

Wyse Converter for PCs

Version 1.0 Administrator's Guide



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.

Copyright © 2017 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

1 Introduction to Wyse Converter for PCs.....	4
Supported operating systems	4
2 Installation methods.....	5
Parameters for silent installation.....	5
Prerequisites to install Wyse Converter for PCs.....	6
Installing Wyse Converter for PCs using third party management software.....	6
Installing Wyse Converter for PCs using the installer on a local device.....	7
3 Getting started.....	9
Logging in to the Wyse Software thin client.....	9
Before configuring your Wyse Software thin clients.....	9
Unified Write Filter.....	10
NetXClean utility.....	12
C-A-D tool.....	13
Registering Wyse Software thin client to Wyse Management Suite.....	13
4 Configuring your Wyse Software thin client.....	16
Using VMware Horizon Client to connect to virtual desktop.....	16
Configuring Citrix receiver session services.....	17
Configuring remote desktop connection session services.....	18
Configuring your Wyse Software thin client using Wyse Management Suite.....	19
Configuring RAM disk size.....	19
5 Wyse Converter for PCs license.....	20
Importing and upgrading Wyse Management Suite license.....	20
6 Uninstallation methods.....	22
Uninstalling Wyse Converter for PCs remotely.....	22
Uninstalling Wyse Converter for PCs using third party management software.....	22
Uninstalling Wyse Converter for PCs using Wyse Management Suite.....	23
Uninstalling Wyse Converter for PCs locally.....	23
7 Troubleshooting Wyse Converter for PCs.....	25



Introduction to Wyse Converter for PCs

Wyse Converter for PCs is a stand-alone software that enables you to provide a thin client like experience on a Windows PC. Wyse Converter for PCs provides a secure, and seamless interface to connect to VDI sessions.

After you install Wyse Converter for PCs, the device is referred to as Wyse Software thin client. You can manage the device using Wyse Management Suite 1.1 and later versions.

Wyse Converter for PCs utilizes the existing Windows operating system on the hardware, and adds the customization but does not replace the operating system. It only locks down the exiting Windows operating system for a more secure user experience.

NOTE: The existing Start menu shortcuts and desktop shortcuts on the system are removed during installation, and the shortcuts can be restored post uninstallation.

Supported operating systems

Wyse Converter for PCs is supported by the following operating systems:

- Microsoft Windows 7 32-bit and 64-bit—Service pack 1 only (English only)
- Microsoft Windows 10 Enterprise 64-bit (English only)

Installation methods

You can install Wyse Converter for PCs using any of the following methods:

- Remote or silent installation from a third party management software such as Microsoft System Center Configuration Manager—see [Installing Wyse Converter for PCs using third party management software](#).
- Local installation on your PC—see [Installing Wyse Converter for PCs using the installer on a local device](#).

The following modifications are made by the Wyse Converter for PCs installer:

- Two new user accounts, WyseAdmin and WyseUser are created, and the existing non administrator accounts are disabled.
- The NetXClean utility is installed to clean extraneous information from the local storage.
- The control settings functions are limited to the user.
- Wyse Device Agent is installed to manage Wyse Software thin client by using Wyse Management Suite.
- The applications such as Wyse Device Agent, Citrix Receiver, Citrix HDX RealTime Media Engine, VMware Horizon client, and TightVNC can be installed on your PC using the installer.
- Dell thin client application, CAD map tool, and RAMDisk applications are installed.
- Unified Write Filter is installed by the Wyse Converter for PCs installed on systems that run on Windows 10 Enterprise operating system.
- Dell wallpaper, desktop theme, and user account Dell logo are added.

NOTE:

- The administrator account and the user accounts which are part of local administrator group are not disabled by Wyse Converter for PCs.
- If you update any of the applications installed by the Wyse Converter for PCs, the applications are not uninstalled when you uninstall Wyse Converter for PCs.
- The supported applications such as Citrix Receiver, Citrix HDX RealTime Media Engine, VMware Horizon client, and TightVNC are not downloaded, deployed or upgraded if any version of the application is already installed on your PC.

Topics:

- [Parameters for silent installation](#)
- [Prerequisites to install Wyse Converter for PCs](#)
- [Installing Wyse Converter for PCs using third party management software](#)
- [Installing Wyse Converter for PCs using the installer on a local device](#)

Parameters for silent installation

The following table provides description on the parameters used for silent installation:



Table 1. Parameters for silent installation

Name	Syntax	Description
install	/install	Runs the installer displaying no user interface and prompts.
adminpassword	/adminpassword:	Sets the password for the administrator account.
userpassword	/userpassword:	Sets the password for the user account.
app	/app:	Installs the applications that you specify.
citrixrcvr	citrixrcvr	Installs Citrix Receiver on your system.
citrixhdxtme	citrixhdxtme	Installs Citrix HDX RealTime Media Engine on your system.
vmware	vmware	Installs VMware Horizon Client on your system.
tightvnc	tightvnc	Installs TightVNC on your system.

Prerequisites to install Wyse Converter for PCs

The following are the prerequisites to install Wyse Converter for PCs:

- Windows QFEs and the drivers should be updated to the latest version.
- Genuine version of the Windows operating system is installed.
- The existing user name should not be WyseUser or WyseAdmin.
- A minimum disk space of 2 GB is available.
- Unified Write Filter is disabled—Applicable only to Windows 10 Enterprise operating systems.
- Disable the antivirus.
- Disable Windows Secure Boot—Applicable only to Windows 10 Enterprise operating systems.

NOTE: Wyse Converter for PCs cannot be installed on a virtual machine.

Installing Wyse Converter for PCs using third party management software

You can install Wyse Converter for PCs on multiple devices simultaneously using a third party management software such as Microsoft System Center Configuration Manager (SCCM).

Perform the following steps for silent installation of Wyse Converter for PCs using SCCM:

- 1 Launch the SCCM console.
- 2 Go to **Software Library > Overview > Application Management > Applications**.
- 3 Right-click **Applications**, and click **Create Application**.
The **Create Application Wizard** window is displayed.
- 4 On the **General** page, click **Manually specify the application information**.
- 5 Click **Next**.
- 6 On the **General Information** page, specify the information about the application and click **Next**.



- 7 On the **Application Catalog** page, specify the information about how you want to display the application when you browse the Application Catalog.
 - 8 On the **Deployment Types** page, click **Add** to create a deployment type.
The **Create Deployment Type Wizard** window is displayed.
 - 9 On the **General** page, click **Manually specify the deployment type information**.
 - 10 Click **Next**.
 - 11 On the **General Information** page, specify the information about the application and click **Next**.
 - 12 On the **Content** page, specify the location of the Wyse Converter for PCs setup file.
 - 13 In the **Installation program** field, enter the parameter `WyseConverterforPCs.exe /install /adminpassword: /userpassword: /app:` and specify the administrator password, user password and the applications you want to install.
For example, `WyseConverterforPCs.exe /install /adminpassword:DellCCCvdi /userpassword:DellCCCvdi /app:citrixrxvr:citrixhdxrtme:vmware:tightvnc`.
- For information on the parameters, see [Parameters for silent installation](#).
- 14 On the **Detection Method** page, select the **Setting Type** as **File System**, and enter `%Windir%\Setup\Logs` in the **Path** field.
 - 15 Specify the type and enter the file or folder name as `InstallWyseConverter.log`, and click **OK**.
 - 16 Click **Next**.
 - 17 On the **User Experience** page, from the **Installation behavior** drop-down list, select **Install for system if resource is device; otherwise install for user**.
 - 18 From the **Logon requirement** drop-down list, select **Whether or not a user is logged on**.
 - 19 From the **Installation program visibility** drop-down list, select **Hidden**.
 - 20 Specify the maximum run time and the estimated installation time of the deployment program for the application, and click **Next**.
 - 21 On the **Requirements** page, click **Next**.
 - 22 On the **Dependencies** page, click **Next**.
 - 23 On the **Summary** page, the summary of the configurations is displayed.
 - 24 Click **Close**.
 - 25 Distribute the content to distribution point to make the content available for deployment. To distribute the content to distribution point, see *Operations and Maintenance for Content Management in Configuration Manager* at technet.microsoft.com.
 - 26 On the target PC, open **Software Center** and select **Wyse Converter for PCs**.
 - 27 Click **Install**.

Installing Wyse Converter for PCs using the installer on a local device

NOTE: To run the installer silently on a local device, log in as an administrator, run the command prompt, and enter `WyseConverterforPCs.exe /install /adminpassword: /userpassword: /app:`.

For example, `WyseConverterforPCs.exe /install /adminpassword:DellCCCvdi /userpassword:DellCCCvdi /app:citrixrxvr:citrixhdxrtme:vmware:tightvnc`.

For information on silent parameters, see [Parameters for silent installation](#).

To install Wyse Converter for PCs on a local device, do the following:

- 1 Double-click the installer package.
The **User Account Control** window is displayed.
- 2 Click **Yes**.
The installer validates the pre-installation requirements.
- 3 If the pre-installation requirements are met, click **OK**.
The **Welcome** screen is displayed.
- 4 Read the **Dell End User License Agreement**, and click **Next**.

NOTE: Abode reader is required to view the Dell End User License Agreement.



- 5 Select the **Setup Type** you want to install, and click **Next**. The available options are:
- Typical—If you select the setup type as **Typical**, the **Typical installation** screen is displayed. The screen lists the program features installed by the Wyse Converter for PCs installer.

NOTE: Typical installation requires minimum user interaction and installs all the typical program features.

- Custom—If you select the setup type as **Custom**, the **Custom installation** screen is displayed, and you can select any of the following applications that you want to install on your system:
 - Wyse Device Agent
 - Citrix Receiver
 - Citrix HDX RealTime Media Engine
 - VMware Horizon Client
 - TightVNC

NOTE:

- Custom installation requires maximum user interactions and allows you to choose the program features to be installed. It is recommended for advanced users.
- Wyse Device Agent is installed by default and the check box is grayed out.
- If applications are already installed on the PC before the installation procedure, they are not reinstalled by the Wyse Converter for PCs.

- 6 Click **Next**.

The **Add user accounts** screen is displayed.

- 7 Clear the **Use default password** check box if you want to change the default password for the administrator and user account. The default administrator and user password is `De11CCcVdi`.

NOTE:

- You cannot change the default administrator user name and standard user name.
- The default password is not applicable when the target device belongs to a domain, and the password complexity is enabled.
- Password must not contain special characters, such as `\ / : * ? " < > |`.

- 8 Click **Next** to install the software.

The **Install** screen with the installation progress is displayed.

- 9 After the installation is complete, click **Restart Now**.

The system restarts and automatically logs in to the WyseAdmin account.

The installer runs the lockdown scripts on the WyseAdmin and WyseUser account, and automatically logs in to the WyseUser account.

The installer takes approximately 25 minutes to complete the installation.

NOTE:

- Write filter is enabled by default after installation on a Windows 10 Enterprise device.
- The system restarts twice to complete the installation and automatically logs in to the WyseUser account.

Getting started

You can log in to Wyse Software thin client as a WyseUser or as a WyseAdmin.

To get started using your Wyse Software thin client, see:

- Logging in to your Wyse Software thin client—see [Logging in to your Wyse Software thin client](#).
- Before configuring your Wyse Software thin client—see [Before configuring your Wyse Software thin clients](#).

Topics:

- [Logging in to the Wyse Software thin client](#)
- [Before configuring your Wyse Software thin clients](#)

Logging in to the Wyse Software thin client

What you see when the Wyse Software thin client turns on or reboots depends on the administrator's configuration. After creating a user account, an administrator can configure the account to log in automatically or manually with user credentials.

When you start the Wyse Software thin client, you automatically log in to the WyseUser desktop by default.

To log in as a different user or administrator on a Windows 10 device:

- 1 Click **Start Menu > User > Sign Out** to log off the current desktop.
- 2 Click anywhere on the lock screen to view the **logon** window.
- 3 You can view the user accounts list on the left-lower corner of your screen. Click the preferred user account and then enter the logon credentials.
 - **Administrators**—The default user name is **WyseAdmin** and default case-sensitive password is **DellCCCvdi**.
 - **Users**—The default user name is **WyseUser** and default case-sensitive password is **DellCCCvdi**.

If automatic login is not enabled, the login window displays when you boot the Wyse Software thin client. You can log in using the options mentioned in step 2 and step 3.

To log in as a different user or administrator on a Windows 7 device:

- 1 Click **Start Menu > Log off** to log off the current desktop while holding the Shift key till the login window is displayed.
- 2 Log in using one of the following options:
 - **Administrators**—The default user name is **WyseAdmin** and default case-sensitive password is **DellCCCvdi**.
 - **Users**—The default user name is **WyseUser** and default case-sensitive password is **DellCCCvdi**.

If automatic login is not enabled, the login window displays when you boot the Wyse Software thin client. You can log in using the options mentioned in step 2.

Before configuring your Wyse Software thin clients

Unified Write Filter Utility is meant to protect your Wyse Software thin clients. If you want to retain certain profile configurations such as printers, monitors and other peripherals, you can configure NetXClean to refrain from cleaning up explicitly declared profiles. These utilities



also prevent undesired flash memory writes, and clean-up extraneous information from being stored on the local disk. The C-A-D tool allows administrators to map the Ctrl+Alt+Del key combination of VDI applications to display the Ctrl+Alt+Del screen of the VDI application. If the C-A-D tool is enabled, you can use the Ctrl+Alt+Del key combination for all VDI applications.

The Wyse Management Suite enables you to centrally configure, monitor, manage, and optimize your Wyse Software thin clients. To manage the Wyse Software thin clients remotely you must register the devices to Wyse Management suite.

However, there are instances where administrators can retain the changed configurations after you log out and restart the Wyse Software thin client.

Before configuring your Wyse Software thin clients, see

- [Using the Unified Write Filter](#)
- [Understanding the NetXClean Utility](#)
- [Understanding the C-A-D tool](#)
- [Registering Wyse Software thin client to Wyse Management Suite](#)

Unified Write Filter

Unified Write Filter (UWF) is a sector-based write filter that protects your storage media on a Windows 10 device. UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. UWF improves the reliability and stability of your device and reduces the wear on write-sensitive media, such as solid-state drives. In UWF, an overlay is a virtual storage space that saves changes made to the underlying protected volumes. Any time the file system attempts to modify a protected sector, UWF instead copies the sector from the protected volume to the overlay, and then modifies the overlay instead. If an application attempts to read from that sector, UWF returns the data from the overlay instead, so that the system maintains the appearance of having written to the volume, while the volume remains unchanged.

⚠ CAUTION: Failure to keep the Write Filter turned on (except for regular maintenance or Application/Driver installs or upgrades) will prematurely wear out your Flash/SSD storage and invalidate your warranty. Dell recommends you to enable write filter while using thin clients. To make any changes on the system, administrators must disable UWF.

For more information, see the Unified Write Filter documentation at technet.microsoft.com.

Using Unified Write Filter

To configure the Wyse Software thin client to use UWF, do the following:

- 1 Log in as WyseAdmin.
If automatic login to a user desktop is enabled, log off from the user desktop and log in as an administrator.
- 2 To disable the Unified Write Filter, double-click the **Dell Wyse WF Disable** icon on the desktop.
This icon disables the filter and reboots the system.
- 3 Configure the Wyse Software thin client as per your requirements.
- 4 After you configure the Wyse Software thin client, to enable the Unified Write Filter, double-click the **Dell Wyse WF Enable** icon on the desktop.
This icon enables the filter and reboots the system. Your configurations on the Wyse Software thin client are now saved, and they persist after you reboot the thin client.

After system start-up, the Unified Write Filter (UWF) starts automatically.

You can add specific files or folders on a protected volume to a file exclusion list to exclude those files and folders from being filtered by UWF using the Dell Wyse Unified Write Control tool. To access the tool, click the Unified Write Filter icon in the system tray. When a file or folder is in the exclusion list for a volume, all writes to that file or folder bypass UWF filtering, and are written directly to the protected volume and persist after the device restarts.

You must log in as an administrator to add or remove file or folder exclusions during run time, and you must restart the device for new exclusions to take effect.

Setting Write Filter controls

To view and manage UWF control settings, use the **Unified Write Filter Control** dialog box. To open the dialog box, double-click the UWF icon in the notification area of the administrator taskbar.

When you configure UWF control settings, some of the fields are unavailable. You can select from the list of available fields during configuration.

The Dell Wyse Unified Write Filter Control dialog box includes the following:

- **UWF status**
 - **Current Status**—Shows the status of the Unified Write Filter. The status may either be Enabled or Disabled.
 - **Boot Command**—Shows the status of the Boot Command. UWF_ENABLE means that the UWF is enabled for the next session; and UWF_DISABLE means that the UWF is disabled for the next session.
 - **RAM used by UWF**—Shows the amount of RAM allocated to the Unified Write Filter in Mega bytes (MB) and Percentage. If **Current Status** is disabled, RAM allocated to UWF is always zero (0).
 - **Amount of RAM used for UWF Cache**—Shows the amount of RAM allocated to the Unified Write Filter cache for the current session in Megabytes (MB).
 - **Warning #1 (%)**—Shows the UWF cache percentage value at which a Low Memory warning message is displayed to the user for the current session.
 - **Warning #2 (%)**—Shows the UWF cache percentage value at which a Critical Memory warning message is displayed to the user.
- **UWF Cache settings**
 - **Amount of RAM to be used for UWF Cache**—Shows the amount of RAM that is to be used as the Unified Write Filter cache for the next session in MB. This value should be in the range of 256 MB to 2048 MB. There is an extra check to ensure that this value does not exceed 50% of Total Available RAM.
- **UWF Warning settings**
 - **Warning #1 (%)**—Shows the UWF cache percentage value at which a Low Memory warning message is displayed to the user (Default value = 80, Minimum value = 50, Maximum value = 80).
 - **Warning #2 (%)**—Shows the UWF cache percentage value at which a Critical Memory warning message is displayed to the user. Once the memory level crosses the warning level 2, system automatically restarts. (Default value = 90, Minimum value = 55, Maximum value = 90)
- **Enable UWF**—Allows you to enable the Unified Write Filter and prompts you to restart the Wyse Software thin client device. To save the changes, restart the Wyse Software thin client. After the system restarts to enable the Unified Write Filter, the Unified Write Filter status icon in the desktop notification area turns green.
- **Disable UWF**—Allows you to disable the Unified Write Filter and prompts you to restart the Wyse Software thin client device. To save the changes, restart the Wyse Software thin client. After disabling the Unified Write Filter, the Unified Write Filter status icon in the desktop notification area turns red and the Unified Write Filter remains disabled after the system restarts.
- **Defaults**—Allows you to reset the UWF Cache Settings area, and the UWF Warning Settings area to their default values.
- **File Commit area**
 - **File Path**—Allows you to add, remove, and commit files to the underlying media. The system does not restart the Wyse Software thin client device. The changes are committed immediately.

 **NOTE: Delete a file path from the list, if the file is not committed.**

- **Current Session Exclusion List**
 - **File/Directory Path**—



Allows you to add and remove a file or directory, to or from the exclusion list for the next session. This retrieves the list of files or directories that are written through in the current session and the title of the pane is shown as Current Session Exclusion List. The Next Session retrieves the list of files or directories that are written through for the next session and the title of the pane is shown as Next Session Exclusion List. The system will not restart the Wyse Software thin client, and the changes are not committed until an administrator restarts the Wyse Software thin client device manually.

NetXClean utility

NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. When multiple users have logon rights to a system, the disk space is used by the profiles stored locally. NetXClean helps to reclaim disk space from latent profiles and can be used to automatically clean-up directories used for temporary caching of information. clean-up is triggered on either service startup or user logoff. It does the clean-up invisibly to the user and is completely configurable.

NetXClean is a Windows utility built to run as a service. It is a standalone utility that uses a configuration file to determine which directories and files to purge, and which profiles to not purge. The utility can be configured to:

- Delete any number of directories and their contents
- Delete just the contents of any number of directories
- Delete any number of files declared explicitly
- Delete any number of files matching wild-character file names
- Refrain from cleaning up any of the profiles
- Refrain from cleaning up any number of explicitly declared profiles
- Refrain from cleaning up any number of the most recently used profiles
- Perform the directory clean-up on service start event, user logoff event, or both events.
- Perform the file clean-up on service start event, user logoff event, or both events.
- Perform the profile clean-up on service start event, user logoff event, or both events.

NetXClean does not clean-up the following directories or any parent to these directories:

- Windows directory
- Windows System directory
- The current directory where the service is installed in

NetXClean does not delete the following profiles:

- Administrator
- skinnynt
- totalcontrol
- Default_User
- Default_user
- The profile of the last user to logon

NOTE:

- NetXClean purge selections are made by the manufacturer and should not be changed without manufacturer supervision.
- NetXClean Utility does not have any dependency on Unified Write Filter (UWF).

NetXClean Utility work flow across multiple user profiles

NetXClean Utility helps you to clean-up user profiles when you have multiple user profiles configured on your system. This is applicable in scenarios where you log in and log off from your user profiles. A typical user scenario is as follows:

- 1 Log in as an administrator.
- 2 In `netxclean.ini`, specify the profile-specific values which you want the NetXClean Utility to perform.

These values are considered by NetXClean Utility after you log off and log in to your user profiles.

If you restart or perform a hard reboot of your system, the profile-specific values are not considered because the NetXClean Utility feature on user profiles is not applicable across reboots.

For more information, see the [Dell Knowledge Base](#).

C-A-D tool

The C-A-D tool allows administrators to map the Ctrl+Alt+Del key combination of VDI applications to display the Ctrl+Alt+Del screen of the VDI application. If the C-A-D tool is enabled, you can use Ctrl+Alt+Del key combination for all VDI applications.

The following are the mapped keys for different VDI applications supported by C-A-D tool:

- Citrix—Ctrl+F1
- Dell vWorkspace—Ctrl+Alt+End
- RDP—Ctrl+Alt+End

NOTE: The C-A-D tool does not work for Xen Desktop in a Citrix session, but works only for the Citrix Xen applications.

The C-A-D tool is disabled by default. To enable the C-A-D tool, do the following:

- 1 Log in as WyseAdmin.
- 2 Disable the Write Filter.
- 3 Launch command prompt in elevated mode.
- 4 Enter `cd c:\windows\system32`.
- 5 Run the `DWKBFilterMon.exe` file and, reboot the Wyse Software thin client.
- 6 Enable the Write Filter.

Registering Wyse Software thin client to Wyse Management Suite

Register the Wyse Software thin client with Wyse Management Suite by using any of the following methods:

- Register manually through the user interface provided by the Wyse Device Agent (WDA) on the device.
- Register automatically by configuring the appropriate option tags on the DHCP server.
- Register automatically by configuring the appropriate DNS SRV records on the DNS server.

Registering Wyse Software thin clients through Wyse Device Agent User Interface

Create a group to register the Wyse Software thin client to the Wyse Management Suite. To register Wyse Software thin clients through Wyse Device Agent User Interface:

- 1 Open the **Wyse Device Agent (WDA)** application on your Wyse Software thin client. The **Wyse Device Agent** window is displayed.
- 2 From the **Management Server** drop-down list, select **Wyse Management Suite**.
- 3 Enter the server address and the port number in the respective fields.
- 4 Enter the group token. For a single tenant, the group token is an optional step.



5 Click **Register**.

After the registration is complete, the **Registered to Wyse Management Suite** message is displayed.

Registering Wyse Software thin clients by using DNS SRV record

DNS based device registration is supported with the Wyse Device Agent: 13.0 or later versions. You can register devices with the Wyse Management Suite server if DNS SRV record fields are set with valid values. The following table lists the valid values for the DNS SRV records:

Table 2. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name —_WMS_MGMT Record FQDN —_WMS_MGMT._tcp.<Domainname> Record Type —SRV	This record points to the Wyse Management Suite server URL. For example, wmsserver.acme.com:443 , where wmsserver.acme.com is the fully qualified domain name of the server where Wyse Management Suite is installed. NOTE: Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite.
Record Name —_WMS_MQTT Record FQDN —_WMS_MQTT._tcp.<Domainname> Record Type —SRV	This record directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, wmsservername.domain.com:1883 . NOTE: MQTT is optional for the latest version of Wyse Management Suite. To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example, US1— us1-pns.wysemanagementsuite.com EU1— eu1-pns.wysemanagementsuite.com
Record Name —_WMS_CAVALIDATION Record FQDN —_WMS_CAVALIDATION._tcp.<Domainname> Record Type —TEXT	This record is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this optional record if you are registering your devices with Wyse Management Suite on public cloud. Enter True , if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter False , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. NOTE: CA Validation is optional for the latest version of Wyse Management Suite.

Registering devices by using DHCP option tags

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

Table 3. Registering device by using DHCP option tags

Option Tag	Description
<p>Name—WMS</p> <p>Data Type—String</p> <p>Code—165</p> <p>Description—WMS Server FQDN</p>	<p>This tag points to the Wyse Management Suite server URL. For example, wmsserver.acme.com:443, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed.</p> <p>NOTE: Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite.</p>
<p>Name—MQTT</p> <p>Data Type—String</p> <p>Code—166</p> <p>Description—MQTT Server</p>	<p>This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, wmsservername.domain.com:1883.</p> <p>To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example,</p> <p>US1—us1-pns.wysemanagementsuite.com</p> <p>EU1—eu1-pns.wysemanagementsuite.com</p>
<p>Name—CA Validation</p> <p>Data Type—String</p> <p>Code—167</p> <p>Description—Certificate Authority Validation</p>	<p>This tag is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this option tag if you are registering your devices with Wyse Management Suite on public cloud.</p> <p>Enter True, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.</p> <p>Enter False, if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.</p>

Configuring your Wyse Software thin client

The following configurations are explained in this section:

- Configuring VMware Horizon Client. See, [Using VMware Horizon Client to connect to virtual desktop](#)
- Configuring Citrix receiver. See, [Configuring Citrix Receiver server sessions](#)
- Configuring Remote Desktop Connections. See, [Configuring Remote Desktop Connection session services](#)
- Configuring using Wyse Management Suite. See, [Configuring your Wyse Software thin client using Wyse Management Suite](#)
- Configuring RAM disk size. See, [Configuring RAM disk size](#).

For more information on other features, see Windows Embedded Standard 7 Professional, Windows 10 IoT Enterprise, and Wyse Management Suite version 1.1 and above Administrator's Guide at dell.com/support/manuals.

Topics:

- [Using VMware Horizon Client to connect to virtual desktop](#)
- [Configuring Citrix receiver session services](#)
- [Configuring remote desktop connection session services](#)
- [Configuring your Wyse Software thin client using Wyse Management Suite](#)
- [Configuring RAM disk size](#)

Using VMware Horizon Client to connect to virtual desktop

VMware Horizon Client is a locally installed software application that communicates between View Connection Server and thin client operating system. It provides access to centrally hosted virtual desktops from your thin clients.

VMware session services can be made available on the network after you install the VMware Horizon 6. It provides virtualized or hosted desktops and applications through a single platform to end users.

To connect to a virtual desktop, use the **VMware Horizon Client** window.

To open and use the **VMware Horizon Client** window:

- 1 Log in as a user or an administrator.
- 2 Access the **VMware Horizon Client** window using one of the following options:
 - From the **Start Menu**, click **VMware > VMware Horizon Client**.
 - Double-click the **VMware Horizon Client** icon on the desktop.

The **VMware Horizon Client** window is displayed.

- 3 In the **VMware Horizon Client** window, use the following guidelines:
 - a To add a new server connection, either click the **New Server** option or double-click the **Add Server** icon in the **VMware Horizon Client** window.

The **VMware Horizon Client** dialog box is displayed.
 - b In the **VMware Horizon Client** dialog box, type a host name or an IP address of a VMware Horizon Connection Server in the connection server box.
 - c Click **Connect**.
 - d In the **Login** dialog box, enter the user name and login password in the respective boxes.
 - e From the **Domain** drop-down list, select the domain where the server is located.

- f Click **Login**.

The VMware Horizon Client connects to the selected desktop. After connection is established, the list of published desktops is displayed.

- g Right-click the particular application or the desktop icon, and then click **Launch** to connect to that application or desktop.

For more information on VMware Horizon Client, see www.vmware.com.

① NOTE:

Certificate checking mode—Certificate checking mode determines how the client proceeds when the client cannot verify that your connection to the server is secure. Dell recommends that you do not change this setting unless instructed by your system administrator.

To access the certificate checking mode, click the icon on the upper-right corner of the window, and then click **Configure SSL** from the drop-down list. In the **VMware Horizon Client SSL configuration** dialog box, select from any of the following options based on your requirements:

- Never connect to untrusted servers
- Warn before connecting to untrusted servers
- Do not verify server identify certificates

Configuring Citrix receiver session services

Citrix Receiver is a server-based computing technology that separates the logic of an application from its user interface. The Citrix Receiver client software installed on the thin client device allows you to interact with the application GUI, while all the application processes run on the server.

Citrix Receiver session services are available on the network using Windows Server 2008 or Windows Server 2012 with Terminal Services and one of the following installed:

- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.8
- XenDesktop 7.9
- XenDesktop 7.11

① NOTE:

If you use a Windows Server 2003, Windows Server 2008, or Citrix XenApp 5.0 with Windows Server 2008, a Terminal Services Client Access License (TSCAL) server must also be accessible on the network. The server grants a temporary license, which expires after 120 days. After the temporary license expires, purchase and install the TSCALs on the server. You cannot establish a connection without a temporary or permanent license.

To configure a Citrix Receiver session, do the following:

- 1 Log in as an administrator.
- 2 Access the Citrix Server using one of the following options:
 - From the **Start Menu**, click **Citrix Receiver**.
 - Double-click the **Citrix Receiver** icon on the desktop.

After you log in to the Citrix server, the **Add Account** window is displayed.

- 3 In the **Add Account** window, enter the server IP address.
- 4 Click **Next**.
 - For secure connections, enter `Fully Qualified Domain Name (FQDN)`.
 - For non-secure connections, enter the IP address.
- 5 Enter the user credentials, and click **Log on**.

You can add an account by providing the IP address, and you can view the details of the Citrix Receiver.



- 6 Click **Yes**, and then click **Next**.
The virtual desktop of the Citrix receiver is displayed.
- 7 In the virtual desktop window, go to **Add Apps (+) > All Applications**.
You can select or clear the application check box. The selected applications are displayed on the virtual desktop.
- 8 On the virtual desktop, click **Settings** to refresh, add or delete server account, and log off.

Configuring remote desktop connection session services

Remote desktop connection is a network protocol that provides a graphical interface to connect another computer over a network connection.

NOTE: If you use a Windows Server 2003, Windows Server 2008, or Citrix XenApp 5.0 with Windows Server 2008, a Terminal Services Client Access License (TSCAL) server must also be accessible on the network. The server grants a temporary license, which expires after 120 days. After the temporary license expires, purchase and install the TSCALs on the server. You cannot establish a connection without a temporary or permanent license.

To configure a remote desktop connection:

- 1 Log in as a user or an administrator.
- 2 From the **Start** menu, click **Remote Desktop Connection**, or double-click the **Remote Desktop Connection** icon on the desktop.
The **Remote Desktop Connection** window is displayed.
- 3 In the **Computer** box, enter the computer or the domain name.
- 4 For advanced configuration options, click **Show Options**.
 - a In the **General** tab, you can enter the login credentials, edit or open an existing RDP connection, or save a new RDP connection file.
 - b In the **Display** tab, manage the display and the color quality of your remote desktop.
 - Move the slider to increase or decrease the size of your remote desktop. To use full screen, move the slider all the way to the right.
 - Select the color quality of your preference for your remote desktop from the drop-down list.
 - Select or clear the **Display the connection bar when I use the full screen** check box to display or hide the connection bar in full screen mode.
 - c In the **Local Resources** tab configure audio, keyboard, or local devices and resources for your remote desktop.
 - In the Remote audio section, click **Settings** for advanced audio settings options.
 - In the **Keyboard** section, choose when and where to apply keyboard combinations.
 - In the **Local devices and resources** section, select devices and resources that you want to use in your remote session. Click **More** for more options.
 - d In the **Experience** tab optimize the performance of your remote session based on the connection quality.

NOTE:

If the Unified Write Filter cache is full, you can disable the Bitmap caching in the **Experience** tab after clicking **Show Options** in the window.

- e In the **Advanced** tab, select the action to be taken when the server authentication fails and configure settings for connection through Remote Gateway.
- 5 Click **Connect**.
 - 6 To connect to the remote session, enter the login credentials in the **Security** dialog box.
The remote desktop is displayed with the connection bar on the top if you select the **Display the connection bar**.

Configuring your Wyse Software thin client using Wyse Management Suite

You can configure your Wyse Software thin client using Wyse Management Suite 1.1 and later version when the device is converted to a thin client using Wyse Converter for PCs. To configure the Wyse Software thin client, the device must be registered on Wyse Management Suite.

- 1 Log in to the Wyse Management Suite console.
- 2 Click **Groups & Configs** on the dashboard.
- 3 Select a group, and click **Edit Policies**.
- 4 Click **Wyse Software Thin Client**.

The **Wyse Software Thin Client** page is displayed.

- 5 After configuring the options, click **Save and Publish**.

For information on registering the Wyse Software thin clients and configuring the policy settings using Wyse Management Suite, see *Wyse Management Suite 1.1 Administrator's Guide* at dell.com/support/manuals.

Configuring RAM disk size

RAM disk is a volatile memory space used for temporary data storage.

The following items are typically stored on the RAM disk:

- Browser web page cache
- Browser history
- Browser cookies
- Browser cache
- Temporary internet files
- Print spooling
- User/system temporary files

To configure the RAM disk size, do the following:

- 1 Log in as an administrator.
- 2 Go to **Start > Dell Thin Client Application**.
The **Dell Thin Client Application** window is displayed.
- 3 On the left navigation bar, click **RAM Disk**.
- 4 In the **RAM disk size** field, type or select the RAM disk size you want to configure, and then click **Apply**.

If you change the size of the RAM disk, you are prompted to restart the system for the changes to take effect.

NOTE:

To permanently save the information, disable the Unified Write Filter (UWF). For more information, see [Before configuring your Wyse Software thin clients](#).



Wyse Converter for PCs license

Wyse Converter for PCs comes with a 45 day trial license. You can use the trial version to convert a PC to a thin client like experience, test the lockdown functionality, and use Wyse Management Suite to configure the Wyse Software thin client. The 45 day trial period starts from the date when Wyse Converter for PCs is installed on your PC. You will receive instructions to download Wyse Converter for PCs and Wyse Management Suite through an email when you sign up for Wyse Converter for PCs. You will also receive details on how to obtain the license key.

NOTE: During the trial period, you can register and manage 25 devices at any given point in time.

After the trial period ends:

- Upgrades through the Wyse Management Suite server are not possible.
- An administrator can continue to manage existing devices using the Wyse Management Suite on-premise server.
- A new Wyse Software thin client cannot be added to the Wyse Management Suite.

After the Wyse Device Agent communicates with the Wyse Management Suite server, the updated license information is imported and the local store is updated.

After 45 days, you can continue to use Wyse Converter for PCs by importing or upgrading the Wyse Management Suite license—see [Importing and upgrading the Wyse Management Suite license](#)

Importing and upgrading Wyse Management Suite license

To import a Wyse Management Suite license to a private cloud, do any of the following:

- **Method 1**
 - a Log in to the Wyse Management Suite private cloud server.
 - b Navigate to **Portal Administration > Account > Subscription > Import License**.
 - c Enter the user name and password.
 - d From the **Data Center** drop-down list, select the data center.
 - e Enter the number of Wyse Software thin client seats or devices you want to add, and click **Import**.

NOTE: The Wyse Management Suite private cloud server must be connected to public cloud to import the license.

- **Method 2**
 - a Log in to the Wyse Management Suite public cloud server.
 - b Navigate to **Portal Administration > Account > Subscription > Export License For Private Cloud**.
 - c Enter the number of Wyse Software thin client seats to be exported.
 - d Click **Export**.
 - e Copy the generated license.
 - f Log in to the Wyse Management Suite private cloud server.
 - g Navigate to **Portal Administration > Account > Subscription > Import License**.
 - h Enter the generated license.
 - i Click **Import**.

NOTE: You will receive your login credentials when you sign up for the Wyse Management Suite trial on www.wysemanagementsuite.com or when you purchase your subscription. You can purchase the Wyse Management Suite subscription from the Dell Sales team or from your local Dell partner. For more details, see www.wysemanagementsuite.com.

To assign a valid license, you must add and register the device to Wyse Management Suite—see [Registering Wyse Software thin client to Wyse Management Suite](#).

To upgrade the Wyse Management Suite license from evaluation to production from a public cloud, contact the Dell Sales team or your local Dell partner. After the Wyse Management Suite license is upgraded, you can log in to the Wyse Management Suite portal as an administrator with the same credentials as before to manage the device.

You can upgrade the license on a private cloud by exporting the license from public cloud account to the private cloud. To import the license on a private cloud, do any of the following:

- Go to **Portal Administration > Subscription**, enter details in the **Import License** section and click **Import**.
- Go to **Portal Administration > Subscription**, enter the license key in the **Import License** section, and click **Import**.

For more information, see *Wyse Management Suite 1.1 Administrator's Guide* at dell.com/support/manuals.



Uninstallation methods

You can uninstall Wyse Converter for PCs using any of the following methods:

- Remote uninstallation—see [Uninstalling Wyse Converter for PCs remotely](#)
- Local uninstallation—see [Uninstalling Wyse Converter for PCs locally](#)

NOTE: The .NET Framework, Microsoft Visual C++ Redistributable, Windows Management Framework, Citrix Receiver, and VMware Horizon client installed during the Wyse Converter for PCs installation are not removed when you uninstall Wyse Converter for PCs.

Topics:

- [Uninstalling Wyse Converter for PCs remotely](#)
- [Uninstalling Wyse Converter for PCs locally](#)

Uninstalling Wyse Converter for PCs remotely

You can uninstall Wyse Converter for PCs remotely using any of the following methods:

- Using third party management software—see [Uninstalling Wyse Converter for PCs using third party management software](#)
- Using Wyse Management Suite—see [Uninstalling Wyse Converter for PCs using Wyse Management Suite](#)

Uninstalling Wyse Converter for PCs using third party management software

You can uninstall Wyse Converter for PCs using a third party management software such as Microsoft System Center Configuration Manager (SCCM).

- 1 Launch the SCCM console.
- 2 Go to **Software Library > Overview > Application Management > Applications**.
- 3 Right-click **Applications**, and click **Create Application**.
The **Create Application Wizard** window is displayed.
- 4 On the **General** page, click **Manually specify the application information**.
- 5 Click **Next**.
- 6 On the **General Information** page, specify the information about the application and click **Next**.
- 7 On the **Application Catalog** page, specify the information about how you want to display the application when you browse the Application Catalog.
- 8 On the **Deployment Types** page, click **Add** to create a deployment type.
The **Create Deployment Type Wizard** window is displayed.
- 9 On the **General** page, click **Manually specify the deployment type information**.
- 10 Click **Next**.
- 11 On the **General Information** page, specify the information about the application and click **Next**.
- 12 On the **Content** page, specify the location of the Wyse Converter for PCs setup file.
- 13 In the **Installation program** field, enter `uninstaller_WyseConverterForPCs.exe`.

- 14 On the **Detection Method** page, select the **Setting Type** as **File System** and enter drive C:\Windows\Setup\Logs\UninstallWyseConvertor.log in the **Path** field.
- 15 Specify the type and the file or folder name, and click **OK**.
- 16 Click **Next**.
- 17 On the **User Experience** page, from the **Installation behavior** drop-down list, select **Install for system if resource is device; otherwise install for user**.
- 18 From the **Logon requirement** drop-down list, select **Whether or not a user is logged on**.
- 19 From the **Installation program visibility** drop-down list, select **Hidden**.
- 20 Specify the maximum run time and the estimated installation time of the deployment program for the application, and click **Next**.
- 21 On the **Requirements** page, click **Next**.
- 22 On the **Dependencies** page, click **Next**.
- 23 On the **Summary** page, the summary of the configurations is displayed.
- 24 Click **Close**.
- 25 Distribute the content to distribution point to make the content available for deployment. To distribute the content to distribution point, see *Operations and Maintenance for Content Management in Configuration Manager* at technet.microsoft.com.

Uninstalling Wyse Converter for PCs using Wyse Management Suite

- 1 Log in to the Wyse Management Suite console.
- 2 Click **Apps & Data**.
- 3 Click **Wyse Software thin client** under **App Policies**.
- 4 Click **Add Policy**.
The **Add Standard App Policy** window is displayed.
- 5 In the **Add Standard App Policy** window do the following:
 - From the **Group** drop-down menu, select the group to which the Wyse Software thin client is registered.
 - From the **Task** drop-down menu, select **Uninstall Application**.
 - From the **OS type** drop-down menu, select **Wyse Software thin client**.
 - From the **Application** drop-down menu, select **Uninstaller_WyseConverterForPCs.exe**.
- 6 Click **Save**.
- 7 Go to the **Jobs** page and schedule the job to start the silent uninstallation of Wyse Converter for PCs.

Uninstalling Wyse Converter for PCs locally

Prerequisites

- The write filter must be disabled—Windows 10 Enterprise operating system only.
- You must uninstall Wyse Converter for PCs from the administrator account available before the Wyse Converter for PCs installation.

Steps

- 1 Go to **Control Panel** and click **Programs and features**.
- 2 From the programs list, select **Wyse Converter for PCs**.
- 3 Click **Uninstall**.
The confirmation screen is displayed.
- 4 Click **Yes**.

After the uninstallation is complete, the **Uninstallation Complete** message is displayed.



i **NOTE:** You can also uninstall Wyse Converter for PCs by double-clicking the Wyse Converter for PCs executable file. Also, you can log in as an administrator, run the command prompt, and enter `uninstaller_WyseConverterForPCs.exe`. For information on silent parameters, see [Parameters for silent installation](#).



Troubleshooting Wyse Converter for PCs

This section provides troubleshooting information for Wyse Converter for PCs.

- Problem—Installation stops during the prerequisite check.

Solution—Ensure that you have met the prerequisites to install Wyse Converter for PCs—see [Prerequisites](#). The logs are available at the current user temp location (%temp%).

- Problem—Installation stops, if any application that you have selected fails to install.

Solution—View the log files **InstallWyseConverter.log** or **UninstallWyseConverter.log** for a detailed error log report.

- Problem—Lock down scripts fail during installation.

Solution—View the log files **AppsInstall.log**, **InstallMon.log**, **UninstallWyseConverter.log** available at **drive C/Windows/setup/logs** for a detailed error log report.

- Problem—License screen is displayed on the WyseUser desktop, after you purchase a valid license.

Solution—Ensure that you have registered the Wyse Software thin client to Wyse Management Suite.

- Problem—Auto logon fails during the lockdown deployment.

Solution—Ensure that the password does not contain special characters, such as \ / : * ? " < > |. If you want to proceed with the current installation, enter the password that was used in the deployment stage.

