Dell Wyse ThinOS

Version 9.1.4234 Operating System Release Notes

Notes, cautions, and warnings

(i) **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

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.

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 9.1.4234	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 version	Release date	Supported platforms	Release Notes
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

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

- 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 to 9.1.3129 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 3. 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.

(i) **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 4. 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 4. 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 4. 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 4. 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 4. 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 4. 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 4. 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 4. 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 5. 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 5. 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 5. 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 5. 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 5. 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 5. 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 6. 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 6. 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.

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.

(i) **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.

(i) **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.

Limitation

- 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.

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.

(i) **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**.

(i) **NOTE:** This feature is not supported on Wyse 3040 Thin Client.

Microsoft Teams optimization feature matrix

Table 7. 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 7. 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.

(i) **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 8. 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 8. 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.

Admin Policy Tool and Wyse Management Suite policy settings updates

- **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**
  - (i) **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**.
  - (i) **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 9. Tested environment—General components

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

Table 10. 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 11. 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 12. 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 13. 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 14. 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 15. 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 16. 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 Windows server 2016 Windows server 2019	14.0.1	14.0.1	14.0.1

Table 17. 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 18. 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 Windows server 2016 Windows server 2019	5.7.6.20822	5.7.6.20822

Table 19. 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 20. 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 Windows server 2016 Windows server 2019	41.6.1.19187	41.6.1.19162

Table 21. 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 22. 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 Windows server 2016 Windows server 2019	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.

Supported peripherals

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

Table 23. 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 23. 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 23. 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 23. 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 23. 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 23. 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 24. 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 24. 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 6.8.1.31, 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
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 25. 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 25. 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 25. 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 26. 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 26. 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.

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 is 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 is 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.
  - (i) **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**.
   - (i) **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.
- (i) **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 27. 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 27. 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 27. 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 27. 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 27. 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 27. 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 note 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 27. 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 27. 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.
  - (i) **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

- 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 registry path **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 is disabled by default in ThinOS. If you enable App protection for Citrix delivery group, you cannot see the published resources in thin client. This limitation is a known issue in ThinOS.
  - 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 28. 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
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

Table 28. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 9.1.4234
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**.

(i) **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 29. 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 30. 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 31. 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 Windows server 2016 Windows server 2019	2.9.400	2.9.400	Skype for Business 2016	Skype for Business 2015

Table 32. 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 Windows server 2016 Windows server 2019	14.0.1	14.0.1	14.0.1

Table 33. 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 Windows server 2016 Windows server 2019	5.7.6.20822	5.7.6.20822

Table 34. 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 Windows server 2016 Windows server 2019	41.10.0.20213.1	41.10.0.20213

Table 35. Tested environment—Cisco Webex Teams

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

Table 36. 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 Windows server 2016 Windows server 2019	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.

Table 37. 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 Windows server 2016 Windows server 2019	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.

Known issues

Table 38. 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.
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	Do not disconnect or hotplug headsets. You must keep the headset connected.

Table 38. Known issues (continued)

Issue ID	Description	Workaround
	Wyse 5470 All-in-One thin clients with Citrix Workspace app version 21.9.0.25.1.	
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.p kg**.
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.

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**.

6

Contacting Dell

Prerequisites

(i) **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.