Dell ThinOS 10.x

Administrator Guide

February 2026
Rev. A05

DELL Technologies

Notes, cautions, and warnings

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

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

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

Contents

1

Introduction

Thin clients running Dell ThinOS firmware are designed solely for optimal thin client security and performance. These efficient purpose-built thin clients offer ultrafast access to applications, files, and network resources within Virtual Desktop Infrastructure (VDI) environments. With zero attack surface, unpublished API, and encrypted data Dell ThinOS is virus and malware resistant.

Dell ThinOS requires a management software to configure, operate, and update thereby eliminating the need for IT support to browse or touch the physical devices. Dell Wyse Management Suite is the Next-Generation management solution that enables you to centrally configure, monitor, manage, and optimize your ThinOS-based thin clients. As the number of devices grows, the Wyse Management Suite offers process automation and helps lower costs for large deployments of thin clients. With secure HTTPS-based communications and active directory authentication for role-based administration, Wyse Management Suite keeps your thin clients always up to date. The mobile application enables IT to view critical alerts, notifications on the dashboard, and send real-time commands.

During the planning phase, the ThinOS 10.x Compatibility Checker plays a critical role. This tool runs on non-qualified devices to assess hardware compatibility with ThinOS. It generates a report that identifies any issues, enabling informed decision-making and reducing risk by validating hardware readiness before deployment.

This guide is intended for administrators of thin clients running Dell ThinOS and using Wyse Management Suite to manage thin clients. It provides information and detailed system configurations to help you design and manage a ThinOS environment using Wyse Management Suite.

Related Links:

Reference materials and supporting documentation

Hardware Compatibility List

The Hardware Compatibility List (HCL) identifies supported Dell and non-Dell hardware platforms for ThinOS 10.x and outlines tools that are used to verify compatibility.

ThinOS 10.x runs on validated Dell thin clients and select non-Dell commercial devices that meet minimum hardware and component requirements.

Compatibility is evaluated using the Hardware Compatibility List (HCL) and the ThinOS 10.x Compatibility Checker, which assess whether a device meets deployment requirements.

Platform support details:

- Validated Dell devices—Listed in ThinOS 10.x Hardware Compatibility List. For more information, see *ThinOS 10.x Hardware Compatibility List* document at Support | Dell.
- Dell devices not listed—Validation requests can be submitted through Dell Sales.
- Non-Dell Devices—Use the Compatibility Checker to confirm minimum requirements. For more information, see Dell ThinOS 10.x Compatibility Checker User Guide.

2

New and enhanced features in ThinOS 10.x

This chapter provides an overview of the new and enhanced features that are introduced in ThinOS 10.x. These updates deliver improvements in device compatibility, connectivity, user experience, security, configuration management, and system monitoring.

New and enhanced features in ThinOS 10.x 2602

Convert Windows 10 IoT Enterprise LTSC to ThinOS 10.x

ThinOS 10.x 2602 introduces seamless migration from Windows 10 IoT Enterprise LTSC environments to ThinOS 10.x. This enhancement simplifies device conversion workflows and streamlines deployment across large fleets.

For more information, see *Dell ThinOS 10.x Migration Guide* at Support | Dell.

Support for NVIDIA GPU on ThinOS 10.x

ThinOS 10.x adds support for NVIDIA GPUs, delivering enhanced graphics performance and extending compatibility for workloads that rely on hardware-accelerated rendering.

Enhancements:

- Added NVIDIA GPU support on supported platforms, including Dell Precision 3280 and Precision 3260, enabling multi-monitor configurations.
- Supports connecting up to four 4K displays, which is the recommended configuration for optimal user experience.
- NVIDIA support is powered by the Nouveau open-source driver, providing basic hardware-accelerated rendering for desktop and window management.

Usage considerations:

- Multi-monitor support enables desktop and window rendering; however, video playback across multiple monitors is not supported.
- This capability is designed for productivity and general desktop workloads, not high-performance graphics, gaming, or multimedia-intensive use cases.
- Due to driver limitations, refresh rates and frame rates may be limited to approximately 30 FPS, depending on the configuration.

Capture device screenshot using WMS

ThinOS 10.x adds support for requesting a screenshot remotely from the WMS **Device Details** page, enabling quick visual troubleshooting and device state verification.

For more information, see Capture device screenshot using WMS.

Support for Wi-Fi 7

ThinOS 10.x adds qualified support for Wi-Fi 7, offering faster wireless speeds, improved reliability, and lower latency for demanding network environments.

For more information, see Configure Wi-Fi 7 (6 GHz) connectivity .

Support for Dynamic Host file

ThinOS 10.x adds dynamic host file updates, allowing the system to modify host entries automatically and simplifying VDI session configuration similar to Citrix Configuration Editor.

For more information, see Configure Dynamic Host file settings.

App Builder enhancements

ThinOS 10.x adds the ability to auto-launch CI applications that is based on configurations set in WMS or APT.

Auto-launch CI applications:

- Applications that are configured in WMS or APT are automatically launched at startup or reboot.
- ThinOS uses the corresponding `.desktop` file to initiate the application during system initialization.

ThinOS 10.x introduces automated icon visibility management for CI applications.

Auto Icon visibility:

- When enabled in APT or WMS, CI application icons automatically appear in the VDI menu.
- When disabled, icons are hidden, ensuring UI behavior aligns with administrative policy.

For more information, see *Dell ThinOS 10.x App Builder User's Guide* at Support | Dell.

Support for new BIOS parameters

ThinOS 10.x adds support for Dell Command | Configure BIOS parameters into the BIOS Common Configuration section within WMS or APT, enabling administrators to remotely manage, modify, and enforce BIOS security and hardware settings directly from centralized management tools.

For more information, see Configure Dell Command | Configure BIOS parameters using WMS or APT.

BIOS password change using multiple passwords

ThinOS 10.x introduces enhanced Current Password support in WMS, enabling administrators to specify up to three possible existing BIOS passwords during a policy deployment.

This capability is designed for environments where devices within a WMS group may have inconsistent or unknown BIOS passwords. WMS automatically evaluates the provided password options, determines which one is valid for each device, and then applies the new unified BIOS password.

WWAN support

ThinOS 10.x adds support for Wireless WAN modules using Qualcomm Snapdragon chipsets, enabling administrators to configure WWAN so devices can connect to mobile networks with an active physical SIM card and establish reliable cellular connectivity.

For more information, see Configure WWAN using WMS or APT.

Enable or disable the Taskbar volume icon

ThinOS 10.x allows administrators to enable or disable local client volume icon centrally through APT or WMS policy configurations.

This change affects only the local device UI, audio functionality within VDI sessions and the browser remains unaffected.

For more information, see Enable or Disable the Taskbar volume icon using WMS or APT.

Improved P2P remote shadow connection times

ThinOS 10.x optimizes peer-to-peer remote shadowing, significantly reducing connection times and improving remote support responsiveness.

- Reduced P2P connection setup time from **40–60** seconds to **10–20** seconds, improving overall session startup speed.
- Improved responsiveness during remote session initiation for a smoother and faster user experience.
- Enhanced scalability and reliability of connection management to support higher session volumes and more stable connectivity.

Loading indicator for browser launch

ThinOS 10.x introduces a loading spinner when launching the browser or browser shortcuts, preventing users from unintentionally opening multiple duplicate tabs during initialization.

- Adds a visual loading spinner to indicate progress during browser launch.
- Provides a user-friendly status message confirming that the browser launch has started.
- Automatically dismisses the spinner once the browser window is fully ready.
- Enhances the overall user experience by offering clear launch feedback and reducing accidental multi-tab openings.

Support for recent Citrix sessions in WMS

ThinOS 10.x adds support for recent Citrix sessions visibility and desktops session names within the **Recent Sessions** section of WMS device details, improving session tracking and troubleshooting.

- Improves visibility and reduces ambiguity in environments where store names and desktop session names are similar.
- Simplifies troubleshooting by enabling administrators to trace the Citrix login path directly from WMS.

For more information, see View recent Citrix Sessions in WMS.

Custom background information fields for group policies

ThinOS 10.x adds support for custom fields in **Group Policies**, enabling granular control of background information to meet institutional or organizational requirements.

- Displays the current date and time directly on the **Desktop Background Information** panel, improving at-a-glance visibility.
- Eliminates the need to open the Start menu or check the taskbar to view system time.
- Provides real-time updates synchronized with the system clock.
- Switching between 12-hour and 24-hour formats requires a device reboot.

For more information, see Configure Background Info Settings using WMS or APT.

Support for Software TPM

ThinOS 10.x adds support to Software TPM (sTPM) on ThinOS 10 to ensure that Full Disk Encryption (FDE) and security features continue to operate reliably even when Hardware TPM (hTPM) is unavailable or cannot be accessed. As part of this enhancement:

- Software TPM is automatically used as a fallback when Hardware TPM is missing or fails to initialize.
- Encryption conversions continue to work even if the TPM is in a locked-out state.
- FDE protections and associated security functions remain fully enforced without any reduction in security posture.

Other enhancements

- Added support for the Tangent Medix 24 v3 as part of the Hardware Compatibility List (HCL) initiative, ensuring reliable ThinOS performance on certified medical-grade hardware.
- Added support for the Dell Ultrasharp 52 Thunderbolt monitor on compatible ThinOS 10.x devices, enabling seamless display integration and Thunderbolt connectivity.

For more information, see *Dell ThinOS 10.x 2602 Release Notes* at Support | Dell.

New and enhanced features in ThinOS 10.x 2511

ThinOS 10.x 2511 introduces a range of enhancements across device compatibility, user experience, security, configuration management, and system monitoring.

Improved subscription license management

ThinOS 10.x 2511 enhances subscription license workflows. Administrators can now:

- Unregister clients from WMS or directly from the device.
- Revoke subscription licenses from both the client and server.
- Use a check-in expiry period to reclaim unused license seats.

These improvements support better license utilization and more flexible device life-cycle management.

NOTE: When the ThinOS 10 subscription expires, the system enters a 30-day trial period during which subscription-based features remain available. During this time, a watermark appears on all VDI session windows, and a warning is displayed on the login screen until the license is renewed.

For more information, see the *ThinOS 10.x 2502, 2505, 2508, and 2511 Migration Guide* at Support | Dell.

WMS payload signing with SHA-512 and WDA Agent update

ThinOS 10.x 2511 introduces enhanced security for WMS communication by implementing two-way payload integrity checks. Request payloads are signed, and response payload signatures are validated using SHA-512 and AES encryption.

Policy-driven check-in enforcement

ThinOS 10.x 2511 introduces a mechanism to enforce WMS check-in compliance. Admins can configure a check-in interval in days. If a device exceeds this interval, a popup appears on the client screen and during VDI login, prompting the user to check in immediately, ensuring accountability and compliance.

For more information, see Configuring Policy-driven check-in enforcement.

Dynamic time zone configuration

ThinOS 10.x 2511 introduces automatic time zone detection using GeoIP. Devices can set their time zone based on geographic location, reducing the need for manual configuration and eliminating the need to maintain multiple policy groups.

For more information, see Configuring Dynamic time zone.

Custom browser User-Agent support

From ThinOS 10.x 2511, you can configure a custom Chrome browser User-Agent string in WMS. This allows compatibility with websites that restrict access based on browser identification, offering greater flexibility and control in web-based workflows.

For more information, see Configuring a Custom browser User-Agent .

Suppression of UI popups during Broker login

ThinOS 10.x 2511 introduces an enhanced login experience for AVD and Omnissa Workspace One by suppressing unnecessary UI popups. Integrated broker screens remain hidden when not in use, and UI elements do not appear during auto-launch scenarios, enabling seamless desktop access without extra prompts.

BIOS package listing based on platform

Starting with the ThinOS 2511 release, administrators now have improved flexibility in managing BIOS deployments across specific platforms. The user interface has been enhanced to clearly organize BIOS packages under their respective platform categories, making it easier to locate and apply the correct package.

If a platform cannot be identified, the associated BIOS package is automatically grouped under the **Others** category.

For more information, see Upgrade BIOS using WMS.

SSPR Imprivata password reset using ThinOS

From ThinOS 10.x 2511, the **Third-party Self-Service Password Reset** (SSPR) function is supported in both Imprivata PIW and PIE modes.

This feature allows ThinOS devices to use a third-party Self-Service Password Reset (SSPR) through Imprivata, enabling users to reset their passwords directly from the login screen.

For more information about how to reset SSPR Imprivata password on ThinOS devices using WMS, see the *ThinOS 10.x 2502, 2505, 2508, and 2511 Release Notes* at Support | Dell.

ControlUp VDI Agent update

From ThinOS 10.x 2511, the ControlUp monitoring agent capability is improved with the following features:

- Inactivity management—Tracks the ThinOS devices inactivity.
- Location support—Captures real-time country or region data.
- ISP Name—Gathers the ISP name from the network connection.
- Wi-Fi SSID—Collects the Wi-Fi SSID information.

Launch broker sessions from the browser using the local VDI client

From ThinOS 10.x 2511, it supports launching Omnissa Workspace ONE, Citrix StoreFront, and AVD sessions from the browser using the local VDI client.

For more information, see Launching broker sessions from the browser using the local VDI client.

Support for SSL certificates across all supported browsers

From ThinOS 10.x 2511, it supports for installing SSL certificates in the browser. You can upload and manage SSL certificates to ensure trusted connections. Uploaded certificates are recognized by supported browsers, eliminating trust errors and meeting enterprise security and compliance requirements.

For more information, see Uploading and managing custom SSL certificates for browser .

Other enhancements

- Removed the **Close** button from the **Connecting to WMS** popup to prevent interruption and ensure policy enforcement.
- Horizon Toolbar is now displayed when using Imprivata PIE, Imprivata PIW, or when Imprivata is not enabled.
- Improved inactivity timeout handling across Chrome and other applications.
- The **Notification** icon now displays the count of unread messages, showing 5+ when more than five notifications are pending.
- Enabled the fcd client package for ThinOS 10,x, allowing users to launch and manage virtual desktops hosted on FPT Cloud with simplified configuration, streamlined authentication, and optimized performance.

New and enhanced features in ThinOS 10.x 2508

ThinOS 10.x 2508 introduces a range of enhancements across device compatibility, user experience, security, configuration management, and system monitoring.

Enhanced Mode

Enhanced Mode is a privileged operating state that grants advanced system access, including the App Builder feature.

To enable Enhanced Mode, do any of the following:

- Log in to WMS as an administrator and select **Groups & Configs** > **<Select a group>** > **Edit Policies** > **ThinOS10.x** > **Advanced** > **Desktop Mode** > **System Operating Mode**, click **Enable Enhanced Mode**.
- Open APT on the device and select **Advanced** > **Desktop Mode** > **System Operating Mode**, click **Enable Enhanced Mode**.

For more information about Enhanced Mode, see *App Builder User's Guide* and *ThinOS 10.x 2502, 2505, and 2508 Administrator Guide* at Support | Dell.

App Builder

The App Builder allows you to create Customer Installed (CI) application packages using uploaded Binaries and Debian packages. These packages can be deployed to ThinOS devices using WMS or APT.

Customer installed (CI) applications can be installed and used only in **Enhanced Mode**, and are not supported in **Appliance Mode**.

To enable App Builder Mode, do any of the following:

- Log in to WMS as an administrator and select **Groups & Configs** > **<Select a group>** > **Edit Policies** > **ThinOS10.x** > **Advanced** > **Desktop Mode** > **System Operating Mode**, and enable **App Builder Mode**.
- Open APT on the device and select **Advanced** > **Desktop Mode** > **System Operating Mode**, and enable **App Builder Mode**.

For more information about creating and deploying application packages using App Builder on ThinOS devices, see *App Builder User's Guide* at Support | Dell.

ThinOS 10.x Compatibility Checker

ThinOS 10.x Compatibility Checker allows you to boot on a nonsupported device and run a compatibility check. This tool identifies if the current device is supported by ThinOS 10.x and provides a report on compatibility issues.

ThinOS 10.x Compatibility Checker is designed to evaluate whether your hardware is compatible for running ThinOS 10.x. It performs two types of checks to guide your installation decisions:

- **Mandatory checks**—Verify that the hardware meets the minimum requirements to install ThinOS 10.x.
- **Optional checks**—Provide additional insights into hardware capabilities, helping you decide whether to proceed or adjust the hardware setup.

NOTE: The Dell ThinOS 10.x image using USB installation performs the ThinOS 10.x Compatibility Checker before imaging to verify that the device meets the minimum hardware requirements. You must review the compatibility check report and validate converted devices in your environment before production deployment. For more information about the ThinOS 10.x Compatibility Checker, see Dell ThinOS 10.x Compatibility Checker User Guide.

NOTE: The ThinOS 10.x subscription license is not revocable or transferable through WMS.

For more information about compatibile Dell and non-Dell platforms, see *ThinOS 10.x Hardware Compatibility List* document at Support | Dell.

Exploring ThinOS 10 in Live Boot

The ThinOS 10.x Compatibility Checker supports a live boot option, which allows you to explore ThinOS 10.x and verify specific hardware and peripheral functionality before installation.

Converting IGEL OS to ThinOS 10.x

ThinOS 10.x 2508 supports converting IGEL OS to ThinOS 10.x, registering an IGEL device with **Universal Management Suite (UMS)**, using the **Scan for Devices** feature to automatically detect IGEL devices within the same subnet as the UMS server or within a specified IP range.

Alternatively, you can register the device using a **One-Time Password (OTP)** generated from the UMS console.

NOTE: It is recommended to run the ThinOS 10.x Compatibility Checker before converting an IGEL device. Intel x86 or x64 configurations are supported for conversion.

For more information about converting IGEL to ThinOS 10.x, see *ThinOS 10.x 2502, 2505, and 2508 Migration Guide* at Support | Dell.

DHC to ThinOS 10.x Config tool

DHC to ThinOS 10.x Config tool is a GUI-based feature that helps in migrating configuration settings from DHC to formats compatible with ThinOS 10.x.

For more information about exporting DHC policies using WMS, see *ThinOS 10.x 2502, 2505, and 2508 Migration Guide* at Support | Dell.

BIOS Common Configuration

ThinOS 10.x 2508 supports BIOS Common Configuration, which acts as a centralized settings page that consolidates all BIOS settings that are supported across all ThinOS 10.x devices. It enables users to view and configure BIOS settings ensuring standardized system configurations across the ThinOS 10.x using the same Active Directory in WMS.

To access the **BIOS Common Configuration** settings in WMS, go to **Advanced Settings** > **BIOS Common Configurations** > **Dell Supported Devices BIOS Settings**.

For more information about BIOS Common Configuration, see *ThinOS 10.x 2502, 2505, and 2508 Migration and Administrator Guide* at Support | Dell.

Support for 32 GB storage and 4 GB RAM

ThinOS 10.x 2508 expands compatibility to devices with 4 GB RAM and 32 GB flash, enabling support for both VDI and browser-based use cases.

The following are the key highlights:

- Enables real-time RAM monitoring on the client and continuously checks available free RAM.
- If available RAM drops below the defined threshold, users receive an alert to save any unsaved work and close unnecessary applications to avoid performance issues or data loss.
- Administrators can configure a minimum RAM threshold that must be met before launching new VDI or browser sessions.
- If RAM is below the threshold at launch, users are notified, and an alert is displayed on the WMS server.
- For CI applications, only low-memory notifications are supported (launch continues).
- During ThinOS 9.x to ThinOS 10.x upgrades, WMS displays a warning to administrators:
- Devices that are upgraded from ThinOS 9.x to 10.x, having less than the recommended RAM size (8 GB), may have few limitations.

For more information, see *ThinOS 10.x 2502, 2505, and 2508 Administrator Guide* at Support | Dell.

Other enhanced features

- Updated desktop icons for a refreshed user interface.
- Rebranded **VMware Horizon** to **Omnissa 2506 Horizon_ClientSDK** starting from ThinOS 10.x 2508.
- ThinOS 10.x 2508 now supports seamless upgrade and downgrade:
  - You can seamlessly upgrade and downgrade between ThinOS 10 N and ThinOS 10 N+1 versions, allowing smooth migration without manual steps or configuration changes through root OS package.
  - For downgrading to the previous version, use the required downgrade package.

New and enhanced features in ThinOS 10.x 2505

ThinOS 10.x 2505 introduces a range of enhancements across device compatibility, user experience, security, configuration management, and system monitoring.

Non-Dell device support

ThinOS 10.x 2505 now supports non-Dell devices, such as the Amulet Hotkey (DX1500 series). These deployments require ThinOS 10 Subscription – Third-Party Client licenses, visible in WMS with associated virtual Service Tags.

Routing proxy selection for Selected Host

Added the **Ignore Host** option to route proxy connections for selected hosts, configurable through WMS server.

The users must add a hostname in **Ignore Host** field under **Proxy Settings**.

Go to WMS and select **Groups & Configs** > **Select a group** > **Edit Policies** > **ThinOS10.x** > **Advanced** > **Network Configuration** > **Proxy Settings** > **Add Row** > **Ignore Host**.

Browser icon customization

Added ConfigUI option to hide default browser icons (Chrome/Firefox) from the menu bar, with customizable shortcuts. (By default, this option is enabled)

For Google Chrome - Go to **WMS** > **Group & Configs** > **Select a group** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Browser Settings** > **Google Chrome Settings** > **Privacy Settings** > **Hide Chrome Icon** > **Save & Publish** .

For Firefox - Go to **WMS** > **Group & Configs** > **Select a group** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Browser Settings** > **Firefox Settings** > **Privacy Settings** > **Hide Firefox Icon** > **Save & Publish** .

NOTE: ThinOS 10.x 2505 does not support the hide icon feature if the user has created browser shortcuts.

FIDO2 key registration

Enables FIDO2 key registration on a local browser with pre-VDI login authentication using fingerprint, facial scan, or PIN for enhanced security compliance.

SCEP connection status in Event Logs

Event Logs now include SCEP connection status and error messages, helping administrators troubleshoot device enrollment failures.

Log in to **WMS** and select **Groups & Configs** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Privacy and Security** > **SCEP**.

Select the options on **SCEP Settings** and click **Save & Publish**.

To view the SCEP logs, go to **System Information** > **Select Event Log**.

ACS ACR40T Smart Card Reader support

Dell ThinOS 10 adds support for the ACS ACR40T smartcard reader.

Microsoft Passkey Authentication (USB Key and Bluetooth Key)

Enables passwordless login to Citrix Workspace App (CWA) or Azure Virtual Desktop (AVD) using Microsoft Passkey, supporting FIDO2 PIN, face recognition, QR code, and Yubikey authentication.

For CWA: Log in to **WMS** and select **Groups & Configs** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Broker Settings** > **Citrix Virtual Apps and Desktop Settings** and enable **Use External Engine for WebLogin**

NOTE:

Use External Engine for WebLogin is disabled by default.

By default, Chrome Browser is selected in WebLogin Engine list.

For AVD: Log in to **WMS** and select **Groups & Configs** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Broker Settings** > **Azure Virtual Desktop Settings** and enable **Enable Azure Desktop Settings**

NOTE: Ensure to disable **Azure Classic (MS PROD)** and enable **Use External Engine for Web Login**.

Telegraf Agent monitoring tool

Introduces Telegraf Agent support for device monitoring and deployment through WMS or APT.

The Telegraf agent collects, monitors device performance such as CPU, Memory, and Ping Latency and sends metrics to a monitoring system like Prometheus.

To enable Telegraf, go to **WMS** > **Groups & Configs** > **Edit Policies** > **ThinOS10.X** > **Advanced** > **System Settings** > **Device Monitoring** > **Telegraf Configuration Editor.** and enable the **Telegraf Agent**.

Once enabled, the following metrics are activated by default: CPU, Memory, Network, and Ping Latency. These metrics can be disabled individually.

NOTE: The default Telegraf output configuration is set to **Prometheus** using port **9273** and metric version **2**.

NOTE: The Telegraf feature is disabled is disabled by default.

BIOS Virtualization Technology (VT) management

Admins can now manage Intel VT settings in the BIOS using WMS with minimal UI changes.

- Log in to **WMS** and select **Groups & Configs** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **BIOS** .
- Select the checkbox for the supported platform on **Select your platform** tab and close.
- Go to **Virtualization Support** and enable **Enable Virtualization** and **Enable Virtualization for Direct I/O** options.

  Once the policy is deployed and the device reboots, these settings are applied at the BIOS level and reflects on the BIOS configuration screen.

  NOTE: The Virtualization Technology options are disabled by default.

QR code error handling

Improves QR code handling with clearer error messages for invalid or expired codes.

ThinOS 10.x 2505 displays the new QR code error: `The QR code is invalid. Contact your system administrator.`

5G or LTE connectivity

Adds support for 5G/LTE connectivity using USB dongle in Wi-Fi or local network outage scenarios.

Keyboard layout switching

Enables keyboard input language switching with **`Windows Key + Spacebar`**, with taskbar indication and WMS or APT configuration support.

1. Go to **WMS 10.x policies** and select **Personalization** > **Shortcut Keys** > **Switch Keyboard Layout - Show List** .
2. Verify that the **Enable Switch Keyboard Layout - Show List** setting is disabled by default.
3. **Enable the Switch Keyboard Layout - Show List** dongle button and verify the default **Switch Key**.
4. Go to **Peripheral Management** > **Keyboard** > **Keyboard Layout List**.

   Select your language of choice, for exaample, English (United Kingdom), French (France), German, Japanese, Polish languages.
5. Click **Save & Publish** to save the policy to the device.
6. Select any added layouts by pressing **`Window Key + Spacebar`** and verify the taskbar.

Improved firmware design

Features a more transparent notification design that enhances user engagement and login field control.

The notification appears on the bottom right corner of the screen as **New Firmware/Application install is available**. Auto installation occurs in 115 seconds.

Two options are displayed: **Next Reboot** and **Update**.

If **Schedule Update** is enabled in WDA settings through WMS or APT on the ThinOS 10 device, a notification appears at the scheduled time with three options: **Next Reboot**, **Install**, and **Schedule**

Security Keys icon

Adds Security Keys Icon option in Account Privileges.

When the **Privilege Level** is set to **Customize**, the administrators can enable or disable the **Manage Security Keys** icon on the taskbar.

On-Screen Keyboard support

The On-Screen Keyboard is disabled by default but can be enabled to appear as a taskbar or floating icon.

Log in to **WMS** or **APT** and select **Groups & Configs** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Peripheral Management** > **Keyboard** > **On-Screen** > **Keyboard Settings** > **Enable On-Screen Keyboard** to enable it.

System information display

Displays device-specific system information about the WMS server based on the active network interface (ENET0 or WLAN0).

To view updated system information for a device:

1. Log in to **WMS**, go to the **Devices** page.
2. Click a specific device to open the **Device Details** page.
3. Open the **System Info** tab to view the details.

The displayed information is based on the active network interface.

- Wireless (WLAN0):
  - Added: SSID, Security Type, EAP Type, and Certificate Information.
- Ethernet (ENET0 and ENET1):

- Added: EAP Type and Certificate Information.

NOTE: This feature is applicable from WMS 5.1 and above only.

Firmware and application logs

Event logs now include entries for firmware and application package updates, installations, and uninstallations.

- Uninstallation (APT/System Tools): When a package is uninstalled using APT, the event log displays "`Package: deleting result - Success`" with the timestamp and package name (for example, Citrix, Omnissa, Zoom).
- Installation (WMS/APT): Upon deploying the package to the client, the installation starts automatically after download. During installation, only the installation window is visible; all other UI elements are hidden. The system auto-reboots after completion. Post-reboot, only the latest logs are retained—installation success logs are not displayed.

Horizon USB device selection

Allows users to choose whether to redirect USB devices into a Horizon Blast session.

After launching a Horizon Blast session, click the **Horizon Session Configuration** icon in the system tray.

From the list, select an active Blast session to view the available USB devices.

Users can **check** or **uncheck** individual USB devices to control whether each device is redirected to the selected session.

Extended sleep support

Supports system sleep periods of up to 10 hours.

Log in to **WMS** and select **Groups & Configs** > **Advanced** > **System Settings** > **Power Sleep Settings** > **Power Plugged in** > **Time When Plugged in**.

PXE image support

Enables ISO image deployment to clients using the PXE image method.

This feature currently supports imaging for Ubuntu 20.04 systems.

Pointer switching shortcut key

Adds a shortcut key for pointer switching across multiple screens.

Log in to **WMS** or **APT** and select **Groups & Configs** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Personalization** > **Shortcut Keys** > **Switch Pointer Shortcut Key**.

Shortpath support for AVD

Adds support for enabling Shortpath on Azure Virtual Desktop (AVD) connections.

By default, Remote Desktop Protocol (RDP) initiates a TCP-based reverse connect transport and attempts to upgrade the session to use UDP. If the UDP connection is successful, the TCP connection is dropped. If not, the session continues over TCP as a fallback.

NOTE: This policy applies only to AVD connections and is not supported for RDP or RDS sessions.

Background information settings

Updates the display of network port names, replacing ENET0 with the device's IP address (LAN) and WLAN0 with the IP address (Wi-Fi). Additionally, a new IEEE802.1x authentication status option has been added to the drop-down menu under: **Personalization** > **Desktop** > **Granular Control of Background**.

If IEEE802.1x authentication is successful, the value displayed is **Yes**. If authentication fails or is disabled, the value is **No**.

Peripherals Firmware Updates page

Adds a new **Peripherals Firmware Updates** page under the **Firmware** section. This feature allows administrators to upload firmware packages for Dell Docking Stations (WD19/WD22) and Dell Monitors (U2724DE). These packages can be published to ThinOS clients, which can then download and install the updates to connected peripherals.

NOTE: Wyse Management Suite 5.2 server is required for this update.

Device system information

ThinOS 10.x 2505 displays only the current information using network interface information.

To view updated system information for a device:

1. Log in to **WMS**, go to the **Devices** page.
2. Click a specific device to open the **Device Details** page.
3. Open the **System Info** tab to view the details.

The displayed information is based on the active network interface.

- Wireless (WLAN0):
  - Added: **SSID**, **Security Type**, **EAP Type**, and **Certificate Information**.
- Ethernet (ENET0 and ENET1):
  - Added: **EAP Type** and **Certificate Information**.

Notification Center

Introduces a unified Notification Center in ThinOS 10 to inform users about important system events such as peripheral connections (such as USB headsets, USB camera, USB storage), Bluetooth devices and VPN status.

This feature enhances the user experience by:

- Reducing the need to manually check event logs.
- Organizing messages into clear, categorized notifications.
- Minimizing redundant alerts.
- Filtering device notifications to show only relevant peripherals.

NOTE: The notifications are disabled by default in the ThinOS 10 taskbar.

They are enabled only when:

The device is in **Admin Mode**, or the Privilege Level is set to **Customize** in **Account Privileges**.

The notifications are supported only for the following USB device classes:

- 0x00 – USB_CLASS_PER_INTERFACE
- 0x01 – USB_CLASS_AUDIO
- 0x0E – USB_CLASS_VIDEO
- 0x08 – USB_CLASS_STORAGE
- 0xEF – USB_CLASS_MISC (Miscellaneous Device)
- 0x07 – USB_CLASS_PRINTER
- 0xFF – USB_CLASS_VENDOR_SPECIFIC

CV and CV3+ support - NFC contactless smartcard reader, finger print, and contact smartcard reader

ThinOS 10.x 2505 supports CV3 and CV3+ that allows the users to register and log in to VDI brokers (Citrix virtual apps and desktops, Omnissa Horizon, or Microsoft RDS) using Imprivata SignOn Server.

CV3 supported platforms include:

- Palm-rest contact smart card reader
- Palm-rest fingerprint reader

CV3+ supported platforms include:

1. Palm rest contact smart card reader
2. Palm-rest fingerprint reader
3. Palm-rest NFC contactless smart card reader (supports only PIV enabled smartcard)

Added CV3, CV3+ support on the following platforms:

- Latitude 5450/Latitude 5440/Latitude 5540/Latitude 5550
- Dell Pro 16 Plus PB16250
- Dell Pro 14 PC14250
- Dell Pro Rugged 14 RB14250

Citrix Workspace App updates

- In ThinOS 10 2505, the Citrix Workspace App (CWA) package version is updated to `Citrix_Workspace_App_25.03.0.66.102_T10.pkg`.
- This package installs the Citrix Workspace App version 2505 on ThinOS 10.x 2505.
- Enable or disable settings to copy and download is supported.
- Sustainability feature for the Citrix Desktop Viewer Toolbar is supported.
- Citrix Workspace window can now be changed to window mode in Citrix native mode.
- Citrix Configuration Editor has added Citrix XML setting 2 which allows you to modify the Citrix AuthManConfig.xml file.
- For more details on Citrix Workspace app updates and limitations, see the Citrix Workspace app updates .

Wi-Fi 7 support

ThinOS 10.x 2505 introduces Wi-Fi 7 support.

3

Upgrading ThinOS firmware

It is recommended to use the Wyse Management Suite version 5.0 or later to upgrade your ThinOS client firmware to the latest ThinOS 10.x version.

The overall upgrade process using **Wyse Management Suite** includes the following tasks:

1. Register your thin client to Wyse Management Suite.
   - Register ThinOS 10.x devices using Central Configuration. See Register ThinOS 10.x devices using Wyse Device Agent.
   - Register ThinOS 10.x devices using IPv4 DHCP option tags. See Register devices by using IPv4 DHCP option tags.
   - Register ThinOS 10.x devices using IPv6 DHCP option tags. See WMS auto discovery by IPv6 DHCP option.
2. Download the ThinOS operating system image. See Download ThinOS firmware, BIOS, and application packages.
3. Upgrade the BIOS on your device to the current version mentioned in the BIOS details section.
4. Upgrade the ThinOS firmware from 9.x to ThinOS 10.x using WMS. See Upgrade ThinOS 9.x to ThinOS 10.x.
5. Deploy the application packages. See Upload and push ThinOS 10.x application packages.

Compatibile platforms and firmware packages—ThinOS 10.x supports a wide range of Dell and non-Dell commercial client devices that meet the minimum hardware and component requirements. The complete list of validated platforms is available in the *ThinOS 10.x Hardware Compatibility List* document at Support | Dell.

- ThinOS 10.x upgrade image: `ThinOS10_YYMM_version.pkg`—used for upgrading supported devices to ThinOS 10.x 26xx.
- Conversion from Dell Hybrid Client (DHC): `DellHybridClient_Ubuntu_To_ThinOS10_conversion_YYMM_version.tar.gz`—used to migrate supported DHC platforms to ThinOS 10.x.
- Conversion from Dell client devices with Ubuntu 24.04 for Managed Clients: `DellHybridClient_Ubuntu_To_ThinOS10_conversion_YYMM_version.tar.gz`—used to streamline ThinOS 10 deployment on supported Ubuntu-based devices.

Supported firmware upgrade scenarios—The following firmware upgrade scenarios are supported for upgrading to the latest ThinOS 10 version:

- ThinOS 10.0052 or later versions > ThinOS10 YYMM

Servicing mode has been added to the installation process. The following changes can be observed as part of this addition:

- **Updated installation order**—The installation sequence is now **BIOS** > **OS** > **Application**.
  - After a BIOS update, ThinOS reboots and goes to update the operating system.
  - After the operating system update, ThinOS reboots again to update the applications.
- **Background downloads**—The operating system, BIOS, and applications are downloaded in the background and installed in servicing mode. You can check the download status by clicking the download icon on the taskbar.
- **Automatic logoff**—ThinOS automatically logs off when entering servicing mode. Login is restricted until the update process is complete.
- **Failure handling**—If the update fails:
  - ThinOS exits servicing mode automatically after a countdown.
  - You can log in and resume work after exiting servicing mode.
  - Failed applications are listed in the Failed Application List.
- **Battery requirement**—Updates do not starts if the battery charge is below 50%, even if the power adapter is connected. The update begins once the battery is charged to 50%.

WMS server or group changes—If you change the WMS server or group in the **Central Configuration** window while an upgrade notification is active, a dialog box notifies you that the upgrade will be terminated.

For detailed information about the upgrade process, see the latest *ThinOS 10.x Migration Guide* at Support | Dell.

Table 1. ThinOS 10.x 2602 packages

ThinOS application package details	ThinOS packages
Amazon_WorkSpaces_Client	Amazon_WorkSpaces_Client_2025.1.5589.319_T10.pkg

Table 1. ThinOS 10.x 2602 packages (continued)

ThinOS application package details	ThinOS packages
Cisco_Jabber	Cisco_Jabber_15.2.224_T10.pkg
Cisco_Webex_App_VDI	Cisco_Webex_App_VDI_45.12.0.33726.214_T10.pkg
Citrix_Workspace_App	Citrix_Workspace_App_25.08.10.111.245_T10.pkg
ControlUp_VDI_Agent	ControlUp_VDI_Agent_2.4.2601.21.201_T10.pkg
eG_VM_Agent	eG_VM_Agent_7.5.2.267_T10.pkg
Firefox	Firefox_140.7.0.292_T10.pkg
Imprivata_PIE	Imprivata_PIE_23.3.0.715913.190_T10.pkg
Jabra	Jabra_8.5.11.277_T10.pkg
Liquidware_Stratusphere_Ux_Connector_ID_Agent	Liquidware_Stratusphere_Ux_Connector_ID_Agent_6.7.0.83.259_T10.pkg
Microsoft_AVD	Microsoft_AVD_3.3.476_T10.pkg
Omnissa_Horizon_ClientSDK	Omnissa_Horizon_ClientSDK_2512.8.17.0.378_T10.pkg
RingCentral_App_Horizon_Plugin	RingCentral_App_Horizon_Plugin_25.4.30.274_T10.pkg
uxm_Endpoint_Agent	uxm_Endpoint_Agent_2026.01.15.270_T10.pkg
Zoom_Universal	Zoom_Universal_6.6.10.26830.292_T10.pkg
App_Builder	App_Builder_2.0.691_T10.pkg
CI_Apps_Onboarding	CI_Apps_Onboarding_1.0.92_T10.pkg
Google_Chrome	Google_Chrome_144.0.7559.109.362_T10.pkg
U2724DE_PFW	U2724DE_PFW_105.118_T10.pkg
fcdclient	fcdclient_3.6.0.123_T10.pkg
DellDock_PFW	DellDock_PFW_01.11.179_T10.pkg

NOTE: If a package fails to update or causes functionality issues, remove all packages, reboot the thin client, and reinstall as needed.

NOTE: Third-party packages are removed during upgrades to ThinOS 10.x 2502 and later. Ensure to reinstall the latest versions post upgrade.

Table 2. Tested BIOS versions and packages

Model	Tested BIOS version
Dell Wyse 5070 Thin Client	bios-5070_1.40.0_T10.pkg
Dell Wyse 5070 Extended Thin Client	bios-5070_1.40.0_T10.pkg
Dell Wyse 5470 All-in-One	bios-5470AIO_1.34.0_T10.pkg
Dell OptiPlex 3000 Thin Client	bios-Op3000TC_1.32.1_T10
Dell Wyse 5470 Mobile Thin Client	bios-5470_1.34.0_T10.pkg
Dell Latitude 3330	bios-Latitude_3330_1.32.1_T10.pkg

Table 2. Tested BIOS versions and packages (continued)

Model	Tested BIOS version
Dell Latitude 3420	bios-Latitude_3420_1.44.0_T10.pkg
Dell Latitude 3440	bios-Latitude_3440_1.25.1_T10.pkg
Dell Latitude 3450	bios-Latitude_3450_1.17.0_T10.pkg
Dell Latitude 5440	bios-Latitude_5440_1.27.2_T10.pkg
Dell Latitude 5450	bios-Latitude_5450_1.19.2_T10.pkg
Dell Latitude 5520	bios-Latitude_5520_1.46.0_T10.pkg
Dell Latitude 5530	bios-Latitude_5530_1.32.1_T10.pkg
Dell Latitude 5540	bios-Latitude_5540_1.26.0_T10.pkg
Dell Latitude 5550	bios-Latitude_5550_1.18.1_T10.pkg
Dell OptiPlex 5400 All-in-One	bios-OptiPlex5400AIO_1.1.54_T10.pkg
Dell OptiPlex All-in-One 7410	bios-OptiPlexAIO7410_1.31.0_T10.pkg
Dell OptiPlex All-in-One 7420	bios-OptiPlexAIO7420_1.21.0_T10.pkg
Dell OptiPlex Micro Plus 7010	bios-OpMicroPl7010_1.31.0_T10.pkg
Dell OptiPlex Micro Plus 7020	bios-OptiMicroPlus7020_1.20.0_T10.pkg
Dell Pro Rugged 13 RA13250/Dell Pro Rugged 14 RB14250	bios-ProRugged_1.11.1_T10.pkg
Dell Pro 14 PC14250	bios-DellPro14PC14250_1.12.0_T10
Dell Pro 16 PC16250	bios-Pr16PC16250_1.12.0_T10
Dell Pro 16 Plus PB16250	bios-DellPro16PlusPB16250_2.9.0_T10.pkg
Dell Pro Max 16 Plus MB16250	bios-PrMx16PlMB16250_2.2.2_T10.pkg
Dell Pro Max 14 MC14250	bios-PrMx14MC14250_1.9.0_T10.pkg
Dell Pro Tower Plus XE5 OEM QBT1250	bios-PrTwrPlQBT1250_1.10.1_T10.pkg
Dell Pro Tower QCT1250	bios-PrTwrQCT1250_1.10.1_T10.pkg
Dell Pro Max Laptops MC16250	bios-PrMx16MC16250_1.9.0_T10.pkg
Dell Pro Slim Low SFF QCS1250	bios-PrSlQCS1250_1.10.1_T10.pkg
Dell Pro Slim Plus XE5 OEM QBS1250	bios-PrSlPlQBS1250_1.10.1_T10.pkg
Dell Precision 3280	bios-Precision3280_1.18.0_T10.pkg
Dell Precision 3260 Compact	bios-Precision3260_3.21.0_T10.pkg
Dell Pro Micro QCM1250	bios-PrMicroQCM1250_1.10.1_T10
Dell Pro 24 All-in-One (65 W) QC24250	bios-Pr24AllQC24250_1.12.1_T10
Dell Pro 24 All-in-One Plus QB24250	bios-Pr24AllPlQB24250_1.12.1_T10
Dell Pro 24 All-in-One QC24251	bios-Pr24AllQC24251_1.8.1_T10

NOTE: The BIOS versions that are listed above are the current tested versions. Newer BIOS versions are expected to be released in the upcoming release.

When you convert a device from another operating system to ThinOS 10.x, ThinOS updates certain BIOS settings during the first boot.

Table 3. BIOS settings during first boot

BIOS settings	Value
BIOS password	Set to **Fireport**
SATA/NVMe Operation	Set to **AHCI/NVMe**
Integrated network interface controller	Set to **Enabled** (set to disable PXE boot support)
Wake-on-LAN	Set to **LAN only**

NOTE: For OptiPlex 3000 Thin Client with SFP module, the option is set to **LAN or SFP NIC**.

Table 4. BIOS settings for SFP module

BIOS settings	Value
Enable Secure Boot	Set to **ON**
Enable USB Boot Support	Set to **OFF**
Enable USB Wake Support	Set to **ON**
Deep Sleep Control	Set to **Disabled**

NOTE: These BIOS settings are applied only if the device has a BIOS password set to **Fireport** or if the BIOS password field is empty.

Table 5. Supported transceivers for OptiPlex 3000 Thin Client

Supported transceivers
Allied Telesis 1 Gbps SFP, fiber (AT-SPSX-90)
Allied Telesis 100 Mbps SFP fiber (AT-SFPX/2-90)
Allied Telesis 10/100/1000 RJ45 SFP, copper
Dell Finisar 1 GB SFP
Dell Finisar 100 Mbps SFP (FTLF1217P2BTL-FC)
Dell 1 Gbps SFP

Before you upgrade

- Before upgrading from ThinOS 9.5.3102 or later version to ThinOS 10.0052, ensure the following:
  - The system is powered on.
  - Sleep mode is disabled.
- If the system enters sleep mode, send a Wake-on-LAN command through Wyse Management Suite before issuing any real-time commands. To use the Wake-on-LAN command, ensure that the Wake-on-LAN option is enabled in the BIOS.

Important notes

- You cannot boot into ThinOS when you perform any of the following operations in BIOS setup:
  - Disable the onboard Network Interface Card (NIC), Trusted Platform Module (TPM), or Platform Trust Technology (PTT).
  - Clear TPM or PTT.
  - Reset BIOS to factory default settings.
- If you power off the ThinOS client by force, a counter in the TPM starts from one. When the counter reaches 32, the client encounters a **Fatal Error**. If the error is displayed, do the following:
  - For ThinOS 10.x 2502 and later versions, every time when the TPM counter reaches 32 and encounters the **Fatal Error** issue, you must reboot manually to recover the client.

- Before you boot a nonsupported device, you must run the **ThinOS Compatibility Checker** to run a compatibility check to identify if the current device is supported by ThinOS 10.x and provides a report on compatibility issues.

Register ThinOS 10.x devices to Wyse Management Suite

NOTE: DHCP and DNS configurations for Wyse Management Suite work when the ThinOS client is not registered yet.

Register ThinOS 10.x devices using Wyse Device Agent

Steps

1. To access the central configuration settings, do the following:
   - **Modern Mode**—From the desktop menu, click **Settings** > **Central Configuration**.
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Central Configuration**.

   The **Central Configuration** dialog box is displayed.
2. Enter the **Group Registration Key** as configured by your administrator for the group.
3. Select the **Enable WMS Advanced Settings** check box.
4. In the **WMS server** field, enter the Wyse Management Server URL.
5. To verify the setup, click **Validate Key**.
   An Alert window is displayed.
6. Click **OK**.
7. If the key is not validated, verify the group key and Wyse Management Suite server URL which you have provided. Ensure that the ports mentioned are not blocked by the network. The default ports are 443 and 1883.

   NOTE: If the Group Token parameter is not specified, the device is moved to the unmanaged group or quarantine group.
8. Enable or disable CA validation based on your license type. For public cloud, select the **Enable CA Validation** check box, and for private cloud, select the **Enable CA Validation** check box if you have imported certificates from a well-known certificate authority into your Wyse Management Suite server.

   To enable the CA validation option in the private cloud, you must install the same self-signed certificate on the ThinOS device as well. If you have not installed the self-signed certificate in the ThinOS device, do not select the **Enable CA Validation** check box. You can install the certificate to the device by using Wyse Management Suite after registration, and then enable the CA validation option.
9. Click **Save** to save the changes.
   The device is registered to Wyse Management Suite.

Register ThinOS 10.x devices by using secure IPv4 DHCP option tags

About this task

You can register the devices by using the following secure IPv4 DHCP option tags:

NOTE: Do not set secure IPv4 DHCP option tags if your current ThinOS version is earlier than 10.00xx.

Table 6. Registering the device by using secure IPv4 DHCP option tags

Option Tag	Description
• Name—WMS • Data Type—String • Code—201 • Description—Secure WMS Server	The tag specifies the secure Wyse Management Suite server.

Table 6. Registering the device by using secure IPv4 DHCP option tags (continued)

Option Tag	Description
• Name—Group Registration Key • Data Type—String • Code—202 • Description—Secure Group Registration Key	The tag directs the device to fetch the secure Group Registration Key for Wyse Management Suite.
• Name—CA Validation • Data Type—String • Code—167 • Description—Certificate Authority Validation	• You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud. • Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. • Enter **False**, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. **NOTE:** CA Validation is optional for Wyse Management Suite 5.0 and later versions. However, it is recommended to configure this option tag.

NOTE: If you use both secure DHCP option tags and legacy DHCP option tags to register devices, secure DHCP option tags take priority over legacy.

To get a secure Wyse Management Suite server and secure Group Registration Key, do the following:

Steps

1. Go to **WMS Server** > **Portal Administration** > **Console Settings** > **WMS Discovery**.
2. Enter the group token.
3. Select **DHCP** from the **Discovery Type** drop-down list.
4. Click **Generate Details**.

   NOTE: Do not set predefined string values for DHCP option tags 201 and 202, as these predefined values are limited to 255 characters. The secure Wyse Management Suite server and secure Group Registration Key can accommodate more than 255 characters. Instead, manually copy and set the secure Wyse Management Suite server and secure Group Registration Key for DHCP option tags 201 and 202.

WMS auto discovery by IPv6 DHCP option

ThinOS 10.x 2502 supports WMS auto discovery by IPv6 DHCP option. The IPv6 DHCP option tags for WMS auto discovery are listed below:

Table 7. WMS auto discovery by IPv6 DHCP option

Option Tag	Description
• Name—WMS • Data Type—String • Code—16500 • Description—WMS Server FQDN	This tag specifies the Wyse Management Suite server URL, such as wmsserver.acme.com, where `wmsserver.acme.com` is the fully qualified domain name of the server hosting the Wyse Management Suite. **NOTE:** The HTTPS:// prefix is not required in the Wyse Management Suite URL.
• Name—WMS • Data Type—String • Code—20100 • Description—Secure WMS Server	This tag specifies the secure Wyse Management Suite server.

Table 7. WMS auto discovery by IPv6 DHCP option (continued)

Option Tag	Description
• Name—CA Validation • Data Type—String • Code—16700 • Description—Certificate Authority Validation	• You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud. • Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. • Enter **False**, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. **NOTE:** CA Validation is optional for Wyse Management Suite 5.0 or later versions. However, it is recommended to configure this option tag.
• Name—Group Registration Key • Data Type—String • Code—19900 • Description—Group Registration Key	The tag directs the device to retrieve the Group Registration Key for Wyse Management Suite. For example, in SCDA-DTOS10SalesGroup, the second part of the Group Registration Key must be 8-31 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character. However, special characters such as \(backslash), "(double quotes), '(single quote) are not allowed. The Group Registration Key is case-sensitive. **NOTE:** Group Token is optional for Wyse Management Suite 5.0 on prem-server. However, due to a known issue, if you do not provide the Group Token, the device is not moved to an unmanaged group. It is recommended to configure the Group Token key.
• Name—Group Registration Key • Data Type—String • Code—20200 • Description—Secure Group Registration Key	The tag directs the device to retrieve the secure Group Registration Key for Wyse Management Suite.

NOTE: If only IPv6 is available in your network and IPv4 is absent, the system requires approximately 5 minutes for the IPv4 DHCP to time out. After this timeout, the system automatically discovers WMS using IPv6 DHCP. To avoid this delay during each reboot, ensure that IPv4 is disabled in your WMS policy.

Register ThinOS 10.x devices by using legacy IPv4 DHCP option tags

You can register the devices by using the following legacy IPv4 DHCP option tags:

Table 8. Registering the device by using legacy IPv4 DHCP option tags

Option Tag	Description
• Name—WMS • Data Type—String • Code—165 • Description—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com`, where wmsserver.acme.com is the fully qualified domain name of the server where Wyse Management Suite is installed. **NOTE:** HTTPS:// is not required in the Wyse Management Suite URL.
• Name—MQTT • Data Type—String • Code—166 • Description—MQTT Server	This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, `wmsservername.domain.com:1883`. WDA automatically fetches the MQTT details when devices check in for the first time.

Table 8. Registering the device by using legacy IPv4 DHCP option tags (continued)

Option Tag	Description
	NOTE: MQTT is optional for Wyse Management Suite 5.0 and later versions.
• Name—CA Validation • Data Type—String • Code—167 • Description—Certificate Authority Validation	• You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud. • Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. • Enter **False**, if you have not imported the SSL certificates from a well-known authority for https communication between the client and the Wyse Management Suite server. **NOTE:** CA Validation is optional for Wyse Management Suite 5.0 and later versions. However, it is recommended that configure this option tag.
• Name—Group Registration Key • Data Type—String • Code—199 • Description—Group Registration Key	This tag directs to the Group Registration Key for the Wyse Management Suite agent. For example, in SCDA-DTOS10SalesGroup, for the second part of the Group registration key, you must use 8-31 characters, with at least 1 upper, 1 lower, 1 number, 1 special character. However, special characters such as \(backslash), "(double quotes), '(single quote) are not allowed. **NOTE:** Group Token is optional for Wyse Management Suite 5.0 and later versions on private cloud. However, there is a known issue that if you do not provide the group token, the device is not moved to an unmanaged group. Therefore, It is recommended to configure the Group Token key.

Register devices using secure DNS records

Steps

1. On the Wyse Management Suite server, go to **Portal Administration** > **WMS Discovery**.
2. Specify the Wyse Management Suite URL, Group Token, select DNS as the **Discovery Type** and click **Generate Details** to get the Wyse Management Suite URL and Group Token encrypt strings.
3. In the DNS server, go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** and right-click the domain.
4. Click **Other New Records**.
5. Select Text (TXT), click Create Record, and do the following:
   - To create the Wyse Management Suite Server record, enter the following values, and click **OK**.
     - Record name—_WMS_MGMTV2.
     - Text—Wyse Management Suite URL encrypt strings from Step 2.
   - To create the Wyse Management Suite Group Token record, enter the following values, and click **OK**.
     - Record name—_WMS_GROUPTOKENV2.
     - Text—Group token encrypt strings from Step 2.
   - To create the Wyse Management Suite CA validation record, enter the following values, and then click **OK**.
     - Record name—_WMS_CAVALIDATION
     - Text—TRUE/FALSE

   If you have not registered your ThinOS client to Wyse Management Suite and if you have set the DNS server with records, the device will automatically register to Wyse Management Suite.

   NOTE: If both secure DNS records and legacy DNS records are set in the DNS server, the secure DNS records take priority.

Register devices using legacy DNS records

Steps

1. In the DNS server, go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** > **_tcp**, and right-click the **_tcp** option.
2. Click **Other New Records**.
   The **Resource Record Type** window is displayed.
3. Select the **Service Location (SRV)**, click **Create Record**, and do the following:
   To create a Wyse Management Suite server record, enter the following details and click **OK**:
   - **Service—`_WMS_MGMT`**
   - **Protocol**—`_tcp`
   - **Port number**—`443`
   - **Host offering this service**—FQDN of WMS server
4. Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain**, and right-click the domain.
5. Click **Other New Records**.
6. Select **Text (TXT)**, click **Create Record**, and do the following:
   - To create Wyse Management Suite Group Token record, enter the following values, and click **OK**:
     - **Record name**—`_WMS_GROUPTOKEN`
     - **Text**—`WMS Group token`
   - To create Wyse Management Suite CA validation record, enter the following values, and then click **OK**:
     - **Record name**—`_WMS_CAVALIDATION`
     - **Text**—`TRUE/FALSE`

Enable Live Update

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Services**, and click **WDA Settings**.
4. Enable or disable **Enable Live Update**.
   If enabled, the thin client starts downloading the firmware and package immediately. 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.
5. Click **Save & Publish**.

   NOTE: The operating system firmware and BIOS firmware download in the background. If the **Live Update** option is disabled, the thin client downloads the operating system firmware and BIOS firmware but cannot complete installation until the next reboot.

Download ThinOS 10.x firmware, BIOS, and application packages

This section describes the steps to download the ThinOS firmware from the Dell support site.

Steps

1. Go to the Support | Dell site.
2. Locate the required ThinOS Image entry and click the download icon.

Table 9. Available ThinOS 10.x 2602 package options

Scenario	ThinOS 10 package title	File name
Upgrade from ThinOS 10.x 2502 to ThinOS 10.x 2602 (same version family)	ThinOS 10 2602 Firmware Upgrade Package	Root_upgrade_2602_10.0555_T10.pkg
Convert Dell Hybrid Client or Ubuntu 24.04 for Managed Clients to ThinOS 10	Dell Hybrid Client/Ubuntu 24.04 for Managed Clients to ThinOS 10 2602 Conversion Package	DellHybridClient_Ubuntu_To_ThinOS10_conversion_2602_10.0555.tar.gz
Download Dell Recovery Image	ThinOS 10 2602 Offline USB Installer Package	ThinOS10_2602_0555.iso
Upgrade from ThinOS 9.5.3102 or later to ThinOS 10.x 2602	ThinOS 9.5.3102 or Later to ThinOS 10 2602 Upgrade Package	Root_2602.10_0555_signed.pkg
Upgrade or downgrade package for ThinOS 10.x	ThinOS 10 2602 10.0xxx Firmware Upgrade and Downgrade Package	Root_2602.10.0555_T10.pkg

3. If you want to use ThinOS packages, locate the package and click the download icon. For more information about ThinOS packages, see Upgrading the ThinOS firmware.
4. If you want to install the latest BIOS package, locate the package entry—ThinOS YYMM <version> BIOS package <version>—for your thin client model and click the download icon.

   For information about BIOS installation, see BIOS Installation.

File naming convention

ThinOS application packages, ThinOS firmware, BIOS packages, and other files can be published from the Wyse Management Suite server.

The file names must adhere to the following character rules:

- Uppercase letters (A–Z)
- Lowercase letters (a–z)
- Numeric characters (0–9)
- Special characters—period (.), hyphen-minus (-), and underscores (_)

NOTE: Using any other characters in the file name results in installation failure.

Upgrade ThinOS 9.x to ThinOS 10.x using Wyse Management Suite or Admin Policy Tool

Upgrade ThinOS 9.x to ThinOS 10.x using Wyse Management Suite

Prerequisites

- Ensure that you are running 9.5.3102 or later versions on your thin client.
- Create a group in Wyse Management Suite with a valid group token. Use this group token to register the ThinOS 9.x devices.
- Register your thin client to Wyse Management Suite.
- The ThinOS 9.x and ThinOS 10.x firmware upgrade and application packages must be copied into the repository—`\WMS\LocalRepo\repository\thinOSConfigFiles`.
- ThinOS 10.x application and firmware packages are available in public cloud, such as the **Operator cloud**.
- Browse to **Firmware** > **Firmware package updates**, and select the ThinOS 9.x to ThinOS 10.x upgrade package.
- Select the required configuration and application packages in the ThinOS 9.x configuration such as Citrix_Workspace_app, ControlUp_VDI_Agent.
- Push the ThinOS 9.x to ThinOS 10.x upgrade package to the ThinOS 9.x group.
- The ThinOS 9.x to ThinOS 10.x upgrade package `Root_2505.10_0076_signed.pkg` installs the root base OS. Selected packages are installed automatically after upgrading to ThinOS 10.

- You can continue using the existing policy configuration until a new configuration is created and assigned within the ThinOS 10.x group.

Steps

1. Log in to **Wyse Management Suite**.
2. Go to the **Groups & Configs** page, and select a group.
3. From the **Edit Policies** drop-down menu, select **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.
4. Go to **Advanced**.
5. In the **Firmware** field, select **OS Firmware Updates**.
6. Click **Browse** to browse and upload the firmware.
   The EULA and vendor details are displayed.
7. Verify the vendor names and license agreement and then click **Accept** to upload the package.
8. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the `Root_2505.10_0076_signed.pkg` package from the local repository.
9. Click **Save & Publish**.
   An alert window is displayed.
10. Click **Save** to save the changes.
11. Click **Download** to check if the package is getting downloaded.
    The thin client begins downloading the firmware, and a notification appears on the screen.
12. Click **Update Now**.
    The thin client downloads the firmware and once the upgrade is successful, it reboots to the desktop screen.
13. Click the **System Information** icon to view the system information window.
14. Go to the **License** tab and check if the license information is displayed or not.
15. Check if the **License Type** is displayed as **BIOS License** or **ThinOS Activation License**.
    The firmware version is upgraded successfully.

Upgrade ThinOS 9.x to ThinOS 10.x using Admin Policy Tool

The firmware upgrade using Admin Policy Tool is supported on ThinOS 10.x.

Prerequisites

- Ensure that you are running ThinOS 9.5.3102 or later versions on your thin client.
- Ensure that you have connected the USB drive to the ThinOS Client.
- Ensure that you copy the `Root_2505.10_0076_signed.pkg` package to the USB drive.

Steps

1. Go to the Admin Policy Tool on the ThinOS client.
2. Click **Advanced** tab.
3. In the **Firmware** field, select **OS Firmware Updates**.
4. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
5. Click **Browse** to browse and upload the `Root_2505.10_0076_signed.pkg` package from the USB drive.
   The EULA and vendor details are displayed.
6. Verify the vendor names and license agreement and then click **Accept** to upload the package.
7. Select the OS firmware package, and click **Save & Publish**.
   The thin client downloads the firmware and once the upgrade is successful, it reboots to the desktop screen. A **System Information** window displays on the screen.
8. Go to the **License** tab.
9. Check if the **License Type** is selected as **BIOS License** or **ThinOS 10 Activation License**.
   The firmware version is upgraded successfully.

Policy configuration

Import and update ThinOS policies as part of the conversion process from ThinOS 9.x to ThinOS 10.x.

- Policy Configuration before conversion:
  1. Go to the **Groups & Configs** page, and select a group.
  2. Click **Import** policies.
  3. From the **Import Policies Wizard**, select the **ThinOS 10.x policies** from **ThinOS 9.x policies**.
  4. Click **Next**. A **Preview** is displayed on the **Import Policies Wizard**.
  5. Click **Next** again.
  6. Click **Import**.

NOTE: All the configurations from the ThinOS 9.x policy are imported to ThinOS 10.x.

- Policy configuration after conversion:
  1. You must install the required packages such as Citrix from Wyse Management Suite or using Admin policy Tool.
  2. You may continue using the same ThinOS 9.x policies in the ThinOS 10.x client.

NOTE: If you change any one of the configurations in ThinOS 10.x, then the ThinOS 9.x policy gets deleted.

Add ThinOS application packages to the repository

Steps

1. Log in to Wyse Management Suite using your tenant credentials.
2. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS 10.x**.
3. Click **Add Package file**.
   The **Add Package** screen is displayed.
4. To select a file, click **Browse** and go to the location where your file is located.
   - If the EULA is embedded in the package, the EULA and vendor details are displayed. Verify the vendor names and license agreement of each vendor. Click **Accept** to upload the package. You can select the **Do not show this again** if you do not want to see the EULA details of the same vendor again. You must accept the license agreement of the packages individually. The package is not uploaded if you click **Decline**.
   - If the EULA is not embedded in the package, go to step 5.
5. Click **Upload**.

   NOTE: The operator can upload the package from the operator account and is visible to all the tenants. The tenants cannot delete or modify these files.

Application Package Updates category

The following are the defined categories:

1. Citrix
   - Citrix Workspace App
2. Omnissa
   - Omnissa Horizon
3. Microsoft
   - Microsoft AVD
4. Zoom
   - Zoom Universal
5. Cisco
   - Cisco Jabber
   - Cisco Webex Meetings VDI
   - Cisco Webex VDI
6. Dell
   - Security Addon

- Hotfix
- ThinOS Telemetry Dashboard
- Customer Apps Enabler
- App Builder

7. Third Party
   - Imprivata PIE
   - Jabra
   - Epos Connect
   - HID Fingerprint Reader
   - Identity Automation QwickAccess
   - ControlUp VDI Agent
   - RingCentral App Omnissa Plugin
   - eG VM Agent
   - uxm Endpoint Agent
   - Liquidware Stratusphere Ux Connector ID Agent
   - Lakeside Virtual Agent
   - Amazon Workspaces Client
8. Other
   - Google Chrome
   - Firefox
   - Telegraf Agent monitoring tool
   - Monitor firmware (Dell Monitor U2724DE)
   - Dell dock firmware upgrade (Dellock_WD19_WD22_PFW)
   - Application packages are not predefined yet.
9. Customer Apps
   - App Builder Packages

For each category, there is a **INSTALL/UNINSTALL** toggle button on the left and one drop-down list **Not Selected** by default on the right. Click the drop-down list, and the uploaded version of the application package is displayed. You can select only one version in the list and the drop-down list title changes to the package name and repository.

NOTE: For **Other** category, you can select multiple application packages and versions, as the application packages are not predefined yet. However, you cannot set **UNINSTALL** for this category. Once you have the application packages in **Other** category, it is recommended you upgrade the Wyse Management Suite configUI. The new Wyse Management Suite configUI sets the application packages in the new category.

If the switch option is set to **INSTALL**, the selected application package version in the drop-down list is published to the ThinOS client to install.

If the switch option is set to **UNINSTALL**, the application package drop-down list is disabled, and the application package is uninstalled from the ThinOS client.

Upload and push ThinOS 10.x application packages using Groups and Configs on Wyse Management Suite

Prerequisites

- Create a group in Wyse Management Suite with a group token. Use this group token to register the ThinOS 10.x devices.
- Register the thin client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 10.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. Click **Advanced**.
4. In the **Firmware** field, click **Application Package Updates**.
5. To select a file, click **Browse** and go to the location where your file is located.

- If the EULA is embedded in the package, the EULA details of the package and the name of the vendors are displayed. You can click the vendor names to read the license agreement of each vendor. Click **Accept** to upload the package. You can select the **Do not show this again** if you do not want to see the EULA details of the same vendor again. If you upload multiple packages, the EULA details of each package are displayed. You must accept the license agreement of the packages individually. The package is not uploaded if you click **Decline**.
- If the EULA is not embedded in the package, go to step 6.

NOTE: You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository or operator cloud repository.

6. Expand the category of the package and select it.
7. Verify and ensure that the switch option of the category is **INSTALL**.
8. Click **Save & Publish**.
   The application package is installed and the thin client restarts.

Upload and install ThinOS 10.x application packages using Admin Policy Tool

Steps

1. Go to the Admin Policy Tool on the ThinOS client.
   The **Configuration Control | ThinOS** window is displayed.
2. Click **Advanced**.
3. In the **Firmware** field, click **Application Package Updates**.
4. Browse and upload the packages from a USB drive.
5. Expand the category of the package and select it.
6. Verify and ensure that the switch option of the category is **INSTALL**.
7. Click **Save & Publish**.
   The application packages are installed and the thin client restarts.

Firmware installation using ThinOS ISO image

You can install ThinOS from a USB drive using the Dell OS Recovery Tool on the validated platforms that are listed in the official ThinOS 10.x Hardware Compatibility List.

For more information about the compatible Dell and non-Dell platforms, see *ThinOS 10.x Hardware Compatibility List* document at Support | Dell.

The **Dell ThinOS 10.x Recovery BIOS** boot option is either preinstalled on devices from the factory or can be added using an ISO image.

For information about installation instructions, see the *Dell ThinOS 10.x Migration Guide* at Support | Dell.

Support for 32 GB storage and 4 GB RAM

ThinOS 10.x 2508 introduces enhancements that improve memory handling and session stability across devices with limited hardware resources. These enhancements expand compatibility to devices with 4 GB RAM and 32 GB storage, while allowing administrators to manage memory usage more effectively through WMS or APT policies and client-side monitoring. You can now:

- Control session launch behavior based on available free RAM.
- Receive server-side alerts for devices that fall below defined memory thresholds.
- Monitor memory usage in real time on the client device.
- Notify users proactively when system memory is low.
- Display WMS warnings during upgrades for devices with insufficient recommended memory.

The following are the key highlights:

- **Application Launch Control**–Prevents launch of new VDI or browser sessions if free RAM is below a configured threshold. Displays a client notification and sends an alert to WMS.

  NOTE: For customer installed (CI) applications, only low-memory notifications are supported; sessions are not blocked.

- **Real-time RAM monitoring**–Continuously checks free memory on the client. If RAM falls below threshold, an on-screen alert prompts users to save data and close unused applications.
- **WMS upgrade warning**–During ThinOS 9.x to ThinOS 10.x upgrades, WMS warns administrators if devices have less than the recommended 8 GB RAM, indicating potential performance limitations.

For more information about configuring memory-based controls, see Configure memory-based controls using WMS.

For more information about limitations on 4 GB RAM, see Limitations.

Configure memory-based controls using WMS

To configure memory-based controls using WMS, enable the feature, set the minimum RAM threshold, and select session types. Also, enable real-time RAM monitoring and set the alert threshold value. This configuration helps monitor low-memory devices and provides alerts as needed.

Steps

1. Log in to WMS as an administrator and select **Groups & Configs** > **<Select a group>** > **Edit Policies**.
2. Go to **Application Launch Control**.
3. Enable the feature by checking the **On** option.
4. Enter the minimum RAM threshold (in MB) required to launch new sessions.
5. Select the **session types** to enforce (VDI or Browser).
6. Go to **Real-Time RAM Monitoring**.
7. Enable monitoring and set the alert threshold value.
8. Click **Save & Publish** to push the updated policy to devices.
9. Monitor the **WMS console** for alerts indicating low-memory devices.

Limitations

This section outlines the session and browser limitations that are observed on 4 GB RAM devices, where memory warnings may appear if users exceed supported thresholds.

Supported benchmarks:

- **Citrix Workspace**–up to eight sessions and applications
- **Horizon Client**–up to 5 sessions/apps
- **AVD/RDS**–up to three sessions
- **Browser (Firefox/Chrome)**–up to five tabs

System alerts:

- **Low RAM Alert**—displayed when usage exceeds the supported benchmark.
- **System - Low memory detected**—displayed when cache memory usage is exceeded.

Upgrade BIOS using WMS

Explains how to upgrade the BIOS on ThinOS devices, use WMS or the Admin Policy Tool after the ThinOS image has been successfully updated.

Prerequisites

- Go to Support | Dell, and download the latest BIOS file.
- If you are upgrading the BIOS using WMS, register the device to WMS.

For a successful upgrade, first upgrade the operating system image, then upgrade the BIOS.Upgrading both simultaneously causes the system to ignore the BIOS upgrade. The system then blocks installation of the same BIOS version, requiring an upgrade to a different version instead.

Steps

1. Open the Admin Policy Tool on the device or go to the ThinOS 10.x policy settings on WMS.
2. On the **Configuration Control | ThinOS** window, click the **Advanced** tab.
3. Expand **Firmware** and click **BIOS Firmware Updates**.
4. Click **Browse** and select the BIOS file to upload.
5. From the **Select the ThinOS BIOS to deploy** dropdown menu, select the BIOS file that you have uploaded.
   After a successful upload, the BIOS package appears under the **BIOS Firmware Updates** list in WMS with the correct **Platform Type** associated with the firmware file.
6. Click **Save & Publish**.

   The device restarts. BIOS is upgraded on your device.

   NOTE: For more information about the latest BIOS version, see the latest *Dell Wyse Management Suite Version 5.x Release Notes* at Support | Dell.

   NOTE: BIOS upgrade requires a display screen (integrated or external) without which the update fails. In this case, you cannot install the BIOS package again. You must install another BIOS version.

   If a power adapter is not connected on any ThinOS Mobile Client, the BIOS update fails. After the power adapter is connected, you must reboot to trigger the BIOS update again.

BIOS setting configuration

Explains how to configure BIOS on ThinOS devices by registering the device, setting a BIOS password, and using WMS or Admin Policy Tool to apply and publish changes for secure, standardized management.

Prerequisites

- If you are using WMS, ensure that you have registered the device and synchronize the BIOS admin password. The WDA stores the current BIOS password to unlock the BIOS and apply the required changes. For more information about using the **Sync BIOS Admin Password** option, see the *Dell Wyse Management Suite Administrator's Guide* at Support | Dell.
- If you have not synced the BIOS password in the WMS server, you can input the current BIOS password in BIOS policy to publish BIOS settings. If you have synced the BIOS password in the WMS server, the **Current BIOS Admin password** option in the BIOS policy is ignored. WMS server uses the synced BIOS password to publish BIOS settings.
- If you are using the Admin Policy Tool, ensure that you enter the current BIOS admin password in the **Advanced** > **BIOS** section.

Steps

1. Open the Admin Policy Tool on the device or go to the ThinOS 10.x policy settings on WMS.
2. In the **Configuration Control | ThinOS** window, click the **Advanced** tab.
3. Expand **BIOS** and select your preferred platform.
4. In the **System Configuration** section, modify the USB ports and audio settings.
5. In the **Security** section, modify the administrator-related configurations.
6. In the **Power Management** section, modify the power-saving options.
7. In the **POST Behavior** section, modify the post behavior options.
8. Click **Save & Publish**.

   NOTE: If the BIOS does not have a password and you set a new one, or if you change the BIOS password using a select group, a reboot is required for the new password to take effect, while other BIOS setting changes are applied after a second reboot.

   NOTE: If you enable **Set Admin Password**, set a new BIOS password, and then reboot the thin client, the new password is automatically synced to the WMS server. However, if you enable **Set Admin Password**, set the password, and then disable the option before rebooting, the BIOS password is cleared and reset to empty.

NOTE: On ThinOS clients, the **Current BIOS Admin Password** option is always blank, and the **Set Admin Password** option is always disabled. These options do not have any impact on the functionality.

BIOS configuration details

The BIOS Common Configuration acts as a centralized settings page in ThinOS that consolidates all BIOS settings that are supported across all ThinOS 10.x devices. This feature ensures consistent BIOS configurations across devices using the same Active Directory in WMS.

To access the BIOS Common Configuration settings in WMS, go to **Advanced Settings** > **BIOS Common Configurations** > **Dell Supported Devices BIOS Settings**.

The following are the key highlights:

- If a platform-specific BIOS configuration exists, that configuration is applied; otherwise, the common BIOS configuration is used.
- Platform-specific settings take precedence over common settings.
- Supports scalable BIOS configuration across many devices.
- Reduces manual effort during deployment by allowing BIOS settings to be pushed centrally.
- Enables easier onboarding of new platforms by falling back to a common configuration until platform-specific values are available.

NOTE: This feature is supported across all platforms. However, if a platform includes a dedicated BIOS settings page, any changes made there overrides the BIOS Common Configuration settings.

Table 10. Supported Configuration

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
Boot Options				
Enable USB Boot Support	Enable/Disable	Enables booting to USB mass storage devices. Disabling prevents this. Does not affect OS-level USB access.	All Devices	Not applicable
PXE Boot Support	Enable/Disable	Allows the device to perform a PXE Boot.	All Devices	Not applicable
USB Port Control				
Enable Rear USB Ports	Enable/Disable	Enables rear USB ports.	3040, OptiPlex 3000 and Wyse 5070 only	Not applicable
Enable USB port Front Top	Enable/Disable	Enables the front top USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	OptiPlex Micro-Plus 7010, Wyse 5070, OptiPlex 3000	Not applicable
Enable USB port Front Medium	Enable/Disable	Enables front medium USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	Wyse 5070	Not applicable
Enable USB port Front Bottom	Enable/Disable	Enables the front bottom USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	OptiPlex Micro-Plus 7010, Wyse 5070, OptiPlex 3000	Not applicable
Enable Side USB Ports	Enable/Disable	Enables USB ports on the side of AIO.	All AIO Devices	Not applicable

Table 10. Supported Configuration (continued)

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
		Keyboard and mouse work in BIOS setup irrespective of this setting.		
Enable Side USB port Top	Enable/Disable	Enables top-side USB port on AIO. Keyboard and mouse work in BIOS setup irrespective of this setting.	5400 AIO and 5470 AIO	Enable Side USB Ports
Enable Side USB port Bottom	Enable/Disable	Enables bottom-side USB port on AIO. Keyboard and mouse work in BIOS setup irrespective of this setting.	5400 AIO and 5470 AIO	Enable Side USB Ports
Enable Rear USB port Top Left	Enable/Disable	Enables rear upper left USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Enable Rear USB port Top Right	Enable/Disable	Enables rear upper right USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Enable Rear USB port Bottom Left	Enable/Disable	Enables rear bottom left USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Enable Rear USB port Bottom Right	Enable/Disable	Enables rear bottom right USB port. Keyboard and mouse work in BIOS setup irrespective of this setting.	All AIO Devices	Enable Rear USB Ports
Audio				
Audio	Enable/Disable	Enables integrated audio controller.	All Devices	Not applicable
Security				
Current BIOS Admin Password	Password Value	Required to edit BIOS settings. If previously synced, the displayed value may differ.	All Devices	Required to make any change
Set New BIOS Admin Password	Enable/Disable	Enables BIOS administrator password. The changes take effect immediately.	All Devices	Not applicable
New BIOS Admin Password	Password Value	Set the new admin password. Must contain at least one digit, one uppercase, one	All Devices	Set New BIOS Admin Password

Table 10. Supported Configuration (continued)

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
		lowercase, and one special character.		
Admin Setup Lockout	Enable/Disable	Prevents access to BIOS Setup when the admin password is set.	All Devices	Not applicable
Power Management				
Auto On Time	Disable, Daily, Workday, Days	BIOS uses UTC (0) time zone. Set UTC-based time, not operating system time.	All Devices	Not applicable
Time	Time Value	BIOS uses UTC (0) time. Set UTC-based time, not operating system time.	All Devices	Auto On Time
Days	Day List	Set specific days to auto power on.	All Devices	Auto On Time
Wake-on-LAN	LAN only, LAN with PXE Boot, Disable	Allows wake from shutdown using LAN or wireless LAN signal.	All Devices	Not applicable
AC Recovery	Power Off, Power On, Last State	Behavior after AC power is restored.	All Devices	Not applicable
Wake On USB	Enable/Disable	Enables USB to wake the system from its hibernate state.	All Devices	Not applicable
Deep Sleep Control	Enabled in S5 only/S4 and S5	Controls system power conservation in shutdown (S5) or hibernate (S4).	All Devices	Not applicable
POST Behavior				
MAC Address Pass Through	Passthrough MAC, Disabled, NIC 1 MAC	Replaces NIC MAC with selected MAC address.	All Devices	Not applicable
BIOS POST Behavior				
Fastboot	Minimal, Auto, Thorough	Speeds up boot by skipping compatibility steps.	All Devices	Not applicable
Extend BIOS Post Time	0 / 5 / 10 seconds	Adds a delay before boot to allow reading POST messages.	All Devices	Not applicable
Keyboard Error Detection	Enable/Disable	Specifies if keyboard errors are reported during boot.	All Devices	Not applicable
BIOS Pre behavior				
Suppress Docking Station Warning Msg	Enable/Disable	Suppresses boot warning message for incompatible device that is connected to DockPort.	All Devices	Not applicable
Virtualization Support				

Table 10. Supported Configuration (continued)

BIOS Configuration	Setting Values	Description	Supported Devices	Dependent BIOS Configuration
Enable Virtualization	Enable/Disable	Enables Virtualization Technology (VT).	All Devices	Not applicable
Enable Virtualization for Direct I/O	Enable/Disable	Enables VT for Direct I/O.	All Devices	Not applicable

Configure BIOS parameters using WMS or APT

Describes how administrators can configure and enforce ThinOS features and BIOS settings using WMS or APT. Using WMS or APT, administrators can centrally configure device behavior, security controls, authentication methods, network settings, and BIOS parameters.

About this task

After applying the configuration, the settings are enforced on the ThinOS device and can be verified through the operating system, user session, browser, or during boot in the BIOS.

Steps

1. To configure the BIOS parameters, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Navigate to the appropriate Advanced configuration section based on the feature.
3. Locate the required setting or policy.

   The following table lists the BIOS and platform setting values that can be configured using Dell Command | Configure. It describes where each setting applies, its purpose, supported configuration values, the configuration path in WMS or APT, and how to verify a successful application.

Table 11. Dell Command | Configure BIOS parameters configuration

Feature/ Parameter	Applies To	Purpose	Supported Values	Path (WMS or APT)	Verification Point
Keyboard Shortcut Blocking	• OS • Browser • Session • OSK	Blocks specific keyboard shortcut combinations to prevent restricted actions	• Enable • Disable (per-key keyboard combination)	Advanced → Peripheral Management → Keyboard → Key Combination → Modifiers	Shortcut action is blocked across browser, OS, session, and OSK
UEFI Boot Path Security	BIOS	Enforces UEFI Boot Path Security settings	• Always Except Internal HDD • Always • Never	Advanced → BIOS Common Configuration → Dell Supported Devices BIOS Settings → Security	BIOS security page (F2)
Chassis Intrusion Option	BIOS	Controls the Chassis Intrusion access level	• Enable • Disable • Silent	Advanced → BIOS Common Configuration → Dell Supported Devices BIOS Settings → Security	BIOS security page (F2)
HTTPS Boot Support	BIOS	Enables or disables HTTPS boot functionality	• Enable • Disable	Advanced → BIOS Common Configuration →	BIOS connections page (F2)

Table 11. Dell Command | Configure BIOS parameters configuration (continued)

Feature/ Parameter	Applies To	Purpose	Supported Values	Path (WMS or APT)	Verification Point
				Dell Supported Devices BIOS Settings → Security	
Function Lock Option (Laptops only)	• BIOS • Keyboard	Controls primary or secondary behavior of function keys	• Fn Lock • Media Key	Advanced → BIOS Common Configuration → Dell Supported Devices BIOS Settings → Security	BIOS keyboard settings
Proxy PAC URL – Manual	Network	Configures the Proxy PAC URL manually	• URL String • Not Configured	Advanced → Network Configuration → Proxy Settings	Proxy activity in event logs/CC Proxy
Proxy PAC URL – DHCP (Option 252)	Network	Automatically applies the Proxy PAC URL using DHCP Option 252	• Enable • Disable	DHCP Server Option 252 + WMS check-in	Proxy activity in CC Proxy logs

4. Select or configure the required option.
5. Click **Save & Publish**.

ThinOS 10.x upgrade or downgrade using WMS

ThinOS 10.x (version 2508 and later) supports seamless upgrade and downgrade between ThinOS 10 N and N+1 versions using Wyse Management Suite (WMS). This capability enables remote management, automatic rollback, and configuration alignment without manual intervention.

The following are the key features:

- **Remote upgrade or downgrade initiation**—IT Administrators can initiate ThinOS 10.x upgrades or downgrades remotely using the Wyse Management Suite (WMS) console, streamlining deployment and minimizing endpoint downtime.
- **Add-on package compatibility**—During the upgrade or downgrade process, existing add-on packages are either retained or automatically updated to maintain compatibility with the target ThinOS version.
- **Automatic configuration updates**—WMS automatically updates endpoint configurations to match the upgraded or downgraded ThinOS version, ensuring consistent user experience and system behavior.
- **Automatic rollback on failure**—If an upgrade or downgrade fails, ThinOS automatically reverts to the last known working version to prevent service disruption and maintain endpoint stability.
- **Failure logging and troubleshooting**—The IT Administrators can access the detailed endpoint logs to support debugging and troubleshooting, enabling quick resolution of upgrade issues.
- **Signing certificate tolerance**—ThinOS upgrades and downgrades between N and N+1 versions are not impacted by changes in signing certificates, ensuring a smooth transition.
- **Certificate retrieval from WMS**—If a signing certificate mismatch occurs, the client fetches the correct certificate from WMS to complete the upgrade successfully.

Delete ThinOS 10.x application packages using Admin Policy Tool

Explains how to remove ThinOS 10.x packages using the device UI or Admin Policy Tool, for single or multiple packages.

Steps

1. Log in to the ThinOS 10.x device.

2. From the system menu, go to **System Tools** > **Packages**.
   All the installed ThinOS 10.x packages are listed.
3. Select a package that you want to delete and click **Delete**.

   NOTE: To delete all the packages, click **Delete all**.

4. Click **OK** to save your settings.

Delete ThinOS 10.x application packages using WMS

Explains how to uninstall ThinOS 10.x application packages using WMS by selecting packages in group policies, using the Standard or Advanced tabs, and publishing the changes for managed devices.

Prerequisites

- Create a group in WMS with a group token.
- Register the device to WMS.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 10.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.
4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.

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

5. Click **Browse** and select the application package to upload.
6. For each category, ensure that the switch is set to **UNINSTALL**. You can select only one version in the list for each category.

   NOTE: For a given ThinOS release, you can install only the supported packages that are mentioned in the corresponding ThinOS Release Notes available at Support | Dell.

7. Click **Save & Publish**.

   NOTE: For the **Other** category, you can select multiple application packages and versions, as the packages are not predefined. However, the **UNINSTALL** option is not supported for this category. After adding application packages to the **Other** category, it is recommended to upgrade the WMS configUI. The updated configUI automatically assigns the application packages to the appropriate new category.

Peripherals Firmware Updates support

ThinOS 10.x 2505 introduces **Peripherals Firmware Updates** page under the **Firmware** section. This feature allows you to upload firmware packages for Dell Docking Stations (WD19/WD22) and Dell Monitor U2724DE, and publish them to ThinOS 10 clients. The clients then automatically download and install the firmware to update connected peripherals.

NOTE: Wyse Management Suite 5.2 server is required for this update.

Dell docking station WD19/WD22

1. After installation, a notification appears prompting the user to unplug and replug the docking station.
2. The docking station is temporarily non-functional during the update (~1 minute).
3. The thin client automatically reboots after the update is applied.

Dell Monitor U2724DE

1. The monitor firmware update is displayed on-screen during installation.
2. The monitor disconnects and reconnects after the update.
3. The thin client automatically reboots after the installation is complete.

Important notes

- Peripheral must remain connected throughout the update process.
- Firmware package download is blocked if the peripheral is not connected.
- If the download is deferred to the next reboot and the peripheral is disconnected, the update fails.
- Only one firmware package should be published at a time. Multiple peripheral firmware updates are not supported.
- Do not publish peripheral firmware alongside OS, application, or BIOS packages.
- Firmware packages are single-use; another peripheral cannot be updated using the same package.
- For monitor firmware updates, ensure that the uplink cable is connected.
- Do not connect Dell Monitor U2724DE to Latitude 5450 using Thunderbolt cable, as it may cause system failure.

Configure Background Info Settings using WMS or APT

Explains how ThinOS 10.x enables IT administrators to configure Background Info settings using WMS or APT, allowing granular control of desktop background information such as date and time for improved customization and user visibility.

About this task

After completing the configuration, ThinOS 10.x automatically applies the selected Background Info elements to the desktop. These settings remain persistent across reboots, upgrades, and downgrades, ensuring consistent presentation of background information based on administrator-defined policies.

Steps

1. To configure Background Info settings, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Personalization** > **Desktop** > **Desktop Settings**.
3. Under **Desktop Settings**, enable the **Background Info Settings**.
4. Go to **Granular Control of Background Info**, select the **Date** and **Time** from the drop-down menu.
5. Click **Save & Publish**.

4

Getting started with ThinOS

This chapter helps you to quickly learn the basics and get started with your ThinOS -based thin client.

End User License Agreement

End User License Agreement (EULA) is added to ThinOS. EULAs must be read and accepted to continue using ThinOS. By default, Dell EULA is added to ThinOS. The third-party EULAs are displayed on the EULA screen depending on the ThinOS application packages that you install on the thin client.

The EULA screen is displayed during the following instances:

- When you boot the thin client for the first time.
- When you reset a thin client that runs ThinOS 10.x to factory settings.

Configure ThinOS using First Boot Wizard

A First Boot Wizard application runs automatically for the first time when you start a thin client with ThinOS. The Thin client starts the First Boot Wizard application before you enter the ThinOS desktop. This application launches before you enter the ThinOS desktop, allowing you to configure system preferences, set up Internet connectivity, load USB configurations, configure management software, and establish broker connections.

Prerequisites

If you are an existing thin client user, and you have upgraded to the ThinOS 10.x, reset your thin client to factory default settings to enter the First Boot Wizard.

NOTE: If DHCP contains the Wyse Management Suite configurations, the ThinOS desktop is loaded without entering the First Boot Wizard and you cannot view the End User License Agreement.

About this task

This section describes how to configure ThinOS using First Boot Wizard. You can also switch between **Light mode** or **Dark mode** as per your preference on the First Boot Wizard.

Steps

1. Connect your thin client to an Ethernet using a wired connection.

   NOTE: If you want to use a wireless connection, you can connect to Wi-Fi on the **Select Your Network** screen at a later stage.

2. Turn on your thin client.

   The thin client checks for a wired network connection. If the network connection is successful, a welcome screen is displayed before the EULA screen. For more information about the EULA screen, see End User License Agreement.

   NOTE: When you reset the device to factory default settings without a network connection, a message `Device is waiting for WMS information from network auto discovery` is displayed. Check **I have reviewed all license agreements** on the welcome screen to go to next screen.

3. Click **Dell EULA** from the right pane to read the respective EULAs. If you have installed the ThinOS application packages, ensure that you read the respective EULAs of the third-party applications.

   NOTE: The EULA screen may be different depending on the client-installed packages.

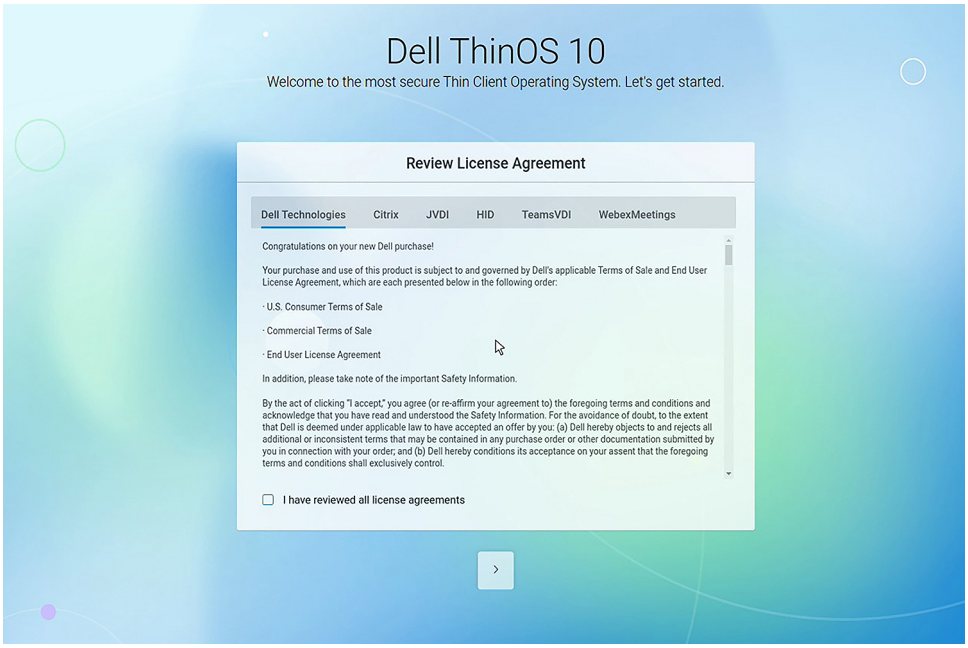

Figure 1. EULA Screen

4. Select the **I have reviewed all license agreements** check box and click the button.
5. Scan your QR code.

   You can scan your QR Code to import the Wyse Management Suite configuration, after which the device exits from First Boot Wizard. If your device does not have an integrated camera or external camera, then you cannot see the QR code.

Figure 2. QR code

6. On the **Select Your Language** screen, select a language from the **Language** drop-down list to start ThinOS in the regional language.

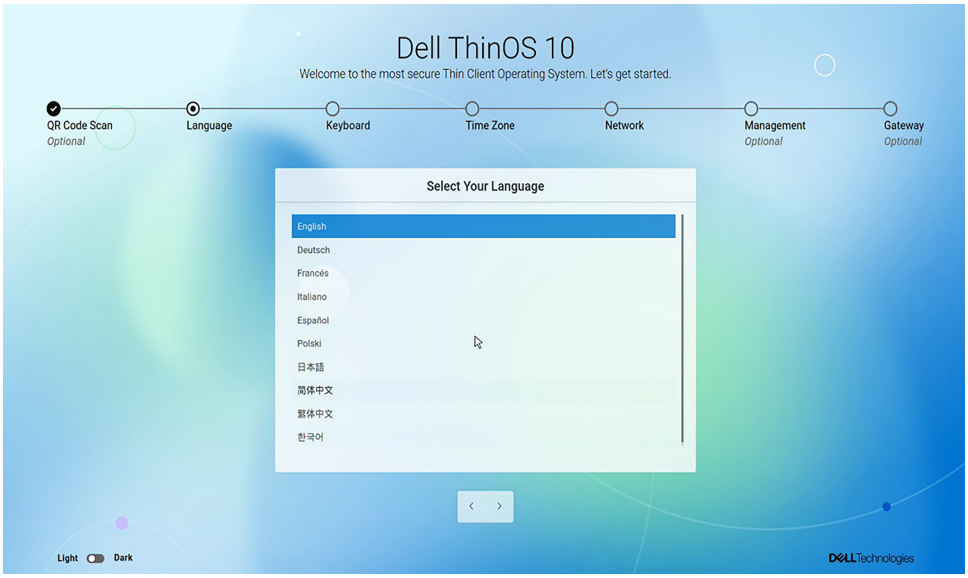

Figure 3. Select Your Language

7. Click › button.
8. On the **Select Your Keyboard** screen, select a keyboard layout from the list.

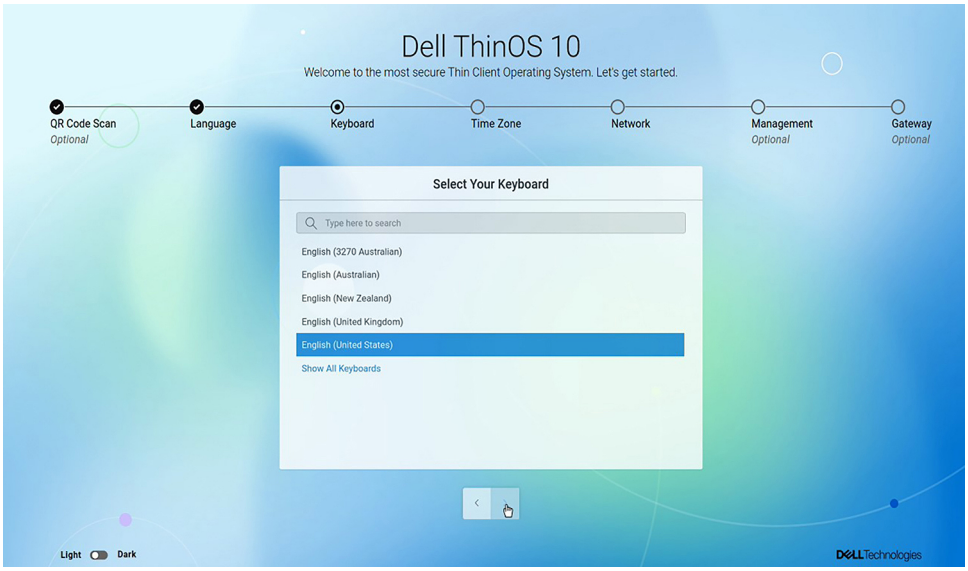

Figure 4. Select Your Keyboard

9. Click › button.
10. On the **Select Your Time Zone** screen, select a time zone from the list to set the time zone for your thin client.

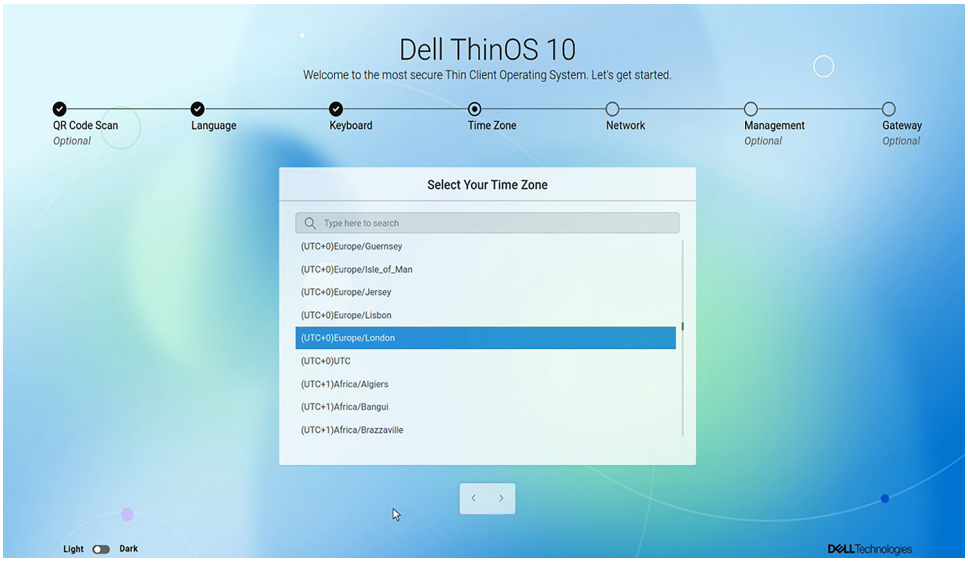

Figure 5. Select Your Time Zone

The time server with IP addresses or host names is also displayed.

11. Click › button.
12. On the **Select Your Network** screen, do either of the following:
    - **Wired Network (Ethernet)**—Click this option if you have connected the thin client to an Ethernet using a wired connection.
    - **Wireless Network (Wi-Fi)** —Click this option if you want to select a wireless network. From the list, select a wireless network, and click **Connect**.

      NOTE: The option to define a wireless connection is not available on thin clients without a WLAN module.

    - **My computer does not connect to the Internet**—Click this option if you do not want to establish a network connection using the First Boot Wizard screen. You can connect to either wired or wireless connection after you boot to the ThinOS desktop.

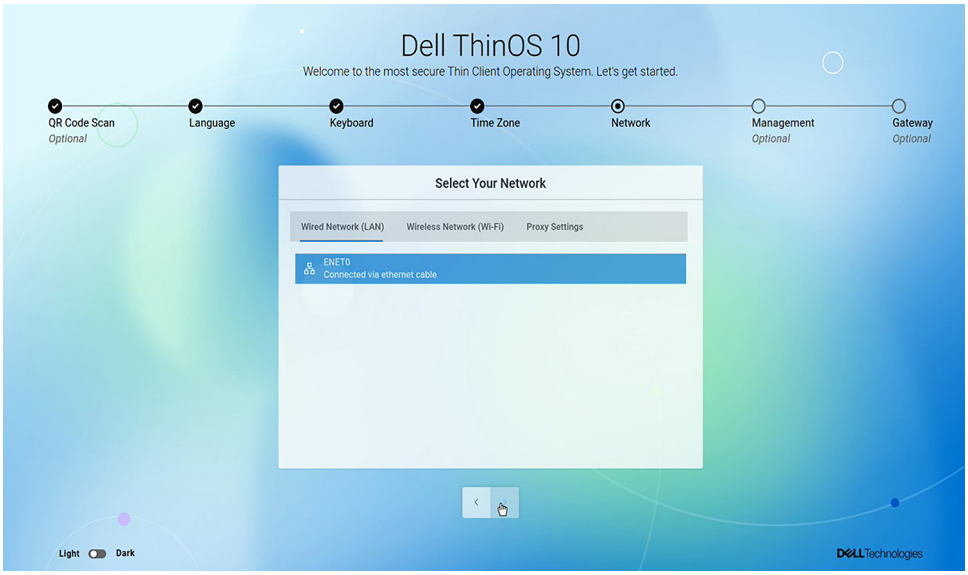

Figure 6. Select Your Network

13. Click › button.

14. On the **Set UP Remote Management** screen, do either of the following:
    - Select **I have a server detail provided by IT Services** from the **Connection Setup** drop-down menu if you want to use Wyse Management Suite to manage your thin clients.

      To register your thin client to Wyse Management Suite, enter the group registration key and the Wyse Management Suite server URL. Select the **CA validation** check box if you want to enable the CA validation feature. The CA validation is required when you import certificates into your Wyse Management Suite server. By default, the CA Validation check box is selected to improve the security when using the Wyse Management Suite cloud. While typing, you can click the eye icon next to **Prefix** and **Group Key** to display the masked values. Click the icon again to hide the values.

    - Select **I have a USB Flash drive with the Server details** from the **Connection Setup** drop-down menu if you want to import system settings from the USB drive.
    - Select **I have a QR Code and Password** from the **Connection Setup** drop-down menu if you do not want to import any ThinOS configurations using the QR code.

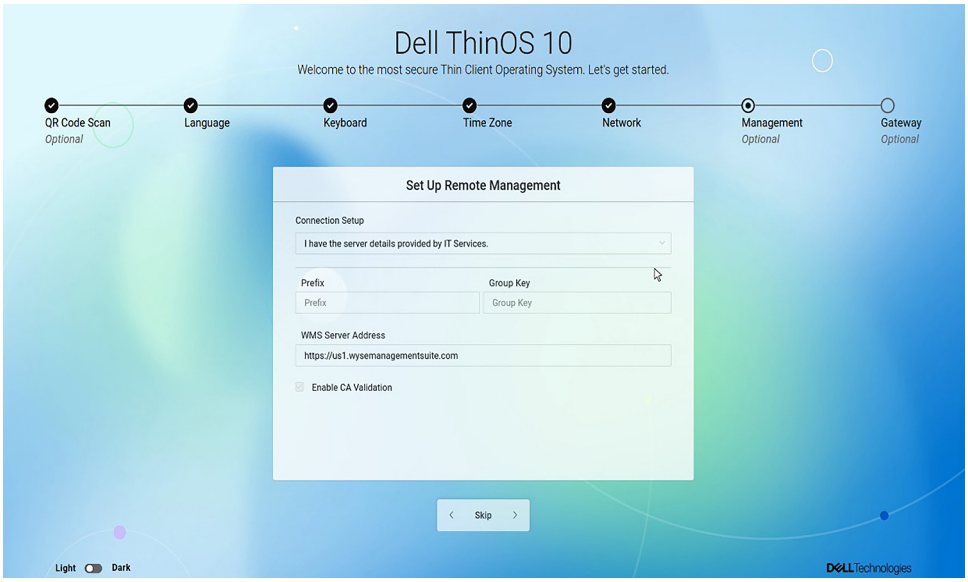

Figure 7. Set Up Remote Management

15. Click button.

    NOTE: Click the **Skip** button if you want to bypass the page without saving the details.

16. On the **Set Up Your Gateway** screen, configure your preferred broker type from the following options:
    - Citrix Virtual Apps and Desktops
    - Omnissa Horizon
    - Azure Virtual Desktop
    - Microsoft Remote Desktop Services
    - Amazon Workspaces
    - Other Broker
    - Multi Broker

    NOTE: Select the **Don't set your broker right now** checkbox and click the **Skip** button to bypass the page without providing or saving configuration details.

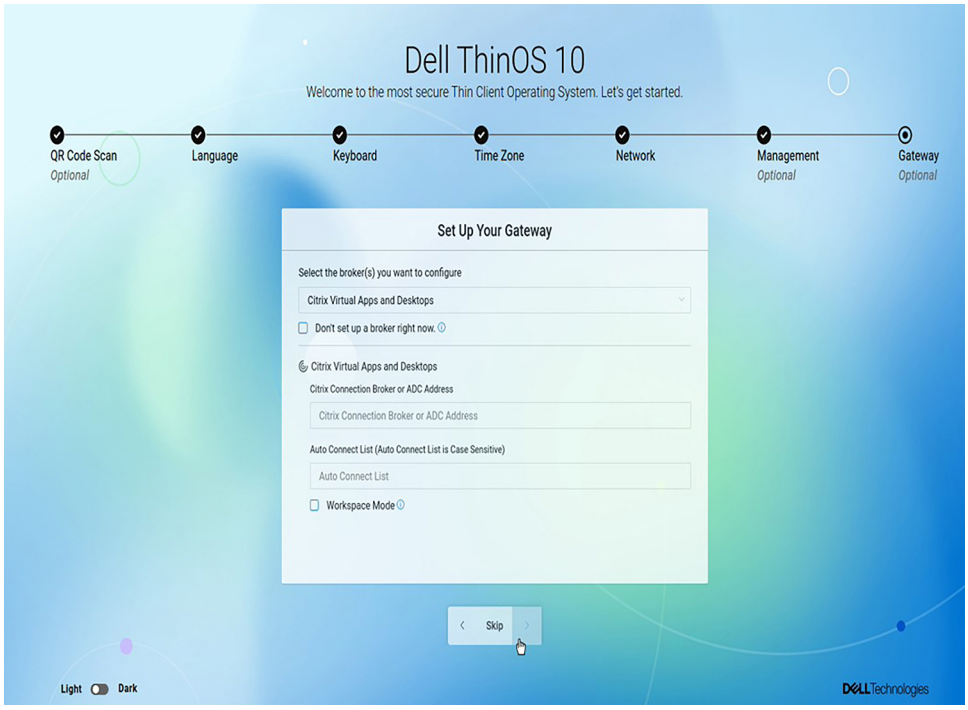

Figure 8. Set Up Your Gateway

17. Click › button.
The **Success!** screen is displayed. The device exists from the First Boot Wizard mode, and the ThinOS desktop is displayed.

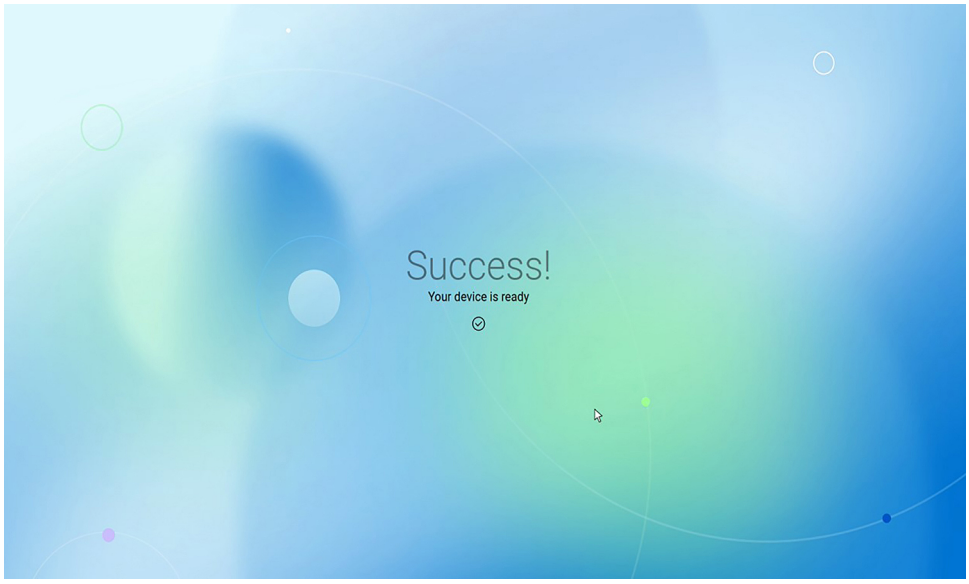

Figure 9. Success!

The device reboots from the First Boot Wizard mode, and the ThinOS desktop page is displayed.

Enhanced ThinOS 10.x installer GUI

ThinOS 10.x has the enhanced UI installer with multiple language support during the installation phase. The enhanced UI appears for the following installation modes:

- When upgrading ThinOS 9.x to ThinOS 10.x.
- When converting Dell Hybrid Client to ThinOS 10.x.

- When converting Dell Ubuntu Base OS to ThinOS 10.x using DCA-Enabler.
- When installing ThinOS 10.x using USB drive and Dell Recovery Tool.

Dell ThinOS 10 installation screen and OS details

- **OS Overview**—ThinOS 10 is the exclusive VDI client solution, which is engineered to meet modern customer needs. With seamless deployment, robust security, and purpose-built design, ThinOS 10 enhances performance in virtual environments.

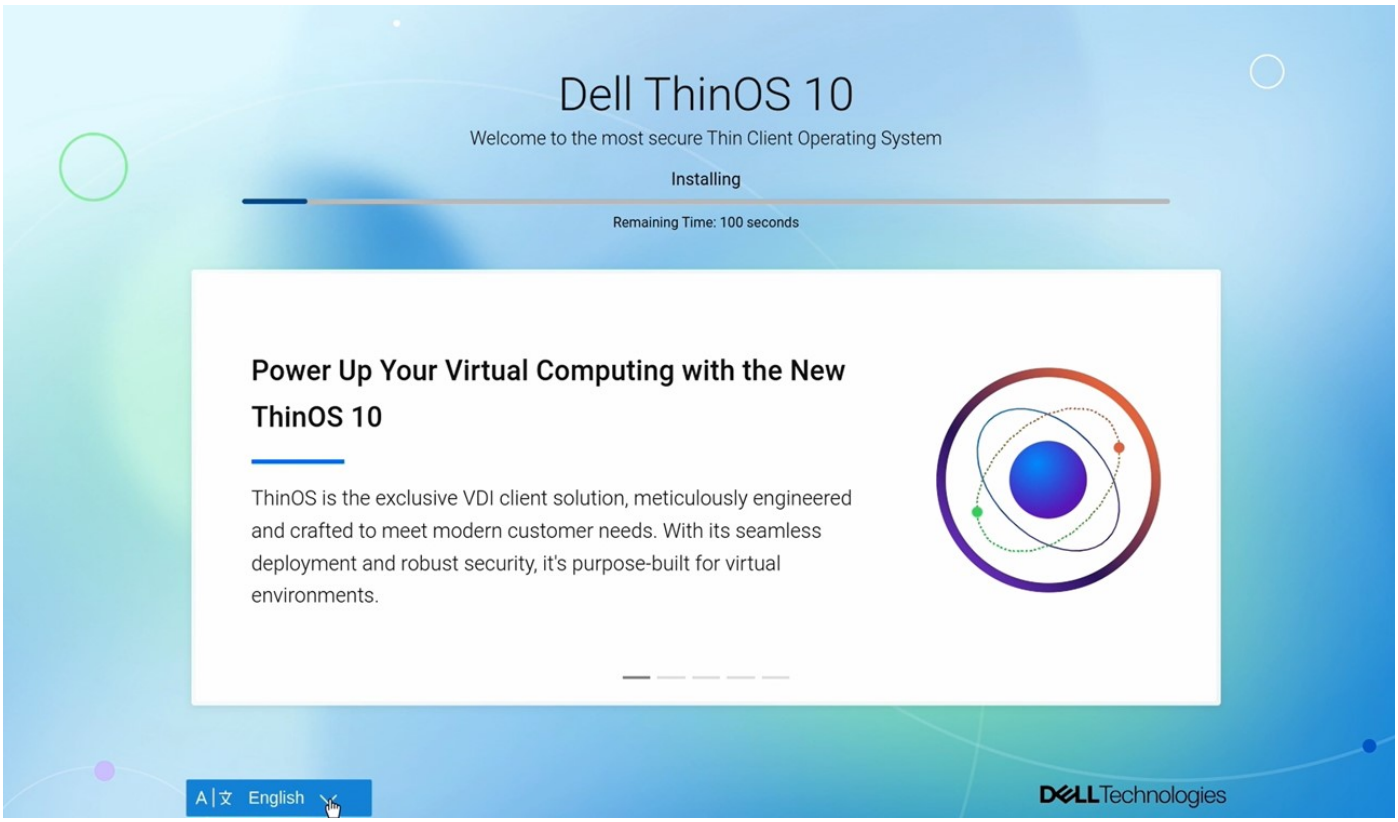

Figure 10. Installation Screen

- **Installation preparation**—The installation process is complete and ready to connect, featuring built-in support for popular virtual workspaces, new browser options, and third-party technology partner solutions, with an optimized architecture for collaboration.

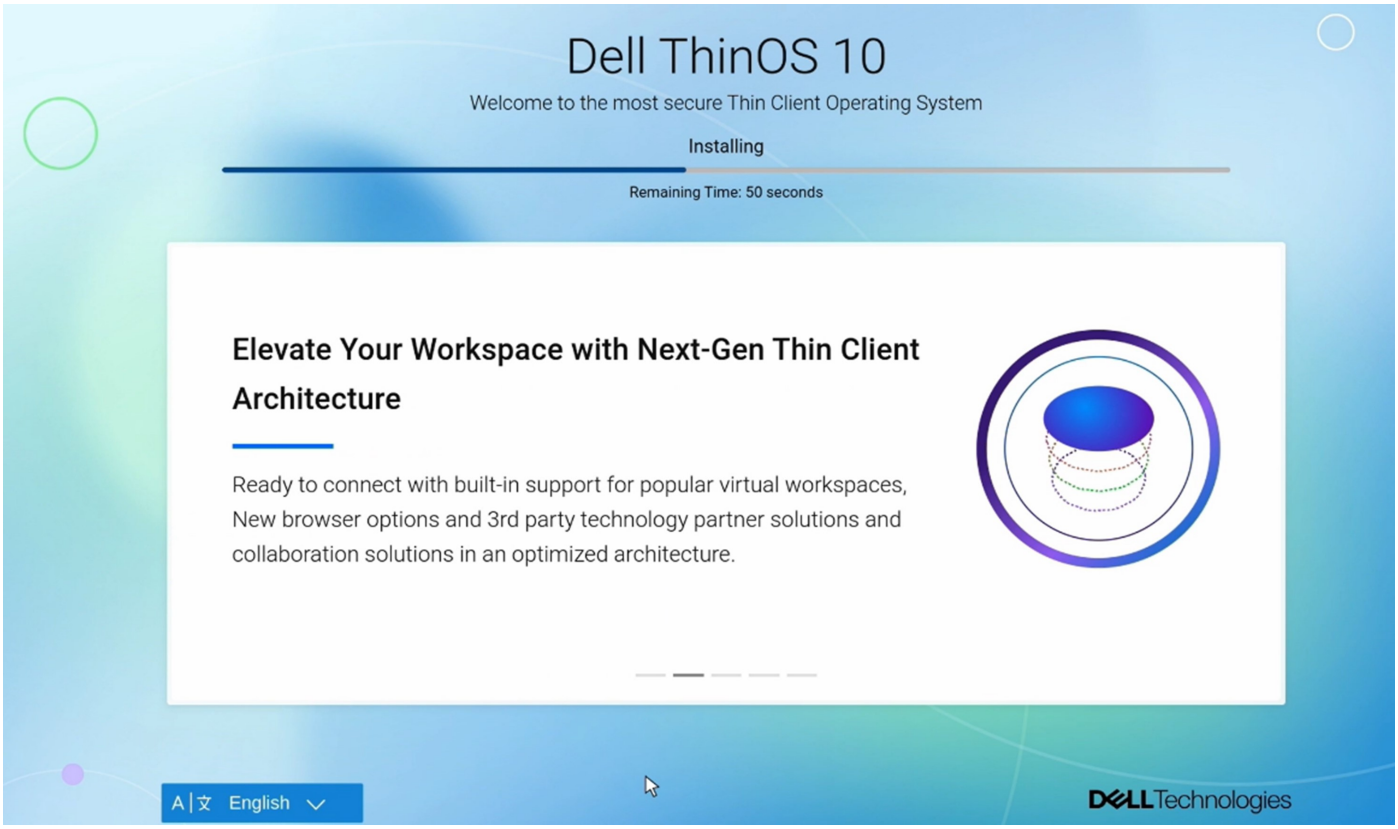

Figure 11. Installation preparation

- **Installing Browser Add-ons**—ThinOS 10 offers a seamless browsing experience with optional commercial browser add-ons for Chrome and Firefox, providing a faster, smoother, and more efficient web browsing experience tailored to individual needs.

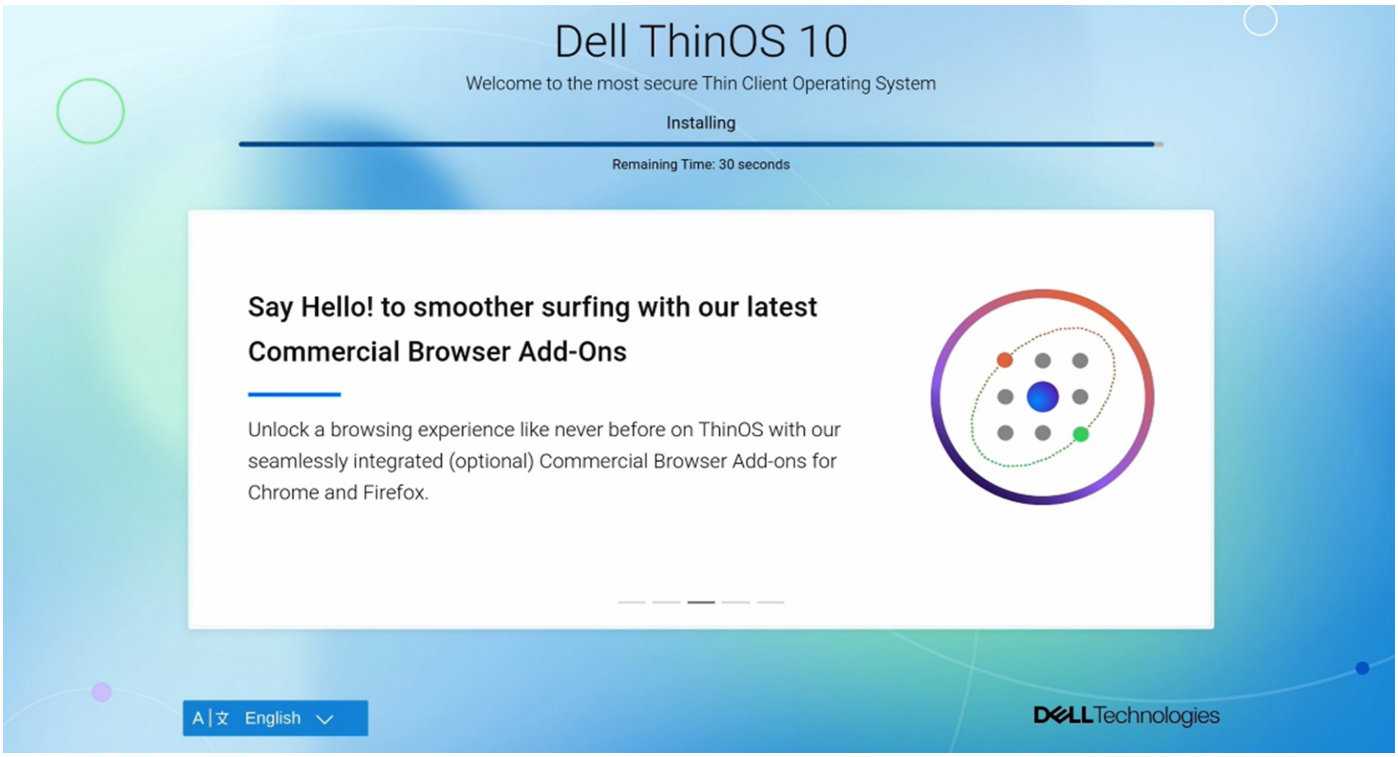

Figure 12. Add-ons installation

- **Simplified User Interface**—ThinOS 10 provides a simplified user interface, featuring a quick start experience and an intuitive taskbar that allows access to session controls and device configuration.

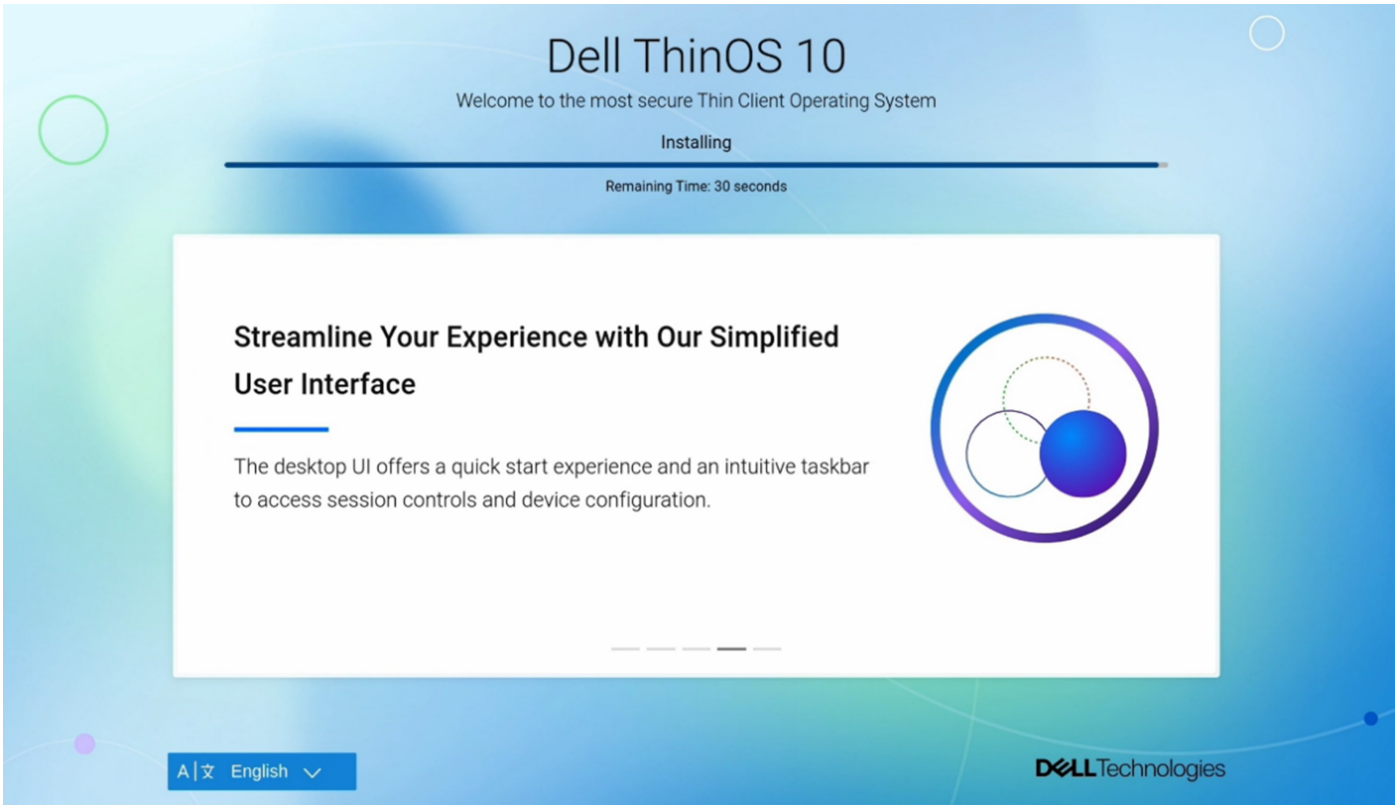

Figure 13. Simplified User Interface

- **Peripheral Support**—ThinOS 10 offers a comprehensive ecosystem that enables seamless peripheral support, centralized management, and optimized performance for virtualized environments, enhancing user productivity.

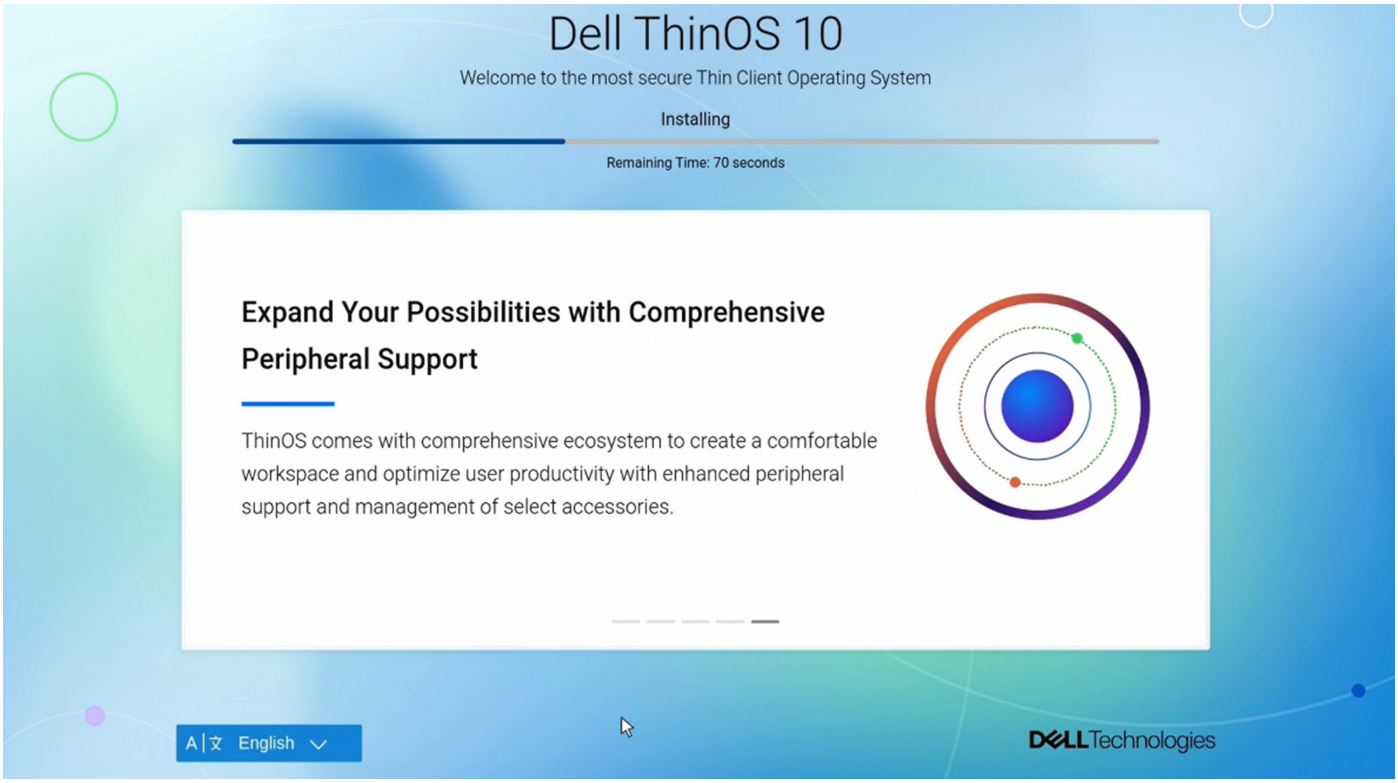

Figure 14. Peripheral support

- **Language Support in ThinOS Installer**—The Installer UI supports 10 languages, including English, Deutsch, Français, Italiano, Español, Polski, Japanese, Simplified Chinese, Traditional Chinese, and Korean, during the installation phase.

Figure 15. Select your language

- **Dell ThinOS is ready**—After language selection and successful installation, the device reboots and displays the final screen, announcing that Dell ThinOS is ready.

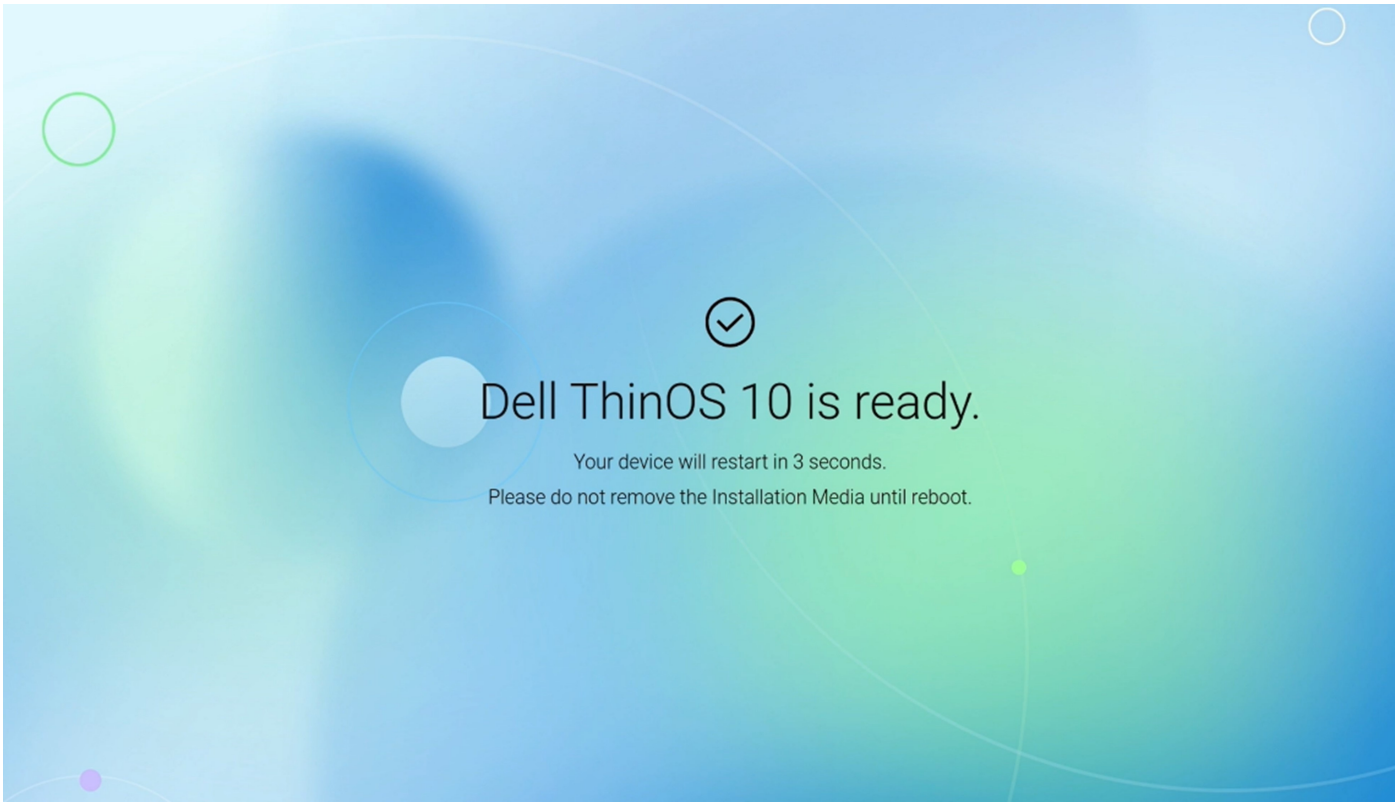

Figure 16. Dell ThinOS is ready

Configure account privileges for ThinOS

Account privilege is used to control the user permission to access Admin Policy Tool and System Menu options. You can change a user privilege to **High**, **Customize**, or **None** from the **Admin Policy Tool** or the Wyse Management Suite console. When you set the user privilege to **Customize**, you can manually select and enable or disable the options in the ThinOS system menu.

The **Administrator Mode** menu in the Admin Policy Tool is disabled by default. You can enable the administrator mode in the Admin Policy Tool or the Wyse Management Suite server, and configure an Administrator username and password.

Configure account privileges using Admin Policy Tool

About this task

This section describes how to configure account privileges using Admin Policy Tool.

Steps

1. From the desktop menu, click **System Setup** > **Admin Policy Tool**.
   The **Configuration Control || ThinOS** window is displayed.
2. Click the **Standard** tab or the **Advanced** tab.
3. Expand **Privacy & Security**.
4. Click **Account Privileges**.
5. Click the **Enable Admin Mode** slider switch if you want to enable the Administrator mode. When enabled, you must specify the Admin username and password.
6. From the **Privilege Level** drop-down list, select a privilege level—**None**, **Customize**, or **High**.

   When you set the user privilege to **Customize**, you can manually select the options that you want to enable or disable in the ThinOS device menu. The **DHCP** option is only available after you enable **Network Setup** and **Granular Control of Peripherals** option is only available after you enable **Peripherals**. **Granular Control of Troubleshooting** option is only available after you enable **Troubleshooting**.
7. Click **Save & Publish**.

Configure account privileges using Wyse Management Suite

About this task

This section describes how to configure account privileges using Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** tab and select your required group.
2. Click **Edit Policies**.
3. Select **ThinOS 10.x** from the drop-down list.
   The **Configuration Control | ThinOS** window is displayed.
4. Click the **Standard** tab or the **Advanced** tab .
5. Expand **Privacy & Security**.
6. Click **Account Privileges**.
7. Click the **Enable Admin Mode** slider switch if you want to enable the Administrator mode. When enabled, you must specify the Admin username and password.
8. From the **Privilege Level** drop-down list, select a privilege level—**None**, **Customize**, or **High**.

   When you set the user privilege to **Customize**, you can manually select the options that you want to enable or disable in the ThinOS device menu. The **DHCP** option is only available after you enable **Network Setup** and **Granular Control of Peripherals** option is only available after you enable **Peripherals**.**Granular Control of Troubleshooting** option is only available after you enable **Troubleshooting**.
9. Click **Save & Publish**.

Connect to a remote server

About this task

This section describes how to manually connect to a remote server.

Steps

1. From the desktop menu, click **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. Click the **Broker Setup** tab and configure the respective VDI broker.
3. Click **Save** and restart the thin client.
   After the thin client restarts, the **Login** dialog box is displayed.
4. Enter the username, password, and domain.
   After authentication is successful, your desktop is presented with your assigned connection that is defined by the broker server.

Connecting a display

Depending on your thin client model, connections to displays can be made using VGA (analog) port, DisplayPort (digital), Mini DisplayPort, USB Type-C port, HDMI, and the proper Dell monitor cables/splitters/adapters.

For more information about ports and connectors, see the hardware documentation of the respective thin clients.

Connecting a printer

To connect a local printer to your thin client, ensure that you obtain and use the correct adapter cables. Before use, you may need to install the driver for the printer by following the printer driver installation instructions. For information about connecting to a printer, see Configuring the printer setup.

Configure WMS settings on the client GUI

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Services**, and click **WMS Settings**.
4. Click **Enable WMS**.
   The option is enabled by default.
5. Enable **Show Advanced Configuration** to display the advanced configuration options.
6. Fill the following fields:
   - **Group prefix**—This field is mandatory.
   - **Group token**—This field is mandatory.
   - **Server**—This field is mandatory.

   NOTE: If you disable, and then enable **Show Advanced Configuration**, all the values that you enter in the mandatory fields are cleared.
7. Enable or disable **CA Validation**.
8. Click **Save & Publish**.

Desktop overview

ThinOS boots to the modern desktop screen. This screen is the default screen that is displayed after you log in to the thin client—without autostart of any connections or applications.

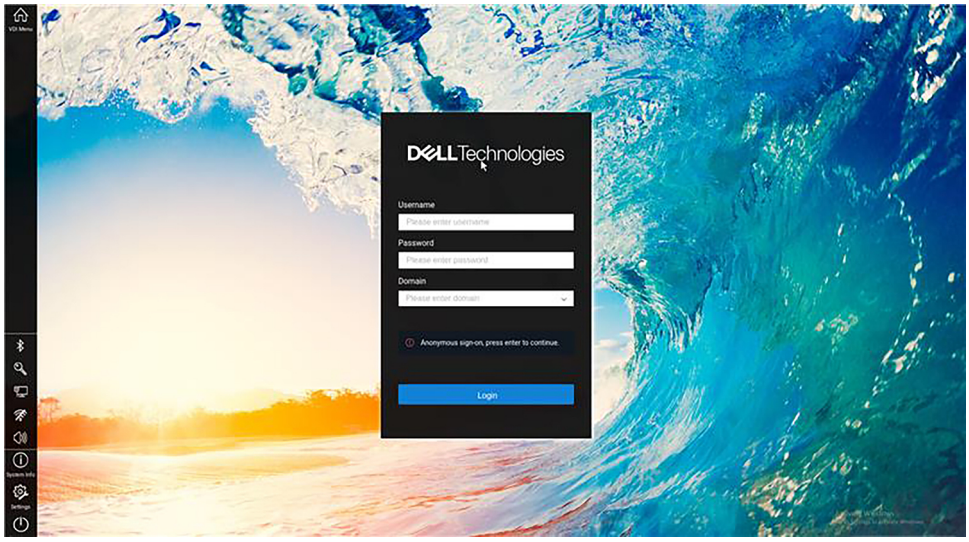

Figure 17. Modern desktop

The ThinOS modern desktop consists of the following screen elements:

- **Floatbar or taskbar**—Contains the system tray area that displays the system icons.
- **Broker login window**—Enables you to log in to the Broker agent session using your login credentials.

Operating modes

This chapter introduces the two ThinOS operating modes—**Appliance Mode**, which is the default mode and provides a locked-down, task-focused user interface, and **Enhanced Mode** is a privileged mode, which enables full access to advanced features and system configuration, including App Builder feature.

Appliance mode

This chapter explains **Appliance Mode**, its key highlights, and when switching to **Enhanced Mode** is required to access advanced functionalities such as the App Builder.

Appliance Mode is the default mode of ThinOS devices and provides a locked-down, task-focused interface.

Switching from **Appliance Mode** to **Enhanced Mode**: When triggered using WMS or APT, this action grants users access to the all applications, including the App Builder, by temporarily relaxing security hardening policies to allow necessary functionality.

The following are the key highlights and limitations of **Appliance Mode**:

- App Builder and other advanced configuration tools are not accessible.
- Only Dell-validated applications can be installed (Customer Installed apps are restricted).
- System is hardened with stricter security controls; no system-level modifications are allowed.
- Switching back from **Enhanced Mode** to **Appliance Mode** triggers a data wipe and system reset (soft or hard reset), resulting in loss of custom data or configuration.

Enhanced Mode

This chapter explains **Enhanced Mode**, its key highlights, and the importance of enabling it for accessing advanced functionalities such as the App Builder.

Enhanced Mode is a privileged operating mode in ThinOS 10.x that allows you to use the **App Builder** feature.

To enable **Enhanced Mode**, use any of the following methods:

- Log in to WMS as an administrator and select **Groups & Configs** > **<Select a group>** > **Edit Policies** > **ThinOS10.x** > **Advanced** > **Desktop Mode** > **System Operating Mode**, click **Enable Enahanced Mode**.
- Open APT on the device and select **Advanced** > **Desktop Mode** > **System Operating Mode**, click **Enable Enahanced Mode**.

The following are the key highlights of the **Enahnced Mode** feature:

- **Privileged Access**: Enables internal application like App Builder, unavailable in Appliance mode. It Allows installation of customer installed (CI) application packages through WMS or APT.
- **Security Consideration**: Reduces overall system security, intended for trusted administrators, or controlled development use only.

Switching from **Enhanced Mode** to **Appliance Mode**: When triggered using WMS or APT, this action wipes all local data and performs a hard reset to restore the device to a secured, production-ready state.

NOTE: Ensure that you back up data before switching out of Enhanced Mode. Changes that are made during Enhanced Mode are lost after reverting.

Modern interactive desktop features

The modern desktop mode (formerly zero desktop) has a Dell default background with the floating toolbar or float bar on the screen.

Table 12. Modern desktop shortcuts

Action	Press
Open a selection box for switching between the desktop and currently active connections.	Ctrl+Alt+Down Arrow
Lock the thin client.	Ctrl+Alt+Left Arrow or Ctrl+Alt+Right Arrow
Capture the active window to the clipboard.	Alt+PrintScreen

Enable modern desktop mode

Steps

1. Go to ThinOS 10.x policy settings on Wyse Management Suite or the Admin Policy Tool on ThinOS.
2. Click the **Advanced** tab and expand **Personalization**.
3. Click **User Experience Settings**.
4. From the **System Mode** drop-down list, select **Modern mode**.
5. From the **Color scheme for Modern mode**, select the color that you want.
6. If you do not want the floatbar to be displayed, enable **Disable Floatbar**. The floatbar can only be displayed by pressing the Windows key on the keyboard when focus is on the ThinOS desktop.
7. From the **Show Floatbar when mouse** drop-down list, select the way that you want to show the floatbar when it is hidden.
8. From the **Floatbar Location on Screen** drop-down list, select the location of the floatbar on the screen.
9. In the Screen ID field, enter the Screen ID on which the floatbar should be shown. You must enter a number 0 to 6. 0 specifies the main screen.
10. If you want to minimize the Login window, enable **Show Login Icon on Floatbar/Taskbar** option. You can click the Login window icon on the taskbar to minimize.
11. Click **Save & Publish**.

Modern toolbar or float bar

The modern toolbar or float bar appears at the left or right corner of the modern desktop. However, depending on administrator configurations, the float bar can be removed or hidden. The toolbar is displayed when a user moves the mouse pointer over the left or right edge of the desktop screen.

NOTE: If you set the **Show Floatbar** option to **Fly Over** on either Admin Policy Tool or Wyse Management Suite, you must quickly move the mouse pointer on the desktop.

NOTE: If you set the **Show Floatbar when mouse** option to **Delay** and the **Delay Floatbar Activation in Milliseconds** to 0, the modern float bar is disabled in a full-screen session. If you press Ctrl+Alt+down key combination to switch to the ThinOS desktop, the float bar is not displayed. You must press Windows key on the keyboard to show the float bar. If you change the mouse pointer size to a number greater than three in a Blast session, you must use Ctrl+Alt to exit the session and view the floating bar on the ThinOS modern desktop.

Table 13. Toolbar icons

Icon	Description
VDI menu	Opens the list of available connections.
System Info	Displays thin client device information.
Settings	Opens the System Settings menu to configure thin client device settings and perform diagnostics.
Shutdown	Click the **Shutdown Terminal** icon to use the Shutdown options available on the thin client.
Wireless network	Displays the wireless connection mode. Clicking the wireless icon displays the SSID scan list. You can directly connect to your preferred WiFi. You can view the wireless IP address information in the Wi-Fi icon tooltip.
Wired network	Displays the wired connected mode.
Volume or Sound	Click this icon to increase or decrease the speaker volume or mute the speaker.
Citrix PNA menu	Displays the Citrix connection options such as Refresh, Disconnect, Reconnect, Logoff, and Manage Security Question. **NOTE:** The Citrix PNA menu button is displayed only after you log in to the Citrix Broker agent.
Battery indicator	Hover over the battery indicator to view the remaining battery percentage. This option is applicable only to the Mobile Thin Client.
Smart Card Self-Service	Click this icon to open the smart card self-service window. You can use this window to view the smart card details, change the PIN, and unlock the PIN. This icon is displayed when you connect a smart card reader to the ThinOS client.

List of connections

On the modern toolbar, you can click the **VDI menu** icon to open your list of assigned connections and published applications. Sometimes, the list contains only default connections.

NOTE: The connection options may be available for use, depending on the user privileges.

Table 14. Connection options

Option	Description
Name of the connection	Opens the connection you want to use.
Gear icon	Displays the sub menu.
Add Connection	Allows you to configure or add new connections.
Global Connection Settings	Use the **Global Connection Settings** dialog box to configure settings that affect all the connection in the list.
Search bar	Enables you to search for a particular connection from the list.

Classic desktop features

This section includes information about desktop guidelines, shortcut menu, desktop menu, and Connection Manager.

Desktop guidelines

The classic desktop has a Dell Wyse default background with a horizontal taskbar at the bottom of the screen.

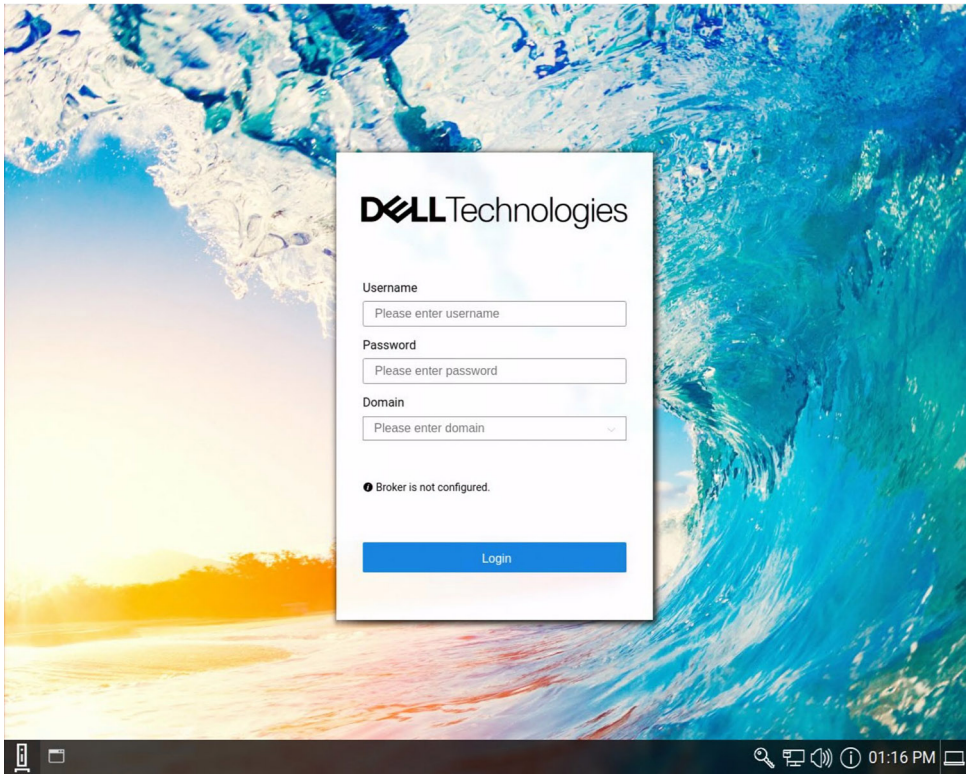

Figure 18. Classic Desktop

Use the following guidelines:

- Icons representing available server connections and published applications are displayed on the desktop. If you pause the mouse pointer over an icon, the information about the connection is displayed. Right-click an icon to open the **Properties** dialog box that displays additional information about the connection. The number of icons that can be displayed on the desktop depends on the desktop resolution and administrator configuration.
- A server connection and published application can be opened by double-clicking a desktop icon. You can also go to the desktop icon by using the tab key and press Enter to initiate the connection.
- Right-clicking the desktop provides a **shortcut menu**.
- Clicking the desktop menu button, or clicking anywhere on the desktop, opens the desktop menu.

Using the taskbar

Use the taskbar to view the date, time, device information, wireless information, volume icon, PNA menu button, and switch to the desktop screen.

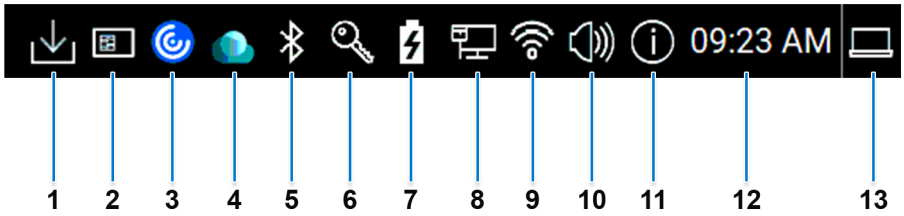

Figure 19. ThinOS Taskbar

1. **Download manager**
2. **Smart card self-service**
3. **Citrix PNA menu**
4. **Omnissa**
5. **Bluetooth**
6. **Security key**
7. **Battery**
8. **Wired network**
9. **Wireless network**
10. **Volume or Sound**
11. **System Information**
12. **Date and time**
13. **Show desktop**

The following table lists the taskbar elements:

Table 15. Taskbar - System tray elements

Element	Description
Show desktop	Click this icon to hide or restore VDI sessions.
Date and time	Displays the date and time.
System Information	Click this icon to view the device information such as general device details, copyright, event logs, Wyse Management Suite status, network connections, and so on. **NOTE:** The Energy Star logo is added to the System Information window of factory shipped OptiPlex 3000 Thin Clients.
Volume or Sound	Click this icon to increase or decrease the speaker volume or mute the speaker.
Wireless icon	• Displays the wireless connection mode. Clicking the wireless icon displays the SSID scan list. You can directly connect to your preferred WiFi. You can view the wireless IP address information in the Wi-Fi icon tooltip. • **Manage Known Networks**: Clicking this option displays all manually added wireless SSIDs. You can select one SSID and click **Forget** to remove it or click **Properties** to modify it. **NOTE:** The wireless SSIDs published from Wyse Management Suite and Admin Policy Tool are not displayed in **Manage Known Networks**.
Wired icon	Displays the wired connected mode.
Battery	Displays the battery percentage. This option is applicable for Wyse 5470 Thin Client.
Security key	Clicking the FIDO2 Security Key Management icon in the ThinOS system tray displays the following features: You can create a PIN, reset your Security Key, and manage your FIDO2 Security Key PIN.
Bluetooth icon	Displays the connection status of Bluetooth devices.
Omnissa	Clicking the Omnissa icon displays the active Blast sessions and Horizon PCoIP sessions list. You can directly view the current sessions and connect to your preferred virtual desktop.

Table 15. Taskbar - System tray elements (continued)

Element	Description
Citrix PNA menu	Click this icon to use the following options: • Refresh • Disconnect • Reconnect • Logoff • Manage Security Question—This option is available when you enable SSPR at the server end. **NOTE:** The PNA menu button is displayed only after you log in to the Citrix broker.
Smart card self service	Click this icon to open the smart card self-service window. You can use this window to view the smart card details, change the PIN, and unlock the PIN. This icon is displayed when you connect a smart card reader to the ThinOS client.
Download manager	Displays the downloaded firmware and packages details.

Taskbar icons are added for all ThinOS windows except the login window and the Admin Policy Tool window. You can use the taskbar icons to minimize and restore the windows.

Table 16. Taskbar - ThinOS local windows icons

Element	Taskbar icon
Network Setup	
Remote Connections	
Central Configuration	
VPN Manager	
System Preferences	
Display	
Peripherals	
Printer Setup	
System Information	
System Tools	
Troubleshooting	
Connection Manager	

Using the shortcut menu

About this task

This section describes how to use the shortcut menu on your thin client.

Steps

1. Right-click on your desktop.
   The shortcut menu is displayed.
2. On the shortcut menu, you can view and use the following options:
   a. **Administrator Mode**—Lets you enter the administrator mode. This option is disabled by default. You must enable the option from the Wyse Management Suite server or Admin Policy Tool.
   b. **Hide all windows**—Brings the full desktop to the foreground.
   c. **Copy to clipboard**—Copies an image of the full screen, current window, or event log to the clipboard. The clipboard contents can be pasted to an Independent Computing Architecture (ICA) session. You can copy the full screen or current window to the clipboard, and can export the screenshots using the **Export Screenshot** option in the **Troubleshooting** dialog box.
   d. **Purge clipboard**—Discards the contents of the clipboard to free up memory. If there are no contents in the clipboard, the **Purge clipboard** option is disabled.
   e. **Lock Terminal**—Puts the thin client in a locked state when the user has logged in to the system with a password. The thin client can only be unlocked using the same password.
   f. **Performance Monitor**—Opens the performance monitor.

Using the desktop menu

About this task

This section describes how to use the desktop menu on your thin client.

Steps

1. Click  or click anywhere on your desktop.
   The desktop menu is displayed.
2. On the desktop menu, use the following options to configure the thin client:
   - **System Setup**—Provides access to the following local system setup dialog boxes:
     - **Network Setup**—Allows selection of DHCP or manual entry of network settings, and server locations.
     - **Remote Connections**—Allows you to configure the Broker agent connection.
     - **Central Configuration**—Allows you to configure the Wyse Management Suite server settings.
     - **VPN Manager**—Allows you to configure the VPN connection.
     - **System Preferences**—Allows you to configure general settings such as screensaver, locale, and time and date.
     - **Display**—Allows you to configure the monitor resolution and rotation.
     - **Peripherals**—Allows you to select the peripherals settings such as audio, keyboard, mouse, serial, camera, and Bluetooth settings.
     - **Printer Setup**—Allows you to configure network printers and local printers that are connected to the thin client.
     - **Admin Policy Tool**—Allows you to configure all the ThinOS settings similar to configuring the settings using Wyse Management Suite.
   - **System Information**—Provides the device information.
   - **System Tools**—Provides information about devices, certificates, and packages.
   - **Troubleshooting**—Displays the performance monitor graphs, trace and event log settings, and other options that are useful for troubleshooting your thin client.
   - **Shutdown**—Allows you to shut down the system, or restart the operating system.

Configure the Connection Manager

The **Connection Manager** has a list of connection entries and command buttons available for use with the connections.

About this task

This section describes how to configure the **Connection Manager** settings.

Steps

1. Go to **System Setup** > **Remote Connections**, and configure the Broker agent setup.
2. Log in to the Broker agent connection.
3. On the taskbar, click  .
   The **Connection Manager** dialog box is displayed.
   NOTE: Nonprivileged users cannot view the Connection Manager.
4. In the **Connection Manager** dialog box, and use the following guidelines:
   - Select a connection from the list, and click **Connect** to establish the VDI connection.
   - Click **Properties** to open the **Connection Settings** dialog box for the selected connection.

   All users can view and edit definitions for the selected connection. Edits are not permanently retained when the user signs-off.

   - Click **Sign-off** to log off from the thin client.
   - If you want to reset a selected virtual connection, select a connection from the list, and click **Reset VM**.
   - Click the **Global Connection Settings** tab to open and configure settings that affect all the connections available in the list.
   - Click **Add** to create an RDP or a PCoIP connection.
   - Click **Delete** to remove the created connection from the list.

Configuring thin client settings and connection broker settings

You can either use the ThinOS local UI or the Wyse Management Suite to do the following:

- Set up your thin client hardware, look and feel, and system settings
  - For configuring these settings using ThinOS local UI, see Configuring connectivity and Configure the thin client local settings.
  - For configuring these settings using Wyse Management Suite, see Edit the ThinOS 10.x policy settings.
- Configure the connection broker settings
  - For configuring these settings using ThinOS local UI, see Configuring the connection brokers.
  - For configuring these settings using Wyse Management Suite, see Edit the ThinOS 10.x policy settings.

Configure ThinOS using Admin Policy Tool

ThinOS 10.x config does not support FTP, HTTP, HTTPS file server, and INI parameter settings. You can configure these settings using a local management tool called Admin Policy Tool.

NOTE: After you reset the thin client to factory default settings, the device starts the First Boot Wizard application by default. You can use the Admin Policy Tool to change the default settings after First Boot Wizard.

Configure the Admin Policy Tool

Steps

1. From the desktop menu, click **System Setup** > **Admin Policy Tool**.
   The **Configuration Control | ThinOS** window is displayed.
2. Click the **Standard** tab or the **Advanced** tab.

   The **Standard** tab lists all the common settings. The **Advanced** tab lists all the advanced settings.
3. Expand the options that you want to configure.
4. In the respective fields, click the option that you want to configure.
5. Click **Save & Publish**.

Feature list of Admin Policy Tool

The following table displays the list of features that are supported by the Admin Policy Tool in ThinOS.

Table 17. Admin Policy Tool

Feature	Subfeature	Restart required
Region & Language Settings	Region & Language	No
Privacy & Security	Account Privileges	No
Privacy & Security	Certificates	No
Privacy & Security	Security Policy	Yes, you must restart the client for all changes to take effect.
Privacy & Security	SCEP	No
Privacy & Security	Device Security	Yes, you must restart the client for all changes to take effect.
Broker Settings	Global Broker Settings	No
Broker Settings	Citrix Virtual Apps and Desktops Settings	No
Broker Settings	Omnissa Horizon Settings	No
Broker Settings	Azure Virtual Desktop Settings	No
Broker Settings	Microsoft Remote Desktop Settings	No
Broker Settings	Amazon WorkSpaces Settings	No
Session Settings	Global Session Settings	No
Session Settings	Citrix Session Settings	No
Session Settings	Blast Session Settings	No
Session Settings	Horizon Session Settings	No
Session Settings	RDP and AVD Session Settings	No
Browser Settings	Global Browser Settings	No
Browser Settings	Browser Shortcuts	No
Browser Settings	Firefox Settings	No
VDI Configuration Editor	Citrix Configuration Editor	Yes, you must restart the client for all changes to take effect.
VDI Configuration Editor	Horizon Blast Configuration Editor	Yes, you must restart the client for all changes to take effect.
VDI Configuration Editor	Zoom Plugin Configuration Editor	Yes, you must restart the client for all changes to take effect.
Login Experience	3rd Party Authentication	No

Table 17. Admin Policy Tool (continued)

Feature	Subfeature	Restart required
Login Experience	Smart card Settings	Yes, you must restart the client for all changes to take effect.
Login Experience	Login Settings	No
Login Experience	Session Settings	No
Personalization	Shortcut Keys	Yes, you must restart the client for all changes to take effect.
Personalization	Device Info	No
Personalization	Desktop	Yes, you must restart the client for all changes to take effect.
Personalization	Screen Saver	No
Personalization	User Experience Settings	No
Peripheral Management	RFIdeas Reader	No
Peripheral Management	Printers	No
Peripheral Management	Audio	Yes, you must restart the client for all changes to take effect.
Peripheral Management	Touch	No
Peripheral Management	Touchpad	No
Peripheral Management	Serial Port	Yes, you must restart the client for all changes to take effect.
Peripheral Management	USB Redirection	No
Peripheral Management	Monitor	No
Peripheral Management	Mouse	No
Peripheral Management	Camera	No
Peripheral Management	Keyboard	No
Peripheral Management	Device Headset Settings	Yes, you must restart the client for all changes to take effect.
Peripheral Management	CCID	Yes, you must restart the client for all changes to take effect.
Peripheral Management	Device Driver	Yes, you must restart the client for all changes to take effect.
Firmware	OS Firmware Updates	No
Firmware	Application Package Updates	No
Firmware	BIOS Firmware Updates	No
System Settings	Power and Sleep Settings	No
System Settings	Scheduled Reboot Settings	No
System Settings	Scheduled Shutdown Settings	No
System Settings	Device Settings	No
System Settings	Device Monitoring	No
Network Configuration	Ethernet Settings	No
Network Configuration	DHCP Settings	No

Table 17. Admin Policy Tool (continued)

Feature	Subfeature	Restart required
Network Configuration	DNS Settings	No
Network Configuration	VPN Settings	No
Network Configuration	Bluetooth Settings	Yes, you must restart the client for all changes to take effect.
Network Configuration	Proxy Settings	No
Network Configuration	Wireless	Captive Portal requires a reboot to take effect.
Network Configuration	Common Settings	No
Network Configuration	SNMPV3 Settings	No
Services	Remote Shadow Settings	No
Services	WMS Settings	No
Services	Troubleshooting Settings	No
Services	WDA Settings	No
BIOS	Dell Wyse 5070	Yes, you must restart the client for all changes to take effect.
BIOS	Dell Wyse 5470	Yes, you must restart the client for all changes to take effect.
BIOS	Dell Wyse 5470 AIO	Yes, you must restart the client for all changes to take effect.
BIOS	Dell OptiPlex 3000	Yes, you must restart the client for all changes to take effect.
BIOS	Dell Latitude 3440	Yes, you must restart the client for all changes to take effect.
BIOS	Dell Latitude 5440	Yes, you must restart the client for all changes to take effect.
BIOS	Dell Latitude 5450	Yes, you must restart the client for all changes to take effect.
BIOS	Dell OptiPlex All-in-One 7410	Yes, you must restart the client for all changes to take effect.
BIOS	Dell OptiPlex All-in-One 7420	Yes, you must restart the client for all changes to take effect.

Important information

- If you are using the **Device Security Allow List Policy** setting, you must first specify **Hub, HID** in the **Class** field by adding a row in **Advanced** > **Device Security** section in the Admin Policy Tool. If you do not add **Hub, HID** to the Allow list, all USB devices are inaccessible when connected to the thin client. You must restart the thin client for the changes to take effect.
- It is not recommended to set **Vendor and Product ID** and **Class** simultaneously in one row. However, if you configure both options simultaneously, the device first checks the **Vendor and Product ID** followed by the **Class** list.
- When you configure the Bluetooth, VNCD server, Bluetooth, VNC Server, NetID License, Serial Port, and Device Security settings using the Admin Policy Tool, ensure that you restart the thin client for the settings to take effect.

Locking the thin client

ThinOS enables you to lock your thin client so that no credentials are required to unlock and use the thin client again. This option is enabled by default. To disable the option, go to **Advanced** > **Login Experience** > **Login Settings** from the Admin Polity Tool or the Wyse Management Suite Policy Settings, and disable **Lock Terminal**.

The **Unlock Terminal Count** is added in **Advanced > Login Experience > Login Settings**. The policy limits the number of tries for unlocking the terminal. If the number of retries exceeds the set number, you can retry again after 15 minutes or sign off or restart the thin client.

NOTE: A lock terminal command from Wyse Management Suite takes priority over the settings and locks the thin client even if the setting is disabled.

Shut down and restart

About this task

This section describes how to use the **Shutdown** dialog box to either shutdown the computer or restart the computer.

Steps

1. From the desktop menu, click **Shutdown**.
   The shutdown dialog box is displayed.
2. Click any of the following options:
   - **Shutdown the system**—Enables you to shut down the computer.
   - **Restart the system**—Enables you to restart the operating system.
3. Click **OK** to save settings.

   NOTE: When you update the operating system, BIOS, or application, a **Notice** dialog box is displayed with **Update Now**, **Next Reboot**, and **Schedule Update** options. If you have clicked **Next Reboot** or **Schedule Update** to defer the operating system, BIOS, or application installation, the shutdown window asks to **Update and shut down** or **Update and restart** with a yellow dot on their respective icons. ThinOS updates first before shutting down or restarting and the **Sleep** option is hidden. **Reset the system settings** is disabled in the **Shutdown** window.

Scheduled Shutdown

Using this option, you can specify a time and a day to shut down the device automatically.

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **System Settings**, and click **Scheduled Shutdown Settings**.
4. Click the **Enable Auto Shutdown** toggle switch to enable the feature.
5. You can use the following settings:
   - **Shutdown after Idle Time**—The client shuts down only if it is left idle for the time that you specify here.
   - **Scheduled Shutdown Time**—Set a time window for the client to shut down. Specify the time in a 24-hour format.
   - **Shutdown Day**—Specify the days when you want the shutdown to happen.
   - **Shutdown Week No.**—Use this option to select a minimum time period to trigger a shutdown from the last shutdown.
6. Click **Save & Publish**.

   NOTE: If you change the time zone on the local client, **Scheduled Shutdown Settings** take effect only after a reboot.

Scheduled Reboot

Using this option, you can specify a time and a day to reboot the device automatically.

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **System Settings**, and click **Scheduled Reboot Settings**.
4. Click the **Enable Auto Reboot** toggle switch to enable the feature.
5. You can use the following settings:
   - **Reboot after Idle Time**—The client reboots only if it is left idle for the time that you specify here.

- **Scheduled Reboot Time**—Set a time window for the client to reboot. Specify the time in a 24-hour format.
- **Reboot Day**—Specify the days when you want the reboots to happen.
- **Reboot Week No.**—Use this option to select a minimum time period to trigger a reboot from the last reboot.

6. Click **Save & Publish**.

NOTE: If you change the time zone on the local client, **Scheduled Reboot Settings** take effect only after a reboot.

Enable or disable shutdown

This option disables the **Shutdown** option in the ThinOS **Shutdown** window, and also disables the physical shutdown button on the thin client.

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Login Experience**, and click **Login Settings**.
4. Click the **Disable Shutdown** toggle switch under **Login Experience** to enable or disable the shutdown.
5. Click **Save & Publish**.

Battery information

This section is only applicable to mobile thin clients. The battery indicator is displayed on the system tray.

The following table contains the battery indicators:

Table 18. Battery indicators

Battery status	Icon
While charging with the AC adapter	
Battery 90% - 100% without connecting the AC adapter	
Battery 50% - 89% without connecting the AC adapter	
Battery 25% - 49% without connecting the AC adapter	
Battery 9% - 24% without connecting the AC adapter	
Battery 0% - 8% without connecting the AC adapter	

- When the battery is lower than 12%, a notification is displayed at the right-bottom with the remaining percentage.
- Plugging in the AC adapter to charge the device increases brightness by 10% and disconnecting the AC adapter decreases brightness by 10%.
- By default, the critical battery level is 5%. When the battery reaches the critical level, ThinOS is turned off automatically. You must plug in the AC power to power on the thin client.

Login dialog box features

The **Login** dialog box enables you to do the following tasks:

- Log in broker to the configured server connection.

- Change or reset your own password, and unlock your account.

View the system information

Use the **System Information** dialog box to view the system information. You can either click **System Information** from the desktop menu or the **System Information** icon on the taskbar.

The **System Information** dialog box includes the following elements:

- **General tab**—Displays the following information:
  - System version
  - Terminal name
  - Serial number
  - System Up Time
  - AssetTag—This element is displayed only when Asset Tag is set in BIOS Setup.
  - Memory size
  - Memory Usage
  - CPU Speed—The CPU speed changes dynamically.
  - SSD size—The storage size of the SSD/eMMC on which ThinOS is installed.
  - CPU Utilization
  - Monitor
  - Main Resolution
  - Parallel ports
  - Serial ports
  - Battery—mobile thin clients only
  - Remaining time—mobile thin clients only
- **Copyright tab**—Displays the software copyright and patent notices. Click the **Acknowledgments** button to view the information that is related to third-party software.
- **Event Log tab**—Displays the thin client start-up steps beginning from system version to checking firmware or error messages that are helpful for debugging issues. The number of displays and USB devices that are connected to the thin client, and the Bluetooth initialization are also displayed.
- **ENET tab**—Displays information about wired network connections.
- **WLAN tab**—Displays information about wireless network connections.
- **About tab**—Displays the following information:
  - Platform name
  - Operating system
  - Build name
  - Build version
  - BIOS name
  - BIOS version
  - Activation License
  - Citrix Workspace App version
  - Omnissa Horizon
  - AVD
  - WMS status
  - MQTT server

NOTE:

- **Kernel mode**—The components are implemented in the Kernel according to the specification. The version is displayed as [max].[min], which is the base version of the protocol or server or client of the component.
- **User mode**—The components are from the source, or binaries from third-party software that are compiled or integrated into the ThinOS operating system. The version is displayed as [max].[min].[svn_revision]. The [max] and [min] is the base version of the third component, and the [svn_revision] is the source control revision of ThinOS. Using the ThinOS specified version, you can identify the changes between different revisions. For example, the Citrix Workspace App version is 24.11.0.85.71. The components are matched to the installed packages. If the packages are removed, the field remains empty in the **About** tab.

Sleep mode

The sleep mode enables the power-saving state and quickly resumes full power operations without loss of data.

The USB interface is closed in sleep mode. All USB devices such as USB drives, Bluetooth, audio devices, video devices, and cameras are reinitialized after resuming from sleep mode.

The wired network, wireless network, and VPN are disconnected in sleep mode. However, the network configurations are saved.

All the ThinOS configurations—VDI configuration, network configuration, and so on—are saved automatically in sleep mode. If you are signed in to a broker agent, all the windows are closed automatically and signed off when entering sleep mode. If you are not signed on to a broker agent, the windows are not closed when entering sleep mode.

Enable sleep manually

To enable the **Sleep** option manually, use either of the following options:

- **ThinOS lock window**—To enter sleep mode using the ThinOS lock window, do the following:
  1. Lock your thin client.
  2. In the ThinOS lock window, click **Sleep**.
  3. Click **OK**.
- **Shutdown dialog box**—To enter sleep mode using the **Shutdown** dialog box, do the following:
  1. Open the **Shutdown** window.
  2. Click **Sleep**, and then click **OK**.

You can wake the thin client from sleep mode by pressing the power button, any key on the keyboard, or by clicking the mouse button. To use the USB keyboard or mouse to wake your thin client, you must enable wake on USB in the BIOS.

Import certificates to ThinOS from Admin Policy Tool or Wyse Management Suite

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Configuration Control | ThinOS** window, click the **Advanced** tab.
3. Expand **Privacy & Security**, and click **Certificates**.
4. Click the **Auto Install Certificates** slider switch to enable autoinstall of certificates on ThinOS.
5. Browse and select the certificate that you want to upload.

   NOTE: Admin Policy Tool supports the `.cer`, `.crt`, `.pfx`, `.der`, and `.pem` certificate file types. Wyse Management Suite supports `.cer`, `.crt`,`.pfx`, `.der`, and `.pem` certificate file types.

6. From the **Select Certificates to Upload** drop-down list, select the certificate that you have uploaded.
7. Click **Save & Publish**.
   The certificate is installed on your thin client.

ThinOS system variables

ThinOS uses system variables or part of a system variable when defining command values. System variables are often used to define unique values for fields such as terminal name or default user. For example, if the client has an IP address 123.123.123.022, ACC&Right($FIP,3) results in a value of ACC022. Using system variables makes it easier to manage groups of devices that require a unique terminal name or default user.

The following are the ThinOS system variables:

Table 19. ThinOS system variables

Variable	Description
$IP	IP address
$IPOCT4	The fourth octet of the IP Address, for example: if the IP address is 10.151.120.15, then the value is **15**.
$MAC	Mac address
$CMAC	Mac address with colon.
$UMAC	Mac address with uppercase letters is used.
$DHCP (extra_dhcp_option)	Extra DHCP options for ThinOS unit, including 169, 140, 141, 166, 167. For example, set a string **test169** for the **tag169** option in the DHCP server, and set **TerminalName=$DHCP(169)** in the Wyse Management Suite policy. Check the terminal name in the UI, and the terminal name is **test169**. **166** and **167** is default for the Wyse Management Suite MQTT Server and Wyse Management Suite CA validation in ThinOS. You must remap the options from the UI or the Wyse Management Suite policy if you want to use **$DHCP(166)** or **$DHCP(167)**.
$DN	Sign on domain name
$TN	Terminal name
$UN	Sign on username
$SUBNET	For subnet notation, the format is **{network_address}_{network_mask_bits}**. For example, if the IP address is 10.151.120.15, the network mask is 255.255.255.0, and 10.151.120.0_24 is used.
$FIP	IP address is used in fixed format with three digits between separators. For example, 010.020.030.040.ini. Using it with the left or right modifier helps to define policy for the subnet. For example, include=&Left($FIP,11).ini is specified to include file 010.020.030.ini for subnet 010.020.030.xxx.
$SN	Serial number or Service tag
$VN	Version number
Right($xx, i) or and Left($xx, i)	Specifies that the variable is to be read from left or right. The **$xx** is any of above parameters, and the parameter **i** specifies the digits for the offset of right or left.
&Right($xx, i) or &Left($xx, i)	Specifies whether the variable is read from left or right. The **$xx** is any of the above System Variables. The option **i** specifies left or right offset digits. For example, in the parameter **TerminalName=CLT-SNRIGHT$07**, if the Serial Number (or Service Tag number) of the thin client is MA00256, the terminal name of the thin client is assigned as below: • First four characters—CLT- • The rest—The last right-most seven digits of the thin client serial number. The resulting terminal name is displayed as CLT-MA00256.
$AT	**Asset Tag** must be enabled in the BIOS settings. **$AT** can be used as terminal name, and the length is limited to 32 characters.

Manual override

The manual override feature enables users to prevent the Wyse Management Suite configured policies from applying to the device after a particular action is performed on the local ThinOS device. When the manual override feature is enabled, and the user performs the required action on the ThinOS local device, the configured policies from Wyse Management Suite for these settings are not applied to the ThinOS device.

Table 20. Manual override support matrix

Settings	Action to be performed on the ThinOS local device	Default value
DHCP Settings	Click the Save button in the Network Setup window	Disabled
DNS Settings	Click the Save button in the Network Setup window	Disabled
Proxy Settings	Click the Save button in the Network Setup window	Disabled
Ethernet Settings	Click the Save button in the Network Setup window	Disabled
Wireless Settings	Click the Save button in the Network Setup window	Disabled
VPN Settings	Add a new VPN, edit a VPN, or remove a VPN	Disabled
Printers	Click the Save button in the Printer Setup window	Disabled
Audio	Change the audio configuration	Disabled
Mouse	Click the Save button in the Peripherals window	Enabled
Keyboard	Change the configuration under the Keyboard tab in the Peripherals window, and click the OK button	Enabled
Touch pad	Click the Save button in the Peripherals window	Enabled
Monitor	Click the Test button and then click OK in the Display Setup window	Disabled
Region & Language - Region Settings	Change the region configuration and click the OK button	Disabled
Region & Language - Language Settings	Change the language configuration and click the OK button	Disabled
Closing the Lid (Mobile Thin Clients only)	Change **When I close the lid configuration** and click **Save**	Disabled
Login Settings	Change the default credentials in the **General Options** tab in **Remote Connections**	Disabled

5

Configuring the global connection settings

About this task

This section describes how to use the **Global Connection Settings** dialog box to configure the connection settings for ICA, Blast, RDP.

Steps

1. Configure the Broker agent connection on ThinOS. See, Configure the Broker Setup.
2. From ThinOS 10.x 2502, **Modern Mode** and **Classic Mode** feature is available. You can switch to **Classic Mode** from **Settings** > **Admin Policy tool** > **Advanced** > **Personalization** > **User Experience Settings** > **System Mode**.

   NOTE: The ThinOS 10.x 2502 client is configured in Modern Mode by default. The step varies for accessing Global Connection Settings for Modern Mode.

3. To configure **Global Connection Settings**, do the following:
   a. For **Modern Mode** , on the desktop bar, click **VDI Menu**, and click **Global Connection Settings**.
   b. For **Classic Mode**, on the desktop taskbar, click
   
   (**Connection Manager**) and then click **Global Connection Settings**.

   The **Global Connection Settings** dialog box is displayed.
4. Click the **Session** tab and configure the following options:
   - **Settings common to all session**—Select the check boxes to enable options that are applied to all sessions. The available options are:
     - **Launch only once**—Select the check box when you want the session to be launched only once simultaneously.
     - **Re-connect after disconnect**—Select the check box when you want the session to launch again after the connection is disconnected.
     - **Mount disks as read-only**—Select the check box when you want to disable write access for storage disks.
     - **Enable Imprivata VC**—Select the check box when you want the Imprivata VC to be redirected to the remote session. If this option is not selected, RFIDEAS or Fingerprint reader can be redirected into the remote session.
     - **Enable HID Fingerprint Reader**—Select the check box when you want to use HID Fingerprint Reader.
     - **Silent Launch**—Select the check box when you want to launch the session without having a notification or dialog box appearing on the screen.
   - **Auto connect to local devices**—Select the check boxes to automatically connect to local devices, such as printers, serials, smart cards, sound devices, and disks at system startup.

     If you want to use the **Disks** option to connect to sessions automatically, ensure that:

     - More than one disk can be used simultaneously. However, the maximum number of USB drives including different subareas is 12.
     - You save all data and sign off from the session before removing the USB drive.
   - **USB device redirection**—Select this check box to allow USB devices to be redirected to the remote session. The available options are:
     - **Exclude disk devices**—Select the check box when you do not want disk devices to be redirected to the remote session.
     - **Exclude printer devices**—Select the check box when you do not want printer devices to be redirected to the remote session.
     - **Exclude audio devices**—Select the check box when you do not want audio devices to be redirected to the remote session.
     - **Exclude video devices**—Select the check box when you do not want video devices to be redirected to the remote session.
5. Click the **ICA** tab, and do the following:
   a. Select the check boxes to enable the options that are applied to all sessions. The available options are:
      - **Seamless window mode**—Select this check box when you want to launch applications and desktops seamlessly.

- **Desktop with fullscreen mode**—Select this check box when you want to launch the desktop session in fullscreen.
- **Enable HDX/MMR**—Select the check box when you want to enable the Multimedia Redirection feature. When this option is enabled, the audio and video is rendered on the endpoint device instead of the server.
- **Enable session reliability**—Select the check box when you want the session to remain active when the network connection is unstable.
- **Enable UDP audio**—Select the check box when you want the Citrix connections to use audio over User Datagram Protocol (UDP).

b. From the **Audio Quality** drop-down list, select an audio quality that is optimized for your connection.

6. Click the **Blast** tab, and select the check boxes to enable the options that are applied to all sessions. The available options are:
   - **Allow BlastCodec decoding**— Select the check box when you want to enable the Blastcodec decoding in Horizon Client. Enabling this option decodes high-end third-party applications, and enhances the performance.
   - **Allow H.264 decoding**—Select the check box when you want to enable the H.264 decoding in Horizon Client. Enabling this option improves the performance of high-end applications. H.264 is enabled by default.
     - **Allow High Color Accuracy**—Select the check box when you want to allow Horizon Client to use a superior color fidelity when H.264 decoding is enabled.
7. Click the **RDP** tab, and do the following:
   a. Select the check boxes to enable the options that are applied to all sessions. The available options are:
      - **Enable NLA**—Select the checkbox when you want to verify users before connecting to an RDP direct connection.
      - **Force Span**—Select the check box when you want to span the session horizontally across two displays. This option enables you to use two displays as one large display.
      - **Record from Local**—Select the check box when you want to enable recording from a local microphone.

   b. **Audio Playback** option determines the audio playback mode and works for the sessions that are published through the broker.
   c. In the **Desktop Scale Factor** box, enter the DPI value in percentage. This option enables you to define the desktop DPI remotely. The Desktop Scale Factor is only applicable for the RDP connection. Setting this option does not impact the display scale of the thin client locally. The DPI range is 100–500. If you enter a nonnumeric character, the value is automatically set to 100. If you enter a value less than 100, the value is automatically set to 100. If you enter a value higher than 500, the value is automatically set to 500.
8. Click **Save** to save your settings.

6

Configuring connectivity

This chapter helps you understand various configuration settings for a secure connection. To configure the settings on ThinOS desktop:

- For **Modern Mode** , click **Settings** from the desktop menu, and use the configurations tabs.
- For **Classic Mode**, click **System Setup** from the desktop menu, and use the configuration tabs.

Configuring the network settings

Use the network options to configure the network connection based on your requirement.

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.

If you disable IPv4 or IPv6 in Wyse Management Suite policy settings or the Admin Policy Tool, then post reboot, the ThinOS client fails to resolve a hostname to IPv4 or IPv6 address using DNS server.

Configure Dynamic Host file settings using WMS or APT

Explains how ThinOS 10.x enables IT administrators to configure dynamic host file settings using WMS or APT. This feature allows effortless mapping of host names to IP addresses, ensuring flexible and efficient session connectivity management.

About this task

After completing the configuration steps, ThinOS 10.x automatically applies the updated host file entries during operation. The system maintains these settings across reboots, upgrades, and downgrades, ensuring consistent and reliable host resolution without requiring additional administrative action.

Steps

1. To configure dynamic host file settings, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **System Settings** > **Device Settings** > **Host File Settings**.
3. In **Host IP Address** input field, enter the required IP Address.
4. In **Host Name** input filed, enter the required Host Name.
5. Click **Save & Publish**.

Configure the general settings

About this task

This section describes how to configure the general network settings on your thin client.

Steps

1. To access the network settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **Network Setup**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Network Setup**.

The **Network setup** dialog box is displayed.

2. Click the **General** tab, and do the following:

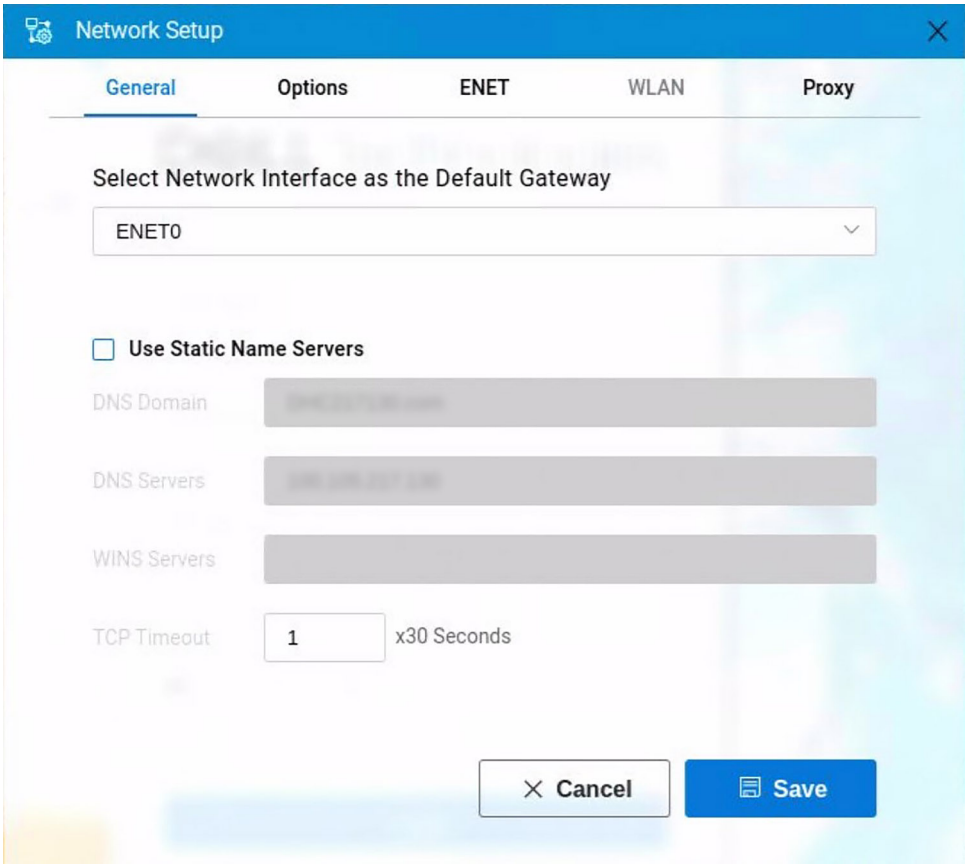

Figure 20. General tab

NOTE: If network interfaces are in the same subnet, connection to the same subnet is prioritized last by the interface to fetch the IP address. Connections to the other subnets are prioritized in the order ENET0, ENET1, and WLAN.

a. To set a default gateway, select the type of network interface from the **Select Network Interface as the Default Gateway** drop-down list.

   ThinOS supports the dual IPv6 network interface. The following network combinations are supported:

   - Wired connection 1 + Wireless connection 1
   - Wired connection 1 + Wired connection 2

   NOTE: The limitation of the dual network is that the device cannot automatically determine which connection to use among the two.

b. **Use Static Name Servers**—By default, this check box is not selected, and the thin client fetches the server IP address from DHCP. To manually assign the static IP addresses, select the **Use Static Name Servers** check box and do the following:

   NOTE: If name servers are changed, the details are displayed in event logs. In dynamic mode, the DNS can be merged from Ethernet and wireless, or from Ethernet 0 and Ethernet 1.

   NOTE: You can upload the host file using the Wyse Management Suite policy settings or the Admin Policy Tool. To upload the file, go to **Advanced** > **System Settings** > **Device Settings** from the Wyse Management Suite policy settings or the Admin Policy Tool, and click **Browse...** next to **Select Host File**. ANSI or UTF-8 encoding is supported, and the maximum supported file size is 10 KB.

   i. Enter the URL address of the DNS domain in the **DNS Domain** field.

      NOTE: You can use multiple DNS domain suffixes. Use ; to separate values.

ii. Enter the IP address of the DNS server in the **DNS Server** field.

NOTE: The use of DNS is optional. DNS enables you to specify remote devices by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. Ensure that you use the DNS domain and the network address of an available DNS server. The function of the DNS domain entry is to provide a default suffix that is used to resolve the name. The values for these two fields may be supplied by a DHCP server. If the DHCP server supplies these values, they replace any locally configured values. If the DHCP server does not supply these values, the locally configured values are used. On ThinOS, error tips are displayed when you set an invalid DNS server. A window with the error message is displayed when you click save the invalid DNS server.

NOTE: You can enter the server addresses, each separated by a semicolon. The character limit is 256. The first address is for the primary DNS server, and the rest are secondary DNS servers or backup DNS servers.

c. Enter the IP address of the WINS server in the **WINS Server** field.

NOTE: Only one WINS server is supported. However, the use of WINS is optional. You must specify the network address of an available WINS name server. WINS enables you to specify remote devices by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. These entries can be supplied through DHCP, if DHCP is used. DNS and WINS provide essentially the same name resolution. If both DNS and WINS are available, the thin client attempts to resolve the name using DNS first and then WINS. You can enter a single WINS Server address.

d. Enter the digit multiplier of 30 s in the **TCP Timeout** box to set the time-out value of a TCP connection. The value must be either 1 or 2 which means the connection time-out value is from 1 x 30 = 30 s to 2 x 30 = 60 s. Setting the time-out period retransmits the sent data and tries to connect to the server again until the connection is established.

3. Click **Save** to save your settings.

Configure the DHCP options settings

About this task

This section describes how to configure the DHCP options settings on your thin client.

Steps

1. To access the network settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **Network Setup**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Network Setup**.

   The **Network setup** dialog box is displayed.
2. Click the **Options** tab, and do the following:

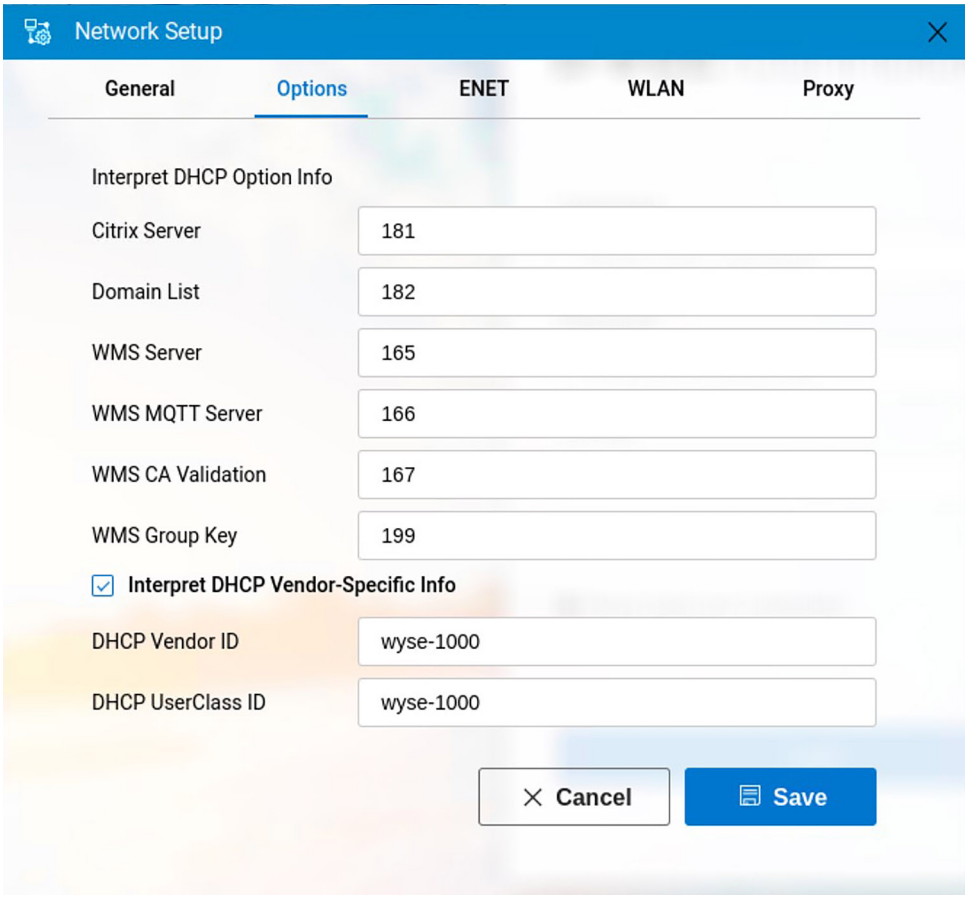

Figure 21. Options tab

a. **Interpret DHCP Option IDs**—Enter the supported DHCP options. Each value can only be used one time after you reset your device to factory default settings.

Table 21. DHCP option tags

Option	Description	Additional information
165	Wyse Management Suite server	Optional string. Specifies the IP address of the Wyse Management Suite server.
166	Wyse Management Suite MQTT server	Optional string. Specifies the IP address of the MQTT server.
167	Wyse Management Suite CA Validation	Optional string. Specifies the CA validation.
181	PNAgent/ PNLite server list	Optional string. The thin client uses the server to authenticate the credentials of the user. The device obtains a list of ICA published applications valid for the validated credentials. The user supplies those credentials when logging in to the thin client.
182	NT domain list for PNAgent/ PNLite	Optional string. The thin client creates a drop-down list of domains from the information that is supplied in the option tag. The list is available during thin client login in the order that is specified in the DHCP option. For example, the first domain that is specified becomes the default option. The selected domain must authenticate the user ID and password. Only the selected domain is used in the authentication process. If the domain list is incomplete and the user credentials must be verified against a domain not in the list, type a different domain name during login. This is based on the assumption that the server in option 181 can authenticate against a domain that is not available in the list.

Table 21. DHCP option tags (continued)

Option	Description	Additional information
199	Wyse Management Suite group registration key	Optional string. Specifies a Wyse Management Suite group registration key for the Wyse Management Suite agent. When Wyse Management Suite is disabled, and the group key of Wyse Management Suite is null, this option takes effect. Wyse Management Suite uses the optional string as the group registration key. If the Wyse Management Suite server or the MQTT server is null, the Wyse Management Suite agent sets the values to the default server values.

b. **Interpret DHCP Vendor-Specific Info**—Select this check box for automatic interpretation of the vendor information.
c. **DHCP Vendor ID**—Displays the DHCP vendor ID when the **Dynamically allocated over DHCP/BOOTP** option is selected.
d. **DHCP UserClass ID**—Displays the DHCP user class ID when the **Dynamically allocated over DHCP/BOOTP** option is selected.

3. Click **Save** to save your settings.

NOTE: The User Class option for the DHCP standard is RFC 2132.

Configure the ENET settings

About this task

This section describes how to configure the Ethernet settings on your thin client.

Steps

1. To access the network settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **Network Setup**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Network Setup**.

   The **Network setup** dialog box is displayed.
2. Click the **ENET** tab, and do the following:

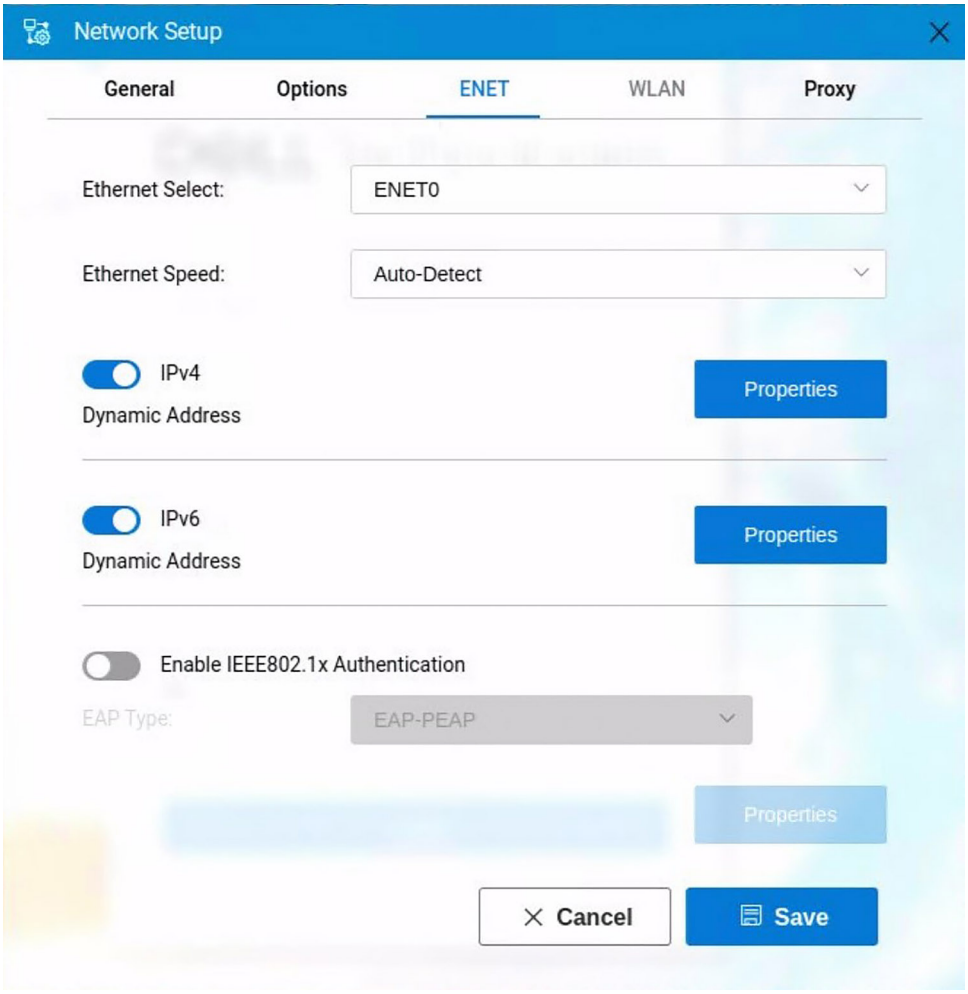

Figure 22. ENET tab

a. From the **Ethernet Select** drop-down list, select a wired network connection.

b. From the **Ethernet Speed** drop-down list, select a value for the Ethernet speed. The default value is **Auto-Detect**. If your network equipment does not support the automatic negotiation, select any of the following values:

- **10 Mbps Half-Duplex**
- **10 Mbps Full-Duplex**
- **100 Mbps Half-Duplex**
- **100 Mbps Full-Duplex**
- **1 Gbps Full-Duplex**

NOTE: The **10 Mbps Full-Duplex** value can be selected locally. However, this mode can be negotiated through **Auto-Detect**.

c. Click the **IPv4** button, and then click **Properties** to configure the following options:

- **Dynamically allocated over DHCP/BOOTP**—Select this option to enable your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server by using DHCP options to provide information. Any value that is entered locally in the **Options** tab is replaced by the DHCP value. If the DHCP server fails to provide replacement values, the locally entered value is used.
- **Statically specified Address**—Select this option to manually enter the IP address, subnet mask, and default gateway.
  - **IP Address**—Enter a valid network address in the server environment. The network administrator must provide this information.
  - **Subnet Mask**—Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices—**same subnet** or **other subnet**. If the location is a different subnet, messages that are sent to that address must be sent through the default gateway. This does not depend on the value that is specified through local configuration or through DHCP. The network administrator must provide this value.

- **Default Gateway**—Use of gateways is optional. Gateways are used to interconnect multiple networks—routing or delivering IP packets between them. The default gateway is used for accessing the Internet or an intranet with multiple subnets. If no gateway is specified, the thin client can only address other systems on the same subnet. Enter the address of the router that connects the thin client to the Internet. The address must exist on the same subnet as the thin client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.

d. Click the **IPv6** button, and on the **Properties** tab, configure the following options:

NOTE: The limitation of the dual IPv6 network is that the device cannot automatically determine which connection to use among the two.

- Select the **Dynamically allocated over DHCP/BOOTP** option to enable your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server (using DHCP options) to provide information. Any value that is entered locally in the **Options** tab is replaced by the DHCP value. If the DHCP server fails to provide replacement values, the locally entered value is used.

  NOTE: Dynamically Allocated over DHCP/BOOTP option is by default enabled.

- Select the **Statically specified Address** option to manually enter the IP address, subnet mask, and default gateway.
  - **IP Address**—Enter a valid network address in the server environment. The network administrator must provide this information.
  - **Subnet Prefix Len**—Enter the prefix length of the IPv6 subnet.
  - **Default gateway**—Use of gateways is optional. For more information, see various IPv4-supported options in this section.

e. Select the **Enable the IEEE 802.1x authentication** check box, and from the **EAP type** drop-down list, select **TLS**, **LEAP**, **PEAP** or **FAST**.

- **TLS**—Select this option, and click **Properties** to configure the **Authentication Properties** dialog box.
  - Select the **Validate Server Certificate** check box because it is mandatory to validate your server certificate.

    NOTE: The CA certificate must be installed on the thin client. The server certificate text field supports a maximum of approximately 255 characters, and supports multiple server names.

  - Select the **Connect to these servers** check box, and enter the FQDN of the server.
  - Click **Browse** to find and select the client certificate file and the private key file you want.

    NOTE: Ensure that you select the PFX file only.

  - Select either **User Certificate** or **Machine Certificate**, base on your choice.
- **LEAP**—Select this option, and click **Properties** to configure the **Authentication Properties** dialog box. Be sure to use the correct username and password for authentication.
- **PEAP**—Select this option, and click **Properties** to configure the **Authentication Properties** dialog box. Be sure to select either **EAP_GTC** or **EAP_MSCHAPv2**, and then use the correct username, password, and domain. Validate Server Certificate is optional.
- **FAST**—Select this option, and click **Properties** to configure the **Authentication Properties** dialog box. Be sure to select either **EAP_GTC** or **EAP_MSCHAPv2**, and then use the correct username, password, and domain.

  NOTE: During the initial connection with EAP-FAST, when there is a request for a Tunnel PAC from the authenticator, the PAC is used to complete the authentication. The first-time connection always fails, and the subsequent connections succeed. Only automatic PAC provisioning is supported. The user/machine PAC provisioning that is generated with the CISCO EAP-FAST utility is not supported.

When **EAP-MSCHAPV2** or **EAP-GTC** is selected for PEAP or FAST authentication, an option to hide the domain is available. Username and password boxes are available for use, but the **domain** text box is disabled. When **EAP-MSCHAPV2** or **EAP-GTC** is selected for PEAP or FAST authentication, a check box to enable the single sign-on feature is available.

3. Click **Save** to save your settings.

Configure the WLAN settings

About this task

This section describes how to configure the wireless settings on your thin client.

Steps

1. To access the network settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **Network Setup**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Network Setup**.

   The **Network setup** dialog box is displayed.
2. Click the **WLAN** tab, and configure the following options:

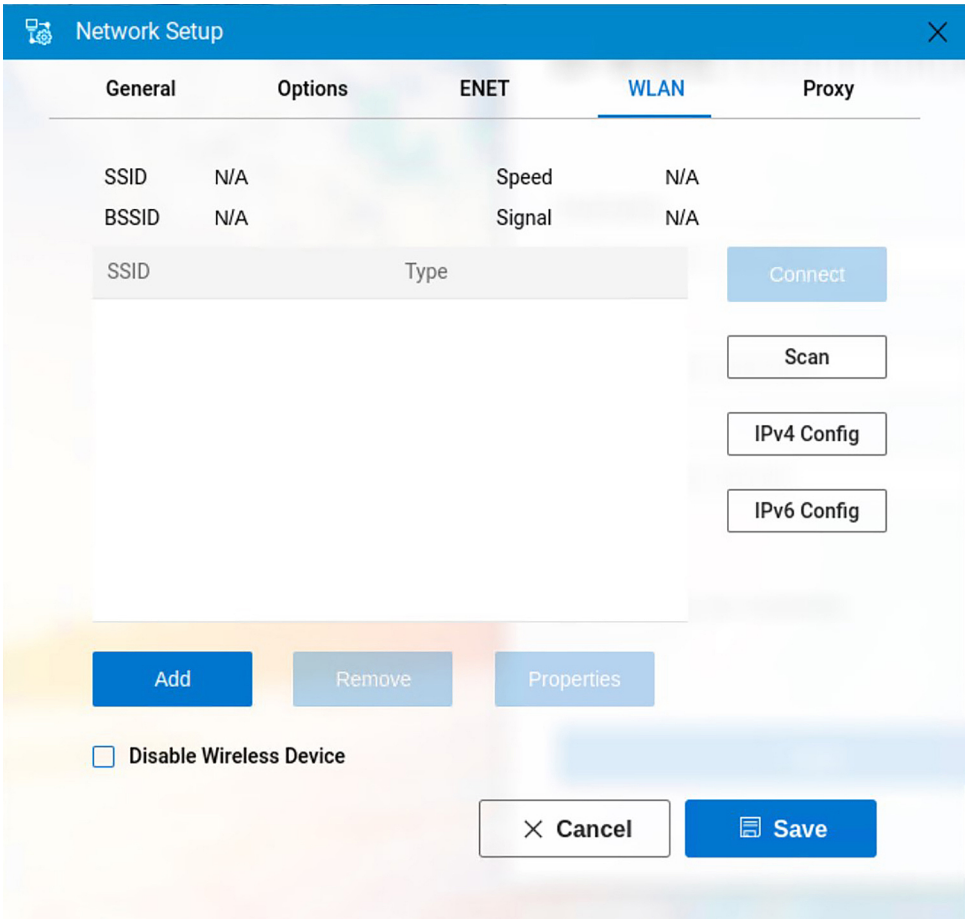

Figure 23. WLAN tab

- **Add**—Use this option to add and configure a new SSID connection. You can configure the SSID connection from the available security type options. After you configure the SSID connection, the added SSID connection is listed on the **WLAN** tab.
- **Remove**—Use this option to remove an SSID connection from the list.
- **Scan**—Use this option to allow your thin client to scan and identify a wireless network connection.
- **Connect**—Use this option to join a wireless network from the list.

  NOTE: When you enter a correct password to connect to the WPA and WPA2 personal wireless connection, the new password is saved. Entering the password again after you restart the device is not required.

- **Properties**—Use this option to view and configure the authentication properties of an SSID connection that is displayed in the list.
- **IPv4 Config**—Click this option to configure the IPv4 settings for the wireless connection. To set an IPv4 connection using either DHCP or static IP address, configure any of the following options:

- If you want to enable your thin client to automatically receive information from the DHCP server, click **Dynamically allocated over DHCP/BOOTP**.
- If you want to manually configure the IP address, click **Statically specified IP Address**, and provide the IPv4 details.

- **IPv6 Config**—Click this option to configure the IPv6 settings for the wireless connection.
  a. To enable the wireless IPv6, click the **IPv6** slider switch.
  b. To set an IPv6 connection using either DHCP or static IP address, configure any of the following options:
     - If you want to enable your thin client to automatically receive information from the DHCP server, click **Dynamically allocated over DHCP/BOOTP**.
     - If you want to manually configure the IP address, click **Statically specified IP Address**, and provide the IPv6 details.
- **Disable Wireless Device**—Select this check box to disable a wireless device.
  - **Always**—Click this radio button if you want to keep the wireless options always disabled.
  - **EnetUp**—Click this radio button if you want to disable the wireless device whenever the wired network is connected.

3. Click **Save** to save your settings.

NOTE: If you have connected to Wi-Fi on a ThinOS device that is connected to the Dell WD19 dock, you may not be able to connect to Wi-Fi again after the ThinOS firmware update is installed. Your device is also automatically restarted. To resolve this issue, you must restart the ThinOS client again.

WiFi 6E

In ThinOS 10.x 2502, WiFi 6E is supported.

Configure WWAN using WMS or APT

WWAN (Wireless Wide Area Network) allows ThinOS 10.x devices to connect to mobile networks using an active physical SIM card. This feature requires enabling the mobile network, configuring the APN, and turning on mobile data to establish seamless cellular connectivity.

Prerequisites

Ensure that an active physical 5G SIM card is inserted into the device before beginning the configuration.

About this task

After inserting the SIM card and rebooting the device, ThinOS automatically establishes a WWAN connection using the inserted SIM. Mobile data configuration is handled by the system, enabling immediate Internet access without requiring manual setup. Data roaming can be enabled if needed. Once the connection is active, the WWAN status updates to reflect the live cellular connection.

Steps

1. Insert an active physical 5G SIM card into the device and reboot the device.
2. To configure WWAN, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
3. Go to **Network Configuration** > **WWAN Settings**.
4. Verify if **Mobile Network** is enabled.

   NOTE: **Mobile Network** is enabled by default. Enable the **Data Roaming** option if required.
5. Click **Save & Publish**.

Configure Wi-Fi 7 (6 GHz) connectivity

Explains how ThinOS 10.x enables IT administrators and users to configure, connect, and verify Wi-Fi 7 (6 GHz) wireless networks through the WLAN settings in the local device interface.

About this task

After following the configuration steps, the device connects to a 6 GHz Wi-Fi 7 network using WPA3 security. ThinOS displays the connection status, speed, and detailed WLAN information, allowing users to validate that the device is successfully operating on the 6 GHz band.

Steps

1. On the ThinOS device, go to **Settings** > **Network Setup**.
2. Select the **WLAN** tab to manage wireless network connections.
3. Click **Scan** to discover available wireless networks.
4. Select an SSID that supports 6 GHz (Wi-Fi 7).
5. Choose **WPA3 Personal** as the **Security Type**.
6. Enter the **WPA key** to configure the network.
7. From the **WLAN** list, select the configured 6 GHz SSID.
8. Click **Connect** to establish the connection.
9. Click **Save**.

Results

The device connects to the selected 6 GHz Wi-Fi 7 network, and the WLAN status and connection details are displayed in the **System Information** panel.

Enable captive portal detection for wireless

When you attempt to connect to WiFi, a web page is displayed to verify the authenticated users, before Internet access is granted. ThinOS supports a captive portal that is based on HTTP redirect. Any captive portal that is based on DNS redirect or ICMP redirect is not supported in the current ThinOS release. If an OPT (options) record with DNS resource record (RR) type 41 is available in a received DNS response, the same OPT record must be available in the Additional records section. ThinOS does not support the DNS response with an OPT record that is available in the Answer section.

Steps

1. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced tab** and expand **Network Configuration**.
3. Click **Wireless**.
4. On the **Global Wireless Settings** page, click the **Enable Captive Portal Detection** toggle switch. Enabling this feature allows the ThinOS client to display the captive portal web page when you attempt to connect to WiFi.
5. In the **Captive Portal Detection Interval Time** field, specify the session timeout.
6. Click the **Allow HTTP protocol redirection** toggle switch if you want to use the HTTP protocol for redirecting to the captive portal web page.
7. Specify the captive portal detection URL. If the URL is not configured, the system default URL is used.
8. You must install **Chrome Browser** application package to enable **Use Broswer For Captive Portal Detection** option to use chrome for **Web Authentication**.
9. Restart your thin client for the settings to take effect.

   NOTE: If your thin client is connected to a wired network, you must set the default gateway to **WLAN0**.

Configure the proxy settings

About this task

This section describes how to configure the proxy settings on your thin client.

Steps

1. To access the network settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **Network Setup**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Network Setup**.

   The **Network setup** dialog box is displayed.

Table 22. Supported protocols

Component	Supported protocols	Additional information
Wyse Management Suite	HTTPS, and SOCKS5	N/A
Citrix RealTime Media Engine (RTME)	HTTP	N/A
Azure Virtual Desktop (AVD)	HTTP	N/A
Horizon	HTTP	N/A

2. Click the **Proxy** tab, and configure the following options:
   - Proxy Types—You can use HTTP proxy, HTTPS proxy, and SOCKS5 proxy types. The proxy type enables the thin client to connect to the application such as Wyse Management Suite.
   - Proxy values—You can enter values for the HTTP proxy, HTTPS proxy, and SOCKS5 proxy types. Adding proxy values enable the thin client to connect to the proxy server.

   NOTE: A client reboot is required when pushing a **Proxy.pac** file for the first time, and supported applications (e.g., AVD or HORIZON) must be manually added in **WMS/APT** > **Settings** > **Admin Policy Tool** > **Advanced** > **Network Configuration** > **Proxy Settings** > **Proxy Application List** before saving.

   A new app list value **HORIZON** is added. For the Omnissa Broker agent to use the proxy, you should specify the **Apply proxy server on** field as **HORIZON**. Unauthenticated proxy is accepted when using **HORIZON**. Username and password are ignored.

   A new proxy app list value that is called **MTOP** is added for Microsoft Teams in an ICA session.

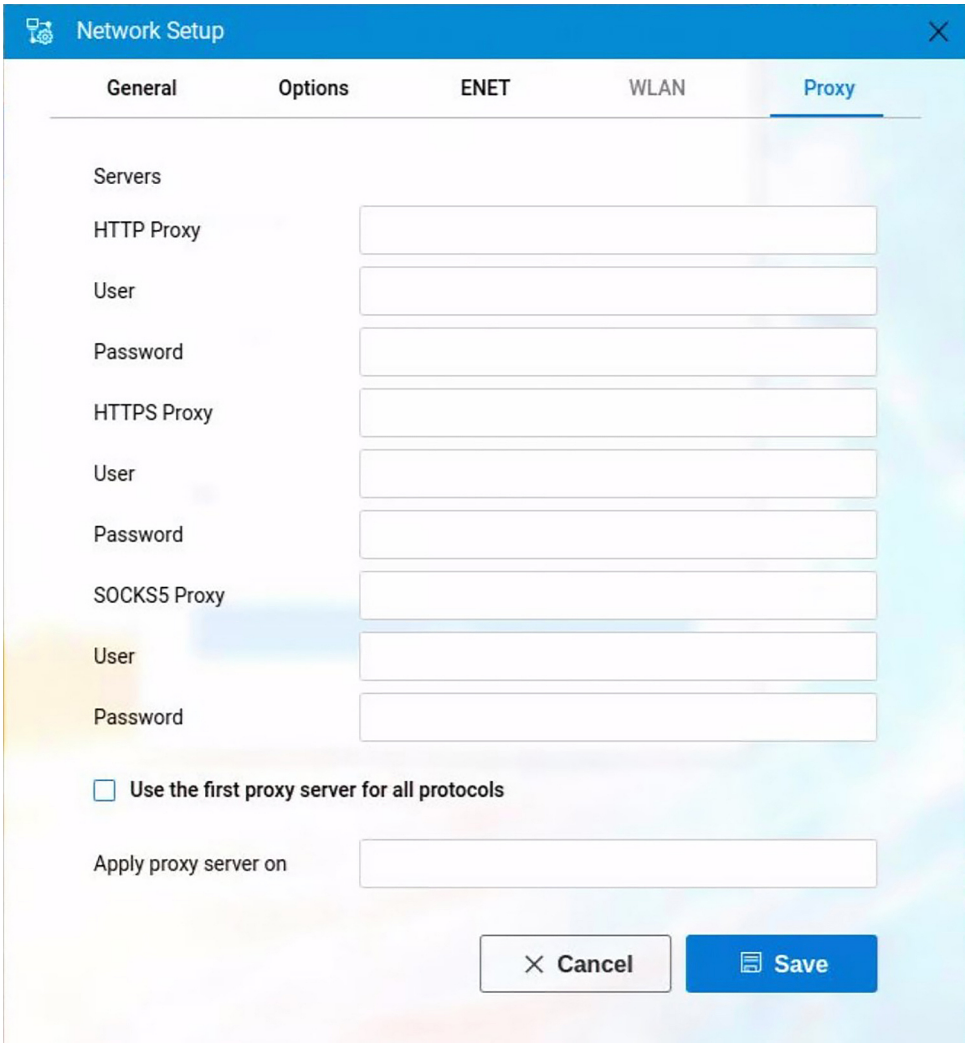

Figure 24. Proxy tab

Use the following guidelines:

a. Configure the proxy servers based on your requirement.

- Enter the HTTP proxy port number or HTTPS proxy port number, username, and password in the respective fields. However, a credential pass through ($UN/$PW) is not recommended because it starts before you sign in. Wyse Management Suite uses both HTTP/HTTPS and MQTT protocols to communicate with the WMS/MQTT server. However, the HTTP proxy cannot redirect TCP packages to the MQTT server which requires a SOCKS5 proxy server. If there is only the HTTP server available, the real-time command that requires MQTT does not work.

  NOTE: The HTTP/HTTPS proxy default port is 8080.

- Enter the SOCKS5 proxy port number, username, and password in the respective fields. If the SOCKS5 proxy is configured, the Wyse Management Suite proxy uses the SOCKS5 only. If SOCKS5 is not configured, then Wyse Management Suite proxy searches for alternative protocols, for example, HTTP in the configuration.

  NOTE: The SOCKS5 proxy default port is 1080.

- Select the **Use the first proxy server for all protocols** check box to enable all the protocols to use the same server in the **HTTP Proxy** fields. Both HTTP and HTTPS proxies use the same host and port, and the SOCKS5 proxy agent uses HTTP host with default Socks5 port (1080).

b. Specify the supported applications as Wyse Management Suite, Azure Virtual Desktop (AVD), and RTME separated by a semicolon in the **Apply proxy server on** field.

3. Click **Save** to save your settings.

ThinOS supports the usage of DHCP option tag 252. The option enables the device to fetch the proxy information from the DHCP server when the device is reset to factory default settings or when you restart the thin client. For example, `http://x.x.x.x/proxy.pac`. The proxy settings from DHCP option 252 are not displayed on the ThinOS UI.

Proxy is enabled only for configured applications regardless of the availability of DHCP option 252. If you configure an empty value on the ThinOS local user interface, the proxy is enabled for all supported applications by default. If you configure an empty value in the Wyse Management Suite policy settings or the Admin Policy Tool, the proxy is not enabled for any applications. If DHCP option 252 is available and is supported by the configured application, WPAD (DHCP 252) takes priority. If DHCP 252 is available, WMS is enabled to go through proxy even if it is not configured in the **Proxy Application List** configuration.

User scenario

Table 23. VDI logon or session launch that goes through proxy

Component	Features	PAC proxy	GUI proxy
Citrix	http broker log in	No	No
	http broker session launch	No	No
	https broker log in	Yes	Yes (RTME value added in the **Apply proxy server on** application list field)
	https broker session launch	Yes	Yes (RTME value added in the **Apply proxy server on** application list field)
Omnissa	broker log in	Yes	Yes (HORIZON value added in the **Apply proxy server on** application list field)
	session launch	Yes	Yes (HORIZON value added in the **Apply proxy server on** application list field)
Azure Virtual Desktop	broker log in	Yes	Yes (AVD value added in the **Apply proxy server on** application list field)
	session launch	No	No
Microsoft Remote Desktop Services	broker log in	No	No
	session launch	No	No
Amazon WorkSpaces	broker log in	No	No
	session launch	No	No
Wyse Management Suite	Wyse Management Suite connection	Yes	Yes (WMS value added in the **Apply proxy server on** application list field)

1. Configure the HTTPS proxy server host and port.
2. Configure the user credentials according to the proxy server settings.

After you restart your device, the client checks in to the Wyse Management Suite server through the HTTPS proxy server.

Route proxy settings through Ignore Host

About this task

In ThinOS 10.x 2505, you can manually specify selected hosts in the WMS to bypass the proxy server address. These designated hosts can route traffic externally without using the internal proxy server.

This feature gives flexibility to ThinOS10 customers to route traffic, connect brokers without routing through the proxy servers.

To add a hostname in the Ignore Host field under Proxy Settings:

Steps

1. Log in to **WMS**.

2. Go to **Group & Configs** > **Select a group** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Network Configuration** > **Proxy Settings** > **Add Row** > **Ignore Host**.

Configure the SNMPV3 settings

SNMPV3 in ThinOS requires a security level with both authentication and privacy. This setting can be configured in the Wyse Management Suite policy by going to **Network Configuration** > **SNMPV3 Settings** . ThinOS supports MIB tree 1.3.6.1.2.1 but not 1.3.6.1.2.1.10, 1.3.6.1.2.1.4.20.1.5, and 1.3.6.1.2.1.4.21.1.10. ThinOS supports private MIB tree 1.3.6.1.4.1.714 as below:

Table 24. Private MIB tree

ThinOS setting	MIB tree version
Serial Number	1.3.6.1.4.1.714.1.2.6.2.1
Undefined yet	1.3.6.1.4.1.714.1.2.6.2.2
Undefined yet	1.3.6.1.4.1.714.1.2.6.2.3
Network speed	1.3.6.1.4.1.714.1.2.6.2.4
Network Gateway	1.3.6.1.4.1.714.1.2.6.2.5
DHCP setting (1 as enabled, 0 as disabled)	1.3.6.1.4.1.714.1.2.6.2.6
DNS setting (1 as static, 0 as dynamic)	1.3.6.1.4.1.714.1.2.6.2.7
DNS server	1.3.6.1.4.1.714.1.2.6.2.8
Send message to client	1.3.6.1.4.1.714.1.2.6.1.2.0
Reboot client	1.3.6.1.4.1.714.1.2.6.1.1.0

NOTE: Set 1.3.6.1.4.1.714.1.2.6.1.2.0 to send message to client. The message character count is increased to 255 characters.

Set 1.3.6.1.4.1.714.1.2.6.1.1.0 to reboot the client. Reboot client behaviors are as below:

- Set to **0**: Reboot immediately.
- Set to **x**: Reboot after x minutes (x is an integer)
- Set to **-1**: Cancel reboot.

NOTE: If you set 1.3.6.1.4.1.714.1.2.6.1.1.0 to reboot the client, you cannot set another value to change the reboot timer directly. You must set the value to -1 to cancel the reboot first, and then set another value to reboot again.

Configuring the remote connections

Use the **Remote Connections** dialog box to configure the connection broker settings, general connection options, and authentication settings.

Configure the broker setup

About this task

This section describes how to configure the broker setup on your thin client.

Steps

1. To access the remote connection settings, do the following:
   a. For **Modern Mode**, from the desktop menu, click **Settings** > **Remote Connections**.
   b. For **Classic Mode**, from the desktop menu, click **System Setup** > **Remote Connections**.

   The **Remote Connections** dialog box is displayed.

2. On the **Broker Setup** tab, select a VDI broker from the **Select Broker type** drop-down list, then select **Broker Server** > **Auto Connect List** and configure the broker settings.
3. Click **Save** to save your settings.

   NOTE: ThinOS enables you to log in to a VDI broker using only a smartcard certificate. To enable this feature, go to **Advanced** > **Login Experience** > **Login Settings** from the Wyse Management Suite policy settings or the Admin Policy Tool, and enable the **Login Use Smartcard Certificate Only** option under **Login Experience**. When the option is enabled, other certificates such as user certificates are ignored.

Configure the General Options

About this task

This section describes how to configure the general options on your thin client.

Steps

1. To access the remote connection settings, do the following:
   a. For **Modern Mode**, from the desktop menu, click **Settings** > **Remote Connections**.
   b. For **Classic Mode**, from the desktop menu, click **System Setup** > **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. Click the **General Options** tab, and do the following:

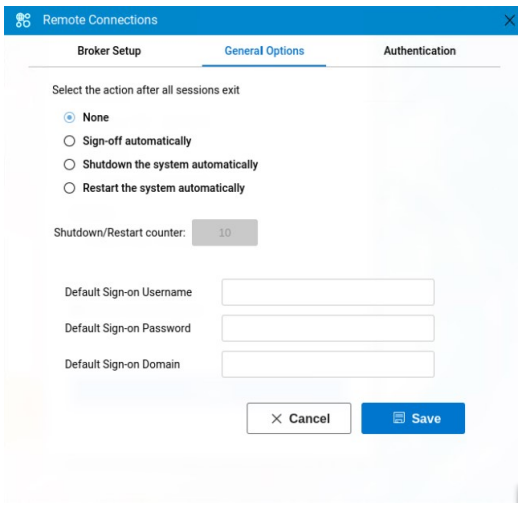

Figure 25. General options

   a. Click one of the following options to set the action that the thin client should perform after you exit all sessions:
      - **None**—By default, **None** is selected and the thin client automatically returns to the terminal desktop.
      - **Sign-off automatically**
      - **Shutdown the system automatically**—If you select this option, you must specify a time period after which the thin client shuts down.
      - **Restart the system automatically**—If you select this option, you must specify a time period after which the thin client restarts.

      NOTE: You can enable or disable the privilege to cancel shutdown or restart. From the Wyse Management Suite policy settings or Admin Policy Tool, go to **Advanced** > **Privacy & Security** > **Account Privileges** > **Previlige Level**, and select **Customize** from the drop-down list. Enabled or disable the **Allow to Stop Forced Reboot/ Shutdown** option. If the option is disabled, when all sessions are ended, users cannot click the **Cancel** button on the reboot or shutdown countdown window to stop the process.

   b. Enter the default username in the **Default Sign-on Username** field.
   c. Enter the default password in the **Default Sign-on password** field.
   d. Enter the default domain in the **Default Sign-on Domain** field.

3. Click **Save** to save your settings.

Configuring the central configurations

Use the **Central Configuration** dialog box to configure the Wyse Management Suite server settings.

Configure the Wyse Management Suite settings

About this task

This section describes how to configure the Wyse Management Suite settings on your thin client.

Steps

1. To access the central configuration settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **Central Configuration**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Central Configuration**.

   The **Central Configuration** dialog box is displayed.
2. From the desktop menu, click **System Setup** > **Central Configuration**.
3. On the **WMS** tab, do the following:

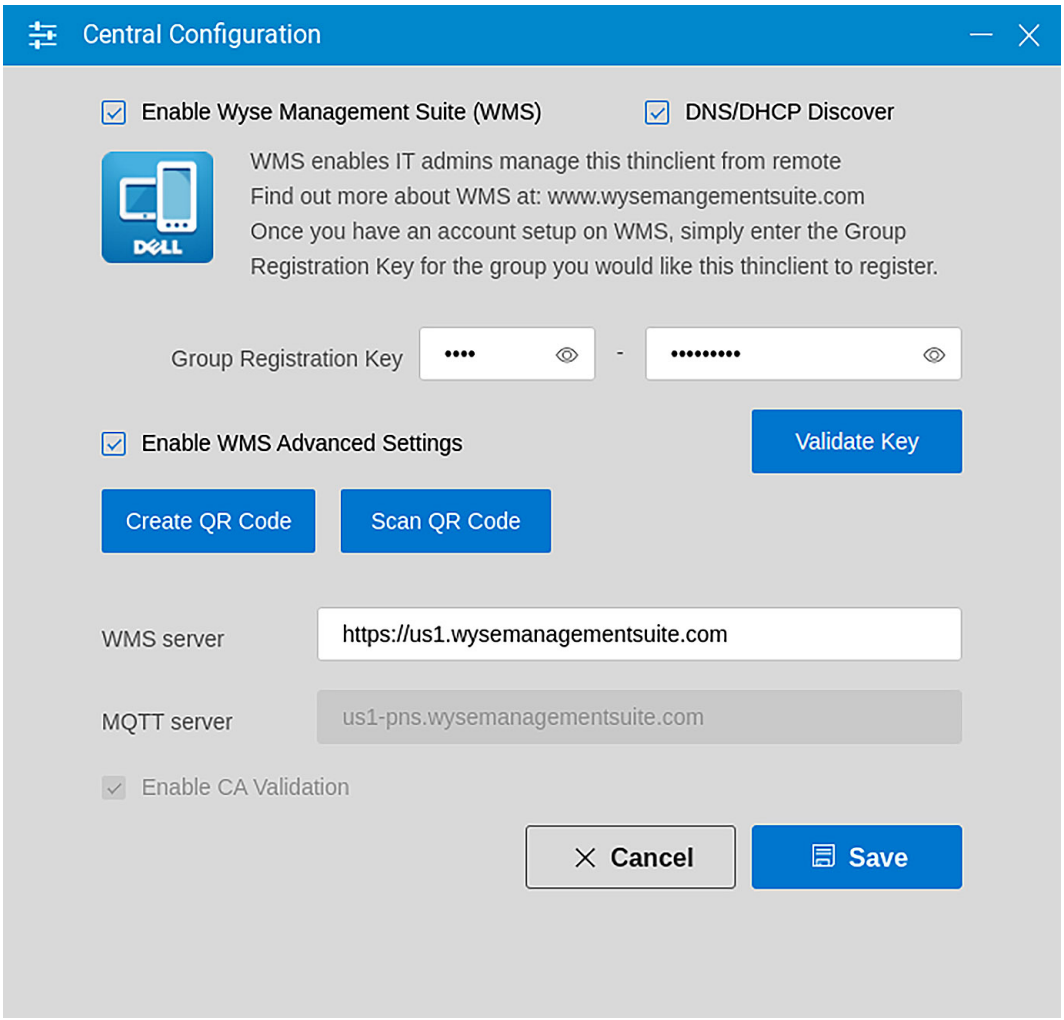

Figure 26. Wyse Management Suite

a. Select the **Enable Wyse Management Suite (WMS)** check box to enable the Wyse Management Suite to discover your thin client. By default, this option is selected. Wyse Management Suite service automatically runs after the client boots.

   NOTE: If the first discovery, for example, the Wyse Management Suite service is not successful, it continues until a discovery is successful. If all discoveries fail, it is started again automatically.

b. Select the **DNS SRV record** check box if you want the thin client to obtain the Wyse Management Suite values through DNS server, and then try to register into the Wyse Management Suite server. By default, the check box is selected. If the check box selection is canceled, the thin client cannot obtain the Wyse Management Suite values through the DNS server.

c. In the **Group Registration Key** field, enter the group registration key as configured by your Wyse Management Suite administrator for your group. To verify the key, click **Validate Key**.

   NOTE: A Group Registration Key is not required for the private Wyse Management Suite server. You can provide the Wyse Management Suite server details to enable the device to check in to Wyse Management Suite. ThinOS registers to a quarantine tenant in Wyse Management Suite.

d. Select the **Enable WMS Advanced Settings** check box to enter the Wyse Management Suite server details and to enable the CA validation. By default, the MQTT server option is disabled. The MQTT server value is populated after the ThinOS device is checked in to the Wyse Management Suite. If you want to use the feature of Create QR Code or Scan QR Code buttons, see Added Create QR Code and Scan QR Code in Central Configuration.

   NOTE: If you enable the external secure MQTT option on the Wyse Management Suite server, the thin client automatically fetches the MQTT server <tls://xxx.xxx.xxx:8443>. If port 1883 is blocked in the Wyse Management Suite server, the ThinOS client cannot switch to the External Secure MQTT server from the External MQTT server. If you are blocking port 1883, select External Secure MQTT as Preferred MQTT in the Wyse Management Suite server first.

   NOTE: The default domain is filled in the login window only when you login and is not displayed in the domain list. If you want to view the domain in the list, configure the domain in **Domain List policy** in the Admin Policy Tool or Wyse Management Suite server.

e. Select the **CA validation** check box if you want to enable the CA validation feature.

   The CA validation is required when you import certificates into your Wyse Management Suite server. By default, the CA Validation check box is selected to improve the security when using the Wyse Management Suite cloud. This change affects connections to any of the following servers:

   - *.dellmobilitymanager.com
   - *.cloudclientmanager.com
   - *.wysemanagementsuite.com

Table 25. CA validation

Wyse Management Suite deployment	CA Validation
Private cloud	When you deploy Wyse Management Suite on a private cloud, the **Enable CA Validation** check box is available to configure after you specify the server details in the **WMS Server** field. By default, the check box is selected.
Public cloud	When you deploy Wyse Management Suite on a public cloud, the **Enable CA Validation** check box is selected by default. You cannot disable the **Enable CA Validation** option.

4. Click **Save** to save your settings.

   NOTE: When you modify the Wyse Management Suite information, a dialog box is displayed prompting you to restart the thin client. To apply the settings immediately, click **Reboot Now**. If you do not want to restart your client, click **Cancel**.

Creating QR Code or Scanning QR Code in Central Configuration

To use the features, do the following:

Steps

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

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

Configure the VPN Manager

VPN Manager is included to manage Virtual Private Network connections. ThinOS uses the OpenConnect client that is based on the SSL protocol for connecting to a VPN.

About this task

This section describes how to configure the VPN Manager on your thin client.

Steps

1. To access the VPN manager settings, do the following:
   - **Modern Mode**—from the desktop menu, click **Settings** > **VPN Manager**.
   - **Classic Mode**—from the desktop menu, click **System Setup** > **VPN Manager**.

   The **VPN Manager** dialog box is displayed.
2. To create a session, click the **+** icon and do the following:

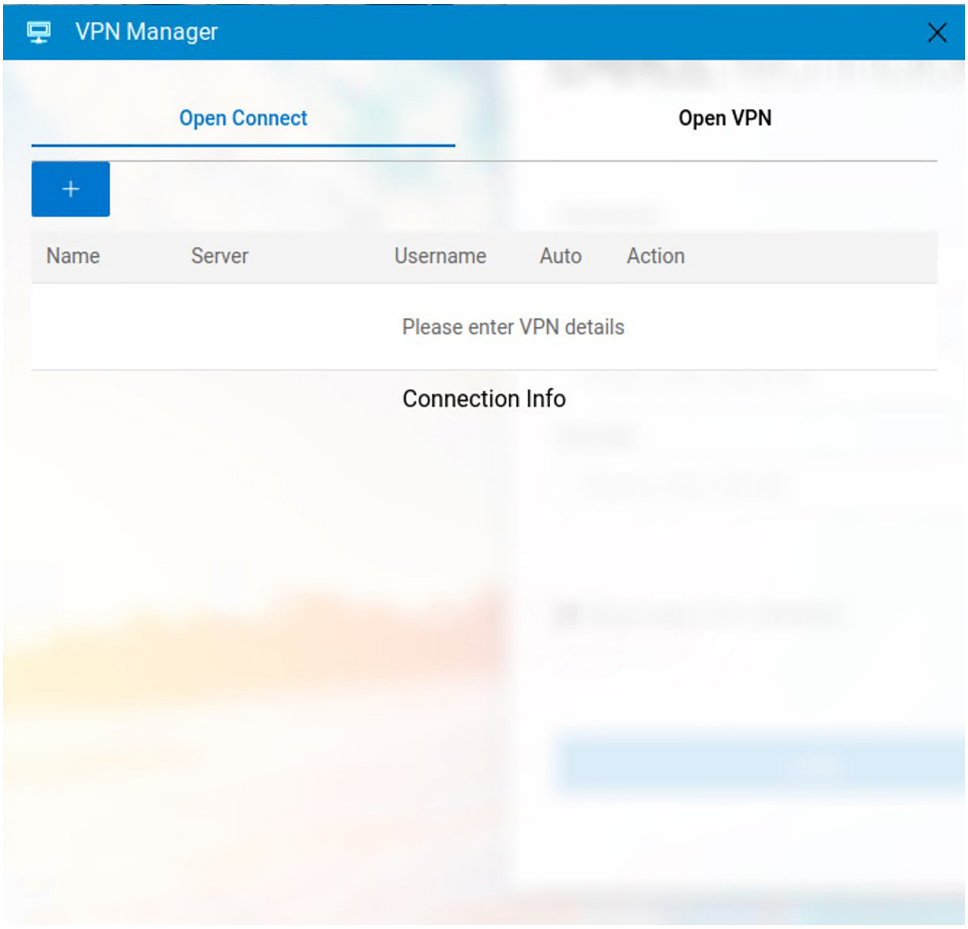

Figure 27. VPN Manager

a. Enter the name of the session in the **Name** field. This option is mandatory. The maximum character limit is 255 characters.
b. Enter the IP address of the VPN server in the **Server** field. This option is mandatory and is defined as either an IP address or a hostname. The maximum character limit is 255 characters.
c. Enter the login username in the **Username** field. This option is not mandatory. The maximum character limit is 255 characters.
d. Enter the password in the **Password** field. This option is not mandatory. The maximum character limit is 255 characters.
e. Select the connection **Protocol**.
f. Select the **Certificate**, if needed, for the connection. To add the certificate from the desktop menu, click **System Settings** > **System Tools** > **Certificate** > **Import**.
g. Click the **Auto-connection on system startup** button to display which connection is automatically connected on the system start up.
h. Click the **Show progress in detail** button to display the progress details of the connection on the system start up.
i. Click the **Show debug information** button to display the VPN debug details for better troubleshooting.
j. Click **Save** to save the changes.

When connections are created, the **Auto** column displays which connection is automatically connected when the device restarts. Only one session can be set to autoconnect.

NOTE: You can connect to VPN with Cisco AnyConnect, Pulse Secure, or Global Protect.

3. Select a session, and click **Action**.

Configuring Dynamic time zone

ThinOS 10.x 2511 introduces automatic time zone detection using GeoIP. Devices can set their time zone based on geographic location, reducing the need for manual configuration and eliminating the need to maintain multiple policy groups.

To configure dynamic time zone on ThinOS devices, do any of the following:

- Configure Dynamic time zone using APT.
- Configure Dynamic time zone using WMS.

Configure Dynamic time zone using APT

You can set the device time zone based on its geographic location automatically using APT.

About this task

After completing the configuration steps, ThinOS automatically updates the time zone based on the network connection. When the device connects to LAN or Wi-Fi, the time zone adjusts accordingly. Rebooting, upgrading, or downgrading the ThinOS 10.x device does not affect this behavior, ensuring consistent and accurate time settings across all actions.

Steps

1. Go to **Admin Policy Tool** on the device.
2. Go to **Advanced** > **Region & Language**.
3. Verify that the **Auto Time Zone** is disabled by default.
4. Enable **Auto Time Zone**.
5. Click **Save & Publish**.

Configure Dynamic time zone using WMS

You can set the device time zone based on its geographic location automatically using WMS.

About this task

After completing the configuration steps, ThinOS automatically updates the time zone based on the network connection. When the device connects to LAN or Wi-Fi, the time zone adjusts accordingly. Rebooting, upgrading, or downgrading the ThinOS 10.x device does not affect this behavior, ensuring consistent and accurate time settings across all actions.

Steps

1. Log in to **WMS** as an administrator.
2. Go to **Groups & Configs** > **Edit Policies** > **ThinOS 10.x**.
3. Go to **Advanced** > **Region & Language**.
4. Verify that the **Auto Time Zone** is disabled by default.
5. Enable **Auto Time Zone**.
6. Click **Save & Publish**.

Configuring Policy-driven check-in enforcement

ThinOS 10.x 2511 introduces a policy-driven enforcement mechanism that displays a pop-up and restricts functionalities when the device does not check in to WMS within the configured interval, ensuring compliance and accountability.

About this task

After completing the configuration steps, ThinOS enforces policy-based check-in behavior. If a device fails to check in with WMS within the configured interval, the system automatically triggers the assigned action—Auto Logoff, Shutdown, or Reboot. This ensures continued policy compliance and prevents unauthorized or unmanaged device use.

Steps

1. To configure policy-driven enforcement, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Login Settings** > **Session Setting** > **Inactive Timeout**.
3. Review the default **Inactive Timeout** value.
4. Set **Inactive Timeout**= **1 minute**.
5. Go to **Enable Auto Log Off** and review the available options:
   - Auto Logoff
   - Shutdown After Logout
   - Reboot After Logout
6. Select the required option based on the intended behavior.
7. Click **Save & Publish** to apply the configuration to devices.

Configure VNC services

Explains how to configure VNC services on ThinOS 10.x devices using APT or WMS, including enabling remote shadowing, set passwords, defining IP/port access, and apply security and timeout options for remote connections.

Steps

1. On the ThinOS device, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Services** and click **Remote Shadow Settings**.
4. To enable VNC shadowing, click the **Allow Remote Shadow** button.
   a. Enter the password in the **Remote Shadow Password** field. The password length is restricted to eight characters from ThinOS 10.x 2502.
   b. Click the **Enable 8 bits** button to use 8-bit color resolution.
   c. Click the **Enable Zlib** button to enable Zlib compression.
   d. Click the **Enable Remote Shadow Prompt** button to display a prompt to allow or reject a VNC shadowing request.

      The shadowing request times out if there is no user interaction. The following options can be set for a timeout.
      - **Select Timeout Type**—Select the action to be performed after the VNC shadowing request times out. You can select Accept or Reject.
      - **Timeout**—Specify a time between 0 to 600 second for the VNC shadowing request to timeout, if there is no user interaction.

   e. Click the **Enable View Only** button to activate the view only mode.
   f. Click the **Active Visible** button to notify the user that the device is being shadowed.
   g. Enter the IP addresses from which VNC connections can be initiated in the **VNCD Server field**. You can only enter a valid IP address in this field.
   h. Specify the VNC port used for TCP-based connections in the **VNCD TCP Port** field.

      The default port is 5900. The current connection is not affected when you change the port. The port change takes effect during the next VNC connection.
5. Click **Save & Publish**.

Configure P2P Protocol services

Explains how for configuring P2P shadowing on ThinOS 10.x devices using APT or WMS, including enabling shadowing, setting passwords, defining timeout behavior, view-only mode, visibility options, and adding watermarks for shared sessions.

Steps

1. On the ThinOS device, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.

3. Expand **Services** and click **Remote Shadow Settings**.
4. To enable P2P shadowing, click the **Allow Remote Shadow** button.
   a. Enter the password in the **Remote Shadow Password** field. The password length is restricted to eight characters from ThinOS 10.x 2502.
   b. Click the **Enable Remote Shadow Prompt** button to display a prompt to allow or reject a P2P shadowing request.

      The shadowing request times out if there is no user interaction. The following options can be set for a timeout.
      - **Select Timeout Type**—Select the action to be performed after the P2P shadowing request times out. You can select Accept or Reject.
      - **Timeout**—Specify a time between 0 to 600 second for the P2P shadowing request to timeout, if there is no user interaction.

   c. Click the **Enable View Only** button to activate the view only mode.
   d. Click the **Active Visible** button to notify the user that the device is being shadowed.
5. In **Remote Shadow Protocols** dropdown menu, select **P2P Protocol**.
6. Click **Enable Remote Shadow Watermark** to enable the watermark for shared screen.

   NOTE: The policy is not applicable when the policy **Active Visible** is disabled.
7. In **Specify Watermark Messege**, enter the custom message that you want to set as a watermark.
8. Click **Save & Publish**.

7

Configuring connection brokers

In a Virtual Desktop Infrastructure (VDI) environment, a connection broker is a software entity that enables you to connect to an available desktop. The connection broker facilitates the VDI environment to securely and efficiently manage the centrally hosted desktop environments.

Configuring Citrix

Citrix offers a complete virtualization solution, where all applications and resources are deployed on a centralized server, and published to remote devices. In ThinOS 10.x 2502, Citrix Receiver is replaced by Citrix Workspace app. Citrix Workspace app, a client software that is released by Citrix, enables you to access all your virtual apps, desktops, and other Citrix products from a single workspace UI. For more information about Citrix Workspace App, see the Citrix documentation at docs.citrix.com.

NOTE: In ThinOS, USB device can only be redirected in to an ICA session when the mouse focus is inside the session.

For the Citrix VDI-related settings in Wyse Management Suite and Admin Policy Tool, it is recommended that configuring the settings before signing in to Citrix broker. If you have already signed in to the broker, you must sign off or reboot the client.

To access Citrix sessions using Citrix Workspace app, do the following:

1. Deploy the Citrix Workspace app package using Wyse Management Suite or Admin Policy Tool.
2. Go to **System Setup** > **Remote Connections** > **Broker setup**, and configure the Citrix broker.

NOTE: The **Enable Volume Control for Client Volume** option added in **Personalization** > **Shortcut Keys**, under Admin Policy Tool or Wyse Management Suite policy settings can be used to control the ThinOS local volume from remote sessions. This option is added to resolve the Citrix limitation.

ThinOS 10.x supports the following updates:

- The battery status light is displayed in the notification area for server VDAs. This feature is enabled by default. In the previous version of the Citrix Workspace app, only Windows VDA such as Windows 10 is supported.
- Adaptive audio works while using User Datagram Protocol (UDP) audio delivery. Adaptive audio is enabled by default, and the feature requires the latest VDA version. For more information, see the Citrix Virtual Apps and Desktops product documentation at docs.citrix.com.

NOTE: You can map a USB drive with NTFS format to Citrix sessions.

For information about the supported Citrix Workspace app features in ThinOS, see the Citrix Workspace app feature matrix table in the *Release Notes* of your ThinOS version at Support | Dell

Support for audio volume synchronization

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

ThinOS 10.x 2502 and Citrix Workspace app 2411 supports audio volume synchronization between the VDA and your audio devices. You can adjust the volume using the VDA audio volume slider. The volume reflects the same level on both your device and the VDA. This feature is enabled by default.

To use this feature, ensure you have VDA version 2411 or later.

To disable audio volume synchronization, follow these steps:

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

8. In the **Value** field, enter **FALSE**.
9. Click **Save & Publish**.
10. Restart the session for the changes to take effect.

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

Support for multiple webcam resolutions

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

ThinOS 10.x 2502 and Citrix Workspace app 2411 supports high-definition webcam streaming for all available client-side resolutions. The application on VDA determines the best resolution to capture. If media type negotiation fails, HDX defaults to VGA resolution (640 x 480 resolution). This feature is enabled by default.

To disable this feature, follow these steps:

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

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

Support for enhanced desktop viewer toolbar

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

The enhanced toolbar includes the following options:

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

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

Limitation

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

Support for customization of the toolbar

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

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

You can customize the Citrix Workspace app toolbar by adding or removing options.

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

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

Support for keyboard shortcuts for enhanced desktop viewer toolbar

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

You can access the enhanced Desktop Viewer toolbar using the keyboard on your endpoint devices. This feature allows you to invoke the toolbar, navigate through options, and select required options using keyboard shortcuts.

Use the following keyboard shortcuts to access the toolbar:

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

The keyboard shortcuts are enabled by default.

To disable this feature, follow these steps:

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

Support for performance optimization for graphics

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

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

Enabling Performance Optimization

To enable this feature, follow these steps:

1. Open the Admin Policy Tool or the Wyse Management Suite policy settings.
2. Go to **Advanced VDI Configuration Editor** > **Citrix Configuration Editor**.

3. In the Citrix INI Settings, click **Add Row**.
4. From the **File** drop-down list, select **wfclient.ini**.
5. From the **Operation** drop-down list, select **Add or Update**.
6. In the **Section** field, enter **WFClient**.
7. In the **Key** field, enter **MultiMonitorPnPEnabled**.
8. In the **Value** field, enter **True**.
9. Click **Save & Publish**.
10. Sign out or restart the device for the settings to take effect.

Using the Automatically Extend Desktop Session

A new UI option, the **Automatically extend desktop session to external monitors** checkbox, is available to enable or disable the monitor **plug and play** feature. By default, the **Automatically extend desktop session to external monitors** checkbox is not selected.

To select this option, follow these steps:

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

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

Limitations

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

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

Enhanced Virtual Desktop Screen Resizing Experience

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

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

Disabling the Feature

To disable this feature, follow these steps:

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

Limitations

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

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

Enhance Samsung Smartphone with USB Redirection for transferring images

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

ThinOS enhances the **Transferring images** function for Samsung smartphones.

To enable this feature, follow these steps:

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

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

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

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

Limitation

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

Support Citrix Native Mode

ThinOS 10.x 2502 and Citrix Workspace App 2411 supports Citrix Native Mode. Citrix Native Mode uses the Citrix Linux binary to launch Citrix sessions, which can improve some Citrix features, like App Protection. But it has some limitations and considerations:

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

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

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

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

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

The following are the important notes for Citrix Native mode:

- Citrix broker login mechanism in Citrix Native Mode is the same as Linux Citrix Workspace App binary.
- Ensure set the Citrix broker address as the full Citrix Storefront URL such as `https://test.storefront.com/citrix/store` if there are more than three stores in your Citrix Storefront server. If only set the Citrix broker address as Citrix Storefront FQDN server name and your Citrix Storefront server has more than three stores, the Citrix broker login gets fail or the client gets stuck during broker login. This is Citrix binary designment.
- The default credentials that are configured from Admin Policy Tool or Wyse Management Suite policy settings are only applicable for login the HTTPS protocol Citrix Storefront server which has enabled the **User name and password** and **HTTP Basic** authentication methods. If you do not setup default user credentials in the Admin Policy Tool or Wyse Management Suite policy settings, the Citrix Workspace login window is displayed on top of the ThinOS login window and ask you for login. For other Storefront and Citrix ADC authentication methods, do not set default credentials in the Admin Policy Tool or Wyse Management Suite policy settings.

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

How to enable Citrix Native Mode

Prerequisites

In the Citrix Storefront server, do the following:

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

Steps

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

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

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

Unsupported WMS policy and Citrix Native Mode features

The following are the unsupported Wyse Management Suite policy settings:

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

The following are the unsupported features in Citrix Native Mode:

- Citrix cloud login
- Citrix ADC server timeout
- PNAgent server
- Connection manager
- PNMenu icon
- HTTP protocol storefront login
- Logon Citrix Storefront or ADC using user pfx format certificate

- Preferences settings in Citrix native mode menu and Citrix Connection Center.

Support App Protection in Citrix Native Mode

Dell ThinOS and Citrix Workspace App supports the Citrix App Protection feature. The App Protection component is in the Citrix Workspace App package. App Protection feature is only applicable for Citrix Native Mode.

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

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

For more information, see Citrix.

Configure the Citrix broker setup

About this task

This section describes how to configure the Citrix broker setup on your thin client.

Steps

1. To access the remote connections, do the following:
   - **Modern Mode**—From the desktop menu, click **Settings** > **Remote Connections**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Remote Connections**

   The **Remote Connections** dialog box is displayed.
2. On the **Broker Setup** tab, select **Citrix Virtual Apps and Desktops** from the **Select Broker Type** drop-down list, and do the following:

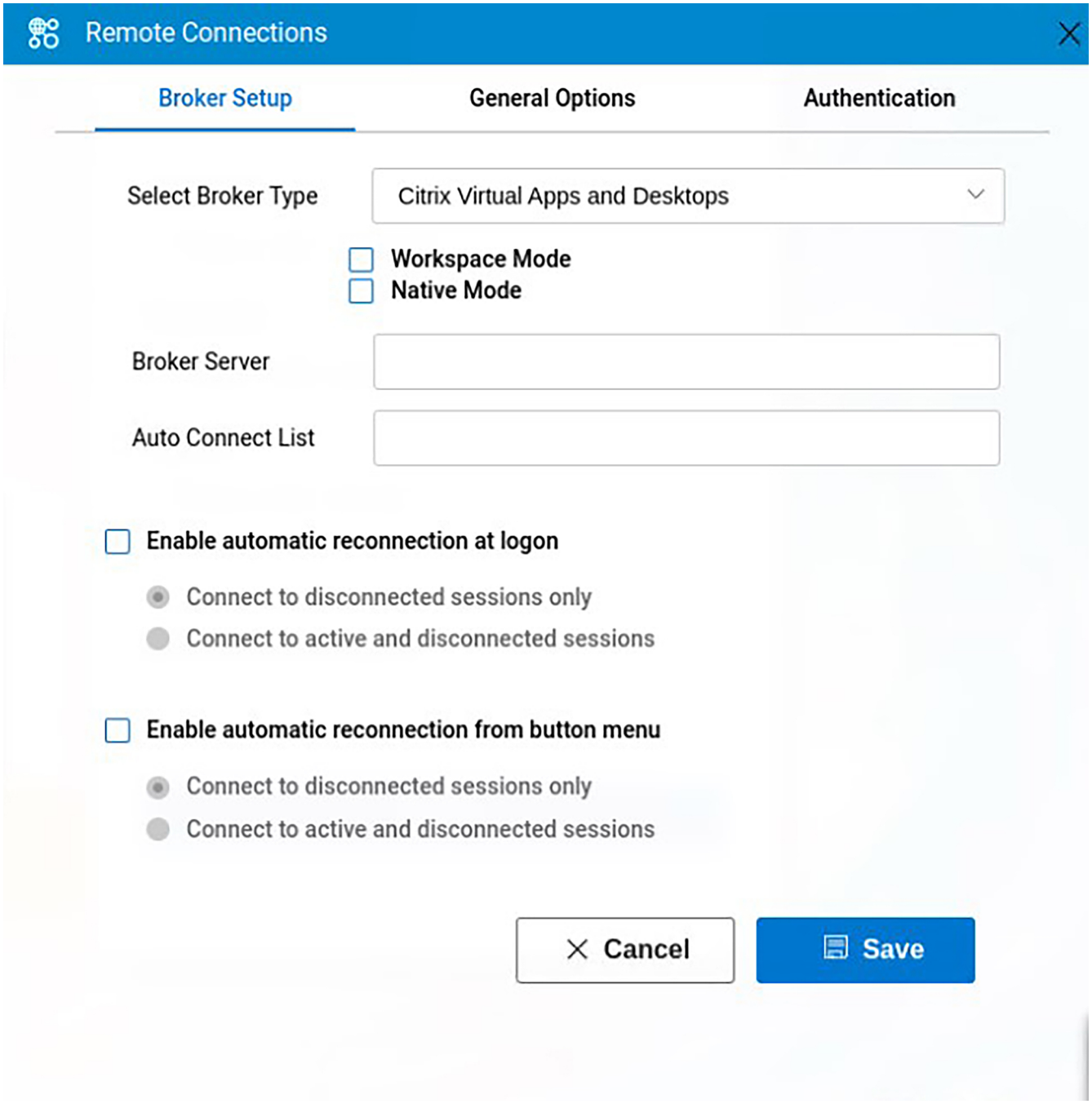

Figure 28. Broker Setup

a. Select the **Workspace Mode** check box if you want to enable the Citrix Workspace based layout of published applications and desktops.
b. In the **Broker Server** field, enter the IP address or hostname or FQDN of the Citrix server. You can enter the Citrix NetScaler Gateway URL, StoreFront URL, or the web interface URL.
c. In the **Auto Connect List** field, enter the name of the connection that is displayed in **Connection Manager** to automatically connect after you log in the Citrix broker. You can enter more than one connection name. Each connection name is separated by semi-colon, and is case-sensitive.

NOTE: On the desktop taskbar, click to open **Connection Manager**.

d. Select the **Enable automatic reconnection at logon** check box if you want to automatically reconnect to the disconnected sessions or both active and disconnected sessions during login. You must click either of the following options:

- **Connect to disconnected session only**
- **Connect to active and disconnected sessions**

e. Select the **Enable automatic reconnection from button menu** check box if you want to automatically reconnect to the disconnected sessions or both active and disconnected sessions by using the **Reconnect** button in the button menu. You must click either of the following options:

- **Connect to disconnected session only**
- **Connect to active and disconnected sessions**

To use the reconnect option, left-click the button menu, and click **Reconnect**.

3. Click **Save** to save your settings.

Classic mode vs Workspace mode

This section summarizes the differences between classic mode and workspace mode.

Figure 29. Classic mode

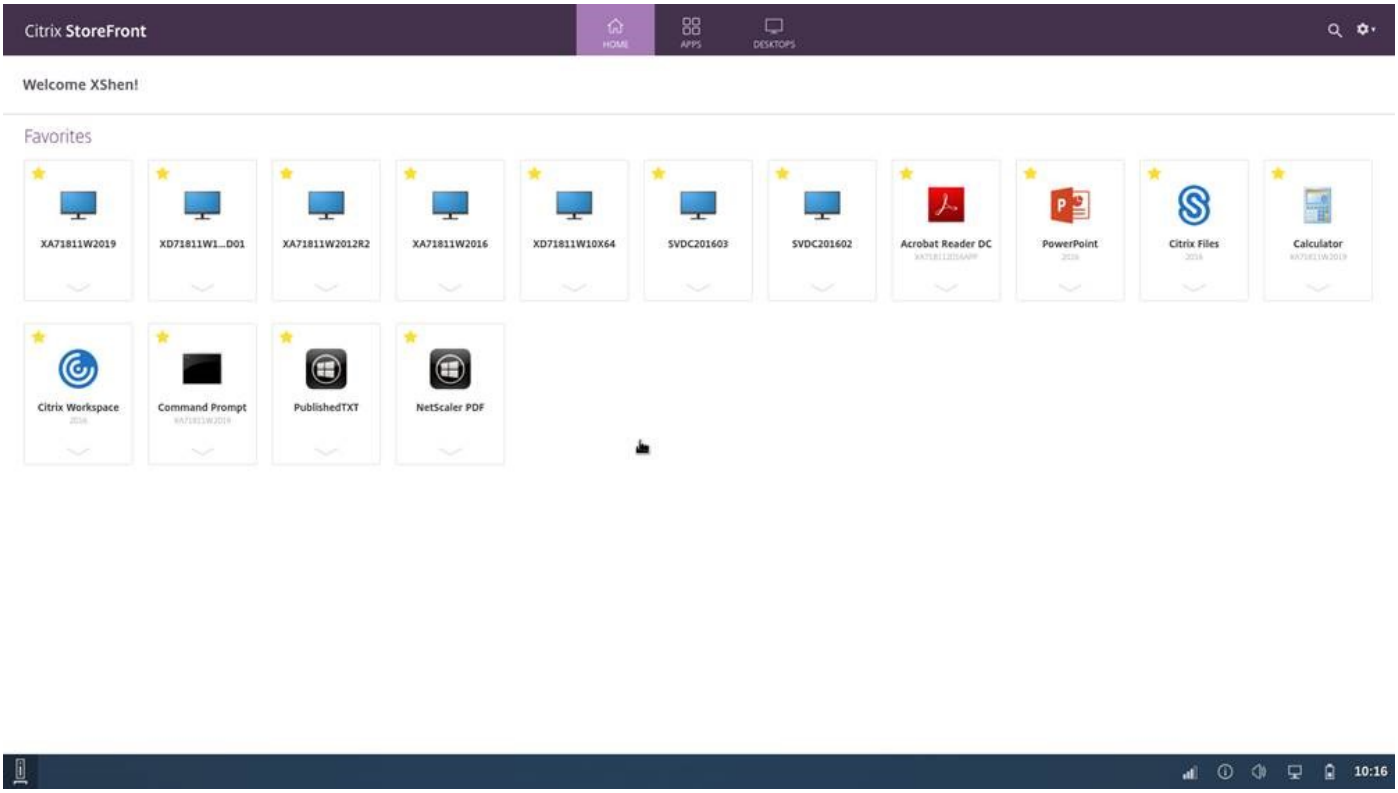

Figure 30. Workspace mode

Table 26. Classic mode vs Workspace mode

Item	Classic mode	Workspace mode
How to enable	By default, the ThinOS loads the classic mode if you do not select the Workspace mode check box during Citrix broker setup.	Select the **Workspace mode** check box during Citrix broker setup.
Desktop elements	Displays the ThinOS full taskbar and the classic desktop.	Displays the ThinOS full taskbar and the workspace desktop.
Access all published desktops	Click the icon on the classic desktop to launch the published desktop.	Click the Desktops icon on the purple ribbon to access all the published desktops.
Access all published apps	Click the icon on the classic desktop to launch the published application.	Click the **APPS** icon on the purple ribbon to access all the published desktops.
Access favorites	Not applicable	Click the **Favorites** icon on the purple ribbon.
Access Connection Manager	On the left corner of the taskbar, click .	Click the button menu in the upper-right corner of the screen, and then click **Connection Manager**.
Switch account when logged in with multi server	Displays all icons of desktop and applications. You cannot switch the account.	Click the button menu in the upper-right corner of the screen, and then click **Accounts**.
Refresh Citrix application	Click the PNAmenu button on the taskbar, and then click **Refresh**.	Click the button menu in the upper-right corner of the screen, and then click **Refresh**.
Reconnect a session	Click the PNAmenu button on the taskbar, and then click **Reconnect**.	Click the button menu in the upper-right corner of the screen, and then click **Connection Center** > **Reconnect**.
Disconnect from the session	Click the PNAmenu button on the taskbar, and then click **Disconnect**.	Click the button menu in the upper-right corner of the screen, and then click **Connection Center** > **Disconnect** .

Table 26. Classic mode vs Workspace mode (continued)

Item	Classic mode	Workspace mode
Log off all the connected ICA sessions	Click the PNAmenu button on the taskbar, and then click **Logoff**.	Click the button menu in the upper-right corner of the screen, and then click **Connection Center** > **Logoff**.
Sign out of broker agent	Click the **Sign-off** button in Connection Manager or from the **Shutdown** menu.	Click the button menu in the upper-right corner of the screen, and then click Sign out. You can also click **Sign out** from the **Shutdown** menu.
Use search bar	Not applicable	Use the search bar on the upper-right of the screen to search for your workspace item. You can open apps directly from the search results.
Access Desktop Viewer/Toolbar	Click the **Desktop Viewer/Toolbar** on the top center of the Citrix session screen to use the following toolbar options: • Home • Switch • Ctrl+Alt+Del • Window/Full-screen • Preferences • Save Layout • Disconnect • Sign Out You can switch a session between a window and a full-screen session window. Save layout is available only for the local AD user session and not for users who use SAML authentication to log in to the Citrix session.	Click the **Desktop Viewer/Toolbar** on the top center of the Citrix session screen to use the following toolbar options: • Home • Switch • Ctrl+Alt+Del • Window/Full-screen • Preferences • Save Layout • Disconnect • Sign Out You can switch a session between a window and a full-screen session window. Save layout is available only for the local AD user session and not for users who use SAML authentication to log in to the Citrix session.

Citrix ADC

ThinOS supports the Citrix Application Delivery Controller (ADC), formerly known as Citrix NetScaler. The following authentication methods are supported on ThinOS:

- Lightweight Directory Access Protocol (LDAP)
- RSA
- DUO
- SMS PASSCODE
- Native OTP
- Federated Authentication Service with Azure active directory
- OKTA
- PingID MFA
- FIDO2 authentication when connecting to on-premises stores

Timeout is enabled for Citrix ADC login by default. To disable the timeout, go to **Advanced** > **Broker Settings** > **Citrix Virtual Apps and Desktops Settings** from the Wyse Management Suite policy settings or the Admin Policy Tool, and disable the **Netscaler/ADC Login Timeout** option.

By default, the **NetScaler/ADC Authentication using web-based login** option is enabled for the applicable Citrix ADC server. To disable the web-based login, go to **Advanced** > **Broker Settings** > **Citrix Virtual Apps and Desktops Settings** from the Wyse Management Suite policy settings or the Admin Policy Tool, and disable the **Netscaler/ADC Authentication using web-based login** option.

NOTE: Dell Technologies recommends that you do not disable the **Netscaler/ADC Authentication using web-based login** option.

Citrix two-factor authentication

ThinOS supports Citrix two-factor authentication that authenticates the identity of the user twice before granting access, adding an extra level of security.

For local authentication, there must be a user profile that is created in the Citrix ADC database. For external authentication, the username and password that is entered must be the same as registered in the authentication server. After a successful validation of the username and password, the user is requested for another level of authentication.

ThinOS supports LDAP, RSA+LDAP, SMS Passcode, DUO, OKTA, and Azure MFA authentications by default. The user must only provide the Citrix ADC gateway address.

To log in to NetScaler Gateway that uses LDAP with RSA authentication, you must select **LDAP+RSA** in the **Wyse Management Suite** policy. You can also go to Admin Policy Tool and configure the **NetScaler/ADC Authentication Method** option in the **Citrix Virtual Apps and Desktops Settings** window.

For specific users who want to use Citrix ADC authentication methods, such as RSA, Dell Technologies recommends that you configure the **NetScaler/ADC Authentication Method with RSA** either using the Wyse Management Suite policy or Admin Policy Tool.

For specific users who want to use Citrix ADC authentication methods, such as LDAP with MFA, it is recommended that you configure the **NetScaler/ADC Authentication Method**with **LDAP** either using the Wyse Management Suite policy or the Admin Policy tool.

For specific users who want to use Citrix ADC authentication methods, such as RSA+LDAP with MFA, Dell Technologies recommends that you configure the **NetScaler/ADC Authentication Method** with **RSA+LDAP** either using the Wyse Management Suite policy or the Admin Policy tool. This setting is supported from Wyse Management Suite 3.5 and later versions.

Configure Citrix ADC using LDAP and RSA

About this task

This section describes how to configure the Citrix ADC (formerly NetScaler) using LDAP and RSA authentication.

Steps

1. Go to **NetScaler** > **NetScaler Gateway** > **Virtual Servers**, and click **Edit**.
2. Set the primary and secondary authentications that are based on the following scenarios:
   - If you use LDAP and RSA login, ensure that the primary authentication is LDAP and secondary authentication is RADIUS. You must also ensure that the **NetScaler Gateway Authentication Method** in the Wyse Management Suite policy or the Admin Policy Tool is configured as LDAP+RSA.
   - If you use RSA and LDAP login, ensure that the primary authentication is RADIUS and secondary authentication is LDAP.
   - If you use only LDAP login, ensure that the primary authentication is LDAP and secondary authentication is none.
3. Go to **System Setup** > **Remote Connections** and select **Citrix Virtual Apps and Desktops** from the **Broker type** drop-down list.
4. Enter the Citrix ADC server address in the **Broker Server** field.
5. Log off from the client desktop, or restart the thin client.
   The login window for Citrix ADC is displayed.

   For more information about configuring Citrix ADC with LDAP, RSA authentication, see the *Citrix NetScaler Gateway Guide* in the Citrix documentation website.

Configuring Citrix ADC using DUO

About this task

To configure the Citrix ADC (formerly NetScaler) using DUO authentication, do the following:

Steps

1. Go to **NetScaler** > **NetScaler Gateway** > **Virtual Servers**, and click **Edit**.
2. Ensure that the primary authentication is RADIUS that is configured with the DUO authentication RADIUS.

3. Ensure that the secondary authentication is none.
4. Enter the broker address in the ThinOS user interface.

Example

For more information about configuring Citrix ADC with DUO authentication, see the *Citrix NetScaler Gateway Guide* in the Citrix Duo website.

Configure Citrix ADC using CensorNet MFA authentication

Prerequisites

SMS PASSCODE is rebranded as CensorNet MFA. You can configure the Citrix ADC (formerly NetScaler) to use a One-Time Passcode or Password (OTP) in the form of a personal identification number (PIN) or passcode. To obtain this one-time password, you must install the CensorNet app on your mobile. After you enter the passcode or PIN, the authentication server invalidates the one-time password. You cannot enter the same PIN or password again. For more information about configuring a one-time passcode, see the Citrix documentation.

Prerequisites

- Citrix ADC (formerly NetScaler) v12.0 and later is installed on your client.
- SMS PASSCODE v9.0 SP1 or later is installed and configured in your network.
- Remote Authentication Dial-In User Service (RADIUS) authentication policy is configured and bind to the Citrix ADC server.
- CensorNet app is installed and configured on your mobile device.

About this task

To use the one-time passcode on ThinOS, do the following:

Steps

1. Log in to ThinOS and connect to the ADC URL.
2. Enter your credentials, and press **Enter**.
   The **PASSCODE** dialog box is displayed and a push notification from the CensorNet App on your phone with the code is received.
3. Click **Save**.
   If the authentication is successful, you are logged into the Citrix session.

Citrix ADC Native OTP

Citrix ADC (formerly NetScaler) Native OTP enables Citrix ADC Gateway to use one-time passwords (OTPs) for authentication without the need of an extra authenticating server. A one-time password that is generated by Google Authenticator is considered to be highly secure as passcodes are randomly generated.

If you access the Broker agent using Citrix ADC native OTP authentication, the lock terminal is not supported as it is a web-based authentication. When you try to use lock terminal, a message is displayed where you can click either **Continue** to log off or click **Cancel** to stay on the screen. You are automatically signed off from the account in sixty seconds for security purposes.

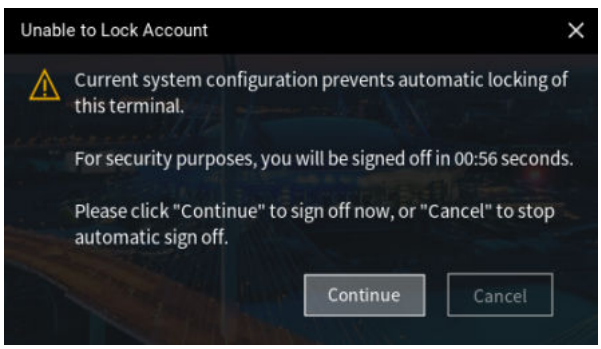

Figure 31. Unable to lock account

After logging into a VDI Broker agent with Web Authentication and locking the ThinOS session, you must set a temporary password to unlock the system.

A temporary password is not required. You can use the password that is used at the time of logging in to unlock the system directly.

For more information about Native OTP support for authentication, see the **NetScaler Gateway12.0 documentation** at docs.citrix.com.

Log in to Citrix ADC using the passcode

Prerequisites

- Ensure that you are using Citrix ADC (formerly NetScaler) 12.0 build 51.24 and later versions.
- Ensure that you have registered your device with Citrix ADC. For a detailed procedure on how to register your device with Citrix ADC, see the Native OTP support for authentication article at docs.citrix.com.

About this task

This section describes how to log in to Citrix ADC using the OTP.

Steps

1. From the desktop menu, click **System setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. Click the **Broker Setup** tab and select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list.
3. Enter the IP address of the Citrix ADC FQDN server in the **Broker Server** field.
   You can configure other options if required.
4. Click **OK**.
   The NetScaler login window is displayed.
5. Launch the Google Authenticator application on your phone and get the passcode.
6. In the Citrix ADC login window, enter the passcode and click **OK**.
   If the authentication is successful, you are logged into Citrix ADC.

Citrix Federated Authentication Service SAML with Microsoft Azure Active Directory

ThinOS supports the Citrix Federated Authentication Service with Microsoft Azure Active Directory during single sign-on to Citrix ADC using the Security Assertion Markup Language (SAML) based authentication. The FAS server delegates the user authentication to the Microsoft ADFS server or Azure AD with Security Assertion Markup Language (SAML). Both, Azure AD Multiple Factors Authentication (MFA) and Self-service password reset (SSPR), are supported.

NOTE: To use this function, you must enable Federated Authentication Service. If the Federated Authentication Service is disabled, the Citrix ADC session fails to launch.

If you access the Broker agent using SAML, the lock terminal is not supported as it is a web-based authentication. When you try to use lock terminal, a message is displayed where you can click either **Continue** to log off or click **Cancel** to stay on the screen. You are automatically signed off from the account in sixty seconds for security purposes.

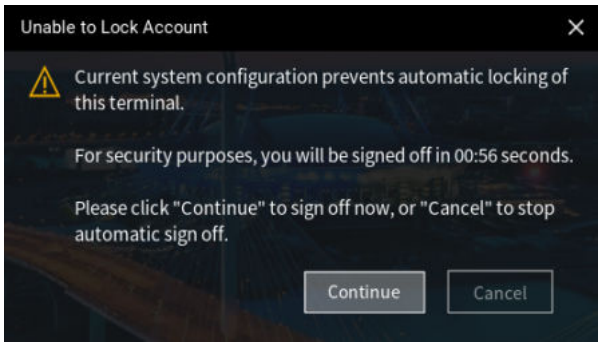

Figure 32. Unable to lock account

After logging into a VDI Broker agent with Web Authentication and locking the ThinOS session, you must set a temporary password to unlock the system.

A temporary password is not required. You can use the password that is used at the time of logging in to unlock the system directly.

Limitation: **Don't ask again for X days** and **Don't show this again** messages are not displayed during Azure SAML MFA login (X means the number of days). This issue also occurs in the Citrix Workspace App Linux binary.

Enable Azure Multiple Factor Authentication for Citrix ADC Single Sign-on with SAML Authentication

Prerequisites

- Create an Azure AD user in Azure Active Directory.
- Enable the Multiple Factor Authentication (MFA) for the user.
- Add the user to Azure AD Citrix ADC (formerly NetScaler) Enterprise application users and groups.
- Ensure that the shadow account of the user exists in the local domain users group.
- Ensure that the SAML authentication policy is enabled. For more information, see the NetScaler Gateway documentation at docs.citrix.com.

About this task

This section describes how to log in to Citrix ADC using SAML with Azure Multiple Factor Authentication.

Steps

1. From the desktop menu, click **System setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. On the **Broker Setup** tab, select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list.
3. Enter the Citrix ADC Gateway URL in the **Broker Server** field, and click **OK**.
   The login window is displayed.
4. Enter the username of the Azure AD user and click **Next**.
5. Enter the initial password for the Azure AD user, and click **Sign in**.
6. In the **More information required** window, click **Next**.
7. On the **Additional Security Verification** page, do the following:
   a. From the **How should we contact you?** drop-down list, select any of the following methods:
      - Authentication phone
      - Mobile app
   b. If you select **Authentication phone**, enter your phone number. If you select **Mobile App**, click **Set up** and follow the on-screen instructions to add an account to the Microsoft authenticator app.
   c. Click **Save**.
8. Enter the Azure AD username with the initial password again.
9. If you are using mobile app, approve the notification. If you are using the authentication phone, verify your information through a phone call or a text code.
10. Log in to Citrix ADC and launch the session.

Enable Azure AD Self-Service Password Reset function for Citrix ADC Single Sign-on with SAML authentication

Prerequisites

1. Create an Azure AD user in Azure Active Directory.
2. Add the user to Azure AD Citrix ADC (formerly NetScaler) Enterprise application users and groups.
3. Ensure that the shadow account of the user exists in local domain users group.
4. Ensure that **Self-Service Password Reset Enabled** option is selected in Azure AD for the user.

About this task

This section describes how to enable Azure AD Self-Service Password Reset function for Citrix ADC Single Sign-on with SAML authentication.

Steps

1. On the **Broker setup** tab, select **Citrix Virtual Apps and Desktops** from the **Broker type** drop-down list.
2. In the **Broker Server** field, enter the Citrix ADC Gateway URL, and click **OK**.
   The login window is displayed.
3. Enter the user credentials of the Azure AD user and click **Next**.
4. On the **Don't lose access to your account!** page, configure the following options:
   - **Authentication Phone**
     a. Click **Set it up now**.
     b. From the drop-down list, select your country code.
     c. Enter your phone number.
     d. Click either **text me** or **call me**. A verification code is received on your phone by call or text message.
     e. Enter the verification code and click **Verify**.
   - **Authentication Email**
     a. Click **Set it up now**.
     b. Enter the valid email address.
     c. Click **email me**. A verification code is sent to your email.
     d. Enter the verification code and click **Verify**.
5. Click **Finish**.
6. Continue with the user login.

Configure Citrix NetScaler using Okta

Okta provides Single Sign-On (SSO) capability using Remote Authentication Dial-In User Service (RADIUS) for Citrix Virtual Apps and Desktops. ThinOS supports Okta through the Citrix NetScaler Gateway 11.0 or later. The Okta RADIUS Agent is used for user authentication. The Okta RADIUS server agent assigns the user authentication to Okta using single-factor authentication (SFA) or multifactor authentication (MFA).

For more information about configuring Citrix NetScaler Gateway to use the Okta RADIUS Agent, see the *Citrix NetScaler Gateway Radius Configuration Guide* at help.okta.com.

NOTE:

- On the ThinOS client, you need UPN at the login window.
- Phone authentication by using Okta is supported only in US and Canada.

Limitation

In ThinOS only OKTA with Citrix Gateway (RADIUS) is verified. However, the StoreFront with OKTA SAML authentication or OKTA with Citrix Gateway (SAML) is not verified. OKTA with Citrix Gateway (SAML) is supported in ThinOS and Citrix Workspace App 2209.

Log in to Citrix ADC using MFA with SAML, OKTA as IDP, and Citrix FAS for SSO to VDA

This section describes how to log in to Citrix Application Delivery Controller (ADC) through Multiple Factors Authentication (MFA) with Security Assertion and Markup Language (SAML). This section also describes how to log in to Citrix ADC using OKTA as the identity provider, and Citrix FAS for Single Sign-On (SSO) to VDA.

Steps

1. From the desktop menu, go to **System setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. Click the **Broker Setup** tab and select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list.

3. Enter the Citrix ADC gateway server URL in the **Broker Server** field. You can also configure other options.
4. Click **OK**.
   The **NetScaler gateway Webview login** window is displayed, and you are redirected to Okta IDP for authentication.
5. Enter the user credentials with UPN format and password.
   If you have not registered your phone with Okta Verify, you are prompted to setup MFA.
6. Select **Enter a code** or **Get a push notification** security method using Okta Verify application.
7. Launch the Okta Verify application on your phone.
   - If you selected **Enter a code** previously, enter the code in the Citrix ADC login window and click **Verify**.
   - If you selected **Get a push notification**, approve the push notification on your phone once you get it.

   If the authentication is successful, you are logged into Citrix ADC.

   NOTE: ThinOS does not support Okta Single Sign-On (SSO) with Certificate Authentication.

   After logging into a VDI Broker agent with Web Authentication and locking the ThinOS session, you must set a temporary password to unlock the system.

   A temporary password is not required. You can use the password that is used at the time of logging in to unlock the system directly

Log in to Citrix ADC using PingID Multi Factor Authentication

You can log in to Citrix ADC (NetScaler) with PingID Multi Factor Authentication.

1. From the desktop menu, go to **System setup > Remote Connections**. The **Remote Connections** dialog box is displayed.
2. Click the **Broker Setup** tab and select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list.
3. Enter the Citrix ADC gateway server URL in the **Broker Server** field. You can also configure other options.
4. Click **OK**. The NetScaler gateway Webview login window is displayed, and you are redirected to PingIdentity for authentication.
5. Enter the user credentials with UPN format and password. When you log in for the first time to PingID, a download link and QR code is displayed that helps install the authenticator in your phone.
6. Launch the PingID application on your phone and **Slide up** in the application to complete the authentication.

FIDO2 authentication when connecting to on-premises stores

You can use the default ThinOS Extension as the WebLogin engine or Citrix Enterprise Browser (CEB) to connect to the on-premises stores.

ThinOS Extension

You can authenticate using FIDO2 security keys, which do not require passwords, when signing in to on-premises stores. Citrix Workspace app uses the **ThinOS Extension** as the default browser for FIDO2 authentication in ThinOS. Administrators can configure the **ThinOS Extension** using Admin Policy Tool or Wyse Management Suite policy settings to authenticate to CWA. To enable FIDO2 authentication for logging in to on-premises stores, do the following:

Steps

1. Open Admin Policy Tool or Wyse Management Suite policy.
2. Go to **Broker Settings > Citrix Virtual Apps and Desktops Settings**.
3. Set **Broker server address** to the address that has enabled FIDO2 authentication method.

   NOTE: FIDO2 Security Key to log in to Citrix ADC with OKTA SAML MFA and FIDO2 Security Key to log in to Citrix ADC with Azure AD MFA are two test environments that can be used in ThinOS.

4. Enable **WebLogin Use External Engine**.

   NOTE: The wording of the setting is updated to **Use External Engine for WebLogin**.

5. Ensure that **WebLogin Use ThinOS Extension** is **ThinOS Extension**. **ThinOS Extension** is the only supported extension and is the default value.

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

NOTE: The wording of **WebLogin Use ThinOS Extension** setting is updated to **WebLogin Engine**.

6. Click **Save & Publish**.
7. Sign out or restart the device for the settings to take effect.
8. In the webview login window, enter the PIN code of the Yubikey device.
9. Touch the Yubikey device to log in to the Citrix broker server.

Citrix Enterprise Browser (CEB)

An Administrator can configure the Citrix Enterprise Browser (CEB) WebLogin Engine using Admin Policy Tool or Wyse Management Suite policy settings to authenticate to CWA. To enable FIDO2 authentication for logging in to on-premises stores, do the following:

Steps

1. Open Admin Policy Tool or Wyse Management Suite policy.
2. Go to **Broker Settings > Citrix Virtual Apps and Desktops Settings**.
3. Set **Broker server address** to the address that has enabled FIDO2 authentication method.

   NOTE: You can use FIDO2 Security Key to log in to Citrix ADC with OKTA SAML MFA and Citrix ADC with Azure AD MFA. The two test environments can be used in ThinOS.

4. Enable **Use External Engine for WebLogin**.
5. Ensure that **WebLogin Engine** is **CEB**.

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

6. Click **Save & Publish**.
7. Sign out or restart the device for the settings to take effect.
8. In the webview login window, enter the PIN code of the Yubikey device.
9. Touch the Yubikey device to log in to the Citrix broker server.

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

FIDO2 Authentication

From ThinOS 2505 build 10.X.XXXX onwards, FIDO2 enrollment and authentication in Omnissa Workspace One Access and smartcard authentication in Azure MFA are supported.

Ensure that the ThinOS Chrome browser package is installed.

To enable the feature, do the following:

- Go to **Omnissa Horizon Settings** in Wyse Management Suite or Admin Policy Tool.
- Enable **WebLogin Use Chrome Browser**.

Verify the Yubikey authentication

Prerequisites

Image and boot the device.

About this task

This section describes how to verify if the notification appears when a Yubikey is inserted into the device.

Steps

1. Insert the Yubikey into the device.
2. Verify whether the notification is displayed or not.
3. Go to **Taskbar** > **Manage security keys** > **Register Yubikey**.
4. Click **Try WEBAUTHN** and follow the instructions to authenticate and authorize.
   Yubikey authentication is now complete.

Citrix Cloud services

ThinOS supports Citrix Cloud services. It acts as a single management console to deploy applications or desktops on any virtual or cloud setup for a secure digital workspace. For more information about Citrix Cloud services, see the Citrix Cloud article at docs.citrix.com.

Getting started with Citrix Cloud

About this task

This section describes how to log in to the Citrix Cloud server on your thin client.

Steps

1. From the desktop menu, click **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. On the **Broker Setup** tab, select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list, and do the following:
   a. Select the **Workspace Mode** check box if you want to enable the Citrix Workspace-based layout of published applications and desktops. If this option is not selected, you are logged in to the classic mode.
   b. In the **Broker Server** field, enter the Citrix Cloud URL.
   c. In the **Auto Connect List** field, enter the name of the desktops that you want to launch automatically after logging in to Citrix Cloud. You can enter more than one desktop. Each desktop name is separated by a semi-colon and is case sensitive.
   d. Select the **Enable automatic reconnection at logon** check box if you want to automatically reconnect to the disconnected sessions or both active and disconnected sessions during login. You must click either of the following options:
      - **Connect to disconnected session only**
      - **Connect to active and disconnected sessions**
   e. Select the **Enable automatic reconnection from button menu** check box if you want to automatically reconnect to the disconnected sessions or both active and disconnected sessions by using the Reconnect button in the button menu. You must click either of the following options:
      - **Connect to disconnected session only**
      - **Connect to active and disconnected sessions**
3. Click **OK** to save your settings.
4. In the login window, enter your domain username and password to log in to Citrix Cloud.
   ICA icons are displayed in **Connection Manager** and on the client desktop.

Android smartphone USB redirection through Citrix Configuration Editor

You can configure the Android smartphone device redirection using **Citrix USB File Settings** in Citrix Configuration Editor. To redirect the Android smartphone into an ICA session, do the following:

Steps

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

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

Automatically configure using DNS for email discovery

You can connect to a Citrix session by using an email address. The email address is used to discover the StoreFront or NetScaler Gateway URL.

Prerequisites

- Install a valid server certificate on the StoreFront/AppController server and Access Gateway appliance.
- The full chain or path to the root certificate must be correct.

About this task

This section describes how to connect to a Citrix session by using email-based discovery.

Steps

1. Add a service record (SRV) to your DNS server to enable email-based discovery. To add a service record to the DNS server, do the following:
   a. Log in to the DNS server.
   b. Go to **DNS** > **Forward Lookup Zone**.
   c. Right-click **Forward Lookup Zone**, and click **Other New Records**.
   d. In the **Resource Record Type** dialog box, select **Service Location (SRV)**.
   e. Click **Create Record**.
   f. In the **Service** field, enter `_citrixreceiver`.
   g. In the **Protocol** field, enter `_tcp`.
   h. In the **Port number** field, enter the port number.
   i. In the **Host offering this service** field, enter the FQDN and the port for the StoreFront/AppController server or Access Gateway appliance.

      NOTE: You cannot use the same FQDN for both StoreFront and the Access Gateway virtual servers.

2. On ThinOS, go to **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
3. On the **Broker Setup** dialog box, select **Citrix Virtual Apps and Desktops** from the **Broker Type** drop-down list.
4. Enter the email address in the **Broker Server** field, and click **OK**.
5. Restart the thin client.
6. In the login window, enter your email address and password to log in to the session.

Citrix HDX Adaptive transport (EDT)

ThinOS supports Citrix HDX Adaptive transport for Citrix Virtual Apps and Desktops. HDX Adaptive transport enables the ICA virtual channels to automatically adapt to varying LAN and WLAN connections and improves the data throughput.

For more information about Citrix HDX Adaptive transport, see the **Citrix documentation** at docs.citrix.com.

Enable HDX Adaptive Transport

About this task

This section describes how to enable the HDX Adaptive Transport policy setting on Citrix Studio.

Steps

1. Go to **Citrix Studio** > **HDX Adaptive Transport** policy.
2. Set the value for HDX Adaptive Transport to either **Preferred** or **Diagnostic mode**.
   For more information about configuration on Citrix Studio, see the Adaptive Transport article at docs.citrix.com.
3. On the ThinOS client, start a session from the Citrix Workspace app.
   The connection is established using adaptive transport.

   NOTE: If the connection type is HDX and the protocol is UDP, EDT is active for the session. If the protocol is TCP, the session is in fallback mode.

   For information about how to verify if HDX Adaptive Transport is active, see the FAQs section in this guide.

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

   a. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.
   b. In the Citrix ICA File Settings, click **Add Row**.
   c. In the **Key** field, enter **`HDXOverUDP`**.
   d. In the **Value** field, enter **`Off`**.
   e. Sign out or restart the device for the settings to take effect.

   To enable HDX Enlightened Data Transport using Citrix Configuration Editor, do the following:

   a. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.
   b. In the Citrix ICA File Settings, click **Add Row**.
   c. In the **Key** field, enter **`HDXOverUDP`**.
   d. In the **Value** field, enter **`Preferred`**.
   e. Sign out or restart the device for the settings to take effect.

Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT)

From ThinOS 2311 and Citrix Workspace App package 23.9.0.24.4, Maximum Transmission Unit (MTU) discovery in Enlightened Data Transport (EDT) is supported.

- MTU increases the reliability and compatibility of the EDT protocol and provides an improved user experience.
- MTU Discovery enables EDT to automatically determine the Maximum Transmission Unit (MTU) when establishing a session.
- This prevents EDT packet fragmentation that might result in performance degradation or failure to establish a session.
- System requirements:
  - Citrix Virtual Delivery Agent (VDA) 2003 and later
  - Citrix Workspace app package version 23.9.0.24.4 and later
  - Session reliability enabled
- MTU Discovery is enabled by default. To disable EDT MTU Discovery, configure the following registry values and restart the VDA:
  - Key: **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`**
  - Value name: **`MtuDiscovery`**
  - Value type: **`DWORD`**
  - Value data: **`0`**

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

- To configure Maximum Segment Size (MSS) when using EDT on networks with nonstandard MTU, do the following:

1. You can set the EDT MTU Discovery Registry key value below to disabled (value 0) and restart the VDA.
   - Key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**
   - Value name: **MtuDiscovery**
   - Value type: **DWORD**
   - Value data: **0**

   NOTE: If the value is **1**, then MTU discovery is enabled. If the value is **0**, MTU discovery is disabled.

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

   NOTE: By design, Citrix Workspace App does not support disable EDT MTU Discovery from the client side. You can enable or disable EDT MTU Discovery on VDA.

HDX Adaptive Display V2

ThinOS supports the selective use of a video codec (H.264) to compress graphics during video playback in an ICA session. This feature combines the H.264 mode and Thinwire Compatible mode for a better user experience.

For more information about HDX Adaptive Display V2, see the **Citrix documentation** at docs.citrix.com.

Enable HDX Adaptive Display V2

About this task

This section describes how to enable HDX Adaptive Display V2 using Citrix Studio.

Steps

1. Go to **Citrix Studio** > **Use video codec for compression policy**.
2. Select the **For actively changing regions** option.
3. On the ThinOS client, launch an ICA desktop.
4. Open the web browser and play your preferred video.

   HDX adaptive display V2 is used for video decoding on the ThinOS client. Thinwire uses JPEG (lossy) for complex or photographic imagery and RLE (lossless) for text imagery. The rest of the screen is decomposed by Thinwire.

   For more information about the Use video codec for compression policy, see the **Graphics Policy Settings** article at docs.citrix.com.

Browser content redirection

Browser content redirection (BCR) enables any web browser content, including HTML 5 videos, to be redirected to the ThinOS client and not redirected on the VDA side.

Browser content redirection proxy setting— If you use the browser content redirection proxy settings, enter a valid proxy address and port number in the browser content redirection proxy configuration policy. Citrix Workspace app follows the server fetch and client render mechanism to fetch URL from VDA and redirect browser content from the client.

NOTE: BCR with Chromium Embedded Framework (CEF) is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.

The Citrix browser content redirection CEF cache file is changed from the default `.ICAClient` to `/tmp/citrix`. CEF cache file in `/tmp/citrix` is cleared when you log out.

Enable Browser Content Redirection

Prerequisites

- If you are using a Chrome browser, import the BCR extension into the browser.
- If you are using an Edge browser, import the BCR extension into the browser.
- If you are using a IE browser, ensure the Citrix HDXJsInjector add-on exists in the browser.
- If you are using an RDS-hosted desktop, and if you are using a IE browser, install the BCR add-on manually from Citrix virtual apps and desktops IOS installer.
- If you want to play a QUMU video, you must add the QUMU video URL to the Citrix policy.

About this task

This section describes how to enable Browser Content Redirection using Citrix Studio.

Steps

1. Go to **Citrix Studio** > **Browser Content Redirection policy**.
2. Select the **Allowed** option.
   This enables the Browser Content Redirection policy.
3. In the **Browser Content Redirection Access Control List (ACL) policy** settings, add URLs that can use the browser content redirection.

   NOTE: Ensure that the URL is not listed in the Browser Content Redirection Blacklist Configuration policy.

4. On the ThinOS client, launch an ICA desktop.
5. Open either IE or Chrome and enter the URL that you have added in the Access Control List (ACL).
   The browser viewport is rendered on the ThinOS client side. Browser attributes such as Address Bar and Status Bar still run on the VDA side.

   For more information about Browser Content Redirection, see the **Browser Content Redirection** article at docs.citrix.com.

HTML5 Video Redirection

HTML5 Video Redirection controls and optimizes the way Citrix Virtual Apps and Desktops servers deliver HTML5 multimedia web content to users. This feature is available for internal web pages only. It requires the addition of JavaScript to the web pages where the HTML5 multimedia content is available, for example, videos on an internal training site.

The following policies must be enabled on the server side:

- **Windows Media redirection**—By default this option is enabled.
- **HTML5 video redirection**—By default this option is disabled.

For more information about the ICA Multimedia policy settings, see the **Citrix documentation** at docs.citrix.com.

For information about how to verify if HTML5 Video Redirection is working, see the FAQs section in this guide.

Windows Media Redirection

Windows Media Redirection enables the audio and video to be rendered on the user device instead of running on the server side. Using the Windows Media Redirection feature, you can optimize the performance of Windows Media player on virtual Windows desktops.

For more information about Windows Media Redirection, see the **Citrix documentation** at docs.citrix.com.

Enable Windows Media Redirection

Prerequisites

Ensure that the **Windows Media redirection** policy is set to **Allowed** in Citrix Studio. By default, the value is set to **Allowed**.

About this task

This section describes how to enable the Windows Media Redirection feature on your thin client.

Steps

1. On the ThinOS desktop, click **Connection Manager**.
2. Click **Global Connection Settings**.
3. Select the **Enable HDX/MMR** check box for the ICA connection.
4. Go to **System Setup** > **Remote Connections**.
5. On the **Broker Setup** tab, select **Citrix Virtual Apps and Desktops** from the **Broker type** drop-down list.
6. Enter the Citrix server in the **Broker Server** field, and click **Save**.
7. Launch an ICA desktop.
8. Open Windows Media Player and play a video or an audio file.

   The following types are supported:

   - H.264 video
   - WMV-9 video
   - WMV-8 video
   - WMV-7 video
   - WMC1 video
   - MP4 video
   - 4K video
   - MOV/AVI video
   - AAC/MP3/WMA file

   For information about how to check if Windows Media Redirection is working, see the FAQs section in this guide.

   For more information about the ICA Multimedia policy settings, see Citrix Product documentation at docs.citrix.com.

QUMU Video Optimization Pack for Citrix

QUMU's Video Optimization Pack (VOP) for Citrix enables you to stream quality videos to endpoints managed by Citrix Virtual Apps and Desktops servers by enabling client-side fetching. The QVOP video player runs on the client side, and the video stream uses the client's network to go directly to QUMU's Video Control Center instead of accessing through VDI desktops.

Prerequisites

Ensure that the **Windows Media redirection** policy is set to **Allowed** in Citrix Studio. By default, the value is set to **Allowed**.

About this task

This section describes how to use QUMU Video Optimization Pack for Citrix on your thin client.

Steps

1. On the ThinOS desktop, click **Connection Manager**.
2. Click **Global Connection Settings**.
3. Select the **Enable HDX/MMR** check box for the ICA connection.
4. Go to **System Setup** > **Remote Connections**, select **Citrix Virtual Apps and Desktops** from the **Broker** type drop-down list.
5. On the **Broker Setup** tab, enter the Citrix server in the **Broker Server** field, and click **Save**.
6. Launch an ICA desktop.
7. Use Citrix Browser Content Redirection to play QUMU videos.

For information about Browser Content Redirection, see Browser Content Redirection. For more information about the ICA Multimedia policy settings, see Citrix Product documentation at docs.citrix.com.

Citrix Self-Service Password Reset

You can reset the password or unlock the account after you complete the security questions enrollment.

Supported Environment

- Citrix Virtual Apps and Desktops 7.11 and later versions
- Support StoreFront Server 3.7 and later versions
- Self-Service Password Reset Server 1.0 and later versions

Supported platforms—All platforms are supported.

Limitation

- Supports only StoreFront Server

Before resetting a password or unlocking an account

Before resetting your password or unlocking your account, you must register for the security questions enrollment. To register your answers for the security questions, do the following:

1. To access the **Security Questions Enrollment** window, do the following step that is applicable to the mode:
   a. In Classic mode, click the **Manage Security Questions** option from the PNAmenu.
   b. In Workspace mode, click the **TASKS** icon on the purple ribbon and click **Start**.
   The **Security Questions Enrollment** window is displayed.
2. Enter the appropriate answers to the question set.
3. Click **OK** to register the security questions.

Use the Account Self-Service

After the security questions enrollment is complete, and when ThinOS is connected to a StoreFront server with Self-Service Password Reset enabled, the **Account Self-Service** icon is displayed in the sign-on window.

NOTE: If you enter the wrong password more than four times in the Sign-on window, the client automatically enters the account unlocking process.

1. Click the **Account Self-Service** icon to unlock your account or reset your password.

   NOTE: You must register the security questions for users before using the **Unlock account** or reset password feature.

2. Click **Unlock account** or **Reset password** based on your choice, and then click **OK**.

Unlock an account

After you register the security questions, do the following to unlock your account:

1. Choose a task (Unlock account) in the **Account Self-Service** window.
2. Enter the username. The **Unlock Account** dialog box is displayed.
3. Enter the registered answers to the security questions. If the provided answers match the registered answers, then the **Unlock Account** dialog box is displayed.
4. Click **OK** to successfully unlock your account.

NOTE: If the provided answers are incorrect, an error message is displayed. If you provide the wrong answers more than three times, you cannot unlock the account or reset the password, and error messages are displayed.

Reset a password

After you register the security questions, do the following to reset your password:

1. Choose a task (Reset password) in the **Account Self-Service** window.
2. Enter the username. The **Reset Password** dialog box is displayed.
3. Enter the registered answers to the security questions. If the provided answers match the registered answers, then the **Reset Password** dialog box is displayed.
4. Enter and confirm the new password.
5. Click **OK** to successfully change the password.

If you provide the wrong answers, you cannot reset the password, and an error message is displayed.

Citrix SuperCodec

Citrix SuperCodec is a H.264 decoder integrated on the ThinOS client side. The server encodes the session image into the H.264 stream and sends it to the client side. The client decodes the H.264 stream by SuperCodec and display the image on the screen. This feature improves the user experience, especially for HDX 3D Pro desktops.

Citrix SuperCodec is supported in Citrix Virtual Apps and Desktops (XenApp and XenDesktop) version 7.5 or later versions.

In Citrix Virtual Apps and Desktops version 7.9 and later, the default setting for **Use video codec for compression** is **Use when preferred**. For best performance on ThinOS device, it is recommended that you set the **Use video codec for compression** policy to **For the entire screen**. You can set the policy to **Do not use video codec**. This policy setting allows ThinOS to use **ThinWire Plus** that saves bandwidth and reduces the CPU overhead. You can also set the policy to **For actively changing regions**. This policy setting allows ThinOS to use **Selective H.264**.

- **ThinWire Plus**—Equivalent to the **Do not use video codec** option
- **Fullscreen H.264**—Equivalent to the **For the entire screen** option
- **Selective H.264**—Equivalent to the **For actively changing** regions

Anonymous logon

The Anonymous logon feature enables the users to log into the StoreFront server configured with unauthenticated store without Active Directory (AD) user credentials. It allows unauthenticated users to access the applications instead of AD accounts.

NOTE: Anonymous logon is not supported with legacy mode of StoreFront server.

NOTE: After ThinOS 2208, **Lock Terminal** is supported for Anonymous logon.

Enable UDP audio in a Citrix session

Citrix recommends that you use audio over User Datagram Protocol (UDP) in low-bandwidth network connections for better audio quality. ThinOS does not support UDP audio over Citrix ADC (formerly NetScaler) due to Linux Citrix Workspace app limitation.

Steps

1. Start the **Admin Policy Tool** on your ThinOS 10.x based device or open the **ThinOS 10.x** Policy settings in Wyse Management Suite.

   If you are using the Admin Policy Tool on ThinOS, you must first select the audio quality as Medium and then enable UPD audio. UPD audio is automatically disabled when you select the audio quality as **High** in Admin Policy Tool. However, the UPD audio is not automatically disabled when you are configuring the setting using Wyse Management Suite. UPD audio may not work if you set the audio quality as High using Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **Citrix Session Settings**.
3. In the **Basic Settings** section, click the **Enable UPD Audio** toggle key to the **ON** state.

   NOTE: Adaptive audio works while using User Datagram Protocol (UDP) audio delivery. Adaptive audio is enabled by default. This feature requires VDA version 2112 or later versions. For more information, see the **Citrix Virtual Apps and Desktops** Citrix documentation website.
4. From the **Audio Quality** drop-down list, select **Medium**.

If you are using the Admin Policy Tool on ThinOS, you must first select the audio quality as **Medium** and then enable UPD audio. UPD audio is automatically disabled when you select the audio quality as **High** on Admin Policy Tool. However, the UPD audio is not automatically disabled when you are configuring the setting using Wyse Management Suite. UPD audio may not work if you set the audio quality as **High** using Wyse Management Suite.

Keyboard layout synchronization in VDA

In the Citrix Workspace app, the Keyboard Dynamic synchronization mode functions differently on a Linux client from a Windows client. In general, on a Linux client, the keyboard output follows the client keyboard layout, which is different from the Windows VDA layout. If a Linux client keyboard is synchronized to a Windows VDA, users may observe unpredictable keyboard output. Also, in dynamic synchronization mode, the Citrix Workspace app for Linux does not support VDA users to switch the keyboard layout inside a VDA session.

In the server default mode, both Linux and Windows use the session (VDA) side keyboard layout with predictable output. You can configure the keyboard layout mode using either Wyse Management Suite or Admin Policy Tool. The keyboard layout that you select on the thin client is not automatically synchronized in the VDA session. ThinOS supports the server default mode that enables VDA users to select or switch the keyboard layout inside the VDA session using the Windows Input Method Editor (IME) language bar. For other modes such as Specific keyboard, Client Setting, or Dynamic Sync, there can be unpredictable mismatch in the keyboard output if you switch the keyboard layout in VDA. This is because the Citrix Workspace app Linux keyboard sync mode does not support switching the layout in VDA.

As a VDA administrator, you must configure the VDA desktop with the required keyboard language layout options. The IME language bar must be enabled on the Windows lock screen. The VDA user can select the appropriate keyboard language layout on the Windows lock screen.

In scenarios such as opening a new application in a VDA session, locking, or unlocking the VDA session, the keyboard layout falls back to the VDA default layout. For example, EN_US. This is a known issue for a Linux client in the **server default** mode.

You can customize VDA registry settings for a consistent keyboard layout in the VDA session.

- For a desktop operating system VDA, the feature is enabled by default.
- For a server operating system VDA, you can enable the feature using the system registry.
  1. In the system registry of VDA, go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout`.
  2. Create a DWORD entry `IgnoreRemoteKeyboardLayout=1`. By default, the `IgnoreRemoteKeyboardLayout` entry is unavailable. The default keyboard is set to ENG, irrespective of the Control Panel setting. For example, open an application, lock, or unlock the session, the keyboard is set to ENG. To resolve this issue, ensure that you set `IgnoreRemoteKeyboardLayout=1`.

For information about the Keyboard Layout Modes and Keyboard Layout rules in the Citrix Workspace app, see the **Citrix Virtual Apps and Desktops keyboard and IME configurations** article at Citrix | Blogs.

Table 27. Citrix Workspace app keyboard layout configuration for VDA users on ThinOS

VDA user scenario	Wyse Management Suite settings	VDA settings	Summary
The client keyboard is synchronized to VDA, and the keyboard layout is not switched in the VDA desktop or application.	Configure the required keyboard layout for local client users and remote VDA users.	Set the VDA policy for Dynamic synchronization.	Keyboard output follows the client Linux keyboard layout and not the Windows layout. As a result, there can be an unpredictable mismatch in the keyboard output. Citrix Workspace app Linux keyboard sync mode does not support switching the layout in VDA.
The client keyboard is synchronized to VDA, and the keyboard layout is switched in the VDA desktop using the IME language bar.			
The client keyboard is synchronized to VDA, and the keyboard layout is switched in VDA published applications			

Table 27. Citrix Workspace app keyboard layout configuration for VDA users on ThinOS (continued)

VDA user scenario	Wyse Management Suite settings	VDA settings	Summary
using the IME language bar.			
The client keyboard is not synchronized to VDA, and the keyboard layout is not switched in the VDA desktop or application.	Configure the required keyboard layout for using the client locally. There is no impact to the keyboard usage on remote VDA.	No specific settings are required. For recommended settings, see the **VDA settings for server default mode** section.	Keyboard layout follows the VDA Windows layout with predictable output. When opening a new application in a VDA session, locking the VDA session, or unlocking the VDA session, the keyboard layout falls back to the VDA default layout. For example, EN_US. The following are the recommended settings for VDA administrators: • Enable multiple layouts in VDA IME. • Enable IME on the Windows lock screen. • Set the default keyboard layout to any non-English keyboard layout. • In the system registry of VDA, go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout` and create the following DWORD entry: `IgnoreRemoteKeyboardLayout=1`. For more information, see the *Citrix article CTX223316* in Citrix | Knowledge Center.
The client keyboard is not synchronized to VDA, and the keyboard layout is not switched in the VDA desktop using the IME language bar.			
The client keyboard is not synchronized to VDA, and the keyboard layout is not switched in VDA published applications using the IME language bar.			

Table 28. Language keyboard layout settings

ThinOS keyboard layout	Windows layout	Wyse Management Suite settings	Citrix Workspace app Linux dynamic synchronization	Recommended settings
Polish	The keyboard layout partially matches with the Windows layout.	Supported	Enabled	• On the client side, select the keyboard layout that fully matches with the Windows layout for local usage. • On the VDA side, select the best layout from the Windows IME language bar after the connection is established. • For VDA administrators, see the **Citrix Workspace app keyboard layout configuration for VDA** users on ThinOS table in this document.
Polish (Legacy)	The keyboard layout fully matches with the Windows layout.	Supported	Enabled	
French (France)	The keyboard layout partially matches with the Windows layout.	Supported	Enabled	
French (Microsoft)	The keyboard layout fully matches with the Windows layout.	Supported	Enabled	
Belgian	The keyboard layout does not match with the Windows layout.	Supported	Enabled	
Belgian (Comma)	The keyboard layout fully matches with the Windows layout.	Supported	Enabled	

Table 28. Language keyboard layout settings (continued)

ThinOS keyboard layout	Windows layout	Wyse Management Suite settings	Citrix Workspace app Linux dynamic synchronization	Recommended settings
Spanish	The keyboard layout does not match with the Windows layout.	Supported	Enabled	

VDA settings for Server Default mode

When set to server default mode, the keyboard layout falls back to the VDA default layout. For example, EN_US. This issue can be related to Citrix Workspace app or Windows server operating system 2016 and 2019. All workarounds may require you to modify registry keys on the server side. For more information about workarounds, see the Citrix articles **CTX269153** and **CTX223316** at support.citrix.com. If you do not want to modify registry keys, contact the Citrix support team or the Microsoft support team.

Table 29. Citrix Workspace app Linux keyboard layout settings—Client and VDA

Mode	Client-side settings	Server or VDA-side settings	Additional information

Server default	• `~/.ICAClient/wfclient.ini`
	• `[WFClient]`
	• `keyboardlayout=(Server Default)`
		Setting is configured on the StoreFront server. For example, `C:\inetpub\wwwroot\Citrix\[store name]\App_Data\default.ica`
		`[WFClient]`
		`keyboardlayout=(Server Default)`
			Set the mode on either the client side or the server side. This mode takes the highest priority.

Specific keyboard	• `~/.ICAClient/wfclient.ini` • `[WFClient]` • `keyboardlayout=French`	**XenApp server version 2006 and higher**—Enable the following policies on the server side: • Set the **Enable Unicode keyboard layout mapping** to **Allowed**. **XenApp server version before 2006**—There are no policies available to enable specific keyboard sync mode. You must set the registry key in the Windows VDA desktop Keyboard sync configuration. The setting is enabled by default on Windows Server 2012 and Windows 10 operating system. The setting is disabled by default on Windows Server 2016 and Windows Server 2019. To enable Unicode Keyboard Layout Mapping for Windows VDA, add the following registry keys: • `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value= DWORD 1` • `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHookvalue=DWORD 1`	Set the mode on either the client side or the server side. You must set the value in `/opt/Citrix/ICAClient/module.ini [KeyboardLayout]`.
Dynamic sync	• `/opt/Citrix/ICAClient/config/module.ini` • `[ICA 3.0]` • `KeyboardSync=On` • `~/.ICAClient/wfclient.ini`	**XenApp server version 2006 and higher**—Enable the following policies on the server end: • Set the **Client Keyboard Layout synchronization and IME improvement** policy to **Support**	Set the mode on both the client side and the server side.

Table 29. Citrix Workspace app Linux keyboard layout settings—Client and VDA (continued)

Mode	Client-side settings	Server or VDA-side settings	Additional information
	• `[WFClient]` • `keyboardlayout=(User Profile)`	**dynamic client keyboard layout sychronization and IME improvement**. • Set the **Enable Unicode keyboard layout mapping** to **Allowed**. **XenApp server version before 2006**—There are no policies available to enable dynamic sync mode. You must set the registry key in the Windows VDA desktop Keyboard sync configuration. The setting is enabled by default on Windows Server 2012 and Windows 10 operating system. The setting is disabled by default on Windows Server 2016 and Windows Server 2019. To enable the setting, add the following registry key: `HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value=DWORD 0`. To enable Unicode Keyboard Layout Mapping for Windows VDA, add the following registry keys: • `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value= DWORD 1` • `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value=DWORD 1`	
Sync once	• `/opt/Citrix/ICAClient/config/module.ini` • `[ICA 3.0]` • `KeyboardSync=Off` • `~/.ICAClient/wfclient.ini` • `[WFClient]` • `keyboardlayout=(User Profile)`	Not available	Not available

Table 30. ThinOS dynamic synchronization support

Keyboard	Synchronization
Arabic (Algeria)	Not supported
Arabic (Bahrain)	Not supported
Arabic (Egypt)	Not supported
Arabic (Iraq)	Not supported
Arabic (Jordan)	Not supported
Arabic (Kuwait)	Not supported
Arabic (Lebanon)	Not supported
Arabic (Libya)	Not supported
Arabic (Morocco)	Not supported

Table 30. ThinOS dynamic synchronization support (continued)

Keyboard	Synchronization
Arabic (Oman)	Not supported
Arabic (Qatar)	Not supported
Arabic (Saudi Arabia)	Not supported
Arabic (Syria)	Not supported
Arabic (Tunisia)	Not supported
Arabic (U.A.E)	Not supported
Arabic (Yemen)	Not supported
Canadian Multilingual	Supported.
Chinese (Simplified)	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Chinese (Traditional)	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Croatian	Supported
Czech (Qwerty)	Supported
Czech	Supported
Danish	Supported
Dutch	Supported
English (3270 Australian)	Supported
English (Australian)	Supported
English (New Zealand)	Supported
English (United Kingdom)	Supported
English (United States)	Supported
Estonian (Estonia)	Supported
Finnish	Supported
French (Canadian Legacy)	Supported
French (Canadian)	Not supported
French (France)	Supported
French (France Microsoft)	Not supported
French (Switzerland)	Supported
German (Switzerland)	Supported
German	Supported
Greek	Supported
Hungarian	Supported
Icelandic	Supported
Italian (Switzerland)	Not supported
Italian	Supported
Japanese (OADG109A)	Supported

Table 30. ThinOS dynamic synchronization support (continued)

Keyboard	Synchronization
Japanese (KWD)	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Korean (Microsoft-IME2002)	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Korean	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Latvian (Latvia)	Supported
Lithuanian (IBM)	Supported
Lithuanian (Standard)	Supported
Norwegian	Supported
Polish	Supported
Polish (Legacy)	Not supported
Portuguese (Brazil)	Supported
Portuguese	Supported
Romanian	Not supported
Russian	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Serbian	Supported
Slovenian	Supported
Spanish	Supported
Swedish	Supported
Turkish	Supported
U.S.International	Not supported

Enable keyboard layout mode

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **Citrix Session Settings**.
3. In the **Basic Settings** section, select one of the following options from the **Keyboard Layout Mode** drop-down list.
   - **Server Default**—ThinOS allows VDA users to use the VDA-side default keyboard when logging in or reconnecting to VDA. The VDA-side default keyboard is the default setting in ThinOS. Any keyboard layout change on the client side is not synchronized to the VDA session.
   - **Specific Keyboard**—ThinOS allows VDA users to use a specific keyboard when logging in or reconnecting to VDA. Any keyboard layout change on the client side is not synchronized to the VDA session. Ensure that you select a specific keyboard on the ThinOS client before configuring the Admin policy tool or the Wyse Management Suite policy. If not selected, you must reboot the thin client to synchronize the specific keyboard into VDA.
   - **Client Setting**—ThinOS allows VDA users to synchronize only the VDA-side keyboard with the client-side default keyboard when logging in or reconnecting to VDA. Any keyboard layout change on the client-side is not synchronized to the VDA session.
   - **Dynamic Sync**—ThinOS allows VDA users to synchronize the VDA-side keyboard with the client-side default keyboard dynamically in the VDA session. When the VDA user changes the client keyboard, the VDA keyboard is synchronized automatically in the session. You must configure both the client and VDA-side settings to enable this mode.
4. Click **Save & Publish**.

The Citrix VDI Configuration Editor is not required to configure the Citrix keyboard Server default mode and Dynamic Sync mode. All the Citrix keyboard layout modes can be configured through the **Keyboard Layout Mode** setting in **Session Settings > Citrix Session Settings**.

Keyboard layout server default mode enhancement

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

To configure, do the following:

1. Set the Keyboard Layout Mode to Server Default using Admin Policy Tool or Wyse Management Suite.
2. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced tab** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
3. In the Citrix INI settings, click Add Row.
4. From the **File** drop-down list, select **wfclient.ini**.
5. From the **Operation** drop-down list, select **Add or Update**.
6. In the **Section** field, enter **`WFClient`**.
7. In the **Key** field, enter **`KeyboardEventMode`**.
8. In the **Value** field, enter **`Scancode`**.
9. Sign out or restart the device for the settings to take effect.

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

Keyboard layout Dynamic Sync mode enhancement

When setting the keyboard layout to **Dynamic Sync**, the switching keyboard progress bar is not displayed in desktop sessions after switching the keyboard language on the thin client. Hence, the keyboard layout in session is not automatically synced with the client. The issue also occurs in Linux Citrix Workspace app binary. To resolve the issue, do the following:

Steps

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

Cursor pattern in ICA session

In ThinOS 10.x 2502, you can change the cursor pattern in the ICA session.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **Citrix Session Settings**.
3. Enter one of the following values in the **Cursor Pattern** field to change the cursor pattern:
   - **`ffff,ffff`**—Enter this value to set the cursor color as black. This value is set by default.
   - **`0,0`**—Enter this value to set the cursor color as white.

- **aaaa,5555**—Enter this value to set the cursor color in a dotted pattern.

4. Click **Save & Publish**.
   For the setting changes to take effect, you must either sign off from the Broker agent or restart the client.

   NOTE: The **Cursor Pattern** setting is deprecated from Citrix Workspace App version 2402. The gray cursor is used, by default, in ICA sessions.

Citrix multiple virtual channels

ThinOS Citrix UC Virtual Channel Settings and Other Citrix Virtual Channels Settings are deprecated. The configuration changes that you make to the **Admin Policy Tool** or the **Wyse Management Suite** policy settings do not affect the **Citrix multiple channel** settings since multiple virtual channels are always enabled on the thin client. However, ensure that you uninstall the Unified Communications (UC) packages that are not required, to prevent the consumption of server and client resources. It is recommended that you install the Citrix Workspace app package first, and then install the Citrix Unified Communications package.

Citrix UC Virtual Channel Settings and Other Virtual Channel Settings in the Admin Policy Tool or Wyse Management Suite server are only applicable for ThinOS 10.x. Admin Policy Tool does not sync the **Citrix Unified Communication Virtual Settings** and **Other Virtual Channel Settings** from Wyse Management Suite policy settings.

The following combinations of UC optimizations and their virtual channel settings are tested on ThinOS:

Table 31. Unified Communication optimizations and their default virtual channel settings

Virtual Channel categories	Settings	Default status	Combination 1	Combination 2	Combination 3	Combination 4	Combination 5	Combination 6	Combination 7
UC Virtual Channel Settings	Microsoft Teams Optimization	Enabled	Enabled	Disabled	Disabled	Enabled	Disabled	Enabled	Disabled
	RTME for Skype for Business	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled
	Zoom Meetings Optimization	Disabled	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled
	JVDI for Cisco Jabber	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
	Cisco Webex Meetings for VDI Plugin	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
	Cisco Webex Teams for VDI Plugin	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
Other Citrix Virtual Channels Settings	USB redirection	Enabled	Enabled	Enabled	Disabled	Disabled	Enabled	Enabled	Enabled
	Imprivata	Enabled	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled

The Zoom Meetings Optimization plug-in uses four virtual channels. To use Zoom Optimizations along with Microsoft Teams or any other Cisco optimizations, you must disable other virtual channels. For example, if you are not using Imprivata SSO, you can

choose to disable the Imprivata virtual channel. Similarly, if you do not use Skype for Business, you can choose to disable the RTME for Skype for Business virtual channel.

NOTE: The default values are of all UC virtual channel settings is changed to **Enabled**.

NOTE: When the UC virtual channels are disabled, the Unified Communication software on ThinOS uses the fallback mode, which uses the HDX webcam and HDX audio. Using the fallback mode consumes more remote desktop resources such as CPU, GPU, RAM, and Network.

NOTE: Enabling or disabling the UC plug-in settings in **VDI Configuration Editor** > **Citrix Configuration Editor** is deprecated from ThinOS 2211.

Configure the Citrix virtual channels settings

About this task

This task is only applicable for ThinOS 10 and earlier versions.

Steps

1. On the ThinOS client, open **Admin Policy Tool**, or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **Citrix Session Settings**.
3. In the **UC Virtual Settings** section, enable one or more Unified Communications (UC) virtual channels as per your preference. The available options are:
   - Microsoft Teams Optimization
   - RTME for Skype for Business
   - Zoom Meetings Optimization
   - JVDI for Cisco Jabber
   - Cisco Webex Meetings for VDI
   - Cisco Webex Teams for VDI
4. In the **Other Citrix Virtual Channel settings**, enable one or more virtual channels as per your preference. The available options are:
   - USB redirection
   - Imprivata
5. Click **Save & Publish**.

   For the list of virtual channel combinations that are tested on ThinOS, see Citrix multiple virtual channels.

   UC Virtual Channel settings in Citrix Session Settings in Admin Policy Tool or Wyse Management Suite policy is enabled again.

   To configure UC Virtual Channel settings in Citrix Session Settings, do the following:
   a. On the ThinOS client, open **Admin Policy Tool**, or go to the ThinOS 10.x policy settings in Wyse Management Suite.
   b. In the **Advanced** tab, expand **Session Settings**, and click **Citrix Session Settings**.
   c. In the **UC Virtual Channel Settings** section, enable or disable one or more Unified Communications (UC) virtual channels as per your preference. The available options are:
      - Microsoft Teams Optimization
      - HDX RealTime Media Engine for Microsoft Skype for Business
      - Zoom Meetings Optimization
      - Cisco Jabber Softphone for VDI (JVDI)
      - Cisco Webex Meetings for VDI
      - Cisco Webex VDI (formerly Cisco Webex Teams)
   d. Sign out or restart the device for the settings to take effect.

   The following UC virtual channels labels are renamed in ThinOS 2502 Admin Policy Tool and Wyse Management Suite version 5.0 using the Configuration UI package vxxxxx:

   - **RTME for Skype for Business** is renamed to **HDX RealTime Media Engine for Microsoft Skype for Business**.
   - **JVDI for Cisco Jabber** is renamed to **Cisco Jabber Softphone for VDI (JVDI)**.
   - **Cisco Webex Meetings for VDI** is renamed to **Cisco Webex Meetings for VDI**.
   - **Cisco Webex Teams for VDI** is renamed to **Cisco Webex VDI** (formerly Cisco Webex Teams).

NOTE: When the UC virtual channels are disabled, the Unified Communication software on ThinOS uses the fallback mode, which uses the HDX webcam and HDX audio. Using the fallback mode consumes more remote desktop resources such as CPU, GPU, RAM, and Network.

NOTE: Enabling or disabling the UC plug-in settings in **VDI Configuration Editor** > **Citrix Configuration Editor** is deprecated from ThinOS 2211.

Configure the Citrix session properties

About this task

This section describes how to configure the Citrix HDX connections on your thin client.

Steps

1. On the taskbar, click **Connection Manager**.
   The **Connection Manager** dialog box is displayed.
2. Select a Citrix connection from the list, and click **Properties**.
3. Click the **Connection** tab and do the following:
   You can view **Server** or **Published Application**, **Connection Description**, **Browser Servers**, **Host Name or Application Name**, and **Encryption Level** but cannot edit these options.
   a. **Display Resolution**—Select the display resolution for this connection.
      If you select the **Published Application** option, the connection display enables you to select the **Seamless Display Resolution** option.
   b. **Window mode** and **Full screen** mode—Select the initial view of the application and desktop in a windowed screen or full screen.
   c. **Autoconnect on start-up**—When this option is selected, the thin client automatically connects the session on start-up.
   d. **Reconnect after disconnect**—When this option is selected, the thin client automatically reconnects to a session after a nonoperator-initiated disconnect. The wait interval is the value that you set in the **Delay before reconnecting** box (enter the number of s 1–3600). The default is 20 s if you are a stand-alone user.
4. Click the **Logon** tab to view **Logging on area**.
   You can view **Login Username**, **Password**, **Domain name**, and **Logon Mode**.
5. Click the **Options** tab, and do the following:
   a. **Autoconnect to local devices**—Select any options—Printers, Serials, Smart Cards, Sound, and Disks—to have the thin client automatically connect to the devices.
      NOTE: USB devices that are connected are managed in **Global Connection Settings**.
   b. **Audio Quality**—From the drop-down list, select your preferred audio quality.
   c. **Enable session reliability**—When enabled, session reliability allows you to momentarily lose connection to the server without having to reauthenticate upon regaining a connection. Instead of the connection time-out, the session is kept alive on the server and is made available to the client upon regaining connectivity. Session reliability is most relevant for wireless devices. From version 21.12.0.18.2, 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.
6. Click **OK** to save your settings.

Using multiple displays in a Citrix session

ThinOS supports ICA desktop multiple displays in Citrix Virtual Apps and Desktops/Citrix Virtual Apps 7.6 and later versions.

Prerequisites

- Increase the value of **MaxVideoMemoryBytes** REG_DWORD to support one or more 4K resolution-displays. For more information, see the **Citrix documentation** at support.citrix.com.
- Increase the display memory limit to support more color depth and higher resolution. For more information, see the **Citrix documentation** at citrix.com.

Steps

1. Connect multiple displays to ThinOS device.
2. Go to **System Setup** > **Display**, disable **Mirror Mode**, and configure the display layout.
3. Launch an ICA desktop. By default, the ICA desktop is launched in the full-screen mode.
4. Move the display blocks as per your requirement.

   NOTE: For more information about the Citrix official multiple displays support, see the **Citrix documentation** at support.citrix.com.

   Limitation—If you set all monitors with either horizontal or vertical layout, the maximum supported resolution is 4x4 K. If you connect five or six monitors with 4x4 K + 1920x1080 or 4x4 K + 2x1920x1080 resolution combinations, you cannot launch ICA desktop by horizontal or vertical layout. It is recommended that using grid layout such as 2x3 or 3x2 or 2x2+1.

USB Printer Redirection

Prerequisites

Go to Citrix Studio, and enable the **Client USB device redirection** policy.

About this task

This section describes how to configure USB Printer Redirection in a Citrix session.

Steps

1. On the ThinOS desktop, open the **Connection Manager** window, and click **Global Connection Settings**.
   The **Global Connection Settings** dialog box is displayed.
2. Clear the **Exclude printer devices** check box, and click **OK**.
3. Log off from Citrix Broker agent, and then log in again.
4. Connect a USB printer to the thin client.
5. Log in to a Citrix session.
6. Go to **Control Panel** > **Devices and Printer**, and verify if the printer driver is automatically installed.
   After the printer drive installation is complete, the redirected printer is listed in the **Printers** section.

USB device redirection using Citrix Desktop Viewer

From ThinOS 2208 and Citrix Workspace App 2207, **Devices** section is able to show in Citrix Desktop Viewer.

Redirect USB devices from the Devices section

To redirect the USB devices from the **Devices** section to session, do the following:

Steps

1. In a desktop session, navigate to the **Desktop Viewer** under **Devices**.
   The USB devices are displayed.
2. To redirect a device to session, select the device from the menu item.

   NOTE: To disconnect a device from the session, clear the required menu item or check boxes next to the devices when the devices are mapping in session.

Redirect the USB devices from the Preferences section

To redirect the USB devices from the **Preferences** section to session, do the following:

Steps

1. Navigate to the **Preferences** > **Devices** section.

The USB devices are displayed.

2. Select the **Redirect** check boxes next to the devices.
3. Click **Save**.

NOTE: To disconnect a device from the session, clear the required menu item or check boxes next to the devices when the devices are mapping in session.

Configure the Citrix UPD printer

Use of Citrix Universal Print Driver (Citrix UPD) ensures that all printers that are connected to the thin client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center. Citrix UPD is the base of Citrix Universal Printer. It is an autocreated printer object that uses the Citrix UPD and is not tied to any specific printer defined on the client.

About this task

This section describes how to configure the Citrix UPD usage on your thin client.

Steps

1. Connect a printer to the ThinOS client.
2. On the ThinOS desktop menu, do the following:
   a. Open the **Connection Manager** window.
   b. Click **Global Connection Settings**.
   c. Go to the **Session** tab and select the **Exclude printer devices** check box.
   d. Click **OK**.
3. From the desktop menu, click **System Setup** > **Printer Setup**.
   The **Printer Setup** dialog box is displayed.
4. Enter the name of the printer in the **Printer Name** box.
5. Enter any string of the Printer identification in the **Printer Identification** box.
6. Select the type of the printer class from the drop-down list, select the check box to enable the printer device, and click **OK**.

   NOTE: In ThinOS, only PS class is supported.

7. Start a Citrix Virtual Apps and Desktops application connection.
8. Open the **Devices and Printers** in the desktop or application. The printer is mapped as the UPD printer by default.

Next steps

To enable the printer server policies for Citrix UPD printer, see the **Citrix documentation** at docs.citrix.com.

Configure the device-specific printer driver

Based on the Citrix Host Printer Policy settings, ThinOS supports device-specific printer drivers. This method allows Citrix hosts to automatically create client-redirected printer queues based on the peripheral management printers settings of the ThinOS client. The host print manager uses the printer name and the printer ID to automatically create the printer queues.

About this task

This section describes how to configure the device-specific printer driver usage on your ThinOS client.

Steps

1. Connect a printer to the ThinOS client.
2. From the desktop menu, click **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
3. On the ThinOS desktop menu, do the following:
   a. Open the **Connection Manager** window.

b. Click **Global Connection Settings**.
c. Go to the **Session** tab and select the **Exclude printer devices** check box.
d. Click **Save**.

4. Enter the name of the printer in the **Printer Name** box.
5. Enter the specific printer driver identification in the **Printer Identification** box.

   NOTE: The specific printer driver identification is installed on the remote Citrix desktop, and you must note the specific printer driver identification.

6. Select the check box to enable the printer device, and click **OK**.

   NOTE: In ThinOS, only printer driver type 3 is supported.

7. Start a Citrix virtual connection.
8. Open the **Devices and Printers** in the desktop or application. The printer is mapped to the session.

Invert cursor color

The cursor color can be inverted based on the background color of a text. As a result, you can locate the position of the cursor in between texts. By default, this feature is disabled. To enable cursor color inverting feature, do the following:

Steps

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In the Citrix INI Settings, click **Add Row**.
3. From the **File** drop-down list, select **wfclient.ini**.
4. From the **Operation** drop-down list, select **Add or Update**.
5. In the **Section** field, enter `Thinwire3.0`.
6. In the **Key** field, enter `InvertCursorEnabled`.
7. In the **Value** field, enter `True`.
8. Sign out or restart the device for the settings to take effect.

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

   From Citrix Workspace App 2402, the inverted cursor is deprecated by Citrix, which means the setting **InvertCursorEnabled=true** or **InvertCursorEnabled=false** in Citrix Configuration Editor is not supported. You can also use a gray cursor in ICA sessions.

Echo cancellation for Microsoft Teams

Microsoft Teams optimization supports echo cancellation. The echo cancellation option for Microsoft Teams is disabled by default.

Enable echo cancellation for Microsoft Teams

Steps

1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. In the Citrix JSON Settings, click **Add Row**.
3. From the **File** drop-down list, select **hdx_rtc_engine/config.json**.
4. From the **Operation** drop-down list, select **Add or Update**.
5. In the **Key** field, enter `EnableAEC`.
6. In the **Value** field, enter `1`.
7. Sign out or restart the device for the settings to take effect.

Limitation: If you set EnableAEC as **1**, and if there is a Microsoft Teams call or meeting happening between a Wyse 5470 thin client and a thin client that is or is not Wyse 5470 thin client, you may encounter audio issues when you enable the camera.

If you encounter audio issues during Microsoft Teams calls or meetings, you can change the default settings to troubleshoot the audio issues (like robotic voice, increased system performance causing audio issues, and so on) by doing the following:

a. In the Citrix JSON Settings, click **Add Row**to add the setting
b. From the **File** drop-down list, select **hdx_rtc_engine/config.json**.
c. From the **Operation** drop-down list, select **Add or Update**.
d. In the **Key** field, enter **`EnableAGC`**.
e. In the **Value** field, enter **`0`**.
f. In the Citrix JSON Settings, click **Add Row** to add the setting.
g. From the **File** drop-down list, select **hdx_rtc_engine/config.json**.
h. From the **Operation** drop-down list, select **Add or Update**.
i. In the **Key** field, enter **`EnableNS`**.
j. n the **Value** field, enter **`0`**.
k. Sign out or restart the device for the settings to take effect.

Multiwindow chat and meetings for Microsoft Teams

Microsoft Teams optimization supports the multiwindow chat and meetings feature. Using this feature, you can view chat and meetings in separate windows.

NOTE: For this feature to work, the Citrix Workspace app package version must be 22.7.0.20.2 or later, Citrix VDA version must be 2502, and Microsoft Teams version must be 1.5.00.11865 or later. You must sign out from Microsoft Teams and restart the device for the feature to be enabled.

UDP audio through Citrix Gateway

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

Enable UDP audio through Citrix Gateway feature

Prerequisites

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

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

Steps

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

Disable UDP audio through Citrix Gateway feature

Steps

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

Multiple audio redirections

The Citrix Workspace app displays all available local audio devices in a session with their names. Plug-and-play support for Bluetooth and HDMI audio devices is also provided. This feature is disabled by default.

About this task

Follow this task to enable the feature.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, go to **Peripheral Management** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
3. In the Citrix INI Settings, click **Add Row**.
4. From the **File** drop-down list, select **module.ini**.
5. From the **Operation** drop-down list, select **Add or Update**.
6. In the **Section** field, enter **`ClientAudio`**.
7. In the **Key** field, enter **`AudioRedirectionV4`**.
8. In the **Value** field, enter **`True`**.
9. Click **Save & Publish**.
10. Sign out and restart the device for the settings to take effect.

    For limitations and known issues, see the *Release Notes* of your ThinOS version at Support | Dell.

    ThinOS 10.x supports multiple audio redirection by default. The Citrix Workspace app displays all available local audio devices in a session with their names. Plug-and-play functionality is also supported. Multiple audio devices redirection feature is enabled by default. In other words, `AudioRedirectionV4=True` parameter has already been configured during Citrix Workspace App 2411 package installation. You need not change the Citrix INI settings in the Citrix configuration editor in Wyse Management Suite or Admin Policy Tool. To disable this feature, do the following:

    a. In the Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
    b. In the **Citrix INI Settings**, click **Add Row**.
    c. From the **File** drop-down list, select **module.ini**.
    d. From the **Operation** drop-down list, select **Add or Update**.
    e. In the Section field, enter **`ClientAudio`**.
    f. In the **Key** field, enter **`AudioRedirectionV4`**.
    g. In the **Value** field, enter **`False`**.
    h. Sign out or restart the device for the settings to take effect.

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

    NOTE: There is an eight-device limitation on HDX session redirection, which is a Citrix VDA limitation.

Citrix multiple audio redirection limitation

If JVDI package is installed in ThinOS, audio devices cannot be switched in the applications in session, and the session is disconnected when you open **Windows** > **Sound**, and go to the **Recording devices** list. If you want to use multiple ICA audio devices, it is recommended that you do not install the JVDI package.

Smart card reader plug and play

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

Disable smart card plug and play

Steps

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

HDX RealTime webcam Video Compression for 32-bit apps

Only 32-bit apps on the virtual desktop with HDX RealTime webcam Video Compression are supported by ThinOS. With this feature, you can customize the camera resolution and frames per second from **System Setup** > **Peripherals** > **Camera**. You can also customize this feature using Admin Policy Tool or Wyse Management Suite policy settings. HDX RealTime webcam Video Compression is compatible with most unified communications clients. The feature has been tested for compatibility with Cisco Webex Meetings, Cisco Webex Teams, Cisco Jabber, Microsoft Teams, Skype for Business 365, and Zoom. You can use a 32-bit browser such as Google Chrome or Mozilla Firefox to verify the webcam redirection online. External USB cameras or the integrated camera can be used with HDX RealTime webcam Video Compression. Webcam bandwidth consumption can vary with webcam models. Different webcams offer different frame rates and resolution. Dell Technologies used the following webcams for initial feature validation:

- Microsoft LifeCam HD-3000—Highest supported resolution with HDX RealTime webcam Video Compression is 1920x800.
- Logitech C920, C922, C930e—Highest supported resolution with HDX RealTime webcam Video Compression is 1600x896.
- Wyse 5470 and 5470 All-in-One thin clients with built-in camera.

HDX RealTime Webcam Video Compression limitations

- Camera with hardware encoding is not supported in ThinOS.
- Since x264 library is not integrated into ThinOS, 64-bit apps with HDX RealTime Webcam Video Compression are not supported by Citrix Workspace App. Hence, only 32-bit apps with HDX RealTime Webcam Video Compression are supported in ThinOS.
- Citrix Workspace App 2112 with HDX RealTime Webcam Video Compression works only with built-in camera. The issue is also reproduced in Linux Citrix Workspace app binary. Hence, from this ThinOS release, HDX RealTime Webcam Video Compression is only supported with Citrix Workspace app 2109.
- Sometimes, the updated Camera Width, Camera Height and Camera FPS settings does not sync from Wyse Management Suite to the thin client. You must reboot the client for the changes to take effect.
- HDX RealTime Webcam Video Compression in ThinOS supports only one webcam at a time. Citrix Workspace Linux binary can update the default webcam by modifying **HDXWebCamDevice** in `$HOME/.ICAClient/wfclient.ini` configuration

file. For example, add **HDXWebCamDevice=/dev/video2** to set the webcam mapped to `/dev/video2` in a system. However, ThinOS does not allow to input the value `/dev/video2` in VDI Configuration Editor due to security reasons.

- If client camera is set to 2304x1296 or 2304x1536 video resolution, the HDX webcam redirection cannot be previewed in the session. This limitation is reproduced in CWA 2109 Linux binary as well.
- If client camera is set to 1920x1080 video resolution, the HDX webcam redirection falls back to 325x288 video resolution in the session. This limitation is reproduced in CWA 2109 Linux binary as well.
- HDX webcam camera sometimes does not work on Webex Meeting call. This limitation is reproduced in CWA 2109 Linux binary as well.
- Zoom application video preview sometimes fails when you use Citrix HDX Webcam. This limitation is reproduced in CWA 2109 Linux binary as well.
- Webex application video fails to preview when you use Citrix HDX Webcam. This limitation is reproduced in CWA 2109 Linux binary as well.
- External USB camera does not work with Citrix HDX Webcam in Citrix Workspace app 2112. Only the built-in camera works. This limitation is reproduced in CWA 2109 Linux binary as well.

Prerequisites for HDX RealTime webcam Video Compression

- On the VDA, HDX RealTime webcam Video Compression is enabled by default. Other configurations are not required. It is recommended to that using Citrix VDA version 1912CU3 or later.
- HDX webcam video compression requires **Multimedia conferencing** and **Windows Media Redirection** policy settings to be enabled. The settings are enabled by default.
- Ensure that `Citrix_Workspace_App_24.11.0.85.73.pkg` is installed.
- To use HDX RealTime webcam Video Compression in the unified communication software in VDA, ensure that the following conditions are met:
  - For Skype for business application, ensure that the software is 32-bit and do not install the Citrix HDX RealTime Connector in VDA.
  - For ZoomVDI application, ensure that the software is 32-bit. Do not install the Zoom_Citrix package in the thin client. Disable Zoom VDI optimization using Admin Policy Tool or Wyse Management Suite policy settings, if you have installed the Zoom package in thin client.
  - For the Microsoft Teams application, ensure that the software is 32-bit. Disable Microsoft Teams VDI optimization in thin client using Admin Policy Tool or Wyse Management Suite policy settings.
  - For Webex meeting application, ensure that the software is 32-bit. Do not install the Webex Meetings VDI package in thin client. Disable Webex Meetings VDI optimization using Admin Policy Tool or Wyse Management Suite policy settings, if you have installed the Webex Meetings VDI package in thin client.
  - For Webex VDI application, ensure that the software is 32-bit. Do not install the Webex VDI package in the thin client. Disable Webex VDI optimization using Admin Policy Tool or Wyse Management Suite policy settings, if you have installed the Webex VDI package in thin client.
  - For Cisco Jabber application, ensure that the software is 32-bit. Do not install the Cisco Jabber package in the thin client. Disable JVDI optimization using Admin Policy Tool or Wyse Management Suite policy settings, if you have installed the Cisco Jabber package in thin client.

Configure camera for HDX RealTime webcam Video Compression using Admin Policy Tool or Wyse Management Suite policy settings

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **Camera**.
3. Click **Enable Camera** to enable the camera.

   By default, the option is enabled. If the option is disabled, the cameras on the thin clients are not shown.
4. Enable **Optimize for CPU**.
   By default the option is enabled. The default settings are **format=RAW**, **resolution=320X240**, and **FPS=10**. Disable the **Optimize for CPU** option to customize the camera format, resolution, and FPS settings. Ensure that the camera supports the custom values before continuing. Increasing the resolution and FPS impacts the performance.
5. Click **Save & Publish.**

HDX RealTime Webcam Video Compression for 64-bit apps

From ThinOS 2208 and Citrix Workspace App 2207, **HDX RealTime Webcam Video Compression** for 64-bit applications is supported. Webcam redirection works for 32-bit and 64-bit applications such as Skype or GoToMeeting. Use a 32-bit browser or 64-bit browser to verify the webcam redirection online. For example, use a 32-bit browser or 64-bit browser and go to www.webcamtests.com.

By default, ThinOS only supports webcam redirection feature for 32-bit apps. To enable webcam redirection feature for 64-bit apps, see Enable HDX RealTime Webcam Video Compression for 64-bit apps.

Enable HDX RealTime Webcam Video Compression for 64-bit apps

Steps

1. On Admin Policy Tool or the Wyse Management Suite policy settings, go to **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. Under **Citrix INI Settings**, click **Add Row**.
3. From the **File** drop-down list, select **wfclient.ini**.
4. From the **Operation** drop-down list, select **Add** or **Update**.
5. In the **Section** field, enter **WFClient**.
6. In the **Key** field, enter **HDXH264InputEnabled**.
7. In the **Value** field, enter **True**.
8. Sign out or restart the device for the settings to take effect.

Export Citrix Workspace App logs

The Citrix Workspace App logs can only be exported from **Troubleshooting** > **General** > **Export Logs**. The Citrix log path is `/var/log/citrix`. Citrix log can be enabled through the **Log Level** setting in **Session Settings > Citrix Session Settings** inside Wyse Management Suite.

Steps

1. From the desktop menu, click **System Tools**.
2. Click the **Packages** tab.
3. Select **Citrix Workspace App**, and click **Advanced**.
   The **Citrix Log Preferences** window is displayed.
4. Right-click the classes that you require, and select **Verbose**.
5. Select the check boxes to select specific log items.
   Click **Set All Enabled** to select all the check boxes.
6. Enter the file name and the output file pat in the **Log Output Path** field.
   The default path is `/var/log/citrix/ICAClient.log`. It is recommended that using the default log output path.
7. Click **Apply Changes** and close the **Citrix Log Preferences** window.
8. Connect the ICA session, reproduce the scenario that you require the log from, and disconnect the ICA session.
9. Connect a USB drive that is formatted with the FAT32 file allocation.
10. From the desktop menu, click **Troubleshooting**.
11. On the **General** tab, click **Export Logs**.
    Citrix Workspace app logs are exported to the USB drive.

Next steps

1. Reopen the **Citrix Log Preferences** window by performing the following steps:
   a. From the desktop menu, click **System Tools**.
   b. Click the **Packages** tab.
   c. Select **Citrix Workspace App**, and click **Advanced**.

   The **Citrix Log Preferences** window is displayed.

2. Click both the **Set All Default** buttons.
3. Click the **Load Default** button.
4. Click **Apply Changes**.

The Citrix Workspace Log capture is disabled.

Configure multifarm for Citrix Broker

Steps

1. Log in to the Wyse Management Suite server.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies > ThinOS 10.x**.
4. Click the Advanced tab.
5. Expand **Broker Settings**, and click **Global Broker Settings**.
6. Select **Default Broker Type** as **Citrix Virtual Apps and Desktops**, then enable **MultiFarm**.
7. Click **Save & Publish**.
8. Check in the thin client to the WMS group, and restart the thin client.
9. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
10. Go to the **Broker Setup** tab, and enter the multi broker server in the **Broker Server** field.
    For example, `https://broker1,https://broker2` or `https://broker1;https://broker2`.
11. You can now log in to multi server with one user.

    NOTE: If there is a server logon failure due to invalid credentials when you enable Multifarm and MultiDomain, the logon continues. If there is no failure, logon exits immediately. You can switch between servers when you are logged in with multiple servers using Citrix Workspace mode. To switch between servers, click the menu button at the upper-right corner, and then click **Accounts**.

Configure multilogon for Citrix Broker

Steps

1. Log in to the Wyse Management Suite server.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies > ThinOS 10.x**.
4. Click the Advanced tab.
5. Expand **Broker Settings**, and click **Global Broker Settings**.
6. Select **Default Broker Type** as **Citrix Virtual Apps and Desktops**, then enable **Multi Logon**.
7. Click **Save & Publish**.
8. Check in the thin client to the WMS group, and restart the thin client.
9. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
10. Go to the **Broker Setup** tab, and enter the multi broker server in the **Broker Server** field.
    For example, `https://broker1,https://broker2` or `https://broker1;https://broker2`.
11. You can now log in to multi server with two different users.

    NOTE: You can switch between servers when you are logged in with multiple servers using Citrix Workspace mode. To switch between servers, click the menu button at the upper-right corner, and then click **Accounts**.

Virtual Display Layout

From ThinOS 10.x 2502 and Citrix Workspace App 2411, virtual display layout on VDA is supported. This section describes how to configure the virtual display layout on VDA.

Prerequisites

- Single-session or multisession operating system VDA must be supported.
- The graphics status indicator policy must be enabled.
- VDA version 2019 or later (Dell Technologies qualified VDA 2203 LTSR and 2206).

NOTE: Only desktop sessions can be configured.

Steps

1. Right-click the graphics status indicator icon from the system tray and select **Configure virtual displays**.
   The virtual display configuration interface is launched.
2. Right-click a virtual display to mark it as the primary monitor.
3. Use the DPI drop-down list to set a preferred scaling factor for the virtual display.
   You can draw horizontal or vertical lines to separate the screen into virtual monitors. The screen is split according to specified percentages of the session monitor resolutions.
4. After defining a virtual display layout, click **OK** to save the layout, or **Cancel** to discard the changes.
   Use **Reset** to undo the configuration and restore the original layout.

Extended keyboard layouts

Japanese 106 keyboard, Portuguese ABNT/ABNT2 keyboards, and Multimedia keyboards are supported in Citrix VDI sessions from ThinOS 10.x 2502 and Citrix Workspace App 2411.

Prerequisites

- To enable the extended keyboard layouts in Citrix VDI session, ensure that the Scancode keyboard input mode is configured.
- Ensure that the setting **Enabled Volume Control for Client Volume** is disabled in Admin Policy Tool or Wyse Management Suite policy. Otherwise, the Multimedia keyboards do not work.

Steps

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

32-bit cursor

- 32-bit cursor is supported on ThinOS 10.x 2502 and Citrix Workspace App 2411.
- The black box around the cursor issue is resolved when using 3D applications in HDX 3D Pro VDA desktop.
- There is a black box around the 32-bit cursor in the Adobe Acrobat reader in the Citrix HDX Pro 3D desktop. This issue is also reproduced in the Citrix Workspace App Linux binary.
- From ThinOS 10.x 2502 and Citrix Workspace App 2411, you can disable support for the 32-bit cursor. By default, a 32-bit cursor is enabled. To disable support for the 32-bit cursor, do the following:
  1. On Admin Policy Tool or Wyse Management Suite policy settings, go to **Advanced > VDI Configuration Editor > Citrix Configuration Editor**.

2. In the Citrix INI Settings, click **Add Row**.
3. From the **File** drop-down list, select **wfclient.ini**.
4. From the **Operation** drop-down list, select **Add or Update**.
5. In the **Section** field, enter `Thinwire3.0`.
6. In the **Key** field, enter `Cursor32bitSupport`.
7. In the **Value** field, enter `False`.
8. Sign out or restart the device for the settings to take effect.

Citrix Workspace app updates

You can manage new Citrix Workspace app features such as enabling copy/download settings, using sustainability mode, switching to native window mode, and updating configuration files.

View recent Citrix sessions in WMS

Explains how ThinOS 10.x IT administrators can configure Citrix broker settings through WMS and verify active or recently launched Citrix sessions directly from WMS.

About this task

After completing the configuration steps, ThinOS devices connect to the Citrix broker as defined in WMS. Once a user launches an app or desktop from the ThinOS device, WMS automatically records and displays session data under **Recent Sessions**, enabling administrators to monitor Citrix activity in real time.

Steps

1. Log in to WMS as an administrator,
2. Go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
3. Go to **Broker Settings** > **Global Broker Settings**, and set **Default Broker Type** to **Citrix Virtual Apps and Desktops**.
4. Go to **Citrix Virtual Apps and Desktops** and enter the **Broker Server** details.
5. Click **Save & Publish**.
6. Log in to the Citrix broker from the ThinOS device and launch the assigned app or desktop.
7. In WMS, open the **Devices** page and select the device where the Citrix session was launched.
8. View the **Recent Sessions** section to verify session activity.

Enable or disable settings for copy and download in Citrix Connection Manager

About this task

NOTE: Starting with Citrix Workspace app 2503, this feature is available.

You can enable or disable the copy and download buttons in Citrix Connection Manager using the Admin Policy Tool or Wyse Management Suite.

Steps

1. Go to **Admin Policy Tool** or **Wyse Management Suite** policy settings, and select **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. Under **Citrix INI Settings**, click **+ Add Row** and enter the following information:

Field	Value
File	**All_Regions.ini**

Field	Value
Operation	**Add or Update**
Section	`Client Engine\GUI`
Key	
For enabling Copy	`CsiCopyButtonVisible`
For enabling Download	`CsiDownloadButtonVisible`
Value	`True`

3. Click **Save & Publish**.
4. Click **Disconnect** to sign out.

   NOTE: The UI does not have a dedicated sign-out option.

Enable the sustainability feature for Citrix Desktop Viewer toolbar

About this task

NOTE: Starting with Citrix Workspace app version 2503, the sustainability feature is disabled by default. If the client-side configuration is not updated, a dialog box is displayed prompting users to either disconnect or sign out of their session.

Steps

1. Go to **Admin Policy Tool** or **Wyse Management Suite** policy settings, and select **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. Under **Citrix INI Settings**, click **+ Add Row** and enter the following information:

Field	Value
File	**wfclient.ini**
Operation	**Add or Update**
Section	`Thinwire3.0`
Key	`CloseDialogVersion`
Value	`1`

3. Click **Save & Publish**.
4. Click **Disconnect** to sign out.

   NOTE: The UI does not have a dedicated sign-out option.

Citrix native mode - Window mode

Starting with ThinOS 10.x 2505 and Citrix Workspace app 2503, the Citrix Workspace window defaults to window mode when using Citrix native mode.

In earlier versions, the window opened in full-screen mode by default.

Citrix Workspace app limitations

Linux Citrix Workspace app:

- Camera switching in Microsoft Teams does not function in Citrix VDI sessions.

- In an ICA session, copying or pasting information from the Connection icon on the Desktop Viewer toolbar is not supported.

ThinOS:

- Deleted parameters in Citrix JSON settings may not work as expected. If you used the keys **`WebrpcLogLevel (value 0)`** or **`WebrtcLogLevel (value 0)`** in config.json, update the values to **5** and **4** respectively after completing log capture.
- If you are unable to log in to Citrix NetScaler in Citrix native mode, try disabling the IPv6.
- If unable to connect to Citrix Cloud in native mode, disable Low Latency Transport (LLT) using the Citrix Configuration Editor. For more information, see Disable LLT using Citrix Configuration Editor.

Disable LLT using Citrix Configuration Editor

About this task

If you are unable to connect to Citrix cloud using Citrix native mode, you can disable LLT using Citrix Configuration Editor.

Steps

1. Go to **Admin Policy Tool** or **Wyse Management Suite** policy settings, and select **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. Under **Citrix XML Settings 2**, click **+ Add Row** and enter the following information:

Field	Value
File	**AuthManConfig.xml**
Operation	**Add or Update**
Tag	**`AuthManLite.longLivedTokenSupport`**
Value	**`false`**

3. Click **Save & Publish**.

Modify the Citrix AuthManConfig.xml file using Citrix XML Settings 2

About this task

In ThinOS, you can modify key and value parameters in the AuthManConfig.xml file using Citrix XML Settings 2.

Steps

1. Go to **Admin Policy Tool** or **Wyse Management Suite** policy settings, and select **Advanced** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
2. Under **Citrix XML Settings**, click **+ Add Row** and enter the following information:

Field	Value
File	**AuthManConfig.xml**
Operation	**Add or Update**
Key	**`FIDO2Enabled`**
Value	**`true`**

NOTE: ThinOS 10.x 2505 also allows the users to modify other parameters as noted in the table:

Table 32. Modify parameters

Modify parameters	Example 1	Example 2	Example 3
Tag	`AADSSOClientId`	`AuthManLite.longLivedTokenSupport`	`Shield.Toggle.ConnectionLeasingEnabled`
Value	`testid`	`false`	`false`

3. Click **Save & Publish**.
4. Sign out or restart the device to apply the settings.

Configuring Omnissa

Omnissa virtualization enables you to run multiple virtual machines on a single physical machine. Omnissa Horizon Client is a locally installed software application that communicates between View Connection Server and the thin client operating system. It provides access to centrally hosted virtual desktops from your thin clients.

In every ThinOS release, the Omnissa Horizon Client version may get updated to a newer version. You must upgrade the Omnissa Horizon package along with the ThinOS firmware. Omnissa Horizon package versions have a dependency on the ThinOS firmware versions. See the *Release Notes* of your ThinOS version at Support | Dell to know the corresponding Omnissa Horizon package version.

You can use touch screen gestures in both remote desktop and application sessions. Both full-screen mode and window mode support touch screen functionality. You can also use touch screen with the Omnissa Horizon Client user interface. Swiping down the screen, touch screen gestures, and multi-touch are not supported. If you enable relative mouse, the touch screen functionality may not work properly.

For information about the latest Omnissa Horizon Client version and the known issues, see the *Release Notes* of your ThinOS version at Support | Dell.

NOTE: If you are upgrading your thin client to the latest ThinOS version, you must ensure that the Horizon server or agent version is updated to support the latest Horizon client version. For more information about the client and server/agent version compatibility, see the **Omnissa Product Interoperability Matrices** page in the Omnissa documentation website.

Configure the Omnissa broker connection

About this task

This section describes how to configure the Omnissa broker setup on your thin client.

Steps

1. To access the remote connection settings, do the following:
   a. For **Modern Mode**, from the desktop menu, click **Settings** > **Remote Connections**.
   b. For **Classic Mode**, from the desktop menu, click **System Setup** > **Remote Connections**.

   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, select **Omnissa Horizon** from the **Select Broker Type** drop-down list, and do the following:
   - **Broker Server**—Enter the IP address/FQDN of the broker server.
   - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. You can enter multiple desktop names. Each desktop name is separated by semicolon, and is case-sensitive.
   - **Security mode**—Select the preferred security mode from the following options:
     - **Full**—Full Security requires an FQDN address with a domain certificate.
     - **Warning**—Warn Security requires an FQDN address with a self-signed certificate, or without any certificate. But the corresponding warning message is displayed for the user to continue.
     - **Low**—Security allows an FQDN or IP address with or without a certificate.

     Connection Protocol—From the drop-down list, select the type of protocol connection. By default, the option is set to **Server Default**. The available options are:

- **Server default**—Select this protocol connection to display the desktop with the default protocol as configured in the Omnissa View Admin console, for each pool in the broker. If a desktop pool is configured with the default protocol as **RDP** in the View Admin console, then only the RDP connection of the desktop is displayed in ThinOS after users sign in to the device.
- **All Supported**—Select this protocol connection to display the desktop in all the available connections. This is applicable when a desktop pool is configured to allow users to select the protocol as **yes**. If the desktop is configured with the default protocol as **PCoIP** and allow user to select protocol as **no**, then ThinOS only displays the desktop in the PCoIP connection.
- **RDP only**—Select this protocol connection to display the desktop in RDP connection only. If a desktop pool is configured with the default protocol as **PCoIP** in the View Admin console, and allow users to select the protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.
- **PCoIP only**—Select this protocol connection to display only the desktop in the PCoIP connection, for each pool in the broker. If a desktop pool is configured with the default protocol as **RDP** in the View Admin console, and allow user to select the protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.
- **Blast only**—Omnissa Blast display protocol can be used for remote applications and for remote desktops that use virtual machines or shared-session desktops on an RDS host. Select this protocol connection to display the desktop with the Blast protocol.
- **RDP and Blast**—Select this protocol connection to display the desktop with the Blast and RDP protocol. If a desktop pool is configured with the default protocol as **PCOIP/RDP** in the View Admin console, and allow user to select the protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.
- **PCoIP and RDP**—Select this protocol connection to display the desktop with the PCOIP and RDP protocol. If a desktop pool is configured with the default protocol as **PCOIP/RDP** in the View Admin console, and allow user to select the protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.
- **PCoIP and Blast**—Select this protocol connection to display the desktop with the Blast and PCOIP protocol. If a desktop pool is configured with the default protocol as **PCOIP/RDP** in the View Admin console, and allow user to select the protocol as **no**, then this desktop is not displayed in ThinOS after user signs in to the device.

- **Log in anonymously using Unauthenticated Access**—Select this check box to anonymously log in to the Omnissa session with application remoting.

3. Click **Save** to save the settings.

   NOTE: If you want to connect Horizon session by RDP protocol, ensure **Enable Credential Security Service Provider** is enabled in **WMS/APT** > **Advanced** > **Broker Settings** > **Omnissa Horizon Settings**, and log in again to the Omnissa broker.

Omnissa Real-Time Audio-Video

About this task

Use the Real-Time Audio-Video feature to run online conference applications on the remote desktop. Both audio and video devices that are connected to your thin client can be used for VoIP in a remote desktop. The Real-Time Audio-Video feature displays the names of redirected devices with **(VDI)** added to the name. For example, the Dell Webcam 5023 is displayed as Dell Webcam 5023(VDI). For audio playback, **(VDI)** is not added to the device name.

To know more about the Omnissa Real-Time Audio-Video support, go to doc.omnissa.com.

NOTE: There is no additional configuration for ThinOS.

To validate the Omnissa Real-Time Audio-Video, do the following:

Steps

1. Connect to the Omnissa PCoIP or Blast desktop with the audio and video devices.

   NOTE: USB redirection must be disabled for the audio and video devices.

2. Verify the audio playback of the system using the Omnissa virtual audio.
3. Verify the system audio recording using the Omnissa virtual microphone.
4. Verify the audio settings in the VoIP application.
5. Verify the video settings in the VoIP application using the Omnissa virtual webcam.
6. Start the audio or video calls.

High Efficiency Video Coding

In ThinOS 10.0052, Omnissa Blast Extreme supports High Efficiency Video Coding (HEVC). HEVC is also known as H.265 and it is the industry successor to H.264. Compared to H.264, H.265 provides 50% more compression by maintaining the same quality as H.264. This feature is disabled by default. 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.

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.

To enable this feature from the local user interface, select the **Allow High Efficiency Video Decoding (HEVC)** check box from **VDI Menu** > **Global Connection Settings** > **Blast**. You can go to the Omnissa Horizon Performance tracker and see **Encoder Name** to verify whether HEVC is working. 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.

NOTE: You must upgrade Wyse Management Suite to version 5.0 to support the HEVC feature.

For more information, see the *Omnissa Blast Extreme Optimization Guide* at Omnissa Techzone site.

Enable or disable HEVC from Admin Policy Tool and Wyse Management Suite Policy settings

Steps

1. Go to the Admin Policy Tool or Wyse Management Suite policy settings.
2. In the **Advanced** tab, expand **Session Settings**.
3. Click **Horizon Session Settings**.
4. Click the **Allow High Efficiency Video Decoding** toggle to enable or disable HEVC.
5. Click **Save & Publish**.

Switch between codecs in Blast sessions

Omnissa Blast sessions support the use of industry-standard codecs such as H.264, HEVC for remoting screen content from Horizon Agent to Horizon Client.

- **Prerequisite**—Horizon Agent 2203 or later must be installed to support High Definition Color for H.264 or HEVC.
- The Horizon administrator can use agent-side group policy settings to activate or deactivate the Omnissa Blast features, including High Definition Color for H.264 and HEVC.
- Horizon Agent uses a hardware codec when your system environment meets the following criteria:
  - The agent machine supports the hardware codec.
  - For HEVC and AV1, the client machine must have a GPU that supports the hardware codec.
- Omnissa Blast options on the client are configured to allow use of the decoding method.
- Currently, thin clients do not support AV1 and HEVC 4:4:4 configurations.
- Horizon Agent chooses a hardware codec according to the following order of preference:
  - HEVC 4:4:4 (high-definition color)
  - H.264 4:4:4 (high-definition color)
  - HEVC 4:2:0 (standard-definition color)
  - H.264 4:2:0 (standard-definition color)
- If hardware codecs are not supported on both the client and agent machines, Horizon Agent chooses a software codec according to the following order of preference and decoding methods that are allowed on the client:
  - BlastCodec (high-definition color)
  - H.264 4:4:4 (high-definition color)
  - H.264 4:2:0 (standard-definition color)
  - Adaptive (high-definition color)

Enable Scanner Redirection

Scanner Redirection feature enables you to scan information from VDI desktops using scanning and imaging devices that are connected to your thin client. Scanner Redirection supports standard scanning and imaging devices that are compatible with TWAIN and Scanner Access Now Easy (SANE) formats. The scanner redirection feature is applicable only for Blast sessions.

Prerequisites

Ensure that the Scanner Redirection feature is installed in the Omnissa Horizon session. You must select this feature in the Omnissa Horizon Agent wizard during the Horizon agent installation.

Steps

1. Log in to the ThinOS client.
2. From the system menu, click **Admin Policy Tool**.
3. In the **Advanced** tab, click **Session Settings**, and expand **Horizon Season Settings**.
4. Configure the following options based on your preference:
   - If the Scanner Class ID starts with 06, click the **Allow USB Imaging Family Device Redirection** toggle switch to enable the Scanner Redirection feature.
   - If the Scanner Class ID does not start with 06, enter the Scanner VID and PID in the format `vid-xxxx_pid-yyyy` in the **Include Vid/Pid USB Device Redirection** field.
5. Click **Save & Publish**.
6. Launch the Horizon desktop on ThinOS.
7. Open the Omnissa Scanner Redirection menu from the Windows system tray.
   The available scanners are listed and can be selected based on your preference.

Enable Serial Port Redirection

Serial Port redirection feature enables you to redirect serial (COM) ports such as integrated RS232 ports or USB ports that are connected locally to serial-USB adapters. You can connect the serial devices to serial ports on your thin client and then use the serial devices in VDI desktops. The serial port redirection feature is applicable only for Blast sessions.

To use the Serial Port Redirection feature, you must install the feature in the Omnissa Horizon session. This feature is installed in the Omnissa Horizon Agent during the Horizon Agent installation. After the Serial Port Redirection feature is enabled in the VDI session, do the following:

1. Launch a Horizon desktop on ThinOS.
2. Open the Omnissa Serial Port Redirection menu from the Windows system tray.

The available serial ports are listed and can be selected based on your preference. In Windows Device Manager, the serial port is displayed as **Serial Port Redirection over Omnissa Horizon (COM1)**.

Enable Session Collaboration

Session Collaboration redirection feature enables you to invite other users to join your remote desktop session. The session collaboration feature is applicable only for Blast sessions.

NOTE: You cannot accept the invitation and join the remote desktop session of other users. This is a limitation on ThinOS.

By default, the session collaboration feature is enabled in the Omnissa session. To invite a user to join your desktop session, do the following:

1. Launch a Horizon desktop on ThinOS.
2. Click the Omnissa Session Collaboration icon from the Windows system tray.
3. Enter the username or email address and click **Send**.

Enable Battery State Redirection

Battery State Redirection feature enables you to redirect the battery information of the ThinOS device to a remote desktop. To use the Battery State Redirection feature, you must ensure that the **Enable Battery State Redirection Agent Policy**

Setting is enabled in Group Policy Management Editor. By default, this feature is enabled. The battery state redirection feature is applicable only for Blast sessions.

Relative mouse

When you enable the relative mouse feature, Horizon Client uses relative coordinates to transmit data about the mouse pointer movement and improve the mouse performance. The relative mouse feature is applicable for both PCoIP and Blast-enabled thin clients.

NOTE: The touchscreen may not work when the relative mouse feature is enabled. This is an Omnissa limitation.

Enable relative mouse using Admin Policy Tool or Wyse Management Suite

Steps

1. On the ThinOS client, start **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **Horizon Session Settings** if you are using Omnissa Horizon Client SDK pkg or click **Horizon Session Settings** if you are using PCoIP desktop with Omnissa Horizon Session SDK pkg.

   NOTE: The name of Blast Session Settings is changed to Horizon Session Settings.

3. Click the **Enable Relative Mouse when launching Horizon session** if you want to enable it in the Horizon desktop with Omnissa Horizon Session SDK pkg.
4. Click **Save & Publish**.

Enable relative mouse using session menu

Steps

1. On the ThinOS client, launch a Horizon PCoIP session or a Blast session.
2. In the system tray, click the Omnissa icon to view the active Blast sessions and Horizon PCoIP sessions. If you are using Horizon PCoIP desktop with Omnissa Horizon Session SDK pkg, click the PCoIP icon in the system tray.
3. Select a session from the menu.
4. Enable **Relative Mouse**.

   NOTE: To disable the relative mouse feature, press Ctrl+ Alt key combination in a Blast session or press Ctrl +Alt+Down key combination in a PCoIP session.

Configure Workspace ONE Mode

Omnissa Workspace ONE mode enables you to connect to remote desktops and applications through the Workspace ONE Web Portal. As a Horizon administrator, you can enable the Workspace ONE mode on a Connection Server instance. Horizon Client users are redirected to a Workspace ONE server to launch their remote desktops and applications.

Steps

1. Open the Omnissa Connection Server console.
2. Go to **Settings** > **Servers** > **Connection Server** > **OmnissaSRV** > **Edit**, and click the **Authentication** tab.
3. From the **Delegation of authentication to Omnissa Horizon (SAML 2.0 Authentication)** drop-down list, select **Required**.
4. Click **Manage SAML Authenticators** to add your Authenticator.
5. Select the **Enable Workspace ONE** mode check box.
6. Enter the Workspace ONE Server hostname and click **OK**.
7. Log in to the ThinOS client.
8. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
   The **Remote Connections** dialog box is displayed.

9. In the **Broker Setup** tab, select **Omnissa Horizon** from the **Select Broker Type** drop-down list.
10. Enter the server URL in the **Broker Server** field.
11. Click **Save** and restart the thin client.
    The **Omnissa Workspace ONE** login window is displayed.
12. Enter the user credentials and click **Sign In**.

    NOTE: The ThinOS lock terminal is not supported in Workspace ONE Mode. When you attempt to lock the terminal, a warning message is displayed prompting for automatic sign-off. Click **Continue** if you want to sign out from the session.

    NOTE: The **Remember this setting** option in the Workspace ONE web portal is not supported due to the customized browser limitation.

Unified Access Gateway

ThinOS supports Unified Access Gateway (UAG) that is used to securely access remote desktops and applications that are outside a corporate firewall. For information about the latest version of Unified Access Gateway, see **Unified Access Gateway Documentation** at docs.omnissa.com.

Omnissa Horizon 7.11 with Unified Access Gateway 3.8 and later uses SAML-based multifactor authentication. It supports many modern cloud-based solutions including the Azure multifactor authentication.

Configure Unified Access Gateway on ThinOS

Prerequisites

- Configure the Unified Access Gateway (UAG) setting on the server side. For more information about configuring the server-side settings for UAG, see the Omnissa Unified Access Gateway documentation at docs.omnissa.com.
- Open the connection server admin page, and specify the UAG information in the following sections:
  - **HTTP(s) Secure Tunnel**
  - **PCoIP Secure Gateway**
  - **Blast Secure Gateway**

Steps

1. Start the ThinOS client.
2. From the desktop menu, click **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
3. On the **Broker Setup** tab, select **Omnissa Horizon** from the **Select Broker Type** drop-down list.
4. In the **Broker Server** field, enter the Unified Access Gateway URL.
5. Click **Save**.

Configure Microsoft Azure Multifactor authentication with Omnissa Unified Access Gateway

Prerequisites

Configure the Unified Access Gateway (UAG) settings and Azure Multifactor authentication settings on the server side. For more information about configuring the server-side settings, see the Microsoft Azure MFA with Omnissa UAG documentation at docs.omnissa.com.

Steps

1. Start the ThinOS client.
2. From the desktop menu, click **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
3. On the **Broker Setup** tab, select **Omnissa Horizon** from the **Select Broker Type** drop-down list.
4. In the **Broker Server** field, enter the Unified Access Gateway FQDN.

5. Click **Save**.
6. On the Azure **Sign In** window, enter the Azure account.
7. Click **Next**.
8. Enter the password to log in to the session.

Device Certificate authentication with Unified Access Gateway and Passthrough

About this task

With the client device certificate authentication feature, Unified Access Gateway authenticates the thin client system. After successful device authentication, you must complete user authentication. For more information about this feature, see the Omnissa documentation at docs.omnissa.com.

Steps

1. Go to **Wyse Management Suite** or **Admin Policy Tool**.
2. Go to **Login Experience** > **Login Settings.**
3. Disable **Login Use Smartcard Certificate Only**.
4. Click **Save**.
5. Import the PFX certificate into ThinOS.
6. Configure the Horizon Broker agent with the UAG server address.
7. Start the Broker agent login process.
8. Select the certificate to log in.

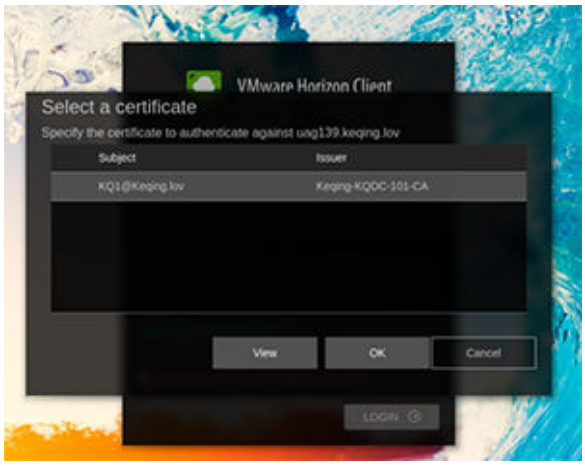

Figure 33. Selecting a certificate

X.509 Certificate Authentication

About this task

You can configure the X.509 certificate authentication in Unified Access Gateway to allow ThinOS to authenticate with certificates. For more information about this feature, see the Omnissa documentation at docs.omnissa.com

Steps

1. Connect the smartcard reader to the ThinOS client.
2. Configure the Horizon Broker agent with UAG server address.
3. Insert the smartcard in the smartcard reader.
4. Select the valid certificate.
5. Enter the PIN to login.

RADIUS Authentication

About this task

RADIUS offers a wide range of third-party, two-factor authentication options. To use RADIUS authentication on Unified Access Gateway, you must have a configured RADIUS server that is accessible on the network from Unified Access Gateway.

Steps

1. Configure the Horizon Broker agent with UAG server address.
2. Enter the RADIUS username and passcode to log in.

RSA SecurID Authentication

About this task

After the Unified Access Gateway appliance is configured as the authentication agent in the RSA SecurID server, add the RSA SecurID configuration information to the Unified Access Gateway appliance.

Steps

1. Configure the Horizon Broker agent with the UAG server address.
2. Enter the RSA username and passcode to log in.

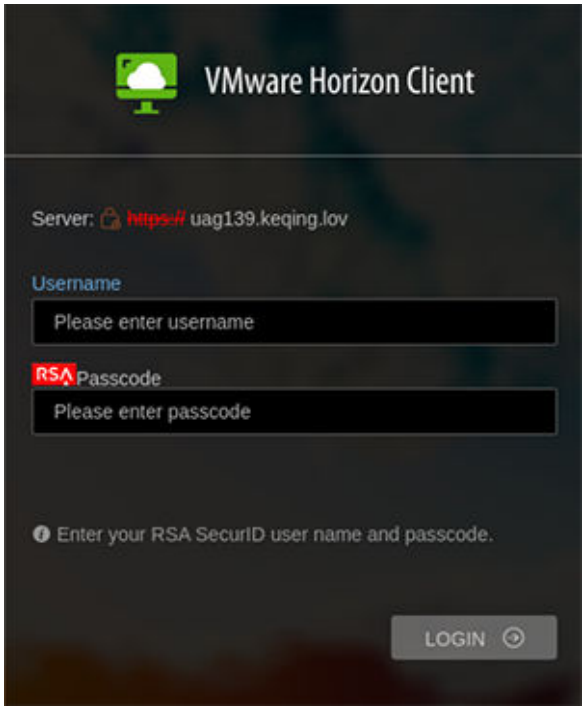

Figure 34. Enter RSA username and passcode

SAML Authentication

About this task

If you are using SAML version 2.0 identity provider, you can directly integrate the identity provider with the Unified Access Gateway (UAG) to support Horizon client user authentication.

To use SAML third-party integration with UAG, you must use Horizon Connection Server 7.11 or later versions.

To integrate the UAG with the identity provider, do the following:

Steps

1. Configure the identity provider with the service provider (UAG) information.
2. Upload the metadata file of the identity provider to the UAG.
3. Configure the Horizon settings on the UAG Admin console.

Next steps

No additional configuration is required in ThinOS. But, after the Broker agent connection is established, you are prompted to do a third-party authentication.

Configure the Omnissa integrated printing settings

About this task

The Omnissa Integrated Printing feature allows you to print to a local or network printer without installing additional printer drivers in the remote desktop. The USB redirection feature enables you to print from a remote desktop using a USB printer that is connected to the local client device. For each printer configured locally on ThinOS, you must map the printer to the Omnissa Blast desktop. ThinOS Blast printer mapping is equivalent to Omnissa client printer redirection.

Currently ThinOS supports only PS printer in blast session since Omnissa has removed Thin print support from Omnissa Horizon 8.0 and Omnissa Horizon Client 2006. Ensure that the Agent version is later than 7.9, and that you select the component Omnissa Integrated Printing. Certain PS model printers may not work in Blast session as it depends on the Omnissa integration printing support.

To map your printer, do the following:

NOTE: LPT printer is considered as an example to explain the printer mapping scenario. Printer mapping in ThinOS works similar to LPT for LPD and SMB printers.

Steps

1. Power on the ThinOS client with the Omnissa View broker configured in the **Broker Setup** tab.
2. Set the connection protocol as **All Supported** from the **Connection Protocol** drop-down list.
3. Go to **Global Connection Settings** > **Session**, and retain the **Exclude printer devices** check box selection. This option is selected by default.
4. Plug in a USB printer to the ThinOS client terminal.
5. Go to **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
6. In the **Printer Setup** dialog box, do the following:
   a. From the **Select Port** drop-down list, select **LPT 1**.
   b. Enter valid printer name and printer identification.
   c. Select the **Enable the printer device** check box.
   d. Click **Save** to save the configuration.
7. Click the **Options** tab, and do the following:
   a. Set **LPT1: <Printername>**as default printer.
   b. Click **Save** to save the configuration.
8. Connect to a Omnissa Blast session and go to **Control Panel** > **Devices and Printers**.
   The printer that is configured locally in ThinOS is mapped to the session. The mapped printer's driver is Omnissa POSTSCRIPT Driver and the port is VMWPORT.
   The Omnissa Integrated Printing feature allows the ThinOS local printer to be mapped to the Omnissa Blast session without installing the printer driver in the session.

Configure the USB Printer Redirection in Omnissa Blast and PCoIP session

Steps

1. Connect a USB printer to the ThinOS client.
2. Go to **Global Connection Settings** > **Session** and clear the **Exclude printer devices** check box. This option is selected by default.

3. Log off from Omnissa Broker agent, and then log in again.
4. Log in to a Blast or a PCoIP session.
5. Go to **Control Panel** > **Devices and Printer** and verify if the printer driver is automatically installed.
   After the printer driver installation is complete, the redirected printer is listed in the **Printers** section.
   NOTE: The drivers of certain printers may not get installed on the target Windows server automatically as the installation depends on the Windows server. In such scenarios, the drivers must be installed manually.

USB Redirection in a VDI session

Upgrading to the ThinOS 10.0052 eliminates the local USB driver dependency on the USB redirection feature.

You can directly use the USB redirection feature in a VDI session without attaching the USB driver that is installed locally on your thin client. The local USB driver is automatically detached when using USB redirection in the VDI session. As a result, the USB redirection in the VDI session is fast and more reliable.

After upgrade, if you are configuring the USB settings on your local thin client, do either of the following:

- Using Global Connection Settings:
  1. On the local ThinOS client, go to the **Global Connection Settings** > **Auto-connect to local devices and USB device redirection**.
  2. Verify if the USB device redirection is selected, and click **Save**.
- Using Admin Policy Tool:
  1. On the Admin Policy Tool, go to **Advanced** > **Session Settings** > **Global Session Settings** > **Local Resources and USB redirection**.
  2. Ensure that the USB redirection option is enabled, and click **Save and Publish**.

Apply these setting changes when you are using the USB Redirection for the first time, after you upgrade from ThinOS 9.5.4x or older versions to ThinOS 10.0052. The setting changes are not required after the first instance. If you are configuring the USB settings using Wyse Management Suite policy settings, you do not have to enable the USB redirection option again after upgrade.

There are no visible UI changes on the ThinOS client. However, the USB redirection speed is improved in the VDI session.

NOTE: USB redirection in a PCoIP session works similarly to USB redirection in a Blast session.

NOTE: To work on Topaz signature pad, use the Split Vid/Pid Device component **vid-06a8_pid-0043(exintf:03)** in Horizon session.

For PCoIP session, ensure that the Group Policy is enabled to make the USB redirection work. Do the following to enable the GPO feature:

1. Open a PCoIP session and press WIN+R to open the Run window.
2. Enter gpedit.msc to open the Local Group Policy Editor.
3. Go to **Computer Configuration** > **Administrative Templates** > **PCoIP Session Variables** > **Not Overridable Administrator Settings**, open **Configure PCoIP USB allowed and unallowed device rules**, select **Enable**, and click **Apply**.

NOTE: These steps are applicable to PCoIP session in Omnissa Horizon broker and Teradici Cloud Access broker. For Teradici Remote Workstation Card and Amazon WorkSpace session, USB redirection is not supported by third party.

NOTE: The SDK integrated in ThinOS for PCoIP does not support the USB redirection feature for all USB drives. This is a limitation from the third party SDK. For Headset and Camera, PCoIP does not support redirection in a session. Use RTAV for audio and video devices.

Enable Multimedia Redirection in Blast session

Steps

1. Access the Omnissa Horizon connection server from the browser.
2. Go to **Settings** > **Edit policies**.
3. Change the **Multimedia Redirection (MMR)** drop-down value to **Allow**.
   The default value is Deny.

4. Click **OK**.

   NOTE: Multimedia Redirection (MMR) is enabled on ThinOS client side by default and there is no configuration item to disable MMR from ThinOS client. To disable the MMR feature, select the value as **Deny** in the Omnissa Horizon connection server. MMR feature uses Windows Media player as the default video player.

Smartphone sync

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

NOTE: Among the smartphones, only Iphone and Samsung phones are tested.

Sync Samsung Android smartphone and iPhone

Steps

1. Go to the Admin Policy Tool or Wyse Management Suite policy settings.
2. In the **Advanced** tab, expand **Session Settings**.
3. Click **Blast Session Settings**.
4. Enable the **Allow USB Imaging Family Device Redirection** option.
5. Click **Save & Publish**.
6. Launch the Blast session and connect your Samsung smartphone or iPhone to the device.
7. Accept the access request on your Samsung smartphone or iPhone.

Omnissa Horizon Kiosk Mode

Omnissa Horizon VDI Broker agent can be connected to Kiosk Mode by entering the username as **`Client Mac`**.

Prerequisites

For information about Kiosk Mode authentication and configuration, go to docs.omnissa.com.

Steps

1. From the desktop menu, click **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. Click the **General Options** tab, and do the following:
   a. Enter the username as **`Client Mac`** in the **Default Sign-on Username** field.

      NOTE: **`Client Mac`** is hard code username, and it is case-sensitive.

   b. Leave the **Default Sign-on password** field empty.
   c. Leave the **Default Sign-on Domain** field empty.
3. Click **Save** to save your settings.

   NOTE: In earlier ThinOS versions, you must click the **LOGIN** button to log in to Omnissa Horizon Broker agent when Kiosk Mode is configured in ThinOS. From ThinOS 10.x 2502, Omnissa Horizon logs in automatically if the Kiosk Mode account **`Client Mac`** is configured as the ThinOS default user.

Configuring other brokers

You can configure other brokers in **Remote Connections**. Leostream, Parallels RAS, and Systancia Workplace brokers are supported in ThinOS 10.x 2502.

- In the **Select Broker Type** drop-down list under **Remote Connections** > **Broker Setup**, **Other Broker** option has been added that supports Leostream and Parallels RAS Broker agents.

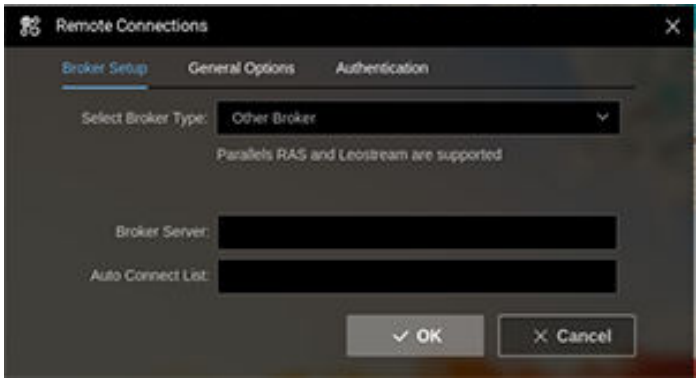

Figure 35. Other Broker option in Remote Connections

- You can also configure the other Broker agents in Wyse Management Suite and Admin Policy Tool by going to **Broker Settings** > **Other Broker Settings**.
  1. In the **Broker Server** field, you can configure the Broker agent server address by adding the URL of the other Broker agent.
  2. In the **Auto Connect List** field, you can configure the desktop and applications that must be automatically connected.
  3. In the **Notice to Broker Connection**, when using Parallels RAS Broker agent, **Enable Password Variables** must be enabled in **Login Experience** > **Login Session**.
     - The server certificate must be imported in ThinOS before connecting to the Broker agent.
     - The Broker agent URL must be in FQDN format.

Leostream

- Leostream connection broker version is 9.0.40.10.
- Leostream agent version is 7.3.8.0.
- Remote Desktop Protocol (RDP) is supported during Leostream desktop sessions. AVD application package must also be installed.

Parallel RAS (Remote Application Server)

- Parallel Remote Application Server (RAS) version is 18.0.22497.
- Remote Desktop Protocol (RDP) is supported during desktop and application sessions. AVD application package must also be installed.

Systancia Workplace

Systancia Workplace is an application and desktop virtualization solution.

NOTE: ThinOS 10.x 2502 provides only experimental support for Systancia Workplace and is going to be supported in future ThinOS releases.

- Supports Systancia Workplace Broker agent.
- Supports RDP for VDI sessions using the Systancia Workplace broker. AVD application package must also be installed.
- **Known Issue**
  - If Systancia Workplace Broker agent does not respond in 5 s, login fails with a timeout error message. As a workaround, log in again when facing the timeout error.

Special Peripheral Support

Nitgen Fingkey Hamster III Fingerprint USB device

Nitgen Fingkey Hamster III Fingerprint USB device redirection is supported in Citrix sessions. To enable Nitgen Fingkey Hamster III Fingerprint USB device redirection, do the following:

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

Bloomberg keyboard support

ThinOS 10.x supports Bloomberg Keyboard STB 100. The keyboard has two connection methods. One method uses a single USB cable to the USB port of the system. The second method is to connect dual USB cables to a KVM USB switch.

In a single USB cable connection, the keyboard device ID is **`vid-1188_pid-9545`**. All the six interfaces are under this device ID.

In the dual USB cable connection, the keyboard device IDs are **`vid-1188_pid-9525`** for one device and **`vid-1188_pid-9535`** for the other five devices.

Configure Bloomberg keyboard in Citrix sessions

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB For ace Redirect** section:
   - Redirect the entire keyboard into the session—The keyboard feature keys, fingerprint reader, and the KVM Keyboard are redirected into the session.
     - For Bloomberg keyboard that is connected with a single USB cable, add one row and enter the device ID. For an example , enter **`0x11889545`** to configure the device.
     - For Bloomberg keyboard that is connected with dual USB cables, add two rows and enter the device IDs. For an example , enter **`0x11889525`** in one row and **`0x11889535`** in the other.
   - Split the keyboard and partly redirect into the session—You can redirect the keyboard feature keys, fingerprint reader, or the KVM Keyboard individually.
     - For Bloomberg keyboard that is connected with a single USB cable, add one row and enter the device ID. For an example , enter **`0x11889545010100`**. This configuration means that the interface 010100 is redirected into session and other interfaces are not redirected.
     - For Bloomberg keyboard that is connected with dual USB cables, add one row and enter the device ID. For example, enter **`0x11889545030001`**. This configuration means that the interface 030001 is redirected into session and other interfaces are not redirected.
4. Click **Save & Publish**.

Configure Bloomberg keyboard in PCoIP sessions

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB Force Redirect** section.
   The Keyboard Feature keys, fingerprint reader, and the KVM Keyboard are redirected into the session.
   - For Bloomberg keyboard that is connected with a single USB cable, enter the device ID **`0x11889545`** to configure the device.
   - For Bloomberg keyboard that is connected with dual USB cables, add two rows in the **vUSB Force Redirect** section, enter **`0x11889525`** in one row and **`0x11889535`** in the other.

   NOTE: PCoIP does not support USB device splitting.
4. Click **Save & Publish**.

Redirect Bloomberg keyboard in Omnissa Horizon Blast sessions

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. In the Advanced tab, click **Broker Settings**, and expand **Omnissa Horizon Settings**.
   - Redirect the entire keyboard into the session—The keyboard feature keys, fingerprint reader, and the KVM Keyboard are redirected into the session.
     - For Bloomberg keyboard that is connected with a single USB cable, enter **`vid-1188_pid-9545`** in the Included **Vid/Pid USB Device Redirection** field.
     - For Bloomberg keyboard that is connected with dual USB cables, enter **`vid-1188_pid-9525;vid-1188_pid-9535`** in the Included **Vid/Pid USB Device Redirection** field.
   - Split the keyboard and partly redirect into the session—You can redirect the keyboard feature keys, fingerprint reader, or the KVM Keyboard individually.
     - For Bloomberg keyboard that is connected with a single USB cable:
       a. Enter **`vid-1188_pid-9545`** in the **Include Vid/Pid USB Device Redirection** field.
       b. Enable the **Allow Auto USB Device Splitting Redirection** button.
       c. Enter **`vid-1188_pid-9545(exintf:00;exintf:01;exintf:02)`** in the **Split Vid/Pid Device** field.

       NOTE: This configuration means that the interfaces 03, 04, and 05 are redirected into session and the other interfaces 00, 01, and 02 are not redirected. 03, 04, and 05 are audio-related interfaces. The analog headset from the audio port in the Bloomberg keyboard can be redirected into the Blast session.
     - For Bloomberg keyboard that is connected with dual USB cables:
       a. Enter **`vid-1188_pid-9535`** in the **Include Vid/Pid USB Device Redirection** field.
       b. Enable the **Allow Auto USB Device Splitting Redirection** button.
       c. Enter **`vid-1188_pid-9535(exintf:00;exintf:01)`** in the **Split Vid/Pid Device** field.

       NOTE: This configuration means that the interfaces 02, 03, and 04 are redirected into session and the other interfaces 00 and 01 are not redirected. 02, 03, and 04 are audio related interfaces. The analog headset from the audio port in the Bloomberg keyboard can be redirected into the Blast session.
3. Click **Save & Publish**.

Remove Bloomberg keyboard force redirection settings for Omnissa Blast

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Session Settings**, and click **Blast Session Settings**.

4. Remove the following Bloomberg keyboard entries from the **Include Vid/Pid USB Device Redirection** field.
   - vid-1188_pid-9545
   - vid-1188_pid-9525
   - vid-1188_pid-9535
5. Click **Save & Publish**.

Bloomberg keyboard limitations

- Hot plugging the Bloomberg keyboard is not supported for Bloomberg keyboard redirection. Configure the keyboard before logging in to the Broker agent and launching the session.
- Disconnecting the Bloomberg keyboard cables when it is redirected into session may cause the session to close or the system to randomly reboot.

Confirm the USB interface redirection

This section contains the steps to confirm whether the USB audio device is redirected into the VDI session. You can confirm the USB redirection from the Device Manager, from the Audio Manager, or from the ThinOS **Event Log**.

Find the Vendor ID or Product ID of the connected device in ThinOS

This section contains the steps to find the Vendor ID (VID) or Product ID (PID) of your device in ThinOS.

Steps

1. Connect the USB device into the thin client.
2. Go to **Settings** > **System Tools** > **Devices**.
3. Expand **USB Bus** to find the name of your connected USB device.
4. Expand the name of the connected USB device to find the device Class, VID, PID, and the device interface.
   For example, if your connected USB device is **Nuance PowerMic II-NS**, the details are displayed as the following:

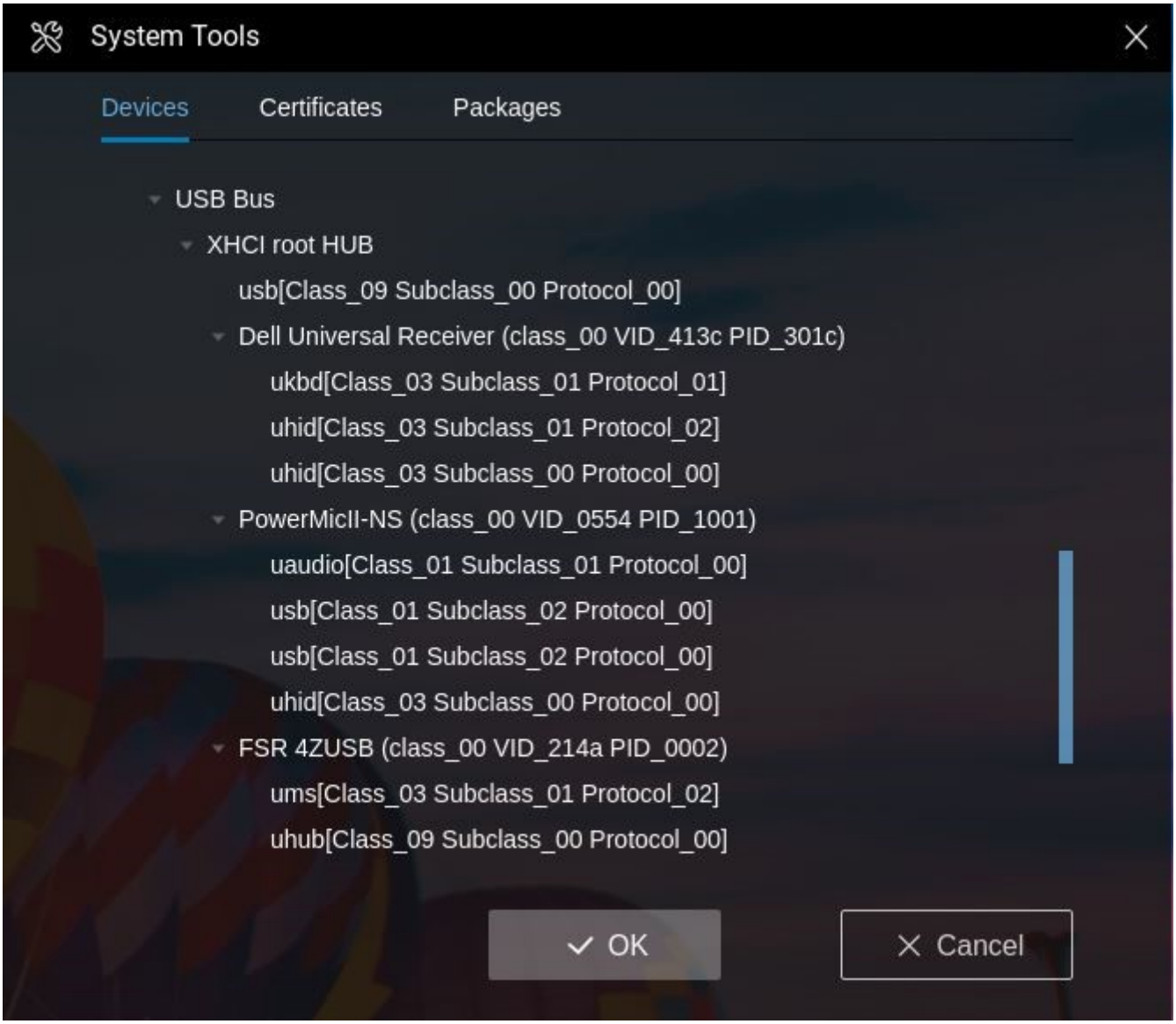

Figure 36. VID and PID

- Device name—**PowerMicII-NS**
- Device class—**class_00**
- VID—**VID_0554**
- PID—**PID_1001**
- Device interface—four interfaces belong to this device.
  - **uaudio (Class_01 Subclass_01 Protocol_00)**
  - **usb (Class_01 Subclass_02 Protocol_00)**
  - **usb (Class_01 Subclass_02 Protocol_00)**
  - **uhid (Class_03 Subclass_00 Protocol_00)**

Disable the USB device local driver during USB device redirection

Steps

1. In Wyse Management Suite setting or ThinOS local Admin Policy Tool, go to **Advanced > Peripheral Managment > USB Redirection > vUSB Force Redirect**.
2. Click **Add Row**.
3. Enter `0xvvvvpppp,NoDriver` or `0xvvvvppppccsspp,NoDriver`.

Results

0xvvvvpppp,NoDriver disables the local driver of the whole device; **v** stands for vendor ID and **p** for production ID. **0xvvvvppppccsspp,NoDriver** disables the local driver of one class of one device and applies only to multifunction devices with different classes.

Confirm the USB interface redirection from Device Manager in ThinOS

Steps

1. Go to **Settings** > **Peripherals**.
   The **Peripherals** dialog box is displayed.
2. Click the **Audio** tab.
3. Expand **USB Bus** to find the name of your connected USB device. If the USB redirection is successful, all the information under the USB device displays a **usb** prefix.
   For example, if your connected USB device is **Nuance PowerMic II-NS**, the details are displayed as the following:

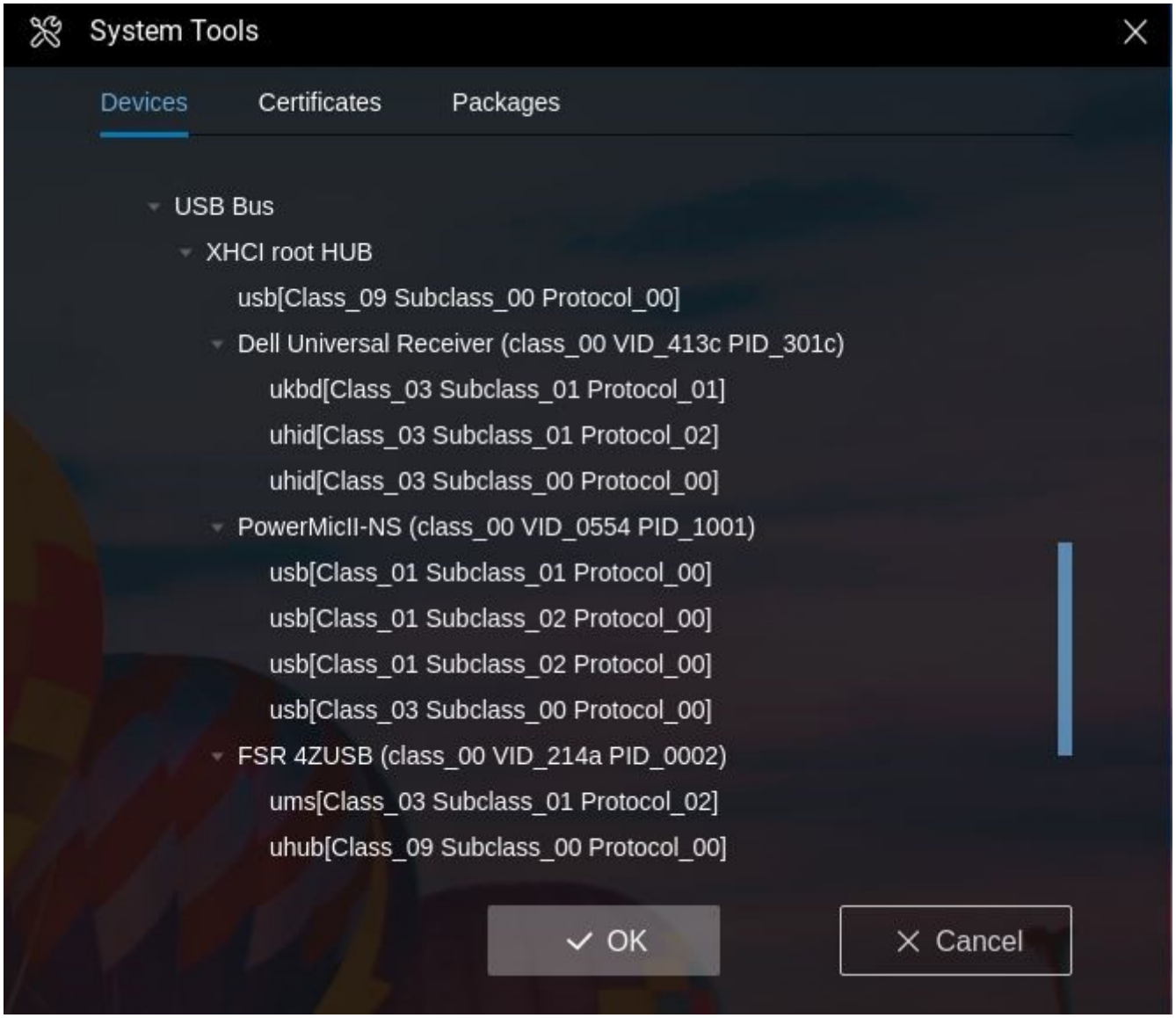

Figure 37. USB redirection

- **usb (Class_01 Subclass_01 Protocol_00)**
- **usb (Class_01 Subclass_02 Protocol_00)**
- **usb (Class_01 Subclass_02 Protocol_00)**

- **usb (Class_03 Subclass_00 Protocol_00)**

Confirm the USB interface redirection from Audio Manager in ThinOS

Steps

1. Go to **Settings** > **Peripherals**.
   The **Peripherals** dialog box is displayed.
2. Click the **Audio** tab. If the USB redirection is successful, the USB device is not displayed in drop-down lists under **Playback Devices** or **Record Devices**.

Confirm the USB interface redirection from ThinOS Event Log

Steps

1. Go to **System Information** > **Event Log**.
2. Verify the logs in the **Event Log** tab to confirm whether the USB redirection is successful.
   For example, the thin client has only two audio devices **HD audio-1** and **PowerMicII-NS**:
   - If your logs display the following details, it means that the **USB device** is redirected into the VDI session and the ThinOS **playback** and **recording** devices are changed to **HD audio-1**.
     - **Change playback to HD audio-1**
     - **Change record to HD audio-1**
   - If your logs display the following details, it means that the **USB device** is released from the VDI session and the ThinOS **playback** and **recording** devices are reverted.
     - **Change playback to PowerMicII-NS**
     - **Change record to PowerMicII-NS**

Set playback or recording devices as default

To set the playback or recording devices as default, see Set default playback or recording devices.

Nuance PowerMic II-NS

The following are the device information of **Nuance PowerMic II-NS**.

- Device ID—**Class 00, VID 0554, PID 1001**
- Device interface:
  - Audio or microphone interface—**010100**
  - HID button interface—**030000**
  - Mouse or track pad interfaces

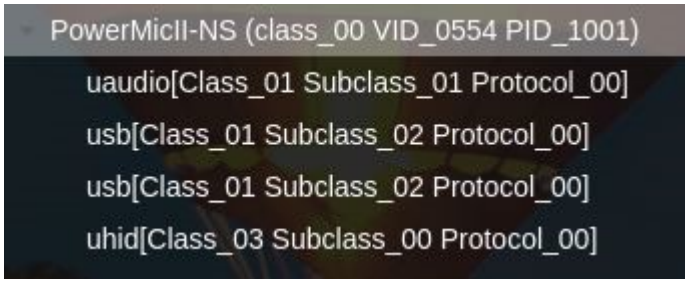

Figure 38. Device interface

NuancePowerMic II-NS redirection in a Citrix session

Full USB redirection in a Citrix session

Except the mouse, all other interfaces are redirected to the VDI session.

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID **`0x05541001`**.
4. Click **Save & Publish**.

Connecting Nuance PowerMic II-NS in a Citrix session

Launch Citrix session and connect **Nuance PowerMic II-NS** into the thin client.

- **Nuance PowerMic II-NS** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Nuance PowerMic II-NS** device is displayed in the Citrix session under **Device Manager** > **Sound, video and game controllers**.
- **Nuance PowerMic II-NS** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- In the **Nuance Dragon Medical One** desktop application, **Nuance PowerMic II-NS** is displayed in the **Microphone** drop-down list. All the HID buttons, voice recording, and audio playback features work in the **Nuance Dragon Medical One** desktop application.

HID buttons redirection in a Citrix session

Only the HID buttons are redirected into the VDI session. Other parts such as Audio or Microphone are kept in the ThinOS local device.

Configuration in ThinOS for HID buttons redirection only

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, go to **Peripheral Management** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
3. In the Citrix INI Settings, click **Add Row**.
4. From the File drop-down list, select **module.ini**.
5. From the Operation drop-down list, select **Add or Update**.
6. In the Section field, enter **`ClientAudio`**.
7. In the Key field, enter **`AudioRedirectionV4`**.
8. In the Value field, enter **`True`**.
9. Go to **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
10. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID **`0x05541001030000`**.
11. Click **Save & Publish**.

Connecting Nuance PowerMic II-NS in a Citrix session with only HID buttons redirection

Launch Citrix session and connect **Nuance PowerMic II-NS** into the thin client.

- **Nuance PowerMic II-NS** device is displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Nuance PowerMic II-NS** device is displayed in the Citrix session under **Device Manager** > **Sound, video and game controllers**.

- **Nuance PowerMic II-NS** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- In the **Nuance Dragon Medical One** desktop application, **Nuance PowerMic II-NS** is displayed in the **Microphone** drop-down list. All the HID buttons, voice recording, and audio playback features work in the **Nuance Dragon Medical One** desktop application.

NOTE: The **module.ini** setting in Citrix is for the Citrix multi audio feature. If you do not add this setting, **Nuance PowerMic II-NS** does not get displayed in Citrix sessions.

NuancePowerMic II-NS redirection in an Omnissa Blast session

Full USB redirection in an Omnissa Blast session

Except for the mouse, all other interfaces are redirected to the VDI session.

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.
3. Enter `vid-0554_pid-1001` in the **Include Vid/Pid USB Device Redirection** field.
4. Click **Save & Publish**.

Connecting Nuance PowerMic II-NS in an Omnissa Blast session

Launch the Omnissa Blast session and connect **Nuance PowerMic II-NS** into the thin client.

- **Nuance PowerMic II-NS** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Nuance PowerMic II-NS** device is displayed in the Omnissa Blast session under **Device Manager** > **Sound, video and game controllers**.
- **Nuance PowerMic II-NS** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- In the **Nuance Dragon Medical One** desktop application, **Nuance PowerMic II-NS** is displayed in the **Microphone** drop-down list. All the HID buttons, voice recording, and audio playback features work in the **Nuance Dragon Medical One** desktop application.

HID buttons redirection in an Omnissa Blast session

Only the HID buttons are redirected into the VDI session. Other parts such as Audio or Microphone are kept in the ThinOS local device.

Configuration in ThinOS for HID buttons redirection only

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, go to **Session Settings** > **Horizon Session Settings**.
3. Enter `vid-0554_pid-1001` in to the **Include Vid/Pid USB Device Redirection** field.
4. Enable **Allow Auto USB Device Splitting Redirection**.
5. Enter `vid-0554_pid-1001(exintf:00;exintf:01;exintf:02)` in to the **Spit Vid/Pid Device** field.
6. Click **Save & Publish**.

Connecting Nuance PowerMic II-NS in an Omnissa Blast session

Launch the Omnissa Blast session and connect **Nuance PowerMic II-NS** into the thin client.

- **Nuance PowerMic II-NS** device is displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Nuance PowerMic II-NS** device is not displayed in the Omnissa Blast session under **Device Manager** > **Sound, video and game controllers**. Only the Omnissa virtual microphone or audio is displayed.
- **Nuance PowerMic II-NS** device cannot be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- In the **Nuance Dragon Medical One** desktop application, **Nuance PowerMic II-NS** is not displayed in the **Microphone** drop-down list. However, all the HID buttons work in the **Nuance Dragon Medical One** desktop application. Voice recording works from both Omnissa Blast session and **Peripherals** > **Audio** > **Recorder** in the local ThinOS user interface. Audio works from both Omnissa blast session and ThinOS local user interface.

NOTE: The audio behaviors are different from Citrix sessions since Omnissa Blast session does not support multiple audio devices.

Nuance PowerMic II-NS redirection in a PCoIP session

Full USB redirection in a PCoIP session

Except the mouse, all other interfaces are redirected to the VDI session.

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in **vUSB Force Redirect** section, and enter the device ID **0x05541001**.
4. Click **Save & Publish**.

Connecting Nuance PowerMic II-NS in a PCoIP session

Launch the PCoIP session and connect **Nuance PowerMic II-NS** into the thin client.

- **Nuance PowerMic II-NS** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Nuance PowerMic II-NS** device is displayed in the PCoIP session under **Device Manager** > **Sound, video and game controllers**.
- **Nuance PowerMic II-NS** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- In the **Nuance Dragon Medical One** desktop application, **Nuance PowerMic II-NS** is displayed in the **Microphone** drop-down list. All the HID buttons, voice recording, and audio playback features work in the **Nuance Dragon Medical One** desktop application.

NOTE: PCoIP does not support USB interface splitting function. Hence, the feature to only redirect HID buttons is not supported in a PCoIP session.

Olympus RecMic DR-2200

The following are the device information of **Olympus RecMic DR-2200**.

- Model—2200
- Device ID—**Class 00,VID 07b4, PID 0254**

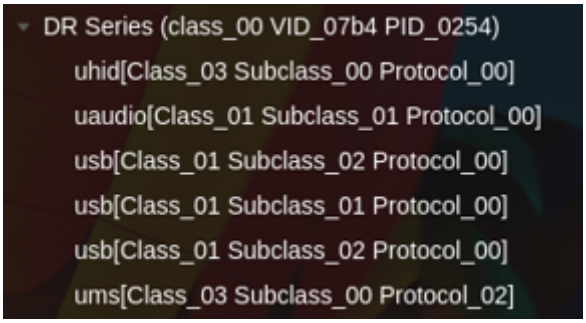

Figure 39. Device information

Olympus RecMic DR-2200 redirection in a Citrix session

Full USB redirection in a Citrix session

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID `0x07b40254`.
4. Click **Save & Publish**.

Connecting Olympus RecMic DR-2200 in a Citrix session

Launch Citrix session and connect **Olympus RecMic DR-2200** into the thin client.

- **Olympus RecMic DR-2200** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Olympus RecMic DR-2200** device is displayed in the Citrix session under **Device Manager** > **Sound, video and game controllers**.
- **Olympus RecMic DR-2200** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- All the control buttons work in the **Olympus Device Configuration Manager** application.
- Audio playback and audio recording works with **Olympus RecMic DR-2200**.

HID buttons redirection in a Citrix session

Only the HID buttons are redirected into the VDI session. Other parts such as Audio or Microphone are kept in the ThinOS local device.

Configuration in ThinOS for HID buttons redirection only

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, go to **Peripheral Management** > **VDI Configuration Editor** > **Citrix Configuration Editor**.
3. In the Citrix INI Settings, click **Add Row**.
4. From the File drop-down list, select **module.ini**.
5. From the Operation drop-down list, select **Add or Update**.
6. In the Section field, enter `ClientAudio`.
7. In the Key field, enter `AudioRedirectionV4`.
8. In the Value field, enter `True`.

9. Go to **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
10. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID **0x07b40254030000**.
11. Click **Save & Publish**.

Connecting Olympus RecMic DR-2200 in a Citrix session with only HID buttons redirection

Launch Citrix session and connect **Olympus RecMic DR-2200** into the thin client.

- **Olympus RecMic DR-2200** device is displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Olympus RecMic DR-2200** device is displayed in the Citrix session under **Device Manager** > **Sound, video and game controllers**.
- **Olympus RecMic DR-2200** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- All the control buttons work in the **Olympus Device Configuration Manager** application.
- Audio playback and audio recording works with **Olympus RecMic DR-2200** in both ThinOS and Citrix sessions.

NOTE: The **module.ini** setting in Citrix is for the Citrix multi audio feature. If you do not add this setting, **Olympus RecMic DR-2200** does not get displayed in Citrix sessions. The recorder performance may not be clear on **Windows Voice Recorder** application when the audio and recording is not redirected. Dell Technologies recommends using other third-party voice recording applications.

Olympus RecMic DR-2200 redirection in an Omnissa Blast session

Full USB redirection in an Omnissa Blast session

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.
3. Enter **vid-07b4_pid-0254** in the **Include Vid/Pid USB Device Redirection** field.
4. Click **Save & Publish**.

Connecting Olympus RecMic DR-2200 in an Omnissa Blast session

Launch the Omnissa Blast session and connect **Olympus RecMic DR-2200** into the thin client.

- **Olympus RecMic DR-2200** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Olympus RecMic DR-2200** device is displayed in the Omnissa Blast session under **Device Manager** > **Sound, video and game controllers**.
- **Olympus RecMic DR-2200** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- While using the **Olympus Device Configuration Manager** application, all the HID buttons work. Audio and voice recording features work using **Olympus RecMic DR-2200**.

HID buttons redirection in an Omnissa Blast session

Only the HID buttons are redirected into the VDI session. Other parts such as Audio or Microphone are kept in the ThinOS local device.

Configuration in ThinOS for HID buttons redirection only

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, go to **Session Settings** > **Horizon Session Settings**.

3. Enter **vid-07b4_pid-0254** in to the **Include Vid/Pid USB Device Redirection** field.
4. Enable **Allow Auto USB Device Splitting Redirection**.
5. Enter **vid-07b4_pid-0254 (exintf:01;exintf:02;exintf:03;exintf:04** in to the **Spit Vid/Pid Device** field.
6. Click **Save & Publish**.

Connecting Olympus RecMic DR-2200 in an Omnissa Blast session

Launch the Omnissa Blast session and connect **Olympus RecMic DR-2200** into the thin client.

- **Olympus RecMic DR-2200** device is displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Olympus RecMic DR-2200** device is not displayed in the Omnissa Blast session under **Device Manager** > **Sound, video and game controllers**. Only the Omnissa virtual microphone or audio is displayed.
- **Olympus RecMic DR-2200** device cannot be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- While using the **Olympus Device Configuration Manager** application, all the HID buttons work.
- Audio can be recorded from a Omnissa Blast session and ThinOS local user interface.
- Audio playback works in both Omnissa Blast session and ThinOS local user interface.

NOTE: The audio behaviors are different from Citrix sessions since Omnissa Blast session does not support multiple audio devices.

Olympus RecMic DR-2200 redirection in a PCoIP session

Full USB redirection in a PCoIP session

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in **vUSB Force Redirect** section, and enter the device ID **0x07b40254**.
4. Click **Save & Publish**.

Connecting Olympus RecMic DR-2200 in a PCoIP session

Launch the PCoIP session and connect **Olympus RecMic DR-2200** into the thin client.

- **Olympus RecMic DR-2200** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Olympus RecMic DR-2200** device is displayed in the PCoIP session under **Device Manager** > **Sound, video and game controllers**.
- **Olympus RecMic DR-2200** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- While using the **Olympus Device Configuration Manager** application, all the HID buttons work. Audio and voice recording features work using **Olympus RecMic DR-2200**.

NOTE: PCoIP does not support USB interface splitting function. Hence, the feature to only redirect HID buttons is not supported in a PCoIP session.

Philips SpeechMike III

The following are the device information of **PHILIPS SpeechMike III**.

- Model—SpeechMike III
- Device ID—**Class 00, VID 0911, PID 0c1c**

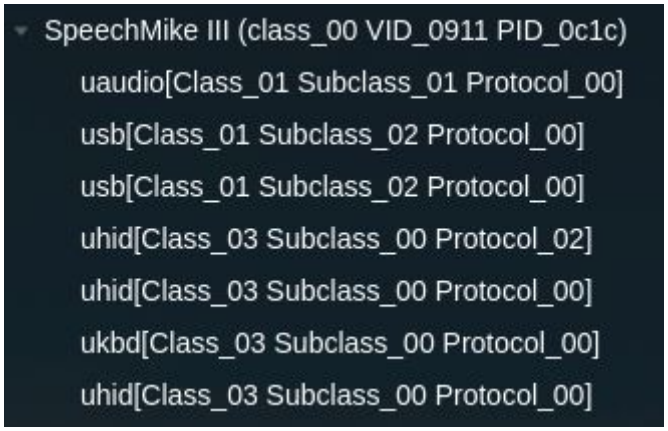

Figure 40. Device information

Philips SpeechMike III redirection in a Citrix session

Full USB redirection in a Citrix session

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID `0x09110c1c`.
4. Click **Save & Publish**.

Connecting Philips SpeechMike III in a Citrix session

Launch Citrix session and connect **Philips SpeechMike III** into the thin client.

- **Philips SpeechMike III** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Philips SpeechMike III** device is displayed in the Citrix session under **Device Manager** > **Sound, video and game controllers**.
- **Philips SpeechMike III** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- All the control buttons work in the **Philips Device Control Center** application.
- Audio playback and audio recording works with **Philips SpeechMike III**.

HID buttons redirection in a Citrix session

Only the HID buttons are redirected into the VDI session. Other parts such as Audio or Microphone are kept in the ThinOS local device.

Configuration in ThinOS for HID buttons redirection only

Steps

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

6. In the Section field, enter **`ClientAudio`**.
7. In the Key field, enter **`AudioRedirectionV4`**.
8. In the Value field, enter **`True`**.
9. Go to **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
10. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID **`0x09110c1c030000`**.
11. Click **Save & Publish**.

Connecting Philips SpeechMike III in a Citrix session with only HID buttons redirection

Launch Citrix session and connect **Philips SpeechMike III** into the thin client.

- **Philips SpeechMike III** device is displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Philips SpeechMike III** device is displayed in the Citrix session under **Device Manager** > **Sound, video and game controllers**.
- **Philips SpeechMike III** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- All the control buttons work in the **Philips Device Control Center** application.
- Audio playback and audio recording works with **Philips SpeechMike III** in both ThinOS and Citrix sessions.

NOTE: The **module.ini** setting in Citrix is for the Citrix multi audio feature. If you do not add this setting, **Philips SpeechMike III** does not get displayed in Citrix sessions. The recorder performance may not be clear on **Windows Voice Recorder** application when the audio and recording is not redirected. Dell Technologies recommends using other third-party voice recording applications.

Philips SpeechMike III redirection in an Omnissa Blast session

Full USB redirection in an Omnissa Blast session

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.
3. Enter **`vid-0911_pid-0c1c`** in the **Include Vid/Pid USB Device Redirection** field.
4. Click **Save & Publish**.

Connecting Philips SpeechMike III in an Omnissa Blast session

Launch the Omnissa Blast session and connect **Philips SpeechMike III** into the thin client.

- **Philips SpeechMike III** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Philips SpeechMike III** device is displayed in the Omnissa Blast session under **Device Manager** > **Sound, video and game controllers**.
- **Philips SpeechMike III** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- While using the **Philips Device Control Center** application, all the HID buttons work. Audio and voice recording features work using **Philips SpeechMike III**.

HID buttons redirection in an Omnissa Blast session

Only the HID buttons are redirected into the VDI session. Other parts such as Audio or Microphone are kept in the ThinOS local device.

Configuration in ThinOS for HID buttons redirection only

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, go to **Session Settings** > **Horizon Session Settings**.
3. Enter `vid-0911_pid-0c1c` in to the **Include Vid/Pid USB Device Redirection** field.
4. Enable **Allow Auto USB Device Splitting Redirection**.
5. Enter `vid-0911_pid-0c1c (exintf:00;exintf:01;exintf:02)` in to the **Spit Vid/Pid Device** field.
6. Click **Save & Publish**.

Connecting Philips SpeechMike III in an Omnissa Blast session

Launch the Omnissa Blast session and connect **Philips SpeechMike III** into the thin client.

- **Philips SpeechMike III** device is displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Philips SpeechMike III** device is not displayed in the Omnissa Blast session under **Device Manager** > **Sound, video and game controllers**. Only the Omnissa virtual microphone or audio is displayed.
- **Philips SpeechMike III** device cannot be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- While using the **Philips Device Control Center** application, all the HID buttons work.
- Audio can be recorded from an Omnissa Blast session and ThinOS local user interface.
- Audio playback works in both Omnissa Blast session and ThinOS local user interface.

NOTE: The audio behaviors are different from Citrix sessions since the Omnissa Blast session does not support multiple audio devices.

Philips SpeechMike III redirection in a PCoIP session

Full USB redirection in a PCoIP session

Connecting Philips SpeechMike III in a PCoIP session

Launch the PCoIP session and connect **Philips SpeechMike III** into the thin client.

- **Philips SpeechMike III** device is not displayed in the ThinOS local audio device list under **System Settings** > **Peripherals** > **Audio**.
- **Philips SpeechMike III** device is displayed in the PCoIP session under **Device Manager** > **Sound, video and game controllers**.
- **Philips SpeechMike III** device can be set as the default device from the **Playback** or **Recording** tabs under **Sound** in Windows.
- While using the **Philips Device Control Center** application, all the HID buttons work. Audio and voice recording features work using **Philips SpeechMike III**.

NOTE: PCoIP does not support USB interface splitting function. Hence, the feature to only redirect HID buttons is not supported in a PCoIP session. Due to Teradici PCoIP limitation, Dell Technologies does not recommend using audio redirection in ThinOS PCoIP session.

Configuration in ThinOS

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in **vUSB Force Redirect** section, and enter the device ID `0x09110c1c`.
4. Click **Save & Publish**.

Wacom One

The following are the device information of **Wacom One**.

- Model—**DTC133**
- Wacom One DTC133 has two modules:
  - Wacom One Monitor—using HDMI port

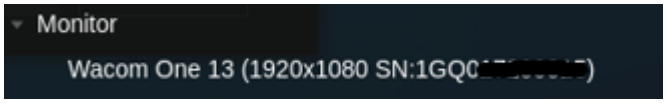

Figure 41. Monitor device information

  - Wacom One Pen Display—Using USB port

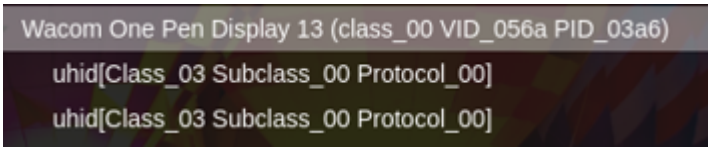

Figure 42. Pen Display device information

  - Class ID—**00, VID: 056a, PID: 03a6**

Configuration in ThinOS for USB redirection in an Omnissa Blast session

Prerequisites

Install Wacom Tablet software in your VDI session.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.
3. Enter `vid-056a_pid-03a6` in the Include **Vid/Pid USB Device Redirection** field.
4. Click **Save & Publish**.

Connecting Wacom One in a Blast session

Connect **Wacom One** into the thin client.

- After you launch a VDI session (Omnissa Blast or HDX), the **Wacom Desktop Center** recognizes your **Wacom One** device automatically. The mouse cursor moves according to the movement of your Pen on the **Wacom One** display.
- **Wacom Tablet Properties** is displayed after you click **Pen Settings** in **Wacom Desktop Center**. If the Wacom One Pen is not redirected to the VDI session, a warning message **No Wacom Device connected to your computer** is displayed.

NOTE: Wacom One Pen works only inside a VDI session. Wacom One Pen does not work in the ThinOS local user interface. Citrix session does not support **Wacom One**.

Topaz Signature Tablet

The following are the device information of **Topaz Signature Tablet**.

- Model—**TOPAZ Mode T-LBK462-B8B-R**
- Device ID— **Class 00, VID 0403, PID 6001**

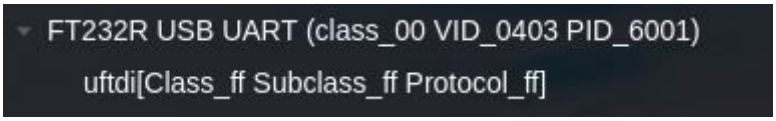

Figure 43. Device information

Configuration in ThinOS for USB redirection in a Citrix session

Prerequisites

- Do not enable Citrix policies **Client COM port redirection** and **Auto connect client COM ports** in Citrix Studio.
- Install Topaz tablet driver and application in the VDI session.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. Go to **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID `0x04036001`.
4. Click **Save & Publish**.

Configuration in ThinOS for USB redirection in an Omnissa Blast session

Prerequisites

Install the Topaz tablet driver and application in the VDI session.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.
3. Enter `vid-0403_pid-6001` in the Include **Vid/Pid USB Device Redirection** field.
4. Click **Save & Publish**.

Connect Topaz Signature Tablet in a VDI session

1. Connect **Topaz Signature Tablet** into the thin client.
2. Launch the VDI Session, go to Windows **Device Manager**. Under the **Ports (COM & LPT)**, make note of the Com port number from **USB Serial Port**.
3. Launch the **Topaz SigPlus Demonstration** application.
4. Go to **Properties** > **Tablet** and enter the **USB Serial Port COM** number in the **Com Port** field.
5. Click **Start**. You can now draw using the tablet.

Wacom Signature Tablet

The following are the details of the supported Wacom Signature Tablets.

- Wacom Signature Tablet STU-500B
  - Model—Wacom STU-500B
  - VID—0x056a pid:0x00a1
- Wacom Signature Tablet STU-520A
  - Model—Wacom STU-520A
  - VID—0x056a pid:0x00a3
- Wacom Signature Tablet STU-530
  - Model—Wacom STU-530
  - VID—0x056a pid:0x00a5
- Wacom Signature Tablet STU-430/G
  - Model—Wacom STU-430/G
  - VID—0x056a pid:0x00a4

USB connection

ThinOS 10.x supports Signature Tablets with USB connection. The device is redirected into the VDI session by USB redirection function.

Configuration in ThinOS for USB redirection in a Citrix session

Prerequisites

- Ensure that Citrix policies **Client COM port redirection** and **Auto connect client COM ports** are enabled in Citrix Studio.
- Install the required driver and application in the VDI session, depending on your Wacom Signature Tablet model.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. Go to **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in the **vUSB Force Redirect** section, and enter the device ID **`0x056a00a1`**.
4. Click **Save & Publish**.

Configuration in ThinOS for USB redirection in an Omnissa Blast session

Prerequisites

- Ensure that the **Serial Port Redirection** feature is installed in Omnissa Horizon Agent in a virtual machine. By default it is disabled.
- Install the required driver and application in the VDI session, depending on your Wacom Signature Tablet model.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the **Wyse Management Suite** policy settings.
2. On the **Advanced** tab, expand **Session Settings**, and click **Blast Session Settings**.
3. Enter **`vid-056a_pid-00a1`** in the Include **Vid/Pid USB Device Redirection** field.
4. Click **Save & Publish**.

Serial Port connection

ThinOS 10.x supports Serial Port connection by default. No additional configuration is required in ThinOS. Follow the configuration instruction for each protocol.

Connect Wacom Signature Tablet using Serial Port

1. Connect **Wacom Signature Tablet** into the thin client using the Serial Port.
2. Launch the VDI Session, and ensure that the **COM Port**used in session.
   - For Citrix session, the default used COM Port is COM1.
   - For Blast session, go to Windows Device Manager and see the **COM Port** number under **Ports (COM & LPT)**.
3. Open any Serial Port Connection tool in the VDI session.
4. Connect the used Serial Port with the speed **9600**.
5. Draw in the Wacom Signature tablet. You can see the Serial Port Connection tool for data prints.

Wacom Intuos Pro M tablet

ThinOS supports Wacom Intuos pen tablets that can be used for a wide range of activities such as drawing and sketching. You must use the Wyse Management Suite or Admin Policy Tool to configure the Wacom tablet mode. The tablet model that is tested on ThinOS is **Intous Pro M**.

NOTE: Wacom Tablet does not work in a Horizon PCoIP session.

For information about limitations, see the *Release Notes* of your ThinOS version at Support | Dell.

Enable Wacom tablet using the session menu

Steps

1. On the ThinOS client, launch a PCoIP session.
2. In the system tray, click the PCoIP icon to view the active PCoIP sessions.
3. Select a session from the menu.
4. Click **Tablet Monitor** and select one or more displays. The selected display is mapped to the tablet.

Table 33. Tablet Monitor settings

User scenario	ThinOS settings	Recommended PCoIP session settings
Map all displays to the tablet.	Click the PCoIP icon, and then click **PCoIP session** > **Table Monitor** > **Full**.	a. In a PCoIP session, open the Wacom tablet properties window. b. Click the **Mapping** tab. c. From the **Screen Area** drop-down list, select **Full**.
Map a specified display to the tablet.	Click the PCoIP icon, and then click **PCoIP session** > **Table Monitor** > **Monitor (x)**.	a. In a PCoIP session, open the Wacom tablet properties window. b. Click the Mapping tab. c. From the **Screen Area** drop-down list, select your preferred display.

5. Click **Tablet Orientation Left-Handed** to set the orientation of the tablet for left-handed use. If enabled, a tick mark is displayed next to the option. The orientation setting applies to all tools and applications. You must rotate your tablet either to the left or to the right based on your selected orientation.

Table 34. Tablet Orientation settings

User scenario	ThinOS settings	Recommended PCoIP session settings
Right-handed tablet orientation.	• Click the PCoIP icon and select the PCoIP session. • Clear the **Tablet Orientation Left-Handed** selection.	a. In a PCoIP session, open the Wacom tablet properties window. b. Click the **Mapping** tab. c. From the **Orientation** drop-down list, select **ExpressKeys Left**.
Left-handed tablet orientation.	• Click the PCoIP icon and select the PCoIP session. • Select the **Tablet Orientation Left-Handed** option.	a. In a PCoIP session, open the Wacom tablet properties window. b. Click the Mapping tab. c. From the **Orientation** drop-down list, select **ExpressKeys Right**.

Next steps

Configure the Wacom tablet mode using Admin Policy Tool or Wyse Management Suite. See, Configure the Wacom tablet mode.

Configure the Wacom tablet mode

Prerequisites

Ensure that you have enabled the Wacom tablet feature in the session menu. See, Enable Wacom tablet using the session menu.

Steps

1. From the **Wacom Tablet Configurations** drop-down list, select either of the following modes:

- **Locally terminated**—Enables the peripheral data to be processed locally at the thin client. Locally terminated tablets have greatly improved responsiveness, and tolerate a network with 25 milliseconds and higher latency.
- **Bridged**—Enables the peripheral data to be sent to the desktop for processing. Bridged Wacom tablets are supported only in low-latency environments. Reduced responsiveness is observed in network environments with greater than 25-millisecond latency.

2. Click **Save & Publish**.

Next steps

1. Connect the tablet to the thin client.
2. Open the Wacom Desktop Center application in the session.
3. Verify the tablet connection.

Configure Wacom Intuos S pen for USB redirection

In ThinOS 10.x 2502 and Citrix Workspace App 2411, the Wacom Intuos S pen can map or redirect in HDX sessions. The device information of the Wacom Intuos S pen is Class ID—**VID: 056a, PID: 0374** by Dell Technologies qualified.

Prerequisites

Install Wacom Tablet software in your VDI session.

Steps

To configure USB redirection on ThinOS, do the following:

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

Steps

To configure mapping on ThinOS, do the following:

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

CV3 and CV3+ support (NFC contactless smartcard reader, fingerprint, and contact smartcard reader)

ThinOS 10.x 2505 supports CV3 and CV3+ that allows the users to register and log in to VDI brokers (Citrix virtual apps and desktops, Omnissa Horizon, or Microsoft RDS) using Imprivata SignOn Server.

CV3 supported platforms contain:

- Palm-rest contact smart card reader
- Palm-rest fingerprint reader

CV3+ supported platforms contain:

- Palm rest contact smart card reader
- Palm-rest fingerprint reader
- Palm-rest NFC contactless smart card reader (supports only PIV enabled smartcard)

Configuring Multi Broker

Broker Logon Settings

From ThinOS 10.x 2502, a configuring **Multi Broker** option is available. Multi Broker option allows you to use **Same Broker Type Failover**, **Stop Logon if Error**, **Multi Logon**, **Sequential Domain**, and other multi broker features while signing in.

Default Broker Type

You can configure **Multi Broker** option from the **Default Broker Type** field in the **Global Broker Settings > Broker Settings**.

Multi Broker Types

You can set the logging in sequence for the Broker agent type. You must use semicolon to separate different Broker agent types including **Citrix, Omnissa, RDS, Other, and Amazon**. The default value of this policy is **Citrix; Omnissa**. The value of this parameter is not case-sensitive.

Same Broker Type Failover

This policy enables failover sign-on when connecting to one Broker agent type. When the policy is enabled, only the first valid Broker agent of the same protocol logs in. If the policy is disabled, all valid Broker agents of the same protocol can log in.

Stop Logon if Error

The policy **Stop Logon if Error** is displayed only when **Multi Logon** policy is disabled. You can enable this policy to stop the logging in process, and raise an error when login has failed when using a Broker agent. The policy is disabled by default.

Multi Logon

The policy **Multi Logon** allows you to enter multiple credentials if the multiple Broker agent types are specified. By disabling this policy, you can log in to the specified Broker agent type with only one credential. The policy is enabled by default.

NOTE: When the **Multi Logon** policy is enabled, a different Broker agent logon page is displayed on the login screen while entering credentials. When logging in using **Multi Farm** policy with **Multi Logon** disabled, the general ThinOS login window is displayed.

NOTE: When the ThinOS client is locked with multiple Broker agents, you can use any password of the different Broker agents to unlock the client.

Sequential Domain

The policy **Sequential Domain** is displayed only when **Multi Logon** policy is enabled. You can enable this policy to authenticate all domains configured in **Login Settings** > **Domain List**. The policy is disabled by default.

Configuring Azure Virtual Desktop

Azure Virtual Desktop (AVD) is a comprehensive desktop and app virtualization service that runs on the cloud. You can access the virtual desktop resources that are created on the Azure cloud from the ThinOS client. AVD session supports Imprivata virtual channel in ThinOS 10.x 2502. When a user logs in to an AVD session using Imprivata PIW or Imprivata PIE, the user could enroll a proximity card and fingerprint through Imprivata agent in the AVD session. Users can also log in Imprivata agent by tapping proximity card or using the fingerprint.

Prerequisites

Ensure that you have an Azure Active Directory that is configured and Azure Virtual Desktop resources are deployed on the Azure cloud.

About this task

This section describes how to configure the Azure Virtual Desktop broker setup on your thin client.

Steps

1. From the desktop menu, click **System Setup** > **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. On the **Broker Setup** tab, select **Azure Virtual Desktop** from the **Select Broker Type** drop-down list, and do the following:
   a. Select the **Enable Azure Virtual Desktop** check box to configure the Azure Virtual Desktop settings.
   b. Select the **Azure Common (ARMv2)** check box if you want to connect to a Workspace using the Azure Resource Manager (ARM) based URL. Specify the following details:
      - Client ID
      - Redirect URL
      - Resource URL
      - Feed URL
   c. Select the **Azure Classic (MS-Prod)** check box if you want to connect to a Workspace using the non-Azure Resource Manager (ARM)-based URL. Specify the following details:
      - Client ID
      - Redirect URL
      - Resource URL
      - Feed URL
3. In the **Remote Connections** dialog box, click the **General Options** tab, and specify the Azure cloud user credentials.

   NOTE: From ThinOS 2208, you can set the default credentials to log in automatically to the Azure Virtual Desktop broker when you start the client.

4. Click **Save** to save your changes.
5. Restart the thin client.
6. In the login window, click **Enter**.
7. Enter the Azure cloud user password.
8. Click **Sign in**.
   The desktops and applications on the Azure cloud are displayed.

   NOTE: You can enter the name of the connection that is displayed in **Connection Manager** to automatically connect after you log in the Azure Virtual Desktop broker. You can enter more than one connection name and each name is separated by semicolon. The connection names are case-sensitive.

Enable printer in Azure Virtual Desktop

ThinOS supports printer in Microsoft Azure Virtual Desktop. RDP session supports LPT, LPD, and SMB printers.

Steps

1. Connect the printer to the client.

2. From the desktop menu, click **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
3. Enter the name of the printer in the **Printer Name** field.
4. Select the **Enable the printer device** check box.
5. Click **Save**.
6. Launch the RDP session. See, Configuring Microsoft Remote Desktop Services.

   NOTE: RDP protocol supports standard printers.

Log in to Azure Virtual Desktop using Active Directory Federation Services

Prerequisites

You can now use your Active Directory Federation Services (ADFS) server login to join the on-premises Active Directory with the Azure Active Directory.

- Ensure that you have created a Microsoft Entra ID.
- Ensure that you have a public domain name.
- Ensure that you have created the on-premises Active Directory.
- Ensure that you have ADFS and Azure AD Connect tools.

Steps

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, select **Azure Virtual Desktop** from the **Select Broker Type** drop-down list.
3. Select the **Enable Azure Virtual Desktop** checkbox.
4. Click **Save** and restart the thin client.
5. Enter the username of the on-premises Active Directory, and click **Next** on the **Azure Virtual Desktop** login window.
6. Enter the credentials of the on-premises Active Directory, and click **OK** on the **ADFS** window.
7. Launch the Azure Virtual Desktop session.

Use camera redirection in an RDP session

Camera Redirection enables the video from the camera to be rendered on the endpoint device instead of running on the server side.

Prerequisites

RDP Broker agent connection must be configured on the ThinOS device.

Steps

1. Connect a camera to your thin client.
2. Log in to the ThinOS desktop.
3. Launch the RDP session.
   The camera is redirected automatically.

Configuring Microsoft Remote Desktop Services

Microsoft Remote Desktop application allows you to access and manage the data and resources of a remote device using an Internet connection. ThinOS supports RC4_HMAC_MD5 for RDP connections to compliment with AES128_HMAC_SHA1 or AES256_HMAC_SHA1.

About this task

This section describes how to configure the Microsoft Remote Desktop Services on your thin client.

Steps

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. In the **Broker Setup** tab, select **Microsoft Remote Desktop Service** from the **Select Broker Type** drop-down list, and do the following:
   - **Broker Server**—Enter the IP address, hostname, or FQDN of the Broker Server.
   - **Auto Connect List**—Enter the name of the desktops that you want to launch automatically after logging in to the respective broker. More than one desktop can be entered. Each desktop name is separated by semi-colon, and is case-sensitive.
3. Click **Save** to save your settings.

Enable Terminal Services Gateway

Terminal Services Gateway (TS Gateway) provides a secure access to a remote desktop. In a TS Gateway II or III connection, the setup uses a two half-duplex communication between the Terminal Server (TS) Gateway server and the thin client. In the WebSocket connection, the session connection setup uses a duplex communication between TS Gateway and thin client. TS Gateway II and TS Gateway III are downward compatible with Windows Server 2016, that means, if the WebSocket connection fails or the TS Gateway server or thin client version does not support WebSocket, then TS Gateway II or TS Gateway III is used.

Steps

1. Log in to Wyse Management Suite or open the Admin Policy Tool on ThinOS.
2. In the **Advanced** tab, expand **Session Settings**, and click **RDP and AVD Session Settings**.
3. Click the **Enable Remote Desktop Services Gateway** toggle switch to enable TS Gateway for your connection.
4. Click **Save & Publish**.
5. Log in to the RDS or AVD Broker agent.
6. Launch the RDS or AVD session.
   TS Gateway connection is established.

Table 35. Supported TS Gateway versions

Server operating system	TS Gateway II	TS Gateway III	WebSocket
Windows Server 2008 R2	Support	Not support	Not Support
Windows Server 2012 R2	Support	Support	Not Support
Windows Server 2016	Support	Support	Support

Configure the Remote Desktop Services collection

ThinOS enables you to access the Remote Desktop Services session collection that is configured on the RDS Broker agent. RDSH collection enables you to group all the desktops and applications that you want to publish.

Steps

1. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.

2. In the **Advanced** tab, expand **Broker Settings**, and click **Microsoft Remote Desktop Settings**.
3. In the **RDSH collections** field, specify the collections that are configured on the RDS Broker agent. Only the applications and desktops within the specified collections are displayed. If the field is empty, all the applications and desktops are displayed.
4. Click **Save & Publish**.

Add a Remote Desktop Protocol connection

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **RDP and AVD Session Settings**.
3. Click **Add Row** in the **RDP Direct connection collection** section.
4. Specify the Remote Desktop Protocol connection details.

   You can automatically connect to a Remote Desktop Protocol connection on system startup by enabling the **Auto Connect** button. Alternatively, you can go to **Add Connection** > **Add RDP Connection** > **Connection** from the VDI menu, and select the **Auto-connect on start-up** check box to connect RDP automatically on system startup.

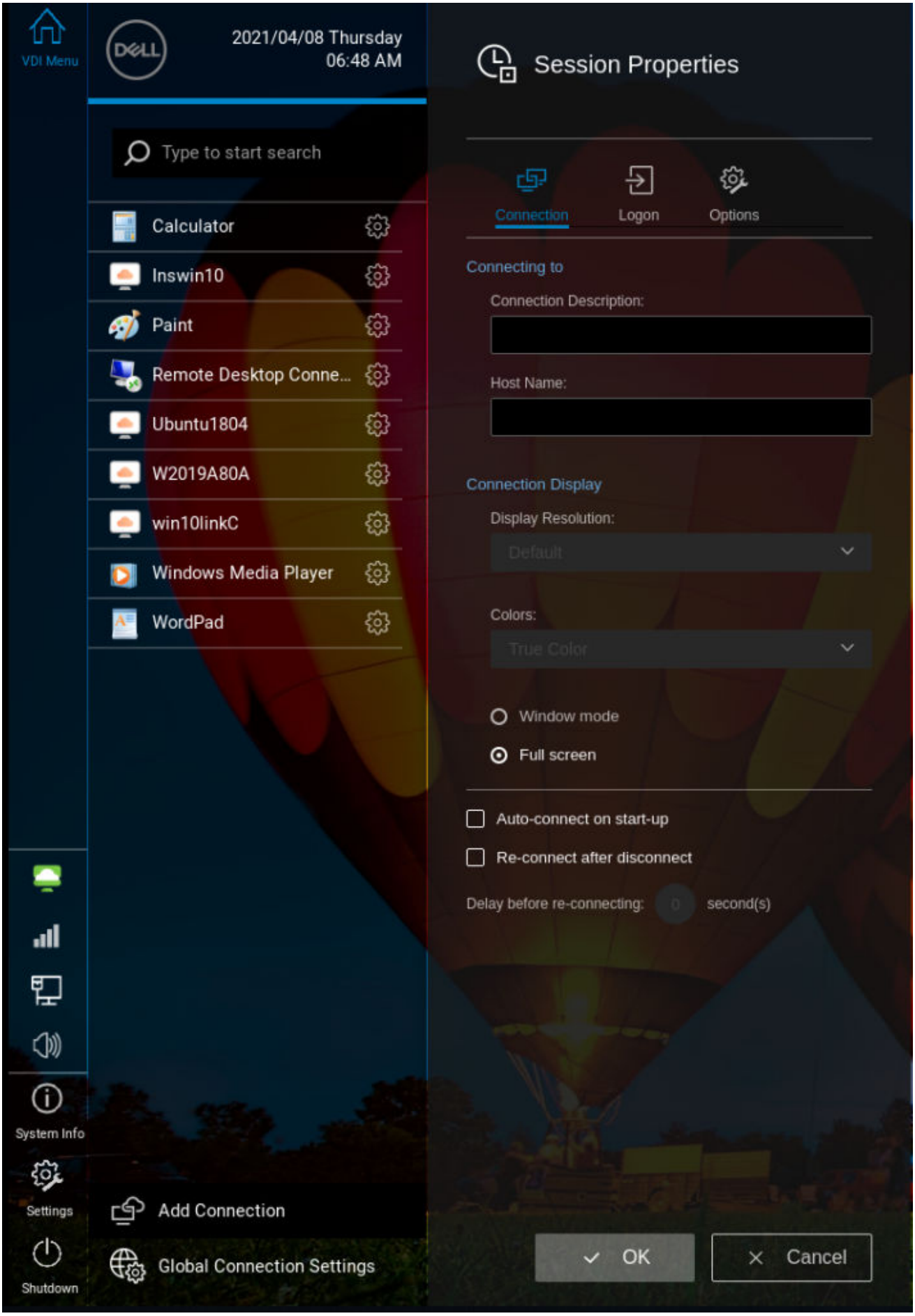

Figure 44. Auto-connect on start-up

NOTE: For the auto connect feature to function, the **Save local connections** option in **Advanced** > **Session Settings** > **Global Session Settings** must be enabled.

5. Click **Save & Publish**.

Log in to RDP session using Remote Desktop Gateway

Steps

1. Go to **Add Connection** > **Add RDP connection** > **Logon** from the VDI menu.

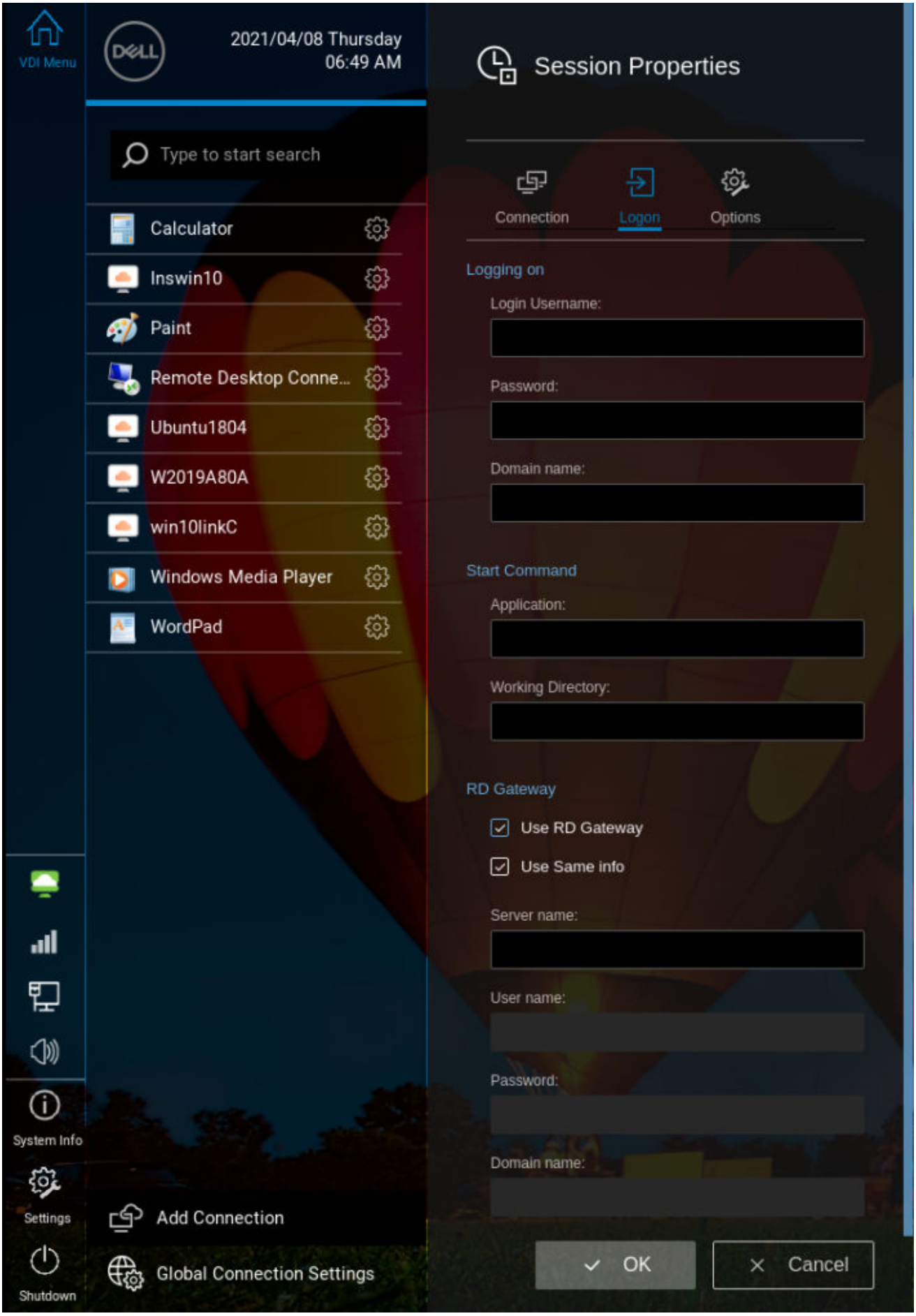

Figure 45. Use RD Gateway

2. Select the **Use RD Gateway** check box.
3. Specify the credentials for Remote Desktop Gateway or select the **Use Same info** check box.
4. Click **OK** to save the settings.

Log in to RDP session using Remote Desktop Gateway from Wyse Management Suite or Admin Policy Tool

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Session Settings**, and click **RDP and AVD Settings**.
4. Click **Add Row** under **Direct RDP Settings**.

   To select a monitor to display the RDP session in full screen, enable **Fullscreen** and **Enable On Screen** options, and select the monitor number in **OnScreen** list. When you launch the RDP session, the session is displayed in full screen in the selected monitor. If the selected monitor number is not present in the ThinOS Display window list, the RDP session is displayed in full screen in the last monitor.
5. Select the **Use RD Gateway** check box.
6. Specify the credentials for Remote Desktop Gateway or select the **Use Same info** check box.
7. Click **Save & Publish**.

Change the display mode for RDP connection using shortcut keys

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Session Settings**, and click **RDP and AVD Session Settings**.
4. Enable or disable **RDP Shortcut Key**.

   By default the option is disabled. When enabled, you can use the shortcut keys to change the display mode after the RDP connection is launched successfully. **Ctrl** + **Shift** + **up** changes the display mode from window mode to fullscreen. **Ctrl** + **Shift** + **Down** changes the display mode from fullscreen to window mode.
5. Click **Save & Publish**.

Enable ThinOS to check the server certificate common name

ThinOS-based clients check the common name of the server certificate when setting up an SSL connection in full security mode. Use Wyse Management Suite or Admin Policy Tool on ThinOS to enable or disable the TLS checker.

Steps

1. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. In the **Advanced** tab, expand **Privacy & Security**, and click **Security Policy**.
3. Click the **TLS Check CN** toggle switch to enable the option.

   Enabling the option allows ThinOS client to check the common name of the server certificate when setting up an SSL connection in full security mode. This option is ineffective to SSL connections for Omnissa View and VPN. The server certificate common name is verified all the time when setting up SSL connections for Omnissa View and VPN.

   NOTE: Use NetBIOS or FQDN values to define an SSL (HTTPS) connection when enabling the TLSCheckCN option. Enabling the TLSCheckCN option results in SSL connection failure when an IP address is defined.
4. Click **Save & Publish**.

Allow Legacy Renegotiation

Unpatched legacy servers require renegotiation. Use Wyse Management Suite or Admin Policy Tool on ThinOS to allow or disallow legacy renegotiation.

Steps

1. Open the Admin Policy Tool in ThinOS or go to the ThinOS 10.x policy settings in Wyse Management Suite.
2. In the **Advanced** tab, expand **Privacy & Security**.
3. Click **Security Policy**.
4. Enable or disable **Allow Legacy Renegotiation** .
5. Click **Save & Publish**.

Select Group

The following are two common scenarios for you to implement **Select Group**:

Scenario 1

You can choose between different brokers that are based on the physical location you are at. For example, when there is an internal and an external Citrix or Omnissa connection point for your organization. With **Select Group**, you can select an internally hosted broker when you are in the office or an externally hosted broker when you are working from home. This can be complemented with normal username or password-based authentication for the internal environment and two-factor authentication for the external environment.

Scenario 2

In call centers, you have to connect to different customer environments based on the shift. **Select Group** helps you to quickly change the broker URL, domain name, and branding (desktop wallpaper) to make it visually clear to which environment you are connecting to.

When moving clients between groups or adding new clients to a group, the following behaviors are expected:

- All ThinOS configuration policy settings and imported client files return to their default values except:
  - **Network Settings**—All wired and wireless network configurations including proxy and VPN settings are preserved.
  - **Certificates**—All client certificates associated to 802.1x network configuration are preserved.
  - **Management**—Wyse Management Suite configurations are preserved.
- If the new group has enabled local override for the settings, all local override settings are preserved.
- All imported files except for those associated with networking or management are deleted. Some examples of these files include Wallpaper, Logo, EULA, and Hosts. If 802.1x wired or wireless, proxy, or VPN connection certificates have been used, the certificate file is preserved.

Configure the Select Group feature to log in to different brokers

Steps

1. Log in to the Wyse Management Suite server.
2. On the **Groups & Configs** page, click the **`Default Device Policy Group`** option.
3. Click +.
4. In the **Add New Group** dialog box, enter the **Group Name** and **Description**.
5. Select the **This is a ThinOS Select group parent** option.
6. Select the group, add some child groups, and set the **Group Token**.
   You can edit the policy in each child group,
7. Set a different Broker agent server in each child group.
8. On the ThinOS client, go to **System Setup** > **Central Configuration**.
9. Check in to any child group token, and reboot the thin client.
10. After the thin client restarts, you can select the child group from the login window.

VDI Configuration Editor

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

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

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

Citrix Configuration Editor

Citrix VDI settings

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

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

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

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

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

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

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

Table 36. Enable or disable UC plug-in settings

UC Plug-ins	Enable UC Plug-in using VDI settings	Disable UC Plug-in using VDI settings	Details
Zoom Citrix	• File: module.ini • Operation: Add or Update • Section: ICA 3.0 • Key: ZoomMedia • Value: On • These settings enable the Zoom optimization with ZoomMedia=On in module.ini. These are the default settings after you install the UC package.	• File: module.ini • Operation: Add or Update • Section: ICA 3.0 • Key: ZoomMedia • Value: Off • These settings disable the Zoom optimization with ZoomMedia=Off in module.ini.	• Change the values On/Off in module.ini to enable or disable the UC plug-in. • Plug-in switch string is in the section [ICA 3.0]. .
Cisco Webex VDI	• File: module.ini • Operation: Add or Update • Section: ICA 3.0	• File: module.ini • Operation: Add or Update • Section: ICA 3.0	• Change the values On/Off in module.ini to enable or disable the UC plug-in.

Table 36. Enable or disable UC plug-in settings (continued)

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

Horizon Blast Configuration Editor

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

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

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

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

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

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

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

Zoom Plugin Configuration Editor

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

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

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

Important notes

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

Table 37. ThinOS settings - Not allowed to be modified

VDI/UC	Configuration files	Deny list
Citrix Workspace app	/opt/Citrix/ICAClient/usb.conf	All
	/opt/Citrix/ICAClient/config/All_Regions.ini	• [Virtual Channels\Serial Port\Device] • LastComPortNum=8 • ComPort1= • ComPort2= • ComPort3= • ComPort4= • ComPort5= • ComPort6= • ComPort7= • ComPort8=

Table 37. ThinOS settings - Not allowed to be modified (continued)

VDI/UC	Configuration files	Deny list
	/opt/Citrix/ICAClient/config/module.ini	• [ICA 3.0] • KeyboardSync=
	~/.ICAClient/wfclient.ini	• [WFClient] • Version= • KeyboardLayout= • KeyboardMappingFile= • KeyboardDescription= • KeyboardType= • CDMAllowed= • DrivePath* • DriveEnabled* • DriveReadAccess* • DriveWriteAccess* • CursorStipple= • TransportReconnectEnabled= • ClientPrinterList= • SFRAllowed • EnableUDPAudio • HDXWebCamWidth • HDXWebCamHeight • HDXWebCamFramesPerSec

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

	~/.ICAClient/appsrv.ini	• [WFClient] • COMAllowed=
Omnissa Horizon	~/.vmware/config	• viewusb.AllowAutoDeviceSplitting= • viewusb.SplitExcludeVidPid= • viewusb.SplitVidPid= • viewusb.ExcludeVidPid= • viewusb.IncludeVidPid= • viewusb.IncludeFamily= • viewusb.ExcludeFamily= • mks.enableFIPSMode= • usb.enableFIPSMode= • viewusb.ExcludeAllDevices=
Zoom Citrix	~/.ICAClient/config/ZoomMedia.ini	• [PROXY] • proxyType= • httpProxyHost= • httpProxyPort= • httpsProxyHost= • httpsProxyPort=
Zoom Horizon	~/.vmware/ZoomMediaVmware.ini	• [PROXY] • proxyType= • httpProxyHost= • httpProxyPort= • httpsProxyHost= • httpsProxyPort=

Table 37. ThinOS settings - Not allowed to be modified (continued)

VDI/UC	Configuration files	Deny list
Key Common Rule	N/A	• Cmd, Command, Drive, Path • special characters, such as: ~`!@#$%^&*()+=;:"'<>,?/ • This rule is applied to Citrix INI Settings, Citrix XML Settings, Citrix JSON Settings, Horizon Blast Key-Value Settings, Zoom INI Settings Key fields, and keyboardID field in Citrix Keyboard Layout. Cmd, Command, Drive, and Path are partially matched. They cannot be contained in any inputs. 'proxyTypeTT' not in the deny list, but 'Cmd', 'Cmd1', 'Cmd2' are in the deny list. Special characters are not applied to Citrix INI Settings and Zoom INI Settings key fields.
Value field constriction	N/A	• Unicode • '..', '/' • %2e%2e%2f— Unicode like input, such as '\u0001', '\uff01' %2e%2e%2f is URL encoding output, denote '../'
Case Insensitive	N/A	Only applied to Citrix INI Settings, Citrix XML Settings, Citrix JSON Settings, Horizon Blast Key-Value Settings, Zoom INI Settings Key fields, and keyboardID field in Citrix Keyboard Layout.

NOTE: Enabling or disabling the UC plug-in settings in **VDI Configuration Editor** > **Citrix Configuration Editor** is deprecated from ThinOS 2211.

Launching broker sessions from the browser using the local VDI client

From ThinOS 10.x 2511, you can launch Omnissa Workspace ONE, Citrix Storefront, and AVD sessions from the browser using the local VDI client.

Prerequisites

Before configuring, ensure that the following prerequisites are met:

- You have active login credentials for WMS.
- A supported web browser package must be installed on the thin client.
- Enable the **Show Login Icon on Floatbar/Taskbar** from **WMS** → **User Experience Settings** → **Personalization**.

About this task

After completing the configuration, ThinOS displays the shortcut on the Home Screen, Floatbar, or Taskbar. Verify its behavior before login and confirm it launches correctly after login.

Steps

1. To launch Omnissa Workspace ONE, Citrix Storefront, and AVD sessions from the browser using the local VDI client , do any of the following:
   - Log in to WMS as an administrator and select **Groups & Configs** > **<Select a group>** > **Edit Policies** > **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Browser Settings** > **Browser Shortcuts**.
3. Configure the following:
   a. Launch Citrix.
   b. Enter the Citrix or Omnissa URL.
   c. Enter the Browser name. For example: Chrome and Firefox.
   d. Enable **Browser Access Without Login toggles**.
4. Click **Save & Publish**.

Configure the VDI settings

Prerequisites

Ensure that you have read the Citrix, Omnissa, or Zoom official documentation for relevant VDI configurations.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on **Wyse Management Suite**.
2. On the **Advanced** tab, expand **VDI Configuration Editor**, and click any of the following options based on your requirement:
   - **Citrix Configuration Editor**
   - **Horizon Blast Configuration Editor**
   - **Zoom Plugin Configuration Editor**

   If you configure the VDI settings using only **Wyse Management Suite** policy settings, the configured settings are not preserved when you change the **Wyse Management Suite** group. Settings are restored to the Citrix Workspace app default values if VDI settings are not configured in the new **Wyse Management Suite** group. If VDI settings are configured in the new **Wyse Management Suite** group, the settings are synced with the new values.
3. Click the **Add Row** option under any of the following sections based on your requirement:
   - Citrix INI settings
   - Citrix XML settings
   - Citrix JSON settings
   - Citrix keyboard layout settings
   - Omnissa key-value settings
   - Zoom INI settings
4. From the **File** drop-down list, select the VDI configuration file.
5. From the **Operation** drop-down list, select the operation to perform—Add, Update, or Delete.
6. In the **Section** field, enter the string.
7. In the **Key** field, enter the key parameter.
8. In the **Value** field, enter the key value.
9. To add multiple settings, repeat step 3.

   If the VDI settings that are configured in any of the sections under **VDI Configuration Editor** in the **Admin Policy Tool** are different from the VDI settings that are configured using the **Wyse Management Suite** policy settings, the settings that are configured from **Admin Policy Tool** persist when you change the **Wyse Management Suite** group. The VDI settings in **Admin Policy Tool** can be erased when you recheckin to **Wyse Management Suite** group. For example, if there are VDI settings configured in **Zoom Plugin Configuration Editor** under **VDI Configuration Editor** in the **Admin Policy Tool** but the **Zoom Plugin Configuration Editor** in the **Wyse Management Suite** policy settings does not have any VDI settings configured, the settings configured from **Admin Policy Tool** persists.

   NOTE: Click to remove the corresponding VDI settings and restore the values to the Citrix Workspace app default values. Click to reset all the VDI settings and restore the values to the Citrix Workspace app default values.
10. Click **Save & Publish**.

Authenticate the domain controller (NTLM) with None Broker agent

Steps

1. Add a device policy group on Wyse Management Suite and go to the ThinOS 10.x policy settings.
2. Click the **Advanced** tab.
3. Expand **Login Experience** and click **Login Settings**.
4. From the **Login Type** drop-down, select **Authentication to Domain Controller**.
5. Enter the AD Group Prefix.
6. Click **Save & Publish**.

7. Add a user policy group under **Group & Configs**.
8. Ensure that the AD Attribute Name is the same as the AD Group Prefix that is set in the device group.
9. Select the device group from the device group-mapping list.

Next steps

If you set the Broker agent connection as None, a login window is displayed after you restart the system. Only users in the Active Directory group that are set in Wyse Management Suite can log in to the device. Any policy that is configured in the user policy group is applied to ThinOS.

If you set the None Broker agent without Authentication to the domain controller, the login window is not displayed after the system reboot. Users are automatically logged in to the ThinOS device as Anonymous users.

8

Unified Communications optimization with ThinOS

Unified Communications and Collaboration solution allows real-time video conferencing, instant messaging, and team collaboration that enables you to work together more effectively.

ThinOS supports the following Unified Communications optimization in a VDI environment:

- Cisco Jabber
- Cisco Webex Teams
- Cisco Webex Meetings
- Microsoft Teams
- Zoom
- RingCentral

NOTE: When using Citrix Unified Communications on ThinOS, do not use the fallback mode, which is the legacy HDX redirection for webcam and audio. Using the fallback mode consumes more remote desktop resources such as CPU, GPU, RAM, and Network.

NOTE: Tested scenario-Audio and video calling or meeting with three to five users using Citrix Unified Communications on ThinOS.

Unified Communications limitation on Wyse 5470 Thin Clients

- The integrated speaker on the Wyse 5470 Thin Client produces an echo when on calls. This issue is observed on all Unified Communication packages, and it is recommended you use a USB headset to make calls.

Cisco Jabber Softphone for VDI

Cisco Jabber Softphone for VDI (JVDI) is the Unified Communications solution that is offered by Cisco for virtual deployments. It supports audio conferencing, and instant messaging on the Hosted Virtual Desktops (HVD). The Cisco Jabber Softphone for VDI software offloads the audio processing from the virtual desktop servers to the thin client. All audio and video signals are routed directly between the endpoints without entering the HVD.

Cisco Jabber Softphone for VDI enables you to make and receive calls using the Cisco Unified Communications application. Cisco Jabber Softphone for VDI consists of the following two components:

- Cisco JVDI Agent
- Cisco JVDI Client

Cisco JVDI Agent is the JVDI connector that runs on the VDI desktop or server. Cisco JVDI client is the JVDI package that runs on the thin client. The Jabber client that runs on the Citrix server handles the authentication and the media processing is achieved on the thin client.

Table 38. Supported environment

Component	Supported platforms
Thin client	• Latitude 3420 • OptiPlex 5400 All-in-one • Latitude 3420 • OptiPlex 5400 All-in-One • Latitude 5450 • Latitude 5440 • Latitude 3440 • OptiPlex AIO 7410 • OptiPlex AIO 7420

Table 38. Supported environment (continued)

Component	Supported platforms
Connection broker for the hosted virtual desktops	• Citrix Virtual Apps and Desktops • Omnissa Horizon published desktop
Cisco Jabber application on the hosted virtual desktop	See the Release Notes for the supported version.
Cisco JVDI agent on the hosted virtual desktop	See the Release Notes for the supported version.
Cisco JVDI client on the thin client	See the Release Notes for the supported Cisco Jabber package.

Install the JVDI package on ThinOS

You must install the Cisco Jabber package to use Cisco Jabber Softphone for VDI. To install the Cisco Jabber package using Wyse Management Suite, see Upload and push ThinOS 10.x application packages.

Setting up the Cisco Jabber Softphone for VDI

About this task

This section describes how to install and use the Cisco Jabber Softphone for VDI on a Citrix or Omnissa desktop.

Steps

1. Go to the Cisco website, and download the following software:
   - Cisco JVDI Agent
   - Cisco Jabber application
2. On the virtual desktop, install Cisco JVDI Agent. Double-click the file and follow the installation wizard steps.
3. On the virtual desktop, install Cisco Jabber.
   For information about the installation procedure, see the installation guide at Cisco.
4. Update the ThinOS firmware, and install the JVDI package on the ThinOS client using Wyse Management Suite.

   NOTE: If ThinOS running Cisco Jabber (JVDI) fails to register with Cisco Unified Communications Manager, add the DNS servers and DNS domains that are used by the Citrix host and the Cisco Unified Communications Manager servers to ThinOS. You can specify the domain name and server IP on the **General** tab in **Network Setup**. Or, you can add the DNS server and domain value to the DHCP server by providing the IP address information to the ThinOS client. For issues related to Cisco Unified Communications, contact Cisco support.

5. Log in to the Citrix virtual desktop, and sign in to Cisco Jabber using your user credentials.
   When you log in for the first time, do the following:
   a. On the Cisco Jabber interface, click **Advanced Settings**.
   b. Select your account type as **Cisco Communications Manager 9 or later**.
   c. Enter the login server address.

   NOTE: If the **Use my computer for calls** option is selected, the Cisco Jabber is automatically registered with Cisco Unified Communications Manager. This option enables Jabber to work as a Softphone, and use the microphone or speaker that is connected to the thin client for phone calls.

Using Cisco Jabber

Use the Cisco Jabber application to perform the following tasks:

- Start an audio call.
- Answer the call.
- Hold or resume the call.
- Stop the video.

- Mute or unmute the audio.
- Turn on or turn off the self-view.
- Enter or exit the full screen.
- Merge the calls.
- Audio conferencing.
- Transfer the call.
- Play voice mail.
- Forward the call to voicemail.
- Forward the call to another number.
- Forward voice messages directly.
- Use the Device Selector menu to switch between headsets.
- Use the Device Selector menu to switch between cameras.
- Set up secure phone capabilities.
- Answer the call on multiple phone devices (Shared Line feature).

For information about troubleshooting your Cisco Jabber, see the Deployment and Installation Guide for Cisco Jabber Softphone for VDI.

Using Device Selector

About this task

Cisco Jabber Softphone for VDI consists of a component called **Device Selector**. Use the **Device Selector** menu to manage your audio devices and cameras.

If you have multiple devices connected to the thin client, you can view your active device, or select a different device. To enable a device, do the following:

Steps

1. In the Windows notification area, click the **Device Selector** icon.
   The available devices are listed.
2. Click a device to make it active.

Verify the Cisco Jabber connection status

About this task

This section describes how to verify the Cisco Jabber connection status on your thin client.

Steps

1. Install the correct connector on the remote desktop.
2. Install the correct package on the ThinOS device.
3. Connect any audio or video devices.
4. Connect to a VDI desktop, and start the Cisco Jabber application.
5. Open the **Settings** menu, and go to **Help** > **Show connection status**.
   The Connection Status window is displayed.
6. Click **JVDI Details**, and confirm the following attributes:
   - JVDI Client version
   - JVDI Agent version
   - Virtual Channel status
   - SIP status
   - Softphone CTI status
7. Establish a video or an audio call.
8. Answer the call by either clicking the mouse or using the headset button.
9. Verify the call statistics.

For more information about verifying your installation and collecting the troubleshooting information, see the **Cisco documentation** at the Cisco website.

Cisco Webex Teams for VDI

Cisco Webex Teams Virtual desktop application is the Unified Communications product from Cisco for messaging and team collaboration in a VDI environment. It supports calling and messaging functionality on the hosted virtual desktops. Cisco Webex Teams offloads media processing from the virtual desktop server to the thin client. All audio and video signals are routed directly between the endpoints without going through the hosted desktop.

Cisco Webex Teams for VDI consists of the following components:

- Cisco Webex Teams virtual desktop application
- Cisco Webex thin client plug-in

Cisco Webex Teams virtual desktop application runs on the VDI desktop or server. Cisco Webex Teams thin client plug-in is the thin client package that runs on the thin client.

Table 39. Supported environment

Component	Supported platforms
Thin Client	• Latitude 3440 • Latitude 5450 • Latitude 5440 • OptiPlex AIO 7410 • OptiPlex AIO 7420
Connection Broker agent for the hosted virtual desktops	• Citrix Virtual Desktops • Omnissa Horizon published desktop
Cisco Webex Teams Virtual Desktop app on the hosted virtual desktop	See the Release Notes for the supported version.
Cisco Webex Teams Plugin on the thin client	See the Release Notes for the supported Webex VDI package.

Ensure that you have used the Compatibility between the Webex Teams and the Thin-Client Plugin table to configure the Webex Teams or VDI optimization mode environment.

To access the compatibility table, do the following:

1. Go to help.webex.com.
2. In the search bar, enter **Webex | VDI Release Notes**, and press Enter.
3. Click **Webex | VDI Release Notes** from results.
4. Click the **Version Support** tab.
5. Scroll down the page to view the Webex app version for VDI and Compatible Thin-Client Plugin Versions table.

Install the Cisco Webex Teams package on ThinOS

You must install the Webex Teams package on ThinOS to use Cisco Webex Teams for VDI. To install the Cisco Webex App VDI package using Wyse Management Suite or Admin Policy Tool, see Upload and push ThinOS 10.x application packages.

Setting up the Cisco Webex App VDI

This section describes how to install and use the Cisco Webex App for VDI on a virtual desktop.

Steps

1. Go to Webex by Cisco and download the supported Webex App HVD installer.
   To know the supported version, refer the *Release Notes* of your ThinOS version at Support | Dell.
2. On the virtual desktop, install the Cisco Webex App Virtual Desktop application.

a. Open Command Prompt with administrator privileges.
b. Run the following command:

```
msiexec /i WebexTeams.msi ALLUSERS=1
AUTOUPGRADEENABLED=0 ENABLEVDI=1
```

NOTE: Replace the file name WebexTeams.msi with the real name of the installer file that you downloaded.

3. Install the following ThinOS packages on the ThinOS client:
   - **Citrix Workspace app package**—Install this package if you want to use the Cisco Webex Teams application with Citrix Desktops.
   - **Omnissa Horizon package**—Install this package if you want to use the Cisco Webex Teams application with Omnissa Horizon server-published desktops.
   - **Cisco Webex App VDI package**—Install this package to use Cisco Webex Teams for VDI.
4. Log in to the virtual desktop, and sign in to the Webex App application using your credentials.

Cisco Webex Teams optimization on Citrix Workspace app feature matrix

Table 40. Cisco Webex Teams optimization on Citrix Workspace app feature matrix

Scenarios	ThinOS
Call—Audio call	Supported
Call—Video call	Supported
Call—Long audio call	Supported
Call—Long video call	Supported
Chat	Supported
Call—Mute or unmute	Supported
Call—Turn on or turn off camera	Supported
Full screen	Supported
Share screen—screen 1	Supported
Call—Chat during video call	Supported
Call—Add guest	Supported
Call—New Whiteboard	Supported
Camera—Camera setting	Supported
Camera—Preview camera	Supported
Camera—Plugin or unplug the Camera	Supported
Camera—Switch camera during video call	Supported
Speaker and Microphone	Supported
Plug or remove the headset	Supported
Switch headset during audio call	Supported
End call	Supported
Group audio call	Not tested
Group video call	Not tested
Group chat	Supported

Table 40. Cisco Webex Teams optimization on Citrix Workspace app feature matrix (continued)

Scenarios	ThinOS
Meetings	Supported
Annotation	Supported

Cisco Webex Teams optimization on Omnissa feature matrix

Table 41. Cisco Webex Teams optimization on Omnissa feature matrix

Scenarios	ThinOS
Call—Audio call	Limited Support—Audio and video calls are supported only by TCP connection.
Call—Video call	Limited Support—Audio and video calls are supported only by TCP connection.
Call—Long audio call	Supported—The device stops responding occasionally during audio and video calls. This is a known issue.
Call—Long video call	Supported
Chat	Supported
Call—Mute or Unmute	Supported
Call—Turn on or turn off camera	Supported
Full screen	Supported
Share screen—Screen 1	Supported
Share screen—Other applications	Not supported—Synchronous with Ubuntu
Share screen—Share system audio	Not supported—Synchronous with Ubuntu
Share screen—Optimize for video	Not supported—Synchronous with Ubuntu
Call—Chat during a video call	Supported
Call—Add guest	Supported
Call—New whiteboard	Supported
Camera—Camera setting	Supported
Camera—Preview camera	Supported—The camera does not display any image during a video call. This is a known issue.
Camera—Plug or unplug the camera	Supported
Camera—Switch camera during a video call	Supported
Speaker and microphone	Supported
Plug or unplug headset	Supported
Switch headset during audio call	Supported
End call	Supported
Group audio call	Supported
Group video call	Supported
Group chat	Supported

Verify the Cisco Webex App connection status

This section describes how to verify if the Cisco Webex App runs in Optimized mode status on your thin client. In Optimized mode, the Webex App application delivers an optimal performance.

Prerequisites

- Ensure that you have installed the supported version of the Cisco Webex App application on the remote desktop.
- Ensure that you have installed the correct Cisco Webex App VDI package on the ThinOS device.

Steps

1. Connect to a virtual desktop session on ThinOS.
2. Start the Cisco Webex App virtual desktop application.
3. From the current user menu, click **Help** > **Health Checker**.
4. In the **Health Checker** window, check if VDI is connected and all services are accessible. Also, verify if the VDI version compatibility and the virtual channel are connected.

Cisco Webex Meetings for VDI

Cisco Webex Meetings Virtual desktop software is the Unified Communications product from Cisco for real-time video conferencing in a VDI environment. It supports audio-video conferencing on the hosted virtual desktops. Cisco Webex Meetings offloads media processing from the virtual desktop server to the thin client. All audio and video signals are routed directly between the endpoints without going through the hosted desktop.

Cisco Webex Meetings Virtual Desktop software enables you to attend meetings in a VDI environment. Cisco Webex Meetings for VDI consists of the following components:

- Cisco Webex Meetings virtual desktop application
- Cisco Webex Meetings thin client plug-in

Cisco Webex Meetings Virtual Desktop app runs on the VDI desktop or server. Cisco Webex Meeting thin client plug-in is the thin client package that runs on the thin client.

From version 42.8 (a special release based on 42.6), Webex Meetings VDI supports the **Virtual Background/Blur image** feature.

Table 42. Supported environment

Component	Supported environment
Thin Client	• Latitude 3440 • Latitude 5450 • Latitude 5440 • OptiPlex AIO 7410 • OptiPlex AIO 7420
Connection Broker agent for the hosted virtual desktops	• Citrix Virtual Desktops • Omnissa Blast VDI
Cisco Webex Meetings Virtual Desktop app on the hosted virtual desktop	See the Release Notes for the supported version.
Cisco Webex Meeting Plugin on the thin client	See the Release Notes for the supported package.

Ensure that you have used the Compatibility between the Webex Meetings Desktop App and the Thin Client Plugin table to configure the Webex Meetings optimization mode environment.

To access the compatibility table, do the following:

1. Go to help.webex.com.
2. In the search bar, enter **Release Notes for Cisco Webex Meetings Virtual Desktop Software Release 41.x**, and press Enter.
3. Click **Release Notes for Cisco Webex Meetings Virtual Desktop Software Release 41.x** from results.
4. Click the **Compatibility List** tab.

5. Scroll down the page to view the Meetings Client Version and Compatible Thin Client Plugin Versions table.

Limitation—On a ThinOS-based device with NVIDIA vGPU, you cannot launch Webex Meetings in a VDI optimized mode. This is a Cisco limitation.

Workaround—Use a combination of GPU pass-through and a Windows registry setting as follows:

- If you are a current user and using Webex Meeting Suite v40.6.7,v40.7.4, v40.8.2, or v40.9.0, add the following to the Windows Registry key on the hosted virtual desktop:
  - Key—`Computer\HKEY_CURRENT_USER\Software\\Cisco Systems, Inc.\CiscoVDI`
  - Values:
    - Name—`isVDIEnv`
    - Type—`REG_EXPAND_SZ`
    - Data—`true`

  NOTE: Restart Webex Meetings after you edit the registry.

- If you are an administrator of the local machine and using Webex Meeting Suite 40.10.5 or 40.11.0, add the following to the Windows Registry key on the hosted virtual desktop:
  - Key:
    - 32-bit operating system—`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Spark Native`
    - 64-bit operating system—`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco Spark Native`
  - Values:
    - Name—`isVDIEnv`
    - Type—`REG_EXPAND_SZ`
    - Data—`true`

  NOTE: Restart Webex Meetings after you edit the registry.

Install the Cisco Webex Meetings VDI package on ThinOS

You must install the Cisco Webex Meetings VDI package on ThinOS to use Cisco Webex Meetings for VDI. To install the Webex Meetings package using Wyse Management Suite or Admin Policy Tool, see Upload and push ThinOS 10.x application packages.

Setting up the Cisco Webex Meetings for VDI

This section describes how to install and use the Cisco Webex Meetings for VDI on a virtual desktop.

Steps

1. Install the Cisco Webex Meetings desktop application when you first join the meeting from the URL.
2. Install the following ThinOS packages on the ThinOS client:
   - **Citrix Workspace app package**—Install this package if you want to use the Cisco Webex Meetings application with Citrix Virtual Desktops.
   - **Cisco Webex Meetings VDI package**—Install this package to use Cisco Webex Meetings for VDI.
3. Log in to the virtual desktop, and join the Cisco Webex Meeting.

Cisco Webex Meetings optimization feature matrix

Table 43. Cisco Webex Meetings optimization feature matrix

Scenarios	ThinOS
Join meeting	Supported
Audio call	Supported
Video call	Supported

Table 43. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS
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—Annotates	Supported
Share screen—Pause or Resume	Supported
Share screen—View—full screen	Supported
Share screen—View—Zoom in/out/to	Supported
Share screen—Start or Stop video during share screen	Supported
Record meeting—Start, Pause, or Stop recording	Supported
Support—Request Desktop Control	Not supported
Support—Request Application Control	Not supported
Stop share screen	Supported

Table 43. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS
Participant	Supported
Close Participant	Supported

Verify the Cisco Webex Meetings connection status

This section describes how to verify if Cisco Webex Meeting runs in optimized mode status on your thin client. In Optimized mode, the Webex Meetings application delivers an optimal performance.

Prerequisites

- Ensure that you have installed the supported version of the Cisco Webex Meetings virtual desktop application on the remote desktop.
- Ensure that you have installed the correct Cisco Webex Meetings package on the ThinOS device.
- Ensure that you have referred the **Compatibility between the Webex Meetings Desktop App and the Thin Client Plugin** table to configure Webex Meetings optimization mode environment. To access the compatibility table, do the following:
  1. Go to help.webex.com.
  2. In the search bar, enter **Cisco Webex Meetings Virtual Desktop Software**, and press Enter.
  3. Click **Cisco Webex Meetings Virtual Desktop Software** from the results.
  4. Scroll down the page to view the **Compatibility between the Webex Meetings Desktop App and the Thin Client Plugin** table.

Steps

1. Connect to a virtual desktop session on ThinOS.
2. Start the Cisco Webex Meetings virtual desktop application.
3. In the Cisco Webex Meetings window, check if **Cisco Webex Meetings - VDI** is displayed on the upper-left corner of the screen.

   If the Webex Meeting does not run in optimized mode, do either of the following:
   - If you are having administrator privileges, go to the Webex Meetings Administration site and ensure that the **Enable meeting client for VDI** check box is selected in the **Common Site Settings** tab.
   - If you do not have administrator privileges, edit the registry in VDI as follows:
     a. In the system registry of VDI, go to **HKEY_CURRENT_USER** > **SOFTWARE** > **Webex** > **NativeVDI**.
     b. Create a DWORD entry `VDIFeatureEnabled` with value `1`.

Cisco Webex Meetings optimization known issues

- The thin client may occasionally stop responding during meetings.

Zoom Meetings for VDI

ZoomMeetings for VDI are the Unified Communications solution that is offered by Zoom for virtual deployments. It supports enterprise video conferencing and screen sharing on the virtual desktops. Zoom offloads media processing from the virtual desktop server to the thin client. All audio and video signals are routed directly between the endpoints. You can use the Zoom application to make and receive calls in the VDI session.

For information about limitations, see the **Release Notes** of your ThinOS version at Support | Dell.

Zoom Meetings for VDI consists of the following components:

- Zoom VDI Client
- Zoom Media Plug-in

Zoom VDI Client is the host installer that runs on the VDI desktop or server. Zoom Media Plugin is the thin client package that runs on the thin client.

NOTE: The VDI Client version must not be older than the plug-in version for Zoom optimization to work on ThinOS. For the Zoom Horizon VDI package to work in a session, it must be uninstalled and reinstalled.

Table 44. Supported environment

Component	Supported platforms and supported versions
Thin Client	• Latitude 3440 • Latitude 5450 • Latitude 5440 • OptiPlex AIO 7410 • OptiPlex AIO 7420
Connection Broker agent for the hosted virtual desktops	• Citrix Virtual Desktops • Omnissa Horizon published desktop
Zoom VDI Client on the hosted virtual desktop	See the Release Notes for the supported version.
Zoom Media Plugin on the thin client	See the Release Notes for the supported Zoom package.

Install the Zoom package on ThinOS

You must install the Zoom package to use Zoom Meetings for VDI. To install the Zoom package using Wyse Management Suite or Admin Policy Tool, see Upload and push ThinOS 10.x application packages.

Setting up the Zoom Meetings for VDI

This section describes how to install and use the Zoom Meetings for VDI on a virtual desktop.

Steps

1. Go to Zoom Support, and download the supported VDI client version.
   To know the supported VDI client version, see the *Release Notes* of your ThinOS version at Support | Dell.
   The `ZoomInstallerVDI.msi` is downloaded to your device.
2. On the virtual desktop, install the Zoom VDI Client. Double-click the file and follow the installation wizard steps.
3. Install the following ThinOS packages on the ThinOS client:
   - If you want to use Zoom with Citrix virtual desktops, install the following packages:
     - **Citrix Workspace app package**
     - **Zoom Universal package**
   - If you want to use Zoom with Omnissa Horizon published desktops, install the following packages:
     - **Omnissa Horizon package**
     - **Zoom Universal package**
   - If you want to use Zoom with RDP, RDS, and AVD desktops, install the following packages:
     - **Microsoft AVD package**
     - **Zoom Universal package**
4. Log in to the virtual desktop, and sign in to the Zoom application using your credentials.

Zoom optimization feature matrix

Table 45. Zoom optimization feature matrix

Scenario	ThinOS
Long audio or video meetings	Supported
New meeting with audio only	Supported
New meeting with audio and video	Supported

Table 45. Zoom optimization feature matrix (continued)

Scenario	ThinOS
Join a meeting	Supported
Schedule a meeting	Supported
Meeting with multiple participants	Supported
End meeting for all	Supported
Leave meeting	Supported
Share screen directly with meeting ID	Supported
Gallery View or Speaker View	Supported
Enter or exit Full screen	Supported
Mute or unmute audio	Supported
Start or stop video	Supported
Security—Lock meeting	Supported
Security—Enable waiting meeting	Supported
Security—Allow participants to share screen	Supported
Security—Allow participants to chat	Supported
Security—Allow participants to rename themselves	Supported
Participants—Invite people to join in meeting	Supported
Polls	Supported
Chat	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
Record meeting—Start, Pause, or Stop recording	Supported
Live Transcript—Show subtitles	Supported
Live Transcript—View full transcript	Supported
Live Transcript—Subtitle settings	Supported
Support—Request Desktop Control	Supported
Support—Request Application Control	Supported
Support—Request computer restart	Supported
Live on custom live streaming service	Not tested
Audio Devices—Plug or unplug headset	Supported
Audio Devices—Switch headset	Supported
Video Devices—Plug or unplug camera	Supported
Video Devices—Switch camera	Supported
Video Devices—Choose virtual background	Supported (only with green screen)
Headset buttons—Answer/Mute/End Call	Limited support—Only Mute button is supported
Annotation	Not supported

Verify the Zoom connection status

This section describes how to verify if Zoom runs in Optimized mode status on your thin client. In Optimized mode, the Zoom application delivers an optimal performance.

Prerequisites

- Ensure that you have installed the correct Zoom VDI client on the remote desktop.
- Ensure that you have installed the correct Zoom package on the ThinOS device.

Steps

1. Connect to a virtual desktop session on ThinOS.
2. Start the Zoom application.
3. Click the **Settings** icon and then click **Statistics**.
4. In the **Overall** tab, check if the VDI Connect Status is displayed as **Connected, Direct**.

Microsoft Teams Optimization from Omnissa Horizon

Omnissa Horizon package version 2106 includes Microsoft Teams media optimization by default for client side. 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. See Enable the optimization by using a Group Policy Editor.

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 **Omnissa 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**.

Enable the optimization by using a Group Policy Editor

Steps

1. Open the Group Policy Editor.
2. Go to **Computer Configuration** > **Administrative Templates** > **Omnissa View Agent Configuration** > **Omnissa HTML5 Features** > **Omnissa WebRTC Redirection Features**.

   NOTE: For steps on how to download and apply the Omnissa Blast ADMX template file (vdm_agent.admx), see **Omnissa Horizon Documentation** at docs.omnissa.com.

3. Double-click **Enable Media Optimization for Microsoft Teams**.
4. Ensure that **Enabled** is selected, and click **OK**.
5. Log off from the Horizon desktop.

Microsoft Teams optimization feature matrix

Table 46. Microsoft Teams optimization feature matrix

Scenario	ThinOS
Long audio call	Supported
Call—Make an audio call	Supported
Call—Answer an audio call	Supported
Call—Make a video call	Supported

Table 46. Microsoft Teams optimization feature matrix (continued)

Scenario	ThinOS
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.
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 calls. 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. As a workaround, 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. The issue is due to a limitation of Microsoft Teams.
- Sharing screen when Microsoft Teams is published as an application is not supported. The issue is due to a limitation of Omnissa Horizon.

- There maybe inconsistencies 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. As a workaround, 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.

Microsoft Teams optimization for RDP protocol sessions

ThinOS 10.x 2502 supports media optimization for Microsoft Teams in RDP protocol sessions.

To enable the Teams optimization feature for RDP protocol sessions, do the following:

1. Install the Microsoft Teams desktop app in RDP protocol sessions. For more information about the Microsoft Teams desktop application installation, see **Use Microsoft Teams on Azure Virtual Desktop** in the Microsoft website.
2. Connect the RDP protocol session with ThinOS to launch Microsoft Teams.
3. In Microsoft Teams, go to **About > Version**.
4. If enabled, **AVD Media Optimized** is displayed.

Table 47. Supported and not supported ThinOS scenarios

Scenario	ThinOS
Long meetings	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 Supported
Call—Start or stop recording	Supported
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—Microsoft PowerPoint	Supported
Chat	Supported
Audio or video call in VDI server desktop	Supported
Audio or video call in published Microsoft Teams application	Not Test
Devices—Plug in or disconnect the headset	Supported

Table 47. Supported and not supported ThinOS scenarios (continued)

Scenario	ThinOS
Devices—Switch headset	Supported
Devices—Plug in or disconnect the camera	Supported
Devices—Switch camera	Supported
Headset buttons—Answer/Mute/End Call	Not Supported

RingCentral

RingCentral brings calling, messaging, and meetings into one application.

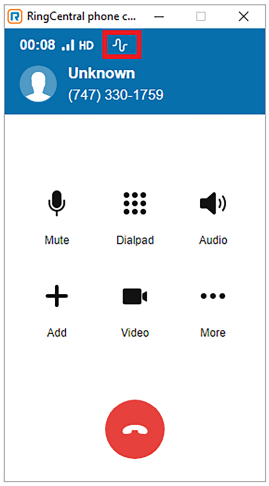

Figure 46. RingCentral

- RingCentral supports audio only.
- For Citrix, you can install citrix-vda-policy (Windows Batch File) in a VDI session. No additional package is required by the client.
- For Omnissa, you can install the RingCentral package on the ThinOS client locally and the Omnissa plug-in in VDI session.
- To use RingCentral application for VDI, you must install the RingCentral package. To install the Omnissa plug-in package using Wyse Management Suite, see Upload and push ThinOS 10.x application packages using Groups and Configs on Wyse Management Suite.

9

Configuring third-party authentication settings

ThinOS supports the following third-party authentication types:

- **Imprivata**—ThinOS supports Imprivata on Citrix, Omnissa, and Microsoft VDI solutions in both Imprivata ProveID Embedded and ProveID Webapi modes. The following are supported VDI solutions:
  - Citrix Desktop
  - Citrix XenApp
  - Microsoft Remote Desktop Services session based and virtual desktop
  - Microsoft Remote Desktop Services Remote PC
  - Microsoft Remote Desktop Services RemoteApp
  - Omnissa Horizon - Desktops
  - Omnissa Horizon - Application
- **Identity Automation**—ThinOS supports RapidIdentity for Healthcare (formerly HealthCast) SSO solution.

Configure the Imprivata OneSign server

OneSign Virtual Desktop Access provides a seamless authentication experience and can be combined with single sign-on for No Click Access to desktops and applications in a virtual desktop environment.

About this task

This section describes how to configure the Imprivata OneSign server on your thin client.

Steps

1. From the desktop menu, click **System Setup** > **Remote Connections** .
   The **Remote Connections** dialog box is displayed.
2. Click the **Authentication** tab, and select the authentication as **Imprivata**.
3. In the **OneSign Server** field, enter either https://ip or https://FQDN values of the OneSign server.
   The security setting for OneSign server in the Admin Policy Tool controls the security level of OneSign. The security level is set as high by default and you must import the certificate of the OneSign server before using the OneSign feature. The certificate is not required if the security level is set as low.
4. Click **Save** to save your changes.
5. Restart the thin client.
   The Imprivata login dialog box is displayed.
   The following OneSign features or actions are supported:
   - Client and Broker authentication
     - Citrix Virtual Apps (formerly Citrix XenApp)
     - Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop)
     - Omnissa Horizon Desktops
     - Omnissa Published Application
     - Microsoft RDS/Remote PC Desktops
     - Microsoft RDS Applications
   - Kiosk Mode
   - Fast User Switching
   - Non-OneSign user VDI access
   - Hotkey Disconnect

- Proximity card reader redirection
- Guided Question and Answer login
- Authenticate w/Password
- Authenticate w/Password + Password Change
- Authenticate w/Password + Password Change | New Password is Invalid
- Authenticate w/Proximity Card + Password
- Authenticate w/Proximity Card + Pin
- Authenticate w/Proximity Card + Pin | Pin not enrolled
- Authenticate w/Proximity Card Alone | Retrieve Password
- Retrieve User Identity Password
- Reset User Identity Password
- Update User Identity Password
- Enroll Proximity Card
- Lock/Unlock Terminal with Proximity CardLock/Unlock Terminal with Proximity Card
- Treat Smart card as proximity card

VDI selection on ThinOS

ThinOS 10.x supports Imprivata on Citrix, Omnissa, and Microsoft VDI solutions in both Imprivata ProveID Embedded and ProveID WebAPI modes.

- **ProveID Webapi Mode**: Select the VDI type from the **Automate access to setting** in the Admin Policy Tool.
- **ProveID Embedded Mode**: The VDI type is determined by the Imprivata OneSign policy.

NOTE: When logging in to the Omnissa Horizon View broker using the Imprivata ProveID Embedded (PIE) mode, the Omnissa Horizon Client PCoIP is used instead of Teradici PCoIP.

Configure Windows 365 connections on ThinOS device

Explains how ThinOS 10.x enables users to configure Windows 365 Cloud PC connections using the Microsoft AVD client, allowing secure access to Windows 365 resources with Microsoft Entra ID authentication.

Steps

1. Log in to the ThinOS device.
2. Go to **System Settings** > **Connections**.
3. Select **Add Connection**.
4. Choose **Microsoft AVD / Windows 365** as the **Connection Type**.
   ThinOS uses the same AVD client for both AVD and Windows 365 connections.
5. In the **Broker / URL** field, enter one of the following:
   - Windows 365 URL—Enter the URL, (for example: https://windows365.microsoft.com).
   - Standard AVD feed—Enter the URL, (for example: https://rdweb.wvd.microsoft.com).
6. Set **Authentication** to **Microsoft Entra ID** (Azure AD).
7. Enter the username in the format—Enter the username, (for example: user@domain.com).
8. Save the configuration.
   The configured Windows 365 Cloud PC appears in the connection list, and users can launch it directly from ThinOS using Microsoft Entra ID authentication.

Configure the VDI settings on the OneSign server

To use Citrix, Omnissa, and Microsoft VDI with OneSign, you must specify the broker server details in the OneSign Server Web Console.

Steps

1. Open the Imprivata OneSign Server Web Console.
2. On the **Computers** page, click the **Virtual Desktops** tab.
3. Add the VDI broker URL in the respective VDI sections.
4. Select the **Allow authentication from devices** checkbox for the respective VDI brokers.
5. Save your settings.

Configure objects on Imprivata Server

About this task

This section describes how to configure different objects on the Imprivata server.

Steps

1. To configure general configuration, do the following:

   On the Imprivata server, click **Computer policy**, and then click **General** tab.

   a. **Allow users to shut down and restart workstation from lock screen**
      - Select the check box to enable the feature. If enabled, the **shutdown** and **restart** icons are displayed in ThinOS login and locked windows.
      - Clear the check box to disable the feature. If disabled, the **shutdown** and **restart** icons are not available.

   b. **Display name format**—Use this option to set different formats for the account name that is displayed in dialog box notifications.

   c. **Authentication**—If OneSign authentication fails, but Windows authentication succeeds, you can log in to the system. Click either **Yes** or **No**. If you are a non-OneSign user, click **No** to log in to the Broker agent.

2. To configure walkway configuration, do the following.

   On the Imprivata server, click **Computer policy**, and then click the **Walk-Away Security** tab.

   a. **Inactivity detection for Keyboard and mouse**
      - When inactivity is detected, OneSign can take action to secure the workstation. **Lock workstation after** and **Show inactivity warning** can be configured.
      - **Advanced Settings**—You can configure **Proximity Card lock behavior**
      - In **Advanced Settings**, you can also configure **Restrict the operations allowed with passive proximity cards**
        - If you want to use a proximity card to lock the thin client, select **Allow lock only**.
        - If you want to lock the thin client and login as a different user, select the **Allow locking and user switching**.

   b. In **Lock and warning behavior**, you can configure **Lock behavior** to set the lock screen type. Only **obscure the desktop type** is supported.

   c. In **Lock and warning behavior**, you can also configure **Warning behavior**.
      - **No Warning**—No warning messages are displayed.
      - **Notification balloon**—ThinOS displays a notification window.
      - **Fade to lock (Screensaver)**—Hides the display contents before the thin client locks.

3. To configure Challenges configuration, do the following.

   On the Imprivata server, click **User policies**, and then click the **Challenges** tab.

   a. **Hot key to lock workstation or log off user**—Use this option to set Hot keys for ThinOS. The following keys are supported:
      - F1
      - F12
      - Backspace
      - Del
      - Down
      - End

- Enter
- Esc
- Home
- Insert
- Left Alt
- Left
- Left Ctrl
- NumLock
- Page Down
- Page Up
- Right Ctrl
- Right
- Right Alt
- Space
- Tab
- Up
- a to z
- A to Z
- 0 to 9
- Modifier +, %, ^ (Shift, Alt, and Control)

b. **At Inactivity Challenge or Pressing Hot Key**—The server configuration controls this feature on ThinOS.

4. To configure customization configuration, do the following:

   On the Imprivata server, click **Computer policy**, and then click the **Customization** tab.

   a. **Login logo and background**—You can upload the logo and background image file in this setting. The logo is displayed in the ThinOS login window, and the background image replaces the ThinOS default background.
   b. **Walk-away security**—Use this to customize your warning messages.
   c. **Password self-service prompt**— Use this to customize your Link text.

5. To configure the password self-services force enrollment feature, do the following:

   On the Imprivata server, click **User policies**, and then click **Self-Service Password/Imprivata PIN Reset**.

   - You can permit users to reset their primary authentication password, to reset their Imprivata PIN, and to request all their application credentials that have been captured by Imprivata using enrolled security questions.
   - You can enable or disable the **Allow users to reset their primary authentication password** option.
   - You can enable or disable the **Require users to re-authenticate after resetting their password** option.

6. To configure RFIDeas Card Readers configuration, do the following:

   On the Imprivata server, click **Computer policies**, and then click the **General** tab.

   a. In **Card Readers**, you can configure **Beep Card reader when user taps card** to control the beep sound when tapping the card.
   b. In **Card Readers**, you can also configure **Configuration 1—4** . These configurations apply to pcProx Plus 82 (RDR-80582/RDR-80082) and IMP-80/IMP-82 models.

Use smart card as proximity card

You can use a smart card as a proximity card to authenticate the user. When you tap the smart card on the smart card reader, the Imprivata agent uses the smart card's unique serial number as the Unique ID (UID) of the proximity card.

About this task

This section describes how to use a smart card as a proximity card.

Steps

1. Log in to the OneSign Administrator console.
2. Go to the **Computers** page and click **Computer Policy**.
3. In the **Smart card readers** section, select the **Treat smart card authentications as proximity card authentications** check box.

Next steps

To authenticate the user using a proximity card, connect a supported reader to the thin client. Before you tap the card, ensure that your card is already enrolled to the user. When you tap your card on the reader, the thin client authenticates the user and starts the VDI connection.

Enroll a proximity card with Imprivata OneSign

About this task

This section describes how to enroll a proximity card with Imprivata OneSign.

Steps

1. Tap the proximity card. The card enrollment page is displayed.
2. Enter the credentials and click **OK**.
   Proximity card is enrolled successfully.

Imprivata Bio-metric Single Sign-On

Fingerprint identification feature is highly reliable, and cannot be replicated, altered, or misappropriated.

The prerequisites of OneSign server are:

- Imprivata v4.9 or later appliance version is needed that supports the WebAPI v5 and later versions.
- Fingerprint identification license is required.
- Fingerprint reader device is required. ET710 (PID 147e VID 2016) and ET700 (PID 147e VID 3001) are the supported devices.

Supported user scenarios

- Signing in or unlocking the ThinOS devices using the Fingerprint authentication.
  - Configure the OneSign server on ThinOS, and then connect the Fingerprint reader device.
  - The ThinOS Fingerprint window is displayed automatically after the OneSign server is initialized.
  - Fingerprint authentication works on the ThinOS unlock window.
- Unlocking the Virtual Desktop using the Fingerprint authentication.
  - Enable the **Imprivata Virtual Channel** option from the ThinOS Global Connection settings.
  - When you lock the virtual desktop in the session, the Fingerprint window is displayed automatically.
- Managing Fingerprints on a virtual desktop.
  - Legend Fingerprint Management is supported.
  - Fingerprint management with Imprivata Confirm ID enabled is not supported.

PCoIP session from ThinOS ProveID Web

- Imprivata Virtual Channel Limitation: In PCoIP sessions with Horizon Agent 2111 or later, the Imprivata Virtual Channel is not supported. As a result, Proximity and Fingerprint authentication methods are unavailable in these sessions.
- Impact on Other Session Types:
  - Blast Sessions: No impact.
  - ThinOS ProveID Embedded (PIE) PCoIP Sessions: No impact.
- Reconnection Delay: A 15-second delay occurs when reconnecting to previous PCoIP sessions with Horizon Agent and Imprivata Agent installed. This issue is resolved in Omnissa Horizon versions 7.13.2, 8.5, or later, with an additional registry key change required on the virtual machine. For more information, see **Delay in reconnecting to Horizon desktop when HTMLAccess and Imprivata OneSign are in use (85892)** in the Omnissa website.

Grace period to skip second authentication factor

Grace period enables you to specify a time limit on OneSign server for logging in without the second authentication factor after the first login session.

NOTE: After you specify the grace period, you must first use the proximity badge, and then enter password or OneSign PIN for the initial login.

If you use the proximity card after the time limit that you specified for grace period, the second authentication factor window is displayed with the message **Grace period expired**.

If you enter a wrong password or PIN, the second authentication factor window is displayed with the warning message **OneSign could not authenticate you. Try again.**

Imprivata OneSign ProveID Embedded

ThinOS supports the Imprivata OneSign ProveID Embedded (PIE) feature that enables secure authentication to virtual desktops and applications. Using this feature, you can seamlessly access the clinical applications. The PIE solution simplifies access to roaming desktops with Citrix Virtual Apps and Desktops, Omnissa Horizon Desktops and Applications, and Remote Desktop Services. You can also deploy a Citrix Virtual App hosted desktop with Fast User Switching (FUS) to eliminate the need for generic user log-ins. For more information about the Imprivata OneSign ProveID Embedded, see the documentation available in the imprivata website.

Table 48. Supported environment

Component	Supported environment
Endpoints (Thin Clients)	• Wyse 5070 Thin Client • Wyse 5470 All-in-One Thin Client • Wyse 5470 Thin Client
VDI environment	• Citrix Desktop • Citrix XenApp • Microsoft Remote Desktop Services session based and virtual desktop • Microsoft Remote Desktop Services Remote PC • Omnissa Horizon - Desktops
Authentication methods	• Network password • Proximity card • Security questions • PIN (as a secondary factor) • Fingerprint biometrics

Table 49. Imprivata ProveID Embedded feature matrix

Feature	Description	ThinOS PIE	ThinOS PIW
General Features and Workflows	Imprivata Appliance failover	Supported	Supported
	Imprivata offline mode	Not applicable	Not applicable
	Imprivata self- service password reset	Supported	Supported
	Third-party self-service password reset	Not applicable	Not applicable
	Non- OneSign user workflow	Supported	Supported
	Spine Combined workflow	Not applicable	Not applicable
	Smartcard as proximity card workflow	Supported	Supported
Imprivata Walk Away Security	Honors lock command	Not applicable	Not applicable
	Fade to Lock screensaver	Supported	Supported
	Notification balloon	Not applicable	Supported
Citrix Workflows	Citrix Virtual Desktops	Supported	Supported

Table 49. Imprivata ProveID Embedded feature matrix (continued)

Feature	Description	ThinOS PIE	ThinOS PIW
	Citrix Virtual Applications	Supported	Supported
	Virtual Kiosk Citrix for Virtual Desktops	Supported	Supported
	Virtual Kiosk for Citrix Published Applications	Supported	Supported
Omnissa Workflows	Omnissa Horizon Desktops	Supported	Supported
	Omnissa Published Application Support	Not applicable	Supported
	Virtual Kiosk for Omnissa Desktops	Not applicable	Supported
	Virtual Kiosk for Omnissa Published Applications	Not applicable	Supported
Microsoft Workflows	Microsoft RDS/Remote PC Desktops	Supported	Supported
	Microsoft RDS Applications	Not applicable	Supported
	Virtual Kiosk for RDS/ Remote PC Desktops	Not applicable	Supported
	Virtual Kiosk for RDS Published Applications	Not applicable	Supported
Primary Authentication Modalities using Endpoint Operating System	Password	Supported	Supported
	Proximity card	Supported	Supported
	Smart card	Not applicable	Not applicable
	Fingerprint biometrics	Supported	Supported
	Question and Answer	Supported	Supported
Authentication/ Re-Authentication Modalities using Virtual Channel	Proximity card	Supported	Supported
	Smart card	Not applicable	Not applicable
	Fingerprint biometrics	Supported	Supported
	Imprivata Hands Free Authentication	Supported	Not applicable

The overall PIE configuration on ThinOS includes the following tasks:

1. Configure the OneSign Admin Console. See, Configure the OneSign Admin Console.
2. Install the Imprivata PIE agent package on ThinOS. See, Install the Imprivata PIE package on ThinOS.
3. Enable the PIE mode on ThinOS using Admin Policy Tool or Wyse Management Suite. See, Enable PIE mode on ThinOS.
4. If the **Security Mode** for Imprivata settings is set to **High**, upload the appliance SSL certificate using any of the following methods:
   - Import the SSL certificate manually.
   - Import the SSL certificate automatically.
5. Configure the FUS on ThinOS (optional step). See, Configure the Fast User Switching on ThinOS.

Configure the OneSign Admin Console

Steps

1. Open the OneSign Admin Console.
2. Log in as an administrator.

3. On the upper-right corner of the page, click the gear icon, and then click **ProveID**.
4. In the **ProveID - API Access** section, select the **Allow full API access via ProveID Web API and ProveID Embedded** check box.
5. Select the **Dell Wyse Cloud Client** check box.
6. Save the configuration.

Install the Imprivata PIE package on ThinOS

Steps

1. Go to Support | Dell and download the Imprivata package that contains the PIE agent. For more information, see Download ThinOS 10.x firmware and packages.
2. Install the Imprivata package using any of the following methods:
   - Using Wyse Management Suite. For more information, see Upload and push ThinOS application packages using Wyse Management Suite.
   - Using Admin Policy Tool. For more information, see Upload and install ThinOS application packages using Admin Policy Tool.

Enable PIE mode on ThinOS

You can either use the ThinOS 10.x policy settings on Wyse Management Suite or the local Admin Policy Tool to enable the Imprivata ProveID Embedded (PIE) mode.

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. In the **Configuration Control | ThinOS** window, click the **Advanced** tab.
3. Expand **Login Experience** and click the **3rd Party Authentication** option.
4. From the **Select Authentication Type** drop-down list, select **Imprivata**.
   The **Imprivata Settings** window is displayed.
5. In the **OneSign Server** field, enter the list of host names or IP addresses with optional TCP port number, or URLs of Imprivata OneSign servers.
6. Click the **Enable ProveID Embedded Mode** slider switch to enable the ProveID Embedded mode on ThinOS.
   - ThinOS supports VDI silent mode. You can click the **VDI silent mode** switch to enable or disable the option. Enabling the option allows ThinOS to load the VDI configurations from the **Remote Connections** window in ThinOS. By default, the Imprivata OneSign policy controls the VDI selection. RDP is not supported in **VDI silent mode**.
   - The option **Enable Omnissa Horizon menu bar** is added under **Enable ProveID Embedded Mode**.
   - **Reboot on monitor connection** is disabled by default.
7. Configure the Imprivata ProveID Embedded options as per your requirement.
8. Click **Save & Publish**.

Uploading OneSign appliance SSL certificate

If the **Disable agent certificate checking** option is enabled, you must upload the OneSign appliance SSL certificate using one of the following methods:

- Import the SSL certificate manually.
- Import the SSL certificate automatically.

Import the OneSign appliance SSL certificate automatically

Prerequisites

- Ensure that you have created a group in Wyse Management Suite with a valid group token.
- Ensure that you have registered the ThinOS devices to Wyse Management Suite.

- Ensure that you have uploaded the SSL certificate to **Apps & Data** > **File Repository** > **Inventory**.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **ThinOS 10.x**.
   The **Configuration Control | ThinOS** window is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Certificates**.
6. Click the **Auto Install Certificates** slider switch to enable autoinstall of certificates on ThinOS.
7. From the **Select Certificates to Upload** drop-down list, select the SSL certificate.
8. Click **Save & Publish**.
   The certificate is installed on your thin client.

Import OneSign appliance SSL certificate manually

Prerequisites

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

Steps

1. Connect the USB drive to the thin client.
2. On the ThinOS client, go to **System Tools** > **Certificates**.
3. From the **Import From** drop-down list, select **USB Storage**.
4. Click **Import**.
5. Browse and select the SSL certificate that is stored in the USB drive.
6. Click **Save**.
   The certificate is imported to your thin client.

Configure Fast User Switching on ThinOS

Fast User Switching (FUS) is a feature of the Imprivata ProveID Embedded (PIE) agent that enables multiple users to securely access the shared environment. You can deploy a virtual desktop with FUS to eliminate the need for generic user log-ins.

Prerequisites

- Ensure that you have configured your virtual desktop.
- Ensure that you have configured the policies on the OneSign server.
- Ensure that you have enabled the PIE mode and configured the OneSign server on Admin Policy Tool or Wyse Management Suite. For more information, see Enable PIE mode on ThinOS.

For more information about how to configure the virtual desktop and OneSign server policies, see the documentation in the Imprivata website.

Steps

1. On ThinOS, go to **System Setup** > **Remote Connection** > **Broker Setup**.
2. In the **Broker Server** field, specify the Citrix Broker agent server details. The format of the Broker agent server must be `https://FQDN/citrix/storeweb`.
3. In the **Auto Connect** List, enter the desktop name to automatically log in to the Citrix session.
4. Click **Save**.
5. Go to **System Setup** > **Remote Connection** > **General Options**.
6. Enter the default sign-on username, password, and domain.
7. Click **Save**.

Configure Imprivata fingerprint reader for Citrix ICA and PCoIP sessions

About this task

Dell Technologies recommends the following fingerprint device settings to get the best experience during fingerprint authentication.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
3. Click **Add Row** in **vUSB Force Local** and enter the fingerprint device ID. For example, enter **`0x147e2016`**.
4. Click **Save & Publish**.

Configure Imprivata fingerprint reader for Blast sessions

About this task

Dell Technologies recommends the following fingerprint device settings to get the best experience during fingerprint authentication.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Standard** or **Advanced** tab, expand **Broker Settings**, and click **Omnissa Horizon Settings**.
3. Enter the fingerprint device ID in to the **Exclude Vid/Pid USB Device Redirection** field. For example, enter **`vid-147e_pid-2016`**.
4. Click **Save & Publish**.

Identity Automation

Identity Automation authentication is an enhanced sign-on solution which uses proximity card technology to quickly and securely access a remote session. You can tap the proximity card (same card that is used for building access or identification purposes) to log in and log out of your session. Using Identity Automation authentication, you do not have to enter the username and password each time you want to access the session. 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. The Identity Automation is independent of the ThinOS firmware and is a separate package.

Configure the Identity Automation

Prerequisites

If you are running ThinOS 10.0052, ensure that you have installed the identity automation package.

Steps

1. From the desktop menu, click **System Setup** > **Remote Connections** .
   The **Remote Connections** dialog box is displayed.
2. Click the **Authentication** tab, and select the Authentication Type as **Identity Automation**.
3. In the **Identity Automation Server** field, enter the Fully Qualified Domain Name (FQDN) for your Identity Automation Lynx server. By default, port 443 is used. However, you can specify a different port by adding a colon and the port number to the

end of the FQDN. For example, **server1.mycompany.com:5000**. In this example, the specified server FQDN and port 5000 on that server are used.

4. In the **API Key** field, enter the server API key.

   The **API Key** field is changed to a password type to hide the input values. To obtain the API key, do the following:

   a. Log in to the Lynx server web application.
   b. Go to **Settings** > **API**.
   c. Click **Copy** to copy the API key.

5. In the **Configuration ID** field, enter the configuration ID number that you want the thin client to use. The configuration ID number is associated with a group of settings that you can specify. Log in to your Lynx server as an administrator to specify a group of settings and obtain the configuration ID number.
6. Click **Save** to save your changes.
7. Connect a supported RFIDeas proximity card reader to the thin client.
8. Restart the thin client.
   The Identity Automation **Tap your badge** screen is displayed.

Install the Identity Automation QwickAccess app package on ThinOS

From ThinOS 10.0052, Identity Automation is an independent package. You must install the Identity Automation QwickAccess package to use Identity Automation. To install the app package using Wyse Management Suite, see Upload and push ThinOS 10.x application packages.

Identity Automation support matrix

The following are the supported features:

- Authentication to Citrix Virtual Apps and Desktops, Omnissa Horizon, and Microsoft Remote Desktop Services by tapping an enrolled proximity card.
- A user can enroll their own proximity card by tapping it on the connected proximity card reader. The user is prompted to provide their credentials, and after the credentials are validated, the proximity card is enrolled. This is a one-time event for the user.
- Authenticate with proximity card and password.
- Authenticate with proximity card and PIN.
- Authenticate with password (for users who do not have a proximity card, or who do not want to use their proximity card).
- Supports seamless change password.
- Lock or Unlock the terminal by tapping a proximity card.
- Supports convenient tap-over functionality.

Enroll a proximity card with Identity Automation on ThinOS

You can enroll the proximity card with Identity Automation on ThinOS. This enrollment is a one-time event for the user. After the proximity card is enrolled on one ThinOS client, you do not need to enroll your proximity card on other ThinOS clients.

About this task

Configure the Identity Automation authentication on ThinOS.

Steps

1. Connect a proximity card reader to the ThinOS client.
2. Tap the proximity card on the reader.
   The proximity card is automatically recognized as an unenrolled card and a dialog box appears prompting you to enroll the proximity card.
3. Click **Yes**.
4. When prompted, enter the Active Directory username and password.

After successful authentication, the username and password are saved. You are automatically connected to the remote session.

Use a proximity card for sign-on with Identity Automation on ThinOS

After you have enrolled the proximity card, you can use it to securely access your remote session. As an administrator, you can determine how often the user is prompted for their password or PIN when using the proximity card.

Prerequisites

- Ensure that you have configured the Identity Automation authentication on ThinOS.
- Ensure that you have enrolled the proximity card with Identity Automation.

Steps

1. Connect a proximity card reader to the ThinOS client.
2. Tap the proximity card on the reader.
   After successful authentication, you are automatically logged in to the remote session.

   If you are away for sometime and attempt to tap in the proximity card again, you may be prompted for either the password or PIN.

Use a proximity card to secure the remote session with Identity Automation on ThinOS

To secure your remote session, tap the proximity card and lock the thin client. When you return within the configurable timeout period, you only need to tap the card again to access the session.

Prerequisites

- Ensure that you have configured the Identity Automation authentication on ThinOS.
- Ensure that you have enrolled the proximity card with Identity Automation.

Steps

1. Tap the proximity card on the reader that is connected to the ThinOS client.

   The thin client is locked, and the remote session is secured.
2. When you return within the configured timeout period, tap the proximity card again on the reader.
   After successful authentication, you are automatically logged in to the remote session.

   If you do not return within the configurable timeout period, the remote session is disconnected from the thin client but left running on the server. You can access the session again on the same thin client or another thin client where Identity Automation authentication is enabled by tapping the proximity card.

Use a proximity card to tap-over another user session with Identity Automation on ThinOS

When a user has locked the thin client, or has walked away from the thin client without securing their work, a second user can access their own session by tapping their own proximity card. The session of the first user is disconnected from the thin client but is left running on the server. The second user is then logged in to their own session.

PIN Reset

You can reset your PIN code from the ThinOS login window by clicking **Forgot your PIN?**.

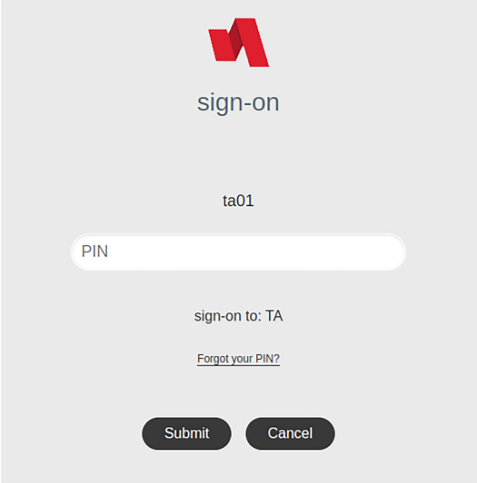

Figure 47. Forgot your PIN option in ThinOS login

To enable PIN reset, Lynx server version 1.7.0.6 is required.

Since ThinOS must match the Configuration ID with the Profile ID that enabled PIN reset, you must set the Profile ID to 1.

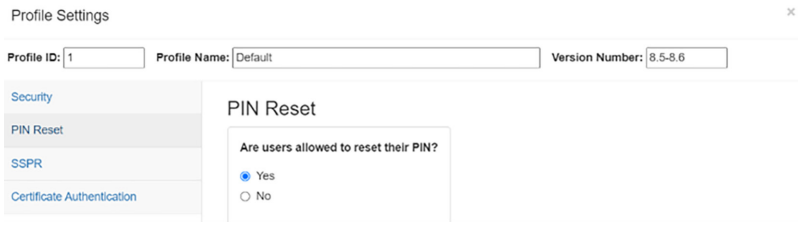

Figure 48. Profile ID for PIN Reset

Self-Service Password Reset (SSPR)

You can reset the password yourself by answering questions. After enrolling yourself to the SSPR feature of your card, follow these steps to reset your password:

Prerequisites

Ensure that the Lynx server version is 1.7.1.x, and the Identity Automation package version is 2.1 or later.

Steps

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

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

Identity Automation feature matrix

Table 50. Identity Automation feature matrix

Identity Automation Feature		ThinOS
Broker Type	Authenticate to Citrix Virtual Apps and Desktops	Supported
	Authenticate to Omnissa Horizon broker	Supported
	Authenticate to Microsoft Remote Desktop Services	N/A
Proxy Card	New card enrolls	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	Supported
	Self-service PIN reset	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

10

Configuring monitoring and management software

Configure Liquidware Stratusphere UX Connector ID Agent

ThinOS 10.x 2502 supports Liquidware Stratusphere UX Connector ID Agent. You can enable Liquidware Stratusphere UX Connector ID Agent and set the package URL in the Wyse Management Suite policy **Device Monitoring** page.

Steps

1. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab and expand **System Settings**.
3. Click **Device Monitoring**.
4. Enable **Liquidware Stratusphere UX Connector ID Agent**.
5. Enter the package URL.
6. Click **Save & Publish**.

Configure ThinOS Telemetry Dashboard

The ThinOS Telemetry dashboard option is added in **System Settings > Device Monitoring**. If enabled, **Telemetry Dashboard** button in **Troubleshooting** window is available on the ThinOS client. You can click the button to open the **Telemetry Dashboard** and check device information and monitor the hardware usage.

Steps

1. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab and expand **System Settings**.
3. Click **Device Monitoring**.
4. Enable **Telemetry Dashboard**.
5. Set **Update Interval in seconds** for the hardware usage monitoring intervals.
6. Click **Save & Publish**.

NOTE: The Telemetry Dashboard content on the ThinOS client is more than the Wyse Management Suite server.

Configure Telegraf Agent package for WMS

Explains how to deploy and configure the Telegraf Agent package through WMS to enable system monitoring and performance metrics collection on ThinOS devices.

ThinOS users can use the Telegraf agent to effectively monitor ThinOS 10.x devices.

ThinOS admin can deploy the Telegraf Agent package using WMS/local APT tool.

The Telegraf agent is used for collecting monitor device performance (CPU, Memory and Ping Latency) and send metrics to a monitoring system like Prometheus.

Install Telegraf package through WMS

Prerequisites

- Ensure that you are running ThinOS10 25xx (10.00xx) on your device.
- The device must be registered to Wyse Management Suite.
- The user must have valid WMS login credentials.
- Valid Telegraf package.

About this task

To verify installation of the Telegraf package from the WMS, follow these steps:

Steps

1. Log in to **Wyse Management Suite**.
2. Go to the **Groups & Configs** page, and select a group.
3. From the **Edit Policies** drop-down menu, select **ThinOS10.X**.
   The **Configuration Control | ThinOS** window is displayed.
4. Go to **Advanced** > **Firmware** > **Application Package Updates**.
   Application Package Updates window is displayed.
5. Select **Browse** and upload the **Telegraf Agent package**.
   The user can upload the Telegraf Agent package.
6. Select the Telegraf package and click **Save & Publish**.
   The configurations are applied from the APT tool.
7. Go to the client page and verify if the Telegraf Agent package is downloaded and installed.
   Telegraf Agent package is downloaded and installed on the Client.
8. Click the **Telegraf Agent package** slider switch to enable the Telegraf Agent package.
   Once enabled, the following metrics are activated by default: CPU, Memory, Network, and Ping Latency. These metrics can be disabled individually.

   NOTE: The default Telegraf output configuration is set to **Prometheus** using port **9273** and metric version **2**.

   NOTE: The Telegraf feature is disabled is disabled by default.

Configure ControlUp

ControlUp helps you manage, monitor, and analyze virtual desktop interfaces and performance of applications.

To install the ControlUp VDI agent package using Wyse Management Suite, see Upload and push ThinOS 10.x application packages using Groups and Configs on Wyse Management Suite.

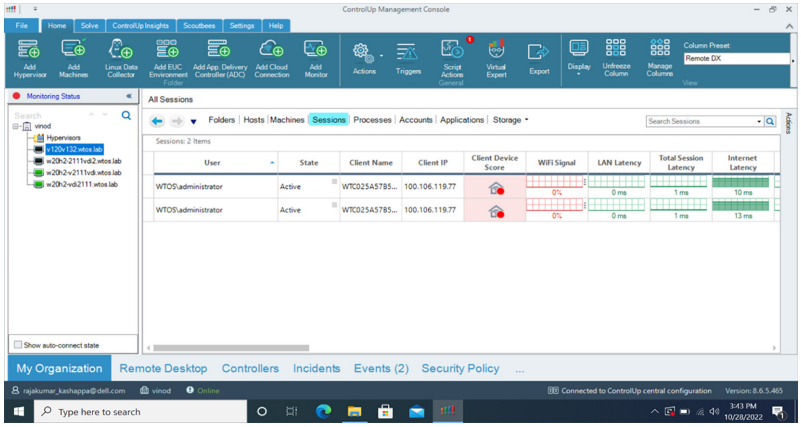

Figure 49. ControlUp Management Console

Configure Lakeside Virtual Agent

- A virtual machine running the Lakeside SysTrack agent is required, which is downloadable from your Lakeside cloud tenant.
- Ensure that the time zone must match with the client and VDA sessions before you install **Lakeside Virtual Agent** application package.
- To check the performance of the client, install the Lakeside virtual agent using Wyse Management Suite.

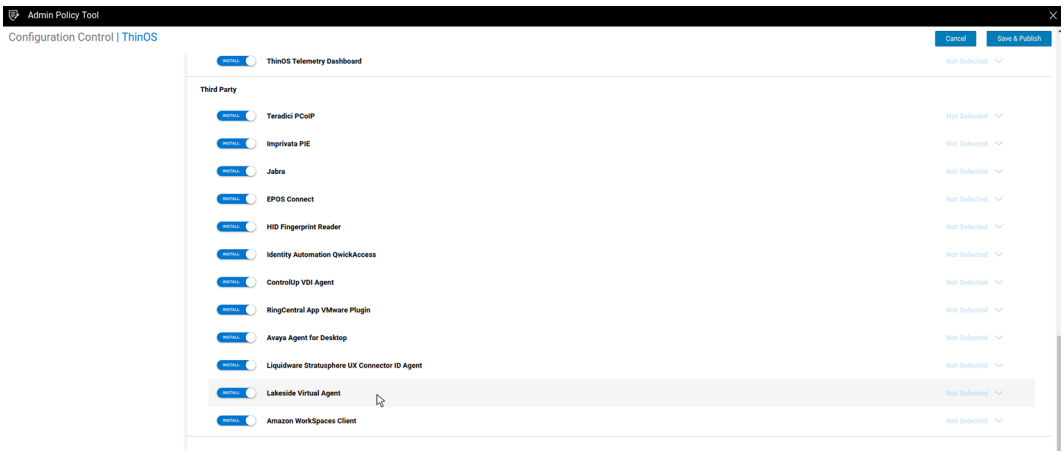

Figure 50. Lakeside virtual agent in Configuration Control

Figure 51. Lakeside Virtual Agent Dashboard

Configure UXM Endpoint Agent

- The UXM Endpoint agent package version is `uxm_Endpoint_Agent_2025.07.03.100_T10.pkg`.
- After enabling **UXM Endpoint Agent**, enter the appropriate values in **URL** and **Agent Key** fields for the date to be populated in the UXM site.

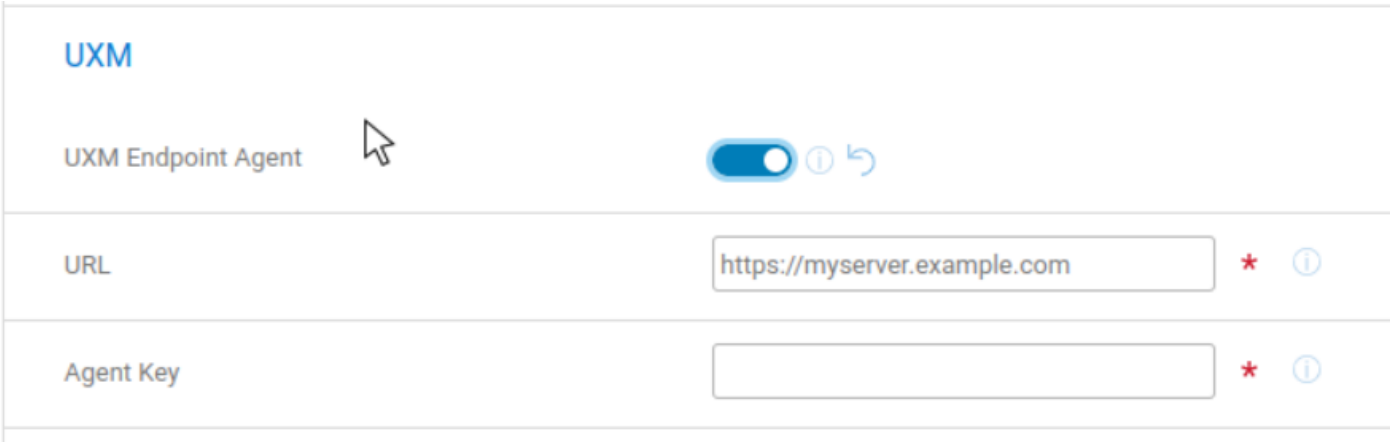

Figure 52. UXM Endpoint Agent

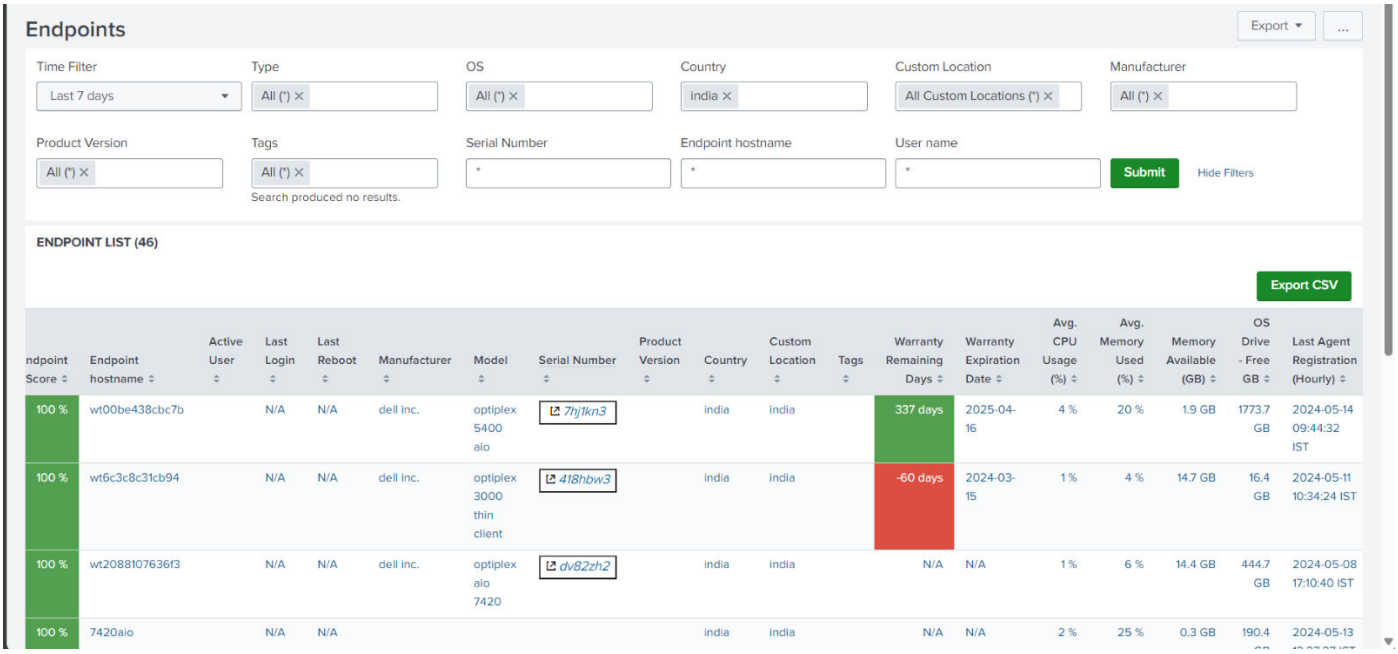

Figure 53. UXM Endpoint Agent server

Configure eG VM Agent

- The eG VM agent package version is `eG_VM_Agent_7.5.2.100_T10.pkg`.
- After enabling the eG Agent, enter the appropriate values in the **Dell ThinOS Client Group Name**, **Remote Agent or eG Manager IP / Name**, and **Remote Agent or eG Manager Port** fields for the date to be populated in the eG site.

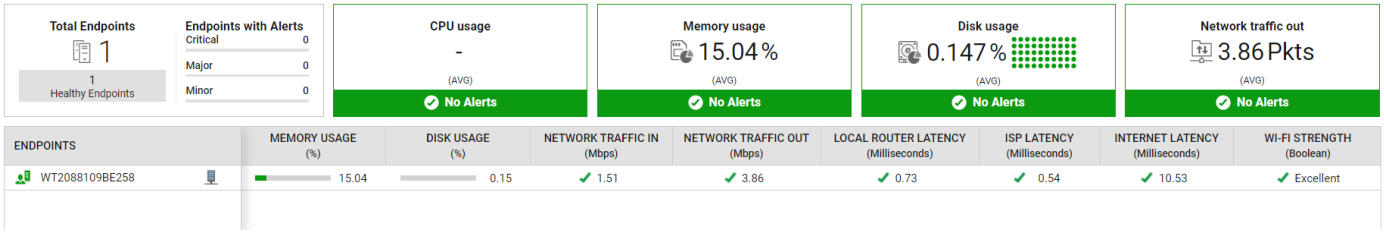

Figure 54. eG VM Agent dashboard

11

Configuring thin client local settings

You can configure the local settings on the thin client using the **System Preferences**, **Display**, **Peripherals**, and **Printer Setup** dialog boxes. Depending on the user privilege level, some dialog boxes and options may not be available for use.

Configuring the system preferences

Use the **System Preference** dialog box to select the system preferences such as screen saver, time/date, and custom information settings.

Configure the general system preferences

About this task

This section describes how to configure the general system settings on your thin client.

Steps

1. To access system preferences, do the following:
   - **Modern Mode**—from the desktop menu, click **System Settings** > **System Preferences**
   - **Classic Mode**—from the desktop menu, click **System Setup** > **System Preferences**

   The **System Preferences** dialog box is displayed.
2. Click the **General** tab, and do the following:

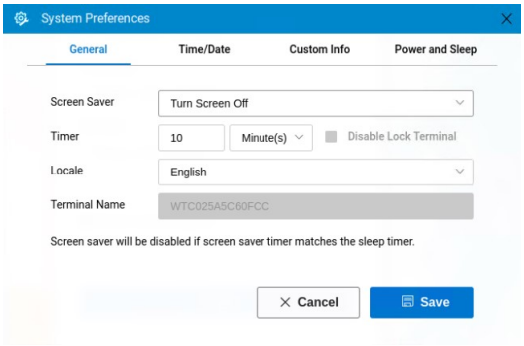

Figure 55. General tab

   a. From the **Screen Saver** drop-down list, select a screensaver for your device. The default value is set to **Turn Off Screen**.
   b. In the **Timer** box, select the idle time after which you want the screensaver to be activated on the thin client. When the thin client is left idle for the specified idle time, the screensaver is initiated. The default value is set to **10** minutes.
   c. From the **Locale** drop-down list, select a language to be activated for the user login-experience. The default language is set to **English**.
   d. In the **Terminal Name** box, view the default name fo the terminal. You cannot change the terminal name on ThinOS GUI.

   NOTE: **<space>**, **+**, **=**, **/**, ****, and **:** are not allowed in the **Terminal Name** field. You can use all other characters.

3. Click **Save** to save your settings.

Set the time and date

About this task

This section describes how to configure the time and date settings on your thin client.

Steps

1. To access system preferences, do the following:
   - **Modern Mode**—from the desktop menu, click **System Settings** > **System Preferences**
   - **Classic Mode**—from the desktop menu, click **System Setup** > **System Preferences**

   The **System Preferences** dialog box is displayed.
2. Click the **Time/Date** tab, and do the following:

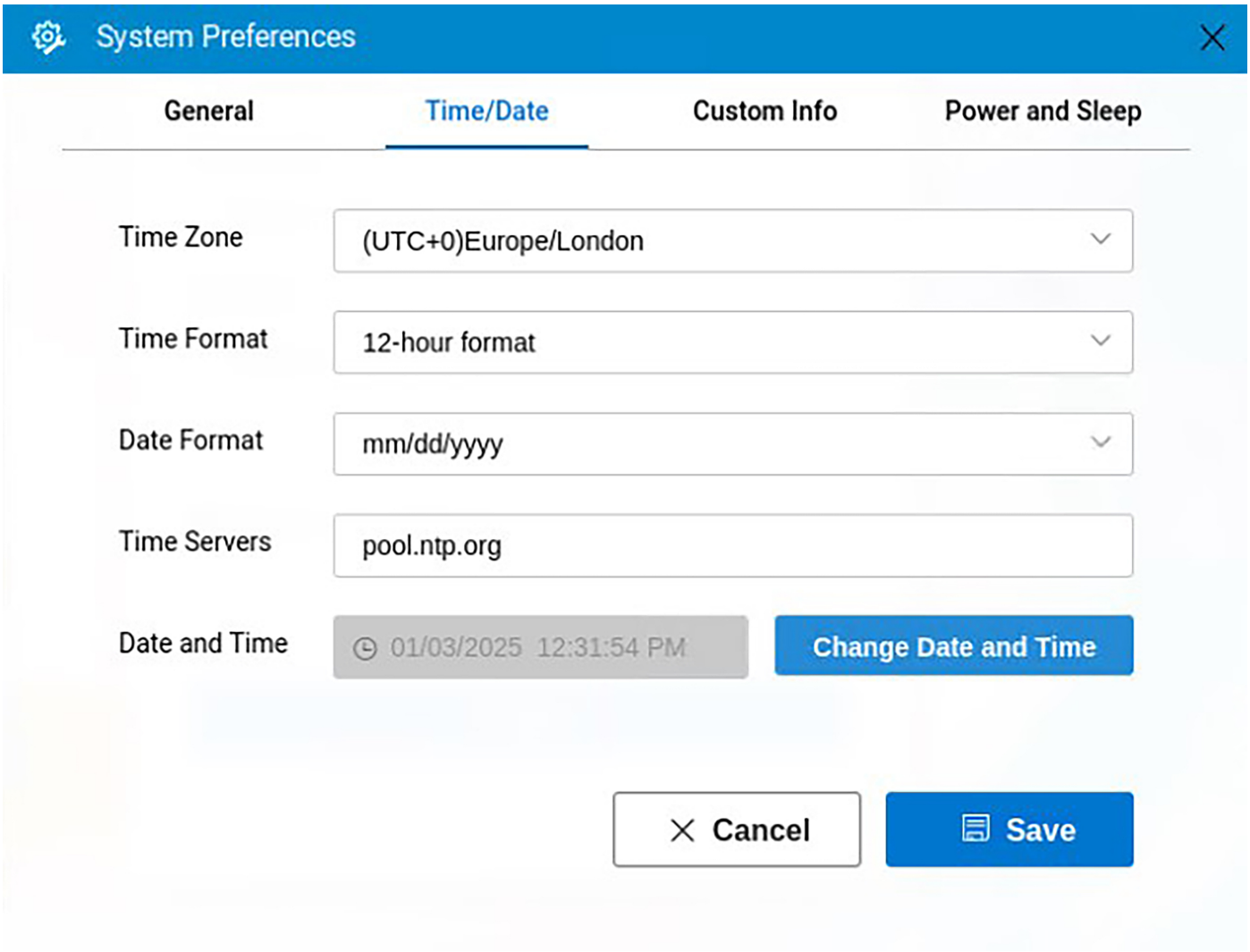

Figure 56. Time and date

   a. From the **Time Zone** drop-down list, select a time zone where the thin client operates.
   b. From the **Time Format** drop-down list, select either **12-hour time format** or **24-hour time format**.
   c. From the **Date Format** drop-down list, select a date format to be used for date and time representation.
   d. In the Time Servers field, enter the IP addresses or host names of the time server.

      The time servers provide the thin client time based on the settings of the time zone and daylight saving information. If DHCP is used, locations can be supplied through DHCP.
   e. Click the **Change Date and Time** button to change the date and time for secure environments.
3. Click **Save** to save your settings.

NOTE: You can enable or disable the privilege of end users to change the date or time. Go to the **Admin Policy Tool** or **Wyse Management Suite** policy settings **Advanced** > **Privacy & Security Account privileges**, and enable or disable the **Allow to change Time/Date from system bar** option.

Set the custom information

About this task

This section describes how to set the custom information about your thin client.

Steps

1. To access system preferences, do the following:
   - **Modern Mode**—from the desktop menu, click **System Settings** > **System Preferences**
   - **Classic Mode**—from the desktop menu, click **System Setup** > **System Preferences**

   The **System Preferences** dialog box is displayed.

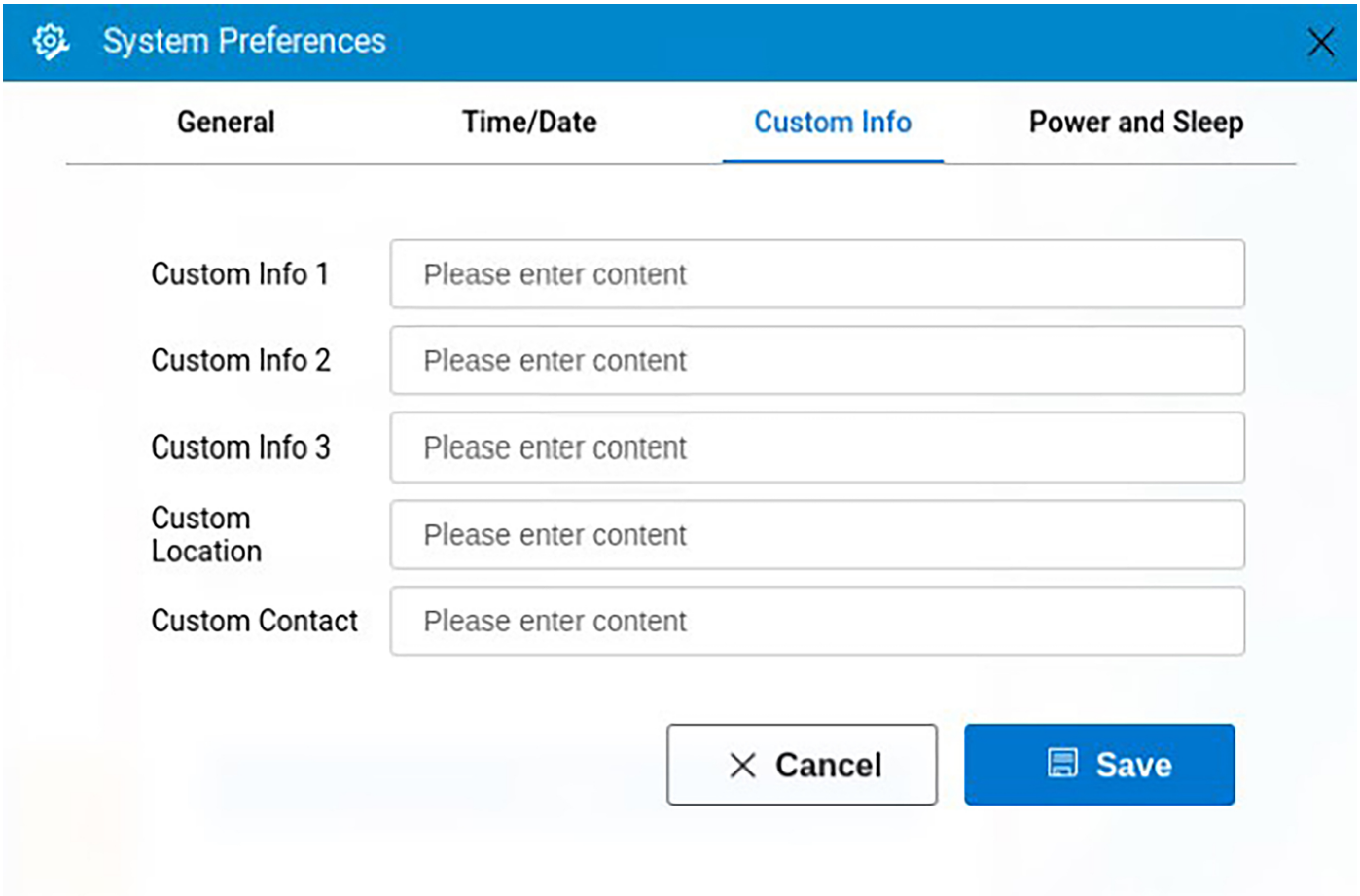

Figure 57. Custom information

2. Click the **Custom Info** tab to enter configuration strings used by the Wyse Management Suite software. The configuration strings can contain information about the location, user, administrator, and so on.
3. Click **Save** to save your settings.

   The custom field information is transferred to the Windows registry. The information is then available to Wyse Management Suite.

Configure power and sleep mode

About this task

This section describes how to configure the power and sleep mode.

Steps

1. To access system preferences, do the following:
   - **Modern Mode**—from the desktop menu, click **System Settings** > **System Preferences**
   - **Classic Mode**—from the desktop menu, click **System Setup** > **System Preferences**

   The **System Preferences** dialog box is displayed.
2. From the desktop menu, click **System Setup** > **System Preferences**.
   The **System Preferences** dialog box is displayed.
3. Click the **Power and Sleep** tab.

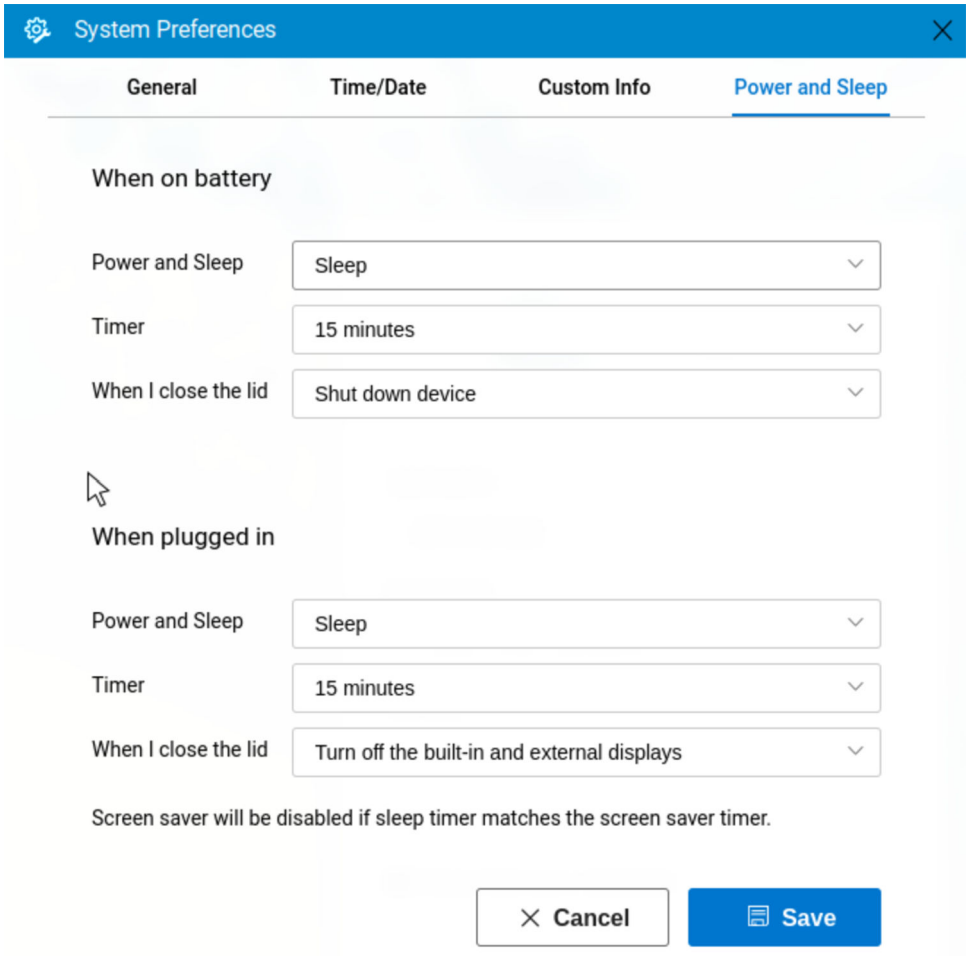

Figure 58. Power and Sleep

4. To set the power and sleep options when the thin client is on battery, change the following options in **When on battery**:
   a. From the **Power and Sleep** drop-down list, select **Power off** or **Sleep**.
   b. From the **Timer** drop-down list, select the duration for the thin client to be idle to enter sleep mode or power off.
   c. From the **When I close the lid** drop-down list, select any of the following options to set the behavior of the thin client when the lid is closed:
      - **Turn off the built-in display**—Turns off only the built-in display.
      - **Turn off the built-in and external displays**—Turns off all the displays that are connected to the thin client.
      - **Shut down device**—shuts down the thin client.

   NOTE: **Power and Sleep** > **When on battery** options are only available on mobile devices.

5. To set the power and sleep options when the thin client is plugged in, change the following options in **Power and Sleep** > **When plugged in**:
   a. From the **Power and Sleep** drop-down list, select **Power off** or **Sleep**.
   b. From the **Timer** drop-down list, select the duration for the thin client to be idle to enter sleep mode or power off.
   c. From the **When I close the lid** drop-down list, select any of the following options to set the behavior of the thin client when the lid is closed:
      - **Turn off the built-in display**—Turns off only the built-in display.
      - **Turn off the built-in and external displays**—Turns off all the displays that are connected to the thin client.
      - **Shut down device**—shuts down the thin client.

      NOTE: Power and Sleep > **When plugged in** > **When I close the lid** drop-down list is only available on mobile devices.
6. Click **Save** to save your settings.

Configuring the display settings

About this task

This section provides instructions for configuring the display settings for connected displays.

NOTE: In All-in-One and mobile devices, the integrated display stays on by default.

By default, the device uses the span mode if a new display is connected. When you change the display settings for the current display setup, the settings are saved. If you reconnect the same display, the device applies the saved monitor layout, including the disable monitor setting.

Steps

1. To access the display settings, do the following:
   - **Modern Mode**—from the desktop menu, click **System Settings** > **Display**
   - **Classic Mode**—from the desktop menu, click **System Setup** > **Display**

   The **Display Setup** dialog box is displayed.
2. In the **Display Setup** dialog box, configure any of following options:

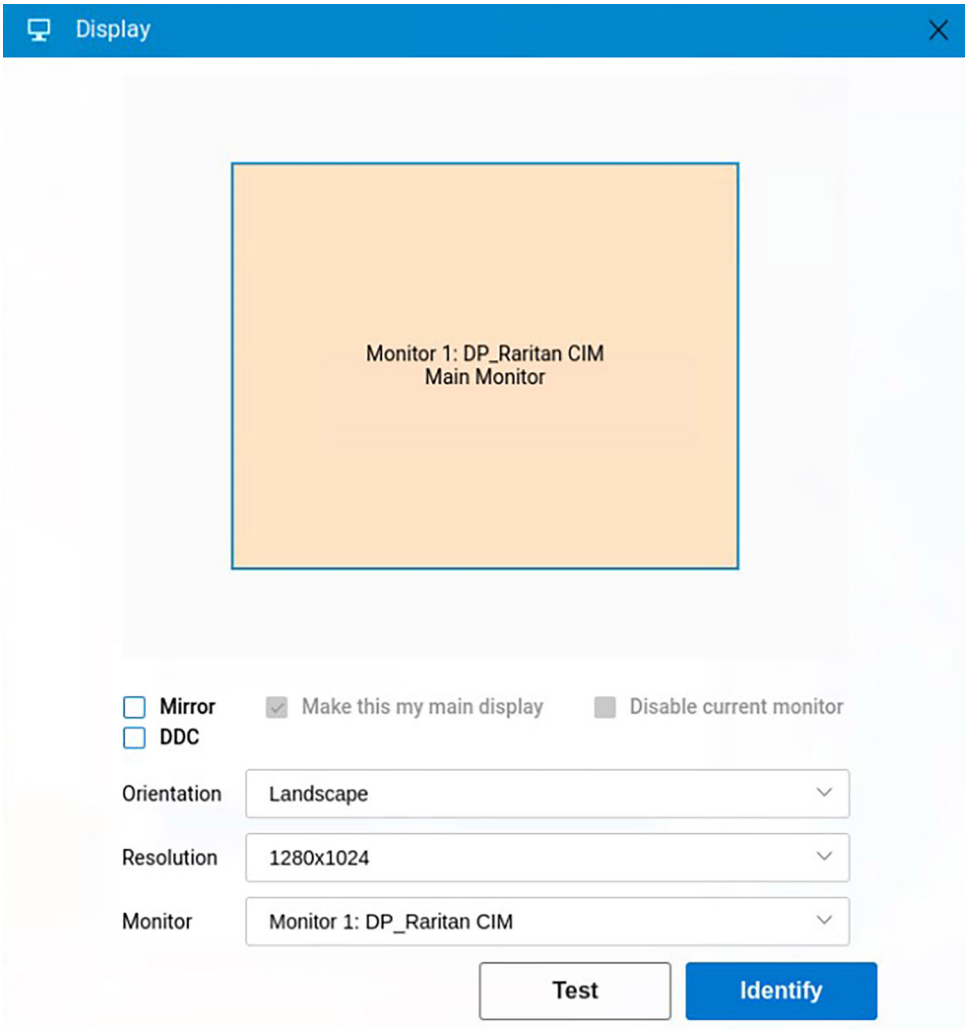

Figure 59. Display

- Select the **Mirror** check box to enable all connected displays to use the same display settings configured on the primary display.
- If you clear the **Mirror** check box, the **Span** mode is enabled.
- Blocks that are displayed on the screen represent the number of displays connected to the thin client. Each block represents a single display screen.

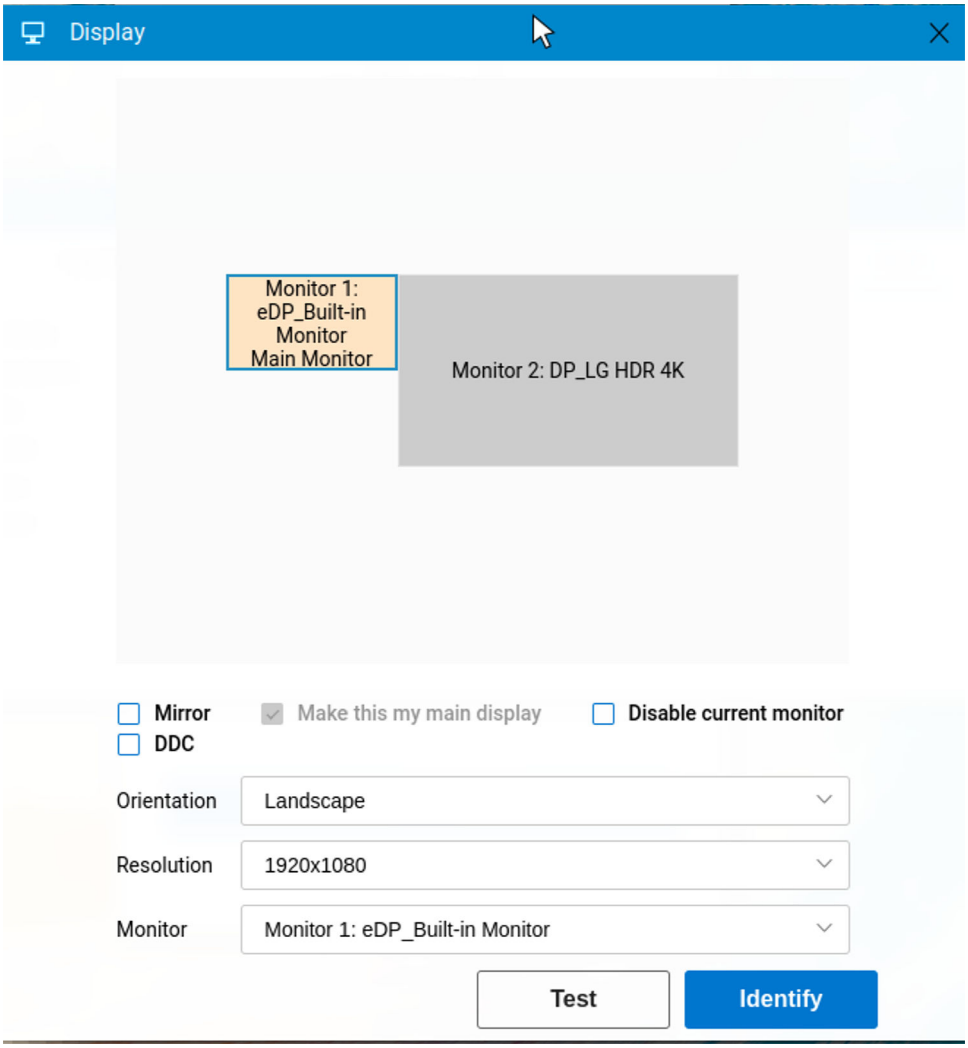

Figure 60. Dual display setup

- Every display contains a unique display order number and display configuration. You can move the blocks horizontally or vertically and construct the multidisplay layout in mixed directions. To construct a new display layout, move the blocks to your preferred position, and click **Apply**. A new display layout is created. However, when the block is moved to an incorrect position, the system sets the block to its default position.

NOTE: The Wyse 5070 Extended thin client supports up to six monitors. The Wyse 5470 Thin Client supports up to three simultaneous displays.

- Select the **Make this my main display** check box to set the display as primary display or the main screen. After you set the display as the main screen, the display block is displayed in yellow, and the **Make this my main display** option is disabled for that display block. The **Make this my main display** option is now available for other display blocks.

NOTE: The **Make this my main display** option is effective only in **Span Mode** and always disabled in **Mirror Mode**.

- Select the **Disable current monitor** check box if you want to disable a display. If you want to enable the disabled display, from the **Monitor** drop-down list, select the disabled monitor, and clear the **Disable current monitor** check box. Click the **Test** button and then click **OK**.
- From the **Orientation** drop-down list, select an option to rotate the display screen in different directions.
- From the **Resolution** drop-down list, select a supported display resolution.

NOTE: The default screen resolution on the Wyse 5470 Thin Client is 1366 x 768 or 1920 x 1080 depending on the configuration. The default screen resolution on the Wyse 5470 All-in-One Thin Client is 1920 x 1080.

  - In **Mirror Mode**, the resolution list is derived from the intersection of resolutions in all connected displays.

- In **Span Mode**, select a display block and change its resolution.
- From the **Monitor** drop-down list, select your preferred display.

3. Click **Test**.
   The new display settings are applied, and you can preview the modified display.
4. Click **Save** to confirm the new settings.

   Use the **Identify** option to know the display order number of the connected displays.

   Important Notes:
   - When connecting a monitor through Display Data Channel (DDC) with 800 x 600 and 640 x 480 resolution to the client, then 800 x 600 and 640 x 480 is listed on the resolution list of the display setup window.
   - If you change the USB-C Prioritization setting on the monitor, a black screen is displayed. You must reconnect the monitor to the device to restore the display.
   - ThinOS does not support the monitor HDR feature.
   - If you set a resolution that the monitor itself does not support, the monitor may display a black screen, or the display may not be correct. In this case, you must set a resolution that the monitor supports and reboot the device to recover.
   - If you connect monitors through the HDMI port, the monitors may not display anything after reboot. Turn on **Fast Wakeup** option on the monitors to avoid this issue.
   - The minimum resolution support for ThinOS 10.x is 1024 x 768.

Multi-Stream Transport (MST) or Daisy Chain

Multi-Stream Transport or Daisy Chain feature enables you to connect multiple external displays to your computer.

The following table displays the computers that support MST along with the maximum resolution that is supported when two or three monitors are connected:

Table 51. MST and maximum monitor resolution

System	Maximum resolution for two monitors	Maximum resolution for three monitors
Dell Pro 14 PC14250	Two 4K (3840 x 2160)	Three 2K (2560 x 1440)
Dell Pro 24 All-in-One QC24251	Two 4K (3840 x 2160)	Three 2K (2560 x 1440)
Dell Pro 16” Plus PB16250	One 4K (3840 x 2160) x one 2K (2560 x 1440)	Three 2K (2560 x 1440)

NOTE: DisplayPort and Type-C port supports MST, however, HDMI port does not support MST.

MST Limitations

- If you enable MST on monitors, display audio does not work.
- If you reboot with multiple monitors connected, one monitor may display a black screen. As a workaround, unplug and plug in the monitor that is connected to ThinOS.
- Do not hot-plug the daisy-chained monitors as this can cause a black screen issue. You can hot plug the monitor that is connected to the ThinOS client.
- If you connect two or three monitors with MST and plug out the monitors, ThinOS stops responding for 15 s to 30 s. When ThinOS stops responding, do not plug in the monitors again. Wait for ThinOS to recover and then plug in the monitors.

Using the On-Screen Display (OSD)

This section is applicable to Wyse 5470 All-in-One thin client.

Use the On-Screen Display (OSD) buttons on the right of the device to adjust the luminance of the backlight. Minimum is 1 and maximum is 100.

- Press and hold the first button from the top to increase brightness.
- Press and hold the second button from the top to decrease brightness.
- Press the third button from the top to turn off or turn on the screen.

Port preferences on the Wyse 5470 Thin Client

- HDMI, DisplayPort over USB Type-C, and USB Type-C ports are prioritized over the VGA port.
- When a USB Type-C display is present, there is no display on the VGA port.
- If a VGA display is present, a third display that is connected is prioritized and the VGA display is turned off.
- If a VGA display is not present, a third display that is connected is ignored, or a blank screen is displayed on the third screen.

Docking Stations

The following docks and computers are supported:

- **Dell Dock - WD19/WD19S/WD19TB(Thunderbolt port is not supported)**

  Table 52. Platforms that support WD19 and their maximum resolution

System	Maximum resolution for one monitor	Maximum resolution for two monitors	Maximum resolution for three monitors
Wyse 5470	4K 30 Hz	2 x (1920 x 1080)	Not Applicable
Latitude 3440	4K 30 Hz	2 x (2560 x 1440)	3 x (1920 x 1080)

- **Dell Thunderbolt Dock - WD22TB4**

  Table 53. Platforms that support WD22TB4 and their maximum resolution

System	Maximum resolution for one monitor	Maximum resolution for two monitors	Maximum resolution for three monitors
Latitude 5440/5450	4K 60 Hz	4K + (2560 x 1440)	3 x (2560 x 1440)

- **Limitations**
  - If multiple monitors are connected, display audio does not work.
  - Do not hot-plug monitors to the docking station as this causes a black screen issue. You can hot-plug the docking station instead.
  - HDMI port and Type-C port cannot support two monitors simultaneously. Only one of these ports can be used as a display device at a time.
  - If you connect two or three monitors to the docking station and plug out the docking station, ThinOS stops responding for 15 s or 30 s. When ThinOS stops responding, do not plug in the docking station again. Wait for ThinOS to recover and then plug in the docking station.
  - If the default resolution of the monitors on the docking station is larger than the maximum supported resolution, the ThinOS client stops responding. For example, if you connect three monitors with default resolution of 4 K with a WD19S dock and then connect the dock to Latitude 3440, the client stops responding.
  - ThinOS only supports one external network port. If there is a network port on the monitor and you connect the monitor to a docking station with type-C cable, the network port on the monitor works. But, the network port on the dock does not work.

Vertical Synchronization

Vertical Synchronization or V-Sync enables the ThinOS client to synchronize the frame rate of a video with the monitor refresh rate to avoid screen tearing. Screen tearing occurs when the graphic processor delivers display frames more than your monitor can process. As a result, the image appears to be cut in half. Enabling VSync synchronizes the output video of the graphics card to the refresh rate of the monitor. V-Sync is enabled by default on ThinOS. V-Sync cannot be disabled in ThinOS 10.x.

Configure the external touch screen settings

Dell Technologies recommends that you use the default resolution while using touch screen. If you use a custom resolution, the touch screen does not calibrate accurately. By default, the touch monitor Dell P2418HT is supported. To use other touch screen monitors, you must configure the **Bind Touch and Monitor** settings either using Admin Policy Tool or Wyse Management Suite.

Steps

1. Connect the touch monitor to the ThinOS client.

   NOTE: You must connect the uplink cable to use the touch screen.

2. Go to **System Information** > **Event Log** and locate the information for the touch monitor. For example, screen1 [0xac10, 0x4114], Touchscreen [0x1fd2, 0x6103].
3. Open the Admin Policy Tool on the ThinOS client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
4. On the **Advanced** tab, expand **Peripheral Management** and click **Touch**.
5. In the **Bind Touch and Monitor** section, click **Add Row**.
6. Specify the screen device ID. For example, ac104114.
7. Specify the touch device ID. For example, 1fd26103.
8. Click **Save & Publish**.

   NOTE: Dell recommends that you use a direct DisplayPort, an HDMI, or a VGA cable for connecting the touch monitor and the thin client. If you are using a convertor, the touch function may not work by default. However, it can work after you configure the **Bind Touch and Monitor** settings either using Admin Policy Tool or Wyse Management Suite.

Configuring the external touch screen settings for VDI sessions

When you connect a touch monitor to the ThinOS client using a USB port, you must configure the settings in the **Global Connection Settings** window.

- **Citrix session**—To use a touch monitor in a Citrix session, do the following:
  1. On the ThinOS client, from the desktop menu, click **Connect Manager**.
  2. Click **Global Connection Settings**.
  3. Clear the **USB devices redirection** check box and click **OK**.
  4. Start the Citrix session.
- **Other VDI sessions**—You do not have to modify the USB devices redirection setting. Connect the touch monitor to the ThinOS client and start the VDI session.

Configuring Touch Screen settings for AIO Devices in VDI sessions

To ensure that the touch screen on an All-In-One (AIO) device functions correctly inside a VDI session, you must redirect the touch input device using vUSB Force Local within the WMS or APT configuration.

Steps

1. Go to **Peripheral Management**.
2. Navigate to **USB Redirection**.
3. Open **USB Redirection Settings**.
4. Locate the **vUSB Force Local** section.
5. Click **Add Row**.
6. Add the Vendor ID and Product ID (VID/PID) of the touch device in the following format:
   0xVVVVPPPP

   Example: Dell OptiPlex 7410 AIO For the Dell 7410 AIO touch screen, add the following entry to vUSB Force Local:

   0x29bd9302

   This forces the touch screen HID device to stay local on the client instead of redirecting into the VDI session, ensuring proper touch functionality.

Configuring the peripherals settings

Use the **Peripherals** dialog box to configure the settings for the keyboard, mouse, audio, serial, camera, and Bluetooth.

Configure the keyboard settings

About this task

This section describes how to configure the keyboard settings on your thin client.

Steps

1. To access the peripherals settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals** > **.**

   The **Peripherals** dialog box is displayed.
2. Click the **Keyboard** tab, and do the following:
   a. From the **Keyboard Layout** drop-down list, select a keyboard layout. The default layout is set to **English (United States)**.

      NOTE: Support for Macedonian, Macedonian – Standard, Belgian, and Belgian (Comma) keyboard layouts are added in the ThinOS 10.x release. You can also use the Admin Policy Tool or the Wyse Management Suite policy settings to configure the keyboard layout. To configure the settings using Admin Policy Tool or Wyse Management Suite, on the Advanced Tab, go to **Peripherals Managements** > **Keyboard** and select the preferred **Keyboard Layout**. Blast session does not support Macedonian, Macedonian – Standard, Belgian, and Belgian (Comma) keyboard layouts.

   b. From the **Delay before Repeat** drop-down list, select the time for Repeat Delay. The time specifies the pause between pressing the key on the keyboard and when the key starts repeating itself.
   c. Click any of the following options to set the **Repeat Rate**:
      - **Slow**
      - **Normal**
      - **Fast**

      Repeat Rate specifies the speed at which the key repeats itself after you press and hold down a key on the keyboard.
   d. Click any of the following options to set the **Numlock** status:
      - **None**
      - **On**
      - **Off**

      Numlock specifies whether the Numlock key on the keyboard must be turned on or turned off when you boot the terminal.
   e. In the **Disabled keys** field, enter the keys on the keyboard that must be disabled. Use a comma to separate multiple entries.

      NOTE: The setting only supports disabled keys a to z, 0 to 9, and PrintScreen/WIN key on standard keyboards that do not include the numeric keyboard.
3. Click **Save** to save your settings.

Function key combinations

The Wyse 5470 Thin Client supports the following Function (Fn) key combinations:

Table 54. Fn key combinations

Key	ThinOS Local	ICA session
Fn + Esc	Fn lock/unlock	Fn lock/unlock
Fn + F1	Mute	Not supported
Fn + F2	Volume down	Not supported
Fn + F3	Volume up	Not supported
Fn + F4	Not applicable—session only	Not supported
Fn + F5	Not applicable—session only	Not supported

Table 54. Fn key combinations (continued)

Key	ThinOS Local	ICA session
Fn + F6	Not applicable—session only	Not supported
Fn + F7	Not applicable	Not applicable
Fn + F8	Opens the ThinOS local display settings window	Not applicable
Fn + F9	Not supported	Not supported
Fn + F10	Keyboard light	Not applicable—ThinOS local only
Fn + F11	Screen dimming	Not applicable—ThinOS local only
Fn + F12	Screen lighting	Not applicable—ThinOS local only
Fn + Ctrl	Right-click mouse	Not supported
Fn + PrtScr	Disable wireless device	Not applicable—ThinOS local only
Fn + Right arrow	Go to the end of the page	Go to the end of the page
Fn + Left arrow	Go to the home page	Go to the home page
Fn + Up arrow	Page up	Page up
Fn + Down arrow	Page down	Page down
Fn + Insert	Sleep mode	Not applicable - ThinOS local only

Latitude 3420, 3440, 5440 devices support the following Function key combinations:

Table 55. Fn key combinations

Key	ThinOS Local	ICA session
Fn + Esc	Fn lock/unlock	Fn lock/unlock
F1	Mute	Not supported
F2	Volume down	Not supported
F3	Volume up	Not supported
F4 (Not supported on Latitude 3420)	Mute microphone	Not supported
F5	Keyboard backlight	Not applicable-ThinOS local only
F6	Screen dimming	Not applicable-ThinOS local only
F7	Screen lighting	Not applicable-ThinOS local only
F8	Opens the ThinOS local display settings window	Not applicable
F9	Not supported	F9
F10	Print Screen	Print Screen
F11	Home	Home
F12	End	End
Fn + Ctrl	Right-click mouse	Not supported
Fn + Up arrow	Page up	Page up
Fn + Down arrow	Page down	Page down

Switch the keyboard layout

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Peripheral Management**, and click **Keyboard**.
4. From the **Keyboard Layout** drop-down list, select a few keyboard layouts.
5. Click **Save & Publish**.
   A **Keyboard Layout** icon is displayed on the taskbar or the floating bar.
6. Click the **Keyboard Layout** icon.
   The **Keyboard Layout** list is displayed.
7. Select a keyboard layout from the list.

   The keyboard layout icon changes after you select the keyboard layout.

   Alternatively, you can use the assigned shortcut keys to display the keyboard layout list or switch between the keyboard layouts.

Use shortcut keys for keyboard layout switching

Prerequisites

Select a few keyboard layouts from the Wyse Management Suite policy settings or the Admin Policy Tool. For more information, see Switch the keyboard layout.

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Personalization**, and click **Shortcut Keys**.
4. Enable the **Enable Switch Keyboard Layout - Quick Selection** option under **Switch Keyboard Layout - Quick Selection**.
5. Select your preferred shortcut key from the **Switch Key** drop-down list.
6. Enable the **Enable Switch Keyboard Layout - Show List** option under **Switch Keyboard Layout - Show List**.
7. Select your preferred shortcut key from the **Switch Key** drop-down list.
8. Click **Save & Publish**.

   You can use the shortcut keys to either switch between the keyboard layouts on the thin client or to display the **Keyboard Layout** list.

Use On-Screen Keyboard

Enable On-Screen Keyboard settings in ThinOS

Prerequisites

Valid WMS credentials must be available.

About this task

Follow these steps to verify the behavior of the Enable On-Screen Keyboard setting in ThinOS:

Steps

1. Log in to WMS or APT.
2. Go to **Settings** > **ThinOS 10.x** > **Advanced** > **Peripheral Management** and select **Keyboard**.

The **Keyboard Settings** page opens.

3. Go to **On-Screen Keyboard Settings**.

   NOTE: The **Enable On-Screen Keyboard** is disabled by default.

4. Turn on the **Enable the On-Screen Keyboard** to enable it.
   The On-Screen Keyboard icon position appears as the **taskbar**.
5. Verify that the On-Screen Keyboard icon position appears as the **taskbar** (which is the default icon position). Ensure that the **Float** option is available in the drop-down menu.
6. Verify the functionality of minimize, maximize, and cancel or close buttons on the On-Screen Keyboard.
7. Go to the Client page and click **On-Screen keyboard** > **Restart**.
   On-Screen Keyboard icon is displayed on the taskbar.
8. Go to the Client page and click **On-Screen keyboard** > **Soft reset**.
   On-Screen Keyboard icon is displayed on the taskbar.

Verify ThinOS 10.x On-Screen Keyboard configuration and functionality as a taskbar

Prerequisites

- Valid WMS credentials must be available.
- ThinOS client must be ready.

About this task

Follow these steps to verify the behavior of Enable On-Screen Keyboard as a taskbar:

Steps

1. Log in to toWMS or APT.
2. Go to **Settings** > **ThinOS 10.x** > **Advanced** > **Personalization** and select **User Experience Settings**.
3. Set the System Mode to **Classic Mode**.
   The client device must reflect the **Classic Mode** user interface and settings after synchronization.
4. Go to **Advanced** > **Peripheral Management** > **Keyboard** > **Enable On-Screen Keyboard** > **Set the On-Screen Keyboard icon position to Taskbar** and click **Save and Publish**.
   The configuration also gets saved and applied to the client device which you can verify in APT.
5. Go to the Client page and verify if the On-Screen Keyboard icon appears on the Taskbar of the ThinOS client.
   On-Screen Keyboard icon is displayed on the taskbar indicating that the keyboard feature is enabled.
6. Double-click the On-Screen Keyboard icon on the taskbar and verify that the On-Screen Keyboard is displayed on the screen.
   The On-Screen Keyboard appears when the icon is double-clicked. It is ready for use and appears over the current window.
7. Ensure that the following tabs on the On-Screen Keyboard are functioning correctly.
   a. **Search**
   b. **Troubleshooting**
   c. **Network setup**
   d. **Remote connection**
   e. **Central configuration**
   f. **Peripherals**
   g. **Printer setup**
   h. **Login Window**

Verify ThinOS 10.x On-Screen Keyboard configuration and functionality for Floatbar

Prerequisites

- Valid WMS credentials must be available.
- ThinOS client must be ready.

About this task

Follow these steps to verify the behavior of Enable On-Screen Keyboard with TaskBar.

Steps

1. Log in to WMS or APT.
2. Go to **Settings** > **ThinOS 10.x** > **Advanced** > **Personalization** and select **User Experience Settings**.
3. Set the System Mode to **Classic Mode**.
   The client device must reflect the **Classic Mode** user interface and settings after synchronization.
4. Go to **Advanced** > **Peripheral Management** > **Keyboard** > **Enable On-Screen Keyboard** > **Set the On-Screen Keyboard icon position to Floatbar** and click **Save and Publish**.
   The configuration also gets saved.
5. Go to the Client page and verify if the On-Screen Keyboard icon appears on the Floatbar of the ThinOS client.
   On-Screen Keyboard icon is displayed on the Floatbar indicating that the keyboard feature is enabled.
6. Double-click the On-Screen Keyboard icon in the Taskbar and verify that the On-Screen Keyboard is displayed on the screen.
   The On-Screen Keyboard appears over the current window when the icon is double-clicked and ready for use.
7. Test and ensure that the following tabs on the On-Screen Keyboard are functioning correctly.
   a. **Search**
   b. **Troubleshooting**
   c. **Network setup**
   d. **Remote connection**
   e. **Central configuration**
   f. **Peripherals**
   g. **Printer setup**
   h. **Login Window**

   All the keys (letters, numbers, and special characters) are functional. The keyboard interacts seamlessly with each tab and input in all fields are validated correctly.

Enable the On-Screen Keyboard and verify functionality inside the browser

Prerequisites

- Valid WMS credentials.
- Availability of ThinOS client.
- Browser package installed in the client.

About this task

Follow these steps to verify the behavior of On-Screen Keyboard inside the browsers:

Steps

On-Screen Keyboard as taskbar:

1. Go to **WMS** > **Settings** > **ThinOS 10.x** > **Advanced** > **Peripheral Management** > **Keyboard** > **On-Screen Keyboard Settings** and enable the **On-Screen Keyboard**.
2. Select **taskbar** in the On-Screen Keyboard icon position drop-down menu.

3. Click **Save and Publish**.
   The **On-Screen Keyboard** is successfully enabled, and the On-Screen Keyboard icon is positioned on the Taskbar on the ThinOS client.
4. Go to the client side and verify that the configuration is applied in APT.
   The ThinOS client receives the configuration from WMS verification in APT.
5. Check if the On-Screen Keyboard icon appears on the Taskbar.
   The On-Screen Keyboard icon is displayed on the Taskbar.
6. Click the On-Screen Keyboard icon and verify that the On-Screen Keyboard is displayed.
   The On-Screen Keyboard icon is displayed on the screen, and the keyboard appears as an overlay above the active window ready for input.
7. Launch the browser (for example, Chrome or FireFox).
   The browser launches successfully. The user is connected to the virtual desktop or application. The On-Screen Keyboard remains accessible in the browser.
8. Verify the On-screen keyboard keys inside the browser.

   The On-Screen Keyboard must function as expected inside the browser. All keys including letters, numbers, and special characters must be responsive and functional for text input in any fields within the browser.

On-Screen Keyboard as float:

9. Go to **WMS** > **Settings** > **ThinOS 10.x** > **Advanced** > **Peripheral Management** > **Keyboard** > **On-Screen Keyboard Settings** and enable the **On-Screen Keyboard**.
10. Select **float** in the On-Screen Keyboard icon position drop-down menu.
11. Click **Save and Publish**.
    The **On-Screen Keyboard** is successfully enabled, and the On-Screen Keyboard icon is positioned as a Float on the ThinOS client. The configuration change is saved and successfully published to the ThinOS client.
12. Go to the client side and verify that the configuration is applied in APT.
    All configuration updates must reflect in APT as well.
13. Check if the On-Screen Keyboard icon appears as Float.
    The On-Screen Keyboard icon is displayed as a floating icon on the screen. This icon can be moved around the workspace, and is not fixed on the Taskbar.
14. Click the On-Screen Keyboard icon and verify that the On-Screen Keyboard is displayed.
    The floating On-Screen Keyboard icon is displayed on the screen. The keyboard appears as an overlay, floating freely, and ready for input.
15. Launch the browser (for example, Chrome or FireFox).
    The browser must start without any issues. The On-Screen Keyboard continues to be available for use within the browser.
16. Verify the On-screen keyboard keys inside the session.

    The On-Screen Keyboard must function as expected inside the browser as a floating icon. All keys including letters, numbers, and special characters must be responsive and functional for text input in any fields within the session.

Enable the On-Screen Keyboard with different keyboard layouts

Prerequisites

- Valid WMS login credentials.
- Availability of ThinOS client with different keyboard layouts.

About this task

Follow these steps to verify the On-Screen Keyboard with different keyboard layouts from WMS:

Steps

1. Log in to WMS or APT.
2. Go to **Settings** > **ThinOS 10.x** > **Advanced** > **Peripheral Management** > **Keyboard** > **On-Screen Keyboard Settings** and enable the **On-Screen Keyboard**.
   The On-Screen Keyboard is successfully enabled and is available as an input option when users log in.
3. Select **taskbar** in the On-Screen Keyboard icon position drop-down menu.
4. Click **Save and Publish**.

The **On-Screen Keyboard** is successfully enabled, and the On-Screen Keyboard icon is positioned on the Taskbar on the ThinOS client.

5. Go to **Keyboard settings** > **Keyboard layout list** > **Select the keyboard layout list** and click **Save and Publish**.

   NOTE: The user is allowed to navigate to the keyboard layout list and select a keyboard layout.

6. Verify the selected keyboard layout in On-Screen Keyboard and type some keys in the text field.
   The typed text must align with the selected keyboard layout.

Enable the On-Screen Keyboard with multiple monitors

Prerequisites

- Valid WMS login credentials.
- Two monitors with ThinOS client.

About this task

Verify multimonitor setup with On-Screen Keyboard.

Steps

1. Image the ThinOS 2505 device and connect to two monitors.
   The ThinOS 2505 image is successfully installed.
2. Go to **APT** > **Settings** > **ThinOS 10.x** > **Advanced** > **Peripheral Management** > **Keyboard** > **On-Screen Keyboard Settings** and enable the **On-Screen Keyboard**.
   You must be able to successfully access the keyboard settings section in ThinOS. The On-Screen Keyboard is enabled and now available for use on the touch-screen device.
3. Select **taskbar** in the On-Screen Keyboard icon position drop-down menu.
4. Click **Save and Publish**.
   The **On-Screen Keyboard** is successfully enabled, and the On-Screen Keyboard icon is positioned on the taskbar on the ThinOS client.
5. Click and drag **On-Screen Keyboard** to the second monitor.
   You will be able to drag the **On-Screen Keyboard** to the second monitor.
6. Now disconnect the second monitor from the device.
   Upon disconnecting the second monitor, the **On-Screen Keyboard** moves to the primary monitor.

Configure the mouse settings

About this task

This section describes how to configure the mouse settings on your thin client.

Steps

1. To access the peripherals settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals** > **.**

   The **Peripherals** dialog box is displayed.
2. Click the **Mouse** tab, and do the following:
   a. To increase or decrease the mouse speed, move the **Mouse Speed** slider either to the right or left.
   b. From the **Pointer size** drop-down list, select a value to increase the size of the local mouse pointer. Restart the computer for the change in pointer size to take effect.
   c. Select the **Swap left and right mouse buttons** check box if you want to swap the mouse buttons for left-handed operations.
   d. Select the **Reverse mouse wheel scroll direction** check box if you want to invert the direction of the mouse scroll wheel.
3. Click **Save** to save your settings.

Configure the touchpad settings

About this task

This section describes how to configure the touchpad settings on the Wyse 5470 Thin Client.

Steps

1. To access the peripherals settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals** > **.**

   The **Peripherals** dialog box is displayed.
2. Click the **Touchpad** tab, and do the following:
   a. To increase or decrease the mouse speed, move the **Touchpad Speed** slider either to the right or left.
   b. Select the **Swap left and right touchpad buttons** check box if you want to swap the touchpad buttons for left-handed operations.
   c. Select the **Reverse touchpad wheel scroll direction** check box if you want to invert the direction of the touchpad scroll wheel.
   d. Select the **Disable touchpad** check box if you want to disable the touchpad on the device.
   e. Click the **Enable Timeout** toggle switch if you to disable the touchpad while typing using the integrated keyboard.

   NOTE: When **Enable timeout** is enabled, touchpad movement is disabled for sometime after a key is used on the keyboard, except Ctrl, Alt, and Shift keys. When **Enable timeout** is disabled, the touchpad always works.

   NOTE: When **Enable timeout** is enabled, touchpad movement is disabled for sometime after a key is used on the keyboard, except Ctrl, Alt, and Shift keys. When **Enable timeout** is disabled, touchpad movement is disabled for sometime after a key is used on the keyboard, except function keys.
3. Click **Save** to save your settings.

Touchpad gestures

This section is only applicable to mobile thin clients.

The touchpad on mobile thin clients contain two buttons for the right and left mouse-clicks. The following table lists the supported touchpad gestures on mobile thin clients:

Table 56. Touchpad gestures

Touchpad gesture	Additional information
Moving the mouse cursor	Moving with one finger, the entire touchpad including the area with the buttons can be used for the mouse cursor movement. **NOTE:** The sensitivity of the cursor movement on the area with the buttons is slower compared to the other areas. This design is for the stability of the buttons.
Left-click	• Tapping with one finger anywhere on the touchpad works as the mouse left-click. • Pressing the left button on the touchpad works as the mouse left-click.
Right-click	• Tapping with two fingers anywhere on the touchpad works as the mouse right-click. • Pressing the right button on the touchpad as the mouse right-click.
Double-click	• Tapping two times with one finger anywhere on the touchpad works as the mouse double-click. • Pressing the left button twice on the touchpad works as mouse double-click.
Moving windows	• Press and hold the left button, and move the window by dragging a second finger on the touchpad. • Dragging a window by tapping twice on the touchpad with one finger.
Zoom	Placing two fingers on the touchpad and pinching or stretching out—Not supported.
Scroll	Tapping two fingers and moving up or down.

Configure the audio settings

About this task

This section describes how to configure the audio settings on your thin client:

Steps

1. To access the peripheral settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals** > **.**

   The **Peripherals** dialog box is displayed.
2. Click the **Audio** tab, and do the following:
   a. From the **Playback Devices** drop-down list, select the type of the audio device.
      - Move the **slider** either to the right or left to control the volume settings for playback devices.
      - Select the **Mute** check box to mute the audio.
      - Select the **Speaker** check box to enable the onboard speaker.

   b. From the **Recorded Devices** drop-down list, select the type of the record device.
      - Move the **slider** either to the right or left to control the volume settings for record devices.
      - Select the **Mute** check box to mute the audio.

   c. Use the **Recorder** tab to collect information about the speaker and microphone being used. You can examine the performance of the speaker and microphone being used.

   NOTE: When the manual override option is enabled, the audio devices that are manually selected take priority. Audio devices remain selected after you reboot the device.
3. Click **Save** to save your changes.

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.

Set default playback or recording devices

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Peripheral Management**, and click **Audio**.
4. Enter playback devices in the **Playback Device** field, each device separated by **;** symbol.
5. Enter recording devices in the **Recording Device** field, each device separated by **;** symbol.
6. Click **Save & Publish**.
7. Restart the thin client for the changes to take effect.

Behavior examples when connecting multiple devices

Table 57. Behavior examples when connecting multiple devices

Setup	Behavior
Set one device name in the list.	If the mentioned device is plugged in, it is selected. If the device is plugged out, the HD audio is selected.
Set one random name in the list. **NOTE:** Here the term random name denotes the name of a manufacturer that you can enter. For example, if you	If a device with the random name is plugged in, then it is selected. If another device with the random name is plugged in, the first device remains selected. The second device is

Table 57. Behavior examples when connecting multiple devices (continued)

Setup	Behavior
give the random name as Jabra, then a connected device that contains the word Jabra in its name can work.	selected after the first device is plugged out. If the second device that is connected is not with a random name, then the HD audio gets selected after the first device is plugged out.
Set two device names in the list.	If a device with the first name in the list is plugged in, then it is selected. If another device with the second name in the list is plugged in, the first device remains selected. The second device is selected after the first device is plugged out.

Configure the serial settings

About this task

This section describes how to configure the serial settings on your thin client.

Steps

1. To access the peripherals settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals** > **.**

   The **Peripherals** dialog box is displayed.
2. Click the **Serial** tab and do the following:
   a. Click any of the **Select Port** options to select a COM port. The default port is set to **COM 1**.
   b. From the **Baud Rate** drop-down list, select the Baud Rate. The Baud rate specifies the number of signal changes that occur per second. The default value is 9600.
   c. Click any of the **Parity** options to set the parity property for the serial port connection.
   d. Click any of the **Stop** options to set the stop bits for the serial port connection. The default value is 1.
   e. Click any of the **Size** options to set the character size for the serial port connection. The default value is 8.
   f. Click any of the **Flow Control** options to set the flow control of bytes in the serial port connection.
3. Click **Save** to save your settings.

Select a starting serial port number

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Peripheral Management**, and click **Serial Port**.
4. Select a serial port number from the **Serial Port Start Number** drop-down list.

   The selected serial port number is considered as the first serial port regardless of the USB port that is being used. If the option is not configured, the serial port numbers are configured according to the USB port numbers.
5. Click **Save & Publish**.
6. Restart the thin client.

Remap a serial port number

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Peripheral Management**, and click **Serial Port**.
4. Enter a pseudonym in the **Remap Serial Port** field.

   The local serial ports can be used with a pseudonym in a Citrix Session.

5. Click **Save & Publish**.
6. Restart the thin client.

Configure the camera device

About this task

This section describes how to enable the camera that is connected to your thin client. When using the HDX RealTime Webcam Video Compression feature of Citrix Virtual Apps and Desktops, you can control options such as resolution and frames per second. The feature works only in Citrix. MJPEG format is supported.

Steps

1. To access the peripherals settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals** > **.**

   The **Peripherals** dialog box is displayed.
2. Click the **Camera** tab.

   By default, **Optimize for CPU** is enabled. The recommended settings for camera format, resolution, and FPS are automatically set. The default settings are **`format=RAW`**, **`resolution=320X240`**, and **`FPS=10`**.

   NOTE: Disable the **Optimize for CPU** option to customize the camera format, resolution, and FPS settings. Only the supported resolution and FPS of the connected camera is displayed in the drop-down list for resolution and frames per second. Increasing the resolution and FPS impacts the performance.
3. From the **Device** drop-down list, select a camera device that is connected to your thin client.
4. Click **Preview**.
   The camera is turned on, and you can see yourself or whatever the camera is pointed at.
5. Click **Stop** to stop the camera preview.
6. Click **Save** to save your settings.

   NOTE: In the current release, only the RAW format of camera is supported. MJPEG format is not supported. The switch camera function from **ThinOS Peripherals** > **Camera** works only in the ThinOS client. It does not work in the Citrix VDA.

   For Wyse 5470 and Wyse 5470 All-in-One thin clients, the integrated camera on the thin client does not support hardware encoding, so the performance is limited.

   For example, on the Wyse 5470 Thin Client with RTME-enabled, the camera performance on Skype for Business is limited to a maximum resolution of 640 x 360 using Dual-Core CPU configuration onboard camera, 960 x 540 using Quad-Core CPU configuration onboard camera, and 1280 x 720 if the Logitech C930e camera is used.

   For information about supported cameras, see the *Release Notes* of your ThinOS version at Support | Dell.

Configure the Bluetooth settings

About this task

This section describes how to configure the Bluetooth settings on your thin client.

Steps

1. To access the peripherals settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Peripherals**.
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Peripherals**.

   The **Peripherals** dialog box is displayed.
2. Click the **Bluetooth** tab.

   Bluetooth-enabled devices such as headsets and mouses that are available in the thin client environment are listed on the Bluetooth page. The following attributes are displayed in the list:
   - **Name**—Specifies the name of the Bluetooth-enabled device.

- **Type**—Specifies the type of the Bluetooth-enabled devices, such as headsets, mouses, and keyboards.

  ThinOS supports Human Interface Devices (HID) devices. HID includes mouse and keyboard. The maximum number of HIDs that can be connected is seven.

  NOTE: ThinOS supports Bluetooth headsets, but only one headset can be connected. Call level audio quality on headsets is supported. Multimedia like team calls and zoom calls are supported. Other types of Bluetooth devices are not scanned and supported. For mouse, keyboard, and headsets, ThinOS supports both Bluetooth 3.0 and 4.0.

- **Status**—The Bluetooth page has two columns, namely, Status and Paired.

Table 58. Bluetooth status

Attribute	Value	Summary
Status	Connected	The Bluetooth device is connected to the ThinOS device. It is ready to be used.
	Connecting	The Bluetooth device is connecting to the ThinOS device.
	Disconnected	The Bluetooth device is not connected to the ThinOS device.
Paired	Yes	The Bluetooth device is paired with the ThinOS device.
	No	The Bluetooth device is not paired with the ThinOS device.

- **Address**—Displays the address of the Bluetooth device that is connected to your thin client.

The following are the user scenarios and corresponding Bluetooth statuses that are displayed on the Bluetooth page:

Table 59. User scenarios

User scenario	Status
Device turned off	Disconnected | Paired
Device turned on	Connected | Paired
Device disconnected from ThinOS	Disconnected | Not Paired

3. Select a Bluetooth device that is not connected, and click **Connect**. If the Bluetooth device is connected successfully, the status is displayed as **Connected** in the Bluetooth window. The following are the functions that are available:
   - **Scan**—Bluetooth devices enter into **Page Scan** mode. Different Bluetooth devices enter into the **Page Scan** mode at different instances. For example, when a specific button is pressed three times or a specific button is pressed and held until the LED turns blue.
   - **Connect**—Select a particularBluetooth-enabled device, and click **Connect** to connect the selected device to the thin client. If the Bluetooth device is connected successfully, the status is displayed as **Connected** in the **Bluetooth** window.
   - **Remove**—Select a particular Bluetooth device, and click **Remove** to disconnect and remove the device from the list.
   - **Auto Connect function**—The Auto Connect function is designed for HIDs.
     - ThinOS has no HIDs connected such as USB or Bluetooth HIDs.
     - The Bluetooth HIDs are configured as Page Scan mode.

   When you start the ThinOS client, the Bluetooth HIDs can connect to ThinOS automatically without scanning or pairing operations. The Bluetooth HIDs automatically reconnect after you restart the ThinOS client.

   - **Reconnect function**—The Reconnect function is designed for HIDs and headsets.

   When you restart the system with the Bluetooth device (HID/headset) that is already paired and connected, the Bluetooth device automatically reconnects within a few seconds.

   For example, you can hover the Bluetooth mouse, and then click a few times for the Bluetooth mouse to reconnect successfully. The Bluetooth headset reconnects automatically, but might require you to manually close or reopen the device on certain occasions.

4. Click **Save** to save your settings.

Calibration

A **Calibration** tab is added in the **Client Settings** > **Peripherals**. If you plug in an external touch monitor to the client without an integrated screen, **Calibration** can be enabled. Click the **Calibrate** button to start the calibration and then click **+** one by one until the calibration is finished.

Secure Digital cards

You can plug in a Secure Digital (SD) card into the Wyse 5470 Thin Client or a microSD 3.0 card into the Dell Latitude 3440. The SD card works as a storage device.

You can plug in an SD card into the Dell OptiPlex 7410 All-in-One. You can map the SD card to Citrix and RDP sessions as a storage device only. You cannot redirect it.

Storage formats

ThinOS only supports FAT32 and NTFS storages. If you want to use exFAT storage, you must redirect it to VDI session.

Configure the Jabra Xpress headset settings

ThinOS 10.x enables you to configure and manage Jabra Xpress headsets that are connected to the thin client. Use Wyse Management Suite or Admin Policy Tool on ThinOS to configure the headset settings.

Prerequisites

Go to jabraxpress.jabra.com and download the ZIP archive file to a local HTTP server.

Steps

1. Create a .INI file with the following commands.

```
[JDU]
ShowGui=true
RunOnSystemStart=true
LocalServerURL=http://xxx.xxx.xxx.xxx:port
```

```
[ADD]
AutoPost=false
ServerURL=
```

NOTE: Ensure that you create the INI file in the Linux operating system and not the Windows operating system.

For more information about the usage of commands, see the *User's Guide* at jabraxpress.jabra.com.

2. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.
3. In the **Advanced** tab, expand **Peripheral Management**, and click **Device Headset Settings**.
4. Click the **Enable Jabra Xpress** toggle switch to enable the option.
5. Browse and upload the configuration file.
6. From the drop-down list, select the uploaded configuration file.
7. Click **Save & Publish**.
8. Restart the thin client for the settings to take effect.

Next steps

1. Start the ThinOS client.
2. Connect the **Jabra Xpress** headset to your thin client.

The **Jabra Device Updater** window is displayed if you have set the `ShowGui` parameter to **True**.

Configure the EPOS headset settings

ThinOS enables you to configure and manage EPOS headsets that are connected to the thin client. Use Wyse Management Suite or Admin Policy Tool on ThinOS to configure the headset settings.

Steps

1. Create a text file with the EPOS Connect configuration details.

   NOTE: Ensure that you specify a valid tenant ID and a tenant URL. Log file configuration is optional.

   For example:

```
log_filepath = /tmp/epos-connect/Logs/
tenant_filepath = <filepath>
log_output = CONSOLE
log_level = TRACE
proxy_setting = <proxyserver>
tenant_id = <id>
tenant_url = <url>
```

   Table 60. EPOS Connect configuration details

Command	Description
log_filepath	Specifies the log file path.
tenant_filepath	Specifies the tenant configuration and device settings file path.
log_output	Specifies where the log entries are to be saved. The default is set to **CONSOLE**. Change the value to **FILE** if you want to write log entires to a log file.
log_level	Specifies the log level. The default is set to **OFF**. Change the value to one of the following options as per your preference: • TRACE • DEBUG • INFO • ERROR • WARN • EXCEPTION • OFF
proxy_setting	Specifies the proxy server.
tenant_id	Specify the tenant ID.
tenant_url	Specify the tenant URL.

2. Open the Admin Policy Tool on ThinOS or go to the ThinOS 10.x policy settings on Wyse Management Suite.
3. In the **Advanced** tab, expand **Peripheral Management**, and click **Device Headset Settings**.
4. Click the **Enable EPOS Connect** toggle switch to enable the option.
5. Browse and upload the configuration file.
6. From the drop-down list, select the uploaded configuration file.
7. Click **Save & Publish**.
8. Restart the thin client for the changes to take effect.

Next steps

1. Start the ThinOS client.
2. Connect the EPOS headset to your thin client.

NOTE: It is recommended that you use the silent deploy type during the firmware upgrade process.

NOTE: For all the supported EPOS devices, see the EPOS website.

Configure the HID Fingerprint reader settings

ThinOS supports using HID Global Identification Software with HID Fingerprint reader in a Citrix ICA session.

Prerequisites

Ensure that you have installed **HID Fingerprint Reader.pkg** on your client.

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **Global Session Settings**.
3. In the **Advanced Settings** section, enable **Enable HID Fingerprint Reader**.

   NOTE: By default the option is disabled.

4. Click **Save & Publish**, and relogin to the Citrix Broker agent to make the setting change successful.
5. Plug in the HID Fingerprint reader device.
6. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 10.x policy settings on Wyse Management Suite.
7. On the **Advanced** tab, expand **Peripheral Management**, and click **USB Redirection**.
8. Click **Add Row** in the **vUSB Force Local** section, and enter the fingerprint device ID **`0xVIDPID`**.
9. Launch the ICA desktop.
   You can use the HID Fingerprint Reader in the ICA desktop. If the HID fingerprint reader does not work in the ICA session, disable 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. For the list of supported devices, see the *Release Notes* of your ThinOS version at Support | Dell.

   NOTE: HID Fingerprint Reader can be configured in ICA desktop without the configuration changes in steps 8, 9 and 10. However, Dell Technologies recommends that you use this configuration for a better user experience.

Configuring the printer settings

Use the **Printer Setup** dialog box to configure network printers and local printers that are connected to the thin client. Through its USB ports, a thin client can support multiple printers. If more than one printer is to be used and another port is not available on your thin client and the port that is to be used must be shared with a USB modem converter, connect a USB hub to the port.

Based on the Citrix Host Printer Policy settings, ThinOS supports the following:

- **Device-Specific Printer Driver support**—This method allows Citrix hosts to automatically create client-redirected printer queues based on the peripheral management printers settings of the ThinOS client. The following details are used by the host print manager to automatically create the printer queues:
  - **Name**—Printer queue name.
  - **Printer ID (Printer Identification)**—Printer driver name.
- **Citrix Universal Print Driver support**—This method allows Citrix hosts to automatically create printer queues based on the peripheral management printers settings of the ThinOS client. The following details are used by the host print manager to automatically create the printer queues:
  - **Name**—Printer queue name.
  - **Class**—Printer class that is associated by the Citrix host registry to a printer-specific driver name.

  NOTE: ThinOS 10.x client associations are limited to the PS class only.

Limitations

- Do not set COM1 and COM2 port as the same Printer Identification as it causes the COM printer to not work properly.
- The ThinOS solution to support the client printer redirection functionality is limited to Type 3 printers only. However, the solution is subject to changes in the future according to the changes made by Citrix.
- ThinOS supports only the PS class when using the Citrix Universal Print Driver policy to automatically create ThinOS client-redirected printers. PCL5 and PCL4 classes are not supported. This is a Citrix limitation.

For known issues and workaround, see the *Release Notes* of your ThinOS version at Support | Dell.

Configure the ports settings

About this task

This section describes how to configure the port settings on your thin client:

Steps

1. To access the printer settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Printer Setup** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Printer Setup** > **.**

   The **Printer** dialog box is displayed.
2. Click the **Ports** tab, and do the following:

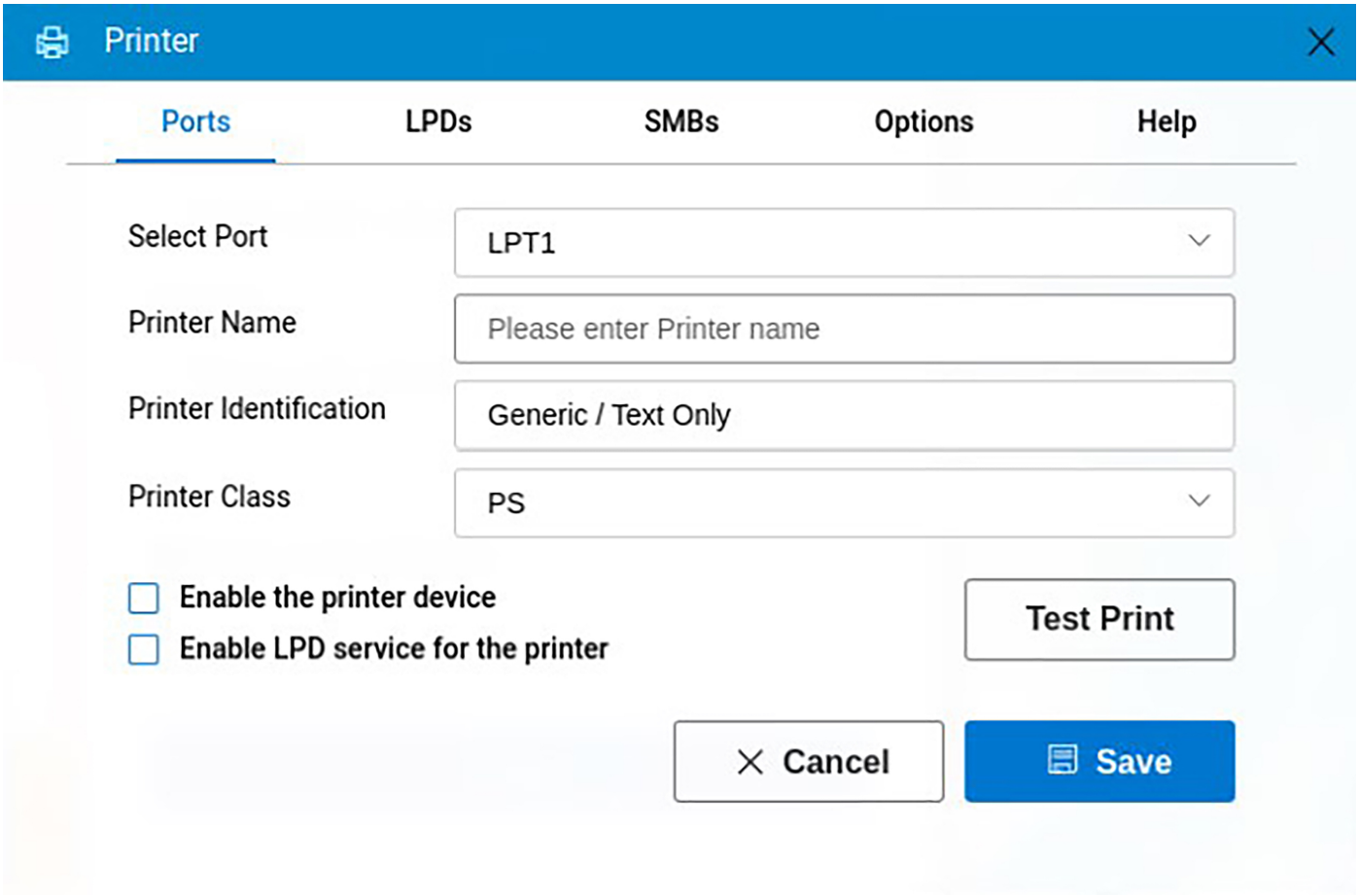

Figure 61. Ports

a. **Select Port**—Select a port from the drop-down list. Selecting **LPT1** or **LPT2** sets the connection to a direct-connected USB printer. If you are using the Wyse 5070 Extended Thin Client, select **LPT2** for the USB printer.

   NOTE: For Wyse 5070 extended thin client with parallel port option installed, if there is LPT1 printer settings that are configured on Wyse Management Suite or the local UI, then it cannot be removed again.

b. **Printer Name**—(Required) Enter the name of the printer.

   NOTE: If **Enable LPD service** for the printer is selected, the printer name becomes the queue name for other clients using LPR to print to this printer.

c. **Printer Identification**—(Required) Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

Printer mapping in a Citrix session on ThinOS uses Citrix UPD (Universal Printer Driver). You can enter any string in the **Printer Identification** field.

d. **Printer Class**—Select the printer class from the drop-down list as **PS**.
e. **Enable the printer device**—Select this option to enable the directly connected printer. It enables the device to be displayed on the remote host.
f. **Enable LPD service for the printer**—Select this option to make the thin client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network.

NOTE: If you want to use thin client as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the client. See Configuring the network settings for more information.

NOTE: If you are configuring Enable LPD service for the printer from the local **Printer Setup** window, restart the client for the LPD service to work in VDI sessions. If you are configuring from the Wyse Management Suite policy, you need not to restart.

3. Click **Save** to save your settings.

Configure the LPDs settings

About this task

This section describes how to configure the LPD settings on your thin client.

Steps

1. To access the printer settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Printer Setup** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Printer Setup** > **.**

   The **Printer** dialog box is displayed.
2. Click the **LPDs** tab, and do the following when printing to a non-Windows network printer:

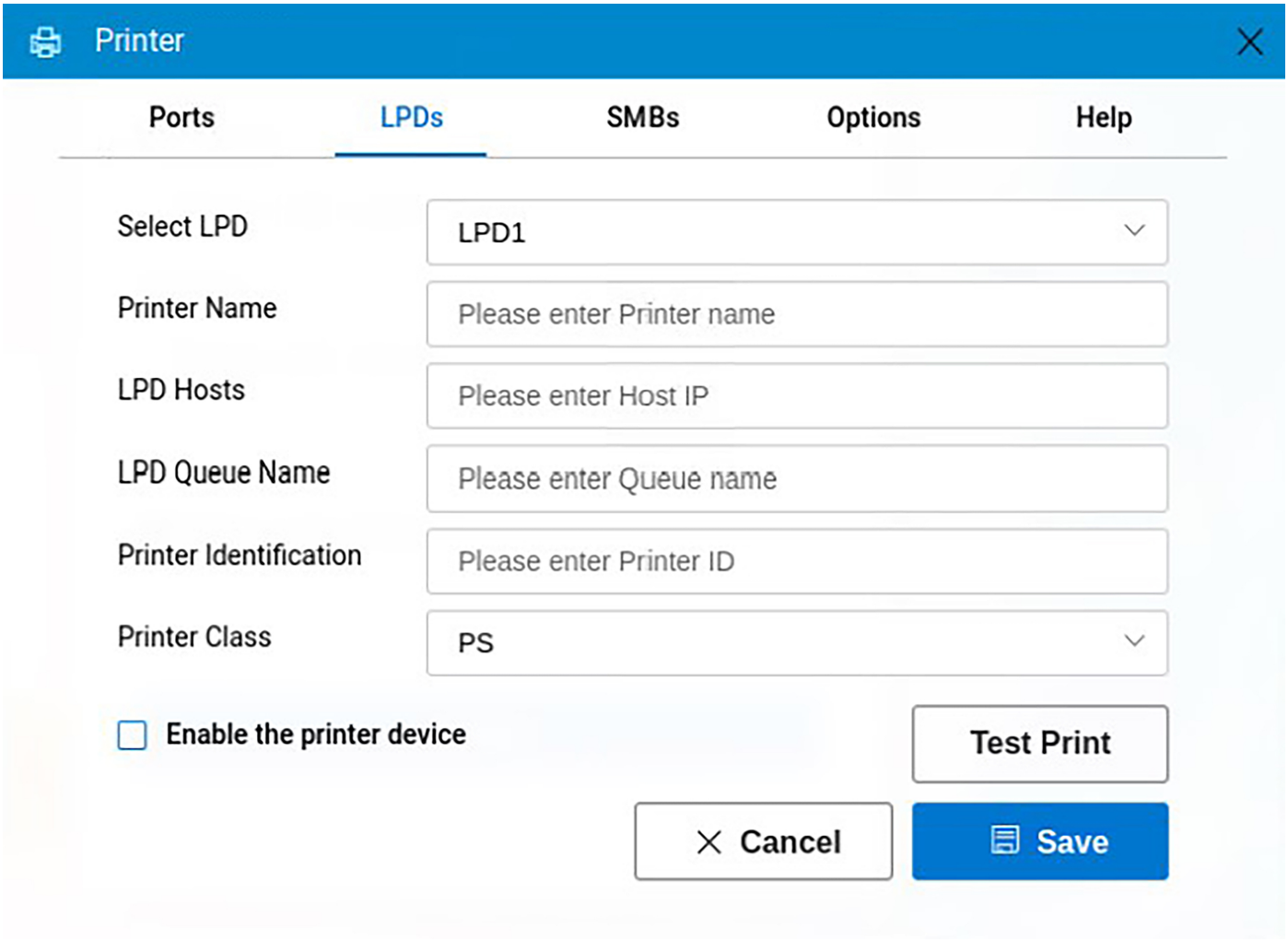

Figure 62. LPD

NOTE: In the local **Printer Setup** window in LPDs settings, **LPD Queue Name** must be entered as **`auto`**. In Wyse Management Suite or Admin Policy Tool, in LPD Printer Settings, **Queue** must be entered as **`auto`**.

NOTE: Be sure to check with your vendor that the printer can accept Line Printer Request print requests.

a. **Select LPD**—Select the LPD port from the drop-down list.
b. **Printer Name** —Enter the name of the printer. If you do not specify a printer name, the LPD queue name is used automatically.
c. **Printer Identification**—(Required) Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

   Printer mapping in a Citrix session on ThinOS uses Citrix UPD (Universal Printer Driver). You can enter any string in the **Printer Identification** field.
d. **LPD Hosts**—(Required) The DNS or WINS name of the server for the network printer. An IP address of the printer on the network can also be entered.
e. **LPD Queue Name**—(Required) An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer to be used.

   This name can be different for each vendor. This field is required and must be correct so that the network printer accepts incoming print jobs properly.

   LPD Queue Name must be entered as **`auto`** or **`generic`**. In Wyse Management Suite or Admin Policy Tool, in LPD Printer Settings, **Queue** must be entered as **`auto`** or **`generic`**.

   NOTE: If the target LPD printer is a thin client sharing a local printer and **Enable LPD service** is enabled for the printer under Ports or SMBs, then in the local **Printer Setup** window in LPDs settings, the **LPD Queue Name** value

must be any value except **auto** and **generic**. In Wyse Management Suite or Admin Policy Tool, in LPD Printer Settings, **Queue** value must be any value except **auto** and **generic**.

f. **Printer Class**—Select the printer class from the drop-down list as **PS**.
g. **Enable the printer device**—Must be selected to enable the printer. It enables the device to be displayed on the remote host.

3. Click **Save** to save your settings.

Configure the SMBs settings

About this task

This section describes how to configure the SMB settings on your thin client.

Steps

1. To access the printer settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Printer Setup** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Printer Setup** > **.**

   The **Printer** dialog box is displayed.
2. Click the **SMBs** tab, and do the following when printing to a Windows network printer:

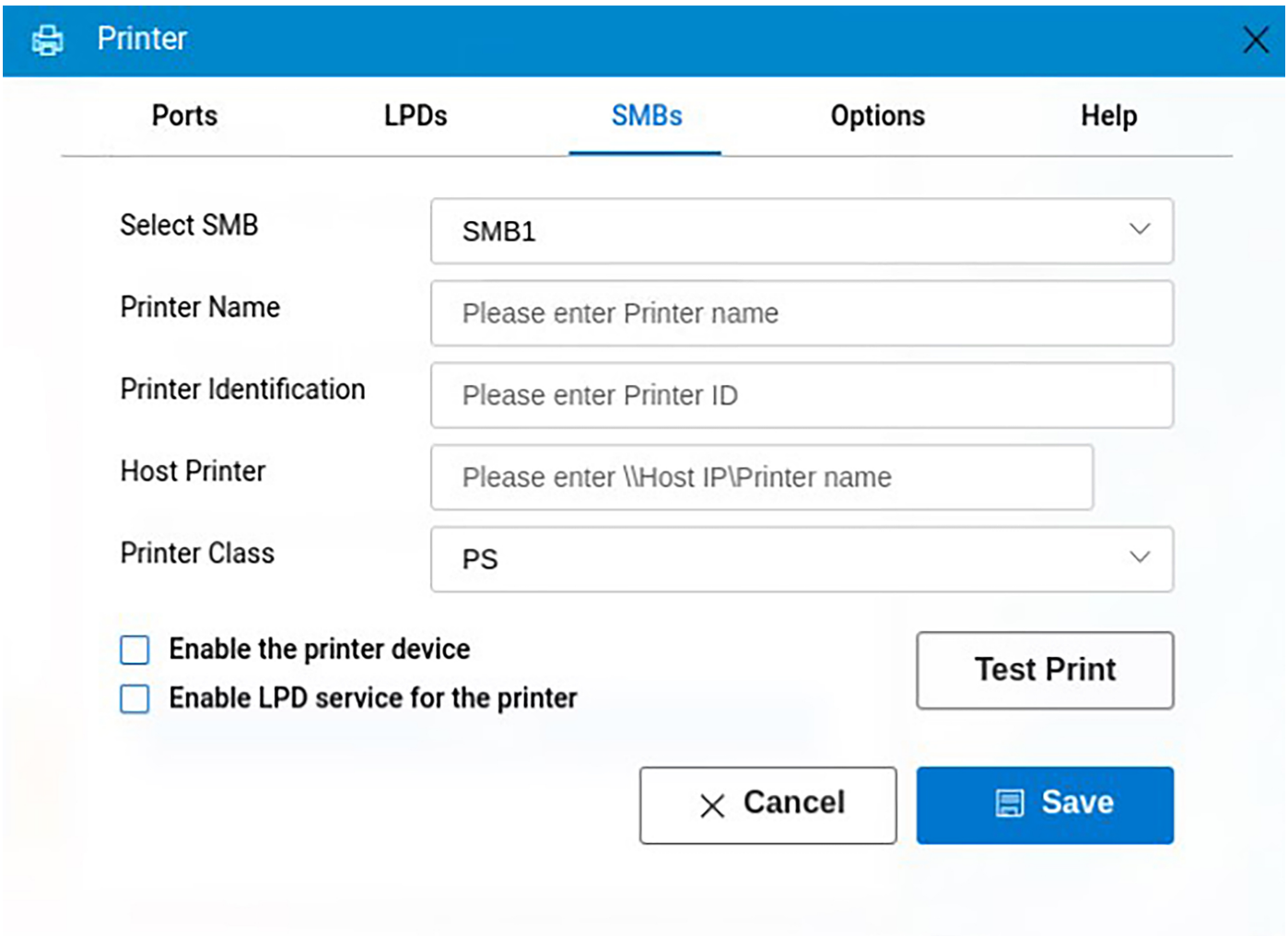

Figure 63. SMB

a. **Select SMB**—Select the SMB port from the drop-down list.

b. **Printer Name**—Enter the name of the printer. If you do not specify a printer name, the SMB shared printer name is used automatically.
c. **Printer Identification**—(Required) Enter the type or model of the printer in the exact text of the Windows printer driver name—including capitalizations and spaces.

   Printer mapping in a Citrix session on ThinOS uses Citrix UPD (Universal Printer Driver). You can enter any string in the **Printer Identification** field.

d. **\\Host\Printer**—(Required) Enter the IP address, system name, or FQDN of the host and specify the shared name of the printer. After you specify the values and move the cursor, the SMB credentials dialog box is displayed. You are prompted to enter the host username, password, and the domain name.

   NOTE: If the host has not joined any domain, enter WORKGROUP in the domain name field.

e. **Printer Class**—Select the printer class from the drop-down list as **PS**.
f. **Enable the printer device**—Must be selected to enable the printer. It enables the device to be displayed on the remote host.
g. **Enable LPD service for the printer**—Select this option to make the thin client an LPD (Line Printer Daemon) network print server for LPR printing requests from the network. If you want to use thin client as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the client. See Configuring the network settings for more information.

   NOTE: If you are configuring Enable LPD service for the printer from the local **Printer Setup** window, restart the client for the LPD service to work in VDI sessions. If you are configuring from the Wyse Management Suite policy, you need not restart.

3. Click **Save** to save your settings.

Using the printer setup options

About this task

This section describes how to configure the printer setup options.

Steps

1. To access the printer settings, do the following:
   - **Modern Mode**—From the desktop menu, click **System Settings** > **Printer Setup** > **.**
   - **Classic Mode**—From the desktop menu, click **System Setup** > **Printer Setup** > **.**

   The **Printer** dialog box is displayed.
2. Click the **Options** tab, and select a printer from the **Default Printer** drop-down list.

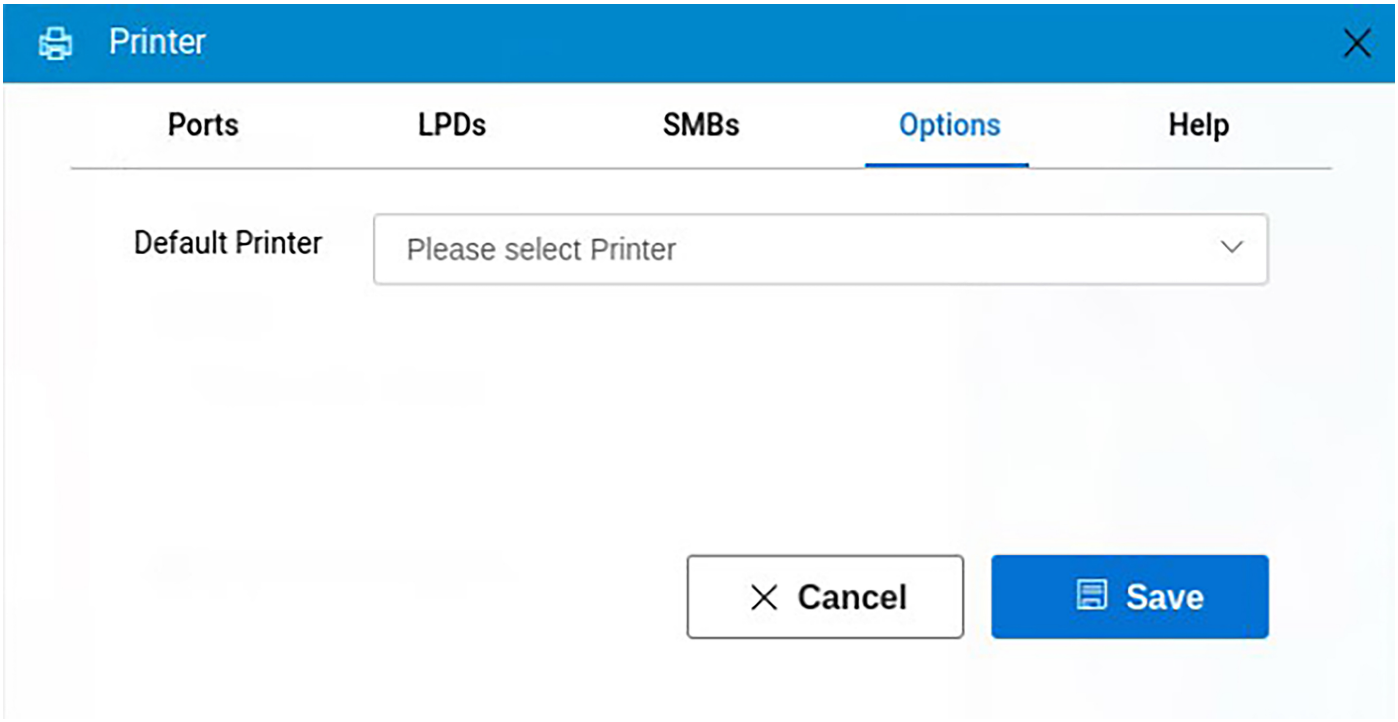

Figure 64. Options

3. Click **Save** to save your settings.

Using the Help

When you click the **Help** tab, the following message is displayed in the text box.

Printer Identification is supplied by printer device. Change it to a Window's printer driver name or setup a driver mapping file.

Enable or Disable the Taskbar volume icon using WMS or APT

Explains how ThinOS 10.x allows IT administrators to enable or disable the local client volume icon using WMS or APT by adjusting privilege level, ensuring consistent control of audio behavior across managed devices.

About this task

After completing the configuration steps, ThinOS 10.x applies the updated volume icon immediately based on the privilege controls defined in WMS or APT. The enable or disable state of the local volume icon remains consistent across reboots, upgrades, and downgrades, ensuring stable and predictable audio behavior on all managed devices.

Steps

1. To configure the local client audio, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Privacy & Security** > **Account Privileges** > **Privilage level**.
3. Select the privilege level as **Customize**.
4. **Enable** or **Disable** the **Volume Icon**.
5. Click **Save & Publish**.

Configuring the Firefox browser

Supports Firefox web browser

ThinOS 10.x supports the Firefox browser as an optional package which can be installed using Wyse Management Suite or Admin Policy Tool.

- **Package Installation using WMS**:
  - Go to **WMS** > **Firmware** > **Application Package Update** > **Other Section**, select the browser package, and click **Save & Publish**.
- **Package installation using APT**:
  - Go to **Admin Policy Tool** > **Advanced** > **Firmware** > **Application Package Update**, click **Browse**, and select the browser package from the USB drive. Then go to **Other Section**, select the browser package, and click **Save & Publish**.

NOTE: You can access Firefox Browser only when you either login as VDI user or none.

Configuring browser shortcuts

By design, prioritizing security, all Firefox browser options are hardened by default. As a result, all browser options are disabled, and users must enable specific options through the WMS/Admin Policy Tool under Firefox settings if they require access to these settings.

From ThinOS 10.x 2502, you can create the browser shortcuts using Wyse Management Suite or Admin Policy Tool.

- **Browser Shortcuts configuration using WMS**:
  1. Go to **Browser Settings** > **Browser Shortcut** using WMS.
  2. Enter the shortcut name in the **Shortcut Name** option.
  3. Provide the URL in the **URL** option, and select the browser as **Firefox** from the **Broswer** drop-down menu.
  4. Enter the details in the **Additional Arguments**, **Monitor ID**, and **Icon for shortcut** options.
  5. Enable the **Auto launch on logon** option if you want the browser shortcuts to launch automatically post restart.
- **Browser Shortcuts configuration using APT**:
  1. Go to **Browser Settings** > **Browser Shortcut** using **APT**.
  2. Enter the shortcut name in the **Shortcut Name** option.
  3. Provide the URL in the **URL** option, and select the browser as **Firefox** from the **Broswer** drop-down menu.
  4. Enter the details in the **Additional Arguments**, **Monitor ID**, and **Icon for shortcut** options.
  5. Enable the **Auto launch on logon** option if you want the browser shortcuts to launch automatically post restart.

Supports Kiosk mode in Firefox browser

ThinOS supports configuring a kiosk mode for the Firefox browser, allowing for a customized, secure, and restricted browsing experience. To configure the kiosk mode using WMS or APT, do the following:

- **Browser Kiosk configuration using WMS**:
  1. Go to **Login Experience** > **Browser Kiosk**.
  2. Enable the **Browser Kiosk mode** option.
  3. Enter the Kiosk URL in the **Kiosk URL Configuration** option.
  4. Select the browser as **Firefox** from the **Kiosk Browser** drop-down menu.
  5. Enable the **Auto Reconnect** option.
  6. Enter the time in seconds in the **Delay before trying to reconnect** option.
- **Browser Kiosk configuration using APT**:
  1. Go to **Login Experience** > **Browser Kiosk**.
  2. Enable the **Browser Kiosk mode** option.
  3. Enter the Kiosk URL in the **Kiosk URL Configuration** option.
  4. Select the browser as **Firefox** from the **Kiosk Browser** drop-down menu.
  5. Enable the **Auto Reconnect** option.
  6. Enter the time in seconds in the **Delay before trying to reconnect** option.

NOTE: You must log out or restart for kiosk mode configurations to reflect in the client. If you want to exit from the kiosk mode, press alt + F4 key. The Auto-Reconnect option, when enabled, reconnects the kiosk mode after the mentioned seconds.

Enable or disable Hide FireFox icon

Prerequisites

FireFox web browser must be installed.

About this task

Verify if the FireFox web browser icon is visible or hidden.

Steps

1. Log in to **WMS**.
2. Go to **Group & Configs** > **Select a group** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Browser Settings** > **FireFox Settings** > **Privacy Settings** and select **Hide FireFox Icon**.

   NOTE: Check the state of the option whether it is enabled or disabled.

   - If the **Hide FireFox Icon** is enabled, disable it and verify the changes.
   - If the **Hide FireFox Icon** is disabled, enable it and verify the changes.
3. Click **Save & Publish**.
   If option is disabled, the user can view or access the default FireFox in the VDI Menu.

   If option is enabled, the default FireFox icon is hidden.

   NOTE: ThinOS 10.x 2505 does not support **Hide FireFox Icon** if the user has created browser shortcuts.

Reset to factory defaults

A high-privileged or standalone user can reset the thin client to factory default settings from the **Shutdown** dialog box. Shutdown reset is disabled for custom-privileged and nonprivileged users.

About this task

This section describes how to reset the thin client to factory default settings.

NOTE: The data sanitization using the **Factory Reset** function achieves clear in accordance with NIST SP800-88r1 and IEEE 2883-2002. To achieve purge in accordance with NIST SP800-88r1 and IEEE 2883-2002, **BIOS Data Wipe** feature can be used. For more information, see Dell Data Wipe.

WARNING: Shutdown reset impacts all configuration items, including but not limited to, network configuration and connections defined in local NV-RAM.

Steps

1. From the desktop menu, click **Shutdown**.
   The **Shutdown** dialog box is displayed.
2. Select the **Reset the system setting** checkbox.
3. If you want to clear all configurations, select **Factory reset**. If you want to clear all configurations except network, certificate, and Wyse Management Suite, select **Soft reset**.

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

Resetting to factory defaults using G-Key reset

Users can reset the thin client to factory default settings using the G-key reset feature. By default the feature is enabled. To reset the thin client to factory default settings, restart the thin client and continuously tap the **G** key during the restart process until you hear a beep sound. To disable the G-key feature, go to **Advanced** > **Personalization** > **Shortcut Keys** from the Wyse Management Suite policy settings or the Admin Policy Tool, and disable the **Enable G key to Reset Device to Factory Default** option.

Support for Google Chrome browser

ThinOS 10.x 2505 supports the Google Chrome browser as an optional package which can be installed using Wyse Management Suite or Admin Policy Tool.

You can install the package using any of the following options:

Using WMS

1. Log in to **WMS**.
2. Go to **Groups & Configs** > **Edit Policies** > **Advanced** > **Firmware** > **Application Package Update**.
3. In the **Third Party** section, select the browser package.
4. Click **Save & Publish**.

Using the Admin Policy Tool

1. In the client, go to **Admin Policy Tool** > **Advanced** > **Firmware** > **Application Package Update**.
2. Click Browse and select the package from the USB drive.
3. In the **Third Party** section, select the browser package.
4. Click **Save & Publish**.

NOTE: You can access Google Chrome only when you either log in as VDI user or none.

Enable or disable Hide Chrome icon

Prerequisites

Chrome must be installed.

About this task

Follow these steps to verify whether the Chrome icon is visible or hidden.

Steps

1. Log in to **WMS**.
2. Go to **Group & Configs** > **Select a group** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Browser Settings** > **Google Chrome Settings** > **Privacy Settings** and select **Hide Chrome Icon**.

   NOTE: Check the state of the option whether it is enabled or disabled.

   - If the **Hide Chrome Icon** is enabled, disable it and verify the changes.
   - If the **Hide Chrome Icon** is disabled, enable it and verify the changes.
3. Click **Save & Publish**.
   If option is disabled, the user can view or access the default Chrome in VDI Menu.

   If option is enabled, the default Chrome icon is hidden.

NOTE: ThinOS 10.x 2505 does not support **Hide Chrome Icon** if the user has created browser shortcuts.

Verify the Chrome icon is visible with the Browser shortcut

Prerequisites

Chrome web browser must be installed.

About this task

Follow these steps to verify if the Chrome Icon is visible or hidden with a Browser shortcut:

Steps

1. Log in to **WMS**.
2. Go to **Group & Configs** > **Select a group** > **Edit Policies** > **ThinOS 10.x** > **Advanced** > **Browser Settings** > **Google Chrome Settings** > **Privacy Settings** and select **Hide Chrome Icon**.

   NOTE: Check the state of the option whether it is enabled or disabled.

   - If the **Hide Chrome Icon** is enabled, disable it and verify the changes.
   - If the **Hide Chrome Icon** is disabled, enable it and verify the changes.

   If option is disabled, the user can view or access the default Chrome in VDI Menu.

   If option is enabled, the default Chrome icon is hidden.
3. Go to **Browser Settings** > **Browser Shortcuts** > **Add Row**.
4. To create a browser shortcut **Icon for shortcut** , enable or disable the **Auto launch on enable**

   NOTE: Verify the changes if **Auto launch on enable** is enabled or disabled.

   If the created browser is Auto Launches on Startup is enabled, the created Browser shortcut auto launches when the computer starts.

   If Auto Launches on Startup is disabled, the created Browser shortcut does not autolaunch when the computer starts.

Configuring a Custom browser User-Agent

From ThinOS 10.x 2511, you configure a custom Chrome browser User-Agent string in WMS. This allows compatibility with websites that restrict access based on browser identification, offering greater flexibility and control in web-based workflows.

To configure a Custom browser User-Agent on ThinOS devices, do any of the following:

- Configure a Custom browser User-Agent using APT.
- Configure a Custom browser User-Agent using WMS.

Configure a custom browser User-Agent using APT

You can set a custom Chrome browser User-Agent using APT on the device, ensuring better website compatibility and flexibility.

About this task

After completing the configuration steps, ThinOS automatically updates the time zone based on the network connection. When the device connects to LAN or Wi-Fi, the time zone adjusts accordingly. Rebooting, upgrading, or downgrading the ThinOS 10.x device should not affect this behavior, ensuring consistent and accurate time settings across all actions.

Steps

1. Go to **Admin Policy Tool** on the device.
2. Go to **Advanced** > **Browser Settings** > **Google Chrome Settings** > **Broswer User Agent**.

3. Verify that the field is blank by default.
4. Enter the following user agent string: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36`.
5. Click **Save & Publish**.

Configure a custom browser User-Agent using WMS

You can set a custom Chrome browser User-Agent using WMS, ensuring better website compatibility and flexibility.

About this task

After completing the configuration steps, ThinOS automatically updates the time zone based on the network connection. When the device connects to LAN or Wi-Fi, the time zone adjusts accordingly. Rebooting, upgrading, or downgrading the ThinOS 10.x device should not affect this behavior, ensuring consistent and accurate time settings across all actions.

Steps

1. Log in to **WMS** as an administrator.
2. Go to **Groups & Configs** > **Edit Policies** > **ThinOS 10.x**.
3. Go to **Advanced** > **Browser Settings** > **Google Chrome Settings** > **Broswer User Agent**.
4. Verify that the field is blank by default.
5. Enter the following user agent string: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36`.
6. Click **Save & Publish**.

Uploading and managing SSL certificates for browser

ThinOS 10.x 2511 supports uploading and managing SSL certificates across all supported browsers, ensuring seamless browser trust and improved security compliance.

To upload and manage SSL certificates for browsers on ThinOS devices, do any of the following:

- Upload and manage SSL certificates using WMS.
- Upload and manage SSL certificates using APT.

Upload and manage SSL certificates for browsers using APT

You can upload and manage SSL certificates across all supported browsers on ThinOS devices using APT.

About this task

After completing the configuration, open an HTTPS URL that uses the certificate. Verify that the page loads securely, showing the padlock icon without any **Not Secure** warning.

Steps

1. Go to **Admin Policy Tool** on the device.
2. Go to **Advanced** > **Import Certificates**.
3. Upload the SSL certificates to the ThinOS device.
4. Verify the Job Status for successful completion.
5. On the ThinOS device, go to **Settings** > **System Tools** > **Certificates**.
6. Verify that the certificate appears under the installed certificate list.
7. Open Chrome Browser and go to **Settings** > **Privacy & Security** > **Security** > **Manage Certificates**.
8. In **Authorities** or **Servers** tab, verify that the certificate appears under the appropriate tab.

Upload and manage SSL certificates for browsers using WMS

You can upload and manage SSL certificates across all supported browsers on ThinOS devices using WMS.

About this task

After completing the configuration, open an HTTPS URL that uses the certificate. Verify that the page loads securely, showing the padlock icon without any **Not Secure** warning.

Steps

1. Log in to **WMS** as an administrator.
2. Go to **Groups & Configs** > **Edit Policies** > **ThinOS 10.x**.
3. Go to **Advanced** > **Import Certificates**.
4. Upload the SSL certificates to the ThinOS device.
5. Verify the Job Status for successful completion.
6. On the ThinOS device, go to **Settings** > **System Tools** > **Certificates**.
7. Verify that the certificate appears under the installed certificate list.
8. Open Chrome Browser and go to **Settings** > **Privacy & Security** > **Security** > **Manage Certificates**.
9. In **Authorities** or **Servers** tab, verify that the certificate appears under the appropriate tab.

Recovery mode using R-Key

Users can remove all the application packages, return the client to the base operating system image, and then reset to factory settings using the R-key feature. By default the feature is enabled. To recover the thin client using the R-key feature, restart the thin client and continuously tap the **R** key during the restart process until you hear a beep sound. To disable the R-key feature, go to **Advanced** > **Personalization** > **Shortcut Keys** from the Wyse Management Suite policy settings or the Admin Policy Tool, and disable the **Enable R key to Enable Recovery Mode** option.

12

Using system tools

Use the **System Tools** option to view all the connected devices, installed packages, and imported certificates into the ThinOS client.

About this task

This section describes how to access system tools on your thin client.

Steps

1. To access the system tools, do the following:
   - **Modern Mode**—from the desktop menu, click **System Settings** > **System Tools**
   - **Classic Mode**—from the desktop menu, click **System Setup** > **System Tools**

   The **System Tools** dialog box is displayed.
2. Click the **Devices** tab to view all the locally attached devices, including USB, on applicable platforms. The details about the displays connected to the thin client are also displayed.

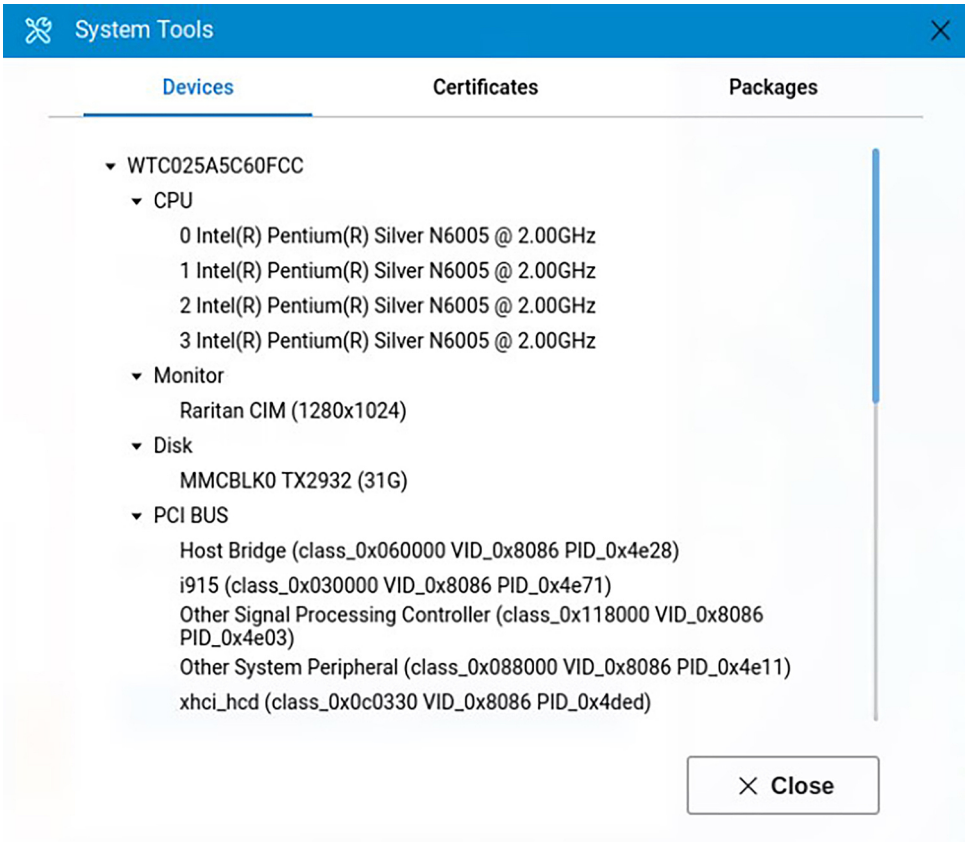

Figure 65. Devices

3. Click the **Certificates** tab to view the list of certificates that are imported to the thin client.

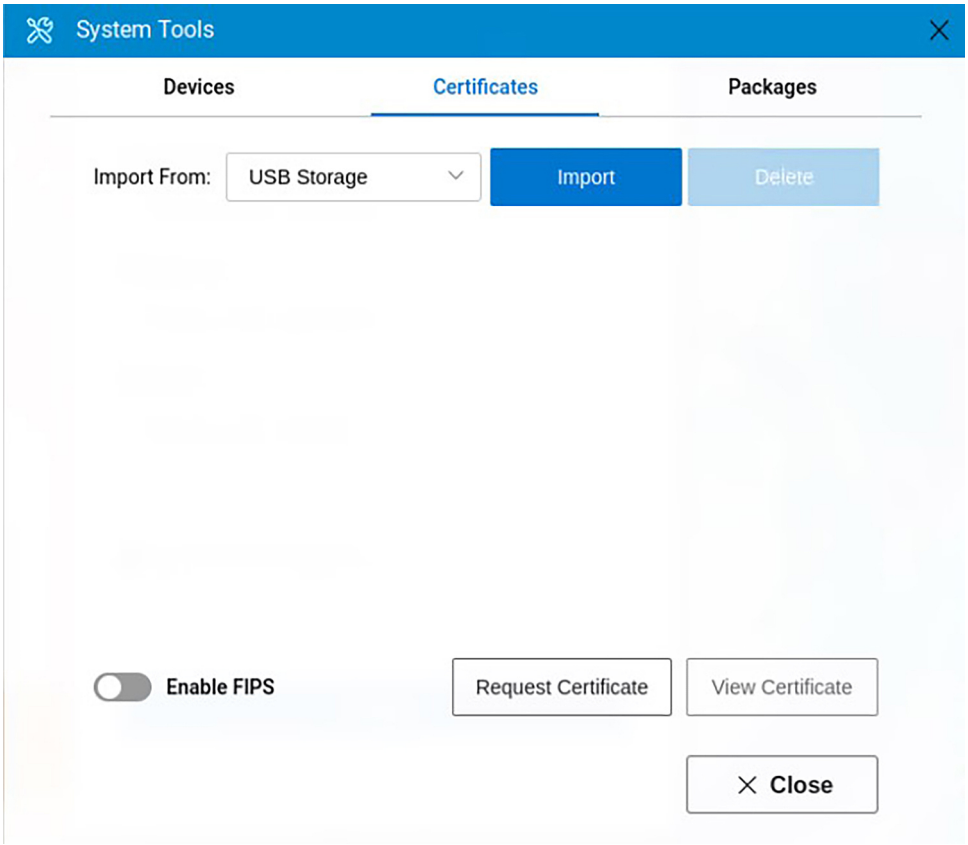

Figure 66. Certificates

- Use the **Enable/Disable FIPS** slide switch to enable or disable the Federal Information Processing Standard (FIPS) Publication 140-2 authentication compliance.
- From the **Import From** drop-down list, select **USB Storage**, and click **Import**. Browse and select the appropriate certificate that is stored in the USB drive.
- Select a certificate from the list, and click **View Certificate** to details such as version, validity, and serial number. You can also view the certificate path and certificate status.
- To manually request a certificate for your client, Click **Request Certificate**, provide the required details, and then click **Request Certificate** again.

NOTE: When you import a private certificate that contains certificate authority (CA) information, the client shows the CA information and the private certificate information under the **Certificates** tab.

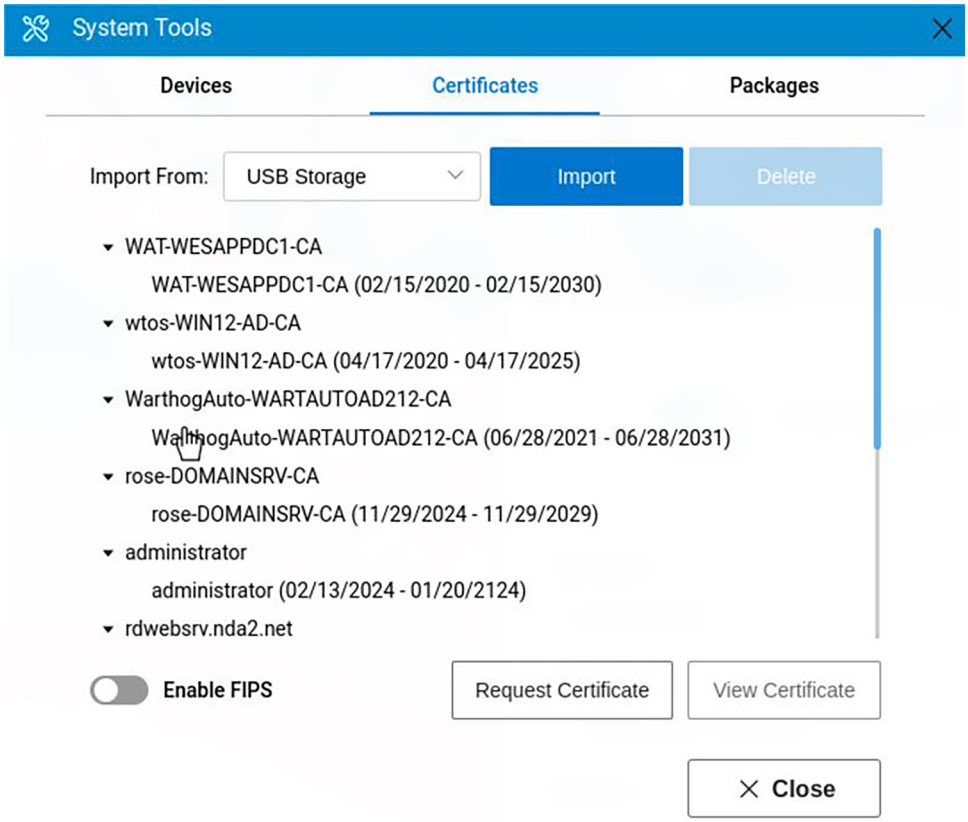

Figure 67. CA information

4. Click the **Packages** tab to view the list of ThinOS packages installed on the thin client.
   - To delete a single package, select the package and click **Delete**.
   - To delete all the packages, click **Delete all**.

   To verify third-party binary versions on your ThinOS client, see How to verify third-party binary versions on your ThinOS client?

   NOTE: In every ThinOS release, the packages may be updated to the latest version.

5. Click **Save** to save your settings.

Simplified Certificate Enrollment Protocol

The simplified Certificate Enrollment Protocol (SCEP) is designed for use in closed networks where all endpoints are trusted. Its primary goal is to securely issue certificates to network devices in a scalable manner. Within an enterprise domain, SCEP enables network devices that do not have domain credentials to enroll for certificates from a Certification Authority (CA).

At the end of the transactions defined by this protocol, the network device obtains a private key and an associated certificate that is issued by the CA. Applications on the device can use the key and its certificate to securely interact with other entities on the network. A common use case for this certificate is authenticating the network device in an IPSec session.

In ThinOS, which is treated as a network device, the SCEP functionality includes:

- Manual certificate requests
- Automatic certificate requests
- Automatic certificate renewal

NOTE: Certificates that are enrolled through SCEP have a prefix of **scep_cert_** in their names. To use the certificate with other features, such as wireless TLS, you must include the prefix **scep_cert_** with the certificate name.

Request certificate manually

About this task

To request the certificate manually, do the following:

Steps

1. Go to **System Tools** > **Certificates** > **Request Certificate**.

   The **Request Certificate** dialog box is displayed.

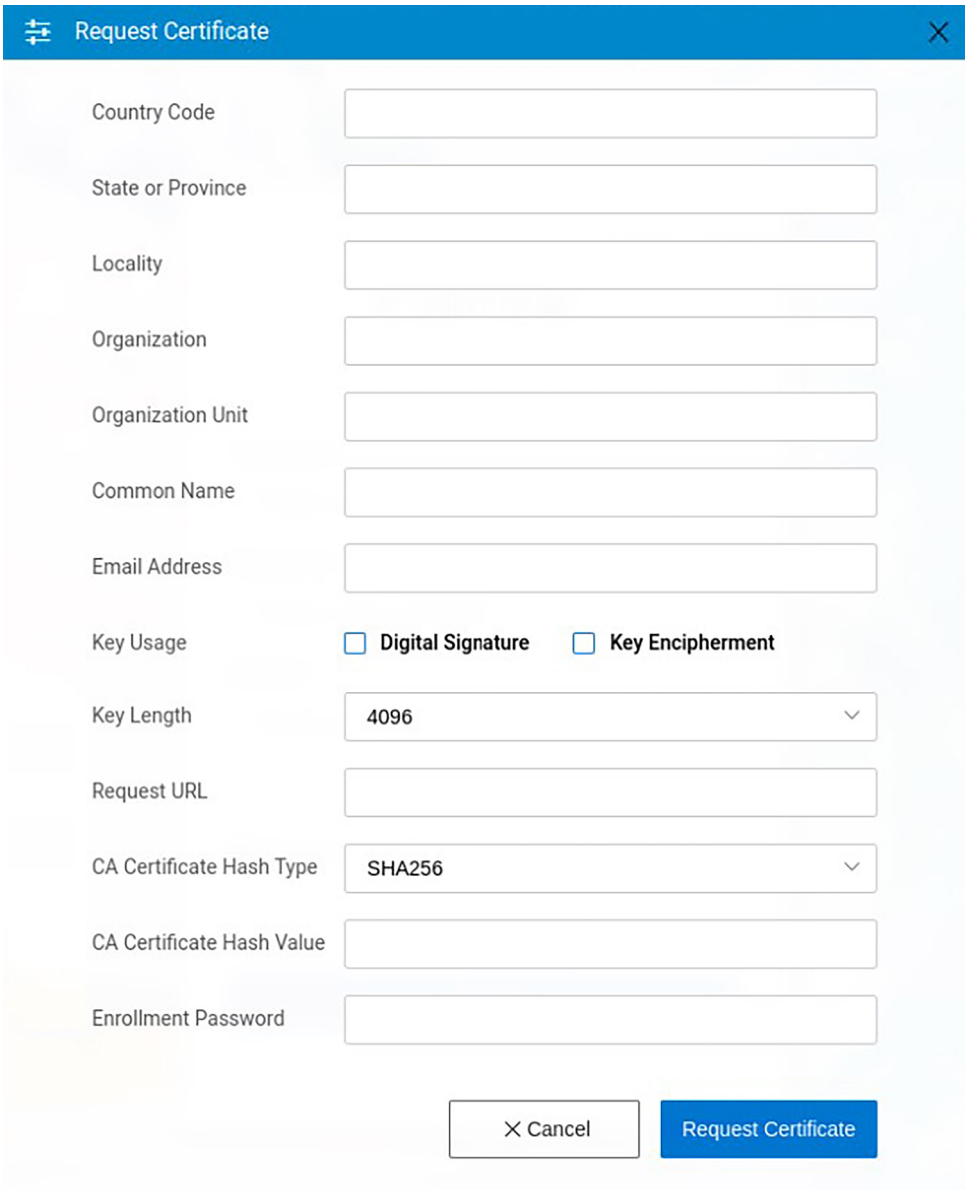

Figure 68. Request Certificate

2. Enter the appropriate values in the **Request Certificate** dialog box, and then click the **Request Certificate** button.
   The certificate request is sent to the server, and the client receives the response from server and installs both CA certificate and client certificate.

   NOTE: You must enter the prefix HTTP or HTTPS in the Request URL field.

3. Click **Save** to save your changes.

   The CA Certificate Hash type supports MD5, SHA1, and SHA256. The request server URL can be an HTTP or HTTPS link. You can add the protocol prefix before the URL.

Request certificate automatically using Wyse Management Suite

Steps

1. Log in to Wyse Management Suite.
2. Go to **Groups & Configs** and select your preferred group.
3. Expand **Edit Policies** and click **ThinOS 10.x**.
   The **Configuration Control | ThinOS** window is displayed.
4. In the **Advanced** tab, click **Privacy & Settings**.
5. Click **SCEP**.
6. Click the **Enable Auto Enrollment** slider switch to enable automatic certificate enrollment using the SCEP server.
7. Click the **Enable Auto Renew** slider switch to automatically renew the certificate.

   The client requires a password to renew the client certificate. If you are using an enrollment password that expires in a short time, ensure that the password is valid when the client initiates the auto-renewal process. Dell Technologies recommends using either administrator credentials or a fixed enrollment password to facilitate both auto-enrollment and auto-renewal of the certificate.
8. Click the **Select Install CA Certificate** slider switch to install the root CA's certificate as a trusted certificate after successfully getting the client certificate.
9. Click **Select Auto Renew Time Frame**.

   The value for this option ranges from 10% to 100%, with a default value of 50%. This means that auto-renewal is triggered after half of the private certificate's validity period has passed. For example, if set to 10%, auto-renewal is triggered after one-tenth of the certificate's validity period. You can verify the validity period of a private certificate in the local menu by navigating to **System tools > Certificates > Check common name**.
10. Specify the country/region name, state, location, and other details.
11. Click **Save & Publish**.

    You can also configure the SCEP Administrator URL, Admin User, Admin User Password, and Admin User Domain options to request for SCEP certificate. If the enrollment password is not specified, the client uses the SCEP Administrator URL, Admin User, Admin User Password, and Admin User Domain options to request SCEP. If you specify the enrollment password, the enrollment password is used for SCEP, even though the password entered is invalid. In this scenario, the SCEP Administrator URL, Admin User, Admin User Password, and Admin User Domain options are ignored.

    NOTE: When using a SCEP Administrator URL and Request URL, you must use the prefix HTTP or HTTPS.

    An option **Ignore Server Certificate Check** is added under **Privacy & Security** > **SCEP**.

    This option is disabled by default. To request a SCEP certificate, you must first install a CA certificate and then use the administrator URL. When using the administrator URL, you must provide the FQDN with the prefix HTTPS. Avoid using an IP address in the URL.

    If this option is enabled, you need not install the CA certificate on the client. You can directly request for a SCEP certificate by using the administrator URL with the prefix HTTPS.

    NOTE: For earlier versions of ThinOS, if you used an IP address in the administrator URL with the **Ignore Server Certificate Check** option disabled, you must update the URL to use the FQDN. If the **Ignore Server Certificate Check** option is enabled, changes to the IP address in the administrator URL are not necessary.

About Default Certificates

Default certificates are embedded in the ThinOS device. The following default certificates are displayed in the **ca-certificates** folder, in an expandable tree structure format:

- AC_RAIZ_FNMT-RCM.crt
- AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt
- ACCRAIZ1.crt
- Actalis_Authentication_Root_CA.crt
- AffirmTrust_Commercial.crt
- AffirmTrust_Networking.crt
- AffirmTrust_Premium.crt
- AffirmTrust_Premium_ECC.crt

- Amazon_Root_CA_1.crt
- Amazon_Root_CA_2.crt
- Amazon_Root_CA_3.crt
- Amazon_Root_CA_4.crt
- ANF_Secure_Server_Root_CA.crt
- Atos_TrustedRoot_2011.crt
- Atos_TrustRoot_Root_CA_ECC_TLS_2021.crt
- Atos_TrustRoot_Root_CA_RSA_TLS_2021.crt
- Autoridad_de_Certification_Fimaprofessional_CIF_A62634068.crt
- Baltimore_CyberTrust_Root.crt
- BJCA_Global_Root_CA1.crt
- BJCA_Global_Root_CA2.crt
- Buypass_Class_2_Root_CA.crt
- Buypass_Class_3_Root_CA.crt
- CA_Disig_Root_R2.crt
- Certainly_Root_E1.crt
- Certainly_Root_R1.crt
- Certigna.crt
- Certigna_Root_CA.crt
- certSIGN_ROOT_CA.crt
- certSIGN_Root_CA_G2.crt
- Certum_EC-384_CA.crt
- Certum_Trusted_Network_CA.crt
- Certum_Trusted_Network_CA_2.crt
- Certum_Trusted_Root_CA.crt
- CFCA_EV_ROOT.crt
- CommScope_Public_Trust_ECC_Root-01.crt
- CommScope_Public_Trust_ECC_Root-02.crt
- CommScope_Public_Trust_RSA_Root-01.crt
- CommScope_Public_Trust_RSA_Root-02.crt
- Comodo_AAA_Services_root.crt
- COMODO_Certification_Authority.crt
- COMODO_ECC_Certification_Authority.crt
- COMODO_RSA_Certification_Authority.crt
- DigiCert_Assured_ID_Root_CA.crt
- DigiCert_Assured_ID_Root_G2.crt
- DigiCert_Assured_ID_Root_G3.crt
- DigiCert_Global_Root_CA.crt
- DigiCert_Global_Root_G2.crt
- DigiCert_Global_Root_G3.crt
- DigiCert_High_Assurance_EV_Root_CA.crt
- DigiCert_TLS_ECC_P384_Root_G5.crt
- DigiCert_TLS_RSA4096_Root_G5.crt
- DigiCert_Trusted_Root_G4.crt
- D-TRUST_BR_Root_CA_1_2020.crt
- D-TRUST_EV_Root_CA_1_2020.crt
- D-TRUST_Root_Class_3_CA_2_2009.crt
- D-TRUST_Root_Class_3_CA_2_EV_2009.crt
- emSign_ECC_Root_CA_-_C3.crt
- emSign_ECC_Root_CA_-_G3.crt
- emSign_Root_CA_-_C1.crt
- emSign_Root_CA_-_G1.crt
- Entrust.net_Premium_2048_Secure_Server_CA.crt
- Entrust_Root_Certification_Authority.crt
- Entrust_Root_Certification_Authority_-_EC1.crt
- Entrust_Root_Certification_Authority_-_G2.crt

- Entrust_Root_Certification_Authority_-_G4.crt
- ePKI_Root_Certification_Authority.crt
- e-Szigno_Root_CA_2017.crt
- GDCA_TrustAUTH_R5_ROOT.crt
- GlobalSign_ECC_Root_CA_-_R4.crt
- GlobalSign_ECC_Root_CA_-_R5.crt
- GlobalSign_Root_CA.crt
- GlobalSign_Root_CA_-_R3.crt
- GlobalSign_Root_CA_-_R6.crt
- GlobalSign_Root_E46.crt
- GlobalSign_Root_R46.crt
- GLOBALTRUST_2020.crt
- Go_Daddy_Class_2_CA.crt
- Go_Daddy_Root_Certificate_Authority_-_G2.crt
- GTS_Root_R1.crt
- GTS_Root_R2.crt
- GTS_Root_R3.crt
- GTS_Root_R4.crt
- HARICA_TLS_ECC_Root_CA_2021.crt
- HARICA_TLS_RSA_Root_CA_2021.crt
- Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt
- Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt
- HiPKI_Root_CA -_G1.crt
- Hongkong_Post_Root_CA_3.crt
- IdenTrust_Commercial_Root_CA_1.crt
- IdenTrust_Public_Sector_Root_CA_1.crt
- ISRG_Root_X1.crt
- ISRG_Root_X2.crt
- Izenpe.crt
- Microsec_e-Szigno_Root_CA_2009.crt
- Microsoft_ECC_Root_Certificate_Authority_2017.crt
- Microsoft_RSA_Root_Certificate_Authority_2017.crt
- NAVER_Global_Root_Certification_Authority.crt
- NetLock_Arany_=Class_Gold=Főtanúsítvány.crt
- OISTE_WISeKey_Global_Root_GB_CA.crt
- OISTE_WISeKey_Global_Root_GC_CA.crt
- QuoVadis_Root_CA_1_G3.crt
- QuoVadis_Root_CA_2.crt
- QuoVadis_Root_CA_2_G3.crt
- QuoVadis_Root_CA_3.crt
- QuoVadis_Root_CA_3_G3.crt
- Sectigo_Public_Server_Authentication_Root_E46.crt
- Sectigo_Public_Server_Authentication_Root_R46.crt
- Secure_Global_CA.crt
- SecureSign_RootCA11.crt
- SecureTrust_CA.crt
- Security_Communication_ECC_RootCA1.crt
- Security_Communication_Root_CA.crt
- Security_Communication_RootCA2.crt
- Security_Communication_RootCA3.crt
- SSL.com_EV_Root_Certification_Authority_ECC.crt
- SSL.com_EV_Root_Certification_Authority_RSA_R2.crt
- SSL.com_Root_Certification_Authority_ECC.crt
- SSL.com_Root_Certification_Authority_RSA.crt
- SSL.com_TLS_ECC_Root_CA_2022.crt
- SSL.com_TLS_RSA_Root_CA_2022.crt

- Starfield_Class_2_CA.crt
- Starfield_Root_Certificate_Authority_-_G2.crt
- Starfield_Services_Root_Certificate_Authority_-_G2.crt
- SwissSign_Gold_CA_-_G2.crt
- SwissSign_Silver_CA_-_G2.crt
- SZAFIR_ROOT_CA2.crt
- Telia_Root_CA_v2.crt
- TeliaSonera_Root_CA_v1.crt
- TrustAsia_Global_Root_CA_G3.crt
- TrustAsia_Global_Root_CA_G4.crt
- Trustwave_Global_Certification_Authority.crt
- Trustwave_Global_ECC_P256_Certification_Authority.crt
- Trustwave_Global_ECC_P384_Certification_Authority.crt
- T-TeleSec_GlobalRoot_Class_2.crt
- T-TeleSec_GlobalRoot_Class_3.crt
- TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt
- TunTrust_Root_CA.crt
- TWCA_Global_Root_CA.crt
- TWCA_Root_Certification_Authority.crt
- UCA_Extended_Validation_Root.crt
- UCA_Global_G2_Root.crt
- USERTrust_ECC_Certification_Authority.crt
- USERTrust_RSA_Certification_Authority.crt
- vTrus_ECC_Root_CA.crt
- vTrus_Root_CA.crt
- XRamp_Global_CA_Root.crt

TLS Cipher list

To improve the security of ThinOS devices, some outdated and less-secure TLS ciphers are removed in the future release. Some TLS ciphers are not secure and are subject to change in the future release.

Table 61. TLS Cipher list

Ciphers	Security Status
ECDHE-RSA-AES128-GCM-SHA256	Secure
ECDHE-RSA-AES256-GCM-SHA384	Secure
ECDHE-RSA-AES128-SHA256	Disabled by default in the future release
ECDHE-RSA-AES256-SHA384	Disabled by default in the future release
ECDHE-RSA-AES128-SHA	Removed in future release
ECDHE-RSA-AES256-SHA	Removed in future release
DHE-RSA-AES128-GCM-SHA256	Removed in future release
DHE-RSA-AES256-GCM-SHA384	Removed in future release
DHE-RSA-AES128-SHA256	Removed in future release
DHE-RSA-AES256-SHA256	Removed in future release
DHE-RSA-AES128-SHA	Removed in future release
DHE-RSA-AES256-SHA	Removed in future release
AES128-SHA256	Not Supported
AES256-SHA256	Not Supported
AES128-SHA	Not Supported

Table 61. TLS Cipher list (continued)

Ciphers	Security Status
AES256-SHA	Not Supported
AES128-GCM-SHA256	Not Supported
AES256-GCM-SHA384	Not Supported
ECDHE-ECDSA-AES128-GCM-SHA256	Secure
ECDHE-ECDSA-AES256-GCM-SHA384	Secure
ECDHE-ECDSA-AES128-SHA256	Disabled by default in the future release
ECDHE-ECDSA-AES256-SHA384	Disabled by default in the future release
ECDHE-ECDSA-AES128-SHA	Removed in future release
ECDHE-ECDSA-AES256-SHA	Removed in future release
DHE-PSK-AES128-GCM-SHA256	Removed in future release
DHE-PSK-AES256-GCM-SHA256	Removed in future release
DHE-PSK-AES128-CBC-SHA256	Removed in future release
DHE-PSK-AES256-CBC-SHA384	Removed in future release
DHE-PSK-AES128-CBC-SHA	Removed in future release
DHE-PSK-AES256-CBC-SHA	Removed in future release
ECDHE-PSK-AES128-CBC-SHA	Removed in future release
ECDHE-PSK-AES256-CBC-SHA	Removed in future release
ECDHE-PSK-AES128-CBC-SHA256	Disabled by default in the future release
ECDHE-PSK-AES256-CBC-SHA384	Disabled by default in the future release
PSK-AES128-GCM-SHA256	Removed in future release
PSK-AES256-GCM-SHA384	Removed in future release
PSK-AES128-CBC-SHA	Removed in future release
PSK-AES256-CBC-SHA	Removed in future release
PSK-AES128-CBC-SHA256	Removed in future release
PSK-AES256-CBC-SHA384	Removed in future release
RSA-PSK-AES128-GCM-SHA256	Removed in future release
RSA-PSK-AES256-GCM-SHA384	Removed in future release
RSA-PSK-AES128-CBC-SHA	Removed in future release
RSA-PSK-AES256-CBC-SHA	Removed in future release
RSA-PSK-AES128-CBC-SHA256	Removed in future release
RSA-PSK-AES256-CBC-SHA384	Removed in future release
ECDHE-ECDSA-CHACHA20-POLY1305	Removed in future release
ECDHE-RSA-CHACHA20-POLY1305	Removed in future release
DHE-RSA-CHACHA20-POLY1305	Removed in future release
RSA-PSK-CHACHA20-POLY1305	Removed in future release
DHE-PSK-CHACHA20-POLY1305	Removed in future release
ECDHE-PSK-CHACHA20-POLY1305	Removed in future release

Table 61. TLS Cipher list (continued)

Ciphers	Security Status
PSK-CHACHA20-POLY1305	Removed in future release
SRP-RSA-AES-256-CBC-SHA	Removed in future release
SRP-AES-256-CBC-SHA	Removed in future release
SRP-RSA-AES-128-CBC-SHA	Removed in future release
SRP-AES-128-CBC-SHA	Removed in future release
TLS_AES_128_GCM_SHA256	Secure
TLS_AES_256_GCM_SHA384	Secure
TLS_CHACB42:D66HA20_POLY1305_SHA256	Secure

Trusted Platform Module version 2.0

All ThinOS devices support disk encryption and decryption through Trusted Platform Module (TPM) version 2.0. If the key in TPM does not match the current build, the ThinOS fails to boot.

NOTE: Do not change the TPM status in BIOS or clear TPM.

The following SSL/TLS ciphers are supported:

- TLS1.2_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS1.2_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS1.3_AES256_GCM_SHA384
- TLS1.3_AES128_GCM_SHA256

13

Using Wyse Management Suite

Functional areas of Wyse Management Suite console

The Wyse Management Suite console is organized into the following functional areas:

- The **Dashboard** page provides information about the current status on each functional area of the system.
- The **Groups & Configs** page employs a hierarchical group policy management for device configuration. Optionally, subgroups of the global group policy can be created to categorize devices according to corporate standards. For example, devices may be grouped based on job function, device type, and so on.
- The **Users** page enables local users and users imported from the Active Directory to be assigned global administrator, group administrator, and viewer roles to log in to Wyse Management Suite. Users are given permissions to perform operations based on the roles assigned to them.
- The **Devices** page enables you to view and manage devices, device types, and device-specific configurations.
- The **Apps & Data** page provides management of device applications, operating system images, policies, certificate files, logos, and wallpaper images.
- The **Waves** page enables administrators to schedule and deploy ThinOS firmware, BIOS, or application packages in a phased manner. This enables the administrator to test the new firmware, BIOS, or packages on selected devices before deploying to a larger group.
- The **Rules** page enables you to add, edit, and enable or disable rules such as auto grouping and alert notifications.
- The **Jobs** page enables you to create jobs for tasks such as reboot, WOL, and application or image policy that need to be deployed on registered devices.
- The **Events** page enables you to view and audit system events and alerts.
- The **Portal Administration** page enables you to configure various system settings such as local repository configuration, license subscription and more.

Managing groups and configurations

The **Groups & Configs** page enables you to define policies that are required to configure your devices. You can create sub groups of the global group policies and categorize devices based on your requirements. For example, devices may be grouped based on job functions, device type, and so on.

By default, the Default Device Policy Group and Default User Policy Group are present on the **Groups & Configs** page.

Devices inherit policies in the order that they are created. The settings that are configured in a default policy group are applied as default settings in all the policies listed in the default policy group. In a group, all devices present in that group have default policy group as their default settings.

Create a default device policy group

You can create groups for the global device group policies and categorize devices based on your requirements.

Steps

1. On the **Groups & Configs** page, click the **Default Device Policy Group** option.
2. Click +.
3. In the **Add New Group** dialog box, enter the **Group Name** and **Description**.
4. Select the **This is a ThinOS Select group parent** option to create a parent select group for ThinOS devices. This step is optional.

   For more information, see Create a ThinOS Select group.
5. In the **Registration** tab, select the **Enabled** check box under Group Token.
6. Enter the group token.

7. Assign a group administrator (optional).

   In the **Administration** tab, select the users from the **Available Group Admins** list and move them to the **Assigned Group Admins** list using the right arrow button. These users will then be responsible for managing this group.

8. Click **Save**.

   The group is added to the list of available groups on the **Groups & Configs** page.

   NOTE: The devices can be registered to a group by entering the group token which is available in the **Groups and Configs** page for the respective group.

Create a ThinOS Select group

Steps

1. On the **Groups & Configs** page, click the **Default Device Policy Group** option or any parent group.
2. Click +.
3. In the **Add New Group** dialog box, enter the **Group Name** and **Description**.
4. Select the **This is a ThinOS Select group parent** option.
5. Select the **Enable Device Exception To Override Select Group Policy** if you want the device exception policies to override the select group policies.

   This option is available only for a Parent Select group and is not available for the default device policy group or any custom device policy group.

6. Select the name of the group administrators who are tasked with managing this group.
   - From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box.
   - To move one group from the **Assigned Group Admins** to **Available Group Admins**, do the reverse.

   These steps are optional.

7. Click **Save**.

   The group is added to the list of available groups on the **Groups & Configs** page.

   To add subgroups to the created parent group, click the parent group on the **Groups & Configs** page, and follow the steps that are mentioned in Create device policy group.

   NOTE: The parent select group can have 10 child select groups, and you can register the devices to the child select group. Profiles can be configured for other operating systems. The created profiles are the same as other custom groups.

   NOTE: Some policies that are changed in subgroups require a client reboot for the changes to take effect.

Wyse Management suite Active Directory group feature matrix

Table 62. Wyse Management suite Active Directory group feature matrix

Feature	Sub-Feature	AD User Group	User Exception	Select Group (Child group)
Region&Language Settings	Region & Language	Supported	Supported	Supported
Privacy&Security	SCEP	Not applicable	Not applicable	Supported
Privacy&Security	Device Security	Not applicable	Not applicable	Supported
Privacy&Security	Account Privileges	Not applicable	Not applicable	Supported
Privacy&Security	Certificates	Not applicable	Not applicable	Supported
Privacy&Security	Security Policy	Supported	Supported	Supported
Privacy&Security	Kerberos	Not applicable	Not applicable	Supported
Broker Settings	Global Broker Settings	Supported	Supported	Supported

Table 62. Wyse Management suite Active Directory group feature matrix (continued)

Feature	Sub-Feature	AD User Group	User Exception	Select Group (Child group)
Broker Settings	Citrix Virtual Apps and Desktops Settings	Supported	Supported	Supported
Broker Settings	Omnissa Horizon Settings	Supported	Supported	Supported
Broker Settings	Azure Virtual Desktop Settings	Supported	Supported	Supported
Broker Settings	Microsoft Remote Desktop Settings	Supported	Supported	Supported
Broker Settings	Amazon WorkSpaces Settings	Supported	Supported	Supported
Session Settings	Global Session Settings	Supported	Supported	Supported
Session Settings	Citrix Session Settings	Supported	Supported	Supported
Session Settings	Blast Session Settings	Supported	Supported	Supported
Session Settings	PCoIP Session Settings	Supported	Supported	Supported
Session Settings	RDP and AVD Session Settings	Supported	Supported	Supported
VDI Configuration Editor	Citrix Configuration Editor	Supported	Supported	Supported
VDI Configuration Editor	Horizon Blast Configuration Editor	Supported	Supported	Supported
VDI Configuration Editor	Zoom Plugin Configuration Editor	Supported	Supported	Supported
VDI Configuration Editor	Avaya Configuration Editor	Supported	Supported	Supported
Login Experience	3rd Party Authentication	Not applicable	Not applicable	Not supported
Login Experience	SmartCard Settings	Not applicable	Not applicable	Supported
Login Experience	Login Settings	Not applicable	Not applicable	Supported
Login Experience	Session setttings	Not applicable	Not applicable	Supported
Personalization	Shortcut Keys	Supported	Supported	Supported
Personalization	Device Info	Supported	Supported	Supported
Personalization	Desktop	Supported	Supported	Supported
Personalization	Screen Saver	Supported	Supported	Supported
Personalization	User Experience Settings	Supported	Supported	Supported
Peripheral Management	RFIdeas Reader	Supported	Supported	Supported
Peripheral Management	Printers	Supported	Supported	Supported
Peripheral Management	Audio	Supported	Supported	Supported

Table 62. Wyse Management suite Active Directory group feature matrix (continued)

Feature	Sub-Feature	AD User Group	User Exception	Select Group (Child group)
Peripheral Management	Touch	Supported	Supported	Supported
Peripheral Management	Serial Port	Supported	Supported	Supported
Peripheral Management	USB Redirection	Supported	Supported	Supported
Peripheral Management	Monitor	Supported	Supported	Supported
Peripheral Management	Mouse	Supported	Supported	Supported
Peripheral Management	Keyboard	Supported	Supported	Supported
Peripheral Management	Camera	Supported	Supported	Supported
Peripheral Management	Device Headset Settings	Supported	Supported	Supported
Peripheral Management	CCID	Not applicable	Not applicable	Supported
Peripheral Management	Touchpad	Supported	Supported	Supported
Firmware	OS Firmware Updates	Not applicable	Not applicable	Supports only the parent select group
Firmware	Application Package Updates	Not applicable	Not applicable	Supports only the parent select group
Firmware	BIOS Firmware Updates	Not applicable	Not applicable	Supports only the parent select group
System Settings	Power and Sleep Settings	Not applicable	Not applicable	Supported
System Settings	Scheduled Reboot Settings	Not applicable	Not applicable	Supported
System Settings	Scheduled Shutdown Settings	Not applicable	Not applicable	Supported
System Settings	Device Settings	Not applicable	Not applicable	Supported
System Settings	Device Monitoring	Not applicable	Not applicable	Supported
Network Configuration	Ethernet Settings	Not applicable	Not applicable	Supported
Network Configuration	DHCP Settings	Not applicable	Not applicable	Supported
Network Configuration	DNS Settings	Not applicable	Not applicable	Supported
Network Configuration	VPN Settings	Not applicable	Not applicable	Supported
Network Configuration	Bluetooth Settings	Not applicable	Not applicable	Supported
Network Configuration	Proxy Settings	Not applicable	Not applicable	Supported

Table 62. Wyse Management suite Active Directory group feature matrix (continued)

Feature	Sub-Feature	AD User Group	User Exception	Select Group (Child group)
Network Configuration	Wireless	Not applicable	Not applicable	Supported
Network Configuration	Common Settings	Not applicable	Not applicable	Supported
Network Configuration	SNMPV3 Settings	Not applicable	Not applicable	Supported
Services	VNC Service	Not applicable	Not applicable	Supported
Services	WMS Settings	Not applicable	Not applicable	Not applicable
Services	WDA Settings	Not applicable	Not applicable	Not applicable
Services	Troubleshooting Settings	Not applicable	Not applicable	Supported
BIOS	Dell Wyse 3040	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell Wyse 5070	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell Wyse 5470	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell Wyse 5470 AIO	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell OptiPlex 5400 AIO	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell OptiPlex 3000	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell Latitude 3420	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell Latitude 3440	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell Latitude 5440	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell OptiPlex All-in-One 7410	Not applicable	Not applicable	Supports only the parent select group
BIOS	Dell OptiPlex All-in-One 7420	Not applicable	Not applicable	Supports only the parent select group

Edit a ThinOS select group

Steps

1. Go to the **Groups & Configs** page and click the ThinOS select group that you want to edit.
2. Click .
3. In the **Editing Default Policy group** dialog box, edit the group information such as **Group Name** and **Description**.
4. In the **Administration** tab, select the name of group administrators who are tasked with managing this group. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box. To move one group from the **Assigned Group Admins** to **Available Group Admins**, click the left arrow. This step is optional.
5. Click **Save**.

Edit a default device policy group

Steps

1. Go to the **Groups & Configs** page and select the **Default Device Policy Group**.
2. In the **Editing Default Device Policy Group** dialog box, edit the required group information.
3. Click **Save**.

Create a user policy group

You can create groups for the global user group policies and categorize users and devices based on their user groups.

Steps

1. On the **Groups & Configs** page, click the **Default User Policy Group** option.
2. Click +.
3. In the **Add New Group** dialog box, enter the **Group Name**, **Description**, **Domain**, **AD Attribute** (AD group or OU group) and **AD Attribute Name** which is the name present in the AD domain. You must use the **Group Name** as the **AD Attribute name**.

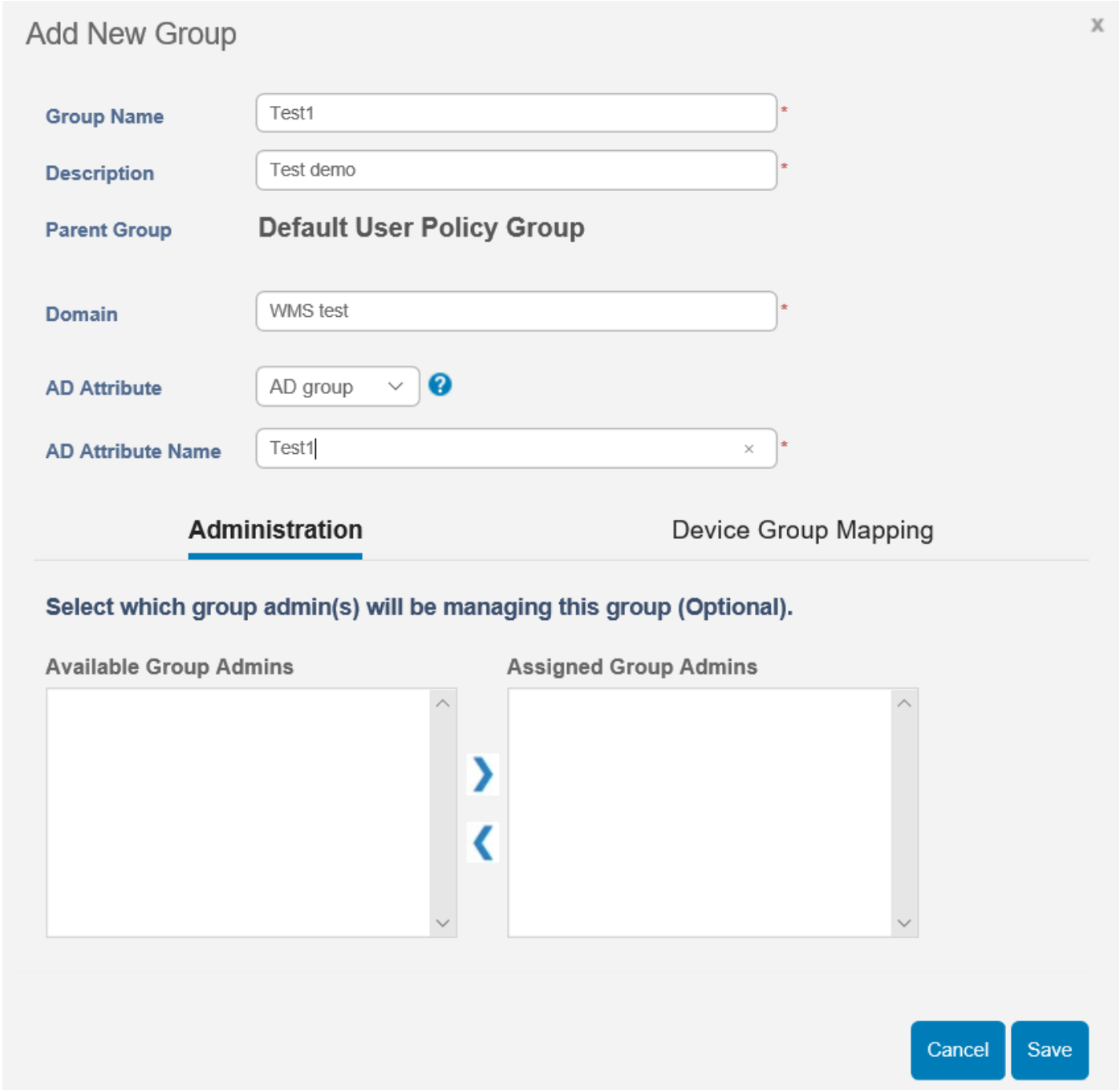

Figure 69. Add a new group

NOTE: If the AD group is inside an OU group in the domain, then you must select the OU group as the AD Attribute.

4. Select the name of the group administrators who are tasked with managing this group.
5. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box.
   To move one group from the **Assigned Group Admins** to **Available Group Admins**, do the reverse.
6. Click **Save**.
   The group is added to the list of available groups on the **Groups & Configs** page.
   NOTE: A user policy group must be mapped to an AD group or an organizational unit, but not both.

7. Select the **Device Group Mapping** option to import user groups with device mapping to control the configurations that are applied to all device groups by default.

   AD User groups which are imported into Wyse Management Suite can be mapped to the respective device group. By mapping the devices, they do not receive unwanted user group policies.

   NOTE: By default, user groups are not mapped to a device group. If you select the **Default device group** policy, all sub-device groups are selected. This feature is available only on Wyse Management Suite Pro license. You can import 100 user groups to Wyse Management Suite.

   NOTE: User group and device group mapping supports up to 25 thousand devices.

   NOTE: Select Group is not supported in Device Group Mapping.

Edit a user policy group

Steps

1. Go to the **Groups & Configs** page and select the default user policy group.
2. Click .
3. In the **Editing Default User Policy group** dialog box, edit the required group information.
4. Click **Save**.

Edit an unmanaged group

Devices that belong to the unmanaged group do not use licenses or receive configuration or application-based policies. To add devices to an unmanaged group, use the unmanaged group device registration key as part of auto registration or manual device registration.

Steps

1. On the **Groups & Configs** page, select **Unmanaged Group**.
2. Click .
   The **Editing Unmanaged Group** page is displayed. The **Group Name** displays the name of the group.
3. Edit the following details:
   - **Description**—Displays a brief description of the group.
   - **Group Token**—Select this option to enable the group token.
4. Click **Save**.

   NOTE: For a public cloud, the group token for an unmanaged group must be enabled to register devices. For a private cloud, the group token for an unmanaged group is automatically enabled.

Remove a group

As an administrator, you can remove a group from the group hierarchy.

Steps

1. In the **Groups & Configs** page, select the group that you want to delete.
2. Click .
   A warning message indicating that this action removes one or more groups from the group tree hierarchy is displayed.
3. From the drop-down list, select a new group to move the users and devices in the current group.
4. Click **Remove Group**.

NOTE: When a device group is deleted, all the devices of the group are moved to a selected device group. When a user group is deleted, there are no devices or users who are associated with it.

Create and import bulk device exception file

From Wyse Management Suite 5.0 or later versions, you can deploy device exception configurations to multiple ThinOS 10.x devices.

Steps

1. Create a bulk device exception file. To create a file, do any of the following:
   - Create a group policy for a test group and then export that policy to a file. If the configuration contains passwords, they are replaced with * in the exported file. For example:

```
{
    "WMSVersion": "4.6.8",
    "exportedDate": "1581466633677",
    "deviceTypes": [
        {
            "type": 6,
            "configurations": {
                "version": "0.0.1",
                "sequence": 1581466506281,
                "parameters": {
                    "AdminModeUsername": {
                        "value": "admin",
                        "updatedAt": "1581466506234"
                    },
                    "AdminModePassword": {
                        "value": "********",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalName": {
                        "value": "outpatient",
                        "updatedAt": "1581466506234"
                    },
                    "TimeServer": {
                        "value": "10.10.10.10",
                        "updatedAt": "1581466506234"
                    },
                    "timeZone": {
                        "value": "America/Phoenix",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalNameCapital": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    },
                    "DeviceNICDefault": {
                        "value": "Wlan",
                        "updatedAt": "1581466506234"
                    },
                    "AdminMode": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    }
                }
            }
        }
    ]
}
```

   - Create a .json file using the following format:

```
{

"devices": {
```

```
<serialnumber>: {
"parameters": {
"<parametername>": {
       "value": <value>
},
"<parametername>": {
       "value": <value>
}
},
configurations: [<configuration name>]
}
}
"configurations": {
<configurationName>: {
"<parametername>": {
       "value": <value>
},
"<parametername>": {
       "value": <value>
}
  }
}
}
```

For example,

```
{
    "devices": {
        "F7TQ3P2": {
            "parameters": {
                "TerminalName": {
                    "value": "Test"
                },
                "vmwareAutoConnectList": {
                    "value": "vm9999"
                },
                "DHCPVendorID": {
                    "value": "Gyomu-200"
                },
            "DirectRDPCollection": {
            "values": [
              {
                "sequence": 1700463704675,
                "parameters": {
                  "DirectRDPFullscreen": {
                    "value": "no",
                    "updatedAt": "1700465732777"
                  },
                  "DirectRDPUsername": {
                    "value": "administrator",
                    "updatedAt": "1700463704701"
```

```
                    },
                    "DirectRDPAddress": {
                      "value": "192.168.1.119",
                      "updatedAt": "1700463704701"
                    },
                    "DirectRDPDomain": {
                      "value": "thegs.in",
                      "updatedAt": "1700463704701"
                    },
                    "DirectRDPDescription": {
                      "value": "wms",
                      "updatedAt": "1700463704701"
                            }
                        }
                      },
                      {
                          "sequence": 1705450533826,
                          "parameters": {
                              "DirectRDPAddress": {
                                  "value": "10.192.64.241:13389",
                                  "updatedAt": "1705450533852"
                              },
                              "DirectRDPDomain": {
                                  "value": "FUEFUKI",
                                  "updatedAt": "1705450533852"
                              },
                              "DirectRDPDescription": {
                                  "value": "DST001C",
                                  "updatedAt": "1705450533852"
                              }
                          }
                      }
                  ]
              }
          }
      }
    }
}
```


2. Compress and encrypt the file.

   NOTE: You can use 7-zip software to compress and encrypt the file.

   NOTE: File size should not be more than 1 MB.

3. Go to **Groups & Configs** and click **Import Policies**.
   The **Import Policies Wizard** screen is displayed.
4. Select **Bulk Device Exceptions**.
5. Click **Browse** and select the password encrypted .zip file.
6. Click **Next**.

   Select the device type configurations to import page is displayed.
7. Click **Next**.

   NOTE: Since you can bulk import a device exception file for ThinOS 10.x devices, you cannot configure the options in the page.

8. Enter the .zip file password that was used to zip the .json file.
9. Click **Next**.
   A summary of the bulk device exceptions import is displayed.
10. Click **Import**.

    After the configurations are imported, a report generation link is generated in the **Group & Configs** page which can be downloaded. A success message is displayed in the **Group & Configs** page.

    NOTE: If a device is not registered and the configurations are imported, exceptions are applied to this device only if the device registers with one of the preloaded serial numbers device in the next 30 days.

    NOTE: If a device is already registered and the configurations are imported with device serial number, then the device exceptions are applied to the device.

NOTE: Imported file is a password protected. AES-256 and ZipCrypto encryption is supported.

NOTE: Configurations such as certificates, wallpaper, logo, and so on, with resources associated with them are not imported.

Editing ThinOS 10.x policy settings

Prerequisites

- Create a group, with a group token, for the devices you want to push the application package.
- Register the thin client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 10.x**.
   The **Configuration Control | ThinOS** window is displayed.

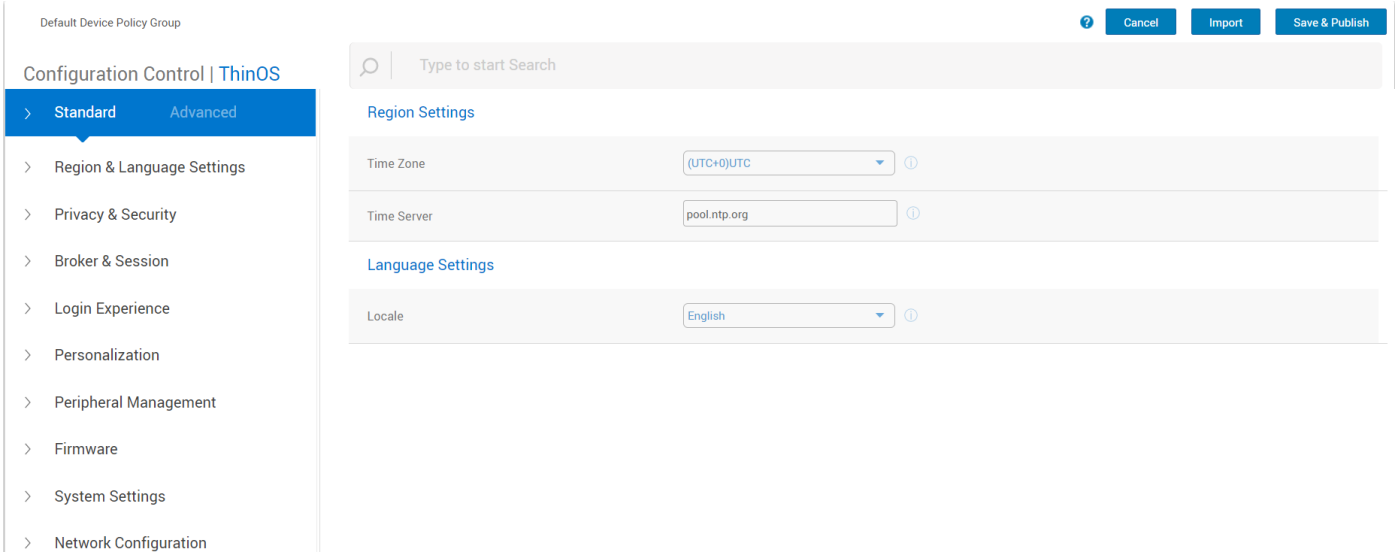

Figure 70. Configuration Control | ThinOS

3. Click the **Advanced** or **Standard** option.
4. Select the options that you want to configure.
5. In the respective fields, click the option that you want to configure.

   You can use the Global search option to find the relevant settings or parameters that are available in the Policy Settings. The search result displays the settings in the following order:
   - Setting
   - Parameter Group
   - Parameter sub group
   - Parameter
6. Configure the options as required.
7. Click **Save & Publish**.

   NOTE: After you click **Save & Publish**, the configured settings are also displayed in the **Standard** tab.

Managing devices

The **Device** page enables you to perform a routine device management task by using the management console. To locate the inventory of the devices, click the **Devices** tab. You can view a subset of the devices by using various filter criteria, such as groups or subgroups, device type, operating system type, status, subnet, platform, or time zone.

You can sort the device list based on the following:

- Name
- Device tag
- Platform type
- Operating system type
- Operating system version
- Serial number
- IP address
- Last user details
- Group details
- Last check-in time
- Health
- Registration status
- Write filter status

To view the **Device Details** page of a particular device, click the device entry that is listed on the page. All the configuration parameters of the device and the group level at which each parameter is applied are displayed on the **Device Details** page.

You can set the configuration parameter that is specific to the device.

NOTE: Parameters that are configured in this section override any parameters that were configured at the groups and/or at the global level.

Search a device using filters on the Devices page

About this task

To search a device using filters on the **Devices** page , do the following:

Steps

1. Go to the **Devices** page.
2. From the **Configuration Groups** drop-down list, select either the default policy group or the groups which are added by an administrator.
3. From the **Status** drop-down list, select any one of the following options:
   - **Registration**
     - Registered
     - Pre-registered
     - Not Registered
     - Enrollment validation
     - Compliant
     - Pending
     - Device exception
     - Non-Compliant
   - **Online Status**
     - Online
     - Offline
     - Unknown
   - **Others**
     - Recently Added
4. From the **OS Type** drop-down list, select ThinOS.
5. From the **OS Subtype** drop-down list, select a subtype for your operating system.

6. From the **Platform** drop-down list, select a platform.
7. From the **OS Version** drop-down list, select an OS version.
8. From the **Agent Version** drop-down list, select an agent version.
9. From the **Subnet/Prefix** drop-down list, select a subnet.
10. From the **Timezone** drop-down list, select the time zone.
11. From the **Device Tag** drop-down list, select the device tag.
12. Click **Save** to save the current filter.
    The **Save Current Filter** dialog box is displayed.
13. Enter the name and description for the filter.
14. Select the check box to set the current filter as the default option.
15. Click **Save Filter**.

View the display parameters

From Wyse Management Suite 5.0 or later versions, you can view the display setup of the devices running a Windows Embedded and ThinLinux operating system. You can view the vendor name, model number, serial number, resolution, aspect ratio, mode, alignment, and rotation details of the display setup.

Steps

1. Go to the **Devices** page.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.

   The **Device Details** page is displayed.

4. Go to **System Info** > **Peripherals**.
   You can view the display setup details.

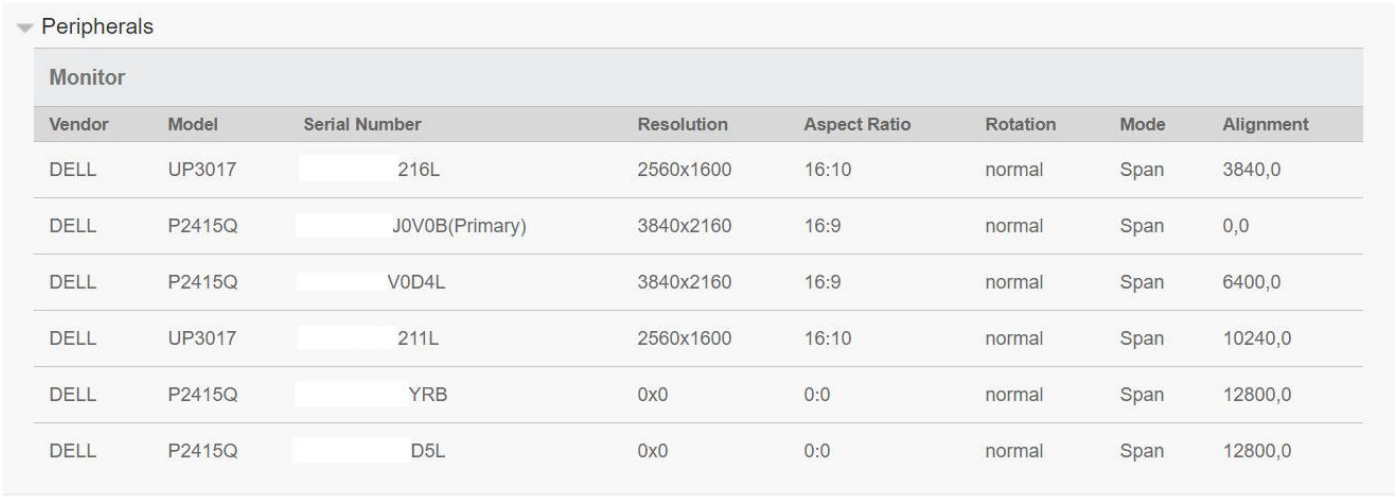

Figure 71. Display parameters

Viewing BIOS details

From Wyse Management Suite 5.0 or later, you can view the BIOS parameter value on the **Device Details** page.

Steps

1. Go to the **Devices** page.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.

3. Click any of the displayed devices.

   The **Device Details** page is displayed. You can view the BIOS details in the **BIOS settings** section of the **SystemInfo** tab.

Managing Jobs

The **Jobs** page enables you to schedule and manage jobs in the management console.

In this page you can see jobs based on the following filtering options:

- **Configuration Groups**—From the drop-down menu, select the configuration group type.
- **Scheduled by**—From the drop-down menu, select a scheduler who performs the scheduling activity. The available options are:
  - Admin
    - App Policy
    - Image Policy
    - Device Commands
  - System
    - Publish Group Configuration
    - Waves
    - Reports
    - Others
- **OS Type**—From the drop-down menu, select the operating system. The available options are:
  - ThinOS
  - ThinOS 10.x
  - WinIoT
  - Linux
  - Wyse Software Thin Client
  - Thin Linux
  - Edge Gateway—Ubuntu Core
  - Edge Gateway—Windows
  - Embedded PC—Windows
  - Embedded PC—Ubuntu
  - Dell Hybrid Client
  - Generic Client
- **Status**—From the drop-down menu, select the status of the job. The available options are:
  - Scheduled
  - Running/In Progress
  - Completed
  - Restarted
  - Canceled
  - Failed
- **Detail Status**—From the drop-down menu, select the status in detail. The available options are:
  - 1 or more failed
  - 1 or more pending
  - 1 or more In progress
  - 1 or more canceled
  - 1 or more completed
- **More Actions**—From the drop-down menu, select the **Sync BIOS Admin Password** option. The available options are:
  - Sync BIOS Admin Password
  - Delete Not Registered Devices
  - Restart Job for Offline Devices

  The Sync BIOS Admin Password Job window is displayed.

Schedule a device command job

Steps

1. On the **Jobs** page, click **Schedule device command job**.
   The **Device Command Job** screen is displayed.
2. Configure the following options:
   a. From the **Command** drop-down list, select a command. The available options are:
      - Restart
      - Wake-on-LAN
      - Initiate UWF Servicing Mode
      - Shutdown
      - Query
      - Re-Image
      - Lock—Applicable for ThinOS 8.x, ThinOS 9.x, and ThinOS 10.x devices
      - Send message—Applicable for Windows Embedded, ThinLinux, ThinOS 8.x, ThinOS 9.x, ThinOS 10.x, and Dell Hybrid Client powered devices
      - Factory Reset—Applicable for ThinOS 8.x, ThinOS 9.x, ThinOS 10.x, and Dell Hybrid Client powered devices
      - Soft Reset—Applicable for ThinOS 8.x, ThinOS 9.x, ThinOS 10.x, and Dell Hybrid Client powered devices
      - Rollback To Last Known Good Configuration—Applicable for ThinOS 8.x, ThinOS 9.x, ThinOS 10.x, and Dell Hybrid Client powered devices

      The device command is a recurring job. On selected days of the week and at a specific time the commands are sent to the selected devices.
   b. From the **OS Type** drop-down list, select the type of operating system.
   c. In the **Name** field, Enter the name of the job.
   d. From the **Group** drop-down list, select a group name.
   e. Enter the **Description** option.
   f. From the **Run** drop-down list and select one of the following:
      - **Immediately**—Enters the immediate time and date.
      - **On selected time zone and date/time**—Enters the particular selected time zone and date time.
      - **On selected date/time (of device time zone)**—Enters the particular selected date/time as per the time zone of the device.
   g. Enter or select the following details:
      - **Effective**—Enter the starting and ending date.
      - **Start between**—Enter the starting and ending time.
      - **On day(s)**—Select the days of the week.
3. Click the **Preview** option to view the details of the scheduled job.
4. On the next page, click the **Schedule** option to initiate the job.

Managing rules

The **Rules** page enables you to add and manage the rules in the Wyse Management Suite console. The following filtering options are provided:

- **Registration**
- **Failed to check-in**
- **Unmanaged Device Auto Assignment**
- **Alert Notification**

Edit a registration rule

About this task

Configure the rules for unmanaged devices by using the **Registration** option. To edit a registration rule, do the following:

Steps

1. Go to the **Rules** page.
2. Click **Registration** and select the unmanaged devices option.
3. Click **Edit Rule**.
   The **Edit Rule** window is displayed.

   You can view the following details:

   - Rule
   - Description
   - Device Target
   - Group
4. From the drop-down menu, select a target client to apply the **Notification Target** option and the time duration to apply the **Notification Frequency** option.

   NOTE: The notification frequency can be configured for every 4 hours, every 12 hours, daily, or weekly basis to the target device.
5. Enter the number of days until you want to apply the rule in the **Apply rule after (1–120 days)** box.

   NOTE: By default, registration of an unmanaged device are unregistered after 30 days.
6. Click **Save**.

Create unmanaged device auto assignment rules

About this task

To create rules for the unmanaged device auto assignment, do the following:

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Click the **Add Rules** tab.
4. Enter the **Name**, and select the **Destination group**.
5. Click the **Add Condition** option, and select the conditions for assigned rules.
6. Click **Save**.
   The rule is displayed in the unmanaged group list. This rule is applied automatically, and the device is listed in the destination group.

   NOTE:
   - If a select group is set as the Destination Group, the condition **Assign device to the destination group** is not available.
   - If a select group is set as the Destination Group, the condition **Create a group under the destination group for each unique value** is not available.

Edit an unmanaged device auto assignment rule

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Select the rule and click the **Edit** option.
4. Enter the **Name** and select the **Destination group**.
5. Click the **Add Condition** option and select the conditions for assigned rules.
6. Click **Save**.

Disable or delete a rule

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Select a rule and click the **Disable Rule** option.
   The selected rule is disabled.
4. Select the disabled rule and click the **Delete Disabled Rule(s)** option.
   The rule is deleted.

Save the rule order

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Select the rule which you want to move and then move it to the top order.
4. Click **Save Rule Order**.

Create a rule for alert notification

About this task

To create a rule for alert notification, do the following:

Steps

1. Click the **Rules** tab.
2. Select the **Alert Notification** option.
3. Click **Add Rule**.
   An **Add Rule** window is displayed.
4. From the **Rule** drop-down list, select a rule.
5. Enter the **Description**.
6. From the **Group** drop-down list, select the preferred option.
7. From the drop-down menu, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.
8. Click **Save**.

Edit an alert notification rule

Steps

1. Click the **Rules** tab.
2. Select the **Alert Notification** option.
3. Click **Edit Rule**.
   An **Edit Rule** window is displayed.
4. From the **Rule** drop-down list, select a rule.
5. Enter the **Description**.
6. From the **Groups** drop-down list, select a group.
7. From the drop-down list, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.
8. Click **Save**.

Managing Events

The **Events** page enables you to view all events and alerts in the management system using the management console. It also provides instructions on viewing an audit of events and alerts for system auditing purposes.

A summary of events and alerts is used to obtain an easy-to-read daily summary of what has happened in the system. The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

Search an event or alert using filters

Steps

1. Click **Events**.
   The **Events** page is displayed.
2. From the **Configuration Groups** drop-down menu, select either the default policy group or the groups which are added by an administrator.
3. From the **Events or Alerts** drop-down menu, select any one of the following options:
   - Events
   - Current Alerts
   - Alert History
4. From the **Timeframe** drop-down menu, select any one of the following operating systems:
   This option enables you to view the events which occurred in a particular timeframe. The available options in the drop-down menu are:
   - Today
   - Yesterday
   - This Week
   - Custom
5. From the **Event Type** drop-down menu, select the operating system.
   All the events are classified under particular groups. The available options in the drop-down menu are:
   - Access
   - Registration
   - Configuration
   - Remote Commands
   - Management
   - Compliance

Wyse Management Suite Security Compliance alerts

The following security compliance alerts are displayed in the Wyse Management Suite server depending on the scenarios on the ThinOS client:

Table 63. Wyse Management Suite Security Compliance alerts

Scenario	Description	Resolution
Device is using deprecated ciphers	ThinOS client is connecting to network with deprecated TLS ciphers.	Update the network environment to use secure TLS ciphers.
Default BIOS password has not been changed	The BIOS password of the ThinOS client is the default password **Fireport** or the field is empty.	Change the BIOS password in the ThinOS 10.x policy by going to **BIOS > Platform > Enable Admin Password > New BIOS Admin Password**.
Admin Mode is not enabled, or the Privilege Level is high	Admin mode is not enabled, or the Privilege Level is set to **High** on ThinOS client.	Enable Admin Mode and set Privilege Level to **None** or **Customize** in ThinOS 10.x policy by going to **Privacy & Security > Account Privileges**.

ThinOS device certificate expiry alerts

The Wyse Management Suite server displays alerts for ThinOS device certificates that are expiring in one to 120 days. The information can also be found on the Wyse Management Suite server Dashboard.

Managing users

The Users page enables you to perform a routine user management task in the management console. The following are the two types of users:

- **Administrators**—Wyse Management Suite administrator can be assigned the role of a global administrator, group administrator, or viewer.
  - A Global Administrator has access to all the Wyse Management Suite functions.
  - A Group Administrator has access to all assets and functions for specific groups that are assigned to them.
  - A viewer has read-only access to all the data and can be assigned permissions to trigger the specific real-time commands, such as shutdown and restart.

  If you select administrator, you can perform any of the following actions:
  - Add Admin
  - Edit Admin
  - Activate Admin (s)
  - Deactivate Admin (s)
  - Delete Admin (s)
  - Unlock Admin (s)
- **Unassigned Admins**—Users imported from the AD server are displayed on the **Unassigned admins** page. You can later assign a role to these users from the portal. For better and faster management of users, select the users of your choice based on the available filter options. If you select **Unmanaged Users**, you can perform any of the following actions:
  - Edit User
  - Activate User (s)
  - Deactivate User (s)
  - Delete User (s)

NOTE: To import users from the .CSV file, click **Bulk Import**.

Add a new admin profile

Steps

1. Go to the **Users** page.
2. Click **Administrator (s)**.
3. Click **Add Admin**.
   The **New Admin User** window is displayed.
4. Enter your email ID and username in the respective fields.
5. Select the check box to use the same username as mentioned in the email.
6. Do one of the following:
   - If you click the **Personal Information** tab, enter the following details:
     - First name
     - Last name
     - Title
     - Mobile phone number
   - If you click the **Roles** tab, enter the following details:
     a. In the **Roles** section, from the **Role** drop-down list, select the **Administrator role**.
        - Global Administrator
        - Group Administrator
        - Viewer

        NOTE: If you select the **Administrator role** as **Viewer**, the following administrative tasks are displayed:

- Query Device
- Unregister Device
- Restart/Shutdown Device
- Change Group Assignment
- Remote Shadow
- Lock Device
- Wipe Device
- Send Message
- WOL Device

b. In the **Password** section, do the following:
   i. Enter the custom password.
   ii. To generate any random password, select the **Generate random password** radio button.

7. Click **Save**.

Create a WMS custom role in Wyse Management Suite

Using Wyse Management Suite 3.1 or later versions, a global administrator can create a new administrator role and provide granular permissions for different functionalities of Wyse Management Suite. You can create multiple users using the Custom Global Administrator role.

Steps

1. Go to the **Users** tab.
2. Click **Administrator(s)**.
3. Click **Add Admin**.
   The **New Admin User** window is displayed.
4. Enter the email ID and username in the respective fields.
5. Click **Roles**.
6. From the **Role** drop-down list, select **Custom WMS Role**.
7. Under each category, select the appropriate function that the user is allowed to perform.
8. Click **Save**.
   The following table provides details about the supported and unsupported permissions that can be assigned to a custom role:

Table 64. Permissions for a custom role

Supported	Not supported
Edit or Remove Configuration	Bulk Device Exception
Add, Edit, Delete Groups	Create of Group Admin
Upload Reference files	Creation of Global Admin
Create device detail exception	Creation of Viewer Admin
Rules	Assigning Role to un-assigned Administrators
Apps and data	Subscription (Export and Import license)
Bulk import End users	Changing WMS server URL
Manage Remote Repository	Changing MQTT URL
Reports	Uploading Config UI
Others	Custom Branding
Active Directory on Portal Admin Page	N/A

Create auto assignment rules for unmanaged devices

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Click the **Add Rules** tab.
4. Enter the **Name** and select the **Destination group**.
5. Click the **Add Condition** option and select the conditions for assigned rules.
6. Click **Save**.

   The rule is displayed in the unmanaged group list. This rule is applied automatically and the device is listed in the destination group.

Add a user

Steps

1. Click the **Users** tab.
2. Click **End Users**.
3. Click **Add User**.
   The **Add User** window is displayed.
4. Enter the username, domain, first name, last name, email address, title, and phone number.
5. Click **Save**.

Bulk import end users

Steps

1. Click **Users**.
   The **Users** page is displayed.
2. Select the **End Users** option.
3. Click **Bulk Import**.
   The **Bulk Import** window is displayed.
4. Click **Browse**, and select the .csv file.
5. Click **Import**.

Create and import bulk device exception file

From Wyse Management Suite 5.0 or later versions, you can deploy device exception configurations to multiple ThinOS 10.x devices.

Steps

1. Create a bulk device exception file. To create a file, do any of the following:
   - Create a group policy for a test group and then export that policy to a file. If the configuration contains passwords, they are replaced with * in the exported file. For example:

```
{
    "WMSVersion": "4.6.8",
    "exportedDate": "1581466633677",
    "deviceTypes": [
        {
            "type": 6,
            "configurations": {
                "version": "0.0.1",
                "sequence": 1581466506281,
                "parameters": {
```

```
                    "AdminModeUsername": {
                        "value": "admin",
                        "updatedAt": "1581466506234"
                    },
                    "AdminModePassword": {
                        "value": "********",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalName": {
                        "value": "outpatient",
                        "updatedAt": "1581466506234"
                    },
                    "TimeServer": {
                        "value": "10.10.10.10",
                        "updatedAt": "1581466506234"
                    },
                    "timeZone": {
                        "value": "America/Phoenix",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalNameCapital": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    },
                    "DeviceNICDefault": {
                        "value": "Wlan",
                        "updatedAt": "1581466506234"
                    },
                    "AdminMode": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    }
                }
            }
        }
    ]
}
```

- Create a .json file using the following format:

```
{

"devices": {

<serialnumber>: {

"parameters": {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}

},

configurations: [<configuration name>]

}

}

"configurations": {

<configurationName>: {

"<parametername>": {
```

```
       "value": <value>

},

"<parametername>": {

       "value": <value>

}

  }

}

}
```

For example,

```
{
    "devices": {
        "F7TQ3P2": {
            "parameters": {
                "TerminalName": {
                    "value": "Test"
                },
                "vmwareAutoConnectList": {
                    "value": "vm9999"
                },
                "DHCPVendorID": {
                    "value": "Gyomu-200"
                },
            "DirectRDPCollection": {
            "values": [
              {
                "sequence": 1700463704675,
                "parameters": {
                  "DirectRDPFullscreen": {
                    "value": "no",
                    "updatedAt": "1700465732777"
                  },
                  "DirectRDPUsername": {
                    "value": "administrator",
                    "updatedAt": "1700463704701"
                  },
                  "DirectRDPAddress": {
                    "value": "192.168.1.119",
                    "updatedAt": "1700463704701"
                  },
                  "DirectRDPDomain": {
                    "value": "thegs.in",
                    "updatedAt": "1700463704701"
                  },
                  "DirectRDPDescription": {
                    "value": "wms",
                    "updatedAt": "1700463704701"
                            }
                        }
                    },
                    {
                        "sequence": 1705450533826,
                        "parameters": {
                            "DirectRDPAddress": {
                                "value": "10.192.64.241:13389",
                                "updatedAt": "1705450533852"
                            },
                            "DirectRDPDomain": {
                                "value": "FUEFUKI",
                                "updatedAt": "1705450533852"
                            },
                            "DirectRDPDescription": {
                                "value": "DST001C",
                                "updatedAt": "1705450533852"
```

```
                                    }
                                }
                            }
                        ]
                    }
                }
            }
        }
    }
}
```

2. Compress and encrypt the file.

   NOTE: You can use 7-zip software to compress and encrypt the file.

   NOTE: File size should not be more than 1 MB.

3. Go to **Groups & Configs** and click **Import Policies**.
   The **Import Policies Wizard** screen is displayed.
4. Select **Bulk Device Exceptions**.
5. Click **Browse** and select the password encrypted .zip file.
6. Click **Next**.
   Select the device type configurations to import page is displayed.
7. Click **Next**.

   NOTE: Since you can bulk import a device exception file for ThinOS 10.x devices, you cannot configure the options in the page.

8. Enter the .zip file password that was used to zip the .json file.
9. Click **Next**.
   A summary of the bulk device exceptions import is displayed.
10. Click **Import**.
    After the configurations are imported, a report generation link is generated in the **Group & Configs** page which can be downloaded. A success message is displayed in the **Group & Configs** page.

    NOTE: If a device is not registered and the configurations are imported, exceptions are applied to this device only if the device registers with one of the preloaded serial numbers device in the next 30 days.

    NOTE: If a device is already registered and the configurations are imported with device serial number, then the device exceptions are applied to the device.

    NOTE: Imported file is a password protected. AES-256 and ZipCrypto encryption is supported.

    NOTE: Configurations such as certificates, wallpaper, logo, and so on, with resources associated with them are not imported.

Portal administration

The **Portal administration** page enables the system administration to perform tasks that are required to set up and maintain your system.

Adding the Active Directory server information

You can import Active Directory users and user groups to the Wyse Management Suite private cloud.

Steps

1. Log in to the Wyse Management Suite private cloud.
2. Go to **Portal Admin** > **Console Settings** > **Active Directory (AD)**.
3. Click the **Add AD Server Information** link.
4. Enter the server details such as **AD Server Name**, **Domain Name**, **Server URL**, and **Port**.

5. Click **Save**.
6. Click **Import**.
7. Enter the username and password.

   NOTE: To search groups and users, you can filter them based on **Search Base**, and **Group name contains** options. You can enter the values as following:

   - `OU=<OU Name>`, for example, `OU=TestOU`
   - `DC=<Child Domain>, DC=<Parent Domain>, DC=com`, for example, `DC=Skynet, DC=Alpha, DC=Com`

   You can enter a space after a comma, but you cannot use single or double quotes.

8. Click **Login**.
9. On the **User Group** page, click **Group name** and enter the group name.
10. In the **Search** field, type the group name that you want to select.
11. Select a group.
    The selected group is moved to the right pane of the page.
12. In the **User Name Contents field**, enter the user name .
13. Click **Import Users** or **Import Groups**.

    NOTE: If you provide an invalid name or do not provide a last name, or provide any email address as name, then the entries cannot be imported into Wyse Management Suite. These entries are skipped during the user import process.

    The Wyse Management Suite portal displays a confirmation message with the number of imported active directory users. The imported active directory users are listed at **Users tab** > **Unassigned Admins**.
14. To assign different roles or permissions, select a user and click **Edit User**.

    After you assign the roles to the active directory user, they are moved to the **Administrators** tab on the **Users** page.

Next steps

Active directory users can log in to the Wyse Management Suite Management portal by using the domain credentials. To log in to the Wyse Management Suite portal, do the following:

1. Start the Wyse Management Suite management portal.
2. On the login screen, click the **Sign in with your domain credentials** link.
3. Enter the domain user credentials, and click **Sign In**.

To log in to the Wyse Management Suite portal using child domain credentials, do the following:

1. Start the Wyse Management Suite management portal.
2. On the login screen, click the **Sign in with your domain credentials** link.
3. Click **Change user domain**.
4. Enter the user credentials and the complete domain name.
5. Click **Sign In**.

The imported Active Directory users can be activated or deactivated on the **Users** page by using the global administrator login. If your account is deactivated, you cannot log in to the Wyse Management Suite Management portal.

NOTE: To import the users using LDAPS protocol, complete the following steps:

1. Import the AD Domain Server Root Certificate into Java Key Store Manually using the keytool. For example, `<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe -importcert -alias "WIN-O358EA52H8H" -keystore "<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"`
2. Restart Tomcat service.

Configuring Active Directory Federation Services feature on public cloud

You can configure Active Directory Federation Services (ADFS) on a public cloud.

Steps

1. On the **Portal Admin** page, under **Console Settings**, click **Active Directory (AD)**.
2. Enter the Wyse Management Suite details to ADFS. To know the location details on the ADFS server where you must upload the Wyse Management Suite .xml files, hover over the **information (i)** icon.

   NOTE: To download the Wyse Management Suite .xml file, click the download link.

3. Set the Wyse Management Suite rules in ADFS. To know the custom claim rule details, hover over the **information (i)** icon.

   NOTE: To view the Wyse Management rules, click the **Show WMS Rules** link. You can also download the Wyse Management Suite rules by clicking the link that is provided in the **Wyse Management Suite Rules** window.

4. To configure the ADFS details, click **Add Configuration**, and do the following:

   NOTE: To allow tenants to follow the ADFS configuration, upload the ADFS metadata file.

   a. To upload the .XML file stored on your thin client, click **Load XML file**.
   The file is available at `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`.
   b. Enter the details of the entity ID and X.509 signing certificate in the respective boxes.
   c. Enter the ADFS login URL address and the ADFS logout URL address in the respective boxes.
   d. To enable tenants to configure Single Sign-On by using ADFS, select the **Enable SSO login using ADFS** check box. This feature follows the Security Assertion and Markup Language (SAML) standard specification.
   e. To validate the configuration information, click **Test ADFS Login**. This enables tenants to test their setup before saving.

   NOTE: Tenants can activate/deactivate SSO login by using ADFS.

5. Click **Save**.
6. After you save the metadata file, click **Update Configuration**.

   NOTE: Tenants can log in and log out by using their AD credentials that are configured from their ADFS. You must ensure that the AD users are imported to the Wyse Management Suite server. On the login page, click **Sign in** and enter your domain credentials. You must provide the email address of your AD user and sign in. To import a user to the public cloud , remote repository must be installed. For more information about the ADFS documentation, go to Technet.microsoft.com.

Results

After the ADFS test connection is successful, import the users using AD connector present in the remote repository.

Import unassigned users or user groups to public cloud through active directory

Steps

1. Download and install the file repository, see Accessing file repository. The repository must be installed by using the company network and must have the access to the AD server to pull the users.
2. Register the repository to public cloud. Once registered, follow the steps mentioned on the UI to import the users to Wyse Management Suite public cloud. You can edit the roles of the AD user after importing to Wyse Management Suite public cloud.
3. Set up ADFS on public cloud.

Access Wyse Management Suite file repository

File repositories are places where **files** are stored and organized. Wyse Management Suite has two types of repositories:

- **Local Repository**—During the Wyse Management Suite private cloud installation, provide the local repository path in the Wyse Management Suite installer. After the installation, go to **Portal Admin** > **File Repository** and select the local repository. Click the **Edit** option to view and edit the repository settings.
- **Wyse Management Suite Repository**—Log in to Wyse Management Suite public cloud, go to ,**Portal Admin** > **File Repository** and download the Wyse Management Suite repository installer. After the installation, register the Wyse Management Suite repository to Wyse Management Suite Management server by providing the required information.

You can enable the **Automatic Replication** option to replicate files that are added to any of the file repositories to other repositories. When you enable this option, an alert message is displayed. You can select the **Replicate existing files** check box to replicate the existing files to your file repositories.

Replicate existing file option is applicable if the repository is already registered. When a new repository is registered, then all the files are copied to the new repository. You can view the file replication status in the **Events** page.

The `Image Pull` templates are not replicated automatically to other repositories. You must copy these files manually.

File Replication feature is supported only on repositories from Wyse Management Suite 2.0 and later versions.

You cannot import self-signed certificate of the remote repository to the Wyse Management Suite server. If the CA Validation is enabled for remote repository, then the replication of files from the remote repository to the local repository fails.

To use Wyse Management Suite repository, do the following:

1. Download the Wyse Management Suite repository from the public cloud console.
2. After the installation process, start the application.
3. On the Wyse Management Suite Repository page, enter the credentials to register the Wyse Management Suite repository to Wyse Management Suite server.
4. If you enable the **Register to Public WMS Management Portal** option, you can register the repository to Wyse Management Suite public cloud.
5. Click the **Sync Files** option to send the sync file command.
6. Click **Check In** and then click **Send Command** to send the device information command to the device.
7. Click the **Unregister** option to unregister the on-premises service.
8. Click **Edit** to edit the files.
9. From the drop-down list of **Concurrent File Downloads** option, select the number of files.
10. Enable or disable **Wake on LAN** option.
11. Enable or disable **Fast File Upload and Download (HTTP)** option.
    - When HTTP is enabled, the file upload and download occurs over HTTP.
    - When HTTP is not enabled, the file upload and download occurs over HTTPS.
12. Select the **Certificate Validation** check box to enable the CA validation for public cloud.

    NOTE: When CA Validation from Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations such as, Apps and Data, Image Pull/Push is successful. If certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate Certificate Authority** under **Events** page. All the operations such as, Apps and Data, Image Pull/Push is not successful. Also, when CA Validation from Wyse Management Suite server is disabled, the communication from server and client happens in secure channel without Certificate Signature validation.

13. Add a note in the provided box.
14. Click **Save Settings**.

Subnet mapping

From Wyse Management Suite 2.0, you can assign a subnet to a file repository. You can associate a file repository up to 25 subnets or ranges. You can also prioritize the subnets that are associated with the repository.

You can deploy the BIOS packages using subnet mapping from Wyse Management Suite 2.1 .You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository, or operator cloud repository. This feature is applicable only on Wyse Management Suite Pro license.

Configure subnet mapping

Steps

1. Go to **Portal Administration** > **File Repositories**.

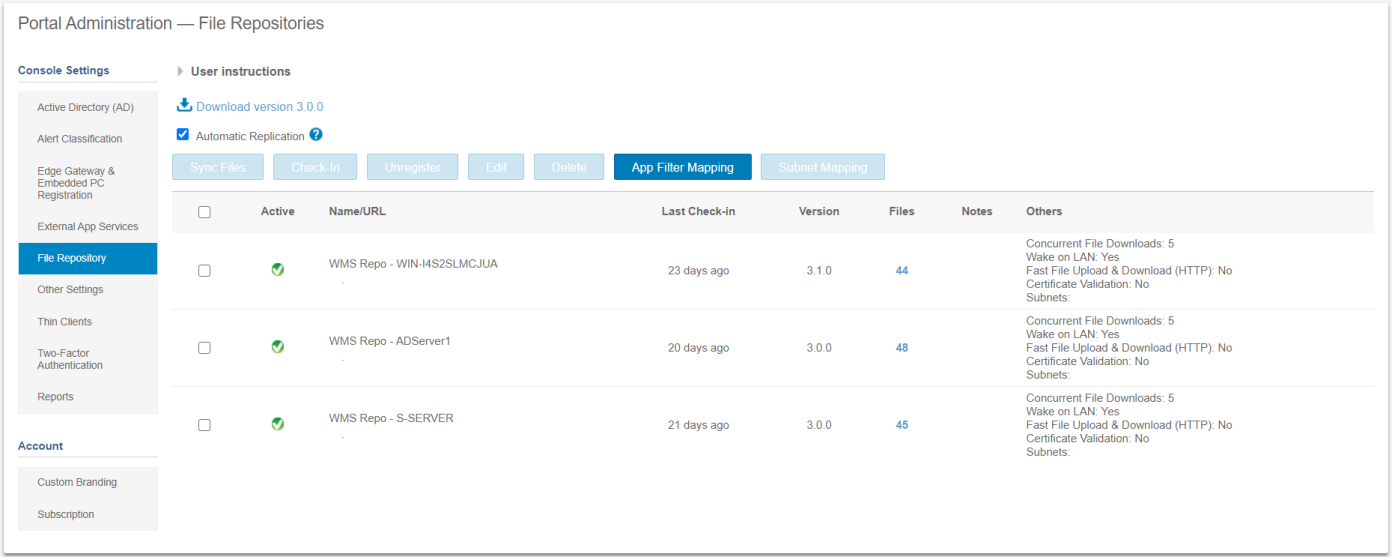

Figure 72. File repository

2. Select a file repository.
3. Click the **Subnet Mapping** option.
4. Enter subnets or ranges, one value per line. You must use hyphen for range separation.
5. Optionally, clear the **Allow devices from subnets not mapped to this file repository to download files from this repository as a fallback method using subnet proximity** check box if you want the file repository to be accessed only through the configured subnets or ranges.

   NOTE: The **Allow devices from subnets not mapped to this file repository to download files from this repository as a fallback method using subnet proximity** option is selected by default.

Capture device screenshot using WMS

Explains how ThinOS 10.x allows administrators to remotely request a screenshot from the Device Details page on WMS, enabling quick visual troubleshooting and device state verification.

About this task

After initiating a screen shot request from WMS, the ThinOS 10.x device displays a consent prompt for the user. Once approved, WMS retrieves the current screen image and displays it in the UI section for administrator review.

Steps

1. Log in to **WMS** as an administrator.
2. Go to the **Devices** page and select the device.
   The **Device Details** page is displayed.
3. Click **Request Screen Shot**.
4. On the ThinOS device, click **Allow** when the consent prompt appears.
   The captured device screenshot appears in the WMS UI page for the selected ThinOS device.

14

Troubleshooting your thin client

About this task

You can use the troubleshooting options on the ThinOS desktop to troubleshoot your device.

Steps

1. From the desktop menu, click **Troubleshooting**.
   The **Troubleshooting** dialog box is displayed.
2. Click the **General** tab, and use the following guidelines:
   - Click **Extract CMOS** to extract the CMOS settings and certain BIOS settings file is stored in `/wnos/trouble_shoot/ bios.json` folder of the USB drive.
   - Click the **Restore CMOS** option to write the CMOS settings and BIOS settings from the USB drive to the target thin client.
   - Click the **Performance Monitor** option to display the CPU usage history with the Memory and Networking information. The graphs display on top of all windows. When you play videos using MMR or HTML5 in a Citrix session, FPS is displayed on the performance monitor graph under the **CPU** tab. Omnissa Horizon Blast does not support this function in ThinOS 10.x.
   - Click the **Force Coredump** option to forcibly generate the debug information for technical investigation when your system is not responding. Both the coredump file and the trap information image are saved to the local drive. After you restart the thin client, both coredump file and trap issue screenshots are uploaded to the `/wnos/troubleshoot/` directory of the file server or a USB drive.
   - Click the **Export System Setting** option to export the system settings file to the USB drive that is connected to the thin client. The password is mandatory for the exported file. The file is stored in the `/wnos/trouble_shoot/` folder of the USB drive.
   - Click the **Export Screenshot** option to export the system screenshots to the USB drive that is connected to the thin client. The file is stored in the root folder of the USB drive.
   - Click the **Export logs** option to export the system log files to the USB drive that is connected to the thin client. The file is stored in the root folder of the USB drive—`system_log_201910107_125610.zip`
     - **Clear logs after exported**—Click the check box if you want the device to clear the logs after exporting it.
     - **Exlude core dumps**—Click the check box if you want the device to exclude the core dumps from exported logs.

     NOTE: You can export logs to a USB drive with NTFS format.
   - Click the **Import System Setting** option to import the system settings file from the USB drive that is connected to the thin client. The file is stored in the `/wnos/trouble_shoot/` folder of the USB drive.

     NOTE: You can import files to a USB drive with NTFS format.
   - Click the **Clear Log** option to delete all logs. After you clear logs, you must reboot the client to generate the logs again.
3. Click the **Capture** tab, and do the following:
   - **Capture Network Packets**—Use this option to capture network-related logs.
     a. To start logging the unexpected error messages, enable the **Capture Network Packets** option.
     b. To stop logging the unexpected error messages, disable the **Capture Network Packets** option.
     c. Connect a USB drive to the thin client.
     d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.zip`.
     e. Extract the `zip` file. The log files are available at `system_log_date,time,year/var/log/netmng/..`
   - **Capture Wireless Packets**—Use this option to capture wireless network-related logs.
     a. To start logging the unexpected error messages, enable the **Capture Wireless Packets** option, and click **OK**.
     b. To stop logging the unexpected error messages, disable the **Capture Wireless Packets** option, and click **OK**.
     c. Connect a USB drive to the thin client.

d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.zip`.
e. Extract the `zip` file. The log files are available at `system_log_date,time,year/var/log/netmng/..`

- If you want to capture the network-related logs for a long time, insert the USB drive, and enable **Capture Network/Wireless/Packets** option. The captured network-related log is directly stored in the `U disk ./wnos/trouble_shoot/` folder. If you want to capture network-related logs for a long time, follow these steps:
  a. Connect a USB drive to the thin client.
  b. Enable the **Capture Network/Wireless/Packets** option.
  c. Disable the **Capture Network/Wireless/Packets** option.
  d. Remove the USB drive as a personal device is required to read it.
  e. The network captures should be in `./wnos/trouble_shoot/`.
- **Capture USB Packets**—Use this option to capture USB packets.
  a. Connect a USB drive to the thin client.
  b. To start logging the unexpected error messages, enable the **Capture USB Packets** option, and click **OK**.
  c. To stop logging the unexpected error messages, disable the **Capture USB Packets** option, and click **OK**.
  d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.zip`.
  e. Extract the `zip` file. The log files are available at `system_log_date,time,year/var/usbdump/`.
- **Capture User Coredump**—Use this option to capture coredump files.
  a. Connect a USB drive to the thin client.
  b. To start logging the unexpected error messages, enable the **Capture User Coredump** option.
  c. To stop logging the unexpected error messages, disable the **Capture User Coredump** option.
  d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.zip`.
  e. Extract the `zip` file. The log files are available at `system_log_date,time,year/var/usbdump/`.
- **Capture Debug Logs**—Use this option to capture the debug logs.
  a. Connect a USB drive to the thin client.
  b. Enable the **Capture Debug Logs** option to set all log levels to the highest debug level. **Capture Debug Logs** is displayed at the bottom-right corner.
  c. Reboot the thin client.
  d. Disable **Capture Debug Logs** to set all log levels to default debug levels.
  e. Set the log file. The log file is automatically stored in the root folder of the `USB drive—system_log_201910107_125610.zip`.

4. Click the **Ping** tab, and do the following:

   NOTE: If you want to ping IPv6, you must first obtain the IPv6 address, and then enter the IPv6 address in the **Ping** input box. If you are entering the FQDN of IPv6, add **-6** to the end of the FQDN.

   a. Enter the IP address, DNS-registered hostname, or WINS-registered hostname of the target.
   b. Click **Start**.
   The data area displays the ping response messages. The ping command sends one echo request per second, calculates round-trip times and packet loss statistics, and displays a brief summary upon completing the calculation. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted by clicking **Stop**.

   NOTE: Ping sends an echo request to a network host. The host parameter is either a valid hostname or an IP address. If the host is operational and on the network, it responds to the echo request. Ping sends one echo request per second and calculates round-trip times and packet loss statistics. It displays a brief summary upon completion of the calculation.

   NOTE: Not all network equipment responds to ping packets, as it is a common mechanism that is used in denial-of-service attacks. Lack of response does not necessarily indicate that the target of the ping is unusable for other purposes.

5. Click the **Trace Route** tab, and do the following:
   a. Enter the IP address, DNS-registered hostname, or WINS-registered hostname of the target.
   b. Click **Start**.
   The data area displays round-trip response time and identifying information for each device in the path.

The trace route utility traces the path from your thin client to a network host. The host parameter is either a valid hostname or an IP address. The tracert utility sends out a packet of information three times to each device (routers and systems) in the path. The round-trip response time and the identifier information are displayed in the message box.

6. Click the **Telnet** tab, and do the following:
   a. Click **Telnet**.
   b. Enter the hostname.
   c. Enter a port number.
   d. Select a color theme.
   e. Click **Connect** to connect to a remote host or device.
7. Click the **Network** tab, and view detailed information that is related to your network connection.
   - Click the **Diagnostics** button to run a diagnostic test on your network connection.
   - Click the **Export log** button to export the network logs to the target device.
8. Click **Save** to save your settings.

Log Structure

The following table summarizes various log file types, their storage locations, and their descriptions.

Table 65. Log Structure

Name	Location	Description
network cap	`/var/log/netmng`	N/A
usb capture data	`/var/usbdump`	Data for USB data captured by usbdump
JVDI log	`/var/log/cisco/`	Log files of JVDI plug-in
WebexTeams	`/var/log/CiscoTeamsVDI/`	Log files directory of WebexTeams
WebexMeetings	`/var/log/ciscouvdi/`	Log files directory of WebexMeetings
Zoom	`home/dell/dell/.zoomvdi/logs/`	Log files directory of Zoom
Citrix	`/apps/Citrix/var/log/RTMediaEngineSRV/`	N/A
	`/var/log/citrix`	
ICA	`/home/warthog/.ICAClient/`	
Omnissa	`/tmp/omnissa-root`	
RDP	`/var/log/wlogd`	
webapp log	`/var/log/webapp/`	Log files for broker login process, Wyse Management Suite check-in, and Wyse Management Suite policy applying
http trace log	`/var/log/webapp/`	Log files for capturing http trace of broker login and Wyse Management Suite.
kernel core dump	`/var/crash`	Kernel coredump files
kernel log	• `/var/log/dmesg` • `/var/log/syslog`	Kernel messages
user applications core dump	`/var/log/usrcore/`	User application core dump files
opensc log	`/home/dell/opensc.log`	pcscd logs
Imprivata PIE log	`/home/dell/imprivata/runtime/log`	PIE logs
window system	`/var/log/win`	window logs

Table 65. Log Structure (continued)

Name	Location	Description
wlogd	/var/log/wlogd	wlogd logs
audio	/var/log/audio	system audio logs
wlan	/var/log/wlan	wlan logs
ramdisk	/var/log/ramdisk	ramdisk boot up logs
samba	/var/log/samba	samba log

Capture an HTTP log using ThinOS

To capture an HTTP log, do the following:

Steps

1. From the desktop menu, click **System Setup** or **System Settings** to access **Admin Policy Tool** > **Advanced** > **Services**. The **Configuration Control || ThinOS** window is displayed.
2. In the **Troubleshooting Settings** window, click the **Enable HTTP Log** option. The HTTP log feature is enabled on the thin client.
3. Log in to the Citrix session.

   If the authentication fails, do the following:

   a. Open the **Troubleshooting** window from the left menu on the ThinOS desktop.
   b. Connect the USB drive to the thin client, and click **Export logs**. All trace files including the event logs are exported to the USB drive. The log file is saved in the root folder of the USB drive—`system_log_20191107_125610.zip`.
   c. Extract the `.zip` file, and verify if the `com.thinos.log.file` file is available.

System crashes, freezes or restarts abruptly

If the system crashes, freezes, or restarts abruptly, coredump is generated. You must export logs to analyze the root cause for failure.

About this task

To export logs, do the following:

Steps

1. Reboot the thin client.
2. Export relevant logs using one of the following methods:
   - Use the **Export logs** option on the **General** tab in the **Troubleshooting** window on the ThinOS client.
   - Use the Wyse Management Suite console.
3. Analyze the detailed error log report.

Broker agent login failure

If log in to a Broker agent connection fails, you must do either of the following:

- Capture an HTTP log and analyze the detailed error log report.
- If the Broker agent can be accessed on a ThinOS 10 client, capture the network log and analyze the detailed error log report.

Citrix desktop and application crashes abruptly

If the Citrix desktop or application crashes abruptly, but the ThinOS client is still working, then a coredump is generated. You must export logs to analyze the root cause for failure.

About this task

To export logs, do the following:

Steps

1. Reboot the thin client.
2. Export relevant logs using one of the following methods:
   - Use the **Export logs** option on the **General** tab in the **Troubleshooting** window on the ThinOS client.
   - Use the Wyse Management Suite console.
3. Analyze the detailed error log report.

Unified Communications software call failure

If the Unified Communications software call fails, but the ThinOS client is still working, then a coredump is generated. You must export logs to analyze the root cause for failure. If the Unified Communications software fails to optimize, you can try to remove the application package and re-install it.

About this task

To export logs, do the following:

Steps

1. Reboot the thin client.
2. Export relevant logs using one of the following methods:
   - Use the **Export logs** option on the **General** tab in the **Troubleshooting** window on the ThinOS client.
   - Use the Wyse Management Suite console.
3. Analyze the detailed error log report.

Request a log file using Wyse Management Suite

Prerequisites

The device must be enabled to pull the log file.

Steps

1. Go to the **Devices** page, and click a particular device.
   The device details are displayed.
2. Click the **Device Log** tab.
3. Click **Request Log File**.
4. After the log files are uploaded to the Wyse Management Suite server, click the **Click here** link, and download the logs.

   NOTE: The ThinOS device uploads the system logs.

View audit logs using Wyse Management Suite

Steps

1. Go to **Events** > **Audit**.
2. From the **Configuration Groups** drop-down list, select a group for which you want to view the audit log.
3. From the **Timeframe** drop-down list, select the time period to view the events that occurred during that time period.
   The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

System log and trace information

Log/trace size and configuration

Table 66. Log/trace size and configuration

Type	Cleanup after maximum size	Comments
System log	10 MB	No encryption. It is required that admin users do not open this access to all other users. Only enable for target users.
Network/wireless trace	200 MB	
USB packet	200 MB	
HTTP log	10 MB	
System configuration	NA	During export, ask admin to encrypt with password

How to enable and collect logs?

Table 67. Enabling and collecting logs

Type	Enabling	Capturing	Collecting
System log	Always enabled	Always captured	Using Wyse Management Suite or USB drive
Network/wireless trace	Enable in Admin Policy Tool	Reboot after enabling	Using Wyse Management Suite or USB drive
USB packet	Enable in Admin Policy Tool	Reboot after enabling	Using Wyse Management Suite or USB drive
HTTP log	Enable in Admin Policy Tool	Reboot after enabling	Using Wyse Management Suite or USB drive

Table 68. Export Logs structure

Name	Location	Description	Export Log from Client	Export Log from WMS
network capture	/var/log/netmng	N/A	✓	Optional
usb capture data	/var/usbdump	data for USB data captured by usbdump	✓	✓
pcoip session log is in folder "client"				
JVDI log	/var/log/cisco/	log files of JVDI plugin	✓	✓
WebexTeams	/var/log/CiscoTeamsVDI/	log files directory of WebexTeams	✓	✓

Table 68. Export Logs structure (continued)

Name	Location	Description	Export Log from Client	Export Log from WMS
WebexMeetings	/var/log/ciscouvdi/	log files directory of WebexMeetings	✓	✓
Zoom	/home/dell/.zoom/logs/	log files direcotry of Zoom	✓	✓
Citrix	/apps/Citrix/var/log/RTMediaEngineSRV/	N/A	✓	✓
	/var/log/citrix			
ICA	/home/dell/.ICAClient/	N/A	✓	✓
Omnissa	/tmp/omnissa-root	N/A	✓	✓
RDP	/var/log/wlogd	N/A	✓	✓
webapp log	/var/log/webapp/	log files for broker login process, WMS check-in, WMS policy applying	✓	✓
http trace log	/var/log/webapp/	log files for capturing http trace of broker login, WMS.	✓	✓
kernel core dump	/var/crash	kernel coredump files	✓	Optional
kernel log	/var/log/kmessage	kernel messages	✓	✓
user applications core dump	/var/log/usrcore/	user app core dump files	✓	✓
opensc log	/home/dell/opensc.log	pcscd logs	✓	✓
Imprivata PIE log	/home/dell/imprivata/runtime/log	PIE logs	✓	✓
window system	/var/log/win	window logs	✓	✓
wlogd	/var/log/wlogd	wlogd logs	✓	✓
audio	/var/log/audio	system audio logs	✓	✓
wlan	/var/log/wlan	wlan logs	✓	✓
ramdisk	/var/log/ramdisk	ramdisk boot up logs	✓	✓
samba	/var/log/samba	samba log	✓	✓

15

Frequently Asked Questions

ThinOS FAQs

This section contains frequently asked questions that are related to Dell ThinOS.

What should I do if the package installation fails?

If the thin client does not work after upgrading to the new firmware, or if the package fails to update, remove all packages and reboot the thin client. After rebooting the thin client, reinstall the package.

Is Wyse Management Suite the only way to manage ThinOS 10.x?

ThinOS 10.x client can be managed using either Wyse Management Suite or Admin Policy Tool.

How can I verify the third-party binary versions on my ThinOS client?

On the ThinOS client, go to **System Tools** > **Packages**, and double-click the third-party package to see the binary version.

Can I use the USB Imaging Tool method to upgrade to ThinOS 10.x?

It is recommended that using Wyse Management Suite version to upgrade your thin clients since you cannot deploy large-scale clients using the USB Imaging Tool. However, you can use the USB Imaging Tool method for installing ThinOS 10.x on a single device.

Does ThinOS support zero desktop?

In ThinOS 10.x, the zero desktop is called modern desktop. You can enable the modern desktop mode using either Wyse Management Suite or the Admin Policy Tool.

How can I redirect my iPhone to the Citrix Desktop session?

Yes, an iPhone can be redirected to the Citrix Desktop session. To enable this, follow these steps:

Steps

1. Open **Global Connection Settings**.
2. Uncheck the options for **Exclude disk devices** and **Exclude audio devices**.

Why is my Android smartphone not displayed in the session when redirected or mapped?

If your Android smartphone is not displayed in the session, you need to ensure that the option to transfer images from your smartphone is selected when you connect the USB cable.

Does Citrix Workspace app replace Citrix Receiver on ThinOS?

In ThinOS 10.x, Citrix Receiver is replaced by Citrix Workspace app. Citrix Workspace app, a client software released by Citrix, enables you to access all your virtual apps, desktops, and other Citrix products from a single workspace UI. You must deploy the ICA package using Wyse Management Suite to install the Citrix Workspace app on ThinOS 10.x.

For more information about deploying packages using Wyse Management Suite, see How to upload and push ThinOS 10.x application packages.

What is Workspace mode on ThinOS?

Workspace mode on ThinOS allows you to customize the look and feel of your ThinOS device to align with the Citrix Workspace-based layout of published applications and desktops. When enabled, Workspace mode displays both the ThinOS full taskbar and the workspace desktop.

To enable Workspace mode, follow these steps:

1. Access the Admin Policy Tool or the Wyse Management Suite policy settings server.
2. Navigate to **Personalization** > **User Experience Settings**. Set the **System Mode** to **Classic**.
3. In **System Setup** > **Remote Connections** > **Broker Setup**, select the Workspace Mode checkbox.

NOTE: Citrix Workspace Mode can be enabled or disabled if the system mode is already configured as either **Mordern** or **Classic**.

Can I enable Flash content to be rendered using a local Flash Player on ThinOS?

ThinOS does not support the Flash Redirection feature. Hence, you cannot enable Flash content to be rendered using a local Flash Player.

How do I verify if the HDX Enlightened Data Transport Protocol is active?

To verify if the HDX Enlightened Data Transport Protocol is active:

- In an ICA desktop session, run the command `netstat -a -p UDP` in command prompt, and check if the VDA is using UDP ports 1494 and 2598.
- In an ICA desktop session, run the command `ctxsession.exe` in command prompt, and check if the transport protocol is using **UDP** > **CGP** > **ICA**.
- Go to Citrix Director, access the session details, and check if the Connection Type or Protocol is UDP.

Alternatively, you can use the HDX Monitor tool to check parameter Component_Protocol=UDP-CGP-ICA.

For more information, see the article **CTX220730** in the Citrix website.

How do I check if HTML5 Video Redirection is working?

Prerequisites

Ensure that you have enabled the HTML5 video redirection policy on the server side.

Steps

1. Launch a Citrix session on your thin client.
2. Open a web browser and play an HTML video.
3. Move the browser on the screen or scroll the browser.
4. Notice a delay or jump in the video window.
   This noticeable lag in the video window indicates that the video is being redirected.

How do I check if QUMU Multimedia URL Redirection is working?

Prerequisites

Ensure that you have installed the QUMU media player on the remote desktop.

Steps

1. Launch a Citrix session on your thin client.
2. Open a web browser and play a QUMU published video.
3. Move the browser on the screen or scroll the browser.
4. Notice a delay or jump in the video window.
   This noticeable lag in the video window indicates that the video is being redirected.

How do I check if Windows Media Redirection is working on my ThinOS device?

Prerequisites

- Ensure that the **Windows Media redirection** policy is set to **Allowed** in Citrix Studio.
- Ensure that you have enabled the **Enable HDX/MMR** check box in the **Global Connection Settings** dialog box on the ThinOS client.

Steps

1. Connect to a Citrix server, and launch an ICA desktop.
2. Play a video or an audio file using Windows Media Player.
3. Drag and move the Windows Media Player.
   Notice that the video graphic and the media player window frame are in different layers.

   You can also determine if Windows Media Redirection is working using the method that is described in the **CTX215173** article at support.citrix.com.

How can I check if Multimedia Redirection is working on my ThinOS device?

When you play a video using Multimedia Redirection, launch the snipping tool, click **New**, and take a screenshot of the screen with the video. If Multimedia Redirection is working, then the image from the video cannot be captured. In the screenshot, a black screen can be seen instead of the video.

Is persistent logging supported in ThinOS 10.x?

Persistent logging is not supported in ThinOS ThinOS 10.x.

Is the tls.txt file included in network traces on ThinOS 10.x?

The tls.txt file is not included in network traces for ThinOS.

Will the ThinOS device automatically reboot if the system crashes?

ThinOS 10.x client automatically reboots when the system crashes. The system backs up the data every one hour. If any key applications, such as ThinOS window crashes, the system still runs and is recovered without a reboot.

Wyse Management Suite FAQs

This section contains frequently asked questions that are related to Wyse Management Suite.

What takes precedence between Wyse Management Suite and ThinOS UI when conflicting settings are enforced?

Any settings that are configured using Wyse Management Suite take precedence over the settings that were configured locally on the ThinOS client or published using the Admin Policy Tool. The settings that are configured locally in the ThinOS are synced to Admin Policy Tool but not to Wyse Management Suite.

The priority order for ThinOS configurations is as follows:

1. Wyse Management Suite Policies
2. Admin Policy Tool
3. Local ThinOS UI

How do I import users from a .csv file?

Steps

1. Click **Users**.
   The **Users** page is displayed.
2. Select the **Unassigned Admins** option.
3. Click **Bulk Import**.
   The **Bulk Import** window is displayed.
4. Click **Browse** and select the .csv file.
5. Click **Import**.

How do I use Wyse Management Suite file repository?

Steps

1. Download the Wyse Management Suite repository from the public cloud console.
2. After the installation process, start the application.
3. On the Wyse Management Suite Repository page, enter the credentials to register the Wyse Management Suite repository to the Wyse Management Suite server.
4. To register the repository to the Wyse Management Suite public cloud, enable the **Register to Public WMS Management Portal** option.
5. Click the **Sync Files** option to send the sync file command.
6. Click **Check In** and then click **Send Command** to send the device information command to the device.
7. Click the **Unregister** option to unregister the on-premises service.
8. Click **Edit** to edit the files.
   a. From the drop-down list of **Concurrent File Downloads** option, select the number of files.
   b. Enable or disable **Wake on LAN** option.
   c. Enable or disable **Fast File Upload and Download (HTTP)** option.
      - When HTTP is enabled, the file upload and download occurs over HTTP.
      - When HTTP is not enabled, the file upload and download occurs over HTTPS.
   d. Select the **Certificate Validation** check box to enable the CA validation for a public cloud.

NOTE:

- When CA Validation from the Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations, such as, Apps and Data, Image Pull/Push is successful. If the certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate Certificate Authority** under **Events** page. All the operations, such as, Apps and Data, Image Pull/Push is not successful.
- When CA Validation from Wyse Management Suite server is disabled, then the communication from server and client happens in a secure channel without Certificate Signature validation.

e. Add a note in the provided box.
f. Click **Save Settings** .

How do I check the version of Wyse Management Suite

Steps

1. Log in to Wyse Management Suite.
2. Go to **Portal Administration** > **Subscription**.
   The Wyse Management Suite version is displayed in the **Server Information** field.

16

Support Resources

This chapter provides FAQs, and support resources for resolving ThinOS 10.x migration issues, including DHCP/DNS setup and log collection.

Resources and support

Accessing documents using product selector

1. Go to Support | Dell.
2. Click **Browse All Products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **Wyse Software**.
6. Click **Dell ThinOS** .
7. Click **Select This Product**.
8. Click **Support Resources** > **Manuals & Documents**.

Reference materials and supporting documentation

This chapter serves as a centralized repository of official Dell ThinOS 10.x documentation. It enables administrators to quickly access key resources for deployment, configuration, compatibility validation, and customization. It provides direct access to key Dell ThinOS 10.x documents that assist IT administrators in various aspects of endpoint management.

Table 69. Document index

Document title	Description	Go to
Dell ThinOS 10.x Administrator Guide	Provides IT administrators with instructions for configuring, managing, and troubleshooting the system.	Dell ThinOS documentation page
Dell ThinOS 10.x Migration Guide	Provides IT administrators with procedures for migrating data, applications, or systems from one environment to another.	
Dell ThinOS 10.x 2602 Release Notes	Provides users with a summary of new features, bug fixes, and known issues for a software release.	
Dell ThinOS 10.x Hardware Compatibility List	Provides IT administrators with details on compatible hardware, software, and supported configurations for the software.	
Dell ThinOS 10.x Compatibility Checker User Guide	Provides IT administrators with the details to repurpose any Dell or non-Dell hardware for ThinOS 10.x using a USB imaging method.	
Dell ThinOS 10.x App Builder User's Guide	Provides users with instructions for using the software, including setup and features.	

Contacting Dell

If you do not have an active Internet connection, you can find contact information about your purchase invoice, packing slip, bill, or Dell product catalog.

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

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