 9.1.5067 before you install the application package.
- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.

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

Steps

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

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

Compatibility

Application package information

- Supported ThinOS application packages—The following ThinOS packages are qualified by Dell Technologies.
  - Citrix_Workspace_App_21.12.0.18_2.pkg
  - VMware_Horizon_2111.8.4.0.18957622_3.pkg
  - Cisco_WebEx_Meetings_VDI_41.12.6.12_1.pkg
  - Cisco_WebEx_VDI_41.12.0.20899_1.pkg (formerly Cisco WebEx Teams)
  - Zoom_Citrix_5.8.4.21112_1.pkg
  - Zoom_Horizon_5.8.4.21112_1.pkg
- Supported Firmware—ThinOS version 9.1.5067.

NOTE: For information about other packages, see ThinOS application package details in the **ThinOS 9.1.5067 Release Notes**.

Previous versions

- Citrix_Workspace_App_21.9.0.25_6.pkg
- VMware_Horizon_2106.8.3.0.18251983_9.pkg
- Cisco_WebEx_Meetings_VDI_41.10.3.19_2.pkg
- Cisco_WebEx_VDI_41.10.0.20213_4.pkg (formerly Cisco WebEx Teams)
- Zoom_Citrix_5.8.0.20927_8.pkg
- Zoom_Horizon_5.8.0.20927_8.pkg

Citrix Workspace app feature matrix

Table 100. Citrix Workspace app feature matrix

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
Citrix Workspace	Citrix Virtual Apps	Supported	Citrix session prelaunch and session linger features are not supported. This is Linux binary design.
	Citrix Virtual Desktops	Supported	There are no limitations in this release.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.
	Auto-client Reconnect	Supported	There are no limitations in this release.

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	URL redirection has limitations in Citrix Workspace app for Linux client. It requires launch client browser through Local app access policy (which is not supported in Linux client) to access the URL redirection blacklist URL. Citrix support recommends using Browser Content Redirection (BCR) in Linux client to replace URL redirection.
	File open in Citrix Workspace app	N/A	Not supported. No local file explorer on ThinOS.
	Browser content redirection	Supported	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	There are no limitations in this release.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	Webcam redirection	Supported	Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. This is Citrix binary design. Citrix Workspace app 2112 only supports built-in camera. External cameras does not work. The issue is also observed in Linux binary.
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	Citrix Linux binary supports only x86 client.
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	Unified Communication Cisco Webex VDI Optimization (tVDI) (formerly Cisco WebEx Teams)	Supported	Supports Cisco Webex VDI (formerly Cisco WebExTeams) optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by Admin Policy Tool or Wyse Management Suite. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Meetings Optimization (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous, and username or password authentications. It does not support the proxy configured by DHCP Option 252. For more information, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported	There are no limitations in this release.
HDX Graphics	H.264-enhanced SuperCodec	Supported	There are no limitations in this release.
	Client hardware acceleration	Supported	There are no limitations in this release.
	3DPro Graphics	Supported	There are no limitations in this release.
	External Monitor Support	Supported	For limitations, see the Dell Wyse ThinOS Version 9.1.5067 Administrator's Guide at www.dell.com/support.

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Active Directory	Supported	There are no limitations in this release.
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.
	TLS 1.0/1.1	Not supported	ThinOS 9.1 does not provide the configuration to change TLS.
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	ThinOS does not provide local browser.
	IPV6	Not supported	Not supported—Can sign in but cannot connect to the session.
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace app release notes but not in feature matrix	Request control in Microsoft Teams (CWA2112)	Not Supported	Not supported
	Support for cursor color inverting (CWA2112)	Supported	For limitations, see the Citrix Workspace app limitations section.
	Microsoft Teams enhancement to echo cancellation (CWA2111)	Supported	There are no limitations in this release.
	Enhancement on smart card support (CWA2112)	Supported	For limitations, see the Citrix Workspace app limitations section.
	Webcam redirection for 64-bit (Technical Preview) (CWA2111)	Not supported	Not supported
	Support for custom web stores (Technical Preview) (CWA2111)	Not supported	Not supported
	Workspace with intelligence (Technical Preview) (CWA2111)	Not supported	Not supported
	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Supported	There are no limitations in this release
	Adaptive audio (CWA2109, CWA2112)	Supported	There are no limitations in this release
	Storebrowse enhancement for service continuity(CWA2109)	Not supported	Not supported

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	Global App Config Service (Public Technical Preview) (CWA2109)	Not supported	Not supported
	EDT MTU discovery (CWA2109)	Not supported	Not supported
	Creating custom user-agent strings in network request (CWA2109)	Not supported	Not supported
	Feature flag management (CWA2109)	Not supported	Not supported
	Battery status indicator (CWA2106, CWA 2111)	Supported	There are no limitations in this release.
	Service continuity (CWA2109)	Not supported	Not supported
	User Interface enhancement (CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106, CWA 2108)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio (CWA2012, CWA2010, and CWA2112)	Not supported	Not supported
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.

Table 100. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.5067 with CWA 2112	Limitations
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

New and enhanced features

Citrix Workspace app updates

Citrix Workspace app package is updated to version 21.12.0.18.2. This package is intended for users who want to install the Citrix Workspace app version 2112 on ThinOS.

Invert cursor color

From Citrix Workspace app 2112 and ThinOS 9.1.5067, the cursor color can be inverted based on the background color of a text. As a result, you can easily locate the position of the cursor in between texts. By default, this feature is disabled. To enable cursor color inverting feature, do the following:

Steps

1. On 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 `Thinwire3.0`.
6. In the **Key** field, enter `InvertCursorEnabled`.
7. In the **Value** field, enter `True`.
8. Sign out or restart the device for the settings to take effect.

   NOTE: If you have enabled the cursor color inverting feature, the **Cursor Pattern** setting from **Advanced** > **Session Settings** > **Citrix Session Settings** in the Admin Policy Tool or Wyse Management Suite policy settings is deprecated.

Limitations for inverting cursor color

Sometimes the cursor color inverting feature does not work after you upgrade or downgrade the Citrix Workspace app package. Workaround is to remove the cursor setting from **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor** and then configure the cursor pattern setting from **Advanced** > **Session Settings** > **Citrix Session Settings** in Admin Policy Tool or Wyse Management Suite policy settings. This issue is planned to be resolved in a future release.

Adaptive audio enhancement

From Citrix Workspace app 2112 and ThinOS 9.1.5067, Adaptive audio works while using User Datagram Protocol (UDP) audio delivery. Adaptive audio is enabled by default. This feature requires VDA version 2112 or later versions. For more information, see the *Citrix Virtual Apps and Desktops* product documentation at www.docs.citrix.com.

UDP audio through Citrix Gateway

From Citrix Workspace app 2112 and ThinOS 9.1.5067, Citrix Workspace app supports Datagram Transport Layer Security (DTLS) protocol for UDP audio. As a result, you can access the UDP audio through Citrix Gateway. By default, this feature is disabled.

Enable UDP audio through Citrix Gateway feature

Prerequisites

Ensure that UDP audio is enabled in ThinOS. To configure the settings, do the following:

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **Session Settings** > **Citrix Session Settings**.
2. Select the **Enable UDP audio** check box.
3. Select **Audio quality** as **Medium**. Ensure that Citrix Audio quality policy is High or Medium in Citrix Studio.
4. Sign off from the session and the broker for the changes to take effect.

Steps

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

Disable UDP audio through Citrix Gateway feature

Steps

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **Session Settings** > **Citrix Session Settings**.
2. Clear the **Enable UDP audio** check box.
3. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
4. Remove the **`EnableUDPThroughGateway`** setting.
5. Sign out or restart the device for the settings to take effect.

Smart card reader enhancement

From Citrix Workspace app 2112 and ThinOS 9.1.5067, Citrix Workspace app supports plug and play functionality for smart card reader. When you insert a smart card, the smart card reader detects the smart card in the server and the client. You can plug and play multiple cards simultaneously, and all these cards are detected. This feature is enabled by default.

Disable smart card plug and play

Steps

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

5. In the **Section** field, enter `SmartCard`.
6. In the **Key** field, enter `DriverName`.
7. In the **Value** field, enter `VDSCARD.DLL`.
8. Sign out or restart the device for the settings to take effect.

Smart card reader limitations

This feature is sometimes disabled after you upgrade or downgrade the Citrix Workspace app package. **DriverName** in smartcard settings under **module.ini** is changed from **VDSCARDV2.DLL** to **VDSCARD.DLL**. This issue is planned to be resolved in a future release.

As a workaround, do the following:

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In the Citrix INI Settings, click **Add Row**.
3. From the **File** drop-down list, select **module.ini**.
4. From the **Operation** drop-down list, select **Add or Update**.
5. In the **Section** field, enter `SmartCard`.
6. In the **Key** field, enter `DriverName`.
7. In the **Value** field, enter `VDSCARDV2.DLL`.
8. Sign out or restart the device for the settings to take effect.

Battery status indicator enhancement

From Citrix Workspace app 2112 and ThinOS 9.1.5067, the battery status indicator is displayed in the notification area for server VDAs. This feature is enabled by default.

Microsoft Teams update

From Citrix Workspace app 2112 and ThinOS 9.1.5067, Microsoft Teams optimization supports echo cancellation. The echo cancellation option for Microsoft Teams is disabled by default.

Enable echo cancellation for Microsoft Teams

Steps

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 `EnableAEC`.
6. In the **Value** field, enter `1`.
7. In the Citrix JSON Settings, click **Add Row** to add the second setting.
8. From the **File** drop-down list, select **hdx_rtc_engine/config.json**.
9. From the **Operation** drop-down list, select **Add or Update**.
10. In the **Key** field, enter `EnableACC`.
11. In the **Value** field, enter `1`.
12. In the Citrix JSON Settings, click **Add Row** to add the third setting.
13. From the **File** drop-down list, select **hdx_rtc_engine/config.json**.
14. From the **Operation** drop-down list, select **Add or Update**.
15. In the **Key** field, enter `EnableNS`.
16. In the **Value** field, enter `1`.

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

Citrix Workspace app limitations

- In Citrix Workspace app 2112, 32-bit apps with HDX webcam redirection are only supported using inbuilt camera. Only the default video resolution is qualified yet by Dell Technologies. External camera does not work with 32-bit apps using HDX webcam redirection. The issue is also observed in Linux binary.
- The following new features from Citrix Workspace app 2111 and Citrix Workspace app 2112 are not supported:
    - Multiple audio devices
    - Request control in Microsoft Teams
    - Webcam redirection for 64-bit (Technical Preview)
    - Custom web stores (Technical Preview)
    - Workspace with intelligence (Technical Preview

VMware Horizon updates

VMware Horizon package is updated to version 2111.8.4.0.18957622.3.

VMware Horizon limitations:

- The following new features of VMware Horizon client for Linux 2111 are not supported on ThinOS:
    - Client settings that take effect in individual desktops is not supported.
    - Configuration option for Blast decoder cache is not supported.
- VMware Horizon blast does not support serial port in this package release due to a known issue.

Cisco WebEx Meetings VDI updates

- Cisco WebEx Meetings VDI application package is updated to version 41.12.6.12.1.
- From this release, registration and invitations in Webex Meetings and Webex Events can be managed by cohosts. Cohosts can import or invite attendees and event panelist. Cohosts can also approve or reject registrants.
- Fixed the issue where the audio can still be heard after ending a call from the taskbar.
- Supports optimization mode through HTTP proxy server with username and password authentication.

Cisco WebEx Meetings VDI feature matrix

Table 101. Cisco WebEx Meetings VDI feature matrix

Scenarios	ThinOS 9.1.5067
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported

Table 101. Cisco WebEx Meetings VDI feature matrix (continued)

Scenarios	ThinOS 9.1.5067
Change speaker device	Supported
Mute by myself	Supported
Unmute	Supported
Lock meeting	Supported
Return meeting	Supported
Hotplug the headset	Supported
Plug out headset	Supported
Plug out headset and plug in new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Polls	Supported
Q & A—Participants ask Questions to Host	Supported
Chat—to everyone	Supported
Chat—to specified participants	Supported
Screen sharing—If 1 monitor connected	Supported
Screen sharing—If multiple monitors connected	Supported
Screen sharing—Whiteboard	Supported
Screen sharing—Share one of the applications	Supported
Screen sharing—Switch share content	Supported
Screen sharing—Annotates	Supported
Screen sharing—Pause or Resume	Supported
Screen sharing—View—full screen	Supported
Screen sharing—View—Zoom in, out, or to	Supported
Screen sharing—Start or stop video during screen sharing	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Breakout sessions	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop screen sharing	Supported
Make Host or Cohost other Participants	Supported
Participant	Supported
Close Participant	Supported
Invite and Remind	Supported
Layout Grid, Stack, Side by Side, or Full-screen view, Names in Video—Automatically Hide names when not Speaking, Show all names, Hide all names, Show participants without video, and Increase or Decrease Video size	Supported
Virtual Background or Blur image	Not supported

Cisco WebEx Meetings VDI limitation

Cisco WebEx Meeting 41.12 is not optimized for Horizon 2111 and it is a Cisco WebEx limitation. Optimization may work in rare occasions.

Cisco WebEx VDI updates

- Cisco WebEx VDI application package is updated to version 41.12.0.20899.1.
- Supports EPOS headset—Dell Technologies has tested only the models EPOS IMPACT MB Pro 2 UC ML and EPOS ADAPT 660.
- If you move around while on a Webex call, the network is changed automatically without any call quality effect or interruption to the call.
- End-to-end encrypted meetings can now be scheduled from the Webex scheduler. You can use the Webex app to join or start an end-to-end encrypted Webex meeting. In the Meeting info and during the meeting, an indicator is displayed to notify the participants that the meeting is encrypted.
- Supports optimization mode through HTTP proxy server with username and password authentication.

Cisco WebEx VDI feature matrix

Table 102. Cisco WebEx VDI feature matrix

Scenarios	ThinOS 9.1.5067
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by myself	Supported
Unmute	Supported
Hotplug the headset	Supported
Plug out headset	Supported
Plug out headset and plug in new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—to everyone	Supported

Table 102. Cisco WebEx VDI feature matrix (continued)

Scenarios	ThinOS 9.1.5067
Chat—to specified participants	Supported
Screen sharing—If 1 monitor connected	Supported
Screen sharing—If multiple monitors connected	Supported
Screen sharing—Whiteboard	Supported
Screen sharing—Pause or Resume	Supported
Screen sharing—View—full screen	Supported
Screen sharing—View—Zoom in, out, or to	Supported
Screen sharing—Start or stop video during screen sharing	Supported
Screen sharing—Annotates	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop screen sharing	Supported
Participant	Supported
Close Participant	Supported
Invite to Meeting only and invite through Meeting link	Supported
Layout Grid, Stack, Side by Side, or Full-screen view and Automatically hide names	Supported
Virtual Background or Blur image	Not supported

Zoom application package updates

- Zoom Citrix application package is updated to version 5.8.4.21112.1.
- Zoom Horizon application package is updated to version 5.8.4.21112.1.
- Virtual background support is added from this release.

Zoom application package feature matrix

Table 103. Zoom application package feature matrix

Scenarios	ThinOS 9.1.5067
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported

Table 103. Zoom application package feature matrix (continued)

Scenarios	ThinOS 9.1.5067
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Hotplug the headset	Supported
Plug out headset	Supported
Plug out headset and plug in new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—to everyone	Supported
Chat—to specified participants	Supported
Screen sharing—If 1 monitor connected	Supported
Screen sharing—If multiple monitors connected	Supported
Screen sharing—Whiteboard	Supported
Screen sharing—Pause or Resume	Supported
Screen sharing—View—full screen	Supported
Screen sharing—View—Zoom in, out or to	Supported
Screen sharing—Start or stop video while screen sharing	Supported
Screen sharing—Annotates	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop screen sharing	Supported
Participant	Supported
Close Participant	Supported
Invite to Meeting only and invite through Meeting link	Supported
Layout Grid, Stack, Side by Side, or Full-screen view and Automatically hide names	Supported
Virtual Background or Blur image	Not supported

Zoom application package limitations

- Zoom application package version 5.8.4 supports HID button for only answering a call. HID button cannot be used to end a call.
- Zoom application performance is low on clients or VDI with 2 cores. Use a client or VDI with 4 cores to avoid performance issues.

Tested environments matrix

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

Table 104. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.5
Imprivata OneSign	7.6
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 105. Test environment—Citrix

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

Table 106. Tested environment—VMware Horizon

VMware Horizon	Windows 10	Windows Server 2016	Windows Server 2019	APPs
VMware Horizon 2111	Tested	Tested	Tested	Tested

Table 107. Tested environment—Skype for Business

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

Table 108. Tested environment—Skype for Business

VMware VDI	Operating system	Skype for Business client	Skype for Business Server
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	Skype for Business 2016	Skype for Business 2015
	Windows server 2016	Skype for Business 2016	Skype for Business 2015
	Windows server 2019	Not tested	Not tested

Table 109. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	14.0.2	14.0.2	14.0.2
	Windows server 2016			
	Windows server 2019			

Table 110. Tested environment—JVDI

VMware VDI	Operating system	JVDI	JVDI agent	Jabber software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	14.0.2	14.0.2	14.0.2
	Windows server 2016	14.0.2	14.0.2	14.0.2
	Windows server 2019	Not tested	Not tested	Not tested

Table 111. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	5.8.4.21112_1	5.8.4.21112
	Windows server 2016		
	Windows server 2019		

Table 112. Tested environment—Zoom

VMware VDI	Operating system	Zoom package	Zoom software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	5.8.4.21112_1	5.8.4.21112
	Windows server 2016	5.8.4.21112_1	5.8.4.21112
	Windows server 2019	Not tested	Not tested

Table 113. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	41.12.0.20899_1	41.12.0.20899
	Windows server 2016		
	Windows server 2019		

Table 114. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2106 VMware Horizon 2111	Windows 10	41.12.0.20899_1	41.12.0.20899
	Windows server 2016	41.12.0.20899_1	41.12.0.20899
	Windows server 2019	Not tested	Not tested

Table 115. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2112	Windows 10	41.12.6.12_1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.12 to 42.4.
	Windows server 2016		
	Windows server 2019		

Table 116. Tested environment—Cisco Webex Meetings

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2106	Windows 10	41.12.6.12_1	The supported compatible version of Webex Meetings
	Windows server 2016		

Table 116. Tested environment—Cisco Webex Meetings (continued)

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
	Windows server 2019		app on the hosted virtual desktop is from 41.12 to 42.4.

Known issues

Table 117. Known issues

Issue ID	Description	Workaround
DTOS-6296	Serial redirection does not work in VMware Horizon Blast	There is no workaround in this release.
DTOS-6386	During a Citrix session, if you enable multiple audio and open the **Recording** tab from the **Sound** window, the session gets disconnected. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Do not open **Sound** > **Recording**. You cannot switch the recording device in Windows Sound settings.
DTOS-6426	There is no audio on the videos played using Multimedia redirection. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Go to **Peripherals** > **Audio** on the client and click **OK**. The audio will resume playing.
DTOS-6757	A green shadow is visible on the session window when a video is played locally using VLC player. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Close and reopen the video.
DTOS-6645	Sometimes, during an ICA session launch or disconnection, an error message is displayed due to a missing **./ICAClient/ appsrv.ini** file. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Uninstall and reinstall the Citrix Workspace app package.
DTOS-6026	If you connect a second camera to the client during an RTME video call, the thin client restarts. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	There is no workaround in this release.
DTOS-6363	Smartcard is not detected after you disconnect a broker session that was logged in using a smartcard. The issue occurs when thin client resumes from sleep mode. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Workaround is to force restart the thin client.
DTOS-5639	CPU utilization reaches 100% during a WebEx Teams VDI call. This issue is observed on Wyse 5470 thin clients.	There is no workaround in this release.
DTOS-6741	The default audio input and output device does not change when you change the default audio device from the application in a session. The default device that is selected on the client is used for audio input and output. The issue occurs when multiple audio is enabled. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Disable multiple audio.
DTOS-6341	**DriverName** in smartcard settings is changed from **VDSCARDV2.DLL** to **VDSCARD.DLL** when you connect to Wyse Management Suite or when you remove the smartcard settings from VDI settings. This issue is observed on Wyse 5470 All-in-One devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Either reset the client to factory settings or manually configure **VDSCARDV2.DLL/VDSCARD.DLL** in Admin policy Tool/Wyse Management Suite policy settings.
DTOS-6028	Inverting the cursor color in Citrix does not work. This issue is observed on devices that run ThinOS version 9.1.5067 with Citrix Workspace app version 2112.	Remove the cursor setting from **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor** and then configure the cursor pattern setting from **Advanced** > **Session Settings** >

Table 117. Known issues (continued)

Issue ID	Description	Workaround
		Citrix Session Settings in Admin Policy Tool or Wyse Management Suite policy settings.
DTOS-6775	If you enable multiple audio and play online videos or sounds, always the inbuilt audio device of the thin client is used. The issue is observed in Windows server 2016 or 2019 VDA.	Disable multiple audio. The audio will resume playing from the audio device that the user selects.

Cisco WebEx Meetings VDI 41.10, Cisco WebEx VDI 41.10, Citrix Workspace app 2109, and HID fingerprint reader 210217_11 packages for ThinOS

Release summary

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

Version

Citrix_Workspace_App_21.9.0.25_1 .pkg

Cisco_WebEx_Meetings_VDI_41.10.3.19_1.pkg

Cisco_WebEx_VDI_41.10.0.20213_1.pkg (formerly Cisco WebEx Teams)

HID_Fingerprint_Reader_210217_11.pkg

Release date

November 2021

Supported platforms

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client

Important notes

- Upgrade the ThinOS firmware to 9.1.4234 before you install the application packages.

  ⓘ **NOTE:** Citrix session gets disconnected if **Adaptive Audio** is enabled when you connect to a VDI desktop that runs on Citrix VDA 2109. You must disable **Adaptive Audio** function to connect to Citrix VDA 2109 desktop. This issue is also observed in the Citrix Workspace app Linux binary. For more information, see Citrix Workspace app updates.
- Cisco WebEx Meetings VDI and Cisco WebEx VDI are qualified for Citrix VDI on ThinOS 9.1.4234 with Citrix Workspace app package 21.9.0.25.1.
- Cisco WebEx Meetings VDI and Cisco WebEx VDI are qualified for VMware Blast VDI on ThinOS 9.1.4234 with VMware Horizon package 2106.8.3.0.18251983_5.

Installing the application package

Download the application packages

Steps

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

Install the application package using Wyse Management Suite

Prerequisites

- Upgrade the ThinOS firmware to 9.1.4234 before you install the application package.
- The thin client must be registered to Wyse Management Suite.
- Create a group in Wyse Management Suite with a group token.

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

Steps

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

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

Compatibility

Application package information

- Supported ThinOS application packages—The following ThinOS packages are qualified by Dell Technologies.
  - Citrix_Workspace_App_21.9.0.25_1 .pkg
  - Cisco_WebEx_Meetings_VDI_41.10.3.19_1.pkg
  - Cisco_WebEx_VDI_41.10.0.20213_1.pkg (formerly Cisco WebEx Teams)
  - HID_Fingerprint_Reader_210217_11.pkg
- Supported Firmware—ThinOS version 9.1.4234.

ⓘ **NOTE:** For information about other packages, see ThinOS application package details in the **ThinOS 9.1.4234 Release Notes**.

Previous versions

- Citrix_Workspace_App_21.6.0.28_10.pkg
- Cisco_WebEx_Meetings_VDI_41.6.1.10_2.pkg
- Cisco_WebEx_VDI_41.6.1.19187_1.pkg (formerly Cisco WebEx Teams)
- HID_Fingerprint_Reader_210217_10.pkg

Citrix Workspace app feature matrix

Table 118. Citrix Workspace app feature matrix

Feature		ThinOS 9.1.4234 with CWA 2109	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	Citrix session gets disconnected if **Adaptive Audio** is enabled when you connect to a VDI desktop that runs on Citrix VDA 2109. You must disable **Adaptive Audio** function to connect to Citrix VDA 2109 desktop.
	Citrix Content Collaboration (Citrix Files)	N/A	N/A
	Citrix Access Control Service	N/A	N/A
	Citrix Workspace Browser	N/A	N/A
	SaaS/Webapps with SSO	Not supported	Not supported
	Citrix Mobile Apps	N/A	N/A
	Intelligent Workspace features	N/A	N/A
Endpoint Management	Auto configure using DNS for Email Discovery	Supported	There are no limitations in this release.
	Centralized Management Settings	Supported	There are no limitations in this release.
	App Store Updates/Citrix Auto updates	N/A	N/A
UI	Desktop Viewer/Toolbar	Supported	There are no limitations in this release.
	Multi-tasking	Supported	There are no limitations in this release.
	Follow Me Sessions (Workspace Control)	Supported	There are no limitations in this release.
HDX Host Core	Adaptive transport	Supported	There are no limitations in this release.
	Session reliability	Supported	There are no limitations in this release.

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	Auto-client Reconnect	Supported	There are no limitations in this release.
	Bi-directional Content redirection	N/A	N/A
	URL redirection	N/A	N/A
	File open in Citrix Workspace app	N/A	N/A
	Browser content redirection	Limited support	Browser Content Redirection (BCR) with CEF is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.
	Multiport ICA	Supported	There are no limitations in this release.
	Multistream ICA	Not supported	Not supported
	SDWAN support	Not supported	Not supported
HDX IO/Devices/Printing	Local Printing	Supported	There are no limitations in this release.
	Generic USB Redirection	Supported	There are no limitations in this release.
	Client drive mapping/File Transfer	Supported	There are no limitations in this release.
HDX Integration	Local App Access	N/A	N/A
	Multi-touch	N/A	N/A
	Mobility pack	N/A	N/A
	HDX Insight	Supported	There are no limitations in this release.
	HDX Insight with NSAP VC	Supported	There are no limitations in this release.
	EUEM Experience Matrix	Supported	There are no limitations in this release.
	Session Sharing	Supported	There are no limitations in this release.
HDX Multi-media	Audio Playback	Supported	There are no limitations in this release.
	Bi-directional Audio (VoIP)	Supported	There are no limitations in this release.
	Webcam redirection	Supported	Webcam redirection works for 32-bit applications. For example, Skype and GoToMeeting. You can use a 32-bit browser to verify webcam redirection online. For example, www.webcamtests.com. This is Citrix binary design.

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	Video playback	Supported	There are no limitations in this release.
	Flash redirection	N/A	N/A
	Microsoft Teams Optimization	Supported	Supports Microsoft Teams optimization through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. This is a Citrix binary design. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Skype for business Optimization pack	Supported	Not supported through proxy server.
	Cisco Jabber Unified Communications Optimization	Supported	For information about limitations, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Unified Communication Zoom Cloud Meeting Optimization	Supported	Support Zoom optimization via HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Unified Communication Cisco Webex Teams Offloading (tVDI)	Supported	Supports Webex Teams optimization mode through HTTP proxy server which is configured in ThinOS Network Proxy by APT/ Wyse Management Suite. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	Unified Communication Cisco Webex Meetings Offloading (wVDI)	Supported	Dell Technologies recommends to wait for 10s to join a second meeting after you end the first meeting. Otherwise, VDI mode may not work. Supports Webex Meetings optimization mode through HTTP proxy server with anonymous authentication. It does not support the proxy configured by DHCP Option 252 or the proxy server configured with non-anonymous authentication. For more information, see the Dell Wyse ThinOS Version 9.1.4234 Administrator's Guide at www.dell.com/support.
	Windows Multimedia redirection	Supported	There are no limitations in this release.
	UDP Audio	Supported (not with NetScaler Gateway)	Limited support—Not supported with Citrix ADC (formerly NetScaler) due to Citrix's limitation.
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	There are no limitations in this release.
	True Multi Monitor	Supported	There are no limitations in this release.
	Desktop Composition redirection	N/A	N/A
	Location Based Services (Location available via API-description	N/A	N/A
Authentication	Federated Authentication (SAML/Azure AD)	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	RSA Soft Token	Supported	There are no limitations in this release.
	Challenge Response SMS (Radius)	Supported	There are no limitations in this release.
	OKTA Multi factor authentication	Limited supported (only supports Radius)	Does not support OKTA SAML authentication.

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	DUO multi factor authentication	Supported	There are no limitations in this release.
	Smart cards (CAC, PIV etc)	Supported	There are no limitations in this release.
	User Cert Auth via NetScaler Gateway (via Browser Only)	N/A	N/A
	Proximity/Contactless Card	Supported	There are no limitations in this release.
	Credential insertion (For example, Fast Connect, Storebrowse)	Supported	There are no limitations in this release.
	Pass Through Authentication	Supported	There are no limitations in this release.
	Save credentials (on-premise and only SF)	N/A	N/A
	NetScaler nFactor Authentication	Not supported	Not supported
	NetScaler Full VPN	Not supported	Not supported
	Netscaler Native OTP	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Biometric Authentication such as Touch ID and Face ID	Supported (only supports Touch ID)	Only supports Touch ID.
	Single Sign-On to Citrix Files App	N/A	N/A
	Single Sign on to Citrix Mobile apps	N/A	N/A
	Anonymous Store Access	Supported	There are no limitations in this release.
	Netscaler + RSA	Not supported	Not supported
	Netsclaer + Client cert authentication	Not supported	Not supported
	Citrix cloud + Azure Active Directory	Not supported	Not supported
	Citrix cloud + Active Directory + Token	Not supported	Not supported
	Citrix cloud + Citrix Gateway	Not supported	Not supported
	Citrix cloud + Okta	Not supported	Not supported
	Citrix cloud + SAML 2.0	Not supported	Not supported
	Netscaler load balance	Not supported	Not supported
Security	TLS 1.2	Supported	There are no limitations in this release.

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	TLS 1.0/1.1	Not supported	Not supported
	DTLS 1.0	Supported	There are no limitations in this release.
	DTLS 1.2	Not supported	Not supported
	SHA2 Cert	Supported	There are no limitations in this release.
	Smart Access	Not supported	Not supported
	Remote Access via Citrix Gateway	Supported	Does not support lock terminal when logging on Netscaler with web-based authentication such as OTP and Azure SAML SSO.
	Workspace for Web Access	N/A	N/A
	IPV6	Not supported	Not supported
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA	Supported	There are no limitations in this release.
	Unicode Keyboard Layout Mapping with Windows VDA	Supported	There are no limitations in this release.
	Client IME Enhancements with Windows VDA	N/A	N/A
	Language Bar Show/Hide with Windows VDA Applications	N/A	N/A
	Option Key mapping for server-side IME input mode on Windows VDA	N/A	N/A
	Dynamic Keyboard Layout Synchronization with Linux VDA	Not supported	Not supported
	Client IME Enhancements with Linux VDA	N/A	N/A
	Language Bar support for Linux VDA Applications	Not supported	Not supported
	Keyboard sync only when a session is launched—client Setting in ThinOS	Supported	There are no limitations in this release.
	Server default setting in ThinOS	Supported	There are no limitations in this release.
	Specific keyboard in ThinOS	Supported	There are no limitations in this release.
New features listed in Citrix Workspace App release notes but not in feature matrix	Session reliability enhancement (CWA2109)	Supported	There are no limitations in this release
	Enhancement to logging (CWA2109)	Not Supported	Not supported
	Adaptive audio (CWA2109)	Not Supported	Not supported

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	Storebrowse enhancement for service continuity(CWA2109)	Not Supported	Not supported
	Global App Config Service (Public Technical Preview) (CWA2109)	Not Supported	Not supported
	EDT MTU discovery (CWA2109)	To be verified	This feature is not verified yet in ThinOS.
	Creating custom user-agent strings in network request (CWA2109)	Not Supported	Not supported
	Feature flag management (CWA2109)	Not Supported	Not supported
	Battery status indicator (CWA2106)	Supported	There are no limitations in this release.
	Service continuity (Technical Preview) (CWA2104, CWA2106)	Not supported	Not supported
	Pinning multi-monitor screen layout (CWA2103)	Not supported	Not supported
	App Protection (CWA2101, CWA2106)	Not supported	Not supported
	Authentication enhancement is available only in cloud deployments (CWA2012)	Not supported	Not supported
	Multiple audio (CWA2012 and CWA2010)	Not supported	Not supported
	Citrix logging (CWA2009)	Supported	There are no limitations in this release.
	Cryptographic update (CWA2006)	Not supported	Not supported
	Transparent user interface (TUI) (CWA1912 and CWA1910)	Not supported	Not supported
	GStreamer 1.x supportexperimental feature(CWA1912)	Supported	There are no limitations in this release.
	App indicator icon (CWA1910)	Not supported	Not supported
	Latest webkit support (CWA1908 and CWA1906)	Supported	There are no limitations in this release.
	Bloomberg audio redirection (CWA1903)	Supported	There are no limitations in this release.
	Bloomberg v4 keyboard selective redirection support(CWA1808)	Supported	There are no limitations in this release.
ThinOS VDI configuration	Broker Setting	Supported	There are no limitations in this release.

Table 118. Citrix Workspace app feature matrix (continued)

Feature		ThinOS 9.1.4234 with CWA 2109	Limitations
	PNA button menu	Supported	There are no limitations in this release.
	Sign on window function	Supported	There are no limitations in this release.
	Workspace mode	Supported	There are no limitations in this release.
	Admin policy tool	Supported	There are no limitations in this release.

New and enhanced features

Citrix Workspace app updates

- Citrix Workspace app package version is updated to 21.9.0.25.1. This package is intended for users who want to install the Citrix Workspace app version 2109 on ThinOS.
- HDX RealTime Media Engine (RTME) within the Citrix Workspace app 2109 package is updated to version 2.9.400.
- Session reliability enhancement—The screen changes when session reliability begins. The session window is disabled and a countdown timer with the time until the next reconnection attempt is displayed.

  NOTE: This feature is only supported on Citrix Virtual Desktops. For more information, see the Citrix documentation at docs.citrix.com.
- Update the HID fingerprint reader to fix the issue where the ICA session does not launch after you upgrade **Citrix Workspace app version 2106** to **version 2109** or if you uninstall and reinstall **Citrix Workspace app version 2109**. See, HID fingerprint reader updates.

Citrix Workspace app limitations and known issues

- **Keyboard Layout Mode = Server Default** in CWA2109 is not working. This issue is also observed in the Citrix Workspace app Linux binary.
- Battery status does not appear on a desktop session that is launched from Wyse 5470 Thin Client. This issue is also observed in the Citrix Workspace app Linux binary.
- Citrix session gets disconnected if **Adaptive Audio** is enabled when you connect to a VDI desktop that runs on Citrix VDA 2109. You must disable Adaptive Audio function to connect to Citrix VDA 2109 desktop.
  - If you are using Desktop Delivery Controller (DDC) version 2109, you can find the **Adaptive Audio** policy, and disable it using the policy settings.
  - If you are using DDC version 1912, change the registry value of **REG_DWORD EnableAdaptiveAudio** to **0** in the following registry paths:
    - Desktop VDA (Windows 10)—**HKLM\Software\Citrix\Audio**
    - Server VDA (Server 2016\2019)—**HKLM\Software\WOW6432Node\Citrix\Audio**
- Users are not able to share screen while using Microsoft Teams in Citrix VDA 2109 with Citrix Workspace app 2106 for Linux.
- The following new features from Citrix Workspace app 2108 and Citrix Workspace app 2109 are not supported:
  - Enhancement to logging—ThinOS does not provide the collectlog.py tool that lets you collect the log files from different folders.
  - Service continuity
  - Support for Service continuity with Citrix Workspace Web Extension for Google Chrome
  - Storebrowse enhancement for service continuity
  - Global App Config Service (Public Technical Preview)
  - Creating custom user-agent strings in network request
  - Feature flag management
  - App protection—App protection component is not installed during Citrix Workspace app package installation in ThinOS. Hence, the App protection feature is not supported in ThinOS. If you continue to enable App protection for Citrix delivery group, you cannot see the published resources in thin client. This limitation is a known issue in ThinOS. In Citrix Workspace app for Linux, the published resources can be seen, however, if you try to launch protected resources, the client displays a warning message.

    - Adaptive audio—Citrix session gets disconnected if **Adaptive Audio** is enabled when you connect to a VDI desktop that runs on Citrix VDA 2109. You must disable **Adaptive Audio** function to connect to Citrix VDA 2109 desktop.
- EDT MTU discovery feature is not qualified by Dell Technologies—MTU Discovery is enabled by default. For more information, see the Citrix documentation at docs.citrix.com.

Cisco WebEx Meetings VDI updates

- Cisco WebEx Meetings VDI package version is updated to 41.10.3.19.1.
- Supports video optimization with WebEx Meetings VDI from this release.

Cisco WebEx Meetings optimization for VMware Horizon feature matrix

Table 119. Cisco Webex Meetings optimization feature matrix

Scenarios	**ThinOS 9.1.4234**
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported
Testing microphone	Supported
Testing speaker	Supported
End meeting	Supported
Leave meeting	Supported
Change microphone device	Supported
Change speaker device	Supported
Mute by self	Supported
Unmute	Supported
Lock meeting	Supported
Return meeting	Supported
Hotplug headset	Supported
Plug out headset	Supported
Plug out headset and plug in a new headset device	Supported
Disconnect network	Not tested
Disconnect desktop	Supported
Music mode	Supported
Polls	Supported
Chat—To everyone	Supported
Chat—To specified participants	Supported
Share screen—If 1 monitor is connected	Supported
Share screen—If multiple monitors are connected	Supported

Table 119. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 9.1.4234
Share screen—Whiteboard	Supported
Share screen—Share one of the applications	Supported
Share screen—Switch share content	Supported
Share screen—Annotate	Supported
Share screen—Pause or Resume	Supported
Share screen—View—Full screen	Supported
Share screen—View—Zoom in, out, or to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported
Participant	Supported
Close Participant	Supported

Cisco WebEx Meetings optimization for VMware Horizon limitations

- If you hot-plug the thin client, the thin client may stop responding during meetings.
- If you use the integrated microphone on the Wyse 5470 and Wyse 5470 All-in-One thin clients, there can be echo.
- The EagleEye mini camera does not work in WebEx Meetings.

HID fingerprint reader updates

HID Fingerprint Reader package is updated to 210217.11. This package resolves the issue where the ICA session does not launch after you upgrade **Citrix Workspace app version 2106** to **version 2109** or if you uninstall and reinstall **Citrix Workspace app version 2109**.

NOTE: Dell Technologies recommends that you disable **Enable HID Fingerprint Reader** before you upgrade the HID fingerprint reader package, and then enable it again after you upgrade the package. The HID fingerprint reader does not work in the ICA session without first disabling the **Enable HID Fingerprint Reader** option before you upgrade HID fingerprint reader package.

If the HID fingerprint reader does not work in the ICA session, disable **Enable HID Fingerprint Reader** from **Advanced** > **Session Settings** > **Global Session Settings** in the **Admin Policy Tool** or **Wyse Management Suite** policy settings, and save the setting changes. Enable the **Enable HID Fingerprint Reader** option again, before you log in to the Citrix server.

Cisco WebEx VDI update

Cisco WebEx VDI package version is updated to 41.10.0.20213.1.

Tested environments matrix

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

Table 120. Tested environment—General components

Component	Version
Wyse Management Suite (cloud and on-premises)	3.5
Imprivata OneSign	7.1.005.42
Citrix ADC (formerly NetScaler)	12.1/13.0
StoreFront	1912 LTSR and later versions

Table 121. Test environment—Citrix

Citrix Virtual Apps and Desktops	Windows 10	Windows Server 2016	Windows Server 2019	APPs
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Tested	Tested	Tested	Tested
Citrix Virtual Apps and Desktops 7 2109	Tested	Tested	Tested	Tested

Table 122. Tested environment—Skype for Business

Citrix VDI	Operating system	RTME Client	RTME Agent	Skype for Business client	Skype for Business Server
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	2.9.400	2.9.400	Skype for Business 2016	Skype for Business 2015
	Windows server 2016				
	Windows server 2019				

Table 123. Tested environment—JVDI

Citrix VDI	Operating system	JVDI	JVDI agent	Jabber software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	14.0.1	14.0.1	14.0.1
	Windows server 2016			
	Windows server 2019			

Table 124. Tested environment—Zoom

Citrix VDI	Operating system	Zoom package	Zoom software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	5.7.6.20822	5.7.6.20822
	Windows server 2016		
	Windows server 2019		

Table 125. Tested environment—Cisco Webex Teams

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3)	Windows 10	41.10.0.20213.1	41.10.0.20213
	Windows server 2016		

Table 125. Tested environment—Cisco Webex Teams (continued)

Citrix VDI	Operating system	Webex VDI	Webex Teams software
Citrix Virtual Apps and Desktops 7 2109	Windows server 2019		

Table 126. Tested environment—Cisco Webex Teams

VMware VDI	Operating system	Webex Teams	Webex Teams software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106	Windows 10	41.10.0.20213.1	41.10.0.20213
	Windows server 2016	41.10.0.20213.1	41.10.0.20213
	Windows server 2019	Not tested	Not tested

Table 127. Tested environment—Cisco Webex Meetings

Citrix VDI	Operating system	Webex Meetings VDI	Webex Meetings software
Citrix Virtual Apps and Desktops 7 1912 LTSR (CU3) Citrix Virtual Apps and Desktops 7 2109	Windows 10	41.10.3.19.1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.10 to 42.2.
	Windows server 2016		
	Windows server 2019		

Table 128. Tested environment—Cisco Webex Meetings

VMware VDI	Operating system	Webex Meetings VDI	Webex Meetings software
VMware Horizon 7.12 VMware Horizon 2103 VMware Horizon 2106	Windows 10	41.10.3.19.1	The supported compatible version of Webex Meetings app on the hosted virtual desktop is from 41.10 to 42.2.
	Windows server 2016		
	Windows server 2019		

Known issues

Table 129. Known issues

Issue ID	Description	Workaround
DTOS-5132	Published apps in **Auto Connect List** under **Broker Connections** do not connect when they are in log off status. The issue is observed on devices with Citrix Workspace app version 21.9.0.25.1.	Connect the apps by clicking them manually.
DTOS-5197	Sometimes the microphone does not work or there is echo from the audio during a video call on Skype for Business (no RTME). The issue is observed on Wyse 5070 Extended and Wyse 5470 All-in-One thin clients with Citrix Workspace app version 21.9.0.25.1.	Configure to RTME or only audio call.
DTOS-5198	When you log in to the Citrix Broker agent after connecting the VPN without adding a DNS address, an incorrect prompt message is displayed. The issue is observed on devices with Citrix Workspace app version 21.9.0.25.1.	There is no workaround in this release.
DTOS-5217	Camera is occupied by an unknown procedure after launching a session desktop. Other apps cannot use the camera unless you sign off and sign in to the desktop again. The issue is observed on devices with Citrix Workspace app version 21.9.0.25.1.	Disconnect or sign out and relaunch session.
DTOS-5153	Noise is observed when recording voice with analog or USB headset in VDI session on Wyse 5070 thin client. The issue is observed on Wyse 5070 Extended with Citrix Workspace app version 21.9.0.25.1.	There is no workaround in this release.

Table 129. Known issues (continued)

Issue ID	Description	Workaround
DTOS-5108	Graphics issue is observed during Webex Meeting calls and also while sharing screen. The issue is observed on Wyse 5070 Standard with Citrix Workspace app version 21.9.0.25.1.	There is no workaround in this release.
DTOS-5194	Background noise is observed even after selecting **Noise Removal** option during WebEx Teams call. The issue is observed on Wyse 5070 Standard and Wyse 5470 All-in-One thin clients with Citrix Workspace app version 21.9.0.25.1.	There is no workaround in this release.
DTOS-5205	Webex Meetings call does not end even after ending the Webex meetings process from Task Manager. The issue is observed on Wyse 5470 All-in-One with Citrix Workspace app version 21.9.0.25.1.	Log in to the session again, after closing the WebEx VDI through task manager.
DTOS-5196	After closing Webex teams apps in task manager, the audio from meeting is still audible. The issue is observed on devices with Citrix Workspace app version 21.9.0.25.1.	Log in to the session again, after closing the WebEx VDI through task manager.
DTOS-5166	If you disconnect the headset from the thin client, the audio from Microsoft Teams echoes. The issue is observed on Wyse 5070 and Wyse 5470 All-in-One thin clients with Citrix Workspace app version 21.9.0.25.1.	Do not disconnect or hotplug headsets. You must keep the headset connected.
DTOS-5224	Video distortion and lag in the video movement when Microsoft Teams window is dragged. The issue is observed on devices with Citrix Workspace app version 21.9.0.25.1.	This issue is only observed when the Microsoft teams window is dragged. There is no workaround in this release.
DTOS-5225	Unable to generate Attendee history report in Cisco Webex Meetings. The issue is observed on Wyse 5470 All-in-One with VMware Horizon 2106.8.3.0.18251983_5.	There is no workaround in this release.
DTOS-5227	Unable to check Highlights, Attendance, and Registration Reports in Event content. The issue is observed on Wyse 5470 All-in-One with VMware Horizon 2106.8.3.0.18251983_5.	There is no workaround in this release.
DTOS-5235	ICA session does not launch after you upgrade **Citrix Workspace app version 2106** to **version 2109** or if you uninstall and reinstall **Citrix Workspace app version 2109**.	Upgrade to the latest Citrix Workspace app and HID fingerprint packages. **Citrix_Workspace_App_21.9.0.25_1.pkg** and **HID_Fingerprint_Reader_210217_11.pkg**.
DTOS-4677	EagleEye mini Camera does not work in Cisco Webex Meetings optimized mode.	There is no workaround in this release.
DTOS-4355	The Horizon Blast session stops responding during Cisco WebEx Meetings call.	Relaunch Horizon Blast session.
DTOS-5334	HID fingerprint reader does not work after you upgrade the HID package.	Disable the **Enable HID Fingerprint Reader** option from **Advanced** > **Session Settings** > **Global Session Settings** in the **Admin Policy Tool** or **Wyse Management Suite** policy settings, and save the setting changes. Enable the **Enable HID Fingerprint Reader** option again, before you log in to the Citrix server.

9

Resources and support

Accessing documents using the product search

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, **`Wyse 3040 thin client`** or **`Wyse ThinOS`**.

   A list of matching products is displayed.
3. Select your product.
4. Click **Documentation**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to www.dell.com/support.
2. Click **Browse all products**.
3. Click **Thin Clients**.
4. Click the desired category, either **Wyse Hardware** or **Wyse Software**.
5. Click the desired product.
6. Click **Documentation**.

10

Contacting Dell

Prerequisites

ⓘ **NOTE:** If you do not have an active internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

About this task

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell sales, technical support, or customer service issues:

Steps

1. Go to www.dell.com/support.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.