



Dell Wyse Management Suite 1.2 HF1 Release Notes

Dell recommends applying this update during your next scheduled release cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers and software).

Current Version: 1.2 HF1
Release Date: August 2018
Previous Version: 1.2

Contents

Release type and definition.....	1
Supported thin clients	1
Server or Device agent details.....	3
Supported browsers.....	3
Windows Server 2012 R2 and Windows Server 2016 configuration requirement.....	4
Supported operating system matrix.....	4
Fixed issues.....	4
Installation methods.....	5
Known issues.....	7

Release type and definition

Dell Wyse Management Suite 1.2 HF1 release contains fixes for problems that are found since the release of the Dell Wyse Management Suite 1.2 software.

Supported thin clients

Table 1. Supported thin clients

Operating system	Device type	Build number
Linux	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client	11.3.106

Operating system	Device type	Build number
	Wyse 7020 thin client	
ThinLinux 1.0	Wyse 5020 thin client Wyse 5060 thin client Wyse 7020 thin client Wyse 3030 LT thin client Wyse 3040 thin client	1.0.71 (Wyse 3040 thin client) 1.0.7 (Wyse 5020 thin client, Wyse 5060 thin client, Wyse 7020 thin client, and Wyse 3030 LT thin client)
ThinLinux 2.0	Wyse 3040 thin client Wyse 5070 thin client Wyse 5070 Extended thin client	2.0.19.31428 (Wyse 3040 thin client) 2.0.22.31472 (Wyse 5070 thin client)
Windows Embedded Standard 7 (WES7)	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 3030 thin client Wyse 7010 Extended thin client	7076 and 7077
Windows Embedded Standard 7P (WES7P)	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 7010 Extended thin client	7065, 7066, 7067
	Wyse 7040 thin client	7065
	Latitude 3460 mobile thin client	7065
	Latitude E7270 mobile thin client	7065
	Wyse 5060 thin client	7067
Windows 10 IoT Enterprise (WIE10)	Wyse 5020 thin client Wyse 7020 thin client Latitude 3480 mobile thin client Latitude 5280 mobile thin client Wyse 5070 thin client Wyse 5070 Extended thin client	0A62

Operating system	Device type	Build number
Windows Embedded 8 Standard (WE8S)	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client	930
ThinOS	Wyse 5040 AIO Wyse 3010 thin client Wyse 3020 thin client Wyse 5010 thin client (ThinOS, PCOIP) Wyse 7010 thin client Wyse 3030 LT thin client Wyse 5060 thin client Wyse 3040 thin client Wyse 5070 thin client Wyse 5070 Extended thin client	8.4_009, 8.4_105, 8.4_112, 8.5_008

Server or Device agent details

Table 2. Server/Device agent details

Server/Device name	File name	Version
Wyse Management Suite server	WMS_1.2_HF1.exe	40599
Unified Wyse Device Agent for Windows	WDA_14.2.0.54_Unified.exe	14.2.0.54

NOTE:

Wyse Device Agent 14.2.0.54 agent is not tested with Wyse Device Manager.

Supported browsers

Table 3. Browser details

Browsers	Version
Chrome	66.0.3359 and later
Firefox	56.0 and later
Internet Explorer	11.0 and later

Windows Server 2012 R2 and Windows Server 2016 configuration requirement

Table 4. Windows Server 2012 R2 and Windows Server 2016 configuration requirement

Server requirement for Wyse Management Suite for 50,000 devices	<ul style="list-style-type: none"> Minimum CPU requirements—4 CPU Minimum disk space—120 GB Minimum memory RAM—16 GB
Server requirement for Wyse Management Suite for 120,000 devices	<ul style="list-style-type: none"> Minimum CPU requirements—16 CPU Minimum disk space—200 GB Minimum memory RAM—32 GB NIC cards—4

Supported operating system matrix

Table 5. Supported operating system matrix

Operating system	Wyse Management Suite server	Wyse Management Suite repository	Remote database
Windows Server 2012 R2 English	Yes	Yes	Yes
Windows Server 2012 R2 French	Yes	Yes	No
Windows Server 2012 R2 Italian	Yes	Yes	No
Windows Server 2012 R2 German	Yes	Yes	No
Windows Server 2012 R2 Spanish	Yes	Yes	No
Windows Server 2016 English	Yes	Yes	Yes
Windows Server 2016 French	Yes	Yes	No
Windows Server 2016 Italian	Yes	Yes	No
Windows Server 2016 German	Yes	Yes	No
Windows Server 2016 Spanish	Yes	Yes	No

Fixed issues

Table 6. Fixed issues

Issue number	Description
STRATUS-17613	When a single device is under a multilevel child group, you cannot schedule the application policy.
STRATUS-17591	The viewer role profile cannot view the custom wallpaper, after migrating from Wyse Management Suite version 1.1 or 1.0 to the latest version.

Issue number	Description
STRATUS-17618	Upgrading from Wyse Management Suite version 1.1 to version 1.2 fails because the Wyse Management Suite database password contains special characters such as, ? or *.
STRATUS-17732	If database password has special character such as , then the installer displays a message to change or update the password.
STRATUS-17651	For Windows Embedded Standard WDA version 14.2.0.54, the configuration by using Wyse Management Suite server must complete even if the server is not reachable.

Installation methods

Dell Wyse Management Suite version 1.2 HF1 is a full installer. You can download the installer file and install the server. If the server is already installed, then you can upgrade it to the latest version. For more details, see *Dell Wyse Management Suite version 1.2 Quick Start Guide*.

Installing Dell Wyse Management Suite version 1.2 HF1

To install Dell Wyse Management Suite version 1.2 HF, do the following:

- 1 Copy the Dell Wyse Management Suite version 1.2 HF1 installer file (**WMS_1.2_HF1.exe**) to the server.
- 2 Double-click the **WMS_1.2_HF1.exe** file.

NOTE: If the database password contains any special characters, such as ' " \ | and space, then the installer displays a warning message. The following table provides the list of special characters that is supported in Dell Wyse Management Suite version 1.2 HF1:

Table 7. Supported special characters

Special characters	Admin password	Database password	Dell Wyse Management Suite version 1.2 HF1
~	Yes	Yes	Supported
!	Yes	Yes	Supported
@	Yes	Yes	Supported
#	Yes	Yes	Supported
\$	Yes	Yes	Supported
%	Yes	Yes	Supported
^	Yes	Yes	Supported
&	Yes	Yes	Supported
*	Yes	Yes	Supported
(Yes	Yes	Supported
)	Yes	Yes	Supported

Special characters	Admin password	Database password	Dell Wyse Management Suite version 1.2 HF1
"-" (hyphen)	Yes	Yes	Supported
"+" (Plus)	Yes	Yes	Supported
}	Yes	Yes	Supported
{	Yes	Yes	Supported
[Yes	Yes	Supported
]	Yes	Yes	Supported
	Yes	Yes	Blocked
:	Yes	Yes	Supported
?	Yes	Yes	Supported
>	Yes	Yes	Supported
<	Yes	Yes	Supported
` (grave)	Yes	Yes	Supported
_ (underscore)	Yes	Yes	Supported
"=" (equal)	Yes	Yes	Supported
;	Yes	Yes	Supported
,	Yes	Yes	Supported
.	Yes	Yes	Supported
/	Yes	Yes	Supported
'	Yes	Yes	Blocked
\	Yes	Yes	Blocked
"	Yes	Yes	Blocked

Upgrading Dell Wyse Management Suite version 1.2 HF1

To upgrade Dell Wyse Management Suite version 1.2 HF1, do the following:

- 1 Copy the Dell Wyse Management Suite version 1.2 HF1 installer (**WMS_1.2_HF1.exe**) file to the server where you have installed the previous version.
- 2 Double-click the **WMS_1.2_HF1.exe** file.
- 3 Click **Next**.
- 4 Click **Next** to start the upgrade process.

The following table provides the information about the supported upgrade path:

Table 8. Supported upgrade path

Upgrading from Dell Wyse Management Suite version 1.0 to Dell Wyse Management Suite version 1.2 HF1	Path	Upgrade support
	1.0 > 1.2 HF1	Yes
	1.0 > 1.1 > 1.2 HF1	Yes
	1.0 > 1.2 > 1.2 HF1	Yes
Upgrading from Dell Wyse Management Suite version 1.1 to Dell Wyse Management Suite version 1.2 HF1	1.1 > 1.2 HF1	Yes
	1.1 > 1.2 > 1.2 HF1	Yes
Upgrading from Dell Wyse Management Suite version 1.02 to Dell Wyse Management Suite version 1.2 HF1	1.2 > 1.2 HF1	Yes

Known issues

Table 9. Known issues

Issue number	Description	Workaround
STRATUS-17533	On the Devices page, select a Configuration group and save the filter as default. The issue is observed when the selected groups are not displayed automatically on the Devices page when the page is refreshed.	There is no workaround.
STRATUS-17513	Wallpaper is reset to default when all the resource files are added in the configuration.	There is no workaround.
STRATUS-17512	INI and local files are downloaded every time that you restart the Wyse Management Suite software.	There is no workaround.
STRATUS-17501	Cloud Connect user role is displayed to the private cloud admin.	There is no workaround.
STRATUS-17488	Unable to upload a certificate to Wyse Management Suite private cloud as wmsssystemadmin.	There is no workaround.
STRATUS-17444	Unable to log in to Wyse Management Suite server with Active Directory user credentials when multiple Active Directory server information is added.	There is no workaround.
STRATUS-17441	The device receives configuration from the previous group, when managed image policy is configured on a custom group device and moved to default policy group.	There is no workaround.
STRATUS-17404	For Wyse Software thin clients, the Update now option for configurations is displayed on the app lock screen.	There is no workaround.
STRATUS-17403	When you configure the apply on check-in policy to multiple devices, then the Update now option is displayed on the lock screen.	There is no workaround.
STRATUS-17390	During a group and user search, Wyse Management Suite stops responding.	There is no workaround.
STRATUS-17368	The language keyboard cannot be removed from Wyse Management Suite server.	There is no workaround.

Issue number	Description	Workaround
STRATUS-17339	When you click Update Now , Wyse Device Agent requires few minutes to restart the static IP configured thin client.	There is no workaround.
STRATUS-17284	Duplicate device entry is found when you upgrade, downgrade, unregister or reregister WDA.	There is no workaround.
STRATUS-17221	When dual monitor settings are applied, display on monitor 3 and monitor 4 is not turned off.	There is no workaround.
STRATUS-17215	On the BIOS screen, enable the main USB option and disable the back USB option. The back USB option is working when you insert a USB device.	There is no workaround.
STRATUS-17157	IEEE settings for WLAN are not displayed on the Groups & Config page.	There is no workaround.
STRATUS-17143	CA validation is not authorized with self-signed certificates.	There is no workaround.
STRATUS-17081	Certificate error is displayed when Wyse Management Suite is installed and launched in a workgroup server.	There is no workaround.
STRATUS-17061	Error: Not a valid zip or exe file is displayed when RSP packages on MUI servers are extracted.	There is no workaround.
STRATUS-17048	ThinOS hostname is reset to the default name when general settings policy is pushed from Wyse Management Suite.	There is no workaround.
STRATUS-16991	Few display payloads that are applied from Wyse Management Suite are missing in Wyse 5070 thin client.	There is no workaround.
STRATUS-16936	When System Personalization policy is changed without modifying the display section, the thin client with multiple displays (includes the onboard Dual as well) is set to single display.	There is no workaround.
STRATUS-16929	Unable to generate Current Alerts report.	There is no workaround.
STRATUS-16919	A device restarts multiple times, when the server certificate is not installed and the HTTPS is used to download a ThinOS.ini file.	There is no workaround.
STRATUS-16853	RemoteFX USB, USB redirection for later plug-in, and redirection of other plug n play, are not available for Wyse Software thin clients.	There is no workaround.
STRATUS-16809	The issue is observed when LocalhostManagerImpl is used for public cloud. The code is applicable for private cloud.	There is no workaround.
STRATUS-16688	You can create, configure, and publish VMware View in appliance mode without VMware remote connection.	There is no workaround.
STRATUS-16687	You can create, configure, and publish Internet Explorer in appliance mode without the Remote Browser Connection.	There is no workaround.
STRATUS-16686	If the SMTP server is configured before saving 2FA, then the server is not validated.	There is no workaround.
STRATUS-16692	Duplicate RDP icon is displayed on the client desktop when a device policy exception is created.	There is no workaround.
STRATUS-16610	Unable to launch Remote Desktop session collection.	There is no workaround.
STRATUS-16427	USB lockdown configuration is not applied after you click Update Now , but applies after you log off and log in again.	There is no workaround.
STRATUS-16358	Policy cannot be changed error appears while adding or removing configuration policy along with the appliance mode.	There is no workaround.

Issue number	Description	Workaround
STRATUS-16256	Unknown error is observed on the Wyse Device Agent UI after Wyse Converter for PCs is installed.	There is no workaround.
STRATUS-15924	Security and Lockdown, User Settings, Domain Settings, and VNC settings do not have description about the configurations.	There is no workaround.
STRATUS-15878	Device hostname changes when you switch the device from LAN to wireless LAN.	There is no workaround.
STRATUS-15009	Unable to schedule a Windows 10 IoT Enterprise upgrade through Wyse Management Suite server on a Wyse 5060 thin client running Windows Embedded Standard 7P.	There is no workaround.
STRATUS-17544	Configuring multiple shared drives fails in Windows Embedded Standard client.	There is no workaround.
STRATUS-17487	The groups page slows down when 42,000 groups and 56,000 devices are imported from Wyse Device Manager to Wyse Management Suite using the import tool.	There is no workaround.
STRATUS-17075	Device is not listed in Jobs page. The Events page displays the status of the devices as Pending or In Progress .	There is no workaround.
STRATUS-17747	The database password does not support the \ special character but in the displayed error message, the/special character is not supported.	There is no workaround.
STRATUS-17694	WDA downgrade process fails on Windows Embedded 8 Standard clients occasionally, as it is unable to know the write filter status.	There is no workaround.
STRATUS-17738	The special character is not supported, but changing the database password from the portal administrator page supports the special character.	There is no workaround.