

Dell Wyse Management Suite

Version 4.x Release Notes



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: Release summary.....	6
Priority and recommendations.....	6
Chapter 2: Version matrix.....	7
Chapter 3: Wyse Management Suite 4.1 Hotfix 1.....	8
Compatibility.....	8
Supported Dell end-points on Wyse Management Suite.....	8
Supported browsers.....	10
Supported operating system matrix.....	10
Important notes.....	10
Server or device agent details.....	11
Windows Server configuration requirements.....	11
Wyse Management Suite upgrade path.....	12
Fixed issues.....	12
Chapter 4: Wyse Management Suite 4.1.....	13
Compatibility.....	13
Supported Dell end-points on Wyse Management Suite.....	13
Supported browsers.....	15
Supported operating system matrix.....	15
New features.....	16
Migration from Community to Mongo database Enterprise for on-premise servers	16
Additional granular controls for ThinOS device logs.....	16
ISO imaging format compatibility for Windows Embedded Standard devices.....	16
Enable Windows Embedded Standard to ThinOS conversion.....	16
Enable ThinLinux to ThinOS conversion.....	17
Improvements to tags workflow.....	17
Report Ethernet speed for ThinOS devices.....	17
Report ThinOS certificate expiry details	17
View the source of the events.....	18
Additional Clear Filters options.....	18
DNS filter.....	18
Support soft reset for ThinOS 9.x.....	18
New configuration user interface support for Windows 10 IoT Enterprise devices.....	18
User interface changes for Windows Embedded Standard devices.....	19
Delay policy execution option added for application policies for Generic clients.....	19
ThinOS administrator password, BIOS password and deprecated protocol.....	19
Support for Dell Hybrid Client 2.5.....	20
Important notes.....	20
Server or device agent details.....	21
Windows Server configuration requirements.....	21
Wyse Management Suite upgrade path.....	21
Fixed issues.....	22

Chapter 5: Wyse Management Suite 4.0.0 Hotfix 3	23
Compatibility.....	23
Supported Dell end-points on Wyse Management Suite.....	23
Supported browsers.....	24
Supported operating system matrix.....	25
Important notes.....	25
Server or device agent details.....	26
Windows Server configuration requirements.....	26
Wyse Management Suite upgrade path.....	26
Steps to apply the Hotfix.....	27
Fixed issues.....	27
 Chapter 6: Wyse Management Suite 4.0.0 Hotfix 2	 28
Compatibility.....	28
Supported Dell end-points on Wyse Management Suite.....	28
Supported browsers.....	29
Supported operating system matrix.....	30
Important notes.....	30
Server or device agent details.....	31
Windows Server configuration requirements.....	31
Wyse Management Suite upgrade path.....	31
Steps to apply the Hotfix.....	32
Fixed issues.....	32
 Chapter 7: Wyse Management Suite 4.0.0 Hotfix	 33
Compatibility.....	33
Supported Dell end-points on Wyse Management Suite.....	33
Supported browsers.....	34
Supported operating system matrix.....	35
Important notes.....	35
Server or device agent details.....	36
Windows Server configuration requirements.....	36
Wyse Management Suite upgrade path.....	36
Steps to apply the Hotfix.....	37
Fixed issues.....	37
 Chapter 8: Wyse Management Suite 4.0.....	 38
Compatibility.....	38
Supported Dell end-points on Wyse Management Suite.....	38
Supported browsers.....	39
Supported operating system matrix.....	39
New and enhanced features.....	40
Vulnerable devices displayed on the dashboard.....	40
Wyse Management Suite repository enhancements and optimizations	41
Dynamic maximum concurrent download based on system configuration.....	42
Update Max concurrent downloads for repository and restart tomcat Service.....	42
Clear concurrent download slot after application download is complete.....	42
Report for Missing QFE.....	43

Report for Installed QFE.....	43
Report for Has not installed QFE.....	43
Generate reports on devices that have exceptions.....	43
Azure Virtual Desktop.....	43
UWF Servicing mode.....	43
Filter Devices as per the Application Package.....	44
Filter Devices as per the Application Policy.....	44
Clearing inactive and unused filters for subnets, time zones, and devices.....	45
DCA-Enabler Agent GUI for WMS Registration	45
WES to ThinOS Conversion.....	45
Wyse Management Suite to support selection of multiple groups while creating Advanced App Policies.....	45
Wyse Management Suite displays option to Restart Jobs for Offline Devices.....	46
Wyse Management Suite enables WES package File Repository in Operator and Tenant Cloud.....	46
Wyse Management Suite supports Dell Hybrid Client 2.x Configuration Policies.....	46
Run Report on Devices.....	47
Important notes.....	47
Server or device agent details.....	47
Windows Server configuration requirements.....	48
Wyse Management Suite upgrade path.....	48
Fixed issues.....	48
Security fixes.....	50
Chapter 9: Installing package.....	51
Downloading the installation file.....	51
Chapter 10: Resources and support.....	52
Chapter 11: Contacting Dell.....	53

Release summary

Wyse Management Suite is the next generation management solution that enables organizations to centrally configure, monitor, manage, and optimize Dell Hybrid Client powered endpoints and Dell thin clients. Wyse Management Suite can be installed On-premise, in your organization's private cloud, or used as a Software as a Service (SaaS) for automatic maintenance of software without any management software to install.

Wyse Management Suite uses industry-standard architecture and components to efficiently manage network devices. Wyse Management Suite is a web-based application where you can access the console using a supported browser and perform all the operations from the web UI. The Wyse Management Suite architecture is designed to manage the endpoint devices in an efficient, reliable, and secure manner. Wyse Management Suite is available in Standard and Pro edition.

- **Standard (Free)**—The Standard edition of the Wyse Management Suite offers basic functionalities and is available for a private cloud deployment. A license key is not required to use the Standard edition. This version can manage Dell Thin Clients. The Standard edition is suitable for small and medium businesses.
- **Pro (Paid)**—The Pro edition of the Wyse Management Suite is a more robust solution. It is available for both public and private cloud deployment. A license key is required to use the Pro edition (subscription-based licensing). With the Pro solution, organizations can adopt a hybrid model and float licenses between private and public clouds if needed. This version is required to manage any Teradici-based devices, Wyse Covert for PCs, and Dell Hybrid Client powered devices. It also offers more advanced features to manage Dell thin clients. For a public cloud deployment, the Pro edition can be managed on noncorporate networks (home office, third party, partners, mobile thin clients, and so on).

Priority and recommendations

Recommended: Dell Technologies recommends that you apply the update during your next scheduled update cycle. The update contains feature enhancements or changes that will help to keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

Version matrix

The following table summarizes the Wyse Management Suite versions:

Table 1. Version matrix

Release Version	Release Date	Release Notes
Wyse Management Suite 4.1 Hotfix 1	July 2023	Wyse Management Suite 4.1 Hotfix 1
Wyse Management Suite 4.1	June 2023	Wyse Management Suite 4.1
Wyse Management Suite 4.0 Hotfix 3	March 2023	Wyse Management Suite 4.0 Hotfix 3
Wyse Management Suite 4.0 Hotfix 2	February 2023	Wyse Management Suite version 4.0 Hotfix 2
Wyse Management Suite 4.0 Hotfix 1	January 2023	Wyse Management Suite version 4.0 Hotfix
Wyse Management Suite 4.0	December 2022	Wyse Management Suite version 4.0

Wyse Management Suite 4.1 Hotfix 1

Wyse Management Suite 4.1 Hotfix 1 addresses issues that are related to device export to CSV and report generation.

If there are any **Report** or **Device Export to CSV** job in a queued state before installing the Hotfix, then you must generate the report from **Portal Administration > Reports** after the Hotfix installation. This clears the previously queued report jobs.

Compatibility

Supported Dell end-points on Wyse Management Suite

Table 2. Supported Dell end-points on Wyse Management Suite

Operating System	Platform	Wyse Device Agent versions
Windows 10 IoT Enterprise 2019 LTSC	Wyse 5070 and 5070 Extended Thin Client	10.04.06.09.19.00, 10.04.06.11.20, 10.04.06.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
	Wyse 5470 Thin Client	10.04.08.09.19.00, 10.04.08.11.20, 10.04.08.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
	Wyse 5470 AIO Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
Windows 10 IoT Enterprise LTSC 2021	Optiplex 3000 Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
ThinOS	<ul style="list-style-type: none"> Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 3030 LT Thin Client (with and without PCoIP) Wyse 5040 Thin Client (ThinOS, PCoIP) Wyse 5010 Thin Client (ThinOS, PCoIP) Wyse 7010 Thin Client (with and without PCoIP) Wyse 5060 Thin Client (with and without PCoIP) 	8.5.x, 8.6.x
	<ul style="list-style-type: none"> Wyse 5070 Thin Client (with and without PCoIP) Wyse 5470 Thin Client (with and without PCoIP) Wyse 5470 AIO Thin Client (with and without PCoIP) 	8.5.x, 8.6.x, 9.1.x, 9.3.x, 9.4.x
	Optiplex 3000 Thin Client	9.1.x, 9.3.x, 9.4.x
	Latitude 3420 Thin Client	9.3.x, 9.4.x

Table 2. Supported Dell end-points on Wyse Management Suite (continued)

Operating System	Platform	Wyse Device Agent versions
	OptiPlex 5400 All-In-One	
	Wyse 3040 Thin Client (with and without PCoIP)	8.6.x, 9.0.x, 9.1.x
	Latitude 3440	9.4.x
	Latitude 5440	
	OptiPlex All-in-One 7410	
Teradici	Wyse 5030 PCoIP zero client	5.x, 6.x, 20.x, 21.x, 22.x, 23x
	Wyse 7030 PCoIP zero client	
	Wyse 5050 AIO Thin Client	
Dell Hybrid Client	Wyse 5070 Thin Client	Ubuntu 18.04, 20.04
	Wyse 5070 Extended Thin Client	Bundle—Dell Hybrid Client version 1.1, 1.1.01, 1.5, 1.6, 1.8 and 2.x
	OptiPlex 7070 Ultra	Dell Client Agent - 1.0.0, 1.1.03, 1.2.0, 1.1.1, 1.3.x, 1.4.x, 1.5.0.x, 2.0.x, DCA_2.5.0-x, and later
	OptiPlex 7090 Ultra	
	OptiPlex 3090 Ultra	
	Latitude 3320	
	OptiPlex 5400 All-In-One	
	Latitude 3330	
	OptiPlex 3000 Thin Client	
	Precision 3260	
	Latitude 3440	
	Latitude 5440	
	OptiPlex All-in-One 7410	
Dell Ubuntu (Generic) Client	Dell Commercial Devices	Ubuntu 18.04, 20.04, 22.04
		DCA_Enabler - 1.0.0-72, DCA_Enabler - 1.1.0-17, DCA_Enabler - 1.2.0-25, DCA_Enabler - 1.2.1-14 DCA_Enabler-1.3.0.23, DCA_Enabler-1.4.0.26, DCA_Enabler_1.5.0-14, DCA_Enabler_1.6.0-9, DCA_Enabler_1.7.0-x, DCA_Enabler_1.7.1-x and later
Wyse Converter for PCs	NA	Version: 2.1.2.141 Wyse Device Agent: 14.6.5.9, 14.6.7.x, and later Version: 3.0.0.4689 Wyse Device Agent: 14.6.6.3, 14.6.7.x, and 14.6.9.x

- NOTE:** WDA version 14.6.3.1 and older versions can only be downgraded from WMS. Manual downgrade of WDA on the device is not supported. If you manually downgrade WDA, then the WMS information is lost, and you cannot upgrade WDA upgrades later. To overcome the issue, WDA must be uninstalled manually, and installed again.
- NOTE:** WDA 14.6.7.x is not supported for Wyse Device Manager. If you downgrade the agent from 14.6.7.x to older versions HA Agent Services are not restored. The administrator of the client must manually uninstall and install the desired WDA.

Supported browsers

Table 3. Supported browsers

Browsers	Version
Chrome	114.0.5735.110 and later
Firefox	102.12.0 and later
Edge browser	114.0.1823.43

NOTE: WMS Portal is no more supported on Microsoft Internet Explorer as The Internet Explorer 11 desktop application is retired on June 15, 2022. For more information, see *Internet Explorer 11 desktop app support ended for certain versions of Windows 10* at <https://docs.microsoft.com/>.

Supported operating system matrix

Table 4. Supported operating systems

Operating system	WMS server	WMS repository	Remote database
Windows Server 2016 English	Supported	Supported	Supported
Windows Server 2016 French	Supported	Supported	Not supported
Windows Server 2016 Italian	Supported	Supported	Not supported
Windows Server 2016 German	Supported	Supported	Not supported
Windows Server 2016 Spanish	Supported	Supported	Not supported
Windows Server 2016 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2016 Japanese	Supported	Supported	Not supported
Windows Server 2019 Standard English	Supported	Supported	Supported
Windows Server 2019 French	Supported	Supported	Not supported
Windows Server 2019 Italian	Supported	Supported	Not supported
Windows Server 2019 German	Supported	Supported	Not supported
Windows Server 2019 Spanish	Supported	Supported	Not supported
Windows Server 2019 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2019 Japanese	Supported	Supported	Not supported
Windows Server 2022 Standard English	Supported	Supported	Supported
Windows Server 2022 French	Supported	Supported	Not supported
Windows Server 2022 Italian	Supported	Supported	Not supported
Windows Server 2022 German	Supported	Supported	Not supported
Windows Server 2022 Spanish	Supported	Supported	Not supported
Windows Server 2022 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2022 Japanese	Supported	Supported	Not supported

Important notes


- Microsoft Gina should be selected when you configure keyboard layouts.
- Language pack should be pre-installed on the Windows 10 IoT Enterprise image to apply the default language configuration.

- Updating substitute keyboard layouts restarts the device twice if Microsoft Gina is enabled.
- For information about the changes or updates to the ThinOS and Dell Hybrid Client configurations, see *ThinOS 9.x Administrator's Guide and Release notes* and *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.
- If you are using Wyse Easy Setup 2.0.0.158 or earlier versions, you must upgrade Wyse Easy Setup to 2.0.0.189 after you upgrade Wyse Device Agent to 14.6.1.4.
- When the Citrix connection is deployed from Wyse Management Suite and if Citrix application is active or in use, and then the default Citrix connection cannot be launched.
- If you are an issue with Wyse Easy Setup issue after upgrading to WDA 14.6.8.1 from WDA 14.6.7.32, you must re-publish the Wyse Easy Setup configuration from Wyse Management Suite.
- From Wyse Management Suite 4.0, you can select multiple groups (up to 100 parent groups) when you create an advanced application policy. When you select multiple groups:
 - **Exceeded maximum number of groups allowed in a policy** message is displayed and the policy creation is blocked when you select more than 100 parent groups or sub-groups.
 - The administrator must select **Include sub-groups** option, if sub-groups must be included in the advanced application policy.
 - The sub-groups selection is not displayed when **Include sub-group** option is selected. However, individual jobs for all parent and sub-groups are created when the policy is scheduled.
 - The policy cannot be scheduled immediately if the total number of applicable devices are more than 25. The administrator must schedule the policy later.

Server or device agent details

Table 5. Server or device agent details

File name	Description	Version
WMS_Hotfix_4.1.0.548.exe	Wyse Management Suite server	4.1.0.548
WMS_Repo_4.1.0.158.exe	Wyse Management Suite repository	4.0.1.41
WDA_14.6.9.21_Unified.exe	Unified WDA for Windows 10 IoT Enterprise	14.6.9.21
DellWMS-ConfigurationUI-Package.zip	configUI_signed.zip	1.9.950
DCA_Enabler_1.7.1-61	DCA Enabler and DCA Enabler Package combined Zipped	1.7.1-61
SoftwareVaultUtility-1.5.0.0.exe	Software Vault Utility	1.5.0.0
ConfigUISupport.exe	Configuration user interface	1.0.0.3

 **NOTE:** The above-listed agents are not tested with WDM.

Windows Server configuration requirements

Table 6. Windows Server configuration requirements


Devices	Server requirements
Minimum server requirements for Wyse management Suite operations with 10,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2016, and Windows Server 2019 Standard and Windows Server 2022 • Minimum CPU requirements—4 CPU • Minimum Disk Space—40 GB • Minimum Memory—8 GB <p> NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for Secure MQTT communications.</p>
Server requirement for Wyse Management Suite operations with 50,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2016, and Windows Server 2019 Standard and Windows Server 2022

Table 6. Windows Server configuration requirements (continued)

Devices	Server requirements
	<ul style="list-style-type: none"> • Minimum CPU requirements—4 CPU • Minimum Disk Space—120 GB • Minimum Memory—16 GB
Server requirement for Wyse Management Suite operations with 120,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2016, and Windows Server 2019 Standard and Windows Server 2022 • Minimum CPU requirements—16 CPU • Minimum Disk Space—200 GB • Minimum Memory—32 GB

Wyse Management Suite upgrade path

Table 7. Wyse Management Suite upgrade path

Upgrade type	Upgrade path	Compatibility
4.1 to 4.1 Hotfix 1	4.1 > 4.1 Hotfix 1	Supported

Fixed issues

Table 8. Fixed issues

Issue ID	Description
WMS-895	Observed a delay in Wyse Management Suite report export.
WMS-896	Export to CSV does not work in Wyse Management US1 tenant.
WMS-897	Reports are not completed in a timely manner in Wyse Management Suite 4.1 cloud.

Wyse Management Suite 4.1

Compatibility

Supported Dell end-points on Wyse Management Suite

Table 9. Supported Dell end-points on Wyse Management Suite

Operating System	Platform	Wyse Device Agent versions
Windows 10 IoT Enterprise 2019 LTSC	Wyse 5070 and 5070 Extended Thin Client	10.04.06.09.19.00, 10.04.06.11.20, 10.04.06.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
	Wyse 5470 Thin Client	10.04.08.09.19.00, 10.04.08.11.20, 10.04.08.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
	Wyse 5470 AIO Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
Windows 10 IoT Enterprise LTSC 2021	Optiplex 3000 Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.7.x, 14.6.9.x, and later
ThinOS	<ul style="list-style-type: none"> Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 3030 LT Thin Client (with and without PCoIP) Wyse 5040 Thin Client (ThinOS, PCoIP) Wyse 5010 Thin Client (ThinOS, PCoIP) Wyse 7010 Thin Client (with and without PCoIP) Wyse 5060 Thin Client (with and without PCoIP) 	8.5.x, 8.6.x
	<ul style="list-style-type: none"> Wyse 5070 Thin Client (with and without PCoIP) Wyse 5470 Thin Client (with and without PCoIP) Wyse 5470 AIO Thin Client (with and without PCoIP) 	8.5.x, 8.6.x, 9.1.x, 9.3.x, 9.4.x
	Optiplex 3000 Thin Client	9.1.x, 9.3.x, 9.4.x
	Latitude 3420 Thin Client OptiPlex 5400 All-In-One	9.3.x, 9.4.x
	Wyse 3040 Thin Client (with and without PCoIP)	8.6.x, 9.0.x, 9.1.x

Table 9. Supported Dell end-points on Wyse Management Suite (continued)


Operating System	Platform	Wyse Device Agent versions
	Latitude 3440 Latitude 5440 OptiPlex All-in-One 7410	9.4.x
Teradici	Wyse 5030 PColP zero client	5.x, 6.x, 20.x, 21.x , 22.x, 23x
	Wyse 7030 PColP zero client	
	Wyse 5050 AIO Thin Client	
Dell Hybrid Client	Wyse 5070 Thin Client	Ubuntu 18.04, 20.04
	Wyse 5070 Extended Thin Client	Bundle—Dell Hybrid Client version 1.1, 1.1.01. 1.5, 1.6, 1.8 and 2.x
	OptiPlex 7070 Ultra	Dell Client Agent - 1.0.0, 1.1.03, 1.2.0, 1.1.1, 1.3.x, 1.4.x, 1.5.0.x, 2.0.x, DCA_2.5.0-x, and later
	OptiPlex 7090 Ultra	
	OptiPlex 3090 Ultra	
	Latitude 3320	
	OptiPlex 5400 All-In-One	
	Latitude 3330	
	OptiPlex 3000 Thin Client	
	Precision 3260	
	Latitude 3440	
	Latitude 5440	
	OptiPlex All-in-One 7410	
Dell Ubuntu (Generic) Client	Dell Commercial Devices	Ubuntu 18.04, 20.04, 22.04 DCA_Enabler - 1.0.0-72, DCA_Enabler – 1.1.0-17, DCA_Enabler – 1.2.0-25, DCA_Enabler - 1.2.1-14 DCA_Enabler-1.3.0.23, DCA_Enabler-1.4.0.26, DCA_Enabler_1.5.0-14, DCA_Enabler_1.6.0-9, DCA_Enabler_1.7.0-x, DCA_Enabler_1.7.1-x and later
Wyse Converter for PCs	NA	Version: 2.1.2.141 Wyse Device Agent: 14.6.5.9, 14.6.7.x, and later Version: 3.0.0.4689 Wyse Device Agent: 14.6.6.3, 14.6.7.x, and 14.6.9.x

- NOTE:** WDA version 14.6.3.1 and older versions can only be downgraded from WMS. Manual downgrade of WDA on the device is not supported. If you manually downgrade WDA, then the WMS information is lost, and you cannot upgrade WDA upgrades later. To overcome the issue, WDA must be uninstalled manually, and installed again.
- NOTE:** WDA 14.6.7.x is not supported for Wyse Device Manager. If you downgrade the agent from 14.6.7.x to older versions HA Agent Services are not restored. The administrator of the client must manually uninstall and install the desired WDA.

Supported browsers

Table 10. Supported browsers

Browsers	Version
Chrome	114.0.5735.110 and later
Firefox	102.12.0 and later
Edge browser	114.0.1823.43

 **NOTE:** WMS Portal is no more supported on Microsoft Internet Explorer as The Internet Explorer 11 desktop application is retired on June 15, 2022. For more information, see *Internet Explorer 11 desktop app support ended for certain versions of Windows 10* at <https://docs.microsoft.com/>.

Supported operating system matrix

Table 11. Supported operating systems

Operating system	WMS server	WMS repository	Remote database
Windows Server 2016 English	Supported	Supported	Supported
Windows Server 2016 French	Supported	Supported	Not supported
Windows Server 2016 Italian	Supported	Supported	Not supported
Windows Server 2016 German	Supported	Supported	Not supported
Windows Server 2016 Spanish	Supported	Supported	Not supported
Windows Server 2016 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2016 Japanese	Supported	Supported	Not supported
Windows Server 2019 Standard English	Supported	Supported	Supported
Windows Server 2019 French	Supported	Supported	Not supported
Windows Server 2019 Italian	Supported	Supported	Not supported
Windows Server 2019 German	Supported	Supported	Not supported
Windows Server 2019 Spanish	Supported	Supported	Not supported
Windows Server 2019 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2019 Japanese	Supported	Supported	Not supported
Windows Server 2022 Standard English	Supported	Supported	Supported
Windows Server 2022 French	Supported	Supported	Not supported
Windows Server 2022 Italian	Supported	Supported	Not supported
Windows Server 2022 German	Supported	Supported	Not supported
Windows Server 2022 Spanish	Supported	Supported	Not supported
Windows Server 2022 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2022 Japanese	Supported	Supported	Not supported

New features

Migration from Community to Mongo database Enterprise for on-premise servers

The installation of Wyse Management Suite 4.1 uses Mongo database Enterprise version if it is installed with embedded database. If you upgrade to Wyse Management Suite 4.1 from the earlier version, the community versions of Mongo database binaries are replaced with Mongo database enterprise binaries.

When 4.1 is installed or upgraded in a distributed or remote Mongo database environment, Wyse Management Suite checks the Mongo database 5.0.18 Enterprise binaries and then goes to upgrade. If the remote Mongo database is not 5.0.18 or if it is not the enterprise version, then a message is displayed and the upgrade is blocked.

NOTE: Occasionally, anti-virus stops the Mongo database service. To overcome this, you must exclude the Mongo database folders from the security scanning or anti-virus scan list.

For more information, see *How to avoid this error "terminate() called. An exception is active; attempting to gather more information"?* article at <https://www.mongodb.com/> and *Mongo DB service getting stopped intermittently* at <https://stackoverflow.com/>.

Additional granular controls for ThinOS device logs

Two additional options for **Network Trace** and **Core Dump** is added when you pull the device log from Wyse Management Suite. The available repository list for the log pull, for example, local repository, remote repository for on-premise and cloud repository, remote repository for cloud environment are displayed.

To access the ThinOS device logs, go to the **Devices** page and select the ThinOS 9.x devices. Click the selected device and go to the **Device Details** page. Go to the **Device Logs** tab and click **Request Log File**. After the device logs are pulled, a download link is displayed in the user interface to download the device logs if the device log is pulled over local repository for on-premise and cloud repository for cloud environment. If the device logs are pulled by selecting the remote repository, then Wyse Management Suite displays a message on how to download the Logs from Remote Repository Server. The logs are uploaded to <Remote Repository Location>\data\logs\<Device ID>.

The log file size limit is 1 GB for cloud repository and 5 GB for remote repository for cloud environment. The log file size limit is configurable from 1 GB to 5 GB for local repository and remote repository for on-premise environment. The value can be configured from **Portal Administration > Other Settings** page.

NOTE: For ThinOS versions earlier than 9.x 2306, ThinOS device uploads the device log to regular repository. For example, local repository for on-premise and cloud repository for public cloud, irrespective of the repository selection.

ISO imaging format compatibility for Windows Embedded Standard devices

Wyse Management Suite 4.1 support Windows IoT images in ISO format.

You must copy the Windows IoT images to the local repository or remote repository under <\repository\osImages\zipped>. The image is displayed in the Wyse Management Suite user interface in the **Apps & Data** tab under **WinIoT / ThinLinux OS Image Repository**. The administrator can create an image policy using the image and deploy to multiple thin clients.

Enable Windows Embedded Standard to ThinOS conversion

From Wyse Management Suite 4.1, you can use `ThinOS_Conversion_Tool.exe` and ThinOS 9.x Firmware package to convert Windows Embedded Standard to ThinOS.

The `ThinOS_Conversion_Tool.exe` can be copied from <\repository\thinClientApps> or uploaded through **Apps & Data > App Inventory - Thin Client > Add WinIoT Package**.

ThinOS 9.x firmware package must be copied to <repository\ thinOSConfigFiles> or uploaded through **Apps & Data > OS Image Repository - ThinOS 9.x > Add Firmware File**.

Both the packages can be deployed on Windows 10 IoT devices by creating a standard application policy or advanced application policy. You must deploy ThinOS_Conversion_Tool.exe initially and then the ThinOS 9.x Firmware package.

NOTE:

- **Show Conversion Packages** checkbox must be selected to display the ThinOS 9.x firmware package in the application policy.
- Sufficient ThinOS activation licenses must be present in to create the conversion application policy.
- **Auto Discovery** must be configured to register back the converted device to Wyse Management Suite.
- The conversion status can be monitored from the **Jobs** page. The job is successful after the device is converted and registered back to Wyse Management Suite.
- Device report can be generated to track the devices which are converted to ThinOS.

Enable ThinLinux to ThinOS conversion

You must copy the TL_Conversion.exe (merlin image) to <repository\osImages\zipped> and wait for the image to get extracted and sync to Wyse Management Suite. The image is displayed in the Wyse Management Suite user interface in the **Apps & Data** tab under **WinIoT / ThinLinux OS Image Repository**. Create an image policy and schedule it.

NOTE:

- Sufficient ThinOS activation licenses must be present in to create the conversion application policy.
- **Auto Discovery** must be configured to register back the converted device to Wyse Management Suite.
- The conversion status can be monitored from the **Jobs** page. The job is successful after the device is converted and registered back to Wyse Management Suite.
- Device report can be generated to track the devices which are converted to ThinOS.

Improvements to tags workflow

When a device is tagged, the tag name is displayed in the **Devices** page and **Device Details** page. The devices without any tag are displayed as **N/A**.

To edit the tag names or to delete tags in bulk, go to **Devices > More Action > Edit Device Tag(S)**.

Device report is also enhanced to show the tag names under a new **Tag** column.

Report Ethernet speed for ThinOS devices

From Wyse Management Suite 4.1, Ethernet speeds are reported and displayed on the **Device Details** page for ThinOS 2306 devices.

Report ThinOS certificate expiry details

ThinOS 9.x devices report installed certificates with the expiry date to Wyse Management Suite. The certificate notification with the count of the certificates that are expiring and the certificates that have expired are displayed on the **Dashboard** in the **Other Device Alerts** section. The details are also displayed in a chart form.


You can configure the notification details such as expiry date and the notification rules in the **Other Settings** section of the **Portal Administration** page. The ThinOS device certificate expiry can be set within the range of 1 to 120 Days, and the default value is 30 days. If this value is changed, then the administrator must wait for the full check-in of the device to view the updated certificate information that is displayed on the **Dashboard** page.

You can also view the certificate alerts in the **Events** page. The **Certificate Expiry** alert is resolved after the certificate is renewed. The resolved events can also be viewed in the **Events** page with the **Certificate Expiration Resolved** option from the **Event Type** drop-down filter.

All the certificate events are categorized as **Critical Events**. These events can also be filtered using the **Current Alerts** and **Critical Events Category** from the **Events** page.

View the source of the events

The global administrator can filter the events based on their source. For example, all the events that are generated by a group administrator can be filtered.

 **NOTE:** The administrators other than global administrators can view only system events and their own events. For security reasons, non-global administrator cannot view events from different sources.

Additional Clear Filters options

The administrator can clear unwanted or unused filters for platform, agent version, operating system version, BIOS version, and DNS. You can also select **Select All Filters** to clear all the unwanted or unused filters which include subnet, time zone, device tag, platform, agent version, operating system version, BIOS version, and DNS parameters.

Individual jobs are created to clear the filters for each parameter and can be tracked from **Jobs** page. The number of records that are deleted per filter parameter can be tracked from the **Events** page.

DNS filter

The administrator can filter the devices based on the DNS IP address. When devices are registered to Wyse Management Suite from different subnet having different DNS, Wyse Management Suite adds the DNS entries reported by the registered devices to the DNS filter.

If a device reports multiple DNS, then Wyse Management Suite adds multiple entries under the DNS filter. For example, a device reports two DNS as 10.10.10.10 and 100.100.100.100 which can be seen under **Device details > System Info > Network adapters Details**, then two individual entries are added under DNS filter—10.10.10.10 and 100.100.100.100.

Support soft reset for ThinOS 9.x

Soft reset option clears all configurations except network related settings such as DNS, Wireless, Proxy, and VPN, and also the certificates. Device is unregistered from Wyse Management Suite after you use the soft reset option.

The administrator can perform soft reset on single or multiple ThinOS 9.x devices from the **Devices** page. You can also perform the function from the **Device Details** page.

Soft Reset command can be scheduled from the **Jobs** page.

New configuration user interface support for Windows 10 IoT Enterprise devices

Wyse Management Suite 4.1 supports the **WinIoT 2.x** configurations through new configuration user interface which provides enhanced user experience. The new interface includes a search function that enables you to locate configuration options easily, saving time and effort.

From Wyse Management Suite 4.1, new Windows IoT related features on the Wyse Management Suite are available under the **WinIoT 2.x** policy. If you are using the **WinIoT (Legacy WES)** policy, you will not have access to these new features.

For the public cloud environment, the new interface is applied automatically.

You must also deploy the `ConfigUISupport.exe` package in the private cloud environment to use the new interface and to ensure that the devices are recognized under the **WinIoT 2.x** policy. After you transition from **WinIoT (Legacy WES)** to **WinIoT 2.x**, you must redo all configurations.

This functionality is supported when you upgrade Wyse Device Agent to version 14.6.9.x and Wyse Easy Setup to version 2.0.0.471.

Prerequisites:

Download the following packages from the Drivers and Downloads page of Wyse Management Suite at <https://www.dell.com/support>.

- `DellApplicationStore_23.06.0.x`—Wyse Device Agent 14.6.9.x is bundled with this package.
- `ConfigUISupport.exe`

1. Log in to the Wyse Management Suite server.
2. Register the device to Wyse Management Suite and add it to a custom group.
3. Copy `DellApplicationStore_23.06.0.x` or later versions and `ConfigUISupport.exe` file to the Wyse Management Suite server local repository or remote repository under `<Repository path>\repository\thinClientApps`.

These packages can also be uploaded from **Apps & Data > Thin Client App Inventory** page

4. If files are copied under local repository or remote repository, then go to **Portal Administration > File Repository**.
5. Select the file repository and click **Sync Files**.
6. Go to **Apps & Data > App Inventory > Thin Client** and verify that the files are listed in the **Thin Client**.
7. Go to **Apps & Data > App Policies > Thin Client > Add Advanced Policy**.
8. Configure the options and select the required packages for the conversion policy in the following order:
 - `DellApplicationStore_23.06.0.x`
 - `ConfigUISupport.exe`
 Use the silent parameter **--silent** to deploy the packages.
9. Schedule and deploy the packages.

After the update, the WDA version in the **Device Details** page should be updated to 14.6.9. When you click **Create/Edit Exceptions** in the **Summary** page of **Device Details**, you should be redirected to the **WinIoT 2.x** configuration page.

User interface changes for Windows Embedded Standard devices

Dashboard and **Devices** displays all individual devices based on different operating system such as ThinOS 8.x, ThinOS 9.x, WinIoT (WES), WinIoT 2.x, Dell Hybrid Client 1.x, and Dell Hybrid Client 2.x.


The **Edit Policy** options in the **Groups & Configs** page are updated. **WES** is updated to **WinIoT (WES)**, and the new option **WinIoT 2.x** is added. Also, WES is updated to WinIoT in all the pages—**Apps & Data**, **Jobs**, **Events**, **Portal Administration**, and so on.

Delay policy execution option added for application policies for Generic clients

The administrator can select **Allow delay of Policy Execution** for Generic clients while creating standard or advanced application policy. The maximum hours per delay that can be configured is 1 to 24 hours and the maximum delays is 1 to 3 times.

On the Generic Client device, you can select the time to delay the policy from the **remind me in** drop-down option. After configuring the option, DCAE agent displays the **Update now** notification again the configured delay.

You can delay the update for a maximum of three times which is configured from the server and is displayed under the **Update notification** count.

 **NOTE:** The maximum delay is not applicable when application policy is created **Apply Policy Automatically** when you use the **Apply to New Devices** option.

ThinOS administrator password, BIOS password and deprecated protocol

ThinOS 9.x 2306 reports alerts to Wyse Management Suite 4.1 if the admin mode username and password is not set, default BIOS password not changed, or devices using deprecated cipher.

The following are the new alert types and description for ThinOS 9.x:

- **Admin Mode username and password not set**—This alert is reported when the account privileges or administrator password are not set, or privilege level is **High**.
- **Default BIOS password not changed**—This alert is reported when the BIOS password is the default password or none.
- **Devices using deprecated cipher**—This alert is reported when the network environment is not upgraded to use secure TLS ciphers.

The following are the resolution for the above alerts:

- **Admin Mode username and password not set**—Enable **Admin Mode** and set **Privilege Level** to **None** or customize in ThinOS 9.x policy under **Privacy & Security > Account Privileges**.
- **Default BIOS password not changed**—Change your BIOS password in the ThinOS 9.x policy under **Advanced > BIOS > Platform > Enable Admin Password > New BIOS Admin Password**.
- **Devices using deprecated cipher**—Update the network environment to use secure TLS ciphers.
- New device status filters are added to filter the vulnerable devices. Also, new event type filters under **Registration** section are added for new ThinOS alerts.

The following are the new event filters:

- Admin Password Not Set
- Admin Password Not Set—Resolved
- BIOS Password Not Changed
- BIOS Password Not Changed—Resolved
- Device Use Deprecated Cipher
- Device Use Deprecated Cipher—Resolved

Support for Dell Hybrid Client 2.5

The following new configurations are supported for Dell Hybrid Client 2.5 from Wyse Management Suite 4.1:

- Citrix Configuration Editor from WMS
- Citrix INI settings
- wfclient.ini settings
- module.ini settings
- All_Regions.ini settings
- wfclient.template settings
- appsrv.ini settings
- AuthManConfig.xml settings
- kbdlayoutmap.tbl settings
- Firmware/Kernel update settings
- Direct Domain Login settings
- Enhanced Inactive Timeout settings


Important notes

- Microsoft Gina should be selected when you configure keyboard layouts.
- Language pack should be pre-installed on the Windows 10 IoT Enterprise image to apply the default language configuration.
- Updating substitute keyboard layouts restarts the device twice if Microsoft Gina is enabled.
- For information about the changes or updates to the ThinOS and Dell Hybrid Client configurations, see *ThinOS 9.x Administrator's Guide and Release notes* and *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.
- If you are using Wyse Easy Setup 2.0.0.158 or earlier versions, you must upgrade Wyse Easy Setup to 2.0.0.189 after you upgrade Wyse Device Agent to 14.6.1.4.
- When the Citrix connection is deployed from Wyse Management Suite and if Citrix application is active or in use, and then the default Citrix connection cannot be launched.
- If you are an issue with Wyse Easy Setup issue after upgrading to WDA 14.6.8.1 from WDA 14.6.7.32, you must re-publish the Wyse Easy Setup configuration from Wyse Management Suite.
- From Wyse Management Suite 4.0, you can select multiple groups (up to 100 parent groups) when you create an advanced application policy. When you select multiple groups:
 - **Exceeded maximum number of groups allowed in a policy** message is displayed and the policy creation is blocked when you select more than 100 parent groups or sub-groups.
 - The administrator must select **Include sub-groups** option, if sub-groups must be included in the advanced application policy.
 - The sub-groups selection is not displayed when **Include sub-group** option is selected. However, individual jobs for all parent and sub-groups are created when the policy is scheduled.
 - The policy cannot be scheduled immediately if the total number of applicable devices are more than 25. The administrator must schedule the policy later.

Server or device agent details


Table 12. Server or device agent details

File name	Description	Version
WMS_4.1.0.536.exe	Wyse Management Suite server	4.1.0.536
WMS_Repo_4.1.0.158.exe	Wyse Management Suite repository	4.0.1.41
WDA_14.6.9.21_Unified.exe	Unified WDA for Windows 10 IoT Enterprise	14.6.9.21
DellWMS-ConfigurationUI-Package.zip	configUI_signed.zip	1.9.950
DCA_Enabler_1.7.1-61	DCA Enabler and DCA Enabler Package combined Zipped	1.7.1-61
SoftwareVaultUtility-1.5.0.0.exe	Software Vault Utility	1.5.0.0
ConfigUISupport.exe	Configuration user interface	1.0.0.3

 **NOTE:** The above-listed agents are not tested with WDM.

Windows Server configuration requirements

Table 13. Windows Server configuration requirements

Devices	Server requirements
Minimum server requirements for Wyse management Suite operations with 10,000 devices	<ul style="list-style-type: none">Supported operating systems—Windows Server 2016, and Windows Server 2019 Standard and Windows Server 2022Minimum CPU requirements—4 CPUMinimum Disk Space—40 GBMinimum Memory—8 GB <p> NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for Secure MQTT communications.</p>
Server requirement for Wyse Management Suite operations with 50,000 devices	<ul style="list-style-type: none">Supported operating systems—Windows Server 2016, and Windows Server 2019 Standard and Windows Server 2022Minimum CPU requirements—4 CPUMinimum Disk Space—120 GBMinimum Memory—16 GB
Server requirement for Wyse Management Suite operations with 120,000 devices	<ul style="list-style-type: none">Supported operating systems—Windows Server 2016, and Windows Server 2019 Standard and Windows Server 2022Minimum CPU requirements—16 CPUMinimum Disk Space—200 GBMinimum Memory—32 GB

Wyse Management Suite upgrade path

Table 14. Wyse Management Suite upgrade path

Upgrade type	Upgrade path	Compatibility
3.8 to 4.1	3.8 > 4.1	Supported
	3.8 > 3.8 Hotfix > 4.1	Supported
4.0 to 4.1	4.0 > 4.1	Supported

Table 14. Wyse Management Suite upgrade path (continued)

Upgrade type	Upgrade path	Compatibility
	4.0 > 4.0 Hotfix 1 > 4.1	Supported
	4.0 > 4.0 Hotfix 1 > 4.0 Hotfix 2 > 4.1	Supported
	4.0 > 4.0 Hotfix 1 > 4.0 Hotfix 2 > 4.0 Hotfix 3 > 4.1	Supported


Fixed issues

Table 15. Fixed issues

Issue ID	Description
WMS-883	On-premise SMTP server name does not work-which is caused by special character or name-length
WMS-872	Canceled jobs return to running status.
WMS-869	Screen saver picture settings do not allow to overwrite and difficult to find where files are applied in policy.
WMS-864	WMS 4.x length_validator error and upload the hor. view cert failed.
WMS-863	Group field is blank when text field is empty on a child group.
WMS-825	Bad credentials for AD message is displayed when password contains £ with AD user authentication
WMS-821	Remote Connections Chromium Browser does not work when applied through WMS policy.
WIN-1921	.pfx certificate do not install in system for current user and personal.
WIN-1922	Pushing files larger than 1.5 GB via advanced policy fails.
WIN-1923	.NET error is observed with latest WDA 14.6.8.1.
WIN-1929	Timeout parameter will not start from 1 min if we provide 1 min from WMS for any policy.
WMSNG-13199	Unaltered configurations which are inherited from parent are displayed as altered configurations in child group.
WMSNG-13198	Not configured values are appearing in child group when parent group parameters are changed after overriding on child group.
WMSNG-13046	Able to create multiple app policies with same name, same group, same OS type and same application.

Wyse Management Suite 4.0.0 Hotfix 3

Dell Wyse Management Suite version 4.0.0.550 Hotfix addresses issues related to parent child inheritance, DHC 2.x and legacy configuration policies, Secure SMTP configurations and email alert notifications, administrator name sorting, report privilege for different role based administrator, and implements device inventory API. For information about how to apply the Hotfix, see [Steps to apply the Hotfix](#).

 **NOTE:** It is recommended to clear the browser cache after you update Wyse Management Suite.

Compatibility

Supported Dell end-points on Wyse Management Suite

Table 16. Supported Dell end-points on Wyse Management Suite

Operating System	Platform	Wyse Device Agent versions
Windows 10 IoT Enterprise 2019 LTSC	Wyse 5070 and 5070 Extended Thin Client	10.04.06.09.19.00, 10.04.06.11.20, 10.04.06.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 Thin Client	10.04.08.09.19.00, 10.04.08.11.20, 10.04.08.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 AIO Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
Windows 10 IoT Enterprise LTSC 2021	Optiplex 3000 Thin Client	10.05.09.01.22.00 10.05.10.01.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
ThinOS	<ul style="list-style-type: none"> Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 3030 LT Thin Client (with and without PCoIP) Wyse 5040 Thin Client (ThinOS, PCoIP) Wyse 5010 Thin Client (ThinOS, PCoIP) Wyse 7010 Thin Client (with and without PCoIP) Wyse 5060 Thin Client (with and without PCoIP) 	8.5.x, 8.6.x
	<ul style="list-style-type: none"> Wyse 3040 Thin Client (with and without PCoIP) Wyse 5070 Thin Client (with and without PCoIP) Wyse 5470 Thin Client Wyse 5470 AIO Thin Client (with and without PCoIP) 	8.6.x, 9.0.x, 9.1.x, 9.3.x

Table 16. Supported Dell end-points on Wyse Management Suite (continued)

Operating System	Platform	Wyse Device Agent versions
	Optiplex 3000 Thin Client	9.1.x, 9.3.x
	Latitude 3420 Thin Client	9.3.x
Teradici	Wyse 5030 PColP zero client	5.x, 6.x, 20.x, 21.x , 22.x
	Wyse 7030 PColP zero client	
	Wyse 5050 AIO Thin Client	
Dell Hybrid Client	Wyse 5070 Thin Client	Ubuntu 18.04, 20.04, 22.04
	Wyse 5070 Extended Thin Client	Bundle—Dell Hybrid Client version 1.1, 1.1.01. 1.5, 1.6, 1.8 and 2.0
	OptiPlex 7070 Ultra	Dell Client Agent - 1.0.0, 1.1.03, 1.2.0, 1.1.1, 1.3.x, 1.4.x, 1.5.0.x, 2.0.x, and later
	OptiPlex 7090 Ultra	
	OptiPlex 3090 Ultra	
	Latitude 3320	
Dell Ubuntu (Generic) Client	OptiPlex 7070 Ultra	Ubuntu 18.04, 20.04, 22.04
	OptiPlex 7090 Ultra	DCA_Enabler - 1.0.0-72, DCA_Enabler - 1.1.0-17
	OptiPlex 3090 Ultra	DCA_Enabler - 1.2.0-25, DCA_Enabler - 1.2.1-14
	Latitude 3320	DCA_Enabler-1.3.0.23, DCA_Enabler-1.4.0.26, DCA_Enabler_1.5.0-14, DCA_Enabler_1.6.0-9, DCA_Enabler_1.7.0-x, and later
	Latitude 3420	
Wyse Converter for PCs	NA	Version: 2.1.2.141
		Wyse Device Agent: 14.6.5.9 and later
		Version: 3.0.0.4689
		Wyse Device Agent: 14.6.6.3, and 14.6.8.x

- NOTE:** WDA version 14.6.3.1 and older versions can only be downgraded from WMS. Manual downgrade of WDA on the device is not supported. If you manually downgrade WDA, then the WMS information is lost, and you cannot upgrade WDA upgrades later. To overcome the issue, WDA must be uninstalled manually, and installed again.
- NOTE:** WDA 14.6.8.x is not supported for Wyse Device Manager. If you downgrade the agent from 14.6.8.x to older versions HA Agent Services are not restored. The administrator of the client must manually uninstall and install the desired WDA.

Supported browsers

Table 17. Supported browsers

Browsers	Version
Chrome	110.0.5481.104 and later
Firefox	102.8.0 and later
Edge browser	110.0.1587.50

- NOTE:** WMS Portal is no more supported on Microsoft Internet Explorer as The Internet Explorer 11 desktop application is retired on June 15, 2022. For more information, see *Internet Explorer 11 desktop app support ended for certain versions of Windows 10* at <https://docs.microsoft.com/>.

Supported operating system matrix

Table 18. Supported operating systems

Operating system	WMS server	WMS repository	Remote database
Windows Server 2012 R2 English	Supported	Supported	Supported
Windows Server 2012 R2 French	Supported	Supported	Not supported
Windows Server 2012 R2 Italian	Supported	Supported	Not supported
Windows Server 2012 R2 German	Supported	Supported	Not supported
Windows Server 2012 R2 Spanish	Supported	Supported	Not supported
Windows Server 2012 R2 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2012 R2 Japanese	Supported	Supported	Not supported
Windows Server 2016 English	Supported	Supported	Supported
Windows Server 2016 French	Supported	Supported	Not supported
Windows Server 2016 Italian	Supported	Supported	Not supported
Windows Server 2016 German	Supported	Supported	Not supported
Windows Server 2016 Spanish	Supported	Supported	Not supported
Windows Server 2016Simplified Chinese	Supported	Supported	Not supported
Windows Server 2016 Japanese	Supported	Supported	Not supported
Windows Server 2019 Standard English	Supported	Supported	Supported
Windows Server 2019 French	Supported	Supported	Not supported
Windows Server 2019 Italian	Supported	Supported	Not supported
Windows Server 2019 German	Supported	Supported	Not supported
Windows Server 2019 Spanish	Supported	Supported	Not supported
Windows Server 2019 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2019 Japanese	Supported	Supported	Not supported

Important notes


- Microsoft Gina should be selected when you configure keyboard layouts.
- Language pack should be pre-installed on the Windows 10 IoT Enterprise image to apply the default language configuration.
- Updating substitute keyboard layouts restarts the device twice if Microsoft Gina is enabled.
- For information about the changes or updates to the ThinOS and Dell Hybrid Client configurations, see *ThinOS 9.x Administrator's Guide and Release notes* and *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.
- If you are using Wyse Easy Setup 2.0.0.158 or earlier versions, you must upgrade Wyse Easy Setup to 2.0.0.189 after you upgrade Wyse Device Agent to 14.6.1.4.
- When the Citrix connection is deployed from Wyse Management Suite and if Citrix application is active or in use, and then the default Citrix connection cannot be launched.
- If you are an issue with Wyse Easy Setup issue after upgrading to WDA 14.6.8.1 from WDA 14.6.7.32, you must re-publish the Wyse Easy Setup configuration from Wyse Management Suite.
- From Wyse Management Suite 4.0, you can select multiple groups (up to 100 parent groups) when you create an advanced application policy. When you select multiple groups:
 - **Exceeded maximum number of groups allowed in a policy** message is displayed and the policy creation is blocked when you select more than 100 parent groups or sub-groups.

- The administrator must select **Include sub-groups** option, if sub-groups must be included in the advanced application policy.
- The sub-groups selection is not displayed when **Include sub-group** option is selected. However, individual jobs for all parent and sub-groups are created when the policy is scheduled.
- The policy cannot be scheduled immediately if the total number of applicable devices are more than 25. The administrator must schedule the policy later.

Server or device agent details


Table 19. Server or device agent details

File name	Description	Version
WMS_Hotfix_4.0.0.550.exe	Wyse Management Suite server	4.0.0.550
WMS_Repo.exe	Wyse Management Suite repository	4.0.1.41
WDA_14.6.8.1_Unified.exe	Unified WDA for Windows 10 IoT Enterprise	14.6.8.1
DellWMS-ConfigurationUI-Package.zip	configUI_signed.zip	1.9.532
WMS_Import_Tool.exe	Wyse Management Suite Import Tool	1.7.5.176
DCA_Enabler_1.6.0-9.zip	DCA Enabler and DCA Enabler Package combined Zipped	1.7.0-20
SoftwareVaultUtility-1.4.0.0.exe	Software Vault Utility	1.4.0.0

 **NOTE:** The above-listed agents are not tested with WDM.

Windows Server configuration requirements

Table 20. Windows Server configuration requirements

Devices	Server requirements
Minimum server requirements for Wyse management Suite operations with 10,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—4 CPU • Minimum Disk Space—40 GB • Minimum Memory—8 GB <p> NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for Secure MQTT communications.</p>
Server requirement for Wyse Management Suite operations with 50,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—4 CPU • Minimum Disk Space—120 GB • Minimum Memory—16 GB
Server requirement for Wyse Management Suite operations with 120,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—16 CPU • Minimum Disk Space—200 GB • Minimum Memory—32 GB

Wyse Management Suite upgrade path

Dell Wyse Management Suite version 4.0.0.550 Hotfix can only be upgraded from version 4.0.0-526 and 4.0.0.540.

Steps to apply the Hotfix

1. Download the Hotfix from <https://www.dell.com/support/home/> based on the Wyse Management Suite version.
2. Double-click the .exe file to begin the Hotfix installation.
3. Click **Next** and then click **Install** to initiate the Hotfix installation.
4. After the installation is complete, click **Finish**.

After Hotfix is successfully installed, the registry value can be seen with the Hotfix version at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WMS\Hotfix`.

The Hotfix logs can be found under `C:\ProgramData\DELL\WMS\Hostfix` with name `WMS_Hostfix-Date&Time`.


Fixed issues

Table 21. Fixed issues

Issue ID	Description
WMSNG-13233	Optimized handling of the application load for better performance.
WMSNG-13337	Fixed the issue related to the invalid username in File replication events.

Wyse Management Suite 4.0.0 Hotfix 2

Dell Wyse Management Suite version 4.0.0.547 Hotfix addresses issues related to parent child inheritance, DHC 2.x and legacy configuration policies, Secure SMTP configurations and email alert notifications, administrator name sorting, report privilege for different role based administrator, and implements device inventory API. For information about how to apply the Hotfix, see [Steps to apply the Hotfix](#).

 **NOTE:** It is recommended to clear the browser cache after you update Wyse Management Suite.

Compatibility

Supported Dell end-points on Wyse Management Suite

Table 22. Supported Dell end-points on Wyse Management Suite

Operating System	Platform	Wyse Device Agent versions
Windows 10 IoT Enterprise 2019 LTSC	Wyse 5070 and 5070 Extended Thin Client	10.04.06.09.19.00, 10.04.06.11.20, 10.04.06.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 Thin Client	10.04.08.09.19.00, 10.04.08.11.20, 10.04.08.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 AIO Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
Windows 10 IoT Enterprise LTSC 2021	Optiplex 3000 Thin Client	10.05.09.01.22.00 10.05.10.01.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
ThinOS	<ul style="list-style-type: none"> Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 3030 LT Thin Client (with and without PCoIP) Wyse 5040 Thin Client (ThinOS, PCoIP) Wyse 5010 Thin Client (ThinOS, PCoIP) Wyse 7010 Thin Client (with and without PCoIP) Wyse 5060 Thin Client (with and without PCoIP) 	8.5.x, 8.6.x
	<ul style="list-style-type: none"> Wyse 3040 Thin Client (with and without PCoIP) Wyse 5070 Thin Client (with and without PCoIP) Wyse 5470 Thin Client Wyse 5470 AIO Thin Client (with and without PCoIP) 	8.6.x, 9.0.x, 9.1.x, 9.3.x

Table 22. Supported Dell end-points on Wyse Management Suite (continued)

Operating System	Platform	Wyse Device Agent versions
	Optiplex 3000 Thin Client	9.1.x, 9.3.x
	Latitude 3420 Thin Client	9.3.x
Teradici	Wyse 5030 PColP zero client	5.x, 6.x, 20.x, 21.x, 22.x
	Wyse 7030 PColP zero client	
	Wyse 5050 AIO Thin Client	
Dell Hybrid Client	Wyse 5070 Thin Client	Ubuntu 18.04, 20.04, 22.04
	Wyse 5070 Extended Thin Client	Bundle—Dell Hybrid Client version 1.1, 1.1.01, 1.5, 1.6, 1.8 and 2.0
	OptiPlex 7070 Ultra	Dell Client Agent - 1.0.0, 1.1.03, 1.2.0, 1.1.1, 1.3.x, 1.4.x, 1.5.0.x, 2.0.x, and later
	OptiPlex 7090 Ultra	
	OptiPlex 3090 Ultra	
	Latitude 3320	
Dell Ubuntu (Generic) Client	OptiPlex 7070 Ultra	Ubuntu 18.04, 20.04, 22.04
	OptiPlex 7090 Ultra	DCA_Enabler - 1.0.0-72, DCA_Enabler - 1.1.0-17
	OptiPlex 3090 Ultra	DCA_Enabler - 1.2.0-25, DCA_Enabler - 1.2.1-14
	Latitude 3320	DCA_Enabler-1.3.0.23, DCA_Enabler-1.4.0.26, DCA_Enabler_1.5.0-14, DCA_Enabler_1.6.0-9, DCA_Enabler_1.7.0-x, and later
	Latitude 3420	
Wyse Converter for PCs	NA	Version: 2.1.2.141
		Wyse Device Agent: 14.6.5.9 and later
		Version: 3.0.0.4689
		Wyse Device Agent: 14.6.6.3, and 14.6.8.x

- NOTE:** WDA version 14.6.3.1 and older versions can only be downgraded from WMS. Manual downgrade of WDA on the device is not supported. If you manually downgrade WDA, then the WMS information is lost, and you cannot upgrade WDA upgrades later. To overcome the issue, WDA must be uninstalled manually, and installed again.
- NOTE:** WDA 14.6.8.x is not supported for Wyse Device Manager. If you downgrade the agent from 14.6.8.x to older versions HA Agent Services are not restored. The administrator of the client must manually uninstall and install the desired WDA.

Supported browsers

Table 23. Supported browsers

Browsers	Version
Chrome	107.0.5304.107 and later
Firefox	102.4.0 and later
Edge browser	107.0.1418.42

- NOTE:** WMS Portal is no more supported on Microsoft Internet Explorer as The Internet Explorer 11 desktop application is retired on June 15, 2022. For more information, see *Internet Explorer 11 desktop app support ended for certain versions of Windows 10* at <https://docs.microsoft.com/>.

Supported operating system matrix

Table 24. Supported operating systems

Operating system	WMS server	WMS repository	Remote database
Windows Server 2012 R2 English	Supported	Supported	Supported
Windows Server 2012 R2 French	Supported	Supported	Not supported
Windows Server 2012 R2 Italian	Supported	Supported	Not supported
Windows Server 2012 R2 German	Supported	Supported	Not supported
Windows Server 2012 R2 Spanish	Supported	Supported	Not supported
Windows Server 2012 R2 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2012 R2 Japanese	Supported	Supported	Not supported
Windows Server 2016 English	Supported	Supported	Supported
Windows Server 2016 French	Supported	Supported	Not supported
Windows Server 2016 Italian	Supported	Supported	Not supported
Windows Server 2016 German	Supported	Supported	Not supported
Windows Server 2016 Spanish	Supported	Supported	Not supported
Windows Server 2016Simplified Chinese	Supported	Supported	Not supported
Windows Server 2016 Japanese	Supported	Supported	Not supported
Windows Server 2019 Standard English	Supported	Supported	Supported
Windows Server 2019 French	Supported	Supported	Not supported
Windows Server 2019 Italian	Supported	Supported	Not supported
Windows Server 2019 German	Supported	Supported	Not supported
Windows Server 2019 Spanish	Supported	Supported	Not supported
Windows Server 2019 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2019 Japanese	Supported	Supported	Not supported

Important notes


- Microsoft Gina should be selected when you configure keyboard layouts.
- Language pack should be pre-installed on the Windows 10 IoT Enterprise image to apply the default language configuration.
- Updating substitute keyboard layouts restarts the device twice if Microsoft Gina is enabled.
- For information about the changes or updates to the ThinOS and Dell Hybrid Client configurations, see *ThinOS 9.x Administrator's Guide and Release notes* and *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.
- If you are using Wyse Easy Setup 2.0.0.158 or earlier versions, you must upgrade Wyse Easy Setup to 2.0.0.189 after you upgrade Wyse Device Agent to 14.6.1.4.
- When the Citrix connection is deployed from Wyse Management Suite and if Citrix application is active or in use, and then the default Citrix connection cannot be launched.
- If you are an issue with Wyse Easy Setup issue after upgrading to WDA 14.6.8.1 from WDA 14.6.7.32, you must re-publish the Wyse Easy Setup configuration from Wyse Management Suite.
- From Wyse Management Suite 4.0, you can select multiple groups (up to 100 parent groups) when you create an advanced application policy. When you select multiple groups:
 - **Exceeded maximum number of groups allowed in a policy** message is displayed and the policy creation is blocked when you select more than 100 parent groups or sub-groups.

- The administrator must select **Include sub-groups** option, if sub-groups must be included in the advanced application policy.
- The sub-groups selection is not displayed when **Include sub-group** option is selected. However, individual jobs for all parent and sub-groups are created when the policy is scheduled.
- The policy cannot be scheduled immediately if the total number of applicable devices are more than 25. The administrator must schedule the policy later.

Server or device agent details


Table 25. Server or device agent details

File name	Description	Version
WMS_Hotfix_4.0.0.547.exe	Wyse Management Suite server	4.0.0.547
WMS_Repo.exe	Wyse Management Suite repository	4.0.1.41
WDA_14.6.8.1_Unified.exe	Unified WDA for Windows 10 IoT Enterprise	14.6.8.1
DellWMS-ConfigurationUI-Package.zip	configUI_signed.zip	1.9.532
WMS_Import_Tool.exe	Wyse Management Suite Import Tool	1.7.5.176
DCA_Enabler_1.6.0-9.zip	DCA Enabler and DCA Enabler Package combined Zipped	1.7.0-20
SoftwareVaultUtility-1.4.0.0.exe	Software Vault Utility	1.4.0.0

 **NOTE:** The above-listed agents are not tested with WDM.

Windows Server configuration requirements

Table 26. Windows Server configuration requirements

Devices	Server requirements
Minimum server requirements for Wyse management Suite operations with 10,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—4 CPU • Minimum Disk Space—40 GB • Minimum Memory—8 GB <p> NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for Secure MQTT communications.</p>
Server requirement for Wyse Management Suite operations with 50,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—4 CPU • Minimum Disk Space—120 GB • Minimum Memory—16 GB
Server requirement for Wyse Management Suite operations with 120,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—16 CPU • Minimum Disk Space—200 GB • Minimum Memory—32 GB

Wyse Management Suite upgrade path

Dell Wyse Management Suite version 4.0.0.547 Hotfix can only be upgraded from version 4.0.0-526 and 4.0.0.540.

Steps to apply the Hotfix

1. Download the Hotfix from <https://www.dell.com/support/home/> based on the Wyse Management Suite version.
2. Double-click the .exe file to begin the Hotfix installation.
3. Click **Next** and then click **Install** to initiate the Hotfix installation.
4. After the installation is complete, click **Finish**.

After Hotfix is successfully installed, the registry value can be seen with the Hotfix version at `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WMS\Hotfix`.

The Hotfix logs can be found under `C:\ProgramData\DELL\WMS\Hostfix` with name `WMS_Hostfix-Date&Time`.

Fixed issues

Table 27. Fixed issues


Issue ID	Description
WMS-850	Firmware information is empty when you hide inherited items.
WMS-847	After upgrading to 4.0 HF, you cannot save DHC 2.0 policy with a trial license.
WMS-842	Parent-child inheritance is broken when a policy is changed.
WMS-841	Filtering administrators by Name column causes an Internal error.
WMS-833	After upgrading to 4.0 version, existing landscape configuration policy in Wyse Management Suite displays a validation error.
WMS-824	Server interrupts download of Device Export to CSV.
WMS-815	On-premise SMTP for email alerts do not work.
WMS-785	Customer unable to receive email Alerts with rules from Wyse Management Suite.

NOTE:

- Policies configured in child group must be reset and configured again, as there could be mismatch of earlier configurations in database (WMS-842).
- Previously generated Devices Report cannot be downloaded by the administrators who do not have the report privilege. The administrator must dismiss the older UI notification manually that is generated before HF2 update (WMS-824).

Wyse Management Suite 4.0.0 Hotfix

Dell Wyse Management Suite version 4.0.0.540 Hotfix addresses issues related to scheduling application and image policy, multi selection of device groups with **Include Sub-Groups** option, and device level configuration. For information about how to apply the Hotfix, see [Steps to apply the Hotfix](#).

 **NOTE:** It is recommended to clear the browser cache after you update Wyse Management Suite.

Compatibility

Supported Dell end-points on Wyse Management Suite

Table 28. Supported Dell end-points on Wyse Management Suite

Operating System	Platform	Wyse Device Agent versions
Windows 10 IoT Enterprise 2019 LTSC	Wyse 5070 and 5070 Extended Thin Client	10.04.06.09.19.00, 10.04.06.11.20, 10.04.06.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 Thin Client	10.04.08.09.19.00, 10.04.08.11.20, 10.04.08.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 AIO Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
Windows 10 IoT Enterprise LTSC 2021	Optiplex 3000 Thin Client	10.05.09.01.22.00 10.05.10.01.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
ThinOS	<ul style="list-style-type: none"> Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 3030 LT Thin Client (with and without PCoIP) Wyse 5040 Thin Client (ThinOS, PCoIP) Wyse 5010 Thin Client (ThinOS, PCoIP) Wyse 7010 Thin Client (with and without PCoIP) Wyse 5060 Thin Client (with and without PCoIP) 	8.5.x, 8.6.x
	<ul style="list-style-type: none"> Wyse 3040 Thin Client (with and without PCoIP) Wyse 5070 Thin Client (with and without PCoIP) Wyse 5470 Thin Client Wyse 5470 AIO Thin Client (with and without PCoIP) 	8.6.x, 9.0.x, 9.1.x, 9.3.x

Table 28. Supported Dell end-points on Wyse Management Suite (continued)

Operating System	Platform	Wyse Device Agent versions
Teradici	Optiplex 3000 Thin Client	9.1.x, 9.3.x
	Latitude 3420 Thin Client	9.3.x
	Wyse 5030 PColP zero client Wyse 7030 PColP zero client Wyse 5050 AIO Thin Client	5.x, 6.x, 20.x, 21.x, 22.x
Dell Hybrid Client	Wyse 5070 Thin Client	Ubuntu 18.04, 20.04, 22.04
	Wyse 5070 Extended Thin Client	Bundle—Dell Hybrid Client version 1.1, 1.1.01, 1.5, 1.6, 1.8 and 2.0
	OptiPlex 7070 Ultra OptiPlex 7090 Ultra OptiPlex 3090 Ultra Latitude 3320	Dell Client Agent - 1.0.0, 1.1.03, 1.2.0, 1.1.1, 1.3.x, 1.4.x, 1.5.0.x, 2.0.x, and later
Dell Ubuntu (Generic) Client	OptiPlex 7070 Ultra	Ubuntu 18.04, 20.04, 22.04
	OptiPlex 7090 Ultra	DCA_Enabler - 1.0.0-72, DCA_Enabler - 1.1.0-17
	OptiPlex 3090 Ultra Latitude 3320 Latitude 3420	DCA_Enabler - 1.2.0-25, DCA_Enabler - 1.2.1-14 DCA_Enabler-1.3.0.23, DCA_Enabler-1.4.0.26, DCA_Enabler_1.5.0-14, DCA_Enabler_1.6.0-9, DCA_Enabler_1.7.0-x, and later
Wyse Converter for PCs	NA	Version: 2.1.2.141 Wyse Device Agent: 14.6.5.9 and later Version: 3.0.0.4689 Wyse Device Agent: 14.6.6.3, and 14.6.8.x

- NOTE:** WDA version 14.6.3.1 and older versions can only be downgraded from WMS. Manual downgrade of WDA on the device is not supported. If you manually downgrade WDA, then the WMS information is lost, and you cannot upgrade WDA upgrades later. To overcome the issue, WDA must be uninstalled manually, and installed again.
- NOTE:** WDA 14.6.8.x is not supported for Wyse Device Manager. If you downgrade the agent from 14.6.8.x to older versions HA Agent Services are not restored. The administrator of the client must manually uninstall and install the desired WDA.

Supported browsers

Table 29. Supported browsers

Browsers	Version
Chrome	107.0.5304.107 and later
Firefox	102.4.0 and later
Edge browser	107.0.1418.42

- NOTE:** WMS Portal is no more supported on Microsoft Internet Explorer as The Internet Explorer 11 desktop application is retired on June 15, 2022. For more information, see *Internet Explorer 11 desktop app support ended for certain versions of Windows 10* at <https://docs.microsoft.com/>.

Supported operating system matrix

Table 30. Supported operating systems

Operating system	WMS server	WMS repository	Remote database
Windows Server 2012 R2 English	Supported	Supported	Supported
Windows Server 2012 R2 French	Supported	Supported	Not supported
Windows Server 2012 R2 Italian	Supported	Supported	Not supported
Windows Server 2012 R2 German	Supported	Supported	Not supported
Windows Server 2012 R2 Spanish	Supported	Supported	Not supported
Windows Server 2012 R2 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2012 R2 Japanese	Supported	Supported	Not supported
Windows Server 2016 English	Supported	Supported	Supported
Windows Server 2016 French	Supported	Supported	Not supported
Windows Server 2016 Italian	Supported	Supported	Not supported
Windows Server 2016 German	Supported	Supported	Not supported
Windows Server 2016 Spanish	Supported	Supported	Not supported
Windows Server 2016 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2016 Japanese	Supported	Supported	Not supported
Windows Server 2019 Standard English	Supported	Supported	Supported
Windows Server 2019 French	Supported	Supported	Not supported
Windows Server 2019 Italian	Supported	Supported	Not supported
Windows Server 2019 German	Supported	Supported	Not supported
Windows Server 2019 Spanish	Supported	Supported	Not supported
Windows Server 2019 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2019 Japanese	Supported	Supported	Not supported

Important notes


- Microsoft Gina should be selected when you configure keyboard layouts.
- Language pack should be pre-installed on the Windows 10 IoT Enterprise image to apply the default language configuration.
- Updating substitute keyboard layouts restarts the device twice if Microsoft Gina is enabled.
- For information about the changes or updates to the ThinOS and Dell Hybrid Client configurations, see *ThinOS 9.x Administrator's Guide and Release notes* and *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.
- If you are using Wyse Easy Setup 2.0.0.158 or earlier versions, you must upgrade Wyse Easy Setup to 2.0.0.189 after you upgrade Wyse Device Agent to 14.6.1.4.
- When the Citrix connection is deployed from Wyse Management Suite and if Citrix application is active or in use, and then the default Citrix connection cannot be launched.
- If you are an issue with Wyse Easy Setup issue after upgrading to WDA 14.6.8.1 from WDA 14.6.7.32, you must re-publish the Wyse Easy Setup configuration from Wyse Management Suite.
- From Wyse Management Suite 4.0, you can select multiple groups (up to 100 parent groups) when you create an advanced application policy. When you select multiple groups:
 - **Exceeded maximum number of groups allowed in a policy** message is displayed and the policy creation is blocked when you select more than 100 parent groups or sub-groups.

- The administrator must select **Include sub-groups** option, if sub-groups must be included in the advanced application policy.
- The sub-groups selection is not displayed when **Include sub-group** option is selected. However, individual jobs for all parent and sub-groups are created when the policy is scheduled.
- The policy cannot be scheduled immediately if the total number of applicable devices are more than 25. The administrator must schedule the policy later.

Server or device agent details


Table 31. Server or device agent details

File name	Description	Version
WMS_Hotfix_4.0.0.540.exe	Wyse Management Suite server	4.0.0.540
WMS_Repo.exe	Wyse Management Suite repository	4.0.1.41
WDA_14.6.8.1_Unified.exe	Unified WDA for Windows 10 IoT Enterprise	14.6.8.1
DellWMS-ConfigurationUI-Package.zip	configUI_signed.zip	1.9.532
WMS_Import_Tool.exe	Wyse Management Suite Import Tool	1.7.5.176
DCA_Enabler_1.6.0-9.zip	DCA Enabler and DCA Enabler Package combined Zipped	1.7.0-20
SoftwareVaultUtility-1.4.0.0.exe	Software Vault Utility	1.4.0.0

 **NOTE:** The above-listed agents are not tested with WDM.

Windows Server configuration requirements

Table 32. Windows Server configuration requirements

Devices	Server requirements
Minimum server requirements for Wyse management Suite operations with 10,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—4 CPU • Minimum Disk Space—40 GB • Minimum Memory—8 GB <p> NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for Secure MQTT communications.</p>
Server requirement for Wyse Management Suite operations with 50,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—4 CPU • Minimum Disk Space—120 GB • Minimum Memory—16 GB
Server requirement for Wyse Management Suite operations with 120,000 devices	<ul style="list-style-type: none"> • Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard • Minimum CPU requirements—16 CPU • Minimum Disk Space—200 GB • Minimum Memory—32 GB

Wyse Management Suite upgrade path

Dell Wyse Management Suite version 4.0.0.540 Hotfix can only be upgraded from version 4.0.0-526.

Steps to apply the Hotfix

1. Download the Hotfix from <https://www.dell.com/support/home/> based on the Wyse Management Suite version.
2. Double-click the .exe file to begin the Hotfix installation.
3. Click **Next** and then click **Install** to initiate the Hotfix installation.
4. After the installation is complete, click **Finish**.

After Hotfix is successfully installed, the registry value can be seen with the Hotfix version at
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WMS\Hotfix.

The Hotfix logs can be found under C:\ProgramData\DELL\WMS\Hostfix with name WMS_Hostfix-Date&Time.

Fixed issues

Table 33. Fixed issues

Issue ID	Description
WMS-823, WMS-830	Failure to configure device level exception.
WMSNG-12904	Unable to schedule application and image policy from Devices page.
WMS-828, WMS-832	Failure to upgrade Wyse Management Suite repository upgrade.

Wyse Management Suite 4.0

Compatibility

Supported Dell end-points on Wyse Management Suite

Table 34. Supported Dell end-points on Wyse Management Suite

Operating System	Platform	Wyse Device Agent versions
Windows 10 IoT Enterprise 2019 LTSC	Wyse 5070 and 5070 Extended Thin Client	10.04.06.09.19.00, 10.04.06.11.20, 10.04.06.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 Thin Client	10.04.08.09.19.00, 10.04.08.11.20, 10.04.08.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
	Wyse 5470 AIO Thin Client	10.04.07.09.19.00, 10.04.07.11.20, 10.04.07.06.21.00, 10.04.06.05.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
Windows 10 IoT Enterprise LTSC 2021	Optiplex 3000 Thin Client	10.05.09.01.22.00 10.05.10.01.22.00, 10.04.XX.05.22.00 Wyse Device Agent: 14.6.5.9, 14.6.8.x, and later
ThinOS	<ul style="list-style-type: none"> Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 3030 LT Thin Client (with and without PColP) Wyse 5040 Thin Client (ThinOS, PColP) Wyse 5010 Thin Client (ThinOS, PColP) Wyse 7010 Thin Client (with and without PColP) Wyse 5060 Thin Client (with and without PColP) 	8.5.x, 8.6.x
	<ul style="list-style-type: none"> Wyse 3040 Thin Client (with and without PColP) Wyse 5070 Thin Client (with and without PColP) Wyse 5470 Thin Client Wyse 5470 AIO Thin Client (with and without PColP) 	8.6.x, 9.0.x, 9.1.x, 9.3.x
	Optiplex 3000 Thin Client	9.1.x, 9.3.x
	Latitude 3420 Thin Client	9.3.x
Teradici	Wyse 5030 PColP zero client	5.x, 6.x, 20.x, 21.x, 22.x
	Wyse 7030 PColP zero client	

Table 34. Supported Dell end-points on Wyse Management Suite (continued)

Operating System	Platform	Wyse Device Agent versions
	Wyse 5050 AIO Thin Client	
Dell Hybrid Client	Wyse 5070 Thin Client	Ubuntu 18.04, 20.04, 22.04
	Wyse 5070 Extended Thin Client	Bundle—Dell Hybrid Client version 1.1, 1.1.01. 1.5, 1.6, 1.8 and 2.0
	OptiPlex 7070 Ultra OptiPlex 7090 Ultra OptiPlex 3090 Ultra Latitude 3320	Dell Client Agent - 1.0.0, 1.1.03, 1.2.0, 1.1.1, 1.3.x, 1.4.x, 1.5.0.x, 2.0.x, and later
Dell Ubuntu (Generic) Client	OptiPlex 7070 Ultra OptiPlex 7090 Ultra OptiPlex 3090 Ultra Latitude 3320 Latitude 3420	Ubuntu 18.04, 20.04, 22.04 DCA_Enabler - 1.0.0-72, DCA_Enabler - 1.1.0-17 DCA_Enabler - 1.2.0-25, DCA_Enabler - 1.2.1-14 DCA_Enabler-1.3.0.23, DCA_Enabler-1.4.0.26, DCA_Enabler_1.5.0-14, DCA_Enabler_1.6.0-9, DCA_Enabler_1.7.0-x, and later
Wyse Converter for PCs	NA	Version: 2.1.2.141 Wyse Device Agent: 14.6.5.9 and later Version: 3.0.0.4689 Wyse Device Agent: 14.6.6.3, and 14.6.8.x

- NOTE:** WDA version 14.6.3.1 and older versions can only be downgraded from WMS. Manual downgrade of WDA on the device is not supported. If you manually downgrade WDA, then the WMS information is lost, and you cannot upgrade WDA upgrades later. To overcome the issue, WDA must be uninstalled manually, and installed again.
- NOTE:** WDA 14.6.8.x is not supported for Wyse Device Manager. If you downgrade the agent from 14.6.8.x to older versions HA Agent Services are not restored. The administrator of the client must manually uninstall and install the desired WDA.

Supported browsers

Table 35. Supported browsers

Browsers	Version
Chrome	107.0.5304.107 and later
Firefox	102.4.0 and later
Edge browser	107.0.1418.42

- NOTE:** WMS Portal is no more supported on Microsoft Internet Explorer as The Internet Explorer 11 desktop application is retired on June 15, 2022. For more information, see *Internet Explorer 11 desktop app support ended for certain versions of Windows 10* at <https://docs.microsoft.com/>.

Supported operating system matrix

Table 36. Supported operating systems

Operating system	WMS server	WMS repository	Remote database
Windows Server 2012 R2 English	Supported	Supported	Supported

Table 36. Supported operating systems (continued)

Operating system	WMS server	WMS repository	Remote database
Windows Server 2012 R2 French	Supported	Supported	Not supported
Windows Server 2012 R2 Italian	Supported	Supported	Not supported
Windows Server 2012 R2 German	Supported	Supported	Not supported
Windows Server 2012 R2 Spanish	Supported	Supported	Not supported
Windows Server 2012 R2 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2012 R2 Japanese	Supported	Supported	Not supported
Windows Server 2016 English	Supported	Supported	Supported
Windows Server 2016 French	Supported	Supported	Not supported
Windows Server 2016 Italian	Supported	Supported	Not supported
Windows Server 2016 German	Supported	Supported	Not supported
Windows Server 2016 Spanish	Supported	Supported	Not supported
Windows Server 2016Simplified Chinese	Supported	Supported	Not supported
Windows Server 2016 Japanese	Supported	Supported	Not supported
Windows Server 2019 Standard English	Supported	Supported	Supported
Windows Server 2019 French	Supported	Supported	Not supported
Windows Server 2019 Italian	Supported	Supported	Not supported
Windows Server 2019 German	Supported	Supported	Not supported
Windows Server 2019 Spanish	Supported	Supported	Not supported
Windows Server 2019 Simplified Chinese	Supported	Supported	Not supported
Windows Server 2019 Japanese	Supported	Supported	Not supported

New and enhanced features

Vulnerable devices displayed on the dashboard

A count indicating security compliance and an alert along with the security resolution link are visible on the dashboard, along with a list of all registered devices that contain a vulnerable hash.

The devices using MD5 and Sha1 as Hashing algorithm are considered as non compliant. The Authentication code is updated from MD5 to SHA3-512, and File checksum is updated from SHA-1 to SHA3-512.

New filters are added:

- In the **Devices** page, go to **Status > Non-Compliant** to filter out devices by type, such as non-compliant with respect to vulnerable hash, device that is not checked in, DHC system password that is not changed, or DHC BIOS password not changed.
- In the **Events** page, go to **Event Type > Registration** to filter **Device use Vulnerable Hash** and **Device use Vulnerable Hash Resolved events**.

You can also filter these devices when you generate a report.

There are new columns that are added in the device report for details such as security compliance status and the reason for noncompliance.

Table 37. Vulnerable versions and the updated versions of the operating systems

Operating system	Vulnerable version	Updated version
ThinOS 8.x	8.6-807 and earlier versions	8.6-810 and later versions
ThinOS 9.x	9.1.6108 and earlier versions	9.3.1129 and later versions
Windows Embedded Standard	Dell Wyse Device Agent version 14.5.5.5 and earlier versions	14.6.0.27 and later versions
Dell Hybrid Client	1.5 and earlier versions	1.6 and later versions

After the update, the new agent or firmware use SHA3-512 Hashing algorithm.

After the server is updated to a new version, the vulnerable devices are displayed as non-compliant when the devices check-in to Wyse Management Suite.

Wyse Management Suite repository enhancements and optimizations

Wyse Management Suite (WMS) administrator can select a location as their preferred repository in **Portal Admin > File Repository > Subnet mapping**. When the preferred repository is selected, the same repository is considered for download from configured subnets. Fall-back does not occur until the repository is offline. The WMS administrator can view the preferred repository setting in the **File Repository Page**.

WMS administrator can map up to 100 subnet values or 100 subnet ranges in **File Repository > Subnet Mapping**.

Scenario 1: Multiple repositories available with no subnet mapped or configured.

- The server provides the Dell Wyse Device Agent with a list of available repositories.
- The Dell Wyse Device Agent runs a test connection for all the repository URLs provided by the server and discards the failed repositories.
- The Dell Wyse Device Agent selects repositories for which the test connection is successful and completes the download from the closest subnet repository.
- If the administrator has two repositories in the same subnet, a test connection is performed, and the fastest repository is selected for download.

Scenario 2: Preferred Repository option is not selected while configuring subnets.

- For application download, the Dell Wyse Device Agent obtains a list of repository URLs, and configured subnets for each repository.
- The Dell Wyse Device Agent checks all the URLs for repositories that are provided by the server. Any repositories where the test connection failed are ignored.
- The Dell Wyse Device Agent selects repositories for which the test connection is successful and completes the download from the mapped subnet repository.
- If the mapped subnets repository is not available, the Dell Wyse Device Agent falls back to other available repositories.



Scenario 3: Preferred Repository option is selected while configuring subnets.

- The WMS server provides the repository list and specified subnets to the Dell Wyse Device Agent.
- The Dell Wyse Device Agent checks all the URLs for repositories that are provided by the server. Any repositories where the test connection failed are ignored.
- The repository with the value preferred repository true is selected for download.
- If the test connection to the preferred repository succeeds, the download does not resort to any other repositories.
- The Dell Wyse Device Agent uses subnet mapping to try alternative repositories when the test connection to the preferred repository fails.

Table 38. Summary of scenarios

Scenario	Repo is Online (Available)	Repo is Online but Busy	Repo is Offline (Not Reachable)
No-Subnet-Mapping	Device calculates nearest repository.	Fall-Back	Fall-Back
Subnet-Mapping	Device goes with mapping send from server.	Fall-Back	Fall-Back

Table 38. Summary of scenarios (continued)

Scenario	Repo is Online (Available)	Repo is Online but Busy	Repo is Offline (Not Reachable)
Same Subnet-Mapped with Multiple Repos	Device picks the repository which is based on configured weight.	Fall-Back to next priority in mapping.	Fall-Back to next priority in mapping.
Subnet Mapping with preferred repository	Device sticks to one repository.	No Fall-Back  NOTE: The download attempt is retried 30 times before the job is terminated.	Fall-Back  NOTE: The fallback occurs instantly, and the preferred repository is not downloaded.


Dynamic maximum concurrent download based on system configuration

The maximum allowed concurrent downloads are automatically determined by Wyse Management Suite (WMS) Server 4.0 which is based on the current system configuration. WMS Repository further sets the maximum allowed concurrent downloads value that is based on the system memory (RAM) and communicates this information to WMS Server upon check-in.

The number of concurrent file downloads can be modified in **Portal Administration > File Repository > Edit Repository UI**, using the text box, which was formerly a drop-down menu. The value can be anywhere from 1 to the maximum allowed number of concurrent downloads.

Table 39. WMS server RAM and maximum concurrent download


RAM	Tomcat Heap Memory	Max Allowed Concurrent Downloads
8 GB	3 GB	300
16 GB	6 GB	600
32 GB	12 GB	1200

 **NOTE:** The maximum allowed concurrent downloads displays 100 when an older version of WMS repository is registered to WMS 4.0. Once WMS repository is updated to version 4.0, the proper count for the maximum allowed concurrent downloads is displayed.

Update Max concurrent downloads for repository and restart tomcat Service

Wyse Management Suite (WMS) 4.0 introduces a new option to update the concurrent download and restart the tomcat service to update the maximum concurrent download in WMS Server and Repository.


To use this feature, Login to **WMS > Portal Administration > File Repositories > File Repo > Edit > update** the count for "Concurrent File Downloads" > **Save settings > Save and Restart**. The Tomcat service of the repository restarts, and the maximum thread count is updated in the Tomcat server configuration file.

 **NOTE:** The WMS administrator maintains ThinOS devices and updates device packages, or firmware, through groups and configuration. Before you restart Tomcat, ensure that there are no deployments in progress. It prevents package download errors at the endpoints. If there are other device types, save the settings instead of restarting. If there are more packages in the repository, service restarts and WMS Server registration may take longer.

Clear concurrent download slot after application download is complete

From Wyse Management Suite 4.0, once the device downloads the application, the agent notifies the WMS server. The WMS server clear concurrent download slots for Job Policy Group devices.

WMS Pro and Standard License holders have access to this feature.

 **NOTE:** This feature only works with WES devices running WDA 14.6.7.x or higher. This function is only compatible with App Policy and does not work with WES Imaging.

Report for Missing QFE

The Wyse Device Agent on a Windows IoT Thin Client notifies WMS of any missing QFEs. This information is reflected in **WMS device details page > System Info > Operating System Details**.

The Missing QFE report is generated from **Portal Administration > Reports > Generate Report > Type QFE > Missing QFE**.

Report for Installed QFE

Wyse Management Suite (WMS) 4.0 displays installed QFEs for WES and Wyse Software Thin Client in the **WMS device details page > System Info > Operating System Details**.

The installed QFE report can be generated from **Portal Administration > Reports > Generate Report > Type QFE > Has Installed QFE**. Provide the QFE numbers such as KB4132216, KB4346087, KB4462930, KB4462917, and so on.

 **NOTE:** The search box allows the entry of single or multiple KB numbers, up to a maximum of 10.

Report for Has not installed QFE

The report for QFE not installed is generated from **Portal Administration > Reports > Generate Report > Type QFE > Has not Installed QFE**. Provide the QFE numbers such as KB4132216, KB4346087, KB4462930, KB4462917, and so on, as per requirement and save.

 **NOTE:** The search box allows the entry of single or multiple KB numbers, up to a maximum of 10.


Generate reports on devices that have exceptions

A filter on **Devices** page can filter the devices with device level exception. Log in to **WMS**, go to **Devices page > Status filter > Has Device Exception**. The device report in WMS is enhanced to display devices with device-level exceptions and configurations. All device reports now include the column **Device Exceptions**. The devices with exceptions are displayed as **TRUE**. Otherwise, **FALSE** is displayed.

Azure Virtual Desktop

To access Azure Virtual Desktop (AVD), go to **Groups & Configs > Edit Policy > WES**. Parent Group, Child Group, and Device Level configuration options are available for Azure Virtual Desktop. The Add Policy button allows you to configure multiple Azure Virtual Desktops.

Wyse Device Agent creates the AVD shortcut using the Edge browser if the browser is installed on the client.

 **NOTE:** Azure Virtual Desktop is not supported on Internet Explorer. You must install a different browser and configure the new browser to be the default one for the Windows Embedded Standard device. The Wyse Device Agent creates the AVD shortcut using the default browser set on the device. Otherwise, Internet Explorer creates an AVD URL shortcut. Azure Virtual Desktop is not supported on Wyse Easy Setup.

UWF Servicing mode

Wyse Management Suite 4.0 introduces UWF Servicing mode, which triggers updates on WIE10 Thin Clients when issued from WMS. For WES thin client devices, this command can be triggered from the Devices page, the Device details page, or the Jobs page to schedule the command on a group of devices. If a command is scheduled, you can check its status on the WMS

events page, device details events, or Jobs page. WMS shows that QFE Updates are up to date under Missing QFE and all newly installed QFE is updated under QFE Info, once all the missing updates are installed.

The Wake On LAN command is triggered from the WMS when the UWF servicing command is performed. It functions whenever the device is in sleep or shutdown mode.

Once UWF command or schedule in client is initiated, the message WMS administrator has initiated a UWF servicing for this device is displayed, and the device reboots.

The last UWF servicing time is displayed in **Device Details page > System Info > Operating System details**.

The UWF Servicing mode is a pro feature. The device must be online to download and install the missing QFE. In servicing mode, the device does not communicate with WMS and cannot be managed. RTC, Apps, and Data are not accessible. Depending on the operating system version and download speed, it may take several minutes or hours to install all missing updates. WMS Server moves the command to fail after 24 hours.

UWF servicing mode requires KB5015807 to be installed on Windows 10 LTSC 2021. If this KB is not installed on the device before the UWF servicing command is performed, the device cannot enter the UWF servicing mode.

There is no option to postpone the UWF Servicing command on WES devices, and by default, the WDA displays the Update Now alert for five minutes. WMS 4.0 and WDA 14.6.7.x and higher versions support this feature. The command status fails if this is performed on devices with an older WDA. WES Images released after June 2022, specifically versions 10.04.xx.05.22.00 and higher, support this feature.

UWF is not supported in some of the older WIE 10 images. If a UWF servicing command is initiated from WMS, WDA 14.6.7.x reports the failure status **This image version is not enabled for UWF servicing** to WMS.

For more information about pre-requisites to enable UWF servicing mode on OptiPlex 3000 and 5070 thin client, see Windows 10 IoT Enterprise LTSC 2021 for OptiPlex 3000 Thin Client Release Notes and Dell Wyse 5070 Thin Client User Guide at <https://www.dell.com/support>.

Filter Devices as per the Application Package

The Wyse Management Suite 4.0 includes a capability that filters devices based on already-installed packages that were updated using WMS. If the same policy is rescheduled, it filters devices that have already installed the same application packages through WMS.

Policy is reapplied:

- If there are new applications that are added to the same application policy.
- If the application package is renamed before creating the application policy.

The MSI, MSU, and EXE package formats are compatible with this feature. Advanced App Policy supports this capability, which is exclusive to WES. WMS 4.0, WDA 14.6.7.x, and higher versions support this capability. This feature supports only app installation.

It is possible to amend the policy and then apply the updated policy to all devices by selecting the **Apply to All Devices**.

To use this feature, Login to **WMS > Apps & Data > Thin Client App Policies > OS Type as WES > Filter Devices**.

Filter Devices as per the Application Policy

Wyse Management Suite (WMS) 4.0 includes a feature that filters devices based on policies that are already applied to WES devices through WMS. If the same policy is rescheduled, it filters devices that have already applied the same application policy through WMS.

Policy is reapplied:

- If there are new applications that are added to the same application policy.
- If the application policy is renamed.
- If the previous policy is deleted and a new policy with the same name is created in WMS Server.

Advanced App Policy supports this feature, which is exclusive to WES. This feature only lets you install applications, and it is compatible with WMS 4.0 and WDA 14.6.7.x and higher versions.

It is possible to amend the policy and then apply the updated policy to all devices by selecting the **Apply to All Devices**.

To use this feature, Login to **WMS > Apps & Data > Thin Client App Policies > OS Type as WES > Filter Devices**.

Clearing inactive and unused filters for subnets, time zones, and devices

When devices are registered to Wyse Management Suite from a different subnet, the subnet is added to the subnet filter. The **Time Zone** and **Device Tags** filters are updated when devices from various subnets are registered and when the WMS administrator adds Device Tags.

If a device is unregistered or untagged, the new subnet, time zone, and device tag filters become inactive because there are no devices to filter. In these instances, use **WMS Clear Filter** option to delete unwanted subnet time zone and device tag filters.


To remove the subnet filter, click the **Clear Filter** option and then from the drop-down menu, select **Subnet**. Finally, click the **Clear Filter** button. In a similar manner, the filters for the time zone and device tag can be removed. The Standard License also supports this feature.

The **Clear Filter** record is found on the **Events and Jobs** page. Log in into **WMS > Devices Page > Clear Filter**, and select a filter from the list.

DCA-Enabler Agent GUI for WMS Registration

For DCA Enabler versions 1.7.0 and higher, the **Registration** Tab has a user interface to access the WMS Server URL, group token, and CA validation. The status can be viewed in the **Registration Status Field** after registration. Click the **Refresh** button to view the status of DCA Enabler.

The Support Tab displays dcae.log and dcaDiscovery.log.


 **NOTE:** DCA-E UI has no Unregister button, and hence WMS administrator must unregister from the portal. DCA-E UI can only display the last 50 lines of DCAE logs.

WES to ThinOS Conversion


Each Wyse Management Suite (WMS) tenant must have a ThinOS activation license and a Thin Client PRO license for the number of devices to be converted. WMS 4.0 provides support to convert Dell Thin Clients 5070, 5470 MTC, and 5470 AIO devices with Windows 10 Image to ThinOS. The binary requirements are WMS 4.0 or higher, WDA 14.6.7.x or higher, and Conversion Merlin Image.

Use the following repository to store the converted file, Repo Directory\repository\OSImages\zipped folder. The repository extracts files that are copied into this folder and moves them to a valid folder.

The conversion files in the local remote repository are displayed in **WMS > Apps & Data > OS Images Repository > WES/ThinLinux** page.

 **NOTE:** The OS type for the conversion image is displayed as ThinOS Conversion Image.

The image policy for converting WES to ThinOS should be created in **WMS > Apps & Data > OS Images Policies > WES/ThinLinux > Add Policy** and scheduled on the group.

 **NOTE:** Force this version must be selected for the Rule field.

The job is created, and each device receives the required package to switch to ThinOS. When making the app policy, you can automatically apply the image policy by selecting **Apply the policy to new devices** or **Apply the policy to devices during check-in**. The job stays open until the device is re-registered with WMS. If the device does not send a report to WMS, the job remains in progress for a week, and then it fails.

When the converted device checks in to WMS, the WES device is unregistered from the server, and the device name is changed according to ThinOS naming conversion. The converted device report is generated from **Portal Admin > Reports Pages > Device Report**. To find out which devices are changed, a new column is added with the text Device Converted with the value TRUE or FALSE.

Wyse Management Suite to support selection of multiple groups while creating Advanced App Policies

Wyse Management Suite (WMS) 4.0 allows creating Advanced App policies with multiple groups. This feature is available only for Pro license. All Thin clients, Wyse Software Thin Client, Hybrid Client, Generic Client support this feature. Advanced App

Policy uses this feature. The Advanced app policy created before WMS 4.0 can be modified to allow multiple groups. If a policy is created with multiple groups, then the same number of jobs are created. If **Include All Subgroups** is selected, user can select up to 100 groups when creating Advanced App Policy.

NOTE: Two policies with same application cannot have common groups. This functionality is not applicable for:

- Edge gateway devices such as Ubuntu core and Embedded personal computer.
- Image Policy and scheduling device commands.
- Standard app policy.

Wyse Management Suite displays option to Restart Jobs for Offline Devices

Wyse Management Suite (WMS) 4.0 provides the option to exclude an offline device from the job queue. The WMS administrator must select the **Exclude Offline Devices** checkbox while scheduling the job to exclude the offline devices. By default, the **Exclude Offline Devices** option is not selected.

WMS administrator can:

- View the list of Excluded Offline Devices by clicking the **Offline Device Count** on the Jobs page.
- Select and restart the job for offline devices by selecting **Restart Job**.

WMS administrator can exclude offline devices while rebooting. A new job is created targeting offline devices, and the **Restart Job for Offline Devices** option is disabled for the previous jobs. In the current job that targets offline devices, **Restart Job for Offline Devices** is no longer available. The restart job for offline devices option is disabled for the previous job. Administrator can restart Offline Jobs until none are left. Once no offline devices remain, **Restart Job for Offline Devices** is disabled.

NOTE:

Schedule Device Command and Image Policy jobs cannot exclude offline devices. Restart cannot be initiated for both Failed Job and Offline Device Job. If **Exclude offline devices** is not selected, WMS includes all devices in the job, and offline devices do not receive the policy.

If a device fails to apply the policy, WMS administrator must use Restart Failed Job. Restart Job for Offline Devices cannot be used to restart this job. WMS administrator can schedule jobs to exclude offline devices.

Wyse Management Suite enables WES package File Repository in Operator and Tenant Cloud

WMS 4.0 has enabled WES package file repository in Operator and Tenant Cloud. This feature is exclusive to the Pro license.

Thin client app inventory provides the following feature:

- Add WES Package File.

The same WES package file may exist in multiple file repositories, including the Global Cloud Repository (operator cloud), Tenant Cloud Repository, and Remote Repository. In policy creation, users can select and push the WES packages.

NOTE:

- The maximum file upload size is 1.5 GB.
- This functionality only supports .msi, .exe, .msu, .zip, .ps1, .bat, .cmd, .msp, .vbs, and .rsp file extensions.
- If the file exists in the Global Cloud Repository, it cannot be uploaded to the Tenant Cloud Repository.

Wyse Management Suite supports Dell Hybrid Client 2.x Configuration Policies

Wyse Management Suite (WMS) 4.0 includes assistance for the Dell Hybrid Client 2.x. A new configuration section has been added to the **Edit Policy** page for Dell Hybrid Client 1.x and 2.x.

WMS administrator can create :

- Dell Hybrid Client 1.x and 2.x device level configurations from **Device details page > Create/Edit Exceptions**.

- Dell Hybrid Client 1.x and 2.x user level configurations for end users.

Using the same Dell Hybrid Client option, a WMS administrator can export and import configurations for both Dell Hybrid Client 1.x and Dell Hybrid Client 2.x.

NOTE: When a device with hybrid client 1.x device exceptions is converted to 2.x, the server clears the preconfigured device level configurations. The WMS administrator must configure Dell Hybrid Client 2.x group policies and exceptions for the group and devices. Wallpaper, certificates, logos, INI files, and so on, are the same for Dell Hybrid Client and 2.x configurations. The resource files that are uploaded for Dell Hybrid Clients are loaded or displayed for 2.x Configurations, and conversely.

Run Report on Devices

Wyse Management Suite (WMS) 4.0 introduces three new filters in the **Events** Page under **Access** category to filter the activity and generate a consolidated event report for the following:

- BIOS password Failure
- Device Admin Login Success
- Device Admin Login Failure

This feature is only available on ThinOS devices.

Important notes

- Microsoft Gina should be selected when you configure keyboard layouts.
- Language pack should be pre-installed on the Windows 10 IoT Enterprise image to apply the default language configuration.
- Updating substitute keyboard layouts restarts the device twice if Microsoft Gina is enabled.
- For information about the changes or updates to the ThinOS and Dell Hybrid Client configurations, see *ThinOS 9.x Administrator's Guide and Release notes* and *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.
- If you are using Wyse Easy Setup 2.0.0.158 or earlier versions, you must upgrade Wyse Easy Setup to 2.0.0.189 after you upgrade Wyse Device Agent to 14.6.1.4.
- When the Citrix connection is deployed from Wyse Management Suite and if Citrix application is active or in use, and then the default Citrix connection cannot be launched.
- If you are an issue with Wyse Easy Setup issue after upgrading to WDA 14.6.8.1 from WDA 14.6.7.32, you must re-publish the Wyse Easy Setup configuration from Wyse Management Suite.

Server or device agent details

Table 40. Server or device agent details

File name	Description	Version
WMS_4.0.0.526.exe	Wyse Management Suite server	4.0.0.526
WMS_Repo.exe	Wyse Management Suite repository	4.0.0.185
WDA_14.6.8.1_Unified.exe	Unified WDA for Windows 10 IoT Enterprise	14.6.8.1
DellWMS-ConfigurationUI-Package.zip	configUI_signed.zip	1.9.532
WMS_Import_Tool.exe	Wyse Management Suite Import Tool	1.7.5.176
DCA_Enabler_1.6.0-9.zip	DCA Enabler and DCA Enabler Package combined Zipped	1.7.0-20
SoftwareVaultUtility-1.4.0.0.exe	Software Vault Utility	1.4.0.0

NOTE: The above-listed agents are not tested with WDM.

Windows Server configuration requirements

Table 41. Windows Server configuration requirements

Devices	Server requirements
Minimum server requirements for Wyse management Suite operations with 10,000 devices	<ul style="list-style-type: none"> Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard Minimum CPU requirements—4 CPU Minimum Disk Space—40 GB Minimum Memory—8 GB <p>NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for Secure MQTT communications.</p>
Server requirement for Wyse Management Suite operations with 50,000 devices	<ul style="list-style-type: none"> Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard Minimum CPU requirements—4 CPU Minimum Disk Space—120 GB Minimum Memory—16 GB
Server requirement for Wyse Management Suite operations with 120,000 devices	<ul style="list-style-type: none"> Supported operating systems—Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Standard Minimum CPU requirements—16 CPU Minimum Disk Space—200 GB Minimum Memory—32 GB

Wyse Management Suite upgrade path

Table 42. Wyse Management Suite upgrade path

Upgrade type	Upgrade path	Compatibility
3.7 to 4.0	3.7 > 4.0	Supported
	3.7 > 3.7 Hotfix > 4.0	Supported
	3.7 > 3.7 Hotfix > 3.8 > 4.0	Supported
	3.7 > 3.7 Hotfix > 3.8 > 3.8 Hotfix > 4.0	Supported
3.8 to 4.0	3.8 > 4.0	Supported
	3.8 > 3.8 Hotfix > 4.0	Supported
1.0 to 4.0	1.0 > 1.1 > 1.2 > 1.3 > 1.4 > 1.4.1 > 2.0 > 2.1 > 3.0 > 3.1 > 3.1.1 > 3.2 > 3.2.1 > 3.3 > 3.3.1 > 3.5 > 3.5.1 > 3.5.2 > 3.6 > 3.6.1 > 3.7 > 3.7 Hotfix > 3.8 > 3.8 Hotfix > 4.0	Supported NOTE: For administrators who want to upgrade Wyse Management Suite, ProSupport is provided only from Wyse Management Suite version 3.6 and later versions.

Fixed issues

Table 43. Fixed issues

Issue ID	Description
WMS-723	Device exceptions for Citrix configuration editor do not work.
WMS-735	ThinOS registers to previous WMS group after 9.3.1129 firmware update.

Table 43. Fixed issues (continued)

Issue ID	Description
WMS-738	Installing the script through WMS has failed.
WMS-743	When Windows 10 IoT device connects to Citrix using the Citrix Connection agent, there is a delay. There is no delay when Citrix Workspace App is used.
WMS-745	Application policies set are not seen under the Edit Policy tab.
WMS-757	The error Failed: Remove Application is not supported by the platform is displayed on the Jobs page when you uninstall ThinOS packages.
WMS-760	DTOS devices revert to the previous WMS group after a firmware update.
WMS-762	Double-byte characters are an issue on WMS.
WMS-763	When signed in with the user, the Custom Role option for all groups is not available in WMS Cloud.
WMS-767	The device brightness decreases after more than 2 hours of inactivity and displays an error while accessing a new application on the Wyse 5070 Thin Client.
WMS-770	In WMS 3.8, an internal error or misconfiguration occurs that is user-specific.
WMS-772	In VMware session of Windows 10 IoT 2019 LTSC MR2, it is not possible to disable the VDI menu bar.
WMS-774	The current WiFi Network column displays N/A for ThinOS devices in the All Devices report.
WMS-777	On the Optiplex 3000 running Windows LTSC, the IPS replicated PoC app failed to deploy from Wyse Management Suite.
WMS-779	On WMS, there is an IPS-replicated incorrect repository representation.
WMS-780	Address few user interface issues with WMS.
WMS-781	Option tag 60 is populated with RTI Agent.
WMS-785	You are unable to receive email alerts with WMS rules.
WMS-788	Issue with the option to save current filter in Wyse Management Suite.
WMS-786	WMS fails when attempting to renew an 802.1X certificate on ThinOS 9.x.
WMS-791	The Dell P2219H and P2222H monitors change the monitor settings.
WMS-792	The WMS API call to US1 has duplicate systems that are listed.
WMS-793	Citrix Connection Agent in Windows 10 IoT Enterprise on Wyse 5070 Thin Client, does authenticating to NetScaler in kiosk mode.
WMS-795	The WMS configuration policy failed to uninstall the application package.
WMS-799	The API retrieves device inventory details in the order of inverse LastCheckIn.

Table 43. Fixed issues (continued)

Issue ID	Description
WMS-801	, There is unexpected behavior when attempting to update the firmware to ThinOS 2208.
WMS-803	Occasionally DtcOperationHandler message appears on Windows Embedded Standard devices.
WMS-805	WMS Japanese UI correction request.
WMS-822	Fixed issue related to Wyse Easy Setup

Security fixes

Wyse Management Suite 4.0 addresses multiple vulnerabilities. For information about the vulnerabilities addressed in this release, see *DSA-2022-329: Dell Wyse Management Suite Security Update for Multiple Vulnerabilities* at [Security Advisories & Notices | Dell](#).

Installing package

Downloading the installation file

1. Go to www.dell.com/support.
2. In the Enter a **Service Tag, Serial Number, Service Request, Model, or Keyword search box**, type **Converter for PCs** and click **Search**.
3. On the opened page click **Drivers and Downloads**.
4. In the same page, you can find **Converter for PCs 3.0.0.4689** and download the application file by clicking **Download**.

Resources and support

Accessing documents using the product search

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name.
For example, **OptiPlex 3000 Thin Client**. A list of matching products is displayed.
3. Select your product.
4. Click **Documentation**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to www.dell.com/support.
2. Click **Browse all products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **OptiPlex Thin Client**.
6. Click **OptiPlex 3000 Thin Client**.
7. Click **Select this Product**.
8. Click **Documentation**.

Contacting Dell

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for technical support or customer service issues, see www.dell.com/contactdell.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.