Dell Wyse ThinOS 9.1.4234

Administrator's Guide

October 2021
Rev. A01

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

Chapter 1: Introduction **11**
Supported platforms 11

Chapter 2: Upgrading the ThinOS firmware **12**
Before you upgrade 14
Important notes 14
Register ThinOS devices to Wyse Management Suite 14
Register ThinOS devices using Wyse Device Agent 14
Register ThinOS devices by using DHCP option tags 15
Enable Live Update 15
Download the ThinOS firmware, BIOS, and application packages 16
File naming convention 17
Add ThinOS 8.6 to ThinOS 9.x firmware to the repository 18
Upgrade ThinOS 8.6 to ThinOS 9.x 18
Upgrade ThinOS 9.x to later versions using Wyse Management Suite 18
Upgrade ThinOS 9.x to later versions using Admin Policy Tool 19
Add ThinOS application packages to the repository 19
Upload and push ThinOS 9.x application packages using Groups and Configs on Wyse Management Suite 20
Upload and install ThinOS 9.x application packages using Admin Policy Tool 20
Firmware installation using Dell Wyse USB Imaging Tool 21
Upgrade BIOS 21
Edit BIOS settings 21
Delete ThinOS application packages 22
Downgrading the ThinOS firmware 22

Chapter 3: Getting started with ThinOS **23**
End User License Agreement 23
Configure ThinOS using First Boot Wizard 23
Configure account privileges for ThinOS 28
Configure account privileges using Admin Policy Tool 29
Configure account privileges using Wyse Management Suite 29
Connect to a remote server 29
Connecting a display 30
Connecting a printer 30
Configure WMS settings on the client GUI 30
Desktop overview 30
Modern interactive desktop features 31
Enable modern desktop mode 31
Modern toolbar or float bar 32
List of connections 33
Classic desktop features 33
Desktop guidelines 33
Enable classic desktop mode 34

Using the taskbar ... 34
Using the shortcut menu ... 36
Using the desktop menu ... 36
Configure the Connection Manager ... 37
Configuring thin client settings and connection broker settings ... 37
Configure ThinOS using Admin Policy Tool ... 37
Configure the Admin Policy Tool ... 38
Admin Policy Tool feature list ... 38
Locking the thin client ... 40
Shut down and restart ... 40
Scheduled Shutdown ... 41
Scheduled Reboot ... 41
Enable or disable shutdown ... 41
Battery information ... 42
Login dialog box features ... 42
View the system information ... 42
Sleep mode ... 43
Enable sleep manually ... 43
Import certificates to ThinOS from Admin Policy Tool or Wyse Management Suite ... 44
ThinOS system variables ... 44

Chapter 4: Configuring the global connection settings ... 46

Chapter 5: Configuring connectivity ... 48
Configuring the network settings ... 48
Configure the general settings ... 48
Configure the DHCP options settings ... 49
Configure the ENET settings ... 51
Configure the WLAN settings ... 53
Configure the proxy settings ... 55
Configuring the remote connections ... 57
Configure the broker setup ... 57
Configure the General Options ... 58
Configuring the central configurations ... 59
Configure the Wyse Management Suite settings ... 59
Configure the VPN Manager ... 60
Configure VNC services ... 61

Chapter 6: Configuring connection brokers ... 63
Configuring Citrix ... 63
Configure the Citrix broker setup ... 63
Citrix ADC ... 67
Citrix Cloud services ... 72
Automatically configure using DNS for email discovery ... 72
Citrix HDX Adaptive transport (EDT) ... 73
HDX Adaptive Display V2 ... 73
Browser content redirection ... 74
HTML5 Video Redirection ... 75
Windows Media Redirection ... 75

QUMU Video Optimization Pack for Citrix....76
Citrix Self-Service Password Reset....76
Citrix SuperCodec....77
Anonymous logon....78
Enable UDP audio in a Citrix session....78
Keyboard layout synchronization in VDA....78
Cursor pattern in ICA session....84
Citrix multiple virtual channels....84
Configure the Citrix session properties....86
Using multiple displays in a Citrix session....86
USB Printer Redirection....87
Configure the Citrix UPD printer....88
Configure the device-specific printer driver....88
Export Citrix Workspace App logs....89
Configure multifarm....94
Configure multilogon....94
Configuring VMware....95
Configure the VMware broker connection....95
VMware Real Time Audio-Video....96
High Efficiency Video Coding....96
Enable Scanner Redirection....97
Enable Serial Port Redirection....97
Enable Session Collaboration....98
Enable Battery State Redirection....98
Relative mouse....98
Configure Workspace ONE Mode....99
Unified Access Gateway....99
Configure the VMware integrated printing settings....100
Wacom tablet support on ThinOS....101
USB Redirection in a VDI session....102
Enable Multimedia Redirection in Blast session....103
Smartphone sync....103
Configuring Windows Virtual Desktop....104
Enable printer in Windows Virtual Desktop....104
Log in to Windows Virtual Desktop using Active Directory Federation Services....105
Configuring Microsoft Remote Desktop Services....107
Enable Terminal Services Gateway....107
Configure the Remote Desktop Services collection....107
Add a Remote Desktop Protocol connection....108
Log in to RDP session using Remote Desktop Gateway....110
Log in to RDP session using Remote Desktop Gateway from Wyse Management Suite or Admin Policy Tool....112
Change the display mode for RDP connection using shortcut keys....112
Configuring the Amazon WorkSpaces broker connection....112
Teradici PCoIP licensing....113
Configure the Teradici Cloud Access broker connection....113
Configuring PCoIP connections using Teradici Remote Workstation card....115
Enable ThinOS to check the server certificate common name....115
Bloomberg keyboard support....116
Configure Bloomberg keyboard in Citrix sessions....116

Configure Bloomberg keyboard in PCoIP sessions....116
Redirect Bloomberg keyboard in VMware Horizon Blast sessions....117
Mapping Bloomberg keyboard in VMware Blast sessions....117
Bloomberg keyboard limitations....117
Configure the Select Group feature to log in to different brokers....118

Chapter 7: Unified Communications optimization with ThinOS....119
Citrix Unified Communications support on Wyse 3040 Thin Clients....119
Citrix HDX RealTime Optimization Pack for Skype for Business....119
Install the Citrix Workspace app package on ThinOS....120
Set up the Skype for Business application....120
Using the Skype for Business application....120
Verify the Skype for Business connection status....121
Citrix RTME call statistics....122
VMware Horizon Virtualization Pack for Skype for Business....122
Install the Horizon package on ThinOS....122
Setting up the Skype for Business in VMware Blast session....122
Optimized mode and Fallback mode....123
Change Optimized mode to Fallback mode....123
Cisco Jabber Softphone for VDI....124
Install the JVDI package on ThinOS....124
Setting up the Cisco Jabber Softphone for VDI....125
Using Cisco Jabber....125
Using Device Selector....126
Verify the Cisco Jabber connection status....126
Cisco Webex Teams for VDI....126
Install the Cisco Webex Teams package on ThinOS....127
Setting up the Cisco Webex Teams for VDI....127
Cisco Webex Teams optimization on Citrix Workspace app feature matrix....128
Cisco Webex Teams optimization on VMware feature matrix....129
Verify the Cisco Webex Teams connection status....130
Cisco Webex Meetings for VDI....130
Install the Cisco Webex Meetings package on ThinOS....131
Setting up the Cisco Webex Meetings for VDI....131
Cisco Webex Meetings optimization feature matrix....131
Verify the Cisco Webex Meetings connection status....133
Cisco Webex Meetings optimization known issues....133
Zoom Meetings for VDI....133
Install the Zoom package on ThinOS....134
Setting up the Zoom Meetings for VDI....134
Zoom optimization feature matrix....134
Verify the Zoom connection status....136
Microsoft Teams Optimization from Citrix Workspace app....136
Microsoft Teams Optimization from VMware Horizon....138
Enable the optimization by using a Group Policy Editor....138
Microsoft Teams optimization feature matrix....138
Microsoft Teams optimization limitations and known issues....139

Chapter 8: Configuring third-party authentication settings....140

Configure the Imprivata OneSign server ... 140
VDI selection on ThinOS ... 141
OMNIKEY readers ... 141
Configure the VDI settings on OneSign server ... 141
Configure objects on Imprivata Server ... 141
Use smart card as proximity card ... 143
Enroll a proximity card with Imprivata OneSign ... 143
Imprivata Bio-metric Single Sign-On ... 143
Grace period to skip second authentication factor ... 144
Imprivata OneSign ProveID Embedded ... 144
Configure the OneSign Admin Console ... 146
Install the Imprivata PIE package on ThinOS ... 146
Enable PIE mode on ThinOS ... 146
Uploading OneSign appliance SSL certificate ... 147
Import the OneSign appliance SSL certificate automatically ... 147
Import OneSign appliance SSL certificate manually ... 147
Configure Fast User Switching on ThinOS ... 148
Configure Imprivata fingerprint reader for Citrix ICA and PCoIP sessions ... 148
Configure Imprivata fingerprint reader for VMware Horizon Blast session ... 148
Identity Automation ... 149
Configure the Identity Automation ... 149
Install the Identity Automation QwickAccess app package on ThinOS ... 149
Identity Automation support matrix ... 149
Enroll a proximity card with Identity Automation on ThinOS ... 150
Use a proximity card for sign-on with Identity Automation on ThinOS ... 150
Use a proximity card to secure the remote session with Identity Automation on ThinOS ... 151
Use a proximity card to tap-over another user session with Identity Automation on ThinOS ... 151
Identity Automation feature matrix ... 151

Chapter 9: Configuring the thin client local settings ... 153
Configuring the system preferences ... 153
Configure the general system preferences ... 153
Set the time and date ... 154
Set the custom information ... 155
Configuring power and sleep mode ... 155
Configure the display settings ... 157
Using the On-Screen Display (OSD) ... 159
Port preferences on the Wyse 5470 Thin Client ... 159
Display limitation on Dell WD19 docking station ... 159
Vertical Synchronization ... 159
Configure the external touch screen settings ... 159
Configuring the peripherals settings ... 160
Configure the keyboard settings ... 160
Configure the mouse settings ... 162
Configure the touchpad settings ... 162
Configure the audio settings ... 163
Configure the serial settings ... 164
Configure the camera device ... 165
Configure the Bluetooth settings ... 166
Secure Digital cards ... 167

Configure the Jabra Xpress headset settings....167
Configure the EPOS headset settings....168
Configure the HID Fingerprint reader settings....169
Configuring the printer settings....169
Configure the ports settings....170
Configure the LPDs settings....171
Configure the SMBs settings....172
Using the printer setup options....173
Using the Help....173
Reset to factory defaults....173
Resetting to factory defaults using G-Key reset....174
Recovery mode using R-Key....174

Chapter 10: Using the system tools....175
Simplified Certificate Enrollment Protocol....177
Request the certificate manually....177
Request the certificate automatically using Wyse Management Suite....179
About Default Certificates....179
Trusted Platform Module version 2.0....181

Chapter 11: Using Wyse Management Suite....183
Functional areas of Wyse Management Suite console....183
Managing groups and configurations....183
Create a default device policy group....183
Create a user policy group....185
Edit an unmanaged group....187
Remove a group....187
Create and import bulk device exception file....188
Edit the ThinOS 9.x policy settings....190
Managing devices....191
Search a device using filters on the Devices page....192
View the display parameters....192
View the BIOS details....193
Managing Jobs....193
Schedule a device command job....194
Managing rules....194
Editing a registration rule....195
Create unmanaged device auto assignment rules....195
Edit an unmanaged device auto assignment rule....195
Disable or delete a rule....196
Save the rule order....196
Create a rule for alert notification....196
Edit an alert notification rule....196
Managing Events....197
Search an event or alert using filters....197
Managing users....197
Add a new admin profile....198
Create a WMS custom role in Wyse Management Suite....199
Create auto assignment rules for unmanaged devices....199

Add a user....200
Bulk import end users....200
Configure end user policy....200
Portal administration....200
Adding the Active Directory server information....200
Wyse Management suite Active Directory group feature matrix....202
Import unassigned users or user groups to public cloud through active directory....205
Access Wyse Management Suite file repository....205

Chapter 12: Troubleshooting your thin client....208
Capture an HTTP log using ThinOS....210
System crashes, freezes or restarts abruptly....210
Broker agent login failure....210
Citrix desktop and application crashes abruptly....210
Unified Communications software call failure....211
Request a log file using Wyse Management Suite....211
View audit logs using Wyse Management Suite....211
System log and trace information....212
Upgrade or conversion troubleshooting and logs....212
How to debug with new support beyond ThinOS 8?....214
How to debug with same support in ThinOS 8?....214

Chapter 13: Frequently Asked Questions....215
ThinOS-related questions....215
How do I upgrade from ThinOS 8.6 to 9.1.4234?....215
What should I do if the package installation fails?....215
Is Wyse Management Suite 3.3.1 the only way to manage ThinOS 9.1.4234?....215
How to verify third-party binary versions on your ThinOS client?....215
Is USB Imaging Tool method a possible option for upgrading to ThinOS 9.1.4234?....215
Can ThinOS be installed on a PCoIP device?....215
Does ThinOS support zero desktop?....215
Does ThinOS support ThinOS configurations using INI files?....216
iPhone cannot be redirected to the Citrix Desktop session....216
Android smartphone is not displayed in the session when redirected or mapped....216
Does Citrix Workspace app replace Citrix Receiver on ThinOS?....216
What is Workspace mode on ThinOS?....216
Can I enable Flash content to be rendered using a local Flash Player on ThinOS?....216
How do I verify if HDX Enlightened Data Transport Protocol is active?....216
How do I check if HTML5 Video Redirection is working?....217
How do I check if QUMU Multimedia URL Redirection is working?....217
How do I check if Windows Media Redirection is working?....217
How to check if Multimedia Redirection is working?....217
Is persistent logging supported in ThinOS?....217
Is tls.txt file included in network traces on ThinOS?....218
Will ThinOS device reboot automatically when the system crashes?....218
Wyse Management Suite-related questions....218
What takes precedence between Wyse Management Suite and ThinOS UI when conflicting settings are enforced?....218
How do I import users from a .csv file?....218
How do I use Wyse Management Suite file repository?....218

How do I check the version of Wyse Management Suite.....219

1

Introduction

Thin clients running Dell Wyse 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 Wyse ThinOS is virus and malware resistant.

Wyse ThinOS requires a management software to configure, operate, and update thereby eliminating the need for IT support to visit 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.

This guide is intended for administrators of thin clients running Wyse 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.

Supported platforms

The Dell Wyse ThinOS firmware is supported on the following Dell Wyse thin clients:

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

NOTE: Wyse 3040 Thin Client is for users who work mostly on tasks with limited multimedia requirements. It is not applicable for using multimedia such as BCR, HTML 5 video redirection, Window multimedia redirection, RTOP video call, JVDI video call, enable video or share screen with Microsoft Teams, Webex Meetings, Webex Teams or Zoom. It is recommended to use Wyse 5070, 5470 AIO, or 5470 thin clients for high multimedia requirements.

2

Upgrading the ThinOS firmware

It is recommended to use the Wyse Management Suite version 3.3.1 or later to upgrade your ThinOS firmware to 9.1.4234. You can also use the USB Imaging Tool version 3.4.0 or later to install the ThinOS 9.1.4234 Merlin image on your thin client. ThinOS 9.1.4234 displays a change group notification message on the device after you change the group in Wyse Management Suite. The client reboots automatically if you do not click **Cancel** before the timer in the message reaches 0. A similar message is displayed when you deploy a new firmware or package using Wyse Management Suite.

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

1. Register your thin client to Wyse Management Suite.
   - Register ThinOS devices using Central Configuration. See Register ThinOS devices using Wyse Device Agent.
   - Register ThinOS devices using DHCP option tags. See Register devices by using DHCP option tags.
2. Download the ThinOS 9.1.4234 operating system image. See Download the ThinOS firmware.
3. Upload the ThinOS 9.1.4234 firmware to the Wyse Management Suite repository. See Add ThinOS firmware to repository.
4. Upgrade BIOS on your device to the current version mentioned in the BIOS details table in this section.
5. Upgrade the ThinOS firmware from 8.6 to 9.x. See Upgrade ThinOS 8.6 to ThinOS 9.x.
6. Upgrade the ThinOS firmware from 9.x to later versions. See Upgrade ThinOS 9.x to later versions.
7. Deploy the application packages. See Upload and push ThinOS 9.x application packages.

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

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

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

For detailed information about the upgrade process, see the *Dell Wyse ThinOS 9.1.4234 Migration Guide* at www.dell.com/support.

Table 1. Firmware images

Platform	ThinOS firmware image for upgrading from 8.6 to 9.1.4234	ThinOS PCoIP image for upgrading from 8.6 to 9.1.4234	ThinOS firmware image for upgrading from 9.x to later versions
Wyse 3040 Thin Client	A10Q_wnos	PA10Q_wnos	DTOS_version.pkg
Wyse 5070 Thin Client —Celeron processor	X10_wnos	PX10_wnos	DTOS_version.pkg
Wyse 5070 Thin Client —Pentium processor	X10_wnos	PX10_wnos	DTOS_version.pkg
Wyse 5070 Extended Thin Client—Pentium processor	X10_wnos	PX10_wnos	DTOS_version.pkg
Wyse 5470 Thin Client	X10_wnos	PX10_wnos	DTOS_version.pkg
Wyse 5470 All-in-One Thin Client	X10_wnos	PX10_wnos	DTOS_version.pkg

Table 2. Package information

Name	Description	Package installation
Citrix_Workspace_App	The package supports Citrix Workspace app with RTME client integrated.	Upload the new package using Wyse Management Suite or Admin Policy Tool.

Table 2. Package information (continued)

Name	Description	Package installation
Teradici_PCoIP	The package supports the Teradici PCoIP connection.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
VMware_Horizon	The package supports VMware Blast.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Imprivata_PIE	The package supports Imprivata with ProveID Embedded feature.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Cisco_Jabber	The package supports Cisco Jabber.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Zoom_Horizon	The package supports Zoom Meetings for VMware Horizon.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Zoom_Citrix	The package supports Zoom Meetings for Citrix.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Cisco_WebEx_Meetings	The package supports Cisco Webex Meetings.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Cisco_WebEx_VDI	The package supports Cisco Webex VDI.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Microsoft_WVD	The package supports Windows Virtual Desktop.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Jabra	The package supports Jabra headsets.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
EPOS_Connect	The package supports EPOS Connect.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
HID_Fingerprint_Reader	The package supports HID Fingerprint Reader.	Upload the new package using Wyse Management Suite or Admin Policy Tool.
Identity_Automation_QwickAccess	The package supports Identity Automation	Upload the new package using Wyse Management Suite or Admin Policy Tool.

NOTE: If the package fails to update, or if the thin client does not work after upgrading to the new firmware, remove all packages and reboot the thin client. Reinstall the package after the reboot.

Table 3. BIOS details

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

If Secure Boot is disabled, and the BIOS password is set as the default value or if there is no BIOS password, the Secure Boot option is automatically enabled after the next reboot. If you want to downgrade to ThinOS 8.6 or ThinOS 9.0 Merlin image, do the following:

1. Reboot the device and press the F2 key to enter the Dell BIOS setup.
2. Go to **Secure Boot** > **Secure Boot Enable** and clear the **Secure Boot Enable** check box.
3. For ThinOS 9.0—Go to **Security** > **TPM 2.0/PTT Security** and select the **clear** check box. If this option is not available in BIOS, you can ignore this step.

Before you upgrade

- If you are using earlier versions of ThinOS 9.x, you must upgrade to ThinOS 9.1.3129 before upgrading to ThinOS 9.1.4234.
- If you are using ThinOS 8.6, you must upgrade to ThinOS 8.6_807 and apply the latest BIOS updates before upgrading to ThinOS 9.1.4234.
- If you are using ThinOS v8.5 or earlier versions, you must first upgrade your device to ThinOS 8.6_807 and apply latest BIOS updates before installing ThinOS 9.1.4234.
- Your system must be powered on and the sleep mode must be disabled on the system. If the system has entered the sleep mode, you must send the WOL command using Wyse Management Suite before using any real-time commands. To use the WOL command, ensure that the Wake-On-LAN (WOL) option is enabled in BIOS.
- The BIOS version on Wyse 5070 Thin Client must be 1.3.1 or later before you upgrade to ThinOS 9.1.4234. If you upgrade to ThinOS 9.1.4234 with older BIOS version first and then upgrade to BIOS 1.3.1 or later, the device fails to boot the ThinOS operating system.

Important notes

- All device settings are erased after you upgrade from ThinOS 8.6 to 9.1.4234 except the following settings:
  - Wyse Management Suite group token and server settings
  - Static DNS
  - Certificates
  - IEEE802.1x wired authentication settings
  - Wireless connections—The WEP/Sharekey security type is changed to Open as they are not supported in ThinOS 9.1.4234.
  - Proxy settings
- You cannot boot into ThinOS 9.1.4234 when you perform any of the following operations in BIOS setup:
  - Disable the on-board Network Interface Card (NIC), Trusted Platform Module (TPM), or Platform Trust Technology (PTT).
  - Clear TPM or PTT.
  - Reset BIOS to factory default settings

Register ThinOS devices to Wyse Management Suite

NOTE: DHCP and DNS configurations for Wyse Management Suite work only after you reset the device to factory default settings.

Register ThinOS devices using Wyse Device Agent

Steps

1. From the desktop menu of the thin client, go to **System Setup** > **Central Configuration**.
   The **Central Configuration** window is displayed.
2. Enter the **Group Registration Key** as configured by your administrator for the wanted group.
3. Select the **Enable WMS Advanced Settings** check box.
4. In the **WMS server** field, enter the Wyse Management Server URL.
5. 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 setup, click **Validate Key**. If the key is not validated, verify the group key and Wyse Management Suite server URL which you have provided. Ensure that 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.

6. 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.

7. Click **OK**.
   The device is registered to Wyse Management Suite.

Register ThinOS devices by using DHCP option tags

About this task

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

Table 4. Registering device by using 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 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. **NOTE:** MQTT is optional for Wyse Management Suite 2.0 and later versions.
Name—CA Validation Data Type—String Code—167 Description—Certificate Authority Validation	You can enable or disable 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 com@Wedding2020munication between the client and the Wyse Management Suite server. **NOTE:** CA Validation is optional for the latest version of Wyse Management Suite 2.0 and later versions. However, it is recommended to configure this option tag.
Name—Group Registration Key Data Type—String Code—199 Description—Group Registration Key	This tag directs to the Group Registration Key for the Wyse Management Suite agent. For example, in SCDA-DTos91SalesGroup, 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 2.0 and later versions on private cloud. However, there is a known issue that if you do not provide the group token, the device is not moved to unmanaged group. Therefore, It is recommended to configure the Group Token key.

Enable Live Update

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 9.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**.

Download the ThinOS firmware, BIOS, and application packages

About this task

This section describes the steps to download the ThinOS firmware, BIOS, and application packages from Dell support site.

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device.
3. Select the product from the searched results to load the product page.
4. On the product support page, click **Drivers & downloads**.
5. Select the operating system as **ThinOS 9.1.4234**.
6. Locate the ThinOS image entry and download the image.

Table 5. ThinOS 9.1.4234 image

Scenario	ThinOS image title
Upgrade your ThinOS 8.6_807 to 9.1.4234	**ThinOS 8.6 to ThinOS 9.1.4234 Image file for Dell Wyse 5070, 5470 and 5470 All-in-One Thin Clients**.
	ThinOS 8.6 to ThinOS 9.1.4234 Image file for Dell Wyse 5070, 5470 and 5470 All-in-One Thin Clients with PCoIP.
	ThinOS 8.6 to ThinOS 9.1.4234 Base Image file for Dell Wyse 3040 Thin Clients.
	ThinOS 8.6 to ThinOS 9.1.4234 Base Image file for Dell Wyse 3040 Thin Clients with PCoIP.
Upgrade your ThinOS 9.1.3129 to 9.1.4234	**ThinOS 9.1.3129 to ThinOS 9.1.4234 Image file for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients (DTOS_9.1.4234 pkg)**.

NOTE: If you are using the Dell Wyse USB Imaging Tool to install the ThinOS image on a single client, you must download the ThinOS 9.1.4234 Merlin image

7. If you want to use ThinOS packages, locate a package and download the package to your device.

Table 6. ThinOS packages

ThinOS packages	ThinOS image title
Citrix_Workspace_App	**ThinOS 9.1 <version> Citrix package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
VMware_Horizon	**ThinOS 9.1 <version> VMware Horizon package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.

Table 6. ThinOS packages (continued)

ThinOS packages	ThinOS image title
Teradici_PCoIP	**ThinOS 9.1 <version> Teradici PCoIP package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Microsoft_WVD	**ThinOS 9.1 <version> Microsoft WVD package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Imprivata_PIE	**ThinOS 9.1 <version> Imprivata package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Zoom_Horizon	**ThinOS 9.1 <version> Zoom Horizon package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Zoom_Citrix	**ThinOS 9.1 <version> Zoom Citrix package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Jabra	**ThinOS 9.1 <version> Jabra headsets package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
EPOS_Connect	**ThinOS 9.1 <version> EPOS Connect package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Cisco_WebEx_VDI	**ThinOS 9.1 <version> Cisco Webex VDI package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Cisco_WebEx_Meetings	**ThinOS 9.1 <version> Cisco Webex Meetings package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Cisco_Jabber	**ThinOS 9.1 <version> Cisco Jabber package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
HID_Fingerprint_Reader	**ThinOS 9.1 <version> HID Fingerprint Reader package <version> for Dell Wyse 3040, 5070, 5470 and 5470 All-in-One Thin Clients**.
Identity_Automation_QwickAccess	**ThinOS 9.1 <version> Identity Automation QwickAccess package <version> for Dell Wyse 3040,5070, 5470 and 5470 All-in-One Thin Clients**.

8. If you want to install the latest BIOS package, locate the package entry—**ThinOS 9.1 <version> BIOS package <version>**—for your thin client model and click the download icon.

   NOTE: After you upgrade the client, install the Citrix Workspace app package first, and then reinstall the Citrix-related application packages such as Cisco WebEx Meeting or HID.

   NOTE: For more information about BIOS installation, see BIOS Installation.

File naming convention

ThinOS application packages, ThinOS firmware, and BIOS packages support the following characters in their file names:

- Uppercase letter
- Lowercase letter
- Numeric character
- Special characters—period (.), hyphen-minus (-), and underscores (_)

If you use other characters in file names, the package installation fails.

Add ThinOS 8.6 to ThinOS 9.x firmware to the repository

Steps

1. Log in to Wyse Management Suite.
2. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS**.
3. Click **Add Firmware file**.
   The **Add File** screen is displayed.
4. To select a file, click **Browse** and go to the location where your file is located.
5. Enter the description for your file.
6. Select the check box if you want to override an existing file.
7. Click **Upload**.

   NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy firmware to a device or a group of devices, go to the respective device or the group configuration page.

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

Upgrade ThinOS 8.6 to ThinOS 9.x

Prerequisites

- Upgrade any earlier versions of ThinOS to 8.6_807.
- Upgrade BIOS on the device to the current version that is mentioned in the ThinOS Release Notes. For more information, see *Dell Wyse ThinOS 8.6 Release Notes* at www.dell.com/support.
- Add the ThinOS conversion image to the ThinOS firmware repository. For more information, see Add ThinOS firmware to repository.
- Create a group in Wyse Management Suite with a group token. Use this group token to register the ThinOS 8.6 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**.
   The **Select ThinOS Configuration Mode** window is displayed.
3. Select **Advanced Configuration Mode**.
4. Go to **Firmware Upgrade**, and click **Configure this item**.
5. Clear **Disable Live Upgrade** if you want to upgrade immediately, and clear the **Verify Signature** check boxes.
6. From the **Platform Type** drop-down list, select the platform.
7. From the **Firmware to auto-deploy** drop-down list, select the firmware added to the repository.
8. Click **Save & Publish**.
   The firmware is deployed to the thin client. The conversion process takes 15 s to 20 s, and the thin client restarts automatically.

Upgrade ThinOS 9.x to later versions using Wyse Management Suite

Prerequisites

- Ensure that you are running 9.1.3129 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.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. Click **Advanced**.
4. In the **Firmware** field, select **OS Firmware Updates**.
5. Click **Browse** to browse and upload the firmware.
   The EULA details of the package and the name of the vendors are displayed.
6. Click the vendor names to read the license agreement of each vendor and then 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.
   NOTE: If you upload multiple packages, the EULA details of each package are displayed. You must accept the license agreement of the packages individually. The firmware is not uploaded if you click **Decline**.
7. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
8. Click **Save & Publish**.
   The thin client downloads the firmware and restarts. The firmware version is upgraded.

Upgrade ThinOS 9.x to later versions using Admin Policy Tool

The firmware upgrade using Admin Policy Tool is supported on ThinOS 9.x.

Prerequisites

Ensure that you are running ThinOS 9.1.3129 or later versions on your thin client.

Steps

1. Go to the Admin Policy Tool on the ThinOS client.
2. In the **Configuration Control | ThinOS** window is displayed. Click **Advanced**.
3. In the **Firmware** field, select **OS Firmware Updates**.
4. Click **Browse** to browse and upload the firmware from USB drive.
5. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
6. Click **Save & Publish**.
   The thin client downloads the firmware and restarts. The firmware version is upgraded.

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 9.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 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. 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 operator account and is visible to all the tenants. Tenants cannot delete or modify these files.

Upload and push ThinOS 9.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 9.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 9.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 is 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. From the **Select the ThinOS Package(s) to deploy** drop-down menu, select the package.
7. Click **Save & Publish**.
   The thin client restarts and the application package is installed.

Upload and install ThinOS 9.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 USB drive.
5. From the **Select the ThinOS Package(s) to deploy** drop-down menu, select the uploaded package.

   NOTE: You can select one or more ThinOS application packages simultaneously.
6. Click **Save & Publish**.
   The thin client restarts and the application packages are installed.

Firmware installation using Dell Wyse USB Imaging Tool

Use the Dell Wyse USB Imaging Tool version 3.4.0 to install the ThinOS 9.1.4234 Merlin image on your thin client. For information about installation instructions, see the *Dell Wyse USB Imaging Tool version 3.4.0 User's Guide*.

If you install the merlin image on the following thin clients, the installation may stop at 100% and does not display the completion status:

- Wye 3040 Thin Client with hard disk size larger than 8 GB
- Wyse 5070 Thin Client with hard disk size larger than 16 GB
- Wyse 5470 Thin Client with hard disk size larger than 16 GB
- Wyse 5470 All-in-One Thin Client with hard disk size larger than 16 GB

However, you can force reboot the thin client as the image is already installed.

Upgrade BIOS

Prerequisites

- Depending on your thin client model, download the relevant BIOS file from Dell.com/support.
- If you are upgrading BIOS using Wyse Management Suite, register your thin client to Wyse Management Suite,

Steps

1. Open the Admin Policy Tool on the thin client or go to the ThinOS 9.x policy settings on Wyse Management Suite.
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** drop-down list, select the BIOS file that you have uploaded.
6. Click **Save & Publish**.

   The thin client restarts. BIOS is upgraded on your device.

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

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

Edit BIOS settings

Prerequisites

- If you are using Wyse Management Suite, ensure that you have registered the thin client and synchronize the BIOS admin password. For more information about using the **Sync BIOS Admin Password** option, see the *Dell Wyse Management Suite v2.1 Administrator's Guide* at www.dell.com/support.
- 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 thin client or go to the ThinOS 9.x policy settings on Wyse Management Suite.
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 **Secure Boot** section, enable the secure boot option. If enabled, you cannot disable it using Admin Policy Tool or Wyse Management Suite. Secure Boot can be disabled only in the BIOS setup window.
7. In the **Power Management** section, modify the power-saving options.
8. In the **POST Behavior** section, enable or disable the MAC Address Pass-Through feature. This option is applicable only to the Wyse 5470 Thin Client.
9. Click **Save & Publish**

   NOTE: If the thin client does not have a BIOS admin password, you can set the password using Admin Policy Tool or Wyse Management Suite. In this scenario, the client reboots first to apply the BIOS admin password and other BIOS settings take effect after the second reboot.

   NOTE: Changing BIOS password using **Select Group** requires a reboot to take effect.

Delete ThinOS application packages

You can use the ThinOS local UI or the Wyse Management Suite to delete one or more ThinOS packages.

About this task

This section describes steps to delete ThinOS packages using the ThinOS local UI.

Steps

1. Log in to the ThinOS client.
2. From the system menu, go to **System Tools** > **Packages**.
   All the installed ThinOS 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.

   For information about how to delete packages using Wyse Management Suite, see the latest *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Downgrading the ThinOS firmware

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

3

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 and HID EULA are 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 9.x to factory settings.

Configure ThinOS using First Boot Wizard

A First Boot Wizard application runs 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. Use this application to perform tasks, such as, configuring system preferences, setting up the Internet connectivity, loading USB configurations, configuring management software, and configuring broker connections.

Prerequisites

If you are an existing thin client user, and you have upgraded to the ThinOS version 9.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.

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 **How do You Connect?** 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 followed by the EULA screen. For more information about the EULA screen, see End User License Agreement.

   NOTE: If there is no network connection, press **Continue** on the welcome screen to go to the EULA screen.

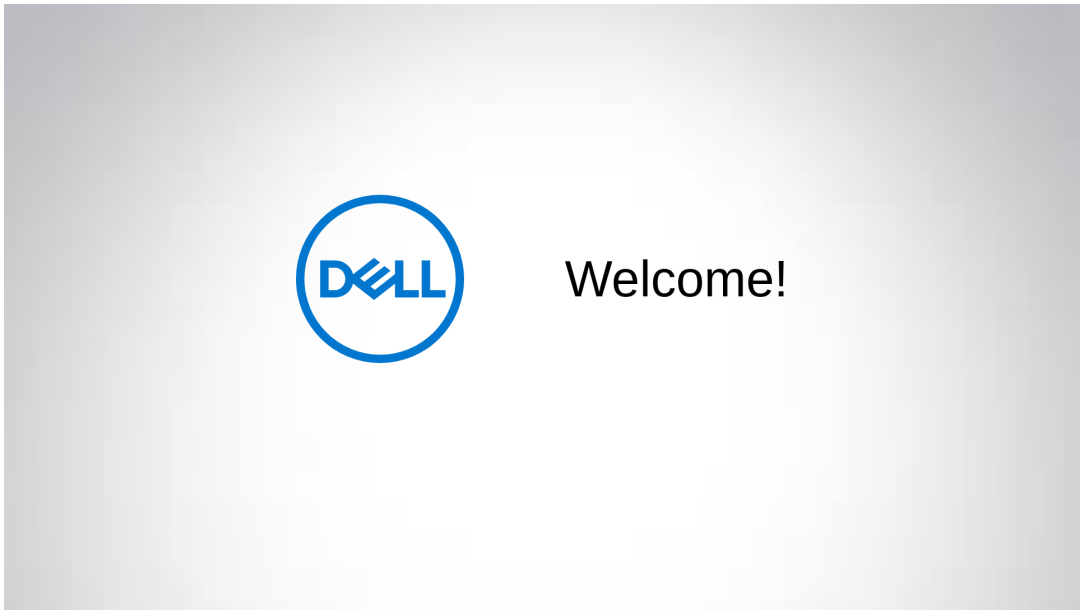


Figure 1. Welcome screen

3. Click **Dell EULA** or **HID 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 different depending on the client installed pkgs.

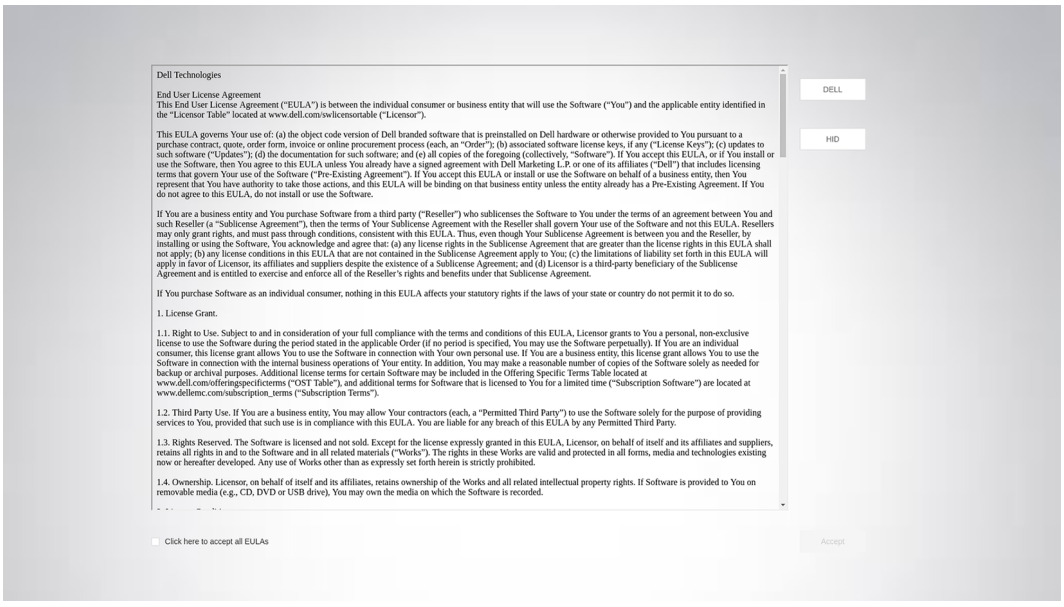


Figure 2. EULA screen

4. Select the **Click here to accept all EULAs** check box and click **Accept**.
5. On the **Select Your Language** screen, select a language from the **Language** drop-down list to start ThinOS in the regional language.

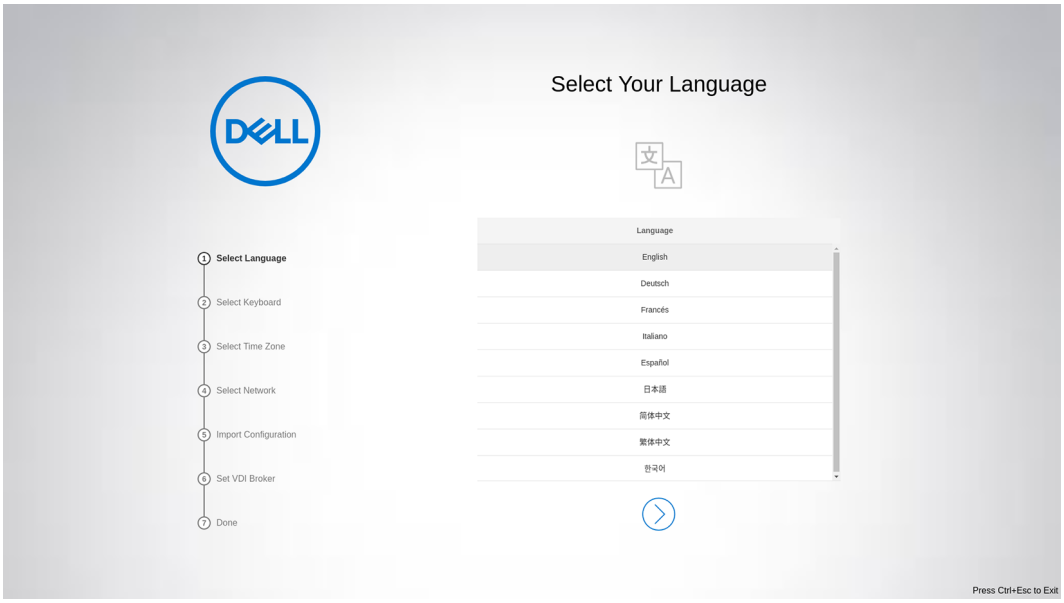


Figure 3. Select Your Language

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

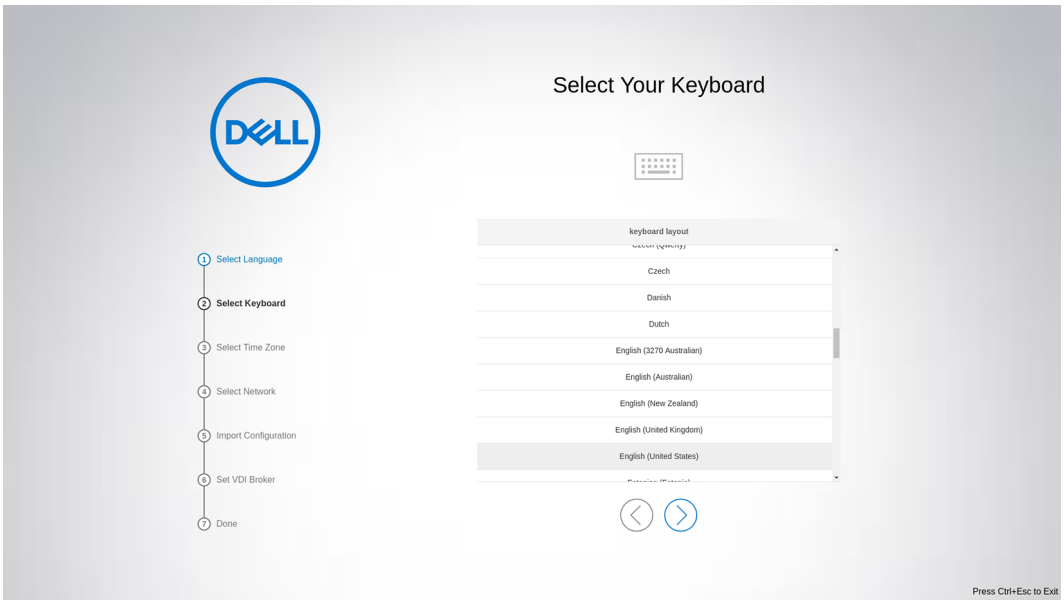


Figure 4. Select Your Keyboard

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

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

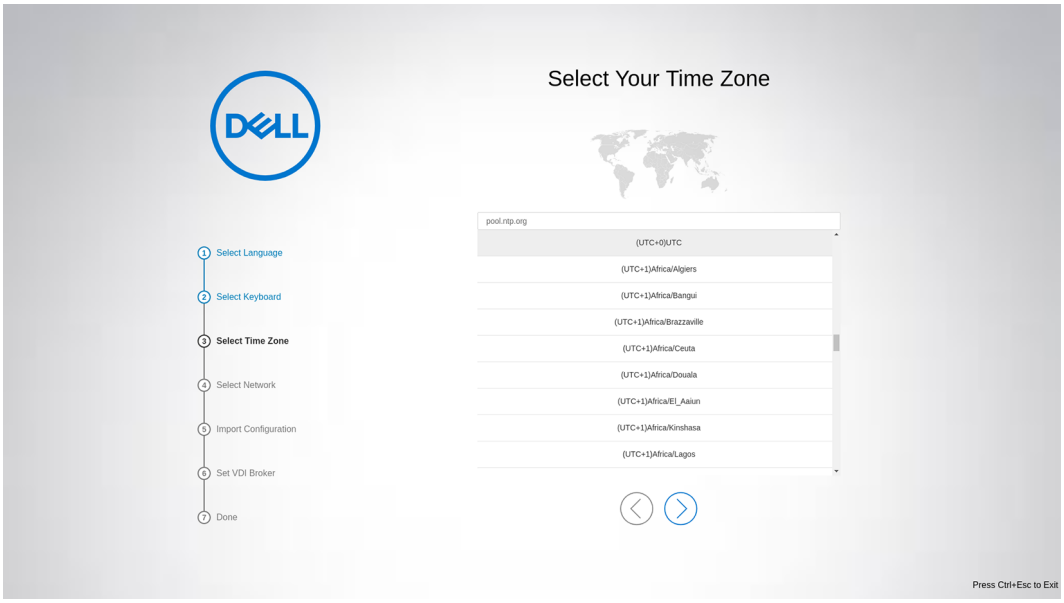


Figure 5. Select Your Time Zone

10. Click  .
11. On the **How do You Connect?** screen, do either of the following:
    - **Local network (Ethernet)**—Click this option if you have connected the thin client to an Ethernet using a wired connection.
    - **Wi-Fi Network**—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.

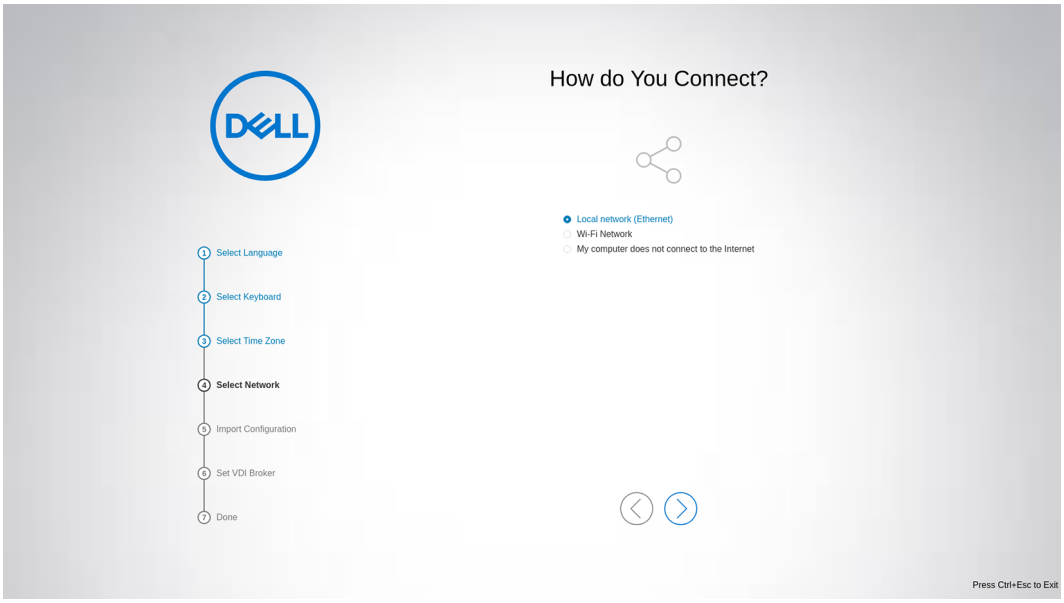


Figure 6. How do You Connect?

12. Click  .
13. On the **How would you like to import your ThinOS configurations?** screen, do either of the following:

- **From Wyse Management Suite**—Click this option 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.

- **From USB**—Click this option if you want to import system settings from the USB drive.
- **Do not import a configuration**—Click this option if you do not want to import any ThinOS configurations using the First Boot Wizard screen.

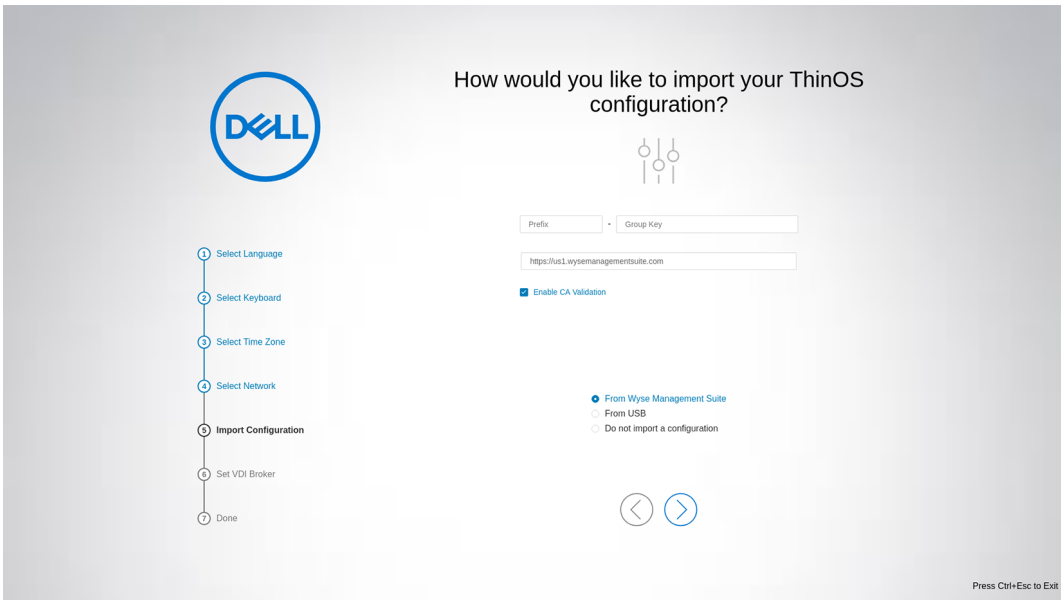


Figure 7. How would you like to import your ThinOS configurations?

14. Click  .
15. On the **Connect to VDI broker** screen, configure your preferred broker type from the following options:
    - Citrix Virtual Apps and Desktops
    - VMware Horizon
    - Windows Virtual Desktop
    - Microsoft Remote Desktop Services
    - Amazon WorkSpaces
    - Teradici Cloud Access

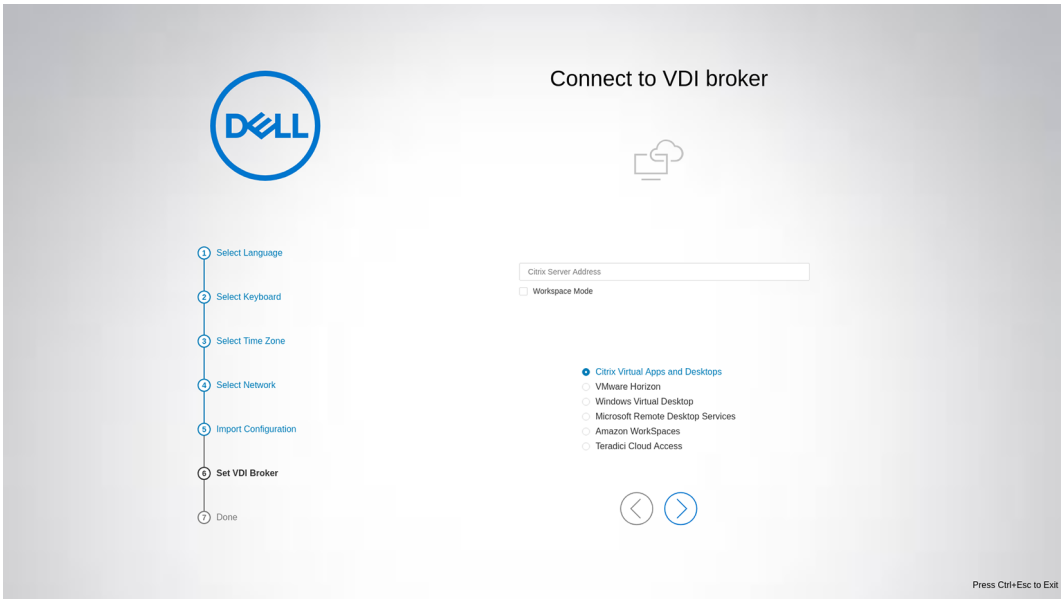


Figure 8. Connect to VDI broker

16. Click  .
The **Done** screen is displayed.

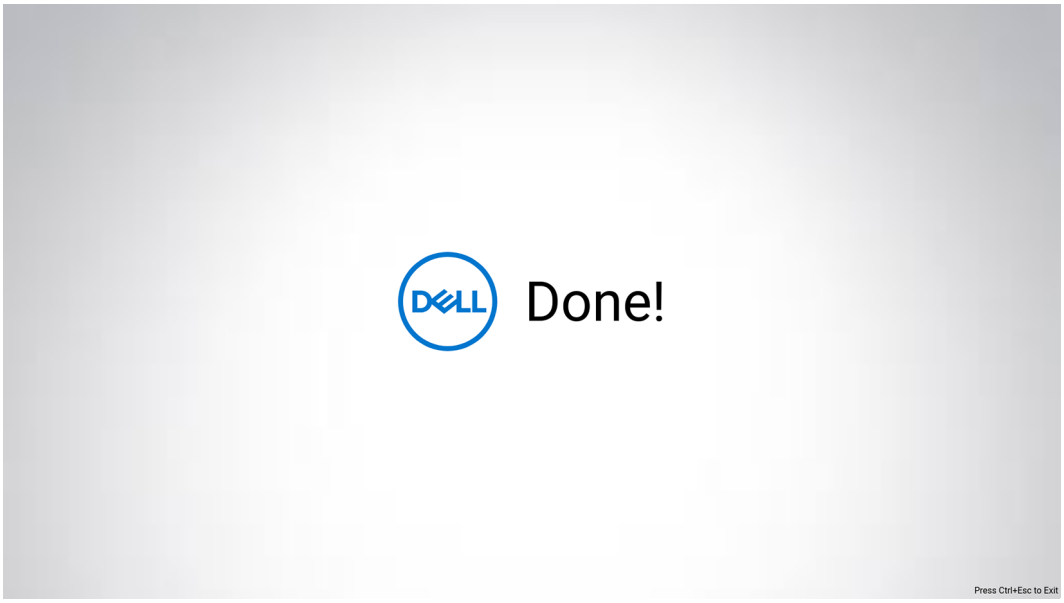


Figure 9. Done

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

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 system menu. In ThinOS 9.1.4234, **DHCP** and **Granular Control of Peripherals** options are added. The **DHCP** option is only available after you enable **Network Setup** and **Granular Control of Peripherals** option is only available after you enable **Peripherals**. From **Granular Control of Peripherals**, you can select the tabs that you want to be displayed in the **Peripherals** window. If no tabs are selected, all tabs will be visible in the **Peripherals** window by default.
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 desired group.
2. Click **Edit Policies**.
3. Select **ThinOS 9.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 system menu. In ThinOS 9.1.4234, **DHCP** and **Granular Control of Peripherals** options are added. The **DHCP** option is only available after you enable **Network Setup** and **Granular Control of Peripherals** option is only available after you enable **Peripherals**.
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 **OK** 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 9.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.

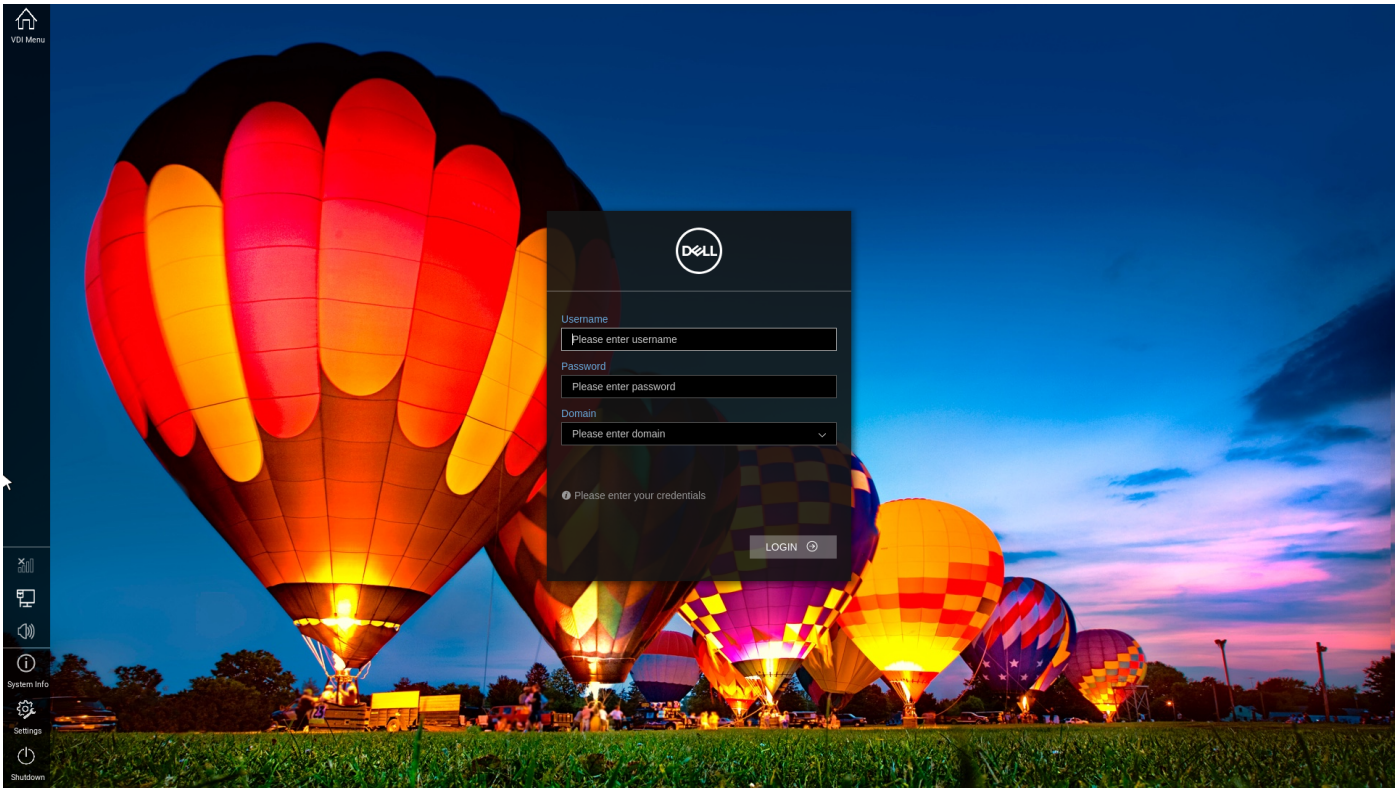


Figure 10. Modern desktop

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.

Modern interactive desktop features

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

NOTE: Citrix Workspace mode is not supported on the modern desktop.

Table 7. Modern desktop shortcuts

Action	Press
Open a selection box for toggling between the desktop and currently-active connections	Ctrl+Alt+DownArrow
Lock the thin client	Ctrl+Alt+LeftArrow or Ctrl+Alt+RightArrow
Capture the full desktop to the clipboard	Print Screen
Capture the active window to the clipboard	Alt+PrintScreen

Enable modern desktop mode

Steps

1. Go to ThinOS 9.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**.
5. From the **Show Floatbar when mouse** drop-down list, select the way that you want to show floatbar when it is hidden.
6. From the **Floatbar Location on Screen** drop-down list, select the location of floatbar on the screen.
7. In the Screen ID field, enter the Screen ID on which floatbar should be shown. You must enter a number 0 to 6. 0 specifies the main screen.
8. 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 Millionseconds** 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 the Windows key using your keyboard to view the float bar. If you change the mouse pointer size to a number greater than 3 in a Blast session, you must use Ctrl+Alt to exit the session and view the floating bar on the ThinOS modern desktop.

Table 8. Toolbar icons

Icon	Description
VDI menu	Opens the list of available connections.
System Info	Displays thin client system information.
Settings	Opens the System Settings menu to configure thin client system 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.
Wired network	Displays the wired connected mode.
Volume or Sound	Click this icon to increase or decrease the speaker volume or mute the speaker.
PNA menu	Displays the Citrix connection options such as Refresh, Disconnect, Reconnect, Logoff, and Manage Security Question. **NOTE:** The PNA menu button is displayed only after you log in to the Citrix Broker agent.
PCoIP	Displays the active PCoIP sessions. This icon is applicable only for PCoIP-enabled clients. You can select a session from the menu, and enable or disable the following PCoIP options in real time: • Relative Mouse • Audio or Video synchronization
Battery indicator	Hover over the battery indicator to view the remaining battery percentage. This option is applicable only to the Wyse 5470 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 PIN, and unlock 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 9. 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.

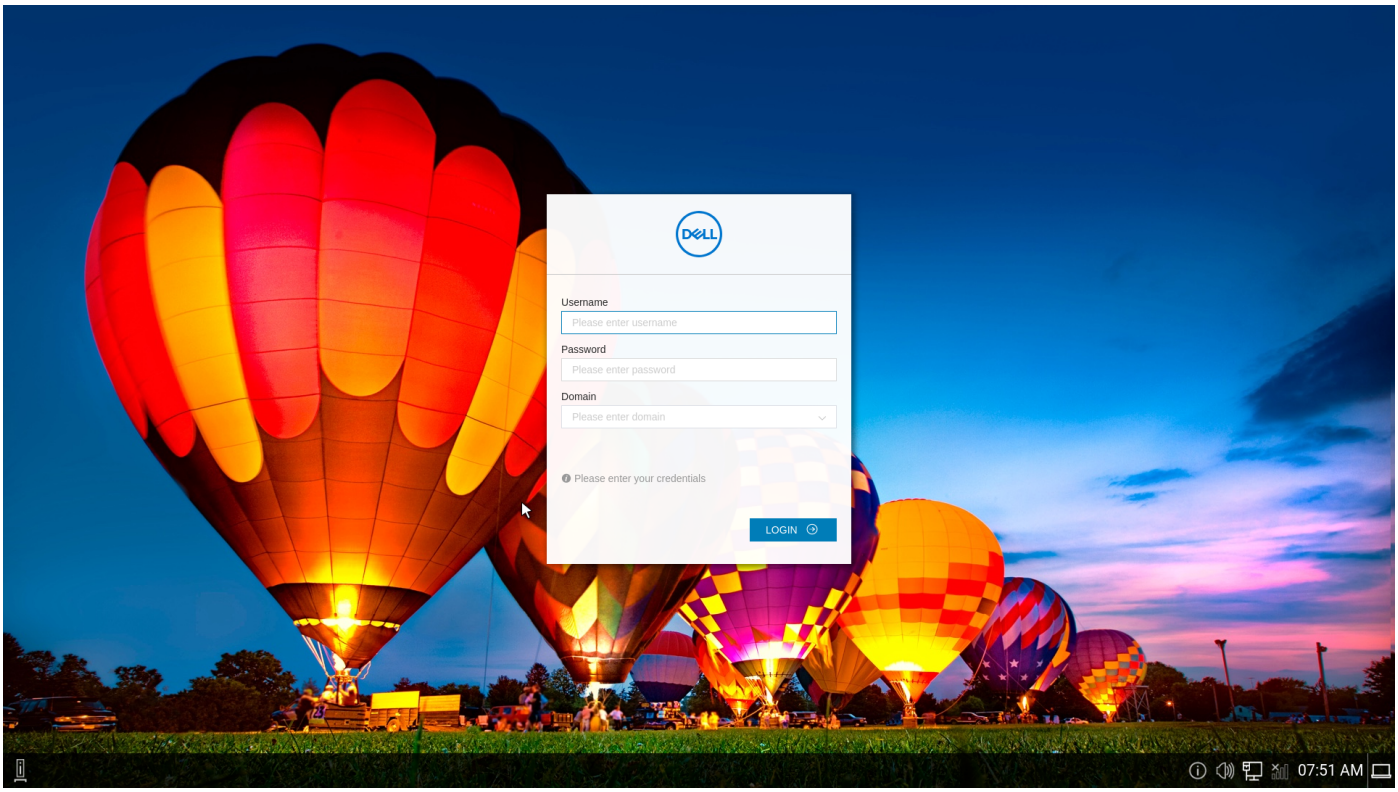


Figure 11. Classic desktop

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 **Connection Settings** 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 on the desktop provides a **shortcut menu**.
- Clicking the desktop menu button, or clicking anywhere on the desktop, opens the desktop menu.

Enable classic desktop mode

Steps

1. Go to ThinOS 9.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 **Classic**.
5. Click **Save & Publish**.

Using the taskbar

Use the taskbar to view the date, time, system information, wireless information, volume icon, PNAmenu button, and switch to the desktop screen.

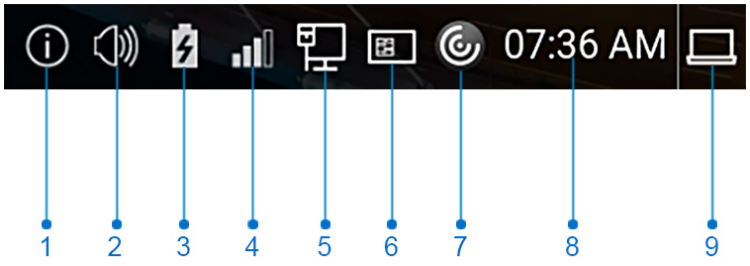


Figure 12. Taskbar

1. **System Information**
2. **Volume or Sound**
3. **Battery**
4. **Wireless network**
5. **Wired network**
6. **Smart card self-service**
7. **Citrix PNA menu**
8. **Date and time**
9. **Show desktop**

The following table lists the taskbar elements:

Table 10. Taskbar - System tray elements

Element	Description
Date and time	Displays the date and time.
Battery	Displays the battery percentage. This option is applicable for Wyse 5470 Thin Client.
Show desktop	Click this icon to hide or restore VDI sessions.
Volume or Sound	Click this icon to increase or decrease the speaker volume or mute the speaker.

Table 10. Taskbar - System tray elements (continued)

Element	Description
System Information	Click this icon to view the system information such as general system details, copyright, event logs, Wyse Management Suite status, network connections, and so on.
Wireless icon	Displays the wireless connection mode. Clicking the wireless icon displays the SSID scan list. You can directly connect to your preferred WiFi.
Wired icon	Displays the wired connected mode.
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 PIN, and unlock PIN. This icon is displayed when you connect a smart card reader to the ThinOS client.
PCoIP 	Click this icon to view the active PCoIP sessions. This icon is applicable only for PCoIP-enabled clients. You can select a session from the menu, and enable or disable the following PCoIP options in real-time: ● Relative Mouse ● Audio/Video synchronization

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 11. Taskbar - ThinOS local windows icons

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

Table 11. Taskbar - ThinOS local windows icons (continued)

Element	Taskbar icon
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 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 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 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 9.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 9.x policy settings.

Configure ThinOS using Admin Policy Tool

ThinOS 9.x 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 for 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**.

Admin Policy Tool feature list

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

Table 12. 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	VMware Horizon Settings	No
Broker Settings	Windows Virtual Desktop Settings	No
Broker Settings	Microsoft Remote Desktop Settings	No
Broker Settings	Amazon WorkSpaces Settings	No
Broker Settings	Teradici Cloud Access Settings	No
Session Settings	Global Session Settings	No
Session Settings	Citrix Session Settings	No
Session Settings	Blast Session Settings	No
Session Settings	PCoIP Session Settings	No

Table 12. Admin Policy Tool (continued)

Feature	Subfeature	Restart required
Session Settings	RDP and WVD Session Settings	No
Login Experience	3rd Party Authentication	No
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	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	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.
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
Network Configuration	Ethernet Settings	No
Network Configuration	DHCP Settings	No
Network Configuration	DNS Settings	No

Table 12. Admin Policy Tool (continued)

Feature	Subfeature	Restart required
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
Services	VNC Service	No
Services	WMS Settings	No
Services	Troubleshooting Settings	No
BIOS	Dell Wyse 3040	Yes, you must restart the client for all changes to take effect.
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.

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 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 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 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**.

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 shut down the system or restart the system.

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 system.
   - **Restart the system**—Enables you to restart the operating system.
3. Click **OK** to save settings.

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 9.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 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 9.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 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 9.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 applicable to the Wyse 5470 Thin Client. The battery indicator is displayed on the system tray.

The following table contains the battery indicators:

Table 13. 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
  - Memory size
  - Memory Usage
  - CPU Speed
  - SSD size—the storage size of the SSD/eMMC on which ThinOS is installed.
  - CPU Utilization
  - Monitor
  - Resolution
  - Parallel ports
  - Serial ports
  - Battery—Wyse 5470 Thin Client only

- Remaining time—Wyse 5470 Thin Client 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
  - Citrix Workspace App version
  - Teradici PCoIP
  - VMware Horizon
  - WVD
  - WMS status
  - MQTT server

  NOTE:
  - **Kernel mode**—The components are implemented in Kernel according to the specification. The version is displayed as [max].[min], which is the base version of 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 19.12.0.19. 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 sleep mode feature is supported on the following platforms:

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

The USB interface is closed in sleep mode. All USB devices such as USB drives, Bluetooth, audio devices, video devices, and camera 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 on to broker agent, all the windows are closed automatically and signed off when entering sleep mode. If you are not signed on to 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 BIOS.

Wyse 5470 Thin Client—The AC power must be connected to wake the Wyse 5470 Thin Client using the USB keyboard or mouse. You can also wake the Wyse 5470 Thin Client by opening the lid.

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 9.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 14. ThinOS system variables

Variable	Description
$IP	IP address
$IPOCT4	The fourth octet of IP Address. For example, if IP is 10.151.120.15, the value is 15.
$UN	Sign-on username
$DN	Sign-on domain name
$DHCP (extra_dhcp_option)	Extra DHCP options for Windows CE unit, including 169, 140, 141, 166, 167. For example, set a string test169 for option tag 169 in DHCP server, and set TerminalName=$DHCP(169) in the Wyse Management Suite server. After the thin client checks in to the Wyse Management Suite server, check the terminal name in GUI, and the terminal name is changed to test169. 166 and 167 is default for CCM MQTT Server and CCM CA Validation in ThinOS. So you need to remap the options from GUI if you want to use $DHCP(166)/ $DHCP(167).
$MAC	MAC address
$CMAC	MAC address with colon

Table 14. ThinOS system variables (continued)

Variable	Description
$UMAC	MAC address with uppercase letters is used.
$TN	Terminal name
$SUBNET	Subnet notation, the format is {network_address}_{network_mask_bits} For example, if the ip address is 10.151.120.15, network mask is 255.255.255.0, 10.151.120.0_24 is used.
$FIP	IP Address with xxx.xxx.xxx.xxx, for example,123.123.123.022
$SN	Serial number
$VN	Version number
Right($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.

4

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, Horizon, RDP and PCoIP.

Steps

1. Configure the Broker agent connection on ThinOS. See, Configure the Broker Setup.
2. On the desktop taskbar, click
   
   (**Connection Manager**) and then click **Global Connection Settings**.
   The **Global Connection Settings** dialog box is displayed.
3. 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 if you want the session to be launched only once at the same time.
     - **Re-connect after disconnect**—Select the check box if you want the session to launch again after the connection is disconnected.
     - **Mount disks as read-only**—Select the check box if you want to disable write access for storage disks.
     - **Enable Imprivata VC**—Select the check box if 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.
   - **Auto connect to local devices**—Select the check boxes to automatically connect to local devices, such as printers, serials, smart cards, audio 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 if you do not want disk devices to be redirected to the remote session.
     - **Exclude printer devices**—Select the check box if you do not want printer devices to be redirected to the remote session.
     - **Exclude audio devices**—Select the check box if you do not want audio devices to be redirected to the remote session.
     - **Exclude video devices**—Select the check box if you do not want video devices to be redirected to the remote session.
4. 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 if you want to launch applications and desktops seamlessly.
      - **Desktop with fullscreen mode**—Select this check box if you want to launch the desktop session in fullscreen.
      - **Enable HDX/MMR**—Select the check box if you want to enable the Multimedia Redirection feature. When this option is enabled, the audio and video is rendered on the user device instead of the server.
      - **Enable session reliability**—Select the check box if you want the session to remain active when the network connection is unstable.
      - **Enable UDP audio**—Select the check box if 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 optimized for your connection.
5. Click the **Horizon** tab, and select the check boxes to enable the options that are applied to all sessions. The available options are:

- **Allow H.264 decoding**—Select the check box if you want to enable the H.264 decoding in Horizon Client. Enabling this option improves the performance of high-end applications. H.264 is disabled by default.
- **Allow High Color Accuracy**—Select the check box if you want to allow Horizon Client to use a superior color fidelity when H.264 decoding is enabled.
- **Allow High Efficiency Video Decoding**—Select ths check box to enable High Efficiency Video Coding (HEVC). For more information, see High Efficiency Video Coding

  NOTE: HEVC in Blast Extreme requires both the ESXi hosts that supports the virtual desktops, and RDSH servers to have NVIDIA Tesla or newer graphics cards to offload its 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.

6. 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 check box if you want to verify users before connecting to a full RDP connection.
      - **Force Span**—Select the check box if 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 if you want to enable recording from a local microphone.

   b. 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
7. Click **OK** to save your settings.

5

Configuring connectivity

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

From ThinOS 9.1.4234, 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.

Configure the general settings

About this task

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

Steps

1. 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 13. 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: From ThinOS 9.1.3112 onwards, 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.
ii. Enter the IP address of the DNS server in the **DNS Server** field.

However, the use of DNS is optional. DNS enables you to specify remote systems 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 systems 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 **OK** 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. 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:

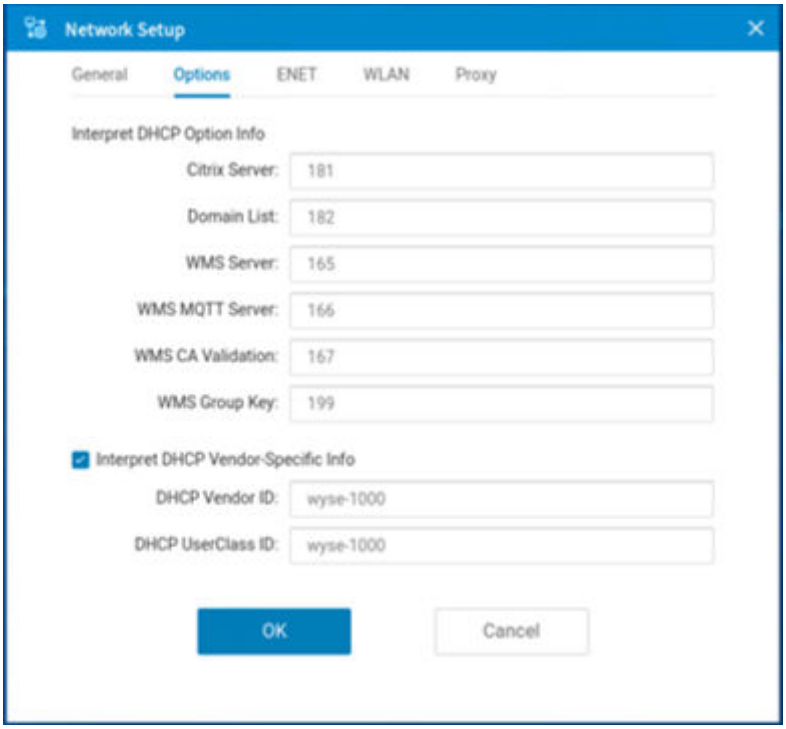


Figure 14. Options tab

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 15. 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 is the one which must authenticate the user ID and password. Only the selected domain is used in the authentication process. If the domain list is incomplete and if the user credentials must be verified against a domain not in the list, you can 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.
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

Table 15. DHCP option tags (continued)

Option	Description	Additional information
		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 **OK** to save your settings.

NOTE: The User Class option for 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. 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:

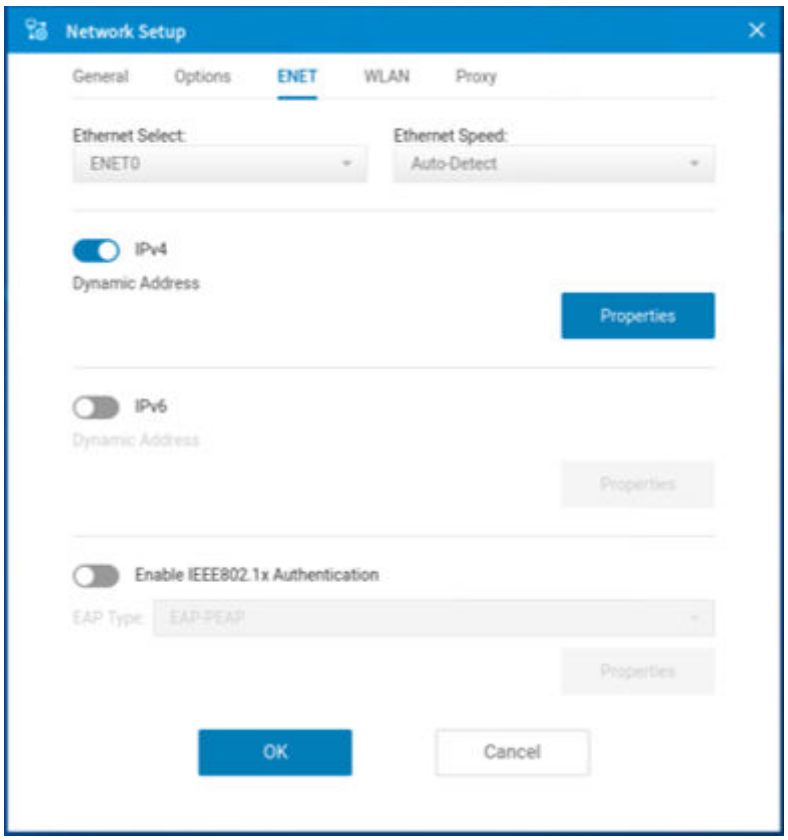


Figure 15. ENET tab

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

NOTE: For Wyse 5070 Thin Client without SFP or RJ45 module, the **ENET0** option is selected by default. For Wyse 5070 thin client with SFP or RJ45 module and Wyse 5470 Thin Client that is connected to Dell WD19 docking station, select either **ENET0** or **ENET1** based on your network preference.

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 MB Half-Duplex**
   - **10 MB Full-Duplex**
   - **100 MB Half-Duplex**
   - **100 MB Full-Duplex**
   - **1000 MB Full-Duplex**

   NOTE: The **10 MB 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 IP 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.
   - Select the **Statically specified IP 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. The maximum length for the username or the password is 31 characters.
- **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 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 **OK** to save your settings.

Configure the WLAN settings

About this task

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

NOTE: On the Wyse 5070 Thin Client with an optional SFP module or RJ45 module, you cannot configure the wireless settings.

Steps

1. 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:

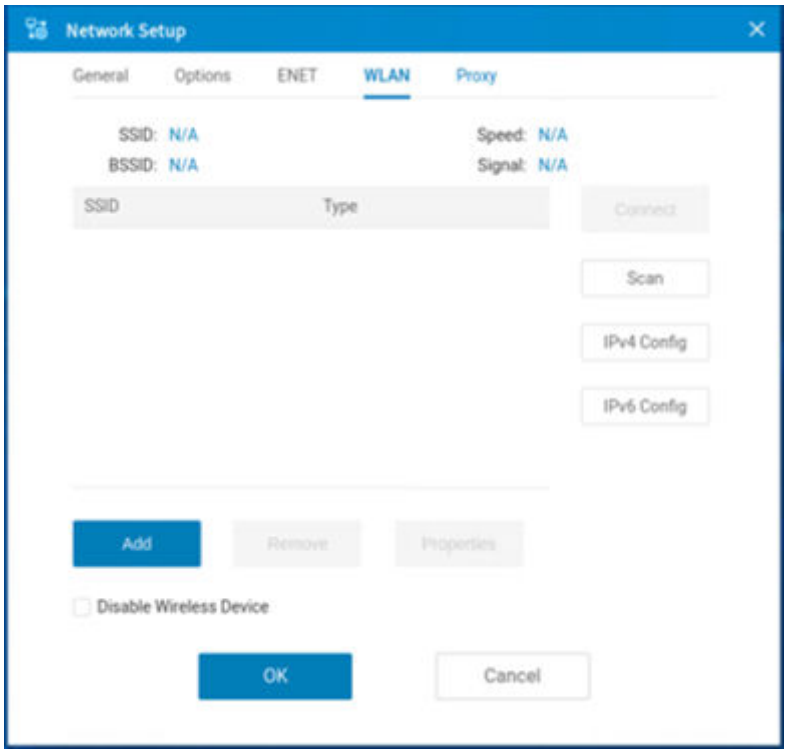


Figure 16. WLAN tab

- **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.
- **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 IPv4 connection using either DHCP or static IP address, configure any one 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 IPv6 connection using either DHCP or static IP address, configure any one 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 **OK** to save your settings.

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

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 9.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. Restart your thin client for 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. From the desktop menu, click **System Setup** > **Network setup**.
   The **Network setup** dialog box is displayed.

Table 16. Supported protocols

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

   In ThinOS 9.1.2101 and 9.1.3112, a new app list value **HORIZON** is added. For the VMware Broker agent logon 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.

   In ThinOS 9.1.3112, a new proxy app list value called **MTOP** is added for Microsoft Teams in an ICA session.

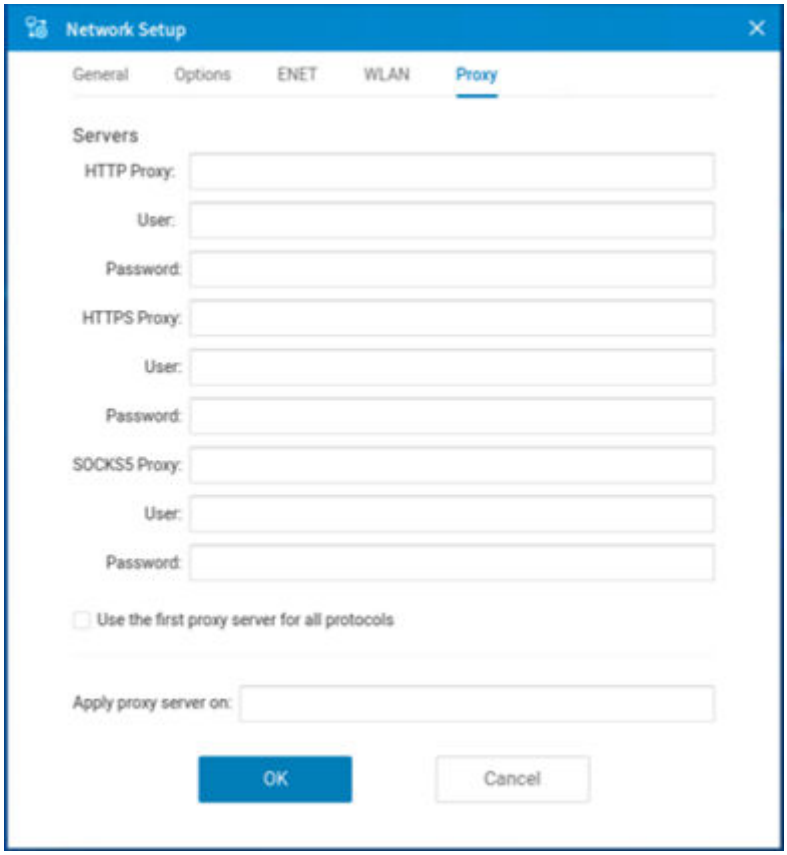


Figure 17. Proxy tab

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, credential pass through ($UN/$PW) is not recommended because it starts before user sign on.

  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 SOCKS5 proxy is configured, 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 proxy use the same host and port, and SOCKS5 proxy agent uses HTTP host with default Socks5 port (1080).

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

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

ThinOS supports the usage of DHCP option tag 252. This 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 GUI.

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, 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, 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.

Table 17. 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)
VMware	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)
Windows Virtual Desktop	broker log in	Yes	Yes (WVD 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
Teradici Cloud	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)

User scenario

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

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

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. 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 **Broker type** drop-down list, and configure the broker settings.
3. Click **OK** 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. 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:

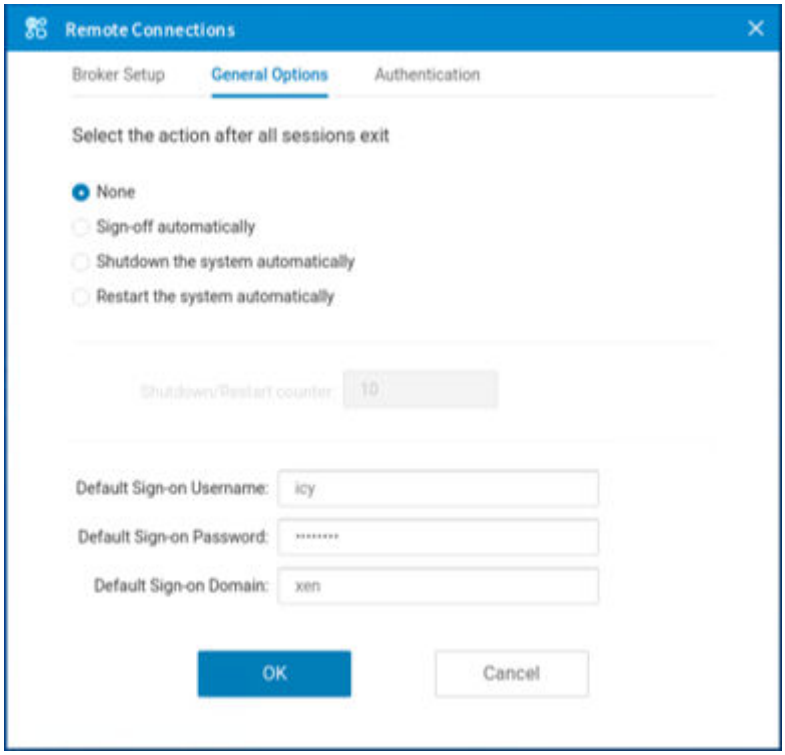


Figure 18. General options

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

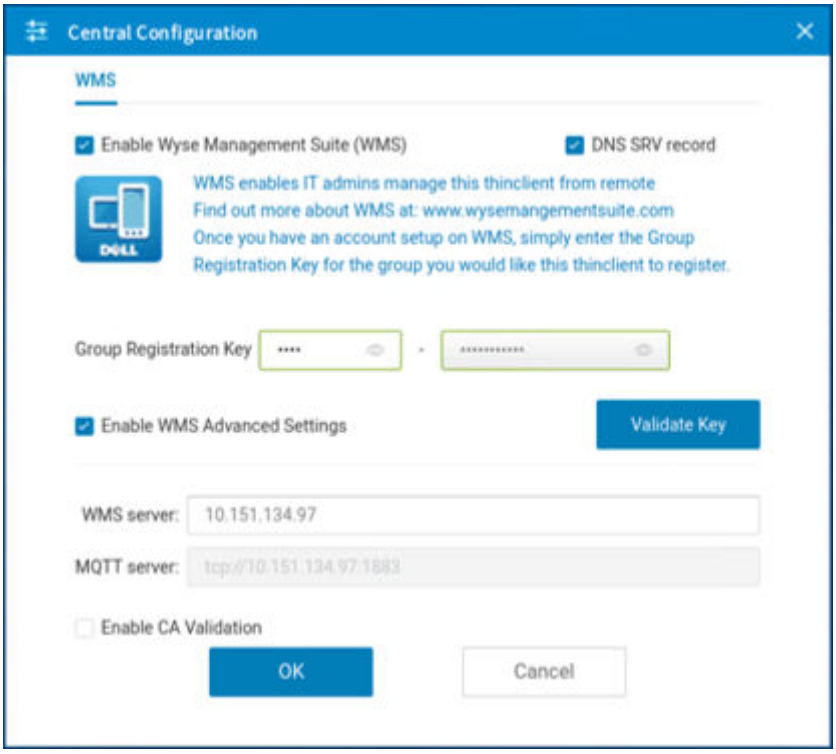


Figure 19. Wyse Management Suite

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.

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.

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 18. 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.

3. Click **OK** 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**. If you do not want to restart your client, click **Cancel**.

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. 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:

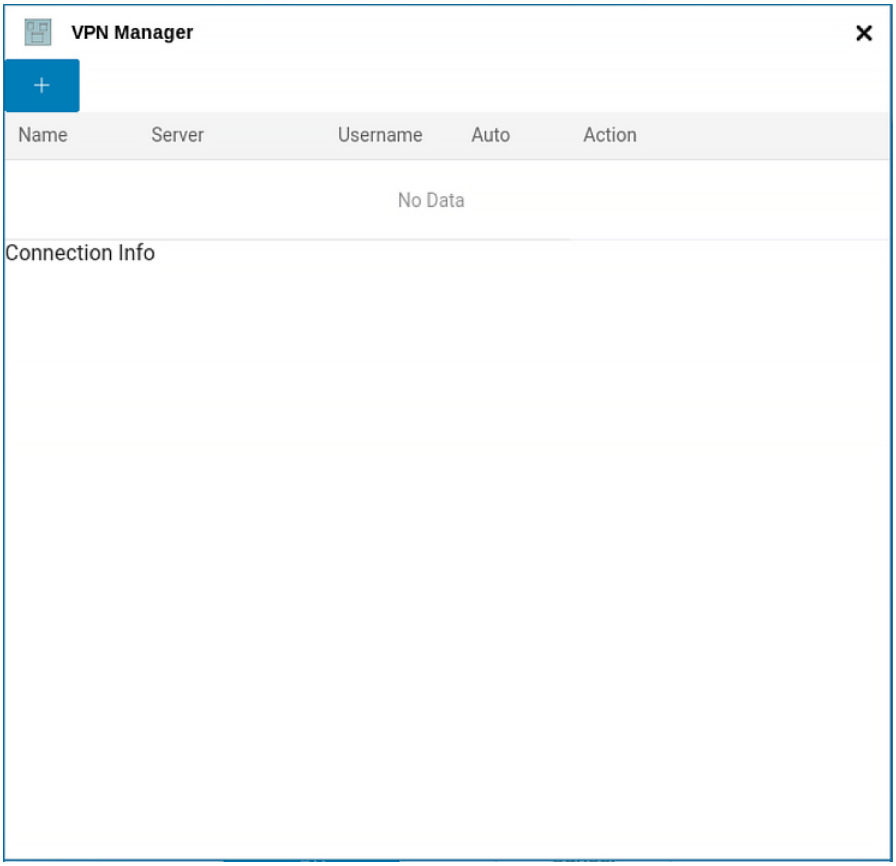


Figure 20. VPN Manager

a. Enter the name of the session in the **Name** field. This option is mandatory. The maximum character limit is 21 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 63 characters.
c. Enter the login username in the **Username** field. This option is mandatory. The maximum character limit is 31 characters.
d. Enter the password in the **Password** field. This option is not mandatory. The maximum character limit is 31 characters.
e. Click the **Auto-connection on system startup** button to automatically connect to the VPN when the device restarts.
f. Click the **Show progress in detail** button to display the VPN connection progress.
g. Click the **Show debug information** button to display the VPN debug details for better troubleshooting.
h. Click **OK**.

   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.

3. Select a session and click **Connect**.
4. Click **OK** to save your changes.

Configure VNC services

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 9.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Services** and click **VNC Service**.
4. To enable VNC shadowing, click the **Enable VNC Daemon** button.
   a. Enter the password in the **Password** field. The password length is restricted to eight characters from ThinOS 9.1.2101.
   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 VNC 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 seconds 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**.

6

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 9.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. 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, Dell Technologies recommends 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 the remote session. This option is added to resolve the Citrix limitation.

For information about the supported Citrix Workspace app features in ThinOS, see the Citrix Workspace app feature matrix table in the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support

Configure the Citrix broker setup

About this task

This section describes how to configure the Citrix 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 **Citrix Virtual Apps and Desktops** from the **Select Broker Type** drop-down list, and do the following:

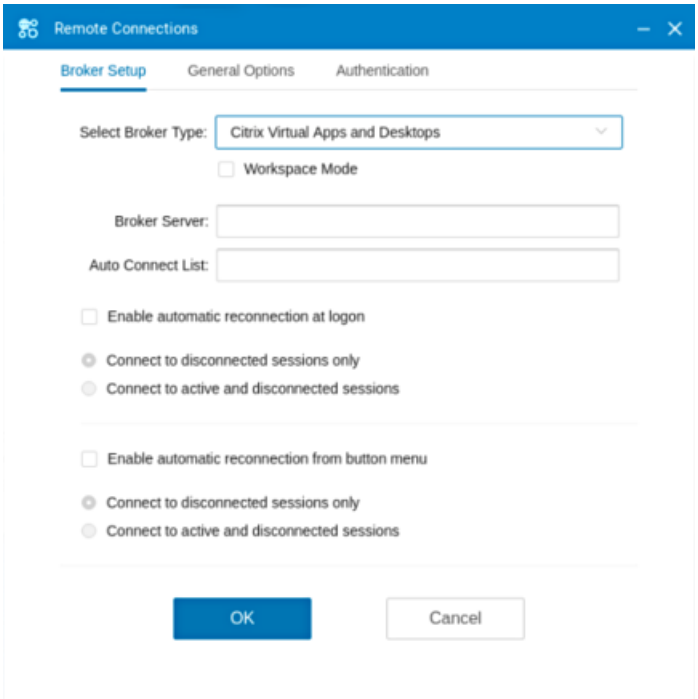


Figure 21. Broker Setup

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.
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 **OK** to save your settings.

Classic mode vs Workspace mode

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

Figure 22. Classic mode

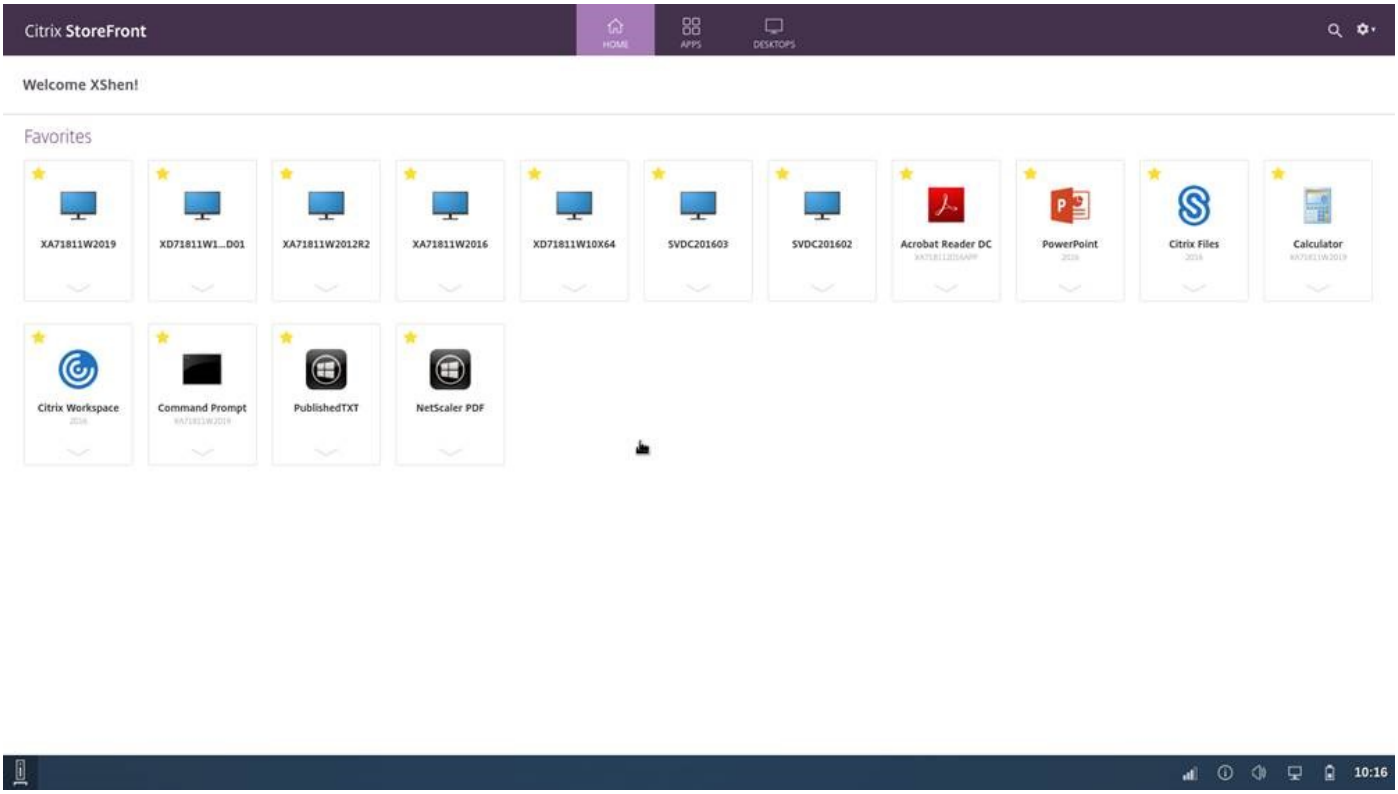


Figure 23. Workspace mode

Table 19. 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** .
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 windowed 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 windowed 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 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

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, Dell Technologies recommends 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.

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 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* at www.citrix.com.

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* at www.duo.com.

Configure Citrix ADC using CensorNet MFA authentication

Prerequisites

SMS PASSCODE is re-branded as CensorNet MFA. You can configure the Citrix ADC (formerly NetScaler) to use a One Time Passcode/Password (OTP) in the form of a personal identification number (PIN) or passcode. To obtain this one-time password, you must install 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 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. You can download the SMS PASSCODE v9.0 file from download.smspasscode.com/public/6260/SmsPasscode-900sp1.
- 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. You will receive a push notification from the CensorNet App on your phone with the code.
3. Click **OK**.
   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, 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.

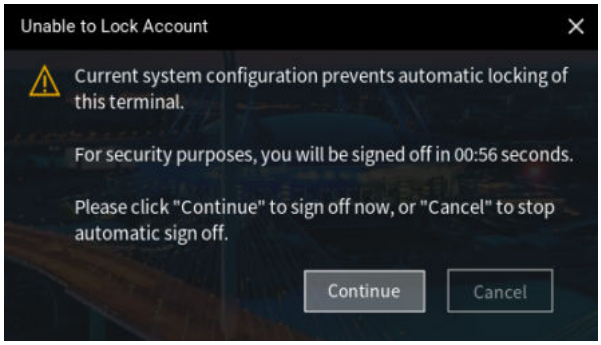


Figure 24. Unable to lock account

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.

If you access the Broker agent using SAML, 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.

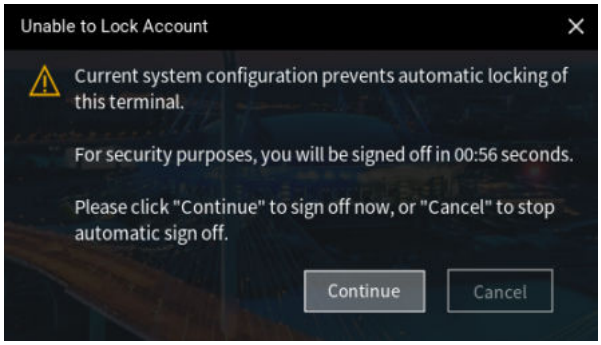


Figure 25. Unable to lock account

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 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 one 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

Only OKTA with Citrix Gateway (RADIUS) is verified. However, the StoreFront with OKTA SAML authentication or OKTA with Citrix Gateway (SAML) is not verified.

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.

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.

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: In ThinOS 9.1.4234, BCR with Chromium Embedded Framework (CEF) is enabled by default. ThinOS does not provide the configuration to change BCR with WebKitGKT+.

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 **OK**.
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 **OK**.
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 unlock account 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.

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 9.0-based device or open the **ThinOS 9.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 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.
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 ON state.
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 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, 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 Citrix Workspace app, see the *Citrix Virtual Apps and Desktops keyboard and IME configurations* article at www.citrix.com/blogs.

Table 20. 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 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* at www.support.citrix.com.
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 21. Language keyboard layout settings

ThinOS keyboard layout	Windows layout	Wyse Management Suite settings	Citrix Workspace app Linux dynamic synchronization	Recommended settings
Polish	Keyboard layout partially matches with the Windows layout.	Not supported; will be supported in future release.	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)	Keyboard layout fully matches with the Windows layout.	Not supported; will be supported in future release.	Enabled	
French (France)	Keyboard layout partially matches with the Windows layout.	Supported	Enabled	
French (Microsoft)	Keyboard layout fully matches with the Windows layout.	Not supported; will be supported in future release.	Enabled	
Belgian	Keyboard layout does not match with the Windows layout.	Not supported; will be supported in future release.	Enabled	
Belgian (Comma)	Keyboard layout fully matches with the Windows layout.	Not supported; will be supported in future release.	Enabled	
Spanish	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 22. 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 mode on either the client side or the server side. You must set the value in `/opt/Citrix/`

Table 22. Citrix Workspace app Linux keyboard layout settings—Client and VDA (continued)

Mode	Client-side settings	Server or VDA-side settings	Additional information
		• 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`	`ICAClient/module.ini [KeyboardLayout].`

Dynamic sync	`/opt/Citrix/ICAClient/config/module.ini`
	`[ICA 3.0]`
	`KeyboardSync=On`
	`~/.ICAClient/wfclient.ini`
	`[WFClient]`
	`keyboardlayout=(User Profile)`
		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 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`
			Set the mode on both the client side and the server side.

Table 22. Citrix Workspace app Linux keyboard layout settings—Client and VDA (continued)

Mode	Client-side settings	Server or VDA-side settings	Additional information
		• 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 23. 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
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

Table 23. ThinOS dynamic synchronization support (continued)

Keyboard	Synchronization
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
Japanese (KWD)	Supported. When you switch to the language Keyboard layout in VDA, the keyboard layout is synchronized to the English layout.
Korean (MS-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

Table 23. ThinOS dynamic synchronization support (continued)

Keyboard	Synchronization
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 9.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. This 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**.

Cursor pattern in ICA session

In ThinOS 9.1.2101, 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 9.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.

Citrix multiple virtual channels

From ThinOS 9.1.3112 and later versions with Citrix Workspace app 2104 and later, 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 does 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. Dell Technologies recommends 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 9.1.2101 or earlier versions. From ThinOS 9.1.3112, 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 9.1.2101 and 131:

Table 24. 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

In ThinOS 9.1.2101 and earlier versions, 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.

Configure the Citrix virtual channels settings

About this task

This task is only applicable for ThinOS 9.1.2101 and earlier versions.

Steps

1. On the ThinOS client, open **Admin Policy Tool**, or go to the ThinOS 9.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.

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 non operator-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 re-authenticate 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.
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.

Table 25. Display details

Platforms	Best Display resolution	Maximum number of system displays	
		Standard or RDS desktop—Windows 10, 2012 R2, and 2016	HDX 3D Pro desktop—Windows 10 with NVIDIA TESLA P40 GPU
Wyse 5070 Extended Thin Client	1920 x 1080	6	4
	2560 x 1440	6	4
	3840 x 2160	4	4
	5120 x 1440	2	2
Wyse 5070 Thin Client—Pentium processor	1920 x 1080	3	3
	2560 x 1440	3	3
	3840 x 2160	3	3
	5120 x 1440	2	2
Wyse 5070 Thin Client—Celeron processor	1920 x 1080	2	2
	2560 x 1440	2	2
	3840 x 2160	2	2
	5120 x 1440	2	2

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. Dell Technologies recommends 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. Connect a USB printer to the thin client.
4. Log in to a Citrix session.
5. 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.

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 **OK**.
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.

Export Citrix Workspace App logs

Steps

1. From the desktop menu, click **System Tools**.
2. Click the **Packages** tab.

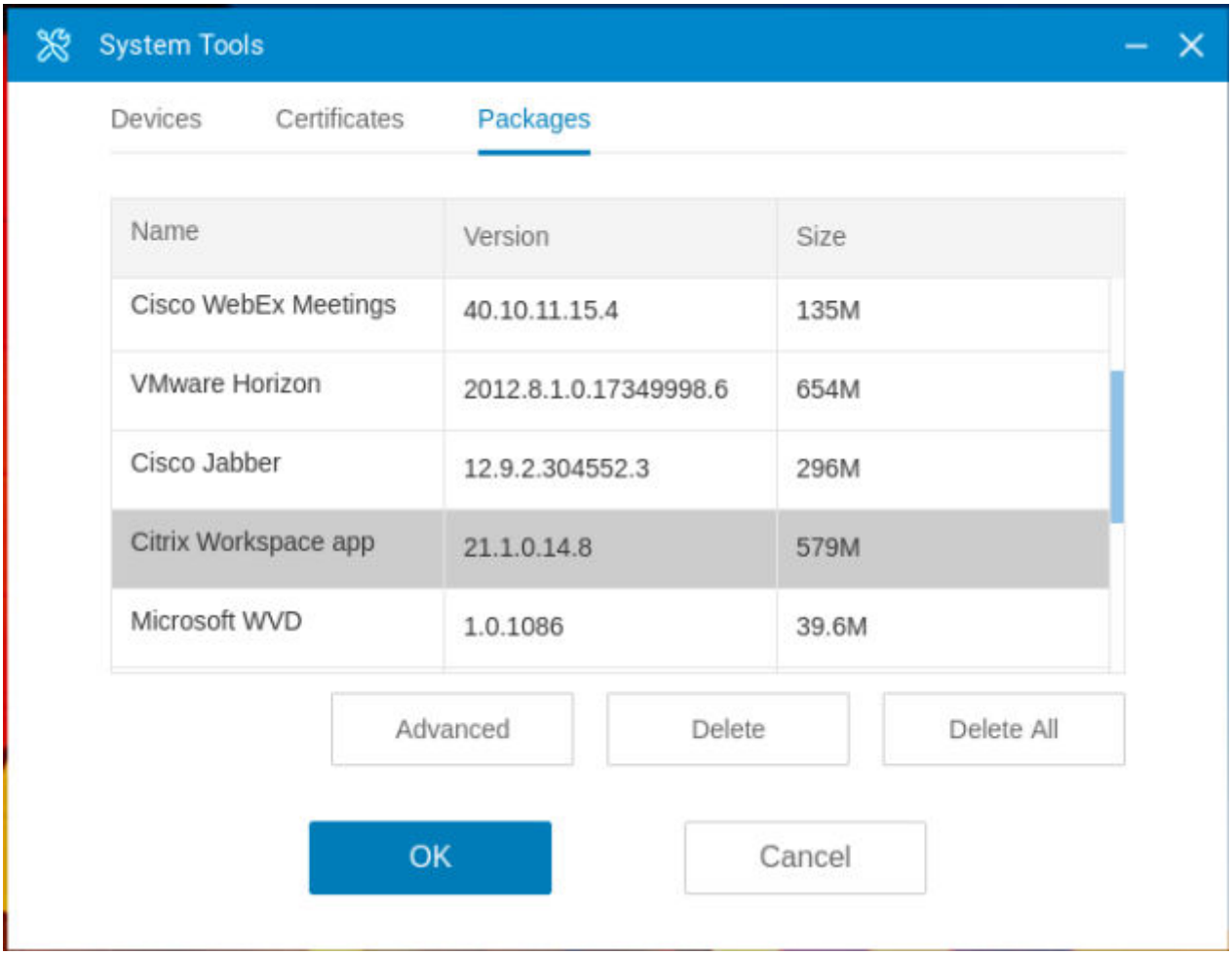


Figure 26. Packages tab

3. Select **Citrix Workspace App**, and click **Advanced**.

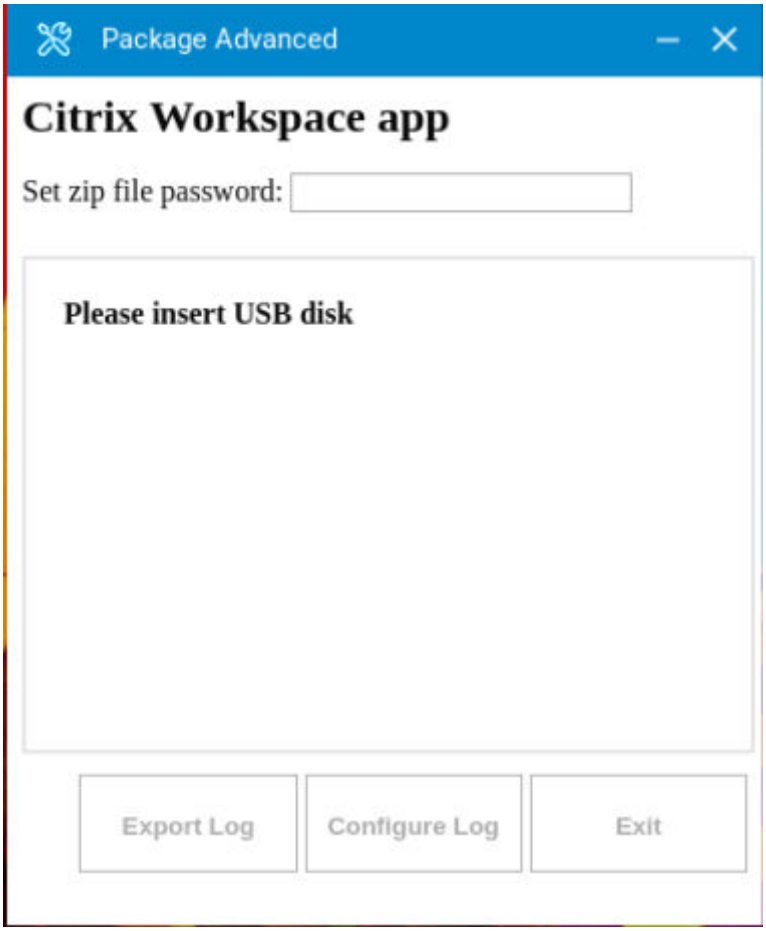


Figure 27. Package Advanced window

The **Package Advanced** window is displayed.

4. Click Configure Log.
   The **Citrix Log Preferences** window is displayed.

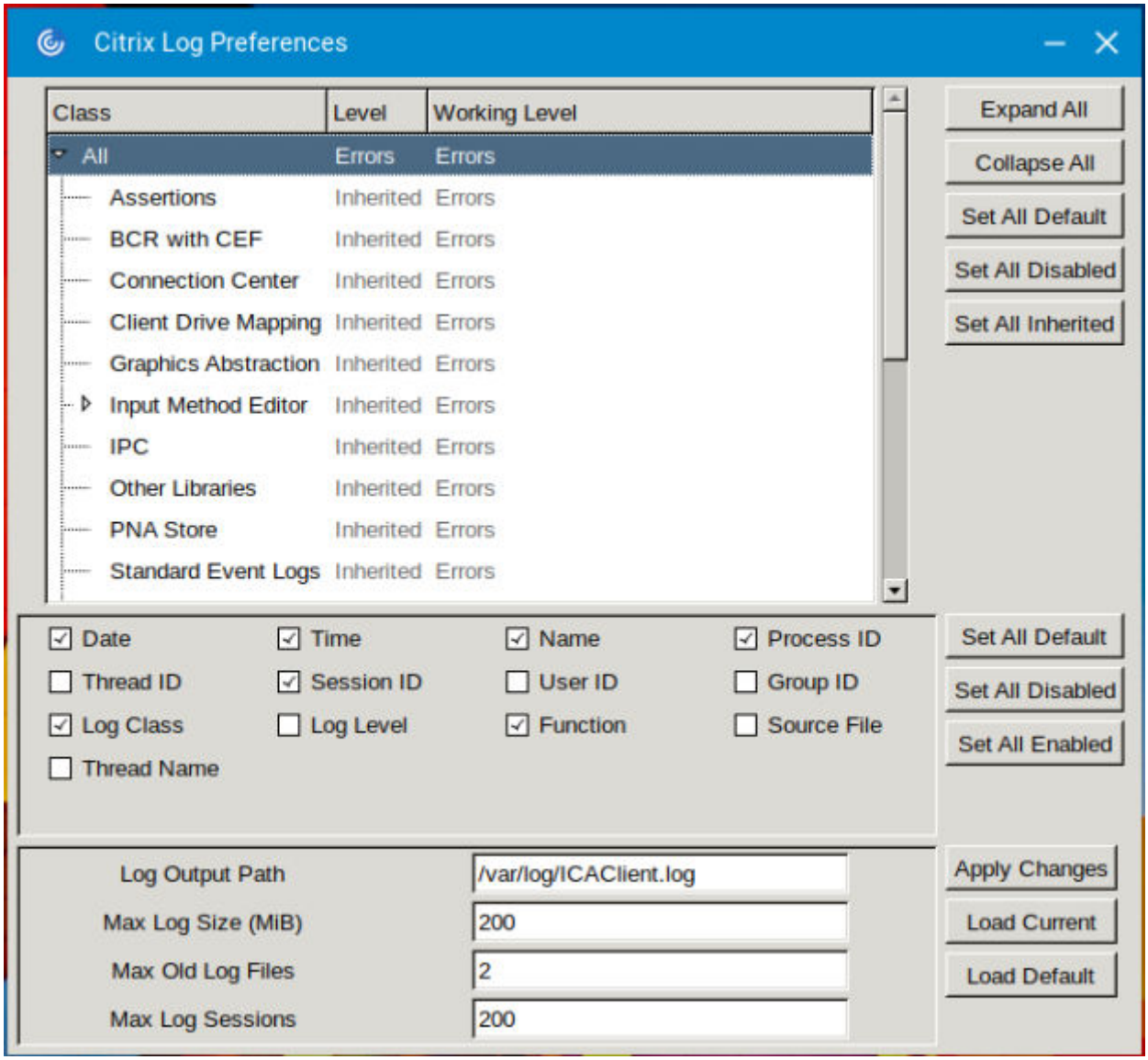


Figure 28. Citrix Log Preferences window

5. Right-click the classes that you require, and select **Verbose**.
6. Select the check boxes to select specific log items.
   Click **Set All Enabled** to select all the check boxes.
7. Enter the file name and the output file pat in the **Log Output Path** field.
   The default path is `var/log/ICAClient.log`. Dell Technologies recommends using the default log output path.
8. Click **Apply Changes** and close the **Citrix Log Preferences** window.
9. Connect the ICA session, reproduce the scenario that you require the log from, and disconnect the ICA session .
10. From the desktop menu, click **System Tools**.
11. Click the **Packages** tab.

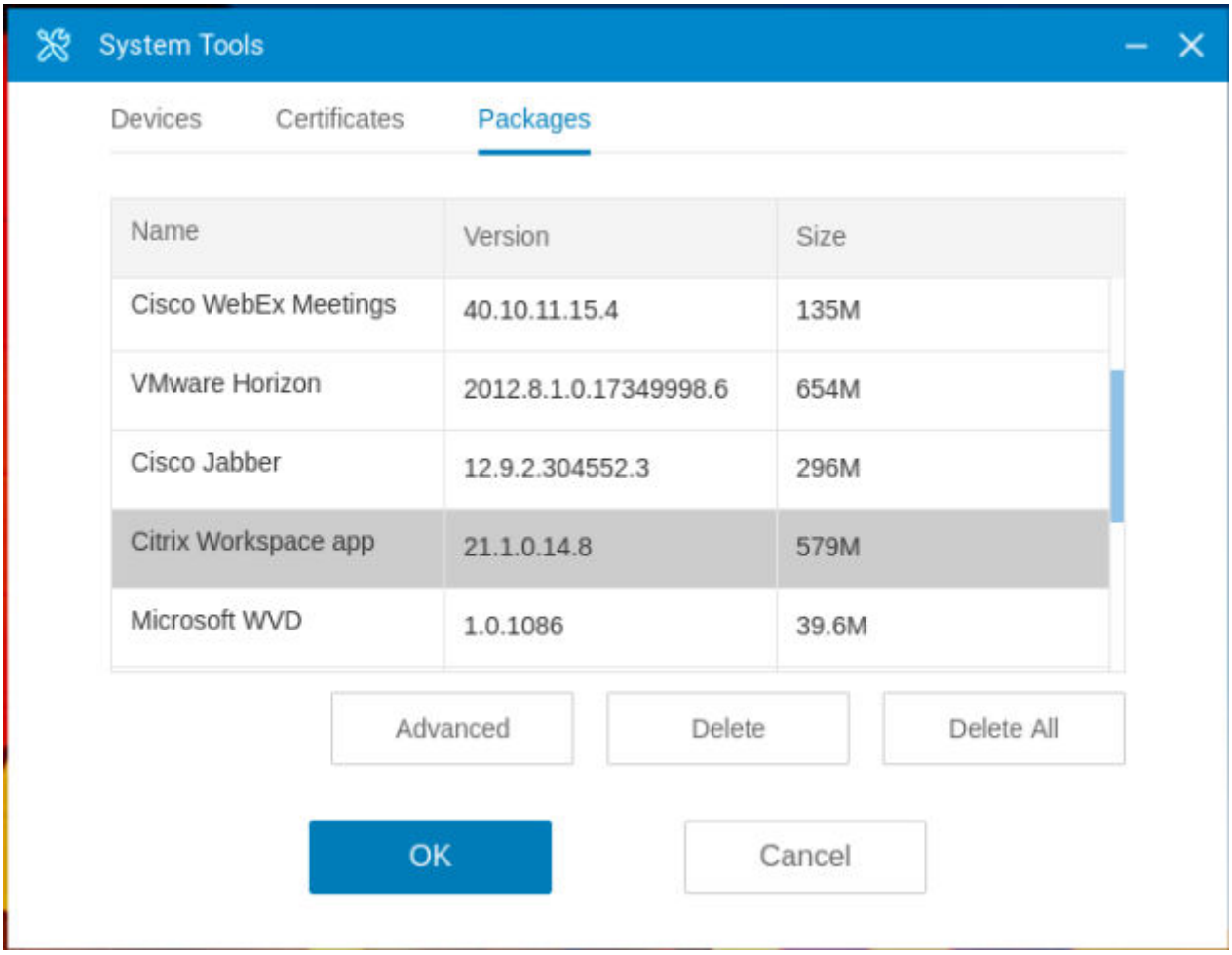


Figure 29. Packages tab

12. Select **Citrix Workspace App**, and click **Advanced**.

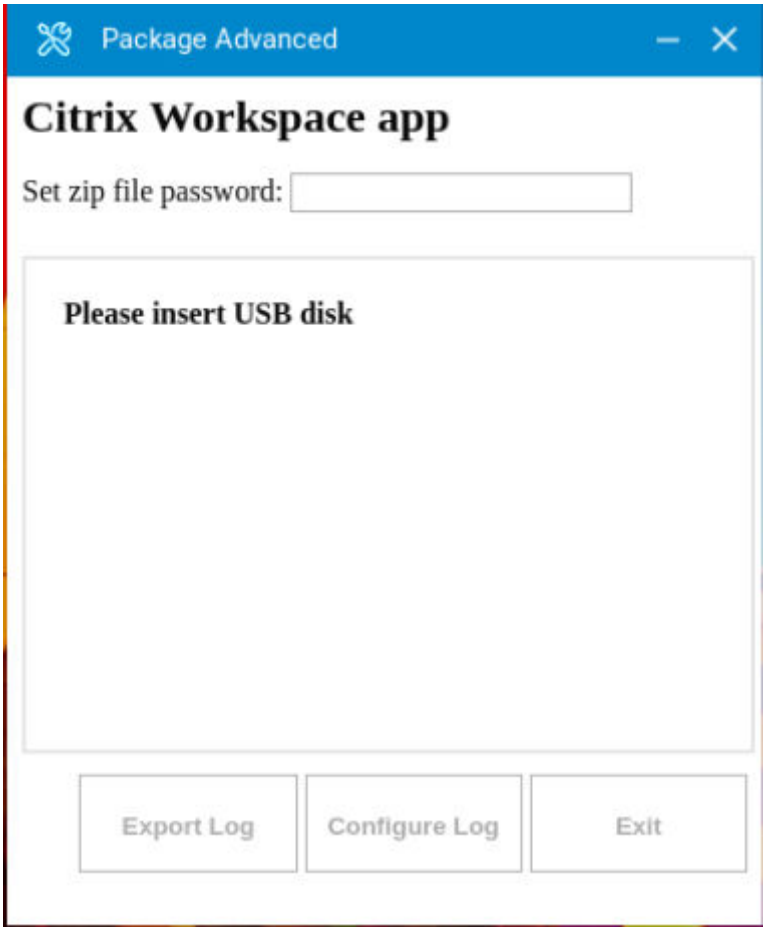


Figure 30. Package Advanced window

The **Package Advanced** window is displayed.

13. Connect a USB drive that is formatted with the FAT32 file allocation.
14. Enter a log password of your choice in the **Set zip file password** field.
15. Click **Export Log**.
    The logs are now exported successfully 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 **Package Advanced** window is displayed.

   d. Click **Configure Log**.

      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.

Limitation—When the **Disk Read Only** setting is enabled from **Advanced** > **Session Settings** > **Global Session Settings** > **Local Resources and USB Redirection** in Wyse Management Suite or the Admin Policy Tool, exporting Citrix Workspace app log sometimes fails. Workaround is to disable the **Disk Read Only** setting and then export the Citrix Workspace app log.

NOTE: Citrix Workspace app log can also be exported from **Troubleshooting** > **General** > **Export logs** in the ThinOS local user interface.

Configure multifarm

In ThinOS, multifarm works with only a Citrix Broker agent. You cannot use multifarm with other connection brokers.

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 9.x**.
4. Click the Advanced tab.
5. Expand **Broker Settings**, and click **Global Broker Settings**.
6. Enable **MultiFarm**.
7. Click **Save & Publish**.
8. Check in the thin client to 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

In ThinOS, multilogon works with only a Citrix Broker agent. You cannot use multilogon with other connection brokers.

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 9.x**.
4. Click the Advanced tab.
5. Expand **Broker Settings**, and click **Global Broker Settings**.
6. Enable **MultiLogon**.
7. Click **Save & Publish**.
8. Check in the thin client to 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**.

Configuring VMware

VMware virtualization enables you to run multiple virtual machines on a single physical machine. VMware 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 VMware Horizon Client version may get updated to a newer version. You must upgrade the VMware Horizon package along with the ThinOS firmware. VMware Horizon package versions have a dependency on the ThinOS firmware versions. See the *Release Notes* of your ThinOS version at www.dell.com/support to know the corresponding VMware Horizon package version.

For information about the latest VMware Horizon Client version and the known issues, see the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.

In ThinOS 9.1.2101, full screen/window mode could be set from both the client and the server side. From ThinOS 9.1.3112, you can set the full screen/window mode only from the client using the Wyse Management Suite policy Settings or the Admin Policy tool. The Horizon Broker fullscreen/window mode setting of Blast, PCoIP, and RDP is ignored. To enable the full screen mode, go to **Advanced** > **Session Settings** > **Global Session Settings** and enable the **Full Screen Mode** option under **Display Settings** from Wyse Management Suite policy settings or the Admin Policy Tool.

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 *VMware Product Interoperability Matrices* page at www.vmware.com.

Configure the VMware broker connection

About this task

This section describes how to configure the VMware broker setup 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 **VMware Horizon** from the **Select Broker Type** drop-down list, and do the following:
   - **Broker Server**—Enter the IP address/Hostname/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 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**.

     NOTE: The **PCoIP only** connection protocol is applicable only to PCoIP clients. If you do not install the Teradici PCoIP package, then the **PCoIP** protocol option is not available.

     The available options are:

     - **Server default**—Select this protocol connection to display the desktop with default protocol as configured in the VMware View Admin console, for each pool in the broker. If a desktop pool is configured with 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 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 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**—This option is available only for PCoIP enabled clients. 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 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**—VMware 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.

- **Log in anonymously using Unauthenticated Access**—Select this check box to anonymously log in to the VMware session with application remoting.

3. Click **OK** to save the settings.

VMware Real Time Audio-Video

About this task

Use the Real-Time Audio-Video feature to run Skype and other 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.

To know more about the VMware Real Time Audio-Video support, go to pubs.vmware.com.

NOTE: There is no additional configuration for ThinOS.

To validate the VMware Real Time Audio-Video, do the following:

Steps

1. Connect to the VMware 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 VMware virtual audio.
3. Verify the system audio recording using the VMware virtual microphone.
4. Verify the audio settings in VoIP application.
5. Verify the video settings in VoIP application using the VMware virtual webcam.
6. Start the audio or video calls.

High Efficiency Video Coding

In ThinOS 9.1.4234, VMware 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 **Connection Manager** > **Global Connection Settings** > **Horizon**. You can go to the VMware Horizon Performance tracker and see **Encoder Name** to verify whether HEVC is working. If 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.

For more information, see the *VMware Blast Extreme Optimization Guide* at techzone.vmware.com.

Enable or disable HEVC from Admin Policy Tool and Wyse Management Suite Policy settings

Steps

1. Go the Admin Policy Tool or Wyse Management Suite policy settings.
2. In the **Advanced** tab, expand **Session Settings**.
3. Click **Blast Session Settings**.
4. Click the **Allow High Efficiency Video Decoding** toggle to enable or disable HEVC.
5. Click **Save & Publish**.

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, Windows Image Acquisition (WIA), 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 VMware Horizon session. You must select this feature in the VMware 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 **Broker & Session**, and expand **VMware Horizon 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 (Scanner) 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 **Exclude Vid/Pid USB Device Redirection** field.
5. Click **Save & Publish**.
6. Launch the Horizon View desktop on ThinOS.
7. Open the VMware 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 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.

NOTE: ThinOS supports the Serial Port Redirection feature only on the Wyse 5070 Thin Client and the Wyse 5070 Extended Thin Client.

To use the Serial Port Redirection feature, you must install the feature in the VMware Horizon session. This feature is installed in the VMware 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 View desktop on ThinOS.
2. Open the VMware 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 VMware 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 VMware session. To invite a user to join your desktop session, do the following:

1. Launch a Horizon View desktop on ThinOS.
2. Click the VMware 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 touch screen may not work when the relative mouse feature is enabled. This is a VMware 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 9.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click either **Blast Session Settings** or **PCoIP Session Settings** based on your preference.
3. Click the **Enable Relative Mouse when launching session** toggle key to enable the relative mouse feature.
4. Click **Save & Publish**.

   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.

Enable relative mouse using session menu

Steps

1. On the ThinOS client, launch a PCoIP session or a Blast session.
2. In the system tray, click the PCoIP icon to view the active PCoIP sessions, or click the VMware icon to view the active Blast sessions.
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

VMware 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 VMware Connection Server console.
2. Go to **Settings** > **Servers** > **Connection Server** and click the **Authentication** tab.
3. From the **Delegation of authentication to VMware 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 **VMware Horizon** from the **Select Broker Type** drop-down list.
10. Enter the server URL in the **Broker Server** field.
11. Click **OK** and restart the thin client.
    The **VMware 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 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.vmware.com.

VMware 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 VMware Unified Access Gateway documentation at docs.vmware.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 **VMware Horizon** from the **Select Broker Type** drop-down list.
4. In the **Broker Server** field, enter the Unified Access Gateway URL.

5. Click **OK**.

Configure Microsoft Azure Multifactor authentication with VMware 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 VMware UAG documentation at docs.vmware.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 **VMware Horizon** from the **Select Broker Type** drop-down list.
4. In the **Broker Server** field, enter the Unified Access Gateway FQDN.
5. Click **OK**.
6. On the Azure **Sign In** window, enter the Azure account.
7. Click **Next**.
8. Enter the password to log in to the session.

   NOTE: ThinOS does not support Single Sign-On (SSO) to Azure MFA with VMware UAG.

Configure the VMware integrated printing settings

About this task

The VMware 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 VMware Blast desktop. ThinOS Blast printer mapping is equivalent to VMware client printer redirection.

Currently ThinOS supports only PS printer in blast session since VMware has removed Thin print support from VMware Horizon 8.0 and VMware Horizon Client 2006. Ensure that the Agent version is later than 7.9, and that you select the component VMware Integrated Printing. Certain PS model printers may not work in Blast session as it depends on the VMware 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 VMware 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 **OK** to save the configuration.

7. Click the **Options** tab, and do the following:
   a. Set **LPT1: <Printername>**as default printer.
   b. Click **OK** to save the configuration.
8. Connect to a VMware 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 VMWARE POSTSCRIPT Driver and the port is VMWPORT.
   The VMware Integrated Printing feature allows the ThinOS local printer to be mapped to the VMware Blast session without installing the printer driver in the session.

Configure the USB Printer Redirection in VMware 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 in to a Blast or a PCoIP session.
4. 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.

Wacom tablet support on ThinOS

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 *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.

Enable Wacom tablet using the session menu

Steps

1. On the ThinOS client, launch a PCoIP session.
2. In 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 26. 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 27. 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. On the ThinOS client, start **Admin Policy Tool** or go to the ThinOS 9.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **PCoIP Session Settings**.
3. 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 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.
4. 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.

USB Redirection in a VDI session

Upgrading to the ThinOS 9.1.3112 eliminates the local USB driver dependency on the USB redirection feature.

From ThinOS 9.1.3112 onwards, you can directly use the USB redirection feature in a VDI session without attaching the USB driver 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** > **Session on local ThinOS UI**.
  2. Verify if the USB device redirection is selected, and click **OK**.
- 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 9.1.2X or older versions to 9.1.3112. 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.

Enable Multimedia Redirection in Blast session

Steps

1. Access the VMware Horizon connection server from the browser.
2. Go to **Settings** > **Global Policy**.
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 VMware Horizon connection server. MMR feature uses Windows Media player as the default video player.

Smartphone sync

In ThinOS 9.1.4234, you can sync your iPhone or Android smartphone into a VMware Blast session.

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

Sync Huawei Android smartphone

Prerequisites

- Download and install HiSuite in Blast session, from https://consumer.huawei.com/en/support/.
- Install HiSuite app on your Huawei smartphone.

Steps

1. Launch the Blast session.
2. Open HiSuite from the Blast session.
3. Connect your Huawei smartphone to the client.
4. Accept the access request on your phone.
   A window that prompts you to enter a verification code from the phone, is displayed in the Blast session.
5. Open the HiSuite app on your phone and enter the verification code from the phone in the Blast session.
6. Click or tap **Connect**.

Sync iPhone

Steps

1. Go 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 (Scanner) Redirection** option.
5. Click **Save & Publish**.

6. Launch the Blast session and connect your iPhone to the device.
7. Accept the access request on your iPhone.

Configuring Windows Virtual Desktop

Windows Virtual Desktop is a comprehensive desktop and app virtualization service that runs on the cloud. You can access the Windows Virtual Desktop resources that are created on Azure cloud from the ThinOS client.

Prerequisites

Ensure that you have an Azure Active Directory configured and Windows Virtual Desktop resources are deployed on the Azure cloud.

About this task

This section describes how to configure the Windows 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 **Windows Virtual Desktop** from the **Select Broker Type** drop-down list, and do the following:
   a. Select the **Enable Windows Virtual Desktop** check box to configure the Windows Virtual Desktop settings.
   b. Select the **Enable Workspace (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
   c. Select the **Enable Workspace (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
3. In the **Remote Connections** dialog box, click the **General Options** tab, and specify the Azure cloud user credentials.
4. Click **OK** 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 Azure cloud are displayed.

Enable printer in Windows Virtual Desktop

ThinOS supports printer in Microsoft Windows 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 **OK**.

6. Launch the RDP session. See, Configuring Microsoft Remote Desktop Services.

   NOTE: RDP protocol supports standard printers.

Log in to Windows 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 an Azure Active Directory.
- 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 **Windows Virtual Desktop** from the **Select Broker Type** drop-down list.

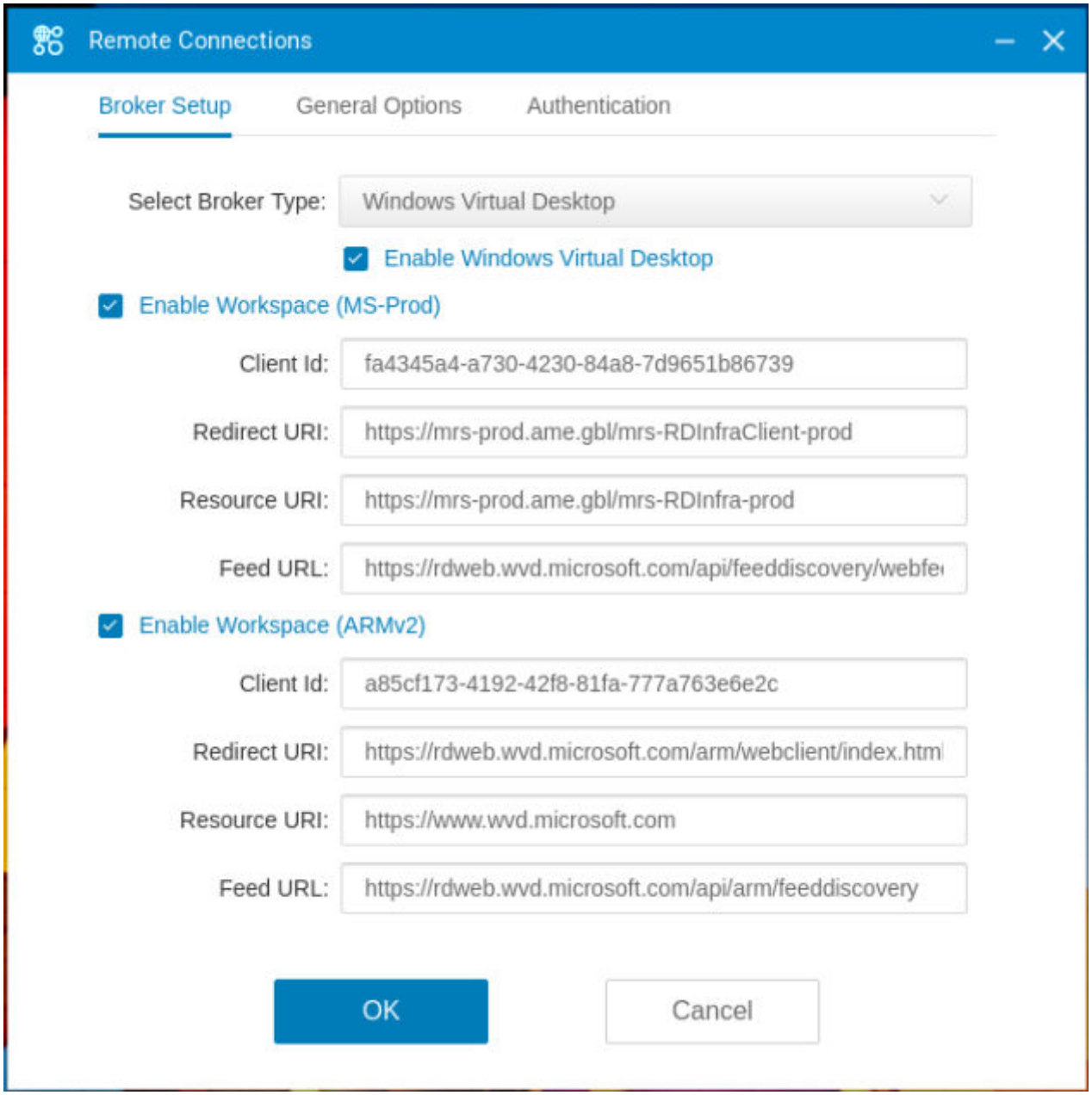


Figure 31. Windows Virtual Desktop drop-down

3. Select the **Enable Windows Virtual Desktop** check box.
4. Click **OK** and restart the thin client.
5. Enter the username of the on-premises Active Directory, and click **Next** on the **Windows Virtual Desktop** login window.
6. Enter the credentials of the on-premises Active Directory, and click **OK** on the **ADFS** window.
7. Launch the Windows Virtual Desktop session.

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 **OK** 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 WVD 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 WVD Broker agent.
6. Launch the RDS or WVD session.
   TS Gateway connection is established.

Table 28. 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 9.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 9.x policy settings on Wyse Management Suite.
2. On the **Advanced** tab, expand **Session Settings**, and click **RDP and WVD 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.

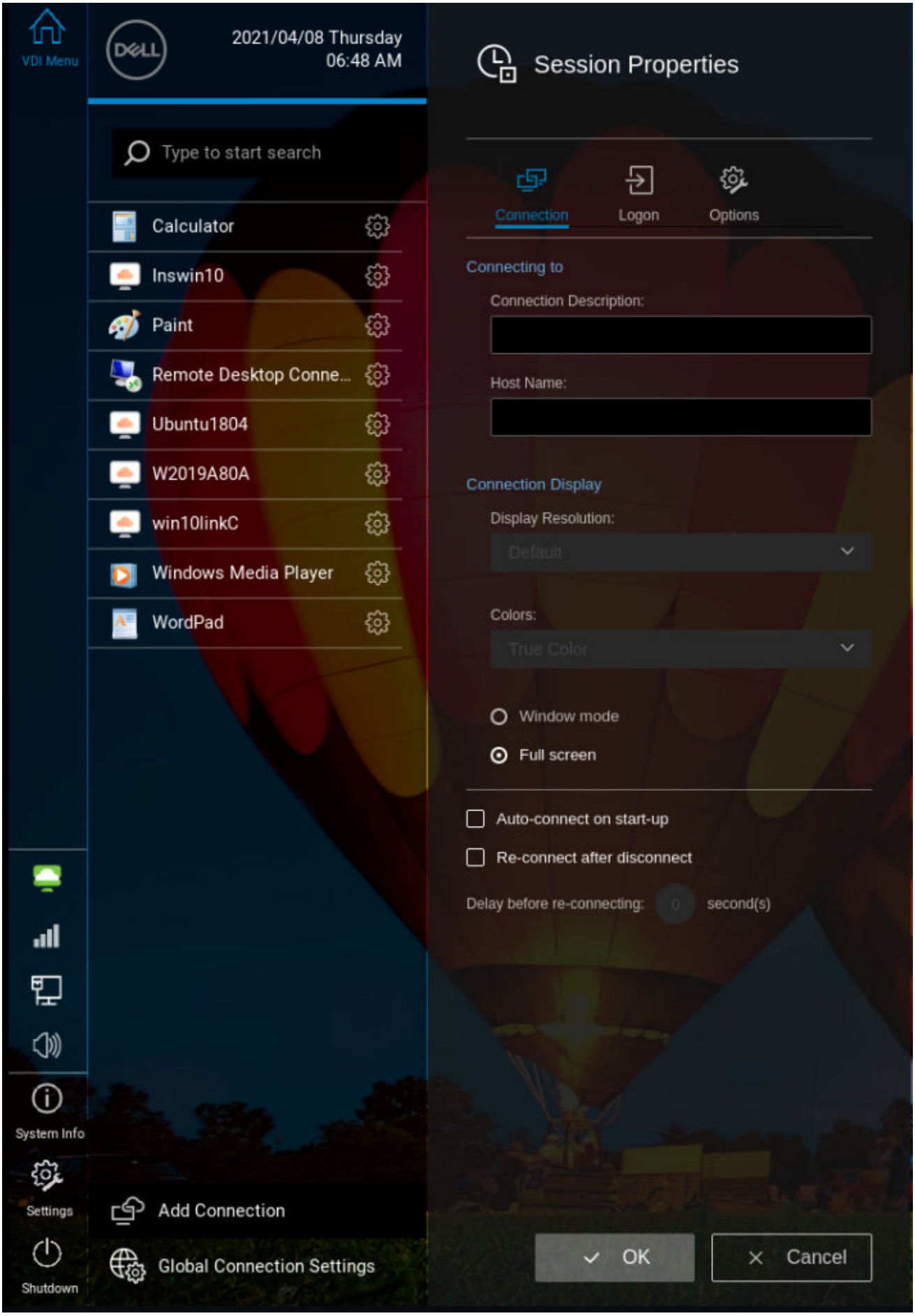


Figure 32. Auto-connect on start-up

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.

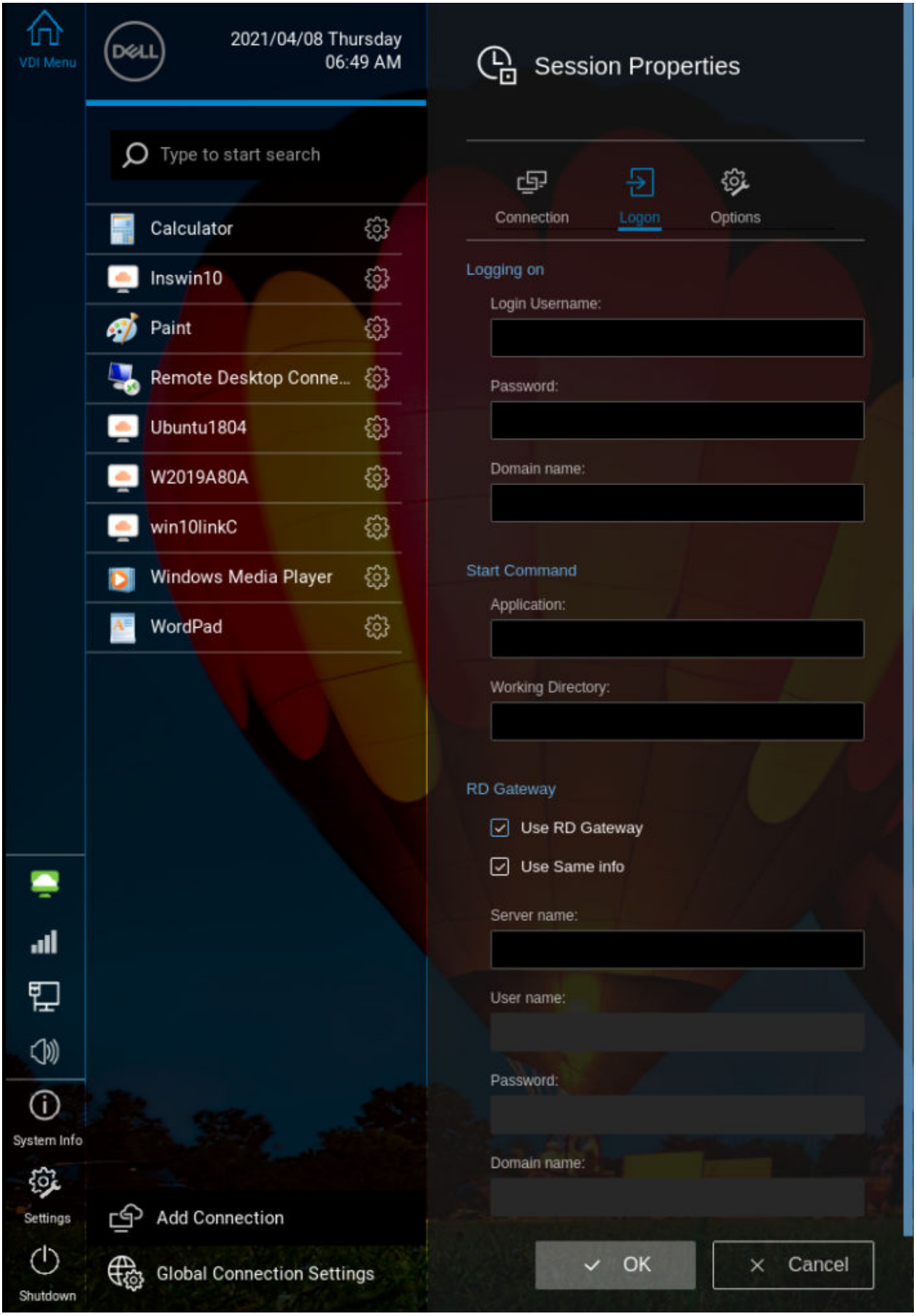


Figure 33. Use RD Gateway

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 9.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Session Settings**, and click **RDP and WVD Settings**.
4. Click **Add Row** under **Direct RDP Settings**.
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 9.x policy settings on Wyse Management Suite.
2. Click the **Advanced** tab.
3. Expand **Session Settings**, and click **RDP and WVD 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**.

Configuring the Amazon WorkSpaces broker connection

Amazon WorkSpace (AWS) is a cloud-based virtual desktop that allows you to access remote applications with ease. Amazon WorkSpaces connection is applicable only for PCoIP clients.

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, from the **Select Broker Type** drop-down list, select **Amazon WorkSpaces**.
3. Based on your preferred connection mode, do the following:
   - If you want to connect to AWS using the registration code, select the **Connect via registration code** check box, and enter the WorkSpaces registration code in the **Registration Code** field. If you want to change the registration code from the Amazon Workspace login window, you must select the **Enable Changing Registration Code from Login window** option using either Admin policy tool or Wyse Management Suite.
   - If your server supports Multi-factor authentication (MFA), enable the MFA option using Wyse Management Suite or Admin Policy Tool.

     The MFA token field is enabled. Use the Google Authenticator on your mobile device and enter the code that is generated.
   - If you want to connect to AWS using the default PCoIP Gateway mode, enter the IP address/Hostname/FQDN of the broker server in the **Broker Server** field.

- If you select the **Enable customized login** option in Admin Policy Tool or Wyse Management Suite, the Amazon Workspace customized login window is displayed.

4. In the **Auto Connect List** field, 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 listed. Each desktop name is separated by a semicolon, and is case-sensitive.
5. Click **OK**

   For information about deploying Amazon WorkSpaces, see the AWS documentation at docs.aws.amazon.com.

Teradici PCoIP licensing

The thin client security key value determines the Teradici PCoIP configurations on ThinOS.

Table 29. ThinOS PCoIP licensing

Security key value	PCoIP configuration
Thin client with a security key value that is entitled to the PCoIP protocol.	After you upgrade from ThinOS 8.6 to ThinOS, brokers that require PCoIP are supported and PCoIP configurations are allowed in the ThinOS UI.
Thin client with a security key value that is not entitled to the PCoIP protocol.	After you upgrade from ThinOS 8.6 to ThinOS, brokers that require PCoIP are not supported and PCoIP configurations are disabled in the ThinOS UI.

Configure the Teradici Cloud Access broker connection

Teradici technology enables you to securely access the remote applications using Teradici Cloud Access. You can manage and optimize your ThinOS PCoIP-enabled clients.

Steps

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
   The **Remote Connections** dialog box is displayed.
2. On the **Broker Setup** tab, from the **Select Broker Type** drop-down list, select **Teradici Cloud Access**, and configure the following options:

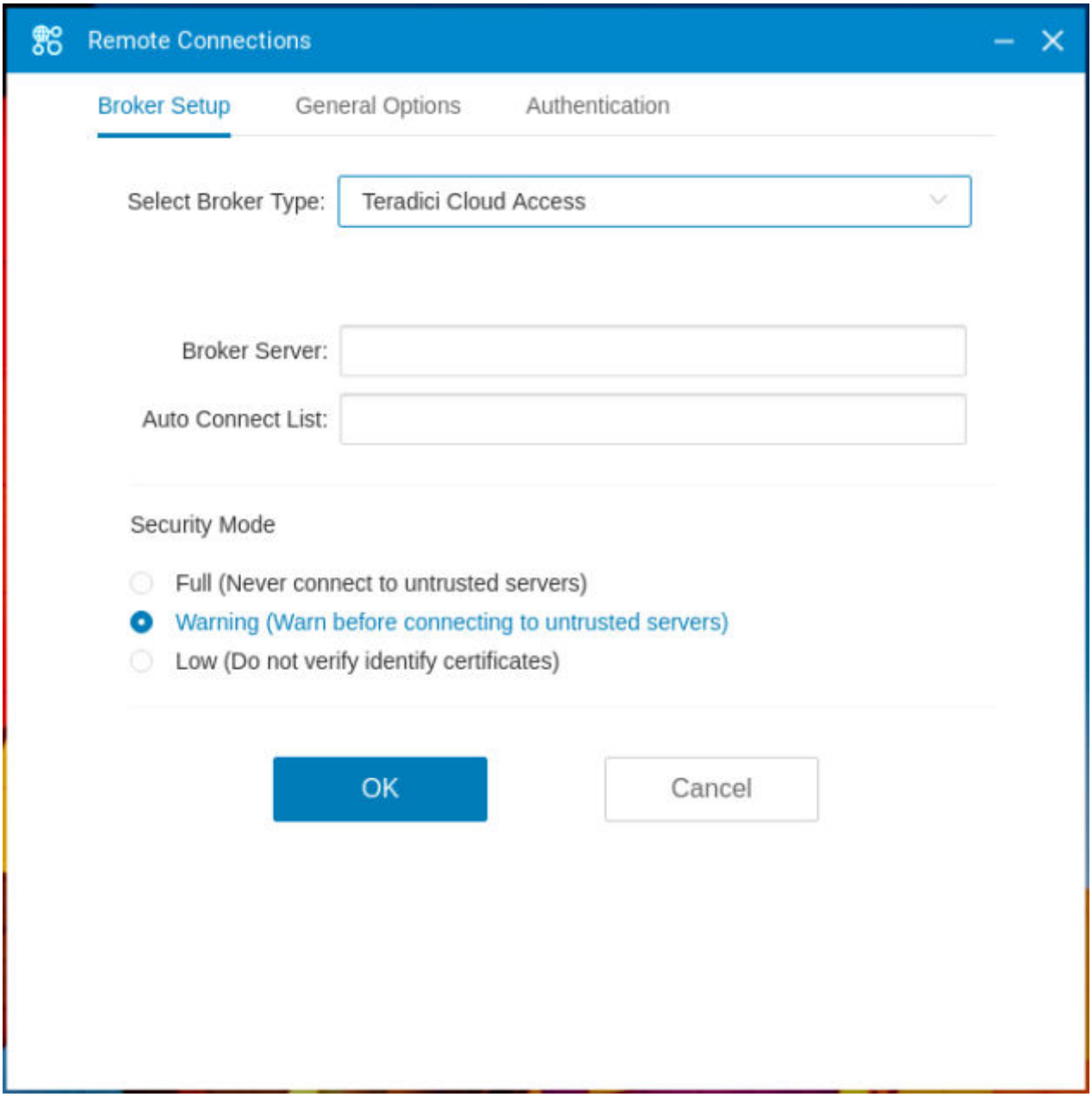


Figure 34. Teradici Cloud Access drop-down

- **Broker Server**—Enter the IP address or FQDN of the Broker agent server.
- **Auto Connect List**—Enter the name of desktops that you want to start automatically after logging in to the respective Broker agent. Use a semicolon to separate each desktop name.

  NOTE: Field values are case-sensitive.

3. Select **Security Mode**.
   - **Full**—Fails to connect to servers with unverified TLS/SSL certificates.
   - **Warning**—A warning message is displayed when you try to connect to servers with unverified certificates.
   - **Low**—Allows the connection without any verification.
4. Click **OK** to save your settings.

Configuring PCoIP connections using Teradici Remote Workstation card

ThinOS enables you to directly configure the PCoIP connection using either the TERA2240 Remote Workstation Card or TERA2220 Remote Workstation Card. This feature is supported only on PCoIP-enabled thin clients. This feature only works with the direct PCoIP connection.

Prerequisites

- Ensure that you install or upgrade Teradici Host Software to 20.04.0.413 or later versions.
- Ensure that host cards are connected to a remote workstation.
- Ensure that host cards are installed correctly, that is, connected to a remote workstation with GPU.

NOTE: The SDK in ThinOS does not function similar to Teradici zero client firmware. For example, the SDK in ThinOS does not support USB redirection and Relative Mouse features with the host card connection. This feature is mainly for workstation users working on the server remotely.

Steps

1. On ThinOS desktop, go to **Connect Manager**.
2. Click **New**, and then click **PCoIP**.
3. In the **Connection Settings (PCoIP)** dialog box, do the following:
   a. Enter the description for the PCoIP connection.
   b. Enter the IP address of the remote host card.
   c. From the **Display Resolution** drop-down list, select a display resolution for the PCoIP connection.

      TERA2220 supports a single display with 2560 x 1600 resolution or two displays with 1920 x 1080 resolution. TERA2240 supports two displays with 2560 x 1600 resolution, four displays with 1920 x 1080 resolution, or a single display with 3840 x 2160 resolution.
   d. Select either the **Window mode** or **Full screen** to set the initial view of the session.
   e. If you want to automatically connect to the session after you restart the thin client, select the **Auto-connect on start-up** check box.
   f. Select the **Re-connect after disconnect** check box if you want to automatically reconnect to a session after the session is disconnected. If you select this option, enter the wait interval in the **Delay before re-connecting** box. The default is 20 seconds.
4. Click **OK** to save your settings.

   NOTE: You can still hear the sound after you mute audio in the Remote Workstation Card session. The behavior is related to Teradici and not ThinOS.

   For information about the Teradici host cards, see the Host Card documentation at www.teradici.com.

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 9.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 VMware View, Amazon WorkSpaces, and VPN. The server certificate common name is verified all the time when setting up SSL connections for VMware View, Amazon WorkSpaces, 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**.

Bloomberg keyboard support

ThinOS 9.1.2101 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 9.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:
   - 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 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 example, enter **`0x11889525`** in one row and **`0x11889535`** in the other.
   - Split 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 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 9.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 VMware Horizon Blast sessions

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 9.x policy settings on Wyse Management Suite.
2. In the Advanced tab, click **Broker Settings**, and expand **VMware 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 Include **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 Include **Vid/Pid USB Device Redirection** field.
   - Split 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 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 Bloomberg keyboard can be redirected into the Blast session.
3. Click **Save & Publish**.

Mapping Bloomberg keyboard in VMware Blast sessions

You can connect the keyboard using either single or dual USB cables. No setting changes or redirection is required. All the function keys work without any redirection.

If you have set force redirection, see Remove Bloomberg keyboard force redirection settings for VMware Blast.

Remove Bloomberg keyboard force redirection settings for VMware Blast

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 9.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.

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.

7

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:

- Skype for Business
- Cisco Jabber
- Cisco Webex Teams
- Cisco Webex Meetings—Only Citrix VDI is supported.
- Microsoft Teams.
- Zoom

NOTE: When using Citrix Unified Communications on ThinOS, Dell Technologies recommends that you 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.

Citrix Unified Communications support on Wyse 3040 Thin Clients

Following features are not supported on Wyse 3040 Thin Clients due to client resource limitations:

- Video call or meeting
- Share screen

To avoid audio choppy issues during the audio call or meeting, users are recommended not to perform the following tasks:

- Move the application window frequently or quickly.
- Scroll down the Microsoft PowerPoint slide, Word document, Excel sheet, or a website page frequently or quickly.
- Play a video in an ICA session frequently.

Citrix HDX RealTime Optimization Pack for Skype for Business

The Citrix HDX RealTime Optimization pack enables you to make high-definition audio and video calls using the Skype for Business application. For more information about HDX RealTime Optimization Pack, see the *Citrix documentation* at docs.citrix.com.

The Citrix HDX RealTime Optimization pack consists of the following two components:

- HDX RealTime Media Engine and Citrix Workspace app that are integrated as a single component on the client-side (Citrix package)
- HDX RealTime Connector as the server-side component

The HDX RealTime Media Engine and Citrix Workspace app are combined to constitute a single component that runs on the thin client. The HDX RealTime connector is the server-side component that runs on the Citrix Virtual Desktops virtual desktops and Citrix Virtual Apps servers. The HDX RealTime connecter that runs on the Citrix server handles the authentication and the media processing is achieved on the thin client.

NOTE: In every ThinOS release, the Citrix package version may be updated to newer versions.

Table 30. Supported environment

Component	Supported platform/supported versions
Endpoints (Thin clients)	• Wyse 5470 All-in-One Thin Client • Wyse 5470 Thin Client • Wyse 5070 Thin Client • Wyse 3040 Thin Client
Citrix environment	• Citrix Virtual Apps and Desktops 7 1811 and later • Citrix Virtual Apps and Desktops (formerly XenDesktop) 5.6, 6.5, 7.x • Citrix Virtual Apps (formerly XenApp) 6.5, 7.x
Skype for Business client	• Skype for Business 2016 • Skype for Business 2015 • Lync 2013 • Lync 2010
Server backend	• Skype for Business Server 2019 • Skype for Business Server 2015 • Skype for Business Online—Microsoft Office 365 hosted Skype for Business Server • Lync 2013 Server
Client component at the endpoint	Citrix package for RTME

Install the Citrix Workspace app package on ThinOS

You must install the Citrix Workspace app package to use Skype for Business application on ThinOS. To install the Citrix Workspace app package using Wyse Management Suite, see Upload and push ThinOS 9.x application packages. Dell Technologies recommends that you install the Citrix Workspace app package first, and then install the Citrix Unified Communications package.

Set up the Skype for Business application

About this task

This section describes how to install and use Skype for Business (SFB) on a Citrix desktop.

NOTE: Ensure that the thin client does not have USB redirection for video and audio devices to have the RealTime Media Engine working correctly on your thin client.

Steps

1. Upgrade the ThinOS firmware and install the Citrix package on the thin client using Wyse Management Suite. For more information about firmware upgrade and package installation, see Firmware upgrade and Upload and publish ThinOS 9.x application packages.
2. Go to www.citrix.com and download the appropriate version of the Citrix RealTime Optimization Pack that contains the Citrix HDX RealTime Connector.
3. Install the Citrix HDX RealTime Connector on the Citrix Virtual Desktops or Citrix Virtual Apps servers.

   NOTE: If you are running an earlier 2.x version, you must upgrade the connector to the latest version.

4. Log in to your Citrix desktop and start the Skype for Business application.

Using the Skype for Business application

The following are the salient features:

- Supports Native Skype For Business client menus and operations
- Supports more call features, such as call delegation, and response group
- Supports video codec H.264-UC and audio codec SILK
- Supports Call Admission Control
- Supports DSCP/QoS Configuration
- Supports Bandwidth Policy Control
- Ability to turn off version mismatch warnings for acceptable combinations of RealTime Connector and RealTime Media Engine
- Better initialization to eliminate DNS confusions

For more information about Skype for Business in VDI environments, see the *Microsoft documentation* at docs.microsoft.com.

Use the Skype for Business application to perform the following tasks:

- Start an audio or video call.
  - Select a user to call.
  - Call from the IM window.
  - Type a name or number to call.
- Answer the call.
  - Answer an audio call.
  - Answer a video call.
  - Use the headset button to answer the call.
- Transfer call, mute, or hold call.
- Control the video—Pause, end, or Picture-in-Picture (PiP).
- Set the volume levels.
- Use the dial pad.
- Make a conference call.
- Help and Hang up.
- Minimize, maximize, or close the call video window.
- Perform a network health check. Right-click the RTME icon on the taskbar and select **Call Statistics** to view attributes, such as received packets, sent packets, video frame rate, video resolution, audio codec, and video codec.

NOTE: Video call/meeting and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations.

Verify the Skype for Business connection status

About this task

This section describes how to verify the Skype for Business status on your thin client.

Steps

1. Install the correct connector on the Citrix Virtual Desktop or Virtual Apps Server.
2. Install the Citrix package on the ThinOS device.
3. Connect the audio or video devices.

   NOTE: Disable the USB redirection for audio or video devices.

4. Connect to a Citrix desktop and start the Skype for Business application.
5. Check the RTOP (bow-tie) icon in the system tray on the taskbar of the virtual desktop.
6. Open the **About** page from the RTOP icon in the system tray and verify the connection attributes.
   If the remote RealTime Media Engine version matches the `mediaEngine.Net` version, the status is displayed as **Connected**.
7. Verify the **Settings** option from the RealTime connector icon.
8. Verify the audio and video devices from the Skype For Business client menus.
9. Establish the video and audio calls.
10. Answer the calls by either clicking the mouse or using the headset button.
11. Click the RealTime connector icon and verify the call statistics.

For more information about verifying your installation and the collecting troubleshooting information, see the *Citrix documentation* at docs.citrix.com.

Citrix RTME call statistics

Table 31. Citrix RTME call statistics

Platform name	RTME version	Call statistics*			Camera
		Video resolution	Video codec	Video frame rate	
Wyse 5470 All-in-One Thin Client	2.9	960 x 540	H.264-UC (SW)	30 fps	Onboard camera
		1280 x 720	H.264-UC (CAM)	30 fps	Logitech C930e
Wyse 5470 Thin Client	2.9	960 x 540	H.264-UC (SW)	30 fps	Onboard camera
		1280 x 720	H.264-UC (CAM)	30 fps	Logitech C930e
Wyse 5070 Thin Client	2.9	1280 x 720	H.264-UC (CAM)	30 fps	Logitech C930e
Wyse 3040 Thin Client	2.9	848 x 480	H.264-UC (CAM)	30 fps	Logitech C930e

*The call statistics data is displayed in the **Call Statistics** window in the **Sent** column.

VMware Horizon Virtualization Pack for Skype for Business

The VMware Horizon Virtualization Pack for Skype for Business enables you to use Skype for Business in a VMware Horizon desktop. Microsoft Skype for Business is a unified communications platform that delivers an optimized user experience for online messaging, audio, and video calling and so on.

ThinOS supports VMware Horizon Virtualization Pack for Skype for Business in a Blast session only. PCoIP and RDP protocols do not support this feature.

NOTE: Video call/meeting and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations

Install the Horizon package on ThinOS

You must install the Horizon package to use Skype for Business application in a VMware desktop on ThinOS. To install the Horizon package using Wyse Management Suite or Admin Policy Tool, see Upload and push ThinOS 9.x application packages.

Setting up the Skype for Business in VMware Blast session

About this task

This section describes how to install and use the Microsoft Skype for Business (SFB) on a VMware Blast desktop.

Steps

1. Log in as horizon administrator, and start the VMware Horizon Agent installation on the virtual desktop.
2. During the VMware Horizon Agent installation, select the **VMware Horizon Virtualization Pack for Skype for Business** option to install the VMware Horizon Virtualization Pack for SFB.

   For Horizon Agent installation information, see the *Setting Up Virtual Desktops in Horizon 7* document at docs.vmware.com.

   The VMware Horizon Virtualization Pack for Skype for Business contains the following components:

- Horizon Media Proxy—This component is installed on the virtual desktop.
- Horizon Media Provider—This component is installed on the thin client.

3. Install the Skype for Business application on the VMware Blast desktop.
4. Update the ThinOS firmware, and install the Horizon Package on the ThinOS client.
5. On ThinOS, log in to the VMware Blast desktop, and sign in to Skype for Business.

Next steps

To verify if the VMware Horizon Virtualization Pack for Skype for Business is installed on the deployed virtual machines, check if the following registry keys exist:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider - GUID (REG_SZ)`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider - GUID (REG_SZ)`

For information about pairing modes for a session, see the *Configuring Skype for Business* document at docs.vmware.com.

For information about configuring Skype for Business group policy settings, see the *VMware Virtualization Pack for Skype for Business Policy Settings* document at docs.vmware.com.

For information about the performance data statistics, see the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.

NOTE: To check the Skype for Business call statistics, right-click the **virtualization pack** icon on the lower-right of the virtual desktop, and click **Call statistics**.

Optimized mode and Fallback mode

In **Optimized mode**, the Skype for Business delivers an optimal performance. In **Fallback mode**, the Skype For Business calls are not optimized. On the lower right of the virtual desktop, the tooltip of the Virtualization Pack icon indicates the VMware Horizon Virtualization Pack for Skype for Business mode.

The following screenshot displays the Virtualization pack for Skype for Business in Optimized mode:

Figure 35. Optimized mode

If the Optimized mode icon is not displayed, the Virtualization Pack is running in Fallback mode. This is because of the version mismatch between the Horizon Client on the thin client and the Horizon Agent on virtual desktop.

For information about compatibility of Horizon Virtualization Pack for SFB components, see the *Horizon Client 4.8 or later and Agent 7.5 or later Virtualization Pack for Skype for Business is not compatible with older Client and Agent releases* article at kb.vmware.com.

Change Optimized mode to Fallback mode

About this task

To change the Optimized mode to Fallback mode, or to disable the Virtualization pack for Skype for Business on the Horizon desktop, do the following:

Steps

1. On the VMware Horizon desktop, open the Windows Registry Editor.

2. Rename the registry keys based on the following deployment scenarios:

Table 32. Registry keys

Deployment scenario	Registry key
View Desktops (64-bit) with Skype for Business (64-bit)	Rename `HKLM/Software/Microsoft/Office/Lync/VdiMediaProvider` to `HKLM/Software/Microsoft/Office/Lync/VdiMediaProviderDisabled`.
View Desktops (64-bit) with Skype for Business (32-bit)	Rename `HKLM/Software/Wow6432Node/Microsoft/Office/Lync/VdiMediaProvider` to `HKLM/Software/Wow6432Node/Microsoft/Office/Lync/VdiMediaProviderDisabled`.
View Desktops (32-bit) with Skype for Business (32-bit)	Rename `HKLM/Software/Microsoft/Office/Lync/VdiMediaProvider` to `HKLM/Software/Microsoft/Office/Lync/VdiMediaProviderDisabled`.

3. Close the Windows Registry Editor.
4. Restart Skype for Business.
   Skype for Business is set to Fallback mode, and Real-Time Audio-Video (RTAV) is used for SFB calls.

Cisco Jabber Softphone for VDI

Cisco Jabber Softphone for VDI (JVDI) is the Unified Communications solution 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 33. Supported environment

Component	Supported platforms/supported versions
Thin client	• Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • Wyse 5070 Thin Client • Wyse 3040 Thin Client
Connection broker for the hosted virtual desktops	• Citrix Virtual Apps and Desktops • VMware Horizon published desktop
Cisco Jabber application on the hosted virtual desktop	Refer the Release Notes for the supported version
Cisco JVDI agent on the hosted virtual desktop	Refer the Release Notes for the supported version
Cisco JVDI client on the thin client	Refer the Release Notes for the supported Cisco Jabber package

Install the JVDI package on ThinOS

About this task

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 9.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 VMware desktop.

Steps

1. Go to www.cisco.com, 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 www.cisco.com.
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 either specify the domain name and server IP on the **General** tab in **Network Setup**, or 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* at www.cisco.com.

For information about Cisco Jabber-related issues, see the *Release notes for Cisco Jabber Softphone for VDI* document at www.cisco.com.

For information about accessories for headsets, speakers, and cameras, see the *Unified Communications Endpoint and Client Accessories* article at www.cisco.com.

Limitation—Following features are not supported on Wyse 3040 Thin Clients due to client resource limitations:

- Video call or meeting
- Screen sharing

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 www.cisco.com.

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 34. Supported environment

Component	Supported platforms/supported versions
Thin Client	• Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • Wyse 5070 Thin Client • Wyse 3040 Thin Client
Connection Broker agent for the hosted virtual desktops	• Citrix Virtual Desktops • VMware Horizon published desktop
Cisco Webex Teams Virtual Desktop app on the hosted virtual desktop	Refer the Release Notes for the supported version.
Cisco Webex Teams Plugin on the thin client	Refer the Release Notes for the supported Webex VDI package.

Ensure that you have referred the Compatibility between the Webex Teams and the Thin Client Plugin table to configure Webex Teams/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 Webex Teams package using Wyse Management Suite or Admin Policy Tool, see Upload and push ThinOS 9.x application packages.

Setting up the Cisco Webex Teams for VDI

This section describes how to install and use the Cisco Webex Teams for VDI on a virtual desktop.

Steps

1. Go to www.webex.com/downloads/teams-vdi.html and download the supported Webex Teams HVD installer.
   To know the supported version, refer the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.
2. On the virtual desktop, install the Cisco Webex Teams 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
```

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.

- **VMware Horizon package**—Install this package if you want to use the Cisco Webex Teams application with VMware Horizon server published desktops.
- **Cisco Webex 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 Teams application using your credentials.

Cisco Webex Teams optimization on Citrix Workspace app feature matrix

Table 35. 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
Meetings	Supported
Annotation	Supported

NOTE: Video call/meeting and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations.

Cisco Webex Teams optimization on VMware feature matrix

Table 36. Cisco Webex Teams optimization on VMware 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. On Wyse 5070 Thin Client, the video screen stays on ThinOS desktop screen if you switch to desktop during a video call.
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

NOTE: Video call/meeting and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations.

Verify the Cisco Webex Teams connection status

This section describes how to verify if Cisco Webex Teams runs in Optimized mode status on your thin client. In Optimized mode, the Webex Teams application delivers an optimal performance.

Prerequisites

- Ensure that you have installed the supported version of the Cisco Webex Teams application on the remote desktop.
- Ensure that you have installed the correct Cisco Webex Teams package on the ThinOS device.

Steps

1. Connect to a virtual desktop session on ThinOS.
2. Start the Cisco Webex Teams 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.

Table 37. Supported environment

Component	Supported environment
Thin Client	• Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • Wyse 5070 Thin Client • Wyse 3040 Thin Client
Connection Broker agent for the hosted virtual desktops	• Citrix Virtual Desktops
Cisco Webex Meetings Virtual Desktop app on the hosted virtual desktop	Refer the Release Notes for the supported version.
Cisco Webex Meeting Plugin on the thin client	Refer the Release Notes for the supported package.

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 **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:
    - For a 32-bit operating system—`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Spark Native`
    - For a 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 package on ThinOS

You must install the Cisco WebEx Meetings 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 9.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 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 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 38. Cisco Webex Meetings optimization feature matrix

Scenarios	ThinOS 9.1.4234
Join meeting	Supported
Audio call	Supported
Video call	Supported
Start video	Supported
Stop video	Supported
Switch camera during meetings	Supported
Adjust volume	Supported

Table 38. Cisco Webex Meetings optimization feature matrix (continued)

Scenarios	ThinOS 9.1.4234
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
Participant	Supported
Close Participant	Supported

NOTE: Video call/meeting and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations.

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.
- On Wyse 5470 and Wyse 5470 All-in-One thin clients, during a call there is occasional echo.

Zoom Meetings for VDI

Zoom Meetings for VDI is the Unified Communications solution, 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.

ThinOS 9.1.4234 supports HTTP Proxy for anonymous authentication. Configure HTTP Proxy server and Proxy Application list as **ZOOM** to make the Zoom optimization function for Citrix work through the proxy server.

For information about limitations, see the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.

NOTE: ThinOS supports the **Virtual Background** (with green screen) feature that enables you to display an image of your choice as your background during Zoom Meetings. Alternatively, you can blur the background as well. For more information, see support.zoom.us. You must have a Zoom account to enable this feature since the feature is available only after you log in to your account.

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.

Table 39. Supported environment

Component	Supported platforms/supported versions
Thin Client	• Wyse 5470 Thin Client • Wyse 5470 All-in-One Thin Client • Wyse 5070 Thin Client • Wyse 3040 Thin Client
Connection Broker agent for the hosted virtual desktops	• Citrix Virtual Desktops • VMware Horizon published desktop
Zoom VDI Client on the hosted virtual desktop	Refer the Release Notes for the supported version.
Zoom Media Plugin on the thin client	Refer 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 9.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 support.zoom.us/hc/en-us/articles/360060317152, and download the supported VDI client version.
   To know the supported VDI client version, refer the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.
   The `ZoomInstallerVDI.msi` is downloaded to your system.
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_Citrix package**
   - If you want to use Zoom with VMware Horizon published desktops, install the following packages:
     - **VMware Horizon package**
     - **Zoom_VMware package**
4. Log in to the virtual desktop, and sign in to the Zoom application using your credentials.

Zoom optimization feature matrix

Table 40. 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
Join a meeting	Supported
Schedule a meeting	Supported

Table 40. Zoom optimization feature matrix (continued)

Scenario	ThinOS
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

NOTE: Video call/meeting and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations.

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 Citrix Workspace app

ThinOS supports audio optimization for Microsoft Teams using Citrix Workspace app 2101.

ThinOS supports HTTP Proxy for anonymous authentication. Configure HTTP Proxy server as MTOP to make the Microsoft Teams Optimization function for Citrix work through the proxy server.

To enable the Teams optimization feature for Citrix, you must meet the following requirements:

- Install the Microsoft Teams on your VDI desktop. For more information about the Microsoft Teams installation, see the *Optimization for Microsoft Teams* article at docs.citrix.com.
- Review the system requirements of Citrix Virtual Desktops and VDA. For more information about the system requirements, see the *Optimization for Microsoft Teams* article at docs.citrix.com.
- Enable the Microsoft Teams redirection policy is enabled in Citrix Studio. For more information about how to enable the Microsoft Teams redirection, see the *Multimedia policy settings* article at docs.citrix.com.

On the ThinOS client side, you must download the Citrix package from Dell.com/support and install the package using Admin Policy Tool or Wyse Management Suite. For information about how to install the ThinOS application packages, see the Upload and install ThinOS 9.x application packages using Admin Policy Tool or Upload and install ThinOS 9.x application packages using Wyse Management Suite.

To verify if the Microsoft Teams application works in the optimized mode, click **About** > **Version** to view the Citrix HDX Optimized legend. For more information about how to verify the Microsoft Teams audio optimization, see the *Optimization for Microsoft Teams* article at docs.citrix.com.

Table 41. Microsoft Teams optimization feature matrix

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

Table 41. Microsoft Teams optimization feature matrix (continued)

Scenario	ThinOS
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—PowerPoint	Supported
Chat	Supported
Audio or video call in VDI server desktop	Supported
Audio or video call in published Microsoft Teams application	Supported
Devices—Plug in or disconnect the headset	Limited support—Do not hot plug headset or the camera during a meeting, or a call. Do not switch the camera during a meeting. It causes the audio and video reception to be inconsistent. Restart Microsoft Teams to resolve this issue. This is also Citrix binary issue.
Devices—Switch headset	Limited support—If you install JVDI package in ThinOS, the switched headset does not work. Dell Technologies recommends to not install JVDI package if you are using Microsoft Teams.
Devices—Plug in or disconnect the camera	Limited support—Do not hot plug headset or the camera during a meeting, or a call. Do not switch the camera during a meeting. It causes the audio and video reception to be inconsistent. Restart Microsoft Teams to resolve this issue. This is also Citrix binary issue.
Devices—Switch camera	Not supported—This is a known Citrix issue.
Headset buttons—Answer/Mute/End Call	Limited support—The Answer/End call button is not supported. This is a Citrix Workspace app limitation.

Limitations

- Video call and share screen features are not supported on Wyse 3040 Thin Clients due to client resource limitations.
- Video call and share screen features are recommended on Wyse 5070 Thin Clients, 5470 Thin Clients, and Wyse 5470 All-in-One Thin Clients with known issues.
  - The audio gets distorted occasionally on a thin client with dual core CPU.
- Other known issues for CWA Teams Optimization
  - Depending on your network bandwidth latency, the audio quality may fluctuate. To avoid this issue, ensure that your network bandwidth is adequate for audio or video call. Citrix recommends 200 kbps or higher network speed for a single client.
  - Session termination or abrupt disconnect may result in unexpected HdxRtcEngine.exe processing exits. This issue is a known Citrix Workspace App limitation [RFLNX-5885].
  - Audio is still played through the first headset when you switch to the second headset during the call. This issue is observed when you have installed the JVDI package on the thin client. Workaround is that if you are using Microsoft Teams (or Zoom), do not install the Cisco JVDI package. This issue is due to Cisco limitation.
  - When using a headset, you cannot answer or end the call through headset buttons. This issue is due to a limitation of Microsoft Teams.

Microsoft Teams Optimization from VMware Horizon

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

Enable the optimization by using a Group Policy Editor

Steps

1. Open the Group Policy Editor.
2. Go to **Computer Configuration** > **Administrative Templates** > **VMware View Agent Configuration** > **VMware HTML5 Features** > **VMware WebRTC Redirection Features**.

   NOTE: For steps on how to download and apply the VMware Blast ADMX template file (vdm_agent.admx), see *VMware Horizon Documentation* at docs.vmware.com.

3. Double-click **Enable Media Optimization for Microsoft Teams**.
4. Ensure that **Enabled** is selected, and click **OK**.
5. Log off from the the Horizon desktop.

Microsoft Teams optimization feature matrix

Table 42. Microsoft Teams optimization feature matrix

Scenario	ThinOS
Long audio call	Supported
Call—Make an audio call	Supported
Call—Answer an audio call	Supported
Call—Make a video call	Supported
Call—Answer a video call	Supported
Call—Turn the camera on or off	Supported
Call—Enter or exit full screen	Supported
Call—Hold or resume a call	Supported
Call—End call	Supported
Call—Mute or unmute audio	Supported
Call—Transfer	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

Table 42. Microsoft Teams optimization feature matrix (continued)

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

Microsoft Teams optimization limitations and known issues

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

8

Configuring third-party authentication settings

ThinOS supports the following third-party authentication types:

- **Imprivata**—ThinOS supports Imprivata on Citrix, VMware, 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
  - VMware Horizon - Desktops
  - VMware 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 **OK** 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)
     - VMware Horizon Desktops
     - VMware 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 supports Imprivata on Citrix, VMware, and Microsoft VDI solutions in both Imprivata ProveID Embedded and ProveID Webapi modes.

- For ProveID Webapi mode, select VDI type from **Automate access to** setting in Admin Policy Tool.
- For ProveID Embedded mode, the VDI selection is controlled by Imprivata OneSign policy.

NOTE: The VMware Horizon Client Native PCoIP is used instead of Teradici PCoIP when you log in to the VMware Horizon View broker using the Imprivata PIE mode.

OMNIKEY readers

The OMNIKEY readers are presented and recognized as smart cards in the PIE mode when the **Treat smart card authentications as proximity card authentications** option is enabled in Computer Policy. If you want to use OMNIKEY readers as proximity card readers, disable the **Treat smart card authentications as proximity card authentications** option in Computer Policy.

For PIW mode, the OMNIKEY readers are always presented and recognized as proximity card readers.

Configure the VDI settings on OneSign server

To use Citrix, VMware, 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** check box 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 the general configuration object, do the following:
   a. On the Imprivata server, click **Computer policy**, and then click **General** tab.
   b. Select the check box to enable users to shut down and restart the device from the lock screen.
      - **Shutdown Allow**
        - Select the check box to enable the feature. If enabled, the **shutdown** and **restart** icons are displayed in the ThinOS login and locked windows.
        - Clear the check box to disable the feature. If disabled, the **shutdown** and **restart** icons are not available.
      - **FailedOneSignAuth Allow**—Click either **Yes** or **No**. If you are a non-OneSign user, click **No** to log in to the broker.
      - **Display name format**— Use this option to set different formats for the account name that is displayed in pop-up notifications.
2. To configure the walkway configuration object, do the following:
   a. On the Imprivata server, click **Computer policy**, and then click the **Walk Away** tab.
   - **Key mouse inactivity enabled and behavior**—Use this option to set the action when the keyboard and mouse are left idle or inactive. The **In addition to keyboard and mouse inactivity** check box is not supported.
   - **Passive proximity cards**—Use this option to enable the proximity card usage.
     - If you want to use a proximity card to lock the thin client, select the **Tap to lock** check box.
     - If you want to lock the thin client and log in as a different user. Select the **Switch users** check box.
   - **Lock warning enabled and type**—Use this option to enable or disable warning messages. The following three types are supported:
     - **None**—No warning messages are displayed.
     - **Notification balloon**—ThinOS displays a notification window.
     - **Screensaver**—Hide the display contents before the thin client locks.
   - **Warning message**—Use this option to customize your warning messages
   - **Lock Screen type**—Use this option to set the lock screen type. Only obscure type is supported.
   - **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~z
     - A~Z
     - 0~9
     - Modifier +, %, ^ (Shift, Alt, and Control)
   - **Suspend action**—The server configuration controls this feature on ThinOS.
3. To configure the Self-Service Password Reset (SSPR) configuration object, select the appropriate options on the screen.

The SSPR configuration object controls the Self-Service Password Reset behavior for a user. The enabled attribute specifies whether the user is allowed to reset their password as part of emergency access. The mandatory attribute specifies whether the user must reset their password as part of emergency access.

4. To configure the RFIDeas configuration object, select the appropriate options on the screen.

   The RFIDeas configuration object controls the behavior of the RFIDeas readers.

5. To configure the custom background configuration object, do the following:
   a. On the Imprivata server, click **Computer policy**.
   b. Click the **Customization** tab and upload a custom background file.
6. To configure the cobranding configuration object, do the following:
   a. On the Imprivata server, click **Computer policy**.
   b. Click the **Customization** tab and upload a logo image file.

      The logo image impacts all the dialog boxes in ThinOS with raw logo.
7. To modify the text that is displayed in the sign-on UI and lock window, configure the SSPR customization configuration object.
8. To configure the password self-services force enrollment feature, select the check box. This enables you to reset the primary authentication password.

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.

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, VMware 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 at www.imprivata.com.

Table 43. Supported environment

Component	Supported environment
Endpoints (Thin Clients)	• Wyse 5470 All-in-One Thin Client • Wyse 5470 Thin Client • Wyse 5070 Thin Client • Wyse 3040 Thin Client
VDI environment	• Citrix Desktop • Citrix XenApp • Microsoft Remote Desktop Services session based and virtual desktop • Microsoft Remote Desktop Services Remote PC • VMware Horizon - Desktops
OneSign server (tested)	7.1.005.42
PIE Agent on the thin client	7.1.005.0039
Authentication methods	• Network password • Proximity card • Security questions

Table 43. Supported environment (continued)

Component	Supported environment
	• PIN (as a secondary factor) • Fingerprint biometrics

Table 44. 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
	Citrix Virtual Applications	Supported	Supported
	Virtual Kiosk Citrix for Virtual Desktops for Desktops	Supported	Supported
	Virtual Kiosk for Citrix Published Applications	Supported	Supported
VMware Workflows	VMware Horizon Desktops	Supported	Supported
	VMware Published Application Support	Not applicable	Supported
	Virtual Kiosk for VMware Desktops	Not applicable	Supported
	Virtual Kiosk for VMware 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

Table 44. Imprivata ProveID Embedded feature matrix (continued)

Feature	Description	ThinOS PIE	ThinOS PIW
	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 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 www.dell.com/support and download the Imprivata package that contains the PIE agent. For more information, see Download ThinOS 9.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 9.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 9.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.
   - VDI silent mode is added from ThinOS 9.1.2101 onwards. 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, Imprivata OneSign policy controls the VDI selection. RDP is not supported in **VDI silent mode**.
   - The option **Enable VMware Horizon menu bar** is added under **Enable ProveID Embedded Mode** from ThinOS 9.1.3112 onwards.
   - In ThinOS 9.1.4234, **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 9.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 **OK**.

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 at www.imprivata.com.

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 **OK**.
5. Go to **System Setup** > **Remote Connection** > **General Options**.
6. Enter the default sign-on username, password, and domain.
7. Click **OK**.

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 9.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 VMware Horizon Blast session

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 9.x policy settings on Wyse Management Suite.
2. On the **Standard** or **Advanced** tab, expand **Broker Settings**, and click **VMware 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 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. From ThinOS 9.1.3112 onwards, the Identity Automation is independent of the ThinOS firmware and is a separate package.

Configure the Identity Automation

Prerequisites

If you are running ThinOS 9.1.3112, 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.
   From ThinOS 9.1.4234, the **API Key** field is changed to 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 **OK** 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 9.1.3112, 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 9.x application packages.

Identity Automation support matrix

The following are the supported features:

- Authentication to Citrix Virtual Apps and Desktops, VMware 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.
- Supports self-service password reset.
- 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.

Identity Automation feature matrix

Table 45. Identity Automation feature matrix

Identity Automation Feature		ThinOS
Broker Type	Authenticate to Citrix Virtual Apps and Desktops	Supported
	Authenticate to VMware Horizon broker	Not supported
	Authenticate to Microsoft Remote Desktop Services	Not supported
Proxy Card	New card enroll	Supported
	Authenticate with proximity card and password	Supported
	Authenticate with proximity card and PIN	Supported
	Authenticate with password	Supported
SSPR	Seamless change password support	Not supported
	Self-service password reset	Not supported
	Self-service PIN reset	Not supported
Lock/Unlock	Lock/Unlock the terminal by tapping a proximity card	Supported
	Convenient tap-over functionality	Supported

Table 45. Identity Automation feature matrix (continued)

Identity Automation Feature		ThinOS
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

9

Configuring the thin client local settings

You can configure the local settings on the device using the **System Preferences**, **Display**, **Peripherals**, and **Printer Setup** dialog boxes. Depending on 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. 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:

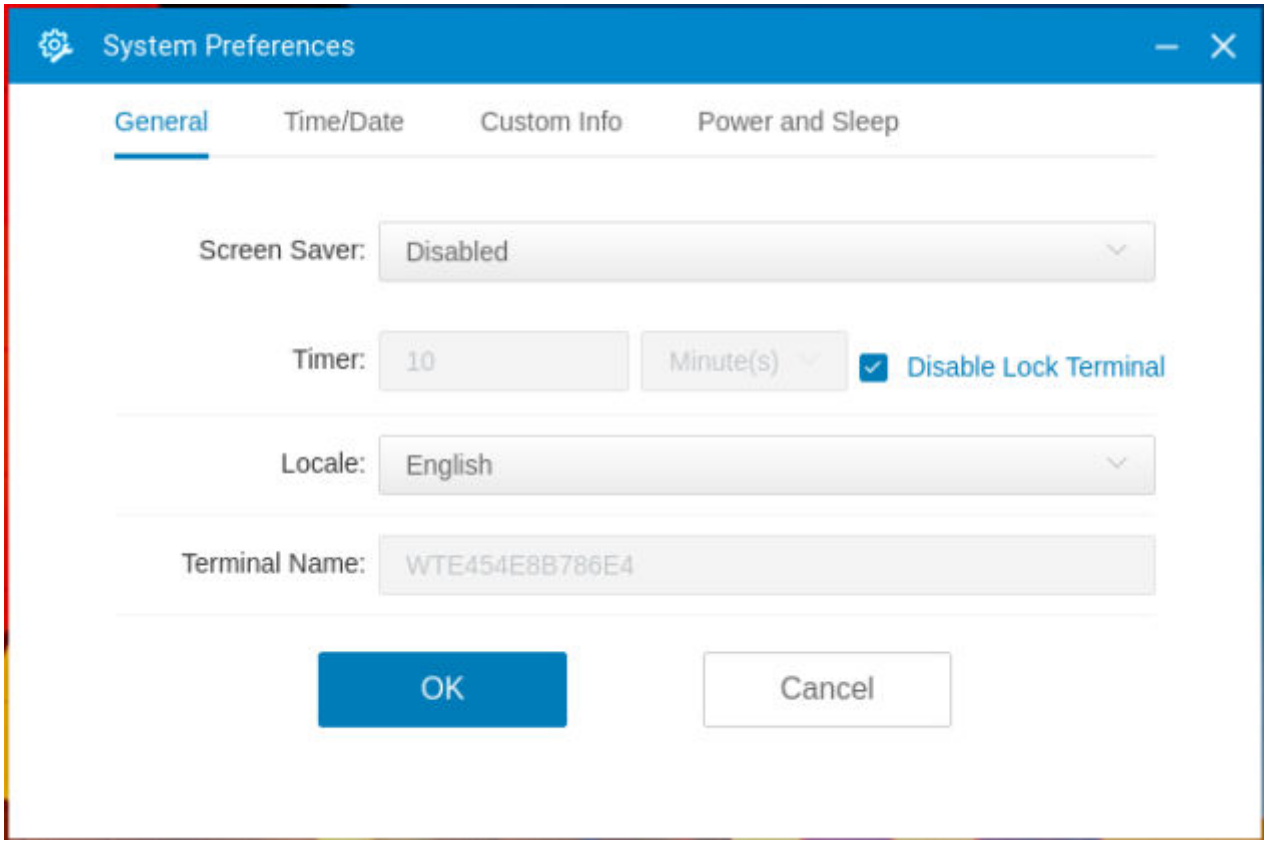


Figure 36. General tab

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 **OK** 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. 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:

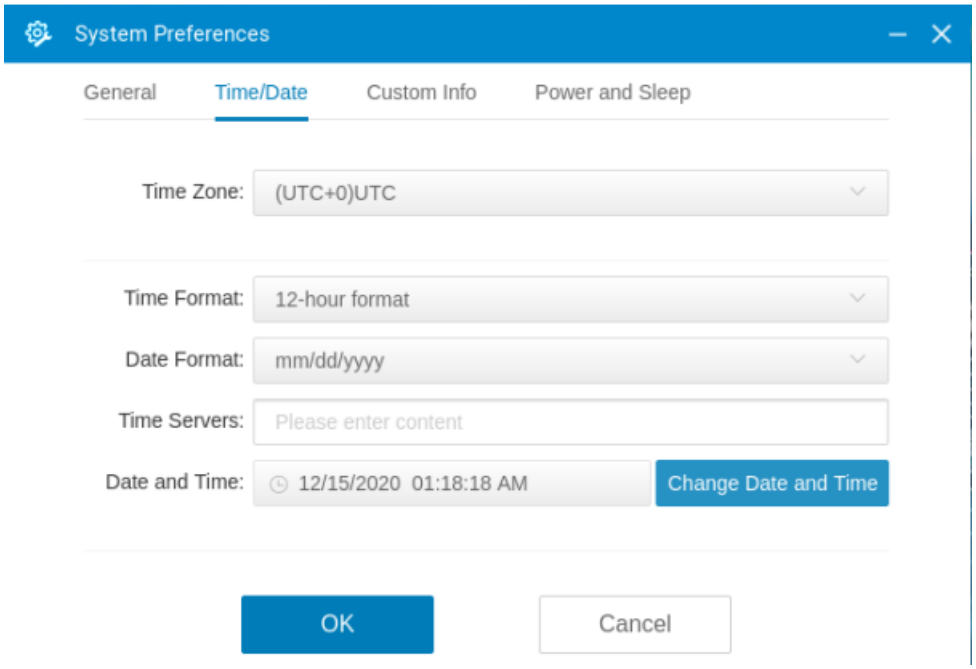


Figure 37. Time and date

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 date and time for secure environments.
3. Click **OK** 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 on your thin client.

Steps

1. From the desktop menu, click **System Setup** > **System Preferences**.
   The **System Preferences** dialog box is displayed.

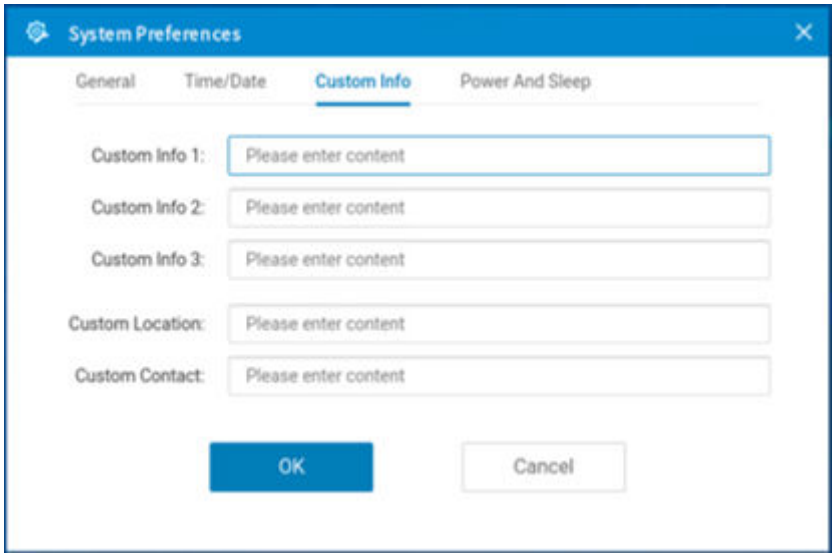


Figure 38. Custom information

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 **OK** to save your settings.
   The custom field information is transferred to the Windows registry. The information is then available to Wyse Management Suite.

Configuring power and sleep mode

About this task

NOTE: **Power And Sleep** tab is not available on Wyse 3040 Thin Client.

This section describes how to configure the power and sleep mode.

Steps

1. From the desktop menu, click **System Setup** > **System Preferences**.
   The **System Preferences** dialog box is displayed.
2. Click the **Power And Sleep** tab.

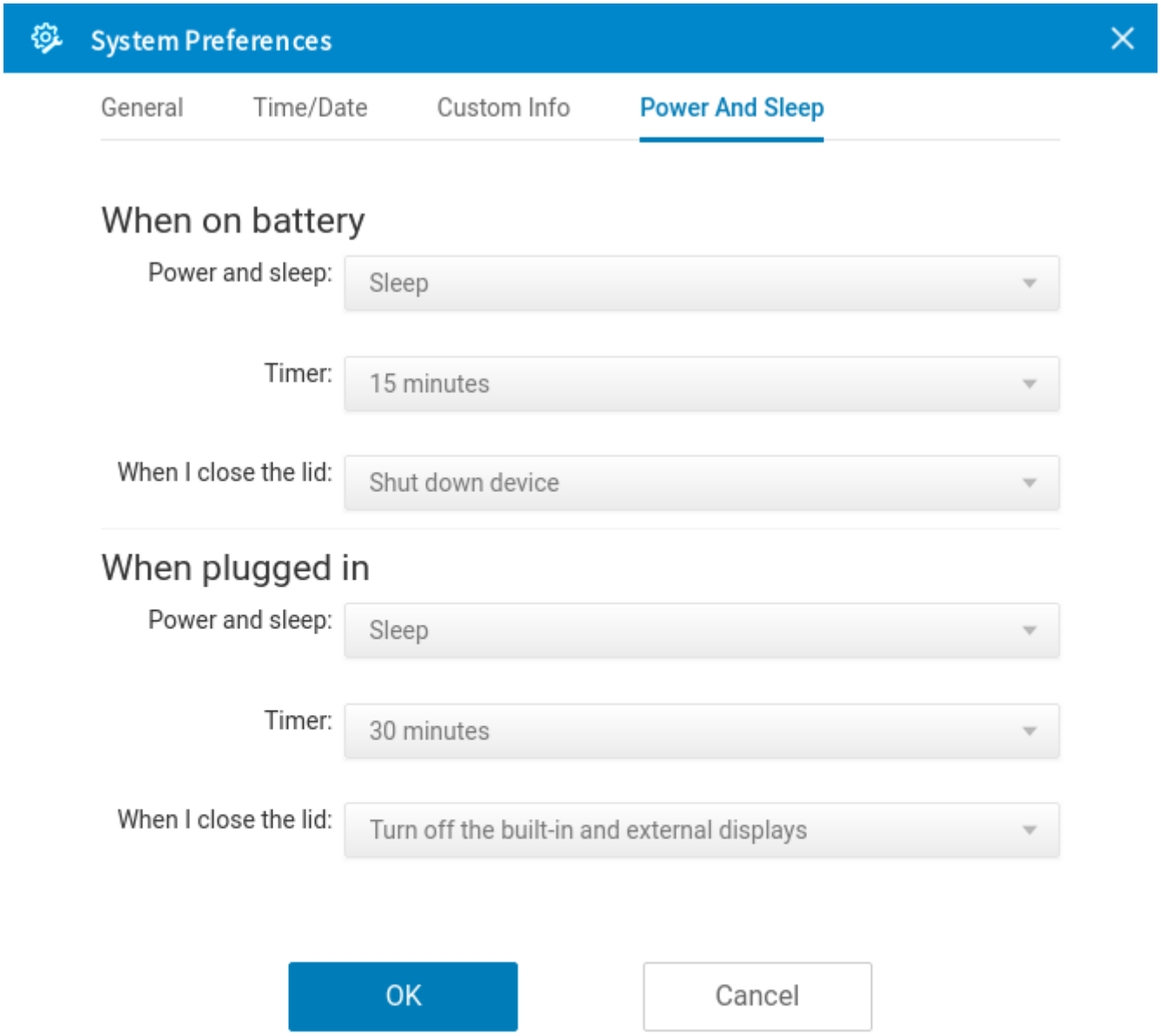


Figure 39. Power And Sleep

3. 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 in Wyse 5470 Thin Client.

4. 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 in Wyse 5470 Thin Client.
5. Click **OK** to save your settings.

Configure the display settings

About this task

This section provides information about how to configure the display settings for the connected displays.

NOTE: On Wyse 5470 Thin Client, the built-in 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 preserved. If you connect the same display again, the device sets the monitor layout (including the disable monitor setting) according to the saved layout.

Steps

1. 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:

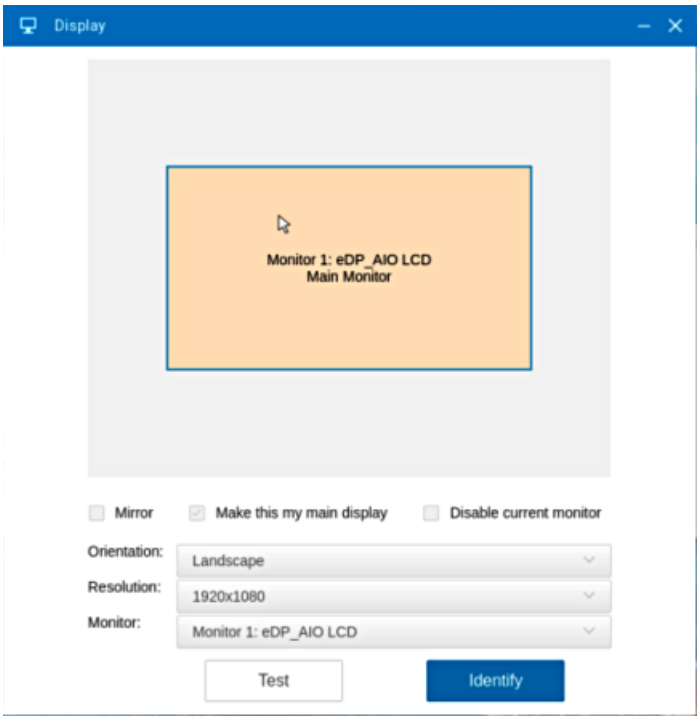


Figure 40. Display

- 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.

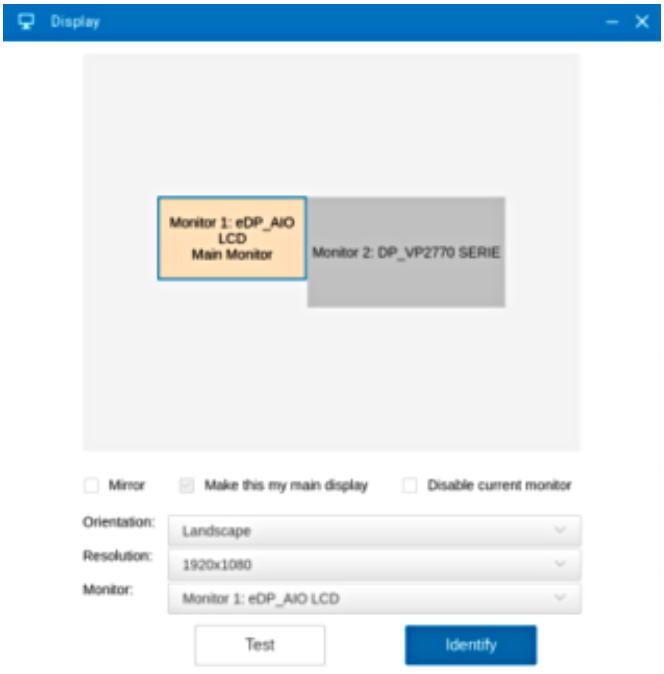


Figure 41. Dual display setup

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 highlighted 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 **OK** to confirm the new settings.
   Use the **Identify** option to know the display order number of the connected displays.

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.

Display limitation on Dell WD19 docking station

On Wyse 5470 Thin Client, ThinOS supports the following monitor connections using a Dell WD19 docking station:

- One Quad HD display at 30 Hz
- Two Full HD displays at 60 Hz

If two displays with resolutions greater than 1920 x 1080 are connected simultaneously, there can be the following behaviors:

- Random resolutions—You must change the resolutions to 1920 x 1080 or lower to make both displays work. Also, disconnect and reconnect the docking station to correct the resolution, if required.
- Second monitor is disabled—You must first enable the monitor in **Display Setup**, and then change the resolutions to 1920 x 1080 or lower to make both displays work. Also, disconnect and reconnect the docking station to correct the resolution, if required.

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 9.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.
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 9.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 Technologies 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.

NOTE: The right-click touch functionality does not work in all VDI sessions due to the limitation on VDI protocols.

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. 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 ThinOS 9.1.2101 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.

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

Function key combinations

The Wyse 5470 Thin Client supports the following Function (Fn) key combinations:

Table 46. Fn key combinations

Key	ThinOS Local	ICA session
Fn + Esc	Fn lock/unlock	Fn lock/unlock
Fn + F1	Mute	Mute
Fn + F2	Volume down	Volume down
Fn + F3	Volume up	Volume up
Fn + F4	Not applicable—session only	Not supported
Fn + F5	Not applicable—session only	Not supported
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

Switch the keyboard layout

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 9.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 9.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.

Configure the mouse settings

About this task

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

Steps

1. 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 **OK** 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. 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.

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

Touchpad gestures

This section is applicable to the Wyse 5470 Thin Client.

The touchpad on the Wyse 5470 Thin Client contains two buttons for the right and left mouse-clicks. The following table lists the supported touchpad gestures on the Wyse 5470 Thin Client:

Table 47. 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. 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.
3. Click **OK** 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.
- **Wyse 5470 Thin Client**—When two monitors that support display audio are connected to Dell WD19 docking station, the **HDMI/DP** audio option disappears if you remove one of the monitors.
- **Wyse 3040 Thin Client**
  - Setting the display resolution higher than 1920x1080 results in a black screen.
  - By default the display audio is disabled. You must enable the display audio in Wyse Management Suite and reboot the client.
  - Display audio does not update real time. If you change the monitor or the DP port, you must reboot the client to update the display audio option.
  - Wyse 3040 Thin Client supports only one display audio. If one DP port is working with display audio, then the other DP port does not work with display audio.

Set default playback or recording devices

Steps

1. Open the Admin Policy Tool on your thin client or go to the ThinOS 9.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 48. Behavior examples when connecting multiple devices

Setup	Behavior
Set one device name in 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 list. **NOTE:** Here the term random name denotes the name of a manufacturer that you can enter. For example, if you give the random name as Jabra, then a connected device that contains the word Jabra in its name can work.	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 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 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. 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 **OK** 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 9.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 9.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.

Steps

1. From the desktop menu, click **System Setup** > **Peripherals**.
   The **Peripherals** dialog box is displayed.
2. Click the **Camera** tab.
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 **OK** to save your settings.

   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 Logitech C930e camera is used.

   For information about supported cameras, see the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.

Configure the Bluetooth settings

About this task

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

Steps

1. 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. However, multimedia is not supported. Other types of Bluetooth devices are not scanned and supported.
   - **Status**—The Bluetooth page has two columns, namely, Status and Paired.

     Table 49. 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 50. 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**—All Bluetooth devices enter into **Page Scan** mode. Different Bluetooth devices enter into the Page Scan mode at different instances such as when a specific button is pressed three times or a specific button is pressed and held until the LED turns blue.
   - **Connect**—Select a particular Bluetooth 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 **OK** to save your settings.

Secure Digital cards

You can plug in a Secure Digital (SD) card into the Wyse 5470 Thin Client. The SD card works as a storage device.

Configure the Jabra Xpress headset settings

ThinOS 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=
```

   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 9.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 51. 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. 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. 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 9.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 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.

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.

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

Steps

1. On the ThinOS client, open **Admin Policy Tool** or go to the ThinOS 9.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 9.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 **Enable HID Fingerprint Reader** from **Advanced** > **Session Settings** > **Global Session Settings** in the **Admin Policy Tool** or **Wyse Management Suite** policy settings, and save the setting changes. Enable the **Enable HID Fingerprint Reader** option again, before you log in to the Citrix server. For the list of supported devices, see the *Dell Wyse ThinOS 9.1.4234 Release Notes* at www.dell.com/support.

   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 better user experience.

   In the ThinOS 9.1.3112 release, HID virtual channel configuration is removed from **Admin Policy Tool/Wyse Management Suite policy settings** > **Session Settings** > **Citrix Session Settings** > **Other Citrix Virtual Channels Settings** > **HID Fingerprint Reader**.

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 8.6 supports the association of PS, PCL5, and PCL4 classes. However, ThinOS 9.0 associations are limited to the PS class only.

Limitations

- 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 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.

Configure the ports settings

About this task

This section describes how to configure the port settings on your thin client:

Steps

1. From the desktop menu, click **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
2. Click the **Ports** tab, and do the following:

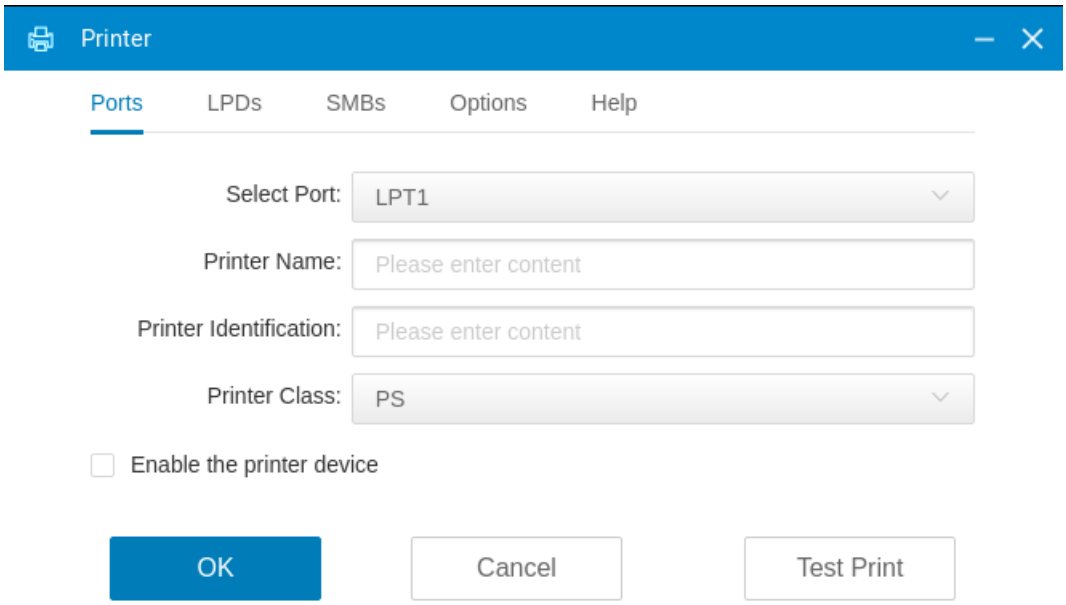


Figure 42. Ports

   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.
   b. **Printer Name**—(Required) Enter the name of the 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.
3. Click **OK** 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. From the desktop menu, click **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
2. Click the **LPDs** tab, and do the following when printing to a non-Windows network printer:

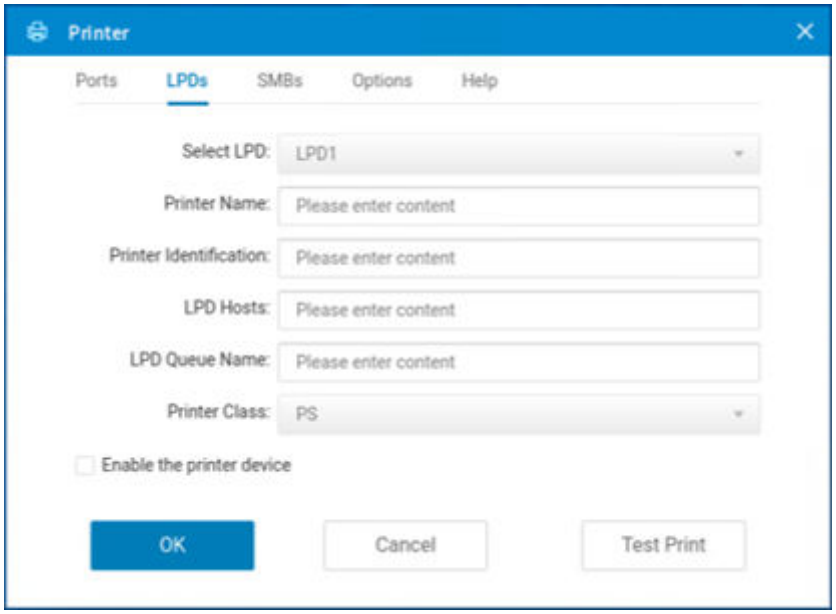


Figure 43. LPD

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.
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 **OK** 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. From the desktop menu, click **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
2. Click the **SMBs** tab, and do the following when printing to a Windows network printer:

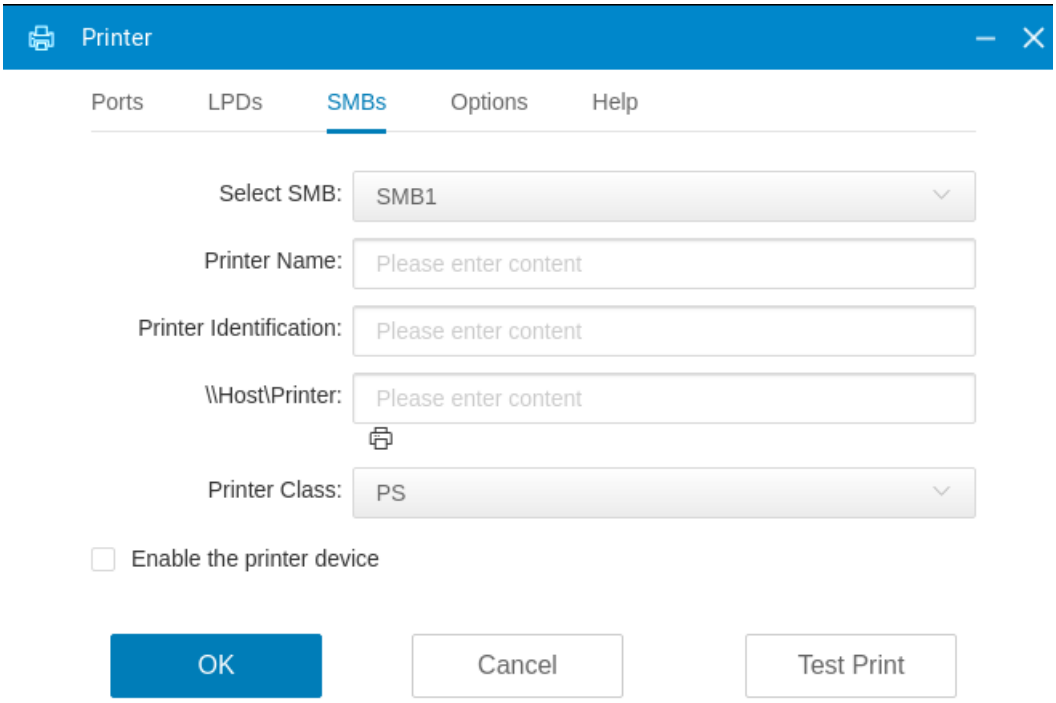


Figure 44. SMB

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, computer 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 which prompts you 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.

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

Using the printer setup options

About this task

This section describes how to configure the printer setup options.

Steps

1. From the desktop menu, click **System Setup** > **Printer**.
   The **Printer Setup** dialog box is displayed.
2. Click the **Options** tab, and select a printer from the **Default Printer** drop-down list.

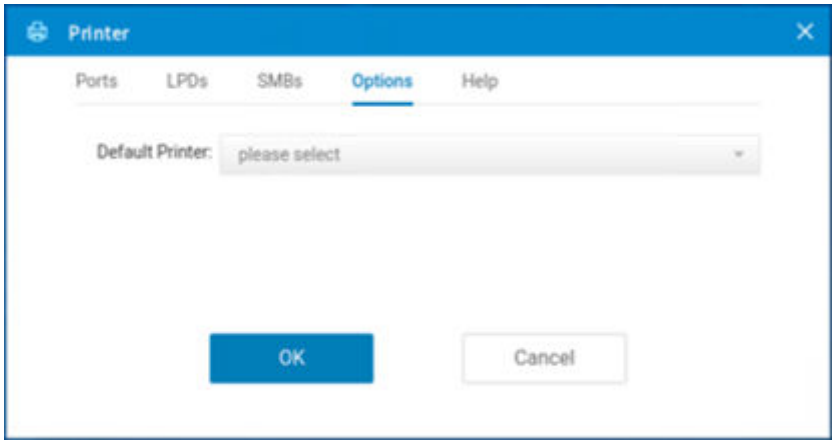


Figure 45. Options

3. Click **OK** 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.

Reset to factory defaults

A high-privileged or stand-alone 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.

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 to factory default** check box to restore your system settings to default factory settings.
3. Click **OK**.

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.

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.

10

Using the 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 the system tools on your thin client.

Steps

1. From the desktop menu, click **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.

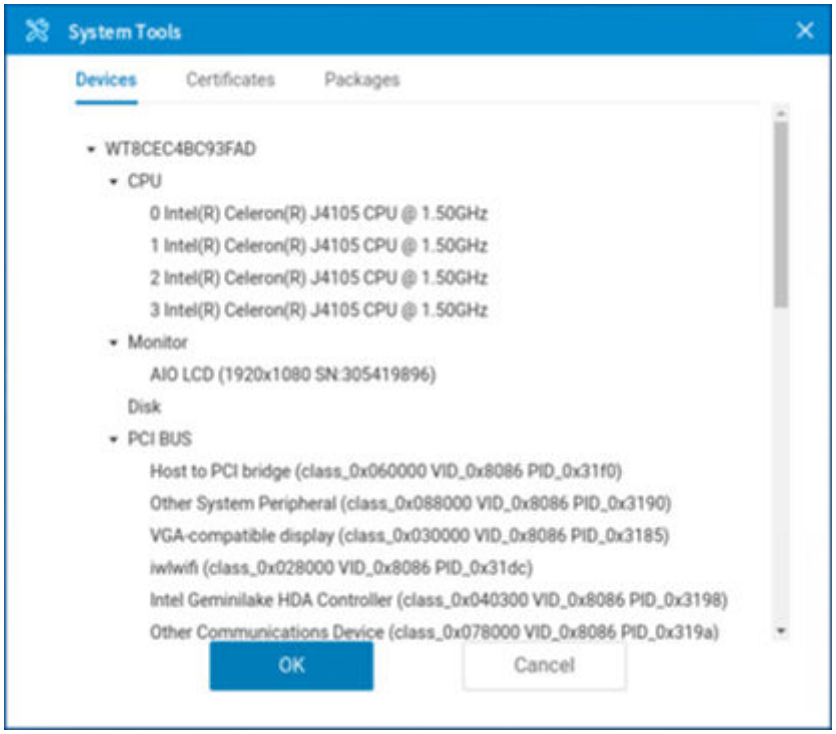


Figure 46. Devices

3. Click the **Certificates** tab to view the list of certificates that are imported to the thin client.

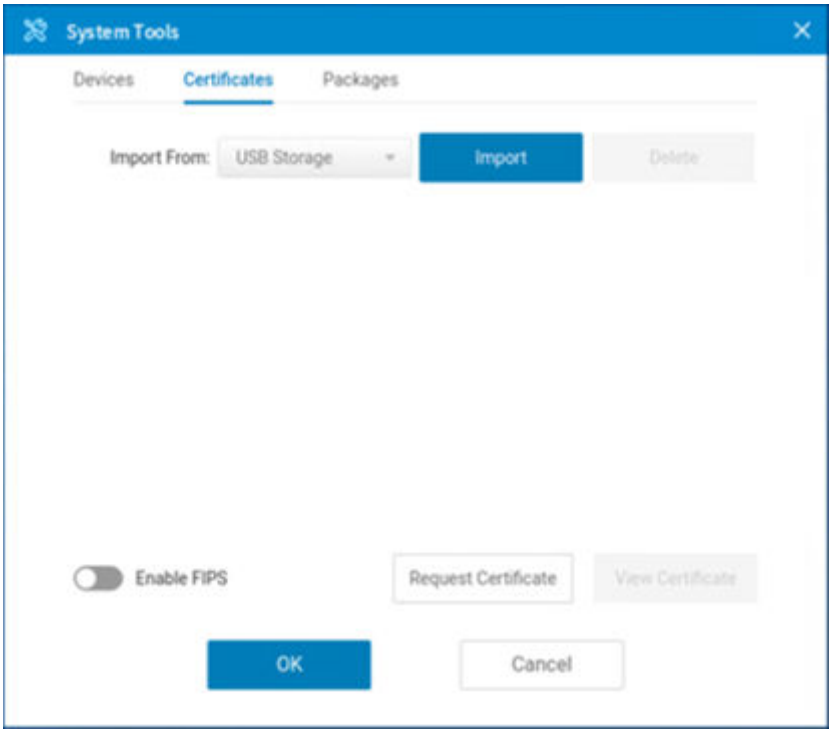


Figure 47. Certificates

- 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.

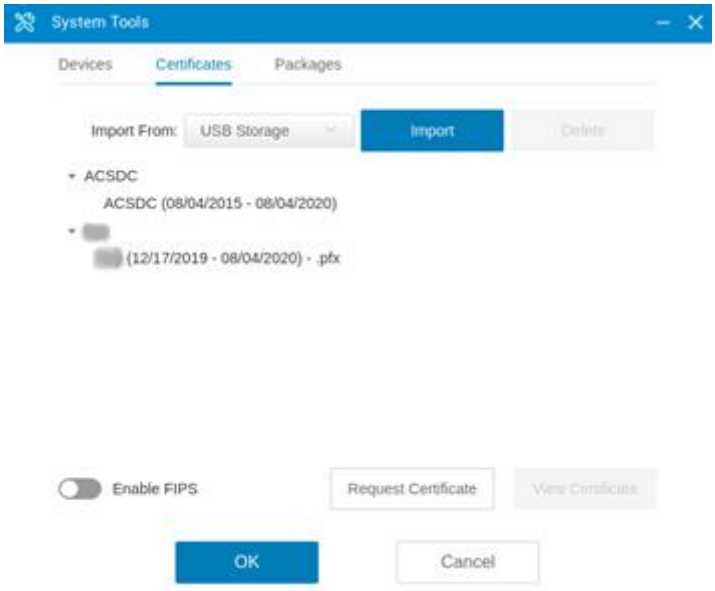


Figure 48. CA information

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 **OK** to save your settings.

Simplified Certificate Enrollment Protocol

Simplified Certificate Enrollment Protocol (SCEP) was used in a closed network where all end-points are trusted. The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner. Within an enterprise domain, it enables network devices that do not run with domain credentials to enroll for certificates from a Certification Authority (CA).

At the end of the transactions that are defined in this protocol, the network device has a private key and associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

ThinOS is treated as a network device. The functionality of ThinOS SCEP includes manual certificate request, automatic certificate request, and automatic renewal of certificate.

Request the 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.

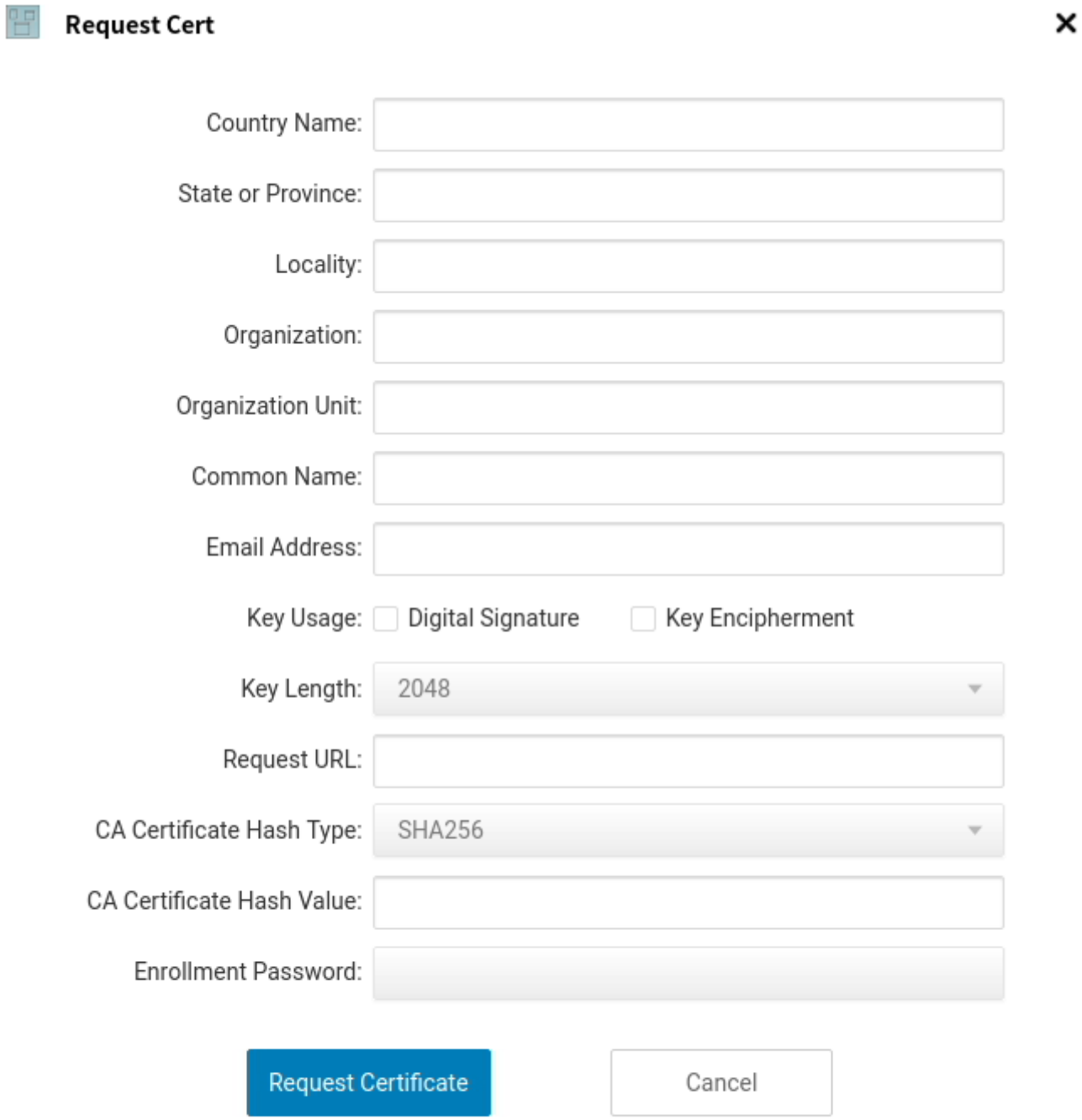


Figure 49. Request Certificate

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.
3. Click **Ok** 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 the 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 9.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. So if you are using an enrollment password that can expire in a short time, the enrollment password must valid at the time when auto renew behavior happens on the client. Dell Technologies recommends using the admin credentials or a fixed enrollment password to auto enroll, and auto renew 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. Specify the country/region name, state, location, and other details.
10. Click **Save & Publish**.

    NOTE: 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.

About Default Certificates

Default certificates are embedded in the ThinOS, on ThinOS 9.1.3112 and the user cannot view the default certificate from**System Settings** > **System Tools** > **Certificates**. The following default certificates are displayed in the **ca-certificates** folder, in an expandable tree structure format:

- Certinomis_-_Root_CA.crt
- Comodo_AAA_Services_root.crt
- GlobalSign_ECC_Root_CA_-_R5.crt
- CA_Disig_Root_R2.crt
- Hongkong_Post_Root_CA_1.crt
- USERTrust_ECC_Certification_Authority.crt
- COMODO_Certification_Authority.crt
- LuxTrust_Global_Root_2.crt
- T-TeleSec_GlobalRoot_Class_2.crt
- Certigna.crt
- EC-ACC.crt
- ePKI_Root_Certification_Authority.crt
- Cybertrust_Global_Root.crt
- SZAFIR_ROOT_CA2.crt
- Amazon_Root_CA_4.crt
- thawte_Primary_Root_CA_-_G2.crt
- DST_Root_CA_X3.crt
- SwissSign_Silver_CA_-_G2.crt
- GeoTrust_Universal_CA_2.crt
- Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt
- DigiCert_High_Assurance_EV_Root_CA.crt

- AffirmTrust_Premium.crt
- VeriSign_Universal_Root_Certification_Authority.crt
- AffirmTrust_Premium_ECC.crt
- VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt
- DigiCert_Global_Root_G2.crt
- OISTE_WISeKey_Global_Root_GB_CA.crt
- Trustis_FPS_Root_CA.crt
- DigiCert_Global_Root_CA.crt
- D-TRUST_Root_Class_3_CA_2_EV_2009.crt
- Chambers_of_Commerce_Root_-_2008.crt
- USERTrust_RSA_Certification_Authority.crt
- IdenTrust_Commercial_Root_CA_1.crt
- Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt
- Entrust_Root_Certification_Authority_-_EC1.crt
- Go_Daddy_Root_Certificate_Authority_-_G2.crt
- TWCA_Global_Root_CA.crt
- CFCA_EV_ROOT.crt
- TrustCor_RootCert_CA-2.crt
- Amazon_Root_CA_3.crt
- Baltimore_CyberTrust_Root.crt
- Actalis_Authentication_Root_CA.crt
- Starfield_Root_Certificate_Authority_-_G2.crt
- Starfield_Class_2_CA.crt
- Go_Daddy_Class_2_CA.crt
- E-Tugra_Certification_Authority.crt
- QuoVadis_Root_CA_1_G3.crt
- XRamp_Global_CA_Root.crt
- SwissSign_Gold_CA_-_G2.crt
- OISTE_WISeKey_Global_Root_GC_CA.crt
- GeoTrust_Primary_Certification_Authority_-_G2.crt
- Starfield_Services_Root_Certificate_Authority_-_G2.crt
- SecureSign_RootCA11.crt
- GeoTrust_Primary_Certification_Authority.crt
- IdenTrust_Public_Sector_Root_CA_1.crt
- Certum_Trusted_Network_CA.crt
- Microsec_e-Szigno_Root_CA_2009.crt
- T-TeleSec_GlobalRoot_Class_3.crt
- GlobalSign_Root_CA_-_R6.crt SSL.
- com_EV_Root_Certification_Authority_RSA_R2.crt
- VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt
- certSIGN_ROOT_CA.crt
- QuoVadis_Root_CA_3_G3.crt
- GeoTrust_Universal_CA.crt
- Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
- thawte_Primary_Root_CA_-_G3.crt
- GlobalSign_ECC_Root_CA_-_R4.crt
- Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt
- Entrust.net_Premium_2048_Secure_Server_CA.crt
- Network_Solutions_Certificate_Authority.crt
- COMODO_RSA_Certification_Authority.crt
- Izenpe.com.crt
- QuoVadis_Root_CA_2.crt
- TrustCor_RootCert_CA-1.crt
- GlobalSign_Root_CA_-_R3.crt
- COMODO_ECC_Certification_Authority.crt
- DigiCert_Assured_ID_Root_G2.crt

- Entrust_Root_Certification_Authority.crt
- QuoVadis_Root_CA_2_G3.crt
- Atos_TrustedRoot_2011.crt
- Staat_der_Nederlanden_Root_CA_-_G3.crt
- Security_Communication_RootCA2.crt
- DigiCert_Global_Root_G3.crt
- OISTE_WISeKey_Global_Root_GA_CA.crt
- DigiCert_Assured_ID_Root_CA.crt
- GlobalSign_Root_CA.crt
- Secure_Global_CA.crt
- ACCVRAIZ1.crt
- Certum_Trusted_Network_CA_2.crt
- TWCA_Root_Certification_Authority.crt
- NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt
- SSL.com_EV_Root_Certification_Authority_ECC.crt
- AffirmTrust_Networking.crt
- GDCA_TrustAUTH_R5_ROOT.crt
- Buypass_Class_3_Root_CA.crt
- D-TRUST_Root_Class_3_CA_2_2009.crt
- SecureTrust_CA.crt
- Entrust_Root_Certification_Authority_-_G2.crt
- TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt
- Entrust_Certification_Authority_-_L1K.crt
- Amazon_Root_CA_1.crt
- DigiCert_Assured_ID_Root_G3.crt
- Staat_der_Nederlanden_EV_Root_CA.crt
- Amazon_Root_CA_2.crt
- DigiCert_Trusted_Root_G4.crt
- Buypass_Class_2_Root_CA.crt
- Global_Chambersign_Root_-_2008.crt
- ISRG_Root_X1.crt
- SSL.com_Root_Certification_Authority_RSA.crt
- Security_Communication_Root_CA.crt
- SSL.com_Root_Certification_Authority_ECC.crt
- EE_Certification_Centre_Root_CA.crt
- AC_RAIZ_FNMT-RCM.crt
- GeoTrust_Global_CA.crt
- TrustCor_ECA-1.crt
- GlobalSign_Root_CA_-_R2.crt
- GeoTrust_Primary_Certification_Authority_-_G3.crt
- Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt
- QuoVadis_Root_CA_3.crt
- thawte_Primary_Root_CA.crt
- AffirmTrust_Commercial.crt
- TeliaSonera_Root_CA_v1.crt
- Taiwan_GRCA.crt

Trusted Platform Module version 2.0

Wyse 5070, Wyse 5470, and Wyse 5470 All-in-One thin clients 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 will fail to boot up.

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

11

Using Wyse Management Suite

Functional areas of Wyse Management Suite console

The Wyse Management Suite console is organized into the following functional areas:

About this task

- 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 **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. In the **Administration** tab, you can 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**, do the reverse. This step is optional.
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.

   NOTE: The parent device policy group can have only 10 child device groups.

Create a ThinOS Select group

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.
5. 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. This step is optional.
6. Click **Save**.

   The group is added to the list of available groups on the **Groups & Configs** page.

   To add sub groups 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 group and you can register the devices to 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 sub groups require a client reboot for changes to take effect.

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**.

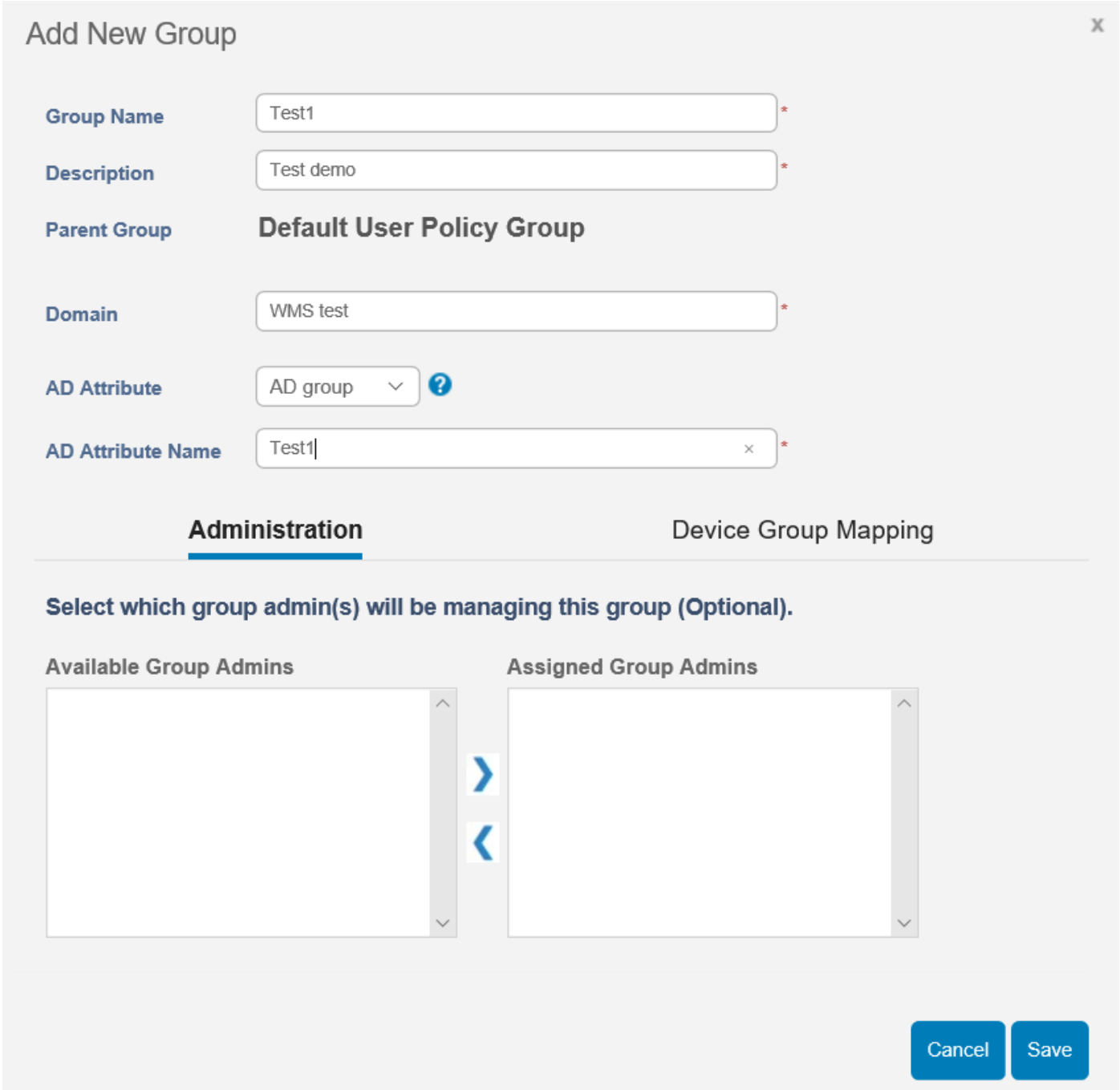


Figure 50. Add a new group

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.

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 3.1, you can deploy device exception configurations to multiple ThinOS 9.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": {
        "9EPDL900051": {
            "parameters": {
                "TerminalName": {
                    "value" : "Cubical 5 - Floor 3"
                },
                "TerminalNameCapital": {
                    "value": "no"
                }
            },
            configurations: ["westWingExceptions"]
        },
        "5LGDO600108": {
            "parameters": {
                "TerminalName": {
                    "value" : "Cubical 15 - Floor 2"
                },
                "TerminalNameCapital": {
                    "value": "no"
                }
            },
            configurations: ["westWingExceptions"]
        }
    },
    "configurations": {
        "westWingExceptions": {
            "DeviceNICDefault": {
                "value": "Wlan"
            },
            "timeZone": {
                "value": "America/Phoenix"
```

```
            },
            "TimeServer": {
                "value": "10.10.10.10"
            },
            "TerminalNameCapital": {
                "value": "yes"
            },
            "AdminMode": {
                "value": "yes"
            },
            "AdminModeUsername": {
                "value": "admin"
            },
            "AdminModePassword": {
                "value": "password"
            }
        }
    }
}
```

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 9.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.

Edit the ThinOS 9.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 9.x**.
   The **Configuration Control | ThinOS** window is displayed.

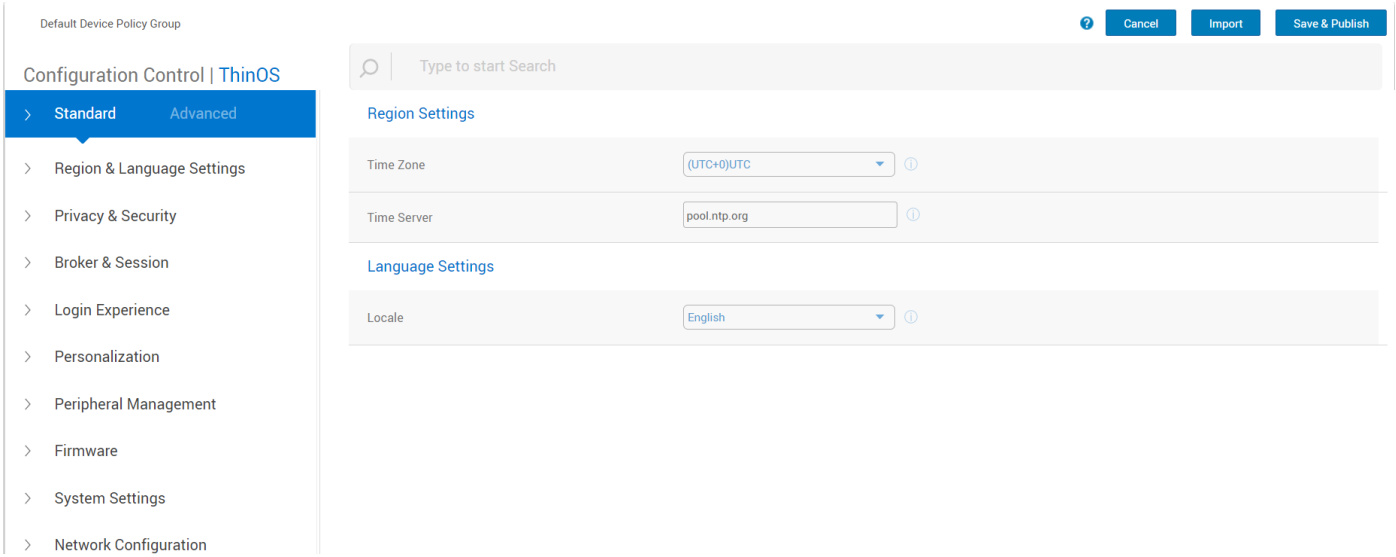


Figure 51. Configuration Control | ThinOS

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 tp 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:

- Type
- Platform
- Operating system version
- Serial number
- IP address
- Last user details
- Group details
- Last check-in time
- 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
     - Compliant
     - Pending
     - 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 3.1, 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.

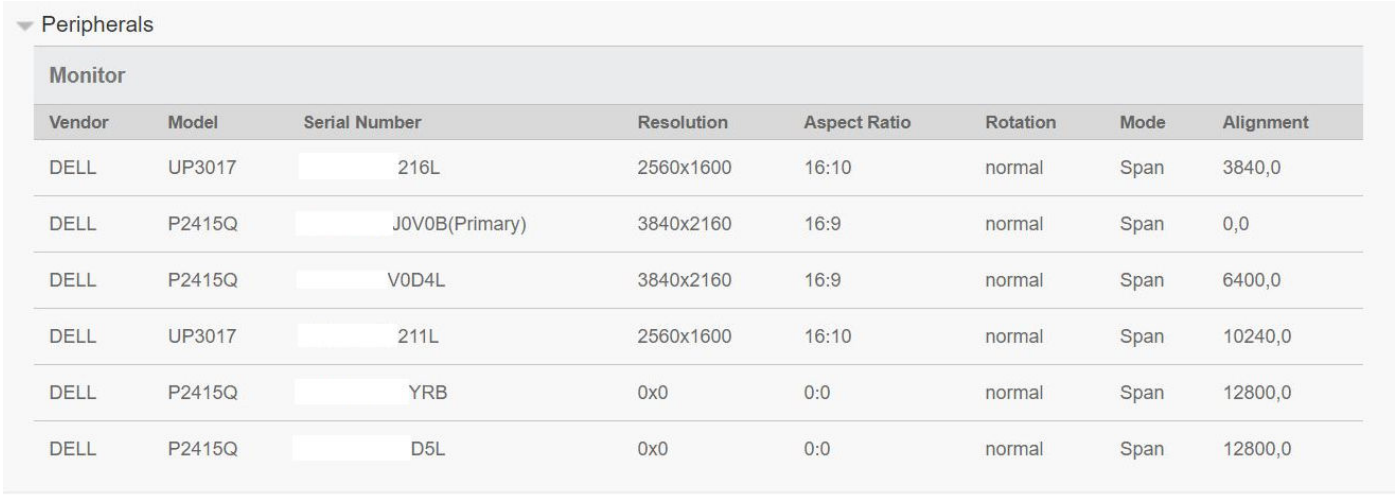
Steps

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.


Peripherals

Monitor

Vendor	Model	Serial Number	Resolution	Aspect Ratio	Rotation	Mode	Alignment
DELL	UP3017	216L	2560x1600	16:10	normal	Span	3840,0
DELL	P2415Q	J0V0B(Primary)	3840x2160	16:9	normal	Span	0,0
DELL	P2415Q	V0D4L	3840x2160	16:9	normal	Span	6400,0
DELL	UP3017	211L	2560x1600	16:10	normal	Span	10240,0
DELL	P2415Q	YRB	0x0	0:0	normal	Span	12800,0
DELL	P2415Q	D5L	0x0	0:0	normal	Span	12800,0

Figure 52. Display parameters

View the BIOS details

From Wyse Management Suite 3.1, 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
    - Others
- **OS Type**—From the drop-down menu, select the operating system.
- **Status**—From the drop-down menu, select the status of the job. The available options are:
  - Scheduled

- Running/In Progress
- Completed
- 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 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
      - Shutdown
      - Query
      - Relmage
      - Lock—Applicable for ThinOS 8.x and ThinOS 9.x devices
      - Send message—Applicable for Windows Embedded, ThinLinux, ThinOS 8.x, ThinOS 9.x, and Dell Hybrid Client powered devices
      - Factory Reset—Applicable for ThinOS 8.x, ThinOS 9.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 job description.
   f. From the **Run** drop-down list, select the date or time.
   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**
- **Unmanaged Device Auto Assignment**
- **Alert Notification**

Editing 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 (1–30 days)** box.

   NOTE: By default, registration of an unmanaged devices 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

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 52. 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	

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**.

Configure end user policy

You can configure and deploy settings to an individual user. The settings are applied to the user account and are applied to the thin client when the user logs in. This option is applicable only to thin clients running the ThinOS 9.x operating system and Dell Hybrid Clients.

Steps

1. Click the **Users** tab.
2. Click **End Users**.
3. Select a user.
   The **End User Details** page is displayed.
4. Click the **Edit Policies** drop-down menu and select the operating system.
5. Configure the required policies and click **Save and Publish**.

NOTE: There is no limit on the number of users in an on-premise environment. You can add 10,000 users in a public cloud environment.

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.

Wyse Management suite Active Directory group feature matrix

Table 53. Wyse Management suite Active Directory group feature matrix

Feature	Sub-Feature	AD User Group	User Exception	Select Group
Region&Language Settings	Region & Language	Supported	Supported	Supported
Privacy&Security	SCEP	Not applicable	Not applicable	Not applicable
Privacy&Security	Device Security	Not applicable	Not applicable	Not applicable
Privacy&Security	Account Privileges	Not applicable	Not applicable	Not applicable
Privacy&Security	Certificates	Not applicable	Not applicable	Not applicable
Privacy&Security	Security Policy	Supported	Supported	Supported

Table 53. Wyse Management suite Active Directory group feature matrix (continued)

Feature	Sub-Feature	AD User Group	User Exception	Select Group
Broker Settings	Global Broker Settings	Supported	Supported	Supported
Broker Settings	Citrix Virtual Apps and Desktops Settings	Supported	Supported	Supported
Broker Settings	VMware Horizon Settings	Supported	Supported	Supported
Broker Settings	Windows Virtual Desktop Settings	Supported	Supported	Supported
Broker Settings	Microsoft Remote Desktop Settings	Supported	Supported	Supported
Broker Settings	Amazon WorkSpaces Settings	Supported	Supported	Supported
Broker Settings	Teradici Cloud Access 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 WVD Session Settings	Supported	Supported	Supported
Login Experience	3rd Party Authentication	Not applicable	Not applicable	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
Peripheral Management	Touch	Supported	Supported	Supported
Peripheral Management	Serial Port	Supported	Supported	Supported
Peripheral Management	USB Redirection	Supported	Supported	Supported

Table 53. Wyse Management suite Active Directory group feature matrix (continued)

Feature	Sub-Feature	AD User Group	User Exception	Select Group
Peripheral Management	Monitor	Supported	Supported	Supported
Peripheral Management	Mouse	Supported	Supported	Supported
Peripheral Management	Keyboard	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	Not applicable
Network Configuration	Ethernet Settings	Not applicable	Not applicable	Supported
Network Configuration	DHCP Settings	Not applicable	Not applicable	Not applicable
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	Not applicable
Network Configuration	Proxy Settings	Not applicable	Not applicable	Supported
Network Configuration	Wireless	Not applicable	Not applicable	Supported
Network Configuration	Common 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

Table 53. Wyse Management suite Active Directory group feature matrix (continued)

Feature	Sub-Feature	AD User Group	User Exception	Select Group
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

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**.

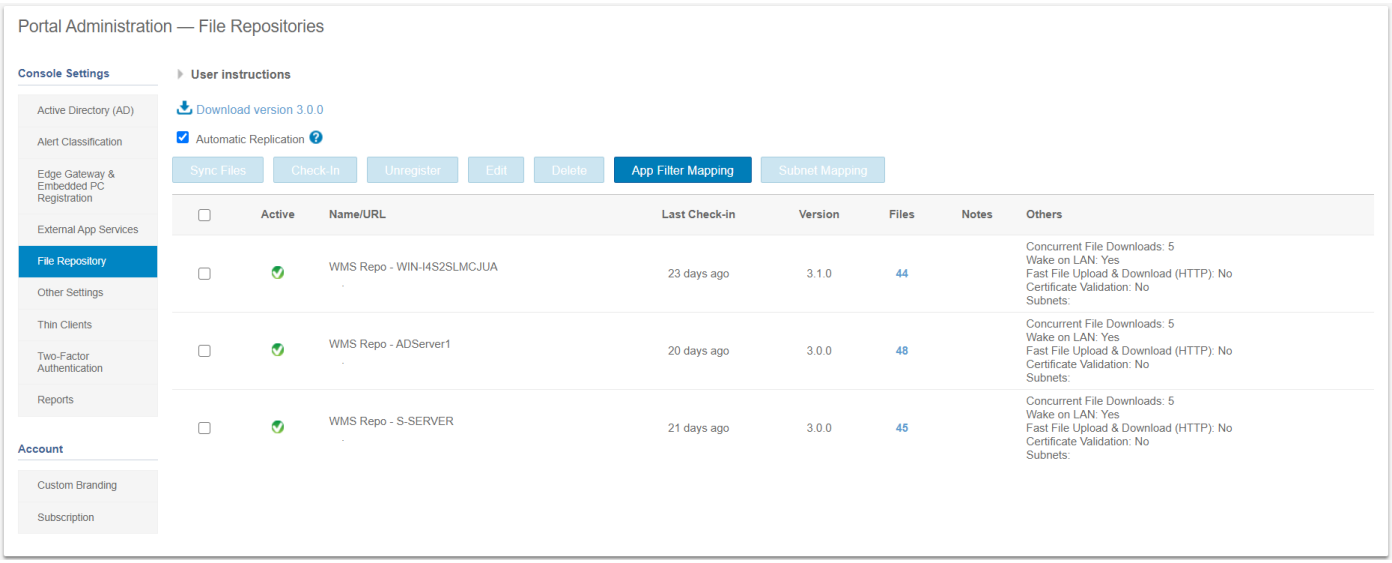


Figure 53. File repository

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.

12

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 the **Extract CMOS** option to extract the CMOS settings and certain BIOS settings to the USB drive or file server based on your target device selection.
   - 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. VMware Horizon Blast does not support this function in ThinOS version 9. 3112.
   - 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 the coredump file and trap issue screenshot file 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. 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.tgz`.
   - 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.
   - 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. Connect a USB drive to the thin client.
     b. To start logging the unexpected error messages, enable the **Capture Network Packets** option, and click **OK**.
     c. To stop logging the unexpected error messages, disable the **Capture Network 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.tgz`.
     e. Extract the `tgz` file. The log files are available at `./var/log/netmng/`.
   - **Capture Wireless Packets**—Use this option to capture wireless network-related logs.
     a. Connect a USB drive to the thin client.
     b. To start logging the unexpected error messages, enable the **Capture Wireless Packets** option, and click **OK**.
     c. To stop logging the unexpected error messages, disable the **Capture Wireless 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.tgz`.
     e. Extract the `tgz` file. The log files are available at `./var/log/netmng/`.
   - **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.tgz`.

e. Extract the `tgz` file. The log files are available at `./compat/linux/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, and click **OK**.
  c. To stop logging the unexpected error messages, disable the **Capture User Coredump** 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.tgz`.
  e. Extract the `tgz` file. The log files are available at `./compat/linux/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.tgz`.

4. Click the **Ping** 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 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 tracert 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 computers) 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 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 **OK** to save your settings.

Capture an HTTP log using ThinOS

About this task

To capture an HTTP log, do the following:

Steps

1. From the desktop menu, click **System Setup** > **Admin Policy Tool**.
   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.tgz`.
   c. Extract the `tgz` file, and verify if the `http.log` 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 login 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 8.6 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 54. 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 55. 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

Upgrade or conversion troubleshooting and logs

Upgrade using Merlin image—individual user

After a successful upgrade process, if there is no Wyse Management Suite, the system reboots to ThinOS 9.x OOBE screen.

Wyse Management Suite deployment

1. Refer Migration Guide or the Administrator's Guide of Wyse Management Suite 3.3.1 or later.
2. Upgrade Wyse Management Suite version to 3.3.1 or later versions.

   At this stage the client is still running ThinOS 8.6.
3. Wyse Management Suite admin user configures two sets of policies—one for ThinOS 8.6 and the other for ThinOS 9.x.

   For example, upload the ThinOS 9.1.4234 conversion image to ThinOS 8.6 policy and upload ThinOS application packages to ThinOS 9.x policy. At this stage the client is still running ThinOS 8.6
4. Push the conversion image from ThinOS 8.6 policy.

   At this stage, the client updates from ThinOS 8.6 to 9.1.4234 and starts reading the policy.
5. To finish the upgrade process, update ThinOS application package from ThinOS 9.x policy.

Wyse Management Suite admin-How to verify whether correct images or PKG files are uploaded?

- Check the Wyse Management Suite uploading progress indicator and completion message.
- Verify whether the uploaded files are showing up in the Wyse Management Suite image or PKG dropdown.

How to verify a download or installation are in progress?

- There is no progress bar or success message from Wyse Management Suite.
- After successful completion, the managed group and unit version information is updated in Wyse Management Suite.
- On ThinOS 8.6, initially there are messages in the event log. After retrieving the image, the installation starts similar to ThinOS 8.6, followed by a system reboot, and the installation continues in ThinOS 9.1.4234. After the installation, the system reboots to ThinOS 9.1.4234.

How to verify whether the image installation is completed successfully?

- After the last auto reboot, the thin client boots up to the Wyse Management Suite configuration from group 9.x policy.
- Verify the success info and system info in the unit system information or package information.

How to recover during a failure?

- If there is a failure message stating *Upgrade break cannot boot up*, use USB recovery.
- If there is a wrong image or PKG, and the device shows wrong screen or info, use USB recovery.

How to verify whether the thin client is working properly?

Go to **System information** > **Event Log** and see if the system info or PKG versions are correct.

If any unexpected issues occur before VDI logon, collect the following data:

- General troubleshooting
  - **General** > **Export system setting**
  - **General** > **Export Screenshot**
  - **General** > **Export logs**
- Network troubleshooting
  - **Capture** > **Capture Network Packets**
  - **Capture** > **Capture Wireless Packets**
- Peripherals troubleshooting
  - **Capture** > **Capture USB Packets**

Logs to capture during VDI logon failure

If you face VDI or cloud sign-on failure, go to **Capture** > **HTTP log** and collect the data for analysis.

Logs to capture when session failure after launch

After you signed on VDI or cloud, if the remote desktop connection failed to launch or failed after launch, go to **General** > **Export logs** and collect the data for analysis.

Important information

- The System configuration export is encrypted with a password and the administrator is prompted to provide password protection upon using this option.

- Administrator must manage the enablement of the export options on the thin client. It is recommended to not enable export options to all users.

How to debug with new support beyond ThinOS 8?

Reproduce the problem with any other ThinOS 9 unit and capture logs/trace from ThinOS 9 for support analysis.

How to debug with same support in ThinOS 8?

Capture the ThinOS 9 related logs/trace and also capture the related logs/trace in ThinOS 8 following same steps where it works. Send both to the support team for comparison and analysis. This can help isolate the root cause sooner.

13

Frequently Asked Questions

ThinOS-related questions

This section contains frequently asked questions related to Wyse ThinOS.

How do I upgrade from ThinOS 8.6 to 9.1.4234?

You must use the Wyse Management Suite version 3.3.1 to upgrade from ThinOS 8.6 to 9.1.4234. For the firmware upgrade procedure, see Firmware upgrade and package deployment or the *Dell Wyse ThinOS 9.1.4234 Migration Guide*.

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 3.3.1 the only way to manage ThinOS 9.1.4234?

ThinOS 9.1.4234-devices can be managed using either Wyse Management Suite or Admin Policy Tool.

How to verify third-party binary versions on your ThinOS client?

On the ThinOS client, go to **System Tools** > **Packages**, and double-click the third-party package to see the binary version.

Is USB Imaging Tool method a possible option for upgrading to ThinOS 9.1.4234?

Dell Technologies recommends to use Wyse Management Suite version 3.3.1 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 9.1.4234 on a single device.

Can ThinOS be installed on a PCoIP device?

ThinOS is supported on PCoIP devices.

Does ThinOS support zero desktop?

In ThinOS 9.1.4234, the zero desktop is called modern desktop. You can enable the modern desktop mode using either Wyse Management Suite or the Admin Policy Tool.

Does ThinOS support ThinOS configurations using INI files?

ThinOS does not support INI files. You need to use Wyse Management Suite 3.1 or the local Admin Policy Tool to configure the advanced ThinOS settings.

iPhone cannot be redirected to the Citrix Desktop session

Steps

1. Open **Global Connection Settings**.
2. Uncheck **Exclude disk devices** and **Exclude audio devices**.

Android smartphone is not displayed in the session when redirected or mapped

You must select the option to transfer images on your smartphone when you connect the USB cable.

Does Citrix Workspace app replace Citrix Receiver on ThinOS?

In ThinOS 9.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 9.x.

For more information about deploying packages using Wyse Management Suite, see How to upload and push ThinOS 9.x application packages.

What is Workspace mode on ThinOS?

Workspace mode enables you to customize the look and feel of your ThinOS to match the Citrix Workspace-based layout of published applications and desktops. Workspace mode displays both the ThinOS full taskbar and the workspace desktop. From the Admin Policy Tool or the Wyse Management Suite policy settings server, go to **Personalization** > **User Experience Settings**, set **System Mode** to **Classic** and select the **Workspace Mode** check box in **System Setup** > **Remote Connections** > **Broker Setup**.

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 HDX Enlightened Data Transport Protocol is active?

To verify if 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/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* at www.support.citrix.com.

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?

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 layer.

   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 to check if Multimedia Redirection is working?

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?

Persistent logging is not supported in ThinOS.

Is tls.txt file included in network traces on ThinOS?

The tls.txt file is not included in network traces for ThinOS.

Will ThinOS device reboot automatically when the system crashes?

ThinOS 9.1.4234 device automatically reboots when the system crashes. 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-related questions

This section contains frequently asked questions 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 following order defines the priority set for ThinOS configurations:

Wyse Management Suite Policies > **Admin Policy Tool** > **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.