

Windows 10 IoT Enterprise for Dell Wyse Thin Clients

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.

© 2018- 2020 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.

| | |
|--|-----------|
| 1 Introduction..... | 6 |
| Technical support..... | 6 |
| About this guide..... | 6 |
| Supported thin clients..... | 6 |
| 2 Getting started..... | 7 |
| Automatic and manual login..... | 7 |
| Before configuring your thin clients..... | 7 |
| Using your desktop..... | 8 |
| Using the Start Menu..... | 8 |
| Using the search box..... | 8 |
| Grouping Applications into Desktops..... | 8 |
| Using Action Center..... | 8 |
| Connecting to a printer or an external device..... | 9 |
| Connecting to a monitor..... | 9 |
| Power state..... | 9 |
| 3 Accessible applications..... | 10 |
| Browsing with Internet Explorer..... | 10 |
| Using the Dell Thin Client Application..... | 10 |
| Configuring Citrix Receiver session services..... | 11 |
| Citrix Workspace app | 11 |
| Configuring remote desktop connection session services..... | 12 |
| Using VMware Horizon Client to connect to virtual desktop..... | 12 |
| Using Ericom Connect and WebConnect client..... | 13 |
| Using Ericom PowerTerm Terminal Emulation..... | 14 |
| Windows Media Player..... | 14 |
| Wyse Easy Setup..... | 14 |
| Overlay Optimizer..... | 15 |
| Dell Secure Client..... | 15 |
| Key features of Dell Secure Client..... | 15 |
| Accessing Dell Secure Client..... | 15 |
| Configuring Dell Secure Client..... | 16 |
| Deploying a configuration..... | 19 |
| Command-line options..... | 19 |
| Generate and view logfiles..... | 21 |
| Tips and best practices..... | 21 |
| Error codes..... | 21 |
| 4 Administrative features..... | 23 |
| Using Administrative tools..... | 23 |
| Configuring component services..... | 23 |
| Viewing events..... | 23 |
| Managing services..... | 24 |

| | |
|---|----|
| Using TPM and BitLocker..... | 24 |
| Initialize TPM and enable BitLocker using the imaging script | 24 |
| Initialize TPM and enable BitLocker manually..... | 25 |
| Configuring Bluetooth connections..... | 26 |
| Configuring wireless local area network settings..... | 27 |
| Using custom fields..... | 27 |
| Configuring RAM disk size..... | 27 |
| Enabling auto logon..... | 28 |
| System shortcuts..... | 28 |
| Viewing and configuring SCCM components..... | 29 |
| System Center Configuration Manager Client 2016 and 2019..... | 29 |
| Devices and printers..... | 29 |
| Adding printers..... | 29 |
| Adding devices..... | 30 |
| Configuring multi-monitor display..... | 30 |
| Managing audio and audio devices..... | 30 |
| Using sound dialog box..... | 31 |
| Setting region..... | 31 |
| Managing user accounts..... | 31 |
| Using Windows Defender..... | 32 |
| Windows Defender Advanced Threat Protection..... | 32 |
| Threat Defense..... | 32 |
| Endpoint Security Suite Enterprise..... | 32 |
| C-A-D tool..... | 32 |
| Wyse Device Agent..... | 33 |
| Citrix HDX RealTime Media Engine..... | 33 |
| Viewing and exporting operating system image manifest files | 33 |
| Viewing and exporting operating system image current manifest information | 33 |
| Viewing operating system image factory manifest information..... | 34 |
| Dell Docking Station WD19 | 34 |

5 Additional administrator utility and settings information.....35

| | |
|--|----|
| Automatically launched utilities..... | 35 |
| Utilities affected by log off, restart, and shut down..... | 35 |
| Unified Write Filter..... | 36 |
| Using Unified Write Filter..... | 37 |
| Running Unified Write Filter command–line options..... | 37 |
| Enabling and disabling the Write Filter using the desktop icons..... | 38 |
| Setting Write Filter controls..... | 38 |
| Application Launch Manager..... | 39 |
| ALM CLI tool..... | 39 |
| Configuration of nodes using ALM..... | 39 |
| xData Cleanup Manager..... | 40 |
| xDCM CLI tool | 40 |
| Configuration of nodes using xDCM..... | 40 |
| Capturing logfiles..... | 41 |
| Configuration of DebugLog XML file..... | 42 |
| Saving files and using local drives..... | 42 |
| Mapping network drives..... | 43 |
| Participating in domains..... | 43 |

| | |
|--|-----------|
| Using the Net and Tracert utilities..... | 44 |
| Managing Users and Groups with User Accounts..... | 44 |
| Creating user accounts..... | 44 |
| Editing user accounts..... | 45 |
| Configuring user profiles..... | 45 |
| Changing the computer name of a thin client..... | 45 |
| 6 System administration..... | 47 |
| Accessing thin client BIOS settings..... | 47 |
| Unified Extensible Firmware Interface and secure boot..... | 47 |
| Booting from DOS USB key | 47 |
| Creating bootable UEFI USB key | 48 |
| Using Dell Wyse Management Suite..... | 48 |
| Ports and slots..... | 48 |
| TightVNC—server and viewer..... | 48 |
| TightVNC—Pre-requisites..... | 49 |
| Using TightVNC to shadow a thin client | 49 |
| Configuring TightVNC server properties on the thin client | 50 |
| 7 Network architecture and server environment..... | 51 |
| Understanding how to configure your network services..... | 51 |
| Using Dynamic Host Configuration Protocol..... | 51 |
| DHCP options..... | 51 |
| Using Domain Name System..... | 52 |
| About Citrix Studio..... | 52 |
| About VMware Horizon View Manager..... | 53 |
| 8 Installing firmware using USB Imaging Tool..... | 54 |
| 9 Frequently asked questions..... | 55 |
| How to install Skype for Business..... | 55 |
| How to set up a smart card reader..... | 55 |
| How to use USB Redirection..... | 55 |
| How to capture and push Windows 10 IoT Enterprise operating system image..... | 55 |
| 10 Troubleshooting..... | 56 |
| Keyboard customization issues..... | 56 |
| Resolving memory issues..... | 56 |
| Using Windows Task Manager..... | 56 |
| Using Unified Write Filter..... | 56 |
| Using File Explorer..... | 56 |
| Blue screen error or BSOD issues..... | 56 |
| WiFi settings configured from Wyse Management Suite are not persistent across multiple Wyse 5070 thin clients..... | 57 |

Introduction

Dell Wyse thin clients that run the Windows 10 IoT Enterprise operating system provide access to applications, files, and network resources. The applications and files are made available on machines hosting Citrix Receiver, Remote Desktop Connection, and VMware Horizon client session.

Other locally installed software permits remote administration of the thin clients and provides local maintenance functions. More add-ons are available that support a wide range of peripherals and features for environments that require a secure user interface with 64-bit Windows compatibility. For more information, see www.microsoft.com.

NOTE:

- **Windows 10 IoT operating system gets activated when you connect the thin client to the Internet. If the Microsoft activation servers are busy, you must wait until the Windows 10 IoT is activated. To check the activation status, go to Start > Settings > Update & Security > Activation.**
- **The features that are mentioned in this guide vary depending on the thin client model at your workplace. For more information about the features applicable for your thin client, see the respective User Guides at <https://support.dell.com/manuals>.**

Technical support

To access technical resources self-service portal, knowledge base articles, software downloads, registration, warranty extensions/RMAs, reference manuals, contact information, and so on, visit <https://support.dell.com>.

About this guide

This guide is intended for thin client administrators running Windows 10 IoT Enterprise. It provides information and detailed system configurations to help you design and manage a Windows 10 IoT Enterprise environment.

Supported thin clients

The following are the list of thin clients that run on Windows 10 IoT Enterprise:

- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- Wyse 5070 Thin Client with Celeron processor
- Wyse 5070 Thin Client with Pentium processor
- Wyse 5070 Extended Thin Client with Pentium processor
- Wyse 5060 Thin Client
- Wyse 7040 Thin Client
- Latitude 3480 mobile Thin Client
- Latitude 5280 mobile Thin Client

-  **NOTE: The Wyse 7040 Thin Client support Windows 10 IoT Enterprise Threshold 1 operating system and the remaining thin clients support Windows 10 IoT Enterprise Redstone 1 operating system. The Wyse 5070 Thin Client supports Windows 10 IoT Enterprise 2019 LTSC and Windows 10 IoT Enterprise 2016 LTSC operating systems.**

Getting started

The Quick Start application launches when you boot into a thin client for the first time. This tool displays the software and hardware features of the thin client. It also provides information about the VDI applications, management software, and supported peripherals.

You can also install the Wyse Easy Setup application using the Quick Start application. The Wyse Easy Setup application enables administrators to quickly and easily deploy configurations on thin clients. For more information, see [Wyse Easy Setup](#).

After you exit the Quick Start application, the user desktop is displayed by default. You can also launch the tool later.

You can log in to the thin client as a user or an administrator. An administrator can configure a user account to login automatically or manually by entering the login credentials.

You can use Wyse Management Suite to centrally configure, monitor, manage, and optimize your thin clients. For more information, see [Using Wyse Management Suite](#).

To start using your thin client, see:

- [Automatic and manual logon](#)
- [Before configuring your thin clients](#)
- [Using the Start menu](#)
- [Using the Search Box](#)
- [Using Action Center](#)
- [Grouping applications into desktops](#)
- [Connecting to a printer or an external device](#)
- [Power state](#)

Automatic and manual login

When a thin client turns on or reboots, you can log in automatically or manually with user or administrator credentials depending on the administrator's configuration.

For more information, see [Managing Users and Groups with User Accounts](#).

NOTE:

- **Ensure that you disable the Unified Write Filter (UWF) before you change a password on the thin client, and then enable UWF after your change. For more information, see [Before configuring your thin clients](#).**
- **To change the password, press Ctrl+Alt+Delete, and then click Change a password. However, this feature is not applicable for User accounts.**

When you start the thin client, you will automatically log in to the user desktop by default.

To log in with a different user account, you must sign out and click the preferred user account on the login screen. You can use the following credentials to log in to different user accounts:

- **Administrators**—The default user name is **Admin** and the default case-sensitive password is **DellCCVdi**.
- **Users**—The default user name is **User** and default case-sensitive password is **DellCCVdi**.
- **Customized User**—Log in to your thin client by entering the user credentials which you have set for the customized user account.

Before configuring your thin clients

Before you configure your thin clients, ensure that you configure Unified Write Filter and xData Cleanup Manager that protect your thin clients. The Unified Write Filter Utility prevents undesired flash memory writes, and xData Cleanup Manager cleans up extraneous information from being stored on the local disk.

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

Using your desktop

The administrator set configurations are displayed when you log in to the thin client at the first instance.

If you log in as an administrator, the **Administrator Desktop** is displayed. On the right of the taskbar, click the **Notifications** icon to open the **Action Center** window. For more information about the Action Center, see [Using Action Center](#).

In addition to the Standard Desktop icons, an extended set of resources for configuring user preference settings and system administration is included in the administrator control panel. To open control panel, go to **Start > Control Panel**. For more information, see [Administrative features](#).

Using the Start Menu

About this task

The **Start Menu** helps you to access all programs, folders, and settings on your thin client. It contains a list of applications that are installed on your thin client.

 **NOTE:** On the Start Menu, you can view the list of frequently used applications under **Most Used**.

Using the search box

About this task

Use the search box on the taskbar to look for applications, files, or settings. You can type what you are searching for in the search box on the taskbar. You can also find results for files, applications, or settings across your thin client. The suggestions and results related to your searched item are displayed in the **Home** window.

Next steps

 **NOTE:** To search for a particular file on your thin client, apply any of the following filters available in the lower pane of the Home window, and then search for your desired file:

- **Applications filter**
- **Settings filter**
- **Documents filter**
- **Folders filter**
- **Photos filter**
- **Videos filter**
- **Musics filter**

Grouping Applications into Desktops

Create virtual desktops, to group your applications together. In the taskbar, click the **Task View** icon, and then in the **New Desktop**, open the applications you need.

To move applications between virtual desktops, click **Task View**, and then drag the application you want from one desktop to another.

Using Action Center

Action center displays important notifications from Windows and your applications on the taskbar, along with quick actions, which get you to your most-used settings and applications instantly.

To view your notifications and quick actions, click the **Action Center** icon on the taskbar. You can also press Windows logo key+A.

- **Notifications at a glance**—When a notification appears on your desktop or when you view it in **Action Center**, expand it to read more or take action without having to open the related application. You can also clear the notification by selecting and dragging it off the screen to the right, or by clicking the **Close** button.

- **Quick Action icons**—Quick Action icons allow you to access **All Settings** and applications that you use often, such as Bluetooth to VPN. Select the **Expand** option to see the settings and applications such as location, the quiet hours, brightness, bluetooth, VPN, the battery saver, project, and connect.

The following are the **Quick Action** options in the Action Center:

- **Tablet Mode**—Tablet mode makes Windows easier and more intuitive to use with touch on devices such as 2-in-1s, or when you do not want to use a keyboard and mouse. To turn on tablet mode, click the **Action Center** icon on the taskbar, and then select **Tablet Mode**.
- **Connect**—Use this option to connect to your wireless and bluetooth devices.
- **All Settings**—Use this option to configure windows settings. For more information, see [Using the Start Menu](#).
- **Airplane mode**—Use this option to turn off the wireless transmission functions on your device and enable **Airplane mode**.

Connecting to a printer or an external device

You can connect USB-interfaced printers or a USB-to-parallel adapter-interfaced printer to your thin client device using a USB port. Follow your printer's USB installation instructions before connecting to a USB port.

To connect to the printer, add the printer to the thin client device by using the **Add Printer** wizard. For more information, see [Adding printers](#).

If you want to connect to an external device, add the device to the thin client device. For more information, see [Adding devices](#).

Connecting to a monitor

Based on the thin client model, you can connect to an external monitor using the following ports:

- HDMI port
- VGA port
- DisplayPort
- DVI port
- DVI-D port
- Type-C port

For more information about configuring a dual monitor display, see [Configuring dual monitor display](#).

Power state

About this task

You can change the power state options of the thin client device by following the steps mentioned here:

Steps

1. On the taskbar, click the **Start Menu** button.
2. Click **Power** on the start menu, and select any of the options:
 - **Sleep**—This mode uses little power, your thin client device starts up faster.
 - **Shut down**—Preferred for closing all your open programs, and to shut down your operating system.
 - **Restart**—The thin client device is turned off and turned on instantly.

To use the power state options press ALT+F4, and then select your preferred option from the drop-down list.

 **NOTE:** If automatic login is enabled, the thin client immediately logs in to the default user desktop.

Accessible applications

When you log in to your thin client as an administrator or a user, the Windows desktop displays certain extended features in the **Start** menu.

You can perform the following tasks:

- [Browse the Internet with Internet Explorer](#)
- [Use the Dell Thin Client Application](#)
- [Configure Citrix Receiver Session Services](#)
- [Configure Remote Desktop Connection Session Services](#)
- [Use VMware Horizon Client to connect to a Virtual Desktop](#)
- [Use Ericom PowerTerm Terminal Emulation](#)
- [Use Ericom Connect-WebConnect Client](#)
- [Windows Media Player](#)
- [Wyse Easy Setup](#)

NOTE: **Keyboard Caps Lock Indicator Application**—Dell Keyboard driver software (KM632) software provides the **Caps Lock** status indication on the desktop. After you log in to your thin client, when you press the **Caps Lock** key to enable the **Caps Lock** feature, the lock symbol is displayed on the desktop. If you press the **Caps Lock** key again to disable the **Caps Lock** feature, the unlock symbol is displayed on the desktop.

Browsing with Internet Explorer

To open Internet Explorer, do either of the following:

- Go to **Start > Windows Accessories > Internet Explorer**.
- Double-click the **Internet Explorer** icon on the desktop.

NOTE:

- **To limit writing to the disk, Internet Explorer settings are set at the factory. The settings prevent you from using the limited amount of disk space available. It is recommended that you do not modify these settings.**
- **Internet Explorer cache settings are set to 100 MB.**

Using the Dell Thin Client Application

Use the Dell Thin Client Application to view the general information about the thin client device, custom fields, RAM disk, auto login, system shortcuts, and support information.

To access the **Dell Thin Client Application** page, go to **Start > Dell Thin Client Application**. You can also access the **Dell Thin Client Application** by clicking the **Dell Thin Client Application** icon on the desktop.

In the left navigation bar, click the following tabs:

- **Client Information**—Displays the thin client device information.
- **QFE**—Displays the list of Microsoft QFEs (previously known as hot fixes) applied to the thin client.
- **Installed Products**—Displays the list of applications that are installed on the thin client.
- **WDM/WMS Packages**—Displays the list of WDM and WMS packages that are applied to the thin client.
- **Copyrights/Patents**—Displays copyrights and patents information.

When you log in as an administrator, you can view the tabs such as **Custom Fields**, **RAM disk**, **Auto Logon**, **System Shortcuts**, and **About and Support** on the **Dell Thin Client Application** page.

Energy Star logo (an electronic logo) for the Energy Star compliance is also displayed on the **Dell Thin Client Application** page.

In the **About and Support** tab, you can view the information related to the application version, support directory, export support data, and HTML view.

For more information, see [Administrative features](#).

NOTE: The information shown in the dialog box varies for different thin client devices and software releases. When you log in as a user, only few tabs such as Client Information, QFE, Installed Products, WDM/WMS Packages, Copyrights/Patents, and About and Support are displayed.

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 enables you to interact with the application GUI, while all the application processes run on the server.

About this task

Citrix Receiver session services are available on the network using Windows Server 2008, Windows Server 2012, or Windows Server 2016 with Terminal Services and one of the following installed:

- Citrix Virtual Apps and Desktops 7.5
- Citrix Virtual Apps and Desktops 7.6
- Citrix Virtual Apps and Desktops 7.8
- Citrix Virtual Apps and Desktops 7.9
- Citrix Virtual Apps and Desktops 7.11
- Citrix Virtual Apps and Desktops 7.18

NOTE:

If you use a Windows Server 2008 R2, 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:

Steps

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.

Citrix Workspace app

You can install Citrix Workspace app on the thin client to access your applications and desktops using Citrix Virtual Apps and Desktops from a remote client device. Citrix Workspace app provides access from your desktop, Start menu, Citrix Workspace user interface, and web browsers. You can use Citrix Workspace app on domain and non-domain joined thin clients. For more information, see *Citrix Workspace app for Windows Embedded Operating System Release Notes* at support.dell.com.

Configuring remote desktop connection session services

Prerequisites

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, or Citrix XenApp 5.0 with Windows Server, 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.

About this task

To configure a remote desktop connection:

Steps

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**.

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.

About this task

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

Steps

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.

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. It is recommended 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**

Using Ericom Connect and WebConnect client

Prerequisites

Ericom Connect and WebConnect client provides you with remote access to Windows desktops and applications from any compatible phone or tablet. It is dedicated for managed broker access. Ericom Connect and PowerTerm WebConnect connections use the Secure Gateway as the address. You can access the Ericom Connect-WebConnect client either as a stand-alone application or on a network.

About this task


To access the Ericom Connect and WebConnect client as a stand-alone application:

Steps

1. Log in as a user or an administrator.
2. Go to **Start > Ericom Connect-WebConnect client > Ericom Connect-WebConnect client** or double-click the **Ericom Connect-WebConnect client** icon on the desktop.

The **Ericom AccessPad** login window is displayed.

3. In the **Ericom AccessPad** login window, enter your credentials, and click **Login**.
The **DELL – Ericom Application Zone** window is displayed.

 **NOTE: By default, the Ericom AccessPad login window is displayed. To set the UI to your preferred language, click the Globe icon in the lower-right corner of the window, and select your preferred language from the drop-down list.**

4. In the **DELL – Ericom Application Zone** window, published applications such as the **Blaze demo server**, **RDP demo server**, the **Ericom server**, and **Paint** are displayed.
Double-click any of the applications to access them.

You can also add your own applications from the server site.

5. To create a shortcut on your desktop, click **Options > Create a shortcut on Desktop** in the **DELL – Ericom Application Zone** window.
6. To log out, click **File > Logout** in the **DELL- Ericom Application Zone** window.

Example

To access the Ericom Connect-WebConnect client through the web browser:

1. Double-click the **Internet Explorer** icon.
The **Internet Explorer** web page is displayed.
2. Enter `http://serverIP/FQDNWebConnect6.0/AppPortal/Index.asp` URL to access the Ericom Power Term Emulation.
The **PowerTerm WebConnect Application Portal** page is displayed.
3. In the **PowerTerm WebConnect Application Portal** page, enter the credentials and the domain name.
4. Click **Login**.
5. After you log in, the published desktops and applications such as the **Blaze demo server**, **RDP demo server**, and **Paint** are displayed.
Double-click any of the applications to access them on a new web page.
You can also add your own applications from the server sit.
6. Click **Logout** on the left side of the **PowerTerm WebConnect Application Portal** page to end the Ericom Power Term WebConnect session.

Using Ericom PowerTerm Terminal Emulation

About this task

To manage your connections using Ericom PowerTerm Terminal Emulation, do the following:

Steps

1. Open the **TELNET : PowerTerm InterConnect for thin clients** window, using one of the following options mentioned:
 - Double-click the **PowerTerm Terminal Emulation** icon on the desktop.
 - From the **Start Menu**, click **Ericom PowerTerm Terminal Emulation > PowerTerm Terminal Emulation**.
2. In the **Connect** dialog box, go to **Session Type > TELNET** to configure the connection of your choice.

Windows Media Player

Windows Media Player provides an intuitive, and easy-to-use interface to play digital media files. It organizes your digital media collection, and you can burn CDs of your favorite music, extract music from CDs, sync digital media files to a portable device, and shop for digital media content from online stores. For more information, see Windows media player documentation at <https://support.microsoft.com>.

Wyse Easy Setup

Wyse Easy Setup enables administrators to quickly and easily deploy configurations on thin clients.

Wyse Easy Setup enables you to:

- Create a dedicated browser-focused client by configuring the Internet Explorer settings.
- Configure multiple broker connections such as Citrix, VMware, and Remote Desktop Protocol (RDP).
- Configure a device to create a dedicated application for a particular line of business.

You can create a kiosk mode to lock down a Windows device to prevent users from accessing any features or functions on the device outside of the kiosk mode. You can also customize the kiosk interface to enable or disable user access to specific settings.

For more information, see Wyse Easy Setup videos at www.youtube.com, and Wyse Easy Setup Administrator's Guide and Release notes at <https://downloads.dell.com/wyse>.

Overlay Optimizer

Overlay Optimizer is a software component that works with Microsoft Unified Write Filter (UWF). Overlay Optimizer provides write protection and extends the uptime of devices. Overlay optimizer works on the Windows 10 IoT Enterprise operating system.

The UWF protects the disk by storing the changes in the RAM overlay. When an application tries to write data to the disk, the write filter redirects the write operations to the RAM overlay. The overlay size is preconfigured and cannot increase dynamically. When the overlay runs out of space over a period, the device restarts.

The Overlay Optimizer monitors the UWFs' overlay space and the content. Overlay Optimizer identifies higher overlay space consumption in write filter and moves the unused content to the Overlay Optimizer's disk overlay. Clearing the UWF overlay extends the device uptime.

For more information, see *Overlay Optimizer Release notes* at <https://downloads.dell.com/wyse/>.

Dell Secure Client

Dell secure client is a security software for Windows-based thin clients. This software applies restrictions to the changes made to files, folders, and registry exclusions.

Key features of Dell Secure Client

The following are the key features of the Dell Secure Client:

- The list of files, folders, and registry exclusions in the write filter is displayed.
- The status of the Dell Secure Client regarding the Unified Write Filter is displayed.
- The Dell Secure Client service acts as a policy engine. It combines the policies of the nested folders and updates the same in the registry hive.
- You can use the Dell Secure Client command-line interface to update the .csv file with the policies when the administrator makes any changes using the user interface.
- The administrator can use the Dell Secure Client to add, view, and remove policies of the excluded files and registries in the write filter.
- You can add, remove, view, or modify the policy based on username, application, and the time of access for each entry in the write filter exclusion list.

 **NOTE: The user name and application name are mandatory.**

- You can import and export the policy configuration data in .csv or .json format.
- You can export the policy as a Self-Contained Executable (SCE) .exe file. The SCE file encapsulates the policy configuration in .json format.
- Multilingual support for the administrator user interface is provided.
- Provision to retain the Dell Secure Client configurations added by the user after you restart the thin client.
- You can configure the policies only after you disable the write filter.
- The default policies are applied to all users when the Dell Secure Client is enabled.
- You can add a policy to a user or a group using the Dell Secure Client user interface or command-line interface. This policy is applied along with the default policy when you log in to the respective user or a group.
- The policies are saved in .csv format that is encrypted.

Accessing Dell Secure Client

You can access the Dell Secure Client by using any one of the following methods:

- By using an administrator account:
 1. Log in as an administrator.
 2. Go to **Start > Dell > DellSecureClient**.
- By using a user account:
 1. Log in as a user.

2. Go to **Start > Dell > DellSecureClient**.

The **User Account Control** window is displayed.

3. Enter the administrator password, and click **Yes**.

Configuring Dell Secure Client

You can configure the Dell Secure Client by using any of the following methods:

- Wyse Management Suite
- Local administrator user interface—Dell Secure Client GUI

Configuring policy using the Dell Secure Client user interface

You can import or export a configuration from the Dell Secure Client user interface.

Import a configuration

Steps

1. Disable the write filter.
The thin client restarts.
2. Log in as an administrator.
3. Double-click the Dell Secure Client application.
The **Dell Secure Client** user interface is displayed.
4. Click **Export/Import**.
5. Enter the path of the configuration file.
6. Click **Import**.
The configuration policy is encrypted and saved as a .csv file at `C:\Program Files\Wyse\DellSecureClient\`.

Export a configuration

Steps

1. Disable the write filter.
The thin client restarts.
2. Log in as an administrator.
3. Double-click the Dell Secure Client application.
The **Dell Secure Client** user interface is displayed.
4. Click **Export/Import**.
5. Enter the path of the configuration file.
6. Select the file format—.csv (Dell Secure Client settings) or .exe (installable package) options.
7. Click **Export**.
The configuration policy is decrypted and exported.

CSV format

The output .csv file is in the following format:

Table 1. .csv format

| Policy Type | File/Folder | Apps | NT Account | Time Range(Optional) |
|-------------|--------------------|---|------------|----------------------|
| file | C:\Temp\Sample.txt | C:\Windows\System32\notepad.exe | User | 0700-1900 |
| folder | C:\Temp\ | C:\Program Files\Windows NT\Accessories\Wordpad.exe | User | 0700-1900 |

| Policy Type | File/Folder | Apps | NT Account | Time Range(Optional) |
|-------------|--|--|------------|----------------------|
| file | C:\Temp\Sample2.txt | C:\Windows\System32\notepad.exe | Admin1 | |
| folder | C:\Program Files\Windows Defender | C:\Windows\System32\mspaint.exe | System | |
| registry | HKLM\SOFTWARE\WOW6432Node\3DMAX | C:\Program Files(x86)\AutoCAD\autocadx86.exe | User | |
| registry | HKLM\SOFTWARE\WOW6432Node\3DMAX | C:\Program Files(x86)\AutoCAD\autocadx86.exe | Admin1 | |
| registry | HKLM\SOFTWARE\WOW6432Node\Dell\CommandUpdate | C:\Program Files\Dell\CommandMonitor\dataeng\bin\dsm_sa_datmgr64.exe | System | |
| registry | HKLM\SOFTWARE\WOW6432Node\Dell\CommandUpdate | C:\Program Files\Dell\CommandMonitor\dataeng\bin\dsm_sa_datmgr64.exe | Admin2 | 0900-1000 |

JSON format

The output .json file is in the following format:

```
{
  "deviceElements": null,
  "deviceElementsV2": null,
  "fullConfiguration": false,
  "shouldSendRemoteCommand": false,
  "isJailBroken": false,
  "compliantStatus": 0,
  "configCompliantStatus": 0,
  "passcodeCompliant": true,
  "encryptionCompliantStatus": 1,
  "computeJailbreak": true,
  "isCaValidationOn": false,
  "personInfoLean": null,
  "lastUpdatedAt": 1534142918777,
  "passcodeProfileDescription": null,
  "deviceQueryId": null,
  "deviceQueryStatus": null,
  "configurations": {
    "contentProvider": null,
    "description": null,
    "configSettings": [
      {
        "targetOS": null,
        "configName": "rcDellSecureClientSettings",
        "configItems": [
          {
            "itemKey": "rcDellSecureClientSettings",
            "itemValue": [
```

```

[
  {
    "itemKey": "policyType",
    "itemValue": "file",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "location",
    "itemValue": " C:\\Program Files\\AutoCAD ",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "application",
    "itemValue": " C:\\Program Files\\AutoCAD\\audtocadx64.exe ",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "user",
    "itemValue": " User ",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "duration",
    "itemValue": "0700-1900",
    "itemValueExtra": null,
    "valueType": "STRING"
  }
],
[
  {
    "itemKey": "policyType",
    "itemValue": "registry",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "location",
    "itemValue": " HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\3DMAX ",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "application",
    "itemValue": " C:\\Program Files (x86)\\AutoCAD\\audtocadx86.exe",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "user",
    "itemValue": "User ",
    "itemValueExtra": null,
    "valueType": "STRING"
  },
  {
    "itemKey": "duration",
    "itemValue": "0700-1900",
    "itemValueExtra": null,
    "valueType": "STRING"
  }
]
],
"itemValueExtra": null,
"valueType": "JSON"
}
],
"contentVersion": "2.3.0"
}
],
},

```

```

"allowUnregistration": true,
"businessRuleInfo": null,
"currentBiosAdminPassword": null,
"mqttUrl": "tcp://10.150.38.10:1883",
"wmsUrl": "https://brl-hackthon-win12R2:443/ccm-web",
"heartbeatIntervalInMins": 0,
"checkInIntervalInHours": 0,
"groupToken": null,
"personalDeviceSettings": null,
"wmsVersion": "4.3.0",
"maxCheckinIntervalInHours": 0
}

```

Self-extracting file

The self-extracting .exe output file consists of the policy configuration file in .json format. The self-extracting .exe file invokes the dscmgr value with import command with the configuration file as an input.

The file can be used to import the configuration to multiple clients using advanced application policy in Wyse Management Suite. The file also returns success codes when you import a policy.

Deploying a configuration






You can deploy a configuration to multiple thin clients by using the following methods:



- Dell Secure Client user interface
- Wyse Management Suite

Command-line options

Table 2. Command-line options

| Command line | Description |
|---|---|
| dscmgr /help or dscmgr ? | Use this command to view the Help menu of the Dell Secure Client. |
| dscmgr /init [Mode] | Use this command to start the Dell Secure Client in application hash or application path mode. Application mode is the default mode and if you do not enter any value, the default mode is selected. [Mode]—Enter the mode to enable or block the access. You can use the application binary hash or application path. This parameter is optional. |
| dscmgr /getappauthenticationmode | This command displays the applied application authentication mode. |
| dscmgr /addpolicy <Path of the file, folder, or registry key> <Local Windows Username> <Application Name> [Time Duration] [Policy Type] | Use this command to add a policy to the Dell Secure Client. This command is enabled after you restart the thin client. Path of the file, folder, or registry key—The modifications to the file, folder, or registry key is monitored by the Dell Secure Client. The path that is entered must be available in the UWF exclusion list. Local Windows Username—Enter the username of the resource to provide access to the Dell Secure Client. Application Name—Enter the application name through which the modifications are enabled to the resource. Time Duration—Enter the time duration during which the modifications are enabled. This parameter is optional. If you do not enter any value, you can modify the policy anytime. |

| Command line | Description |
|--|---|
| | <p>Policy Type—Determines the type of policy. The value can be a file or registry only. This parameter is optional.</p> <p>For example, the command <code>dscmgr /addpolicy C:\Users\Administrator\Test.txt Administrator C:\Windows\System32\notepad.exe 0900-1100</code> enables an administrator to modify C:\Users\Administrator\Test.txt during 9 AM to 11 AM using notepad.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <pre>dscmgr /removepolicy <Path of File or Folder or Registry Key> <Local Windows Username> <Application Name> [Time Duration]</pre> | <p>Use this command to remove a policy to the Dell Secure Client. This command is enabled after you restart the thin client.</p> <p>Path of the file, folder, or registry key—The modifications to the file, folder, or registry key is monitored by the Dell Secure Client. The path that is entered must be available in the UWF exclusion list.</p> <p>Local Windows Username—Enter the username of the resource to provide access to the Dell Secure Client.</p> <p>Application Name—Enter the application name through which the modifications are enabled to the resource.</p> <p>Time Duration—Enter the time duration during which the modifications are enabled. This parameter is optional. If you do not enter any value, you can modify the policy anytime.</p> <p>Policy Type—Determines the type of policy. The value can be a file or registry only. This parameter is optional.</p> <p>For example, the command <code>dscmgr /removepolicy C:\Users\Administrator\Test.txt Administrator C:\Windows\System32\notepad.exe 0900-1100</code> removes access to C:\Users\Administrator\Test.txt for an administrator during 9 AM to 11 AM using notepad.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <pre>dscmgr /enabledsc</pre> | <p>Use this command to enable the Dell Secure Client. This command is enabled after you restart the thin client.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <pre>dscmgr /disabledsc</pre> | <p>Use this command to disable the Dell Secure Client. This command is enabled after you restart the thin client.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <pre>dscmgr /exportpolicy <File Path></pre> | <p>Use this command to export the policies from the Dell Secure Client to a file.</p> <p>File Path—Enter the file path where the policies must be exported. File extension should be .json or .csv. If the file is not present, a new file is created. If the file exists, the contents of the file are updated.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <pre>dscmgr /importpolicy <File Path></pre> | <p>Use this command to import the policies to the Dell Secure Client from a file. The file must have valid set of policies as mentioned in the /addpolicy command. This command is enabled after you restart the thin client.</p> |

| Command line | Description |
|---|---|
| | <p><code>File Path</code>—Enter the file path where the policies must be imported. File extension should be .json or .csv.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <code>dscmgr /exportinstallablepackage <Folder Path></code> | <p>Use this command to export the policies to the Dell Secure Client as a self-extractable executable file. The file can be used to deploy the same policies on multiple devices.</p> <p><code>Folder Path</code>—Enter the file path where the policies must be exported. <code>DefaultDSCPolicy.exe</code> file is created in the folder.</p> <p> NOTE: To use this command, the write filter must be disabled.</p> |
| <code>dscmgr /getdscstate</code> | <p>Use this command to view the current state of the Dell Secure Client. If the Dell Secure Client is enabled, 1 is displayed, and if it is disabled, 0 is displayed.</p> |

Generate and view logfiles

About this task

Log files contain a record of events of the Dell Secure Client. This section describes the steps to generate and view the logfiles.

Steps

1. Go to `C:\Program Files\Wyse\WyseLoggingLevel.ini`.
2. Update the `[LoggingLevel] DSCSVC` parameter to 4.
You can view the logfiles for different Dell Secure Client components at `C:\Wyse\WDA\DellSecureClient`.

Tips and best practices

This section provides information about the best practices, and tips that help you to work effectively on the Dell Secure Client.

- Before you enable and configure the Dell Secure Client, ensure that the UWF Overlay is set to RAM.
- It is recommended to disable the write filter before you configure the Dell Secure Client user interface.
- It is recommended that you do not disable the Dell Secure Client to secure the write filter exclusion list.
- The policies are displayed in the respective folders in the **Write Filter Exclusion** field in the Dell Secure Client user interface.

Error codes

Table 3. Error codes

| Error code | Description |
|--------------------------------------|--|
| <code>localInvalidFileError</code> | Select a valid file path to export the Dell Secure Client configuration. |
| <code>localExportFormatMsg</code> | Select the export format. |
| <code>cliPolicyExistsErrorMsg</code> | Policy exists. |
| <code>cliPolicyDoesntExist</code> | Policy does not exist. |
| <code>cliInvalidPolicy</code> | Invalid policy for the configuration. |
| <code>cliIgnorePolicy</code> | Ignore the policy. |
| <code>cliInvalidFileExtension</code> | Invalid file extension is entered. |

| Error code | Description |
|--------------------------------|---|
| localEnterAppPath | Enter the application path. |
| localEditSuccess | Edit is successful. |
| localFinishAddEditMsg | Complete the add or edit message. |
| localExceptionInConfigMsg | Invalid exception value in the policy of the configuration file. |
| localWriteFilterEnabledWarning | To modify the Dell Secure Client state and policies, you must disable the write filter. |
| localInvalidData | Invalid data at index is entered. |
| localAbortEditMsg | Aborting edit. |
| cliErrorDSCState | Error while querying the state of Dell Secure Client. |
| localCorruptFileErrorMsg | The configuration file may be corrupted. If the file is corrupted in the next boot, default policies are applied. |
| cliPolicyLocationErrorMsg | Policy location is not found in the UWF exclusion list. |
| cliInvalidCommandErrorMsg | Invalid Command. Enter <code>dscmgr help</code> to list the commands available in the Dell Secure Client. |
| cliInvalidCommand | Invalid Command |
| cliErrorConfigFileRead | Error while reading the configuration file. |
| localAddPolicyErrorMsg | Mandatory fields are not provided, and the policy cannot be added. |

Administrative features

Admin is a default user profile created for the user who is a member of the administrator group.

To log in as an administrator, see [Automatic and manual login](#). When you log in to your thin client device as an administrator, you can access certain notable extended features in the Control Panel.

To access the **Control Panel**, on the taskbar, click **Start Menu > Control Panel**.

You can perform the following functions as an administrator:

- [Using the administrative tools](#)
- [Using TPM and BitLocker](#)
- [Using custom fields](#)
- [Configuring RAM disk size](#)
- [Enabling auto logon](#)
- [Using system shortcuts](#)
- [Viewing and configuring SCCM components](#)
- [Adding devices](#)
- [Adding printers](#)
- [Configuring dual monitor display.](#)
- [Using the sound dialog box.](#)
- [Setting region and Language preferences.](#)
- [Managing users and groups with user accounts.](#)
- [Using Windows Defender.](#)
- [Using Windows Defender Advanced Threat Protection \(ATP\)](#)
- [Threat Defense](#)
- [Endpoint Security Suite Enterprise](#)
- [Using the CAD tool.](#)
- [Configuring Wyse Device Agent.](#)
- [Configuring Citrix HDX RealTime Media Engine.](#)

Using Administrative tools

To access the **Administrative Tools** window, click **Start > Control Panel > Administrative Tools**.

You can use the **Administrative tools** window to perform the following tasks:

- [Configuring the component services](#)
- [Managing the services](#)

Configuring component services

About this task

To access and configure the component services, event viewer, and local services use the **Component Services** console.

For more information, see *Administrative Tools in Windows 10* at <https://support.microsoft.com>.

Viewing events

About this task

To view monitoring and troubleshooting messages from Windows and other programs, use the Event Viewer window.

In the Component Services console, click the **Event Viewer** icon from the **Console Root** tree. The summary of all the logs of the events that have occurred on your computer is displayed. For more information, see *Event Viewer* at <https://support.microsoft.com>.

Managing services

To view and manage the services installed on the thin client device, use the **Services** window. To open the **Services** window, go to **Start > Control Panel > Administrative Tool Services**.


Steps

1. In the **Component Services** console, click the **Services** icon from the console tree. The list of services is displayed.
2. Right-click the service of your choice. You can perform Start, Stop, Pause, Resume, and Restart operations.

You can select the Startup type from the drop-down list:

- Automatic (Delayed Start)
- Automatic
- Manual
- Disabled

For more information, see *Component Services Administration* at <https://support.microsoft.com>.

 **NOTE: Ensure that the Write Filter is disabled while managing the services.**

Using TPM and BitLocker

Trusted Platform Module (TPM)—A TPM is a microchip that provides basic security-related functions, that primarily involve encryption keys.

BitLocker Drive Encryption (BDE)—A BDE is a full disk encryption feature that protects data by providing encryption for entire volumes. By default, it uses the AES encryption algorithm in Cipher Block Chaining (CBC) mode with a 128-bit key. This algorithm is combined with the Elephant diffuser for extra disk encryption-specific security.

Windows 10 IoT Enterprise does not support sysprep on a BitLocker encrypted device. Due to this limitation, you cannot encrypt the device, perform a sysprep, and pull the image. To overcome this issue, you must add or modify the TPM script. The device must not be encrypted before sysprep (pull). The device encryption is handled by the post push script that uses the `TPM_enable.ps1` script that is at `C:\Windows\setup\tools\`. The post push script must be included before enabling the UWF and after sysprep scripts. The PIN used to encrypt the client must be passed to the script as an argument.

You can initialize TPM and enable BitLocker using any of the following methods:

- [Initialize TPM and enable BitLocker using the imaging script.](#)
- [Initialize TPM and enable BitLocker manually.](#)

Initialize TPM and enable BitLocker using the imaging script

Prerequisites

Enable alphanumeric pin support for TPM and BitLocker using the following steps:

1. Log in to the administrator account.
2. Disable Unified Write Filter.
The thin client restarts.
3. Log in to the administrator account again.
4. Open `gpedit.msc` using the run command menu.
5. Go to **Local Group Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Allow enhanced PINs**.
The **Allow enhanced PINs for startup** window is displayed.
6. Select the **Enabled** option.

7. Click **Apply** and then click **OK**.
8. Open `gpupdate /force` using the run command.
9. Restart the thin client to apply the group policies.

Steps

1. Log in to the administrator account.
2. Disable Unified Write Filter.
The thin client restarts.
3. Log in to the administrator account again.
4. Uncomment the following lines and update the pin—minimum of six characters—for TPM encryption:
 - If you are using Wyse Management Suite or USB Imaging tool—Go to `C:\Windows\Setup\CustomSysprep\Modules\Post_CustomSysprep.psm1` and uncomment the following lines:
 - `#cd C:\Windows\setup\Tools\TPM\`
 - `#.TPM_enable.ps1 -pin TC#1234`
 - If you are using System Center Configuration Manager—Go to `C:\Windows\Setup\ConfigMgrSysprep\Modules\Admin_ConfigMgrSysprep.psm1` and uncomment the following lines:
 - `#cd C:\Windows\setup\Tools\TPM\`
 - `#.TPM_enable.ps1 -pin TC#1234`
5. Change the password to an alphanumeric format.
6. Go to `C:\Windows\Setup`.
7. Run **Build_master**.
8. Run **Custom Sysprep** if you are using Wyse Management Suite or USB Imaging tool or **ConfigMgr Sysprep** if you are using System Center Configuration Manager.
The thin client automatically turns off.
9. Turn on the thin client and pull the image from the thin client.
10. After the image pull is complete, push the image to the target client. Wait for the execution of first boot scripts and BitLocker encryption to complete.
When the Sysprep is completed the target thin client reboots and the **TPM** is enabled.
11. Enter the BitLocker password and verify the new alphanumeric password.
12. Log in to the administrator account and verify the encryption of the C drive.

- NOTE:** To update the BIOS in BitLocker encryption do the following:
- a. Copy the BIOS executable file to the USB drive.
 - b. Connect the USB to the respective thin client.
 - c. Right-click the BIOS executable and select Run as administrator.
 - d. Select the Suspend BitLocker Drive Encryption checkbox and then click Update. Thin client reboots and the BIOS is updated. Also the BitLocker is suspended for one reboot.
 - e. Reboot the thin client to ensure that the BitLocker is active.

Initialize TPM and enable BitLocker manually

Steps

1. Log in to the administrator account.
2. Disable Unified Write Filter.
The thin client restarts.
3. Log in to the administrator account again.
4. Open `tpm.msc` using the run command menu.
5. Verify the TPM status in **Trusted Platform Module Management** on the thin client.
The status should be displayed as **The TPM is ready for use**.
6. Click **Close** in **Trusted Platform Module Management** on the thin client.
7. Open `gpedit.msc` using the run command menu.

8. Go to **Local Group Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require additional authentication**.
9. In the **Require additional authentication at startup** window select the **Enabled** option. The **Allow BitLocker without a compatible TPM** check box is selected by default.
10. Clear the **Allow BitLocker without a compatible TPM** check box.
11. Click **Apply** and then click **OK**.
12. Go to **Local Group Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Allow enhanced PINs for startup**.
13. In the **Allow enhanced PINs for startup** window select the **Enabled** radio button and click **Apply**.
14. Click **OK**.
15. Go to **Local Group Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Configure TPM platform validation profile for native UEFI firmware Configurations**.
16. In the **Configure TPM platform validation profile for native UEFI firmware Configurations** window select the **Enabled** radio button and click **Apply**.
17. Click **OK**.
18. Open `gpupdate /force` using the run command.
You can also restart the thin client to apply the group policies.
19. Go to **Control Panel** and click **BitLocker Drive Encryption**.
20. Click **Turn on BitLocker** in the **Operating system drive** section.
21. Select **Enter a PIN (recommended)** in the **BitLocker Drive Encryption (C:)** window.
22. Enter the **PIN (alphanumeric characters allowed)** using the keyboard and reenter **PIN** in the **BitLocker Encryption Drive (C:)** window.
23. Click **Set Pin**.
24. Select **Save to a file** in the **BitLocker Encryption Drive (C:)** window.
25. Click **Next**.
26. Select the **Encrypt entire drive (Slower but best for PCs and drives already in use)** option in the **BitLocker Encryption Drive (C:)** window.
27. Click **Next**.
28. Select the **Run BitLocker system** check box and click **Continue**.
29. Click **Restart Now** in the **BitLocker Drive Encryption** window.
30. Enter the pin set in the **BitLocker** screen to boot to the thin client.
31. Log in to the administrator account.
32. Double-click **BitLocker** icon in the system tray and check for encryption status of the **C:** drive.
33. Click **Close**.
34. Go to **This PC** and verify that the **C:** drive is successfully encrypted.

Configuring Bluetooth connections

You can use your thin client device with other Bluetooth enabled devices, if it has Bluetooth capability.

Prerequisites

 **NOTE:** To retain your settings, disable the Unified Write Filter (UWF) and configure Application Launch Manager and xData Cleanup Manager. For more information, see [Before Configuring your thin clients](#).

About this task

To configure Bluetooth connections, see *Connect a Bluetooth device* at <https://support.microsoft.com>.

Configuring wireless local area network settings

To configure the wireless local area network settings, use **Setup a new connection or network** window, if wireless support is allowed on the thin client device.

About this task

To configure the wireless local area network settings, see *Setting up a wireless network* at <https://support.microsoft.com>.

Using custom fields

To enter configuration strings for use by the Wyse Device Manager (WDM) and Wyse Management Suite (WMS), use the **Custom Fields** dialog box. The configuration strings can contain information such as location, user, administrator, and so on.

About this task

To enter the information that can be used by the WDM and Wyse Management Suite server, do the following:

Steps

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 **Custom Fields**.
4. Enter the custom field information in the custom field boxes, and click **Apply**.

The custom field information is transferred to the Windows registry which is then available to the WDM/WMS server.



CAUTION:

To permanently save the information, ensure that you disable/enable the Unified Write Filter (UWF). For more information, see [Before Configuring your thin clients](#).



NOTE:

For details about the custom field information, see the WDM and WMS documentation at www.dell.com/support.

Configuring RAM disk size

About this task

RAM disk is a volatile memory space used for temporary data storage. It can also be used for temporary storage of other data according to administrator discretion. For more information, see [Saving files and using local drives](#)

The following items are 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:

Steps

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 thin clients](#).

Enabling auto logon

Automatic logon to a user desktop is enabled by default on the thin client device. To enable or disable auto logon, and to change the default user name, password, and domain for a thin client, use the auto logon feature.

About this task

To enable/disable auto logon:

Steps

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 **Auto Logon**.
4. To start with the admin logon page, enter `Admin` in the **Default User Name** field.

NOTE: By default, the **Enable Auto Logon** check box is selected.

5. If you want to start with the **Logon** window with default administrator and user selections and other accounts, clear the **Enable Auto Logon** check box.

CAUTION: To permanently save the information, disable/enable the Unified Write Filter (UWF). For more information, see [Before Configuring your thin clients](#).

NOTE:

If auto login is enabled and you log off from your current desktop, the lock screen is displayed. Click anywhere on the lock screen to view the Logon window. Use this window to log in to your preferred administrator or user account.

System shortcuts

About this task

The **System shortcuts** page allows you to directly access some applications, directory, files, and folders without navigating through the **Start** menu or control panel.

Steps

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 **System Shortcuts**.
The following shortcuts are listed in the **System Shortcuts** area:
 - Administrative Tools
 - All Control Panel Items
 - System Directory
 - Program Files
 - Temporary Folder
 - My Documents
 - Recent Accessed Files
 - Dell Thin Client Application Folder
 - Application Data Folder

4. Click any of the shortcuts to access the respective folders/files/applications.

Viewing and configuring SCCM components

To view and configure the SCCM components that are installed on your thin client device, use the **Configuration Manager Properties** dialog box.

About this task

To open the **Configuration Manager Properties** dialog box:

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > Configuration Manager**.
The **Configuration Manager Properties** dialog box is displayed.

Next steps

For more information about how to use the **Configuration Manager Properties** dialog box, see *Managing Windows-based Dell Wyse Thin Clients using System Center Configuration Manager Administrator's Guide* at support.dell.com/manuals.

System Center Configuration Manager Client 2016 and 2019


Microsoft System Center Configuration Manager (SCCM) helps you to empower devices and applications which must be productive, while maintaining corporate compliance and control. It accomplishes the corporate compliance and control with a unified infrastructure that gives a single pane of glass to manage physical, virtual, and mobile clients.

It also provides tools and improvements that make easier for you to do the jobs. With SP1, it provides integration with **Windows Intune** to manage PCs and mobile devices, both from the cloud and on-premises, from a single administrative console. For more information, see *Managing Windows-based Dell Wyse Thin Clients using System Center Configuration Manager Administrator's Guide* at support.dell.com/manuals.

Devices and printers

To add devices and printers, use the **Devices and Printers** window.

Prerequisites

 **CAUTION:** To refrain from cleaning up your settings, disable/enable the Unified Write Filter (UWF) and configure Application Launch Manager and xData Cleanup Manager. For more information, see [Before Configuring your thin clients](#).

About this task

To add a device or a printer to the thin client, do the following:

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > Devices and Printers**.
The **Devices and Printers** window is displayed.

Adding printers

About this task

To add a printer to the thin client:

Steps

1. Click the **Devices and Printers** icon in Control Panel.
The **Devices and Printers** window is displayed.
2. To open and use the **Add a Printer** wizard, click **Add a Printer**.

The **Add a Printer** wizard session starts.

A Dell Open Print Driver is installed on the thin client along with other built-in print drivers. To print full text and graphics to a local printer, install the driver provided by the manufacturer according to the instructions.

Printing to network printers from **Citrix Receiver**, **Remote Desktop Connection** or **VMware Horizon Client** applications can be achieved through printer drivers on the servers.

Printing to a local printer from **Citrix Receiver**, **Remote Desktop Connection** or **VMware Horizon Client** application using the printer drivers of the server produces full text and graphics functionality from the printer. Install the printer driver on the server, and the text only driver on the thin client using the following procedure:

- a) Click **Add a local printer**, and click **Next**.
- b) Click **Use an existing port**, select the port from the list, and then click **Next**.
- c) Select the manufacturer and model of the printer, and click **Next**.
- d) Enter a name for the printer and click **Next**.
- e) Select **Do not share this printer** and click **Next**.
- f) Select whether to print a test page and click **Next**.
- g) Click **Finish** to complete the installation.

A test page will print after installation if this option was selected.

Adding devices

About this task

To add a device to the thin client:

Steps

1. Click the **Devices and Printers** icon in Control Panel and open the **Devices and Printers** window.
2. To open and use the **Add a Device** wizard, click **Add a Device**.
The **Add a Device** wizard session starts. You can use the wizard to add a device of your choice to the thin client.

Configuring multi-monitor display

You can use the **Screen Resolution** window to configure dual monitor settings on your dual-monitor capable thin client device.

About this task

To open the **Screen Resolution** window, do the following:

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > Display > Change Display Settings**.
The **Screen Resolution** window is displayed. For detailed instructions on how to configure the screen resolution, go to www.microsoft.com.

For information about setting up multiple monitors, see the *How to Set up Multiple Monitors in Windows 10* at support.dell.com.

Managing audio and audio devices

To manage your audio and audio devices, use the **Sound** dialog box.

About this task

To manage audio and audio devices, log in as an administrator, and open the **Sound** dialog box.

Using sound dialog box

To manage your audio devices, use the **Sound** dialog box.

About this task

To open the **Sound** dialog box:

Steps

1. Go to **Start > Control Panel > Sound**.

The **Sound** dialog box is displayed.

2. Use the following tabs, and configure the sound related settings:

- **Playback**—Select a playback device and modify the settings.
- **Recording**—Select a recording device and modify the settings.
- **Sounds**—Select an existing or modified sound theme for events in Windows or programs.
- **Communications**—Click an option to adjust the volume of different sounds when you are using your thin client to place or receive telephone calls.

3. Click **Apply**, and click **OK**.



NOTE:

- **It is recommended that you use powered speakers.**
- **You can also adjust the volume using the Volume icon in the notification area of the taskbar.**

Setting region

To select your regional formats including keyboard and the Windows display languages, use the **Region** dialog box.

About this task

To select your regional formats, do the following:

Steps

1. Log in as an administrator.

2. Go to **Start > Control Panel > Region**.

The **Region** dialog box is displayed.

3. In the **Formats** tab, select the language, date, and time.

To customize the formats, do the following:

- a) Click **Additional Settings**.

The **Customize Format** window is displayed.

- b) Customize the settings, and click **OK**.

4. Click **Apply**, and then click **OK**.

5. In the **Location** tab, select a particular location to display additional information such as news and weather.

6. In the **Administrative** tab, change the language to be displayed in programs that do not support Unicode, and copy the settings.

Managing user accounts

To manage users and groups, use the **User Accounts** window.

About this task

To open the **User Accounts** window, do the following:

Steps

1. Log in as an administrator.

2. Go to **Start > Control Panel > User Accounts**.

For more information on using the **User Accounts** window, see [Managing Users and Groups with User Accounts](#).

Using Windows Defender

To scan your computer and protect against spyware and malware, use the **Windows Defender** dialog box.

About this task

To open the **Windows Defender** window, do the following:

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > Windows Defender**.

The **Windows Defender** window is displayed. In the **Home** tab, select a scan option, and click **Scan Now**.

Example

To configure and manage your thin client device, you can use anti-malware software settings in the **Settings** tab.

Next steps

Windows Defender is anti-spyware software that is included with Windows and runs automatically when you turn on your thin client. Using anti-spyware software, helps you to protect the device against spyware and other potentially unwanted software. Spyware can be installed on your device without your knowledge any time you connect to the internet, and it can infect your computer when you install some programs using a CD, DVD, or other removable media. Spyware can also be programmed to run at unexpected times, not just when it is installed.

 **NOTE: Windows Defender updates automatically at 1:00 AM on second Sunday of every month.**

Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (ATP) is a new service that helps enterprises to detect, investigate, and respond to advanced attacks on their networks.

Windows Defender ATP works with existing Windows security technologies on endpoints, such as Windows Defender, AppLocker, and Device Guard. It also works with third-party security solutions, and anti-malware products. For more information, see the *Windows Defender Advanced Threat Protection* documentation at docs.microsoft.com

Threat Defense

Dell Data Protection | Threat Defense Agent (powered by Cylance) detects and blocks malware before it can affect your computer. Cylance uses a mathematical approach for malware identification. It uses machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes. Dell Data Protection | Threat Defense analyzes potential file executions for malware in the operating system.

Endpoint Security Suite Enterprise

The Advanced Threat Prevention element of the Dell Endpoint Security Suite Enterprise version 10.1 is supported. This feature is supported only on Wyse 5070 thin client, Wyse 5470 thin client, and Wyse 5470 All-in-One thin client.

Endpoint Security Suite Enterprise provides data security for business data, systems and reputations. The suite offers an integrated client that includes advanced threat prevention, Enterprise class encryption, all centrally-managed through a single console. You can easily enforce and prove compliance for all endpoints using the consolidated compliance reporting and flexible email notifications.

C-A-D tool

The C-A-D tool enables 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. Also, you can use Win+L and Ctrl+Alt+Delete key function in the remote session such as Remote Desktop, Citrix, and VMware sessions.

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

- Citrix—Ctrl+F1
- RDP—Ctrl+Alt+End
- VMware—Ctrl+Alt+Insert

NOTE: The C-A-D tool does not work for Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) in a Citrix session, but works only for the Citrix Virtual Apps.

The C-A-D tool is enabled by default..

Wyse Device Agent

Wyse Device Agent (WDA) is a unified agent for all thin client management solutions. Installing WDA on a thin client makes it manageable by Dell Wyse Device Manager (WDM), and Dell Wyse Management Suite (WMS). For more information, see the latest *Dell Wyse Device Agent Release Notes* at support.dell.com/manuals.

NOTE: You cannot manage Wyse 5070 thin client, Wyse 5470 thin client, and Wyse 5470 All-in-One thin client using Wyse Device Manager.

Citrix HDX RealTime Media Engine

Citrix HDX RealTime Optimization Pack for Microsoft Lync provides highly scalable solution for delivering real-time audio-video conferencing and the VoIP enterprise telephony through Microsoft Lync in the XenDesktop and XenApp environments to users on Linux, Mac, and the Windows devices. HDX RealTime Optimization Pack applies your existing Microsoft Lync infrastructure and inter operates with other Microsoft Lync endpoints running natively on devices.

For more information, see [Citrix documentation](#).

Viewing and exporting operating system image manifest files

About this task

Manifest file is an xml document which contains metadata about the operating system image. The current and the factory manifest files can be compared to find change on the thin client. The following are the two types of manifest files that are based on the source of data collection:

Table 4. Manifest files

| Manifest Source | Installed Products | QFE | Drivers |
|------------------|--------------------|-----|---------|
| Current Manifest | Yes | Yes | Yes |
| Factory Manifest | Yes | Yes | Yes |

Installed products, QFE, and driver details from current and the factory manifest files can be compared to find the change on the thin client with respect to the installed applications, QFEs, and drivers respectively.

NOTE: Installed products refer to all the installed applications on the thin client.

Viewing and exporting operating system image current manifest information

Steps

1. Log in as an administrator.

2. Go to **Start > Control Panel > Dell Wyse Software Manifest Utility**.

3. Click **Export Support Data**.

The data is exported to the default path `C:/Users/Public/Public Documents/Wyse`.

NOTE:

You can also export the data to a custom folder by selecting **Custom Path** and browsing to the required folder.

4. Click **Support Directory**.

The `DellTCASupportInfo` folder is displayed.

The support directory contains the applications, drivers, and QFE of current manifest information of the thin client.

Viewing operating system image factory manifest information

Steps

1. Log in as an administrator.

2. Go to `C:\Windows\Setup\Tools`.

The `BuildContent` folder contains the factory manifest of the thin client.

3. View the information of the operating system image manifest.

- To view the information of the installed products in the factory at the time of shipment, go to **Apps > InstalledProducts.xml file**.
- To view the information of the QFEs installed in the factory at the time of shipment, go to **Qfe > QFE.xml file**.
- To view the information of the currently installed drivers manifest information, go to **Drivers > Drivers.xml file**.

Example

NOTE:

- **The InstalledProducts, QFE, and Drivers .xml files generated through the Dell Wyse Software Manifest utility (current manifest information set) and the .xml files present in the `<drive C>\Windows\Setup\Tools\BuildContent` folder (factory manifest information set) can be compared to find the changes with respect to the installed application and QFEs.**
- **You can share the support data and the build content data with the support team during troubleshooting.**

Dell Docking Station WD19

The Dell Docking Station WD19 is a device that links all your electronic devices to your thin client using a USB Type-C cable interface. Connecting the thin client to the docking station enables you to access all peripherals (mouse, keyboard, stereo speakers, external hard drive, and large-screen displays) without having to plug each one into the computer.

The Wyse 5470 thin client supports the Dell Docking Station WD19.

For more information, see *Dell Docking Station WD19 User's Guide* and *Microsoft Windows 10 IoT Enterprise for Dell Wyse 5470 thin client Release Notes* at support.dell.com/manuals.

Additional administrator utility and settings information

This section provides additional information about utilities and settings available for administrators.

- [Automatically launched utilities](#)
- [Utilities affected by log off, restart, and shut down](#)
- [Using the Unified Write Filter](#)
- [Using Application Launch Manager](#)
- [Using xData Cleanup Manager](#)
- [Saving files and using local drives](#)
- [Mapping network drives](#)
- [Participating in domains](#)
- [Using the Net and Tracert utilities](#)
- [Managing users and groups with user accounts](#)
- [Changing the computer name of a thin client](#)

Automatically launched utilities

The following utilities start automatically after you turn on the system, or after you log in to the thin client:

- **Unified Write Filter**—After you turn on the system, the Unified Write Filter utility starts automatically. The icon in the notification area of the taskbar indicates the active or inactive status of the Unified Write Filter. For more information, see [Using the Unified Write Filter \(UWF\)](#).

NOTE: While the Dell Wyse Write Filter icons and functionality are currently supported, it is recommended that you use the UWF as described in the Microsoft documentation available at www.microsoft.com, and navigate to the Unified Write Filter documentation.

- **Application Launch Manager**— The Application Launch Manager (ALM) version 1.0 enables you to start any application based on pre-defined events such as service startup, user log off or system shutdown in session zero. The application also allows you to configure multi-level logs which is essential for easy troubleshooting.
- **xData Cleanup Manager**— xData Cleanup Manager (xDKM) version 1.0 keeps extraneous information from being stored on the local disk. xDKM can be used to automatically clean-up directories used for temporary caching of information. Clean-up is triggered on either service startup, user logoff, or system shutdown. It does the clean-up invisibly to the user and is completely configurable.
- **VNC Server**—After you log in to your thin client, the Windows VNC Server utility starts automatically. VNC allows a thin client desktop to be accessed remotely for administration and support. For more information, see [Using Tight VNC to Shadow a thin client](#).

Utilities affected by log off, restart, and shut down

The following utilities are affected by logging off, restarting, and shutting down the thin client device:

- **Unified Write Filter**—After you turn on the system, the Unified Write Filter utility starts automatically. It is recommended that you use the UWF as described in the Microsoft documentation. For more information, see www.microsoft.com, and navigate to the Unified Write Filter documentation.
- **Application Launch Manager**— The Application Launch Manager (ALM) version 1.0 enables you to start any application based on pre-defined events such as service startup, user log off or system shutdown in session zero. The application also allows you to configure multi-level logs which is essential for easy troubleshooting.
- **xData Cleanup Manager**— xData Cleanup Manager (xDKM) version 1.0 keeps extraneous information from being stored on the local disk. xDKM can be used to automatically clean-up directories used for temporary caching of information. Clean-up is triggered on either service startup, user logoff, or system shutdown. It does the clean-up invisibly to the user and is completely configurable.

- **Power Management**—A Monitor Saver turns off the video signal to the monitor, allowing the monitor to enter a power-saving mode after a designated idle time. To access the power settings, go to **Start > Control Panel > Power Options**.
- **Wake-on-LAN**—This feature discovers all thin clients connected to your LAN, and enables you to wake them by clicking a button. For example, to perform image updates and remote administration functions on devices that have been shut down or are on standby. To use this feature, the thin client power must be turned on.

Unified Write Filter

About this task

Unified Write Filter (UWF) is a sector-based write filter that protects your storage media. UWF redirects the write attempts to a virtual overlay, and intercepts the write attempts to the protected volume. This improves the stability, reliability of the device thereby reducing the wear on write media, such as solid-state drives. In UWF, overlay is a virtual storage space that saves changes made on the protected volume. If the file system attempts to modify a protected sector, UWF will copy the sector from the protected volume to the overlay, and the overlay is updated. If an application tries to read from that sector, UWF returns the data from the overlay, so that the system appears to have written to the volume, while the volume remains unchanged. For more information, see the Unified Write Filter documentation at www.microsoft.com.

 **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.**


Next steps

The following are the default file folders excluded from being filtered by UWF:

- C:\Users\Admin\AppData\LocalLow
- C:\Users\User\AppData\LocalLow
- C:\Program Files\Windows Defender
- C:\Program Files (x86)\Windows Defender
- C:\Windows\WindowsUpdate.log
- C:\Windows\Temp\MpCmdRun.log
- C:\Windows\system32\spp
- C:\ProgramData\Microsoft\Windows Defender
- C:\program files\Wyse\WDA\Config
- C:\Users\Public\Documents\Wyse
- C:\Wyse\WCM\ConfigMgmt
- C:\Wyse\WCM
- C:\Wyse\WDA

The following are the default registries excluded from being filtered by UWF:

- HKLM\SYSTEM\CurrentControlSet\Control\WNT\DWCADTool
- HKLM\Software\Wyse\ConfigMgmt
- HKLM\SOFTWARE\Microsoft\Windows Defender
- HKLM\SYSTEM\CurrentControlSet\Control\WNT\UWFSvc
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList
- HKLM\SYSTEM\WPA

 **CAUTION: Please follow proper write filter and Windows Page File usage instructions at all times. Such instructions include making sure that the write filter is enabled during regular use and is disabled only temporarily by an administrator when required for image upgrades, applying security patches, registry changes and application installation. The write filter should be re-enabled as soon as such tasks are completed. Such instructions further include never enabling the Windows Page File feature during regular use of the thin client. Any operation of a Dell Wyse Windows Embedded Thin Client with the write filter turned off during regular use and/or with the Windows Page file enabled will prematurely wear out your Flash/SSD storage, decrease performance and decrease the lifespan of the product. Dell is not responsible for, and will not, warrant, support, repair or replace any thin client device or component that fails to operate properly due to a failure to follow these instructions.**

Using Unified Write Filter

About this task

To configure thin client devices using UWF, do the following:

Steps

1. Log in as an administrator.
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 thin client device as per your requirements.
4. After you configure the thin client device, 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 thin client device are now saved, and they persist after you reboot the thin client.

Next steps

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

Running Unified Write Filter command-line options


There are several command lines you can use to control the Unified Write Filter. Command-line arguments cannot be combined.

Use the following guidelines for the command-line option for the Unified Write Filter. You can also use the commands if you open the command prompt window with elevated privilege by entering command in the **Run** box.

Table 5. Running Unified Write Filter command-line options

| Command-line options | Description |
|--|---|
| <code>uwfmgr</code> | This command-line tool configures and retrieves settings for Unified Write Filter (UWF). If there are no command-line options available, it displays the command help. |
| <code>uwfmgr filter enable</code> | This command-line enables the Unified Write Filter after the next system restart. The Unified Write Filter status icon is green when the Unified Write Filter is enabled. |
| <code>uwfmgr filter disable</code> | This command-line option disables the Unified Write Filter after the next system restart. The Unified Write Filter status icon remains red while disabled. |
| <code>uwfmgr file commit C: <file_path></code> | <p>This command-line commits changes to a specified file to overlay for a Unified Write Filter-protected volume. Administrator-level permissions are required to use this command.</p> <p>The <file> parameter must be fully qualified, including the volume and path. <code>uwfmgr.exe</code> uses the volume specified in the <file> parameter to determine which volume contains the file exclusion list for the file. There is a single space between volume name and file_path. For example, to commit a file <code>C:\Program Files\temp.txt</code> the command would be <code>uwfmgr commit C: \Program Files\temp.txt</code>.</p> |

| Command-line options | Description |
|---|---|
| <code>uwfmgr file add-exclusion C: <file_or_dir_path></code> | This command-line adds the specified file to the file exclusion list of the volume protected by Unified Write Filter. Unified Write Filter starts excluding the file from filtering after the next system restart. For example, to add a registry directory HKLM\SYSTEM\WPA, the command is <code>UWfmgr.exe registry add-exclusion HKLM\SYSTEM\WPA</code> . |
| <code>uwfmgr file remove-exclusion C: <file_or_dir_path></code> | This command-line removes the specified file from the file exclusion list of the volume protected by Unified Write Filter. Unified Write Filter stops excluding the file from filtering after the next system restart. |
| <code>uwfmgr overlay get-config</code> | This command-line displays configuration settings for the Unified Write Filter overlay. Displays information for both the current and the next session. |
| <code>uwfmgr registry /?</code> | This command-line displays configuration settings for exclusions of registry keys. |

 **NOTE:** If you open a command prompt window and enter `uwfmgr ?` or `uwfmgr help`, all available commands are displayed. For information on a command, use `uwfmgr help <command>`. For example, for information on the command, volume, enter `uwfmgr help volume`.

 **CAUTION:**

- Administrators should use file security to prevent unwanted usage of these commands.
- Do not attempt to flush the data to the disk while another flush operation is in progress.

Enabling and disabling the Write Filter using the desktop icons

The Unified Write Filter can also be enabled or disabled using the Write Filter Enable/Disable desktop icons. The icon in the notification area of the taskbar indicates the active or inactive status of the Unified Write Filter by the colors green and red respectively.

- **Dell Wyse WF Enable Icon (Green)**—Double-clicking this icon enables the Unified Write Filter. This utility is similar to running the `uwfmgr filter enable` command-line. However, double-clicking this icon immediately restarts the system and enables the Unified Write Filter. The Unified Write Filter status icon in the notification area of the taskbar is green when the Unified Write Filter is enabled.
- **Dell Wyse WF Disable Icon (Red)**—Double-clicking this icon disables the Unified Write Filter. This utility is similar to running the `uwfmgr filter disable` command-line option. However, double-clicking this icon restarts the system immediately. The Unified Write Filter status icon in the notification area of the taskbar remains red if the Unified Write Filter is disabled.

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 thin client device. To save the changes, restart the 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 thin client device. To save the changes, restart the 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 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 thin client, and the changes are not committed until an administrator restarts the thin client device manually.

Application Launch Manager

The Application Launch Manager (ALM) version 1.0 enables you to start an application that is based on predefined events such as service startup, user login/logoff, or system shutdown in system account. You can also configure multilevel logs which are essential for troubleshooting using the `DebugLog.xml` file.

You can add or remove application configuration nodes from the ALM configuration file using the command-line interface.

ALM CLI tool

You can use the ALM CLI tool to add or remove application configuration nodes from ALM configuration file `ApplicationLaunchConfig.xml`. This tool is available at the installation path of the ALM application. By default, the tool is available at `%systemdrive%\Program Files\ALM`.

Configuration of nodes using ALM

You can use the following options and parameters to configure application nodes in `ApplicationLaunchConfig.xml`:

Table 6. Options to configure nodes

| Option | Description |
|---------------------|---------------------------------------|
| Add -Application | Option to add an application node. |
| Remove -Application | Option to delete an application node. |

Table 7. Parameters to configure nodes

| Parameter | Values |
|---|---|
| Name : <name of the application> | [Application name] |
| Path : <path of the application> | [Application path] |
| Arguments : < specify the configuration information when the application is launched> | [Argument] |
| Event : <event to execute the command> | USER_LOGOFF SVC_STARTUP ON_SHUTDOWN USER_LOGIN |

Examples to configure nodes using xDCM

Table 8. Examples to configure nodes using xDCM

| Scenario | Command |
|--|--|
| Adding an application node that is used by ClientServiceEngine service to run the TestApp.exe file with an argument -t when you log off from the system. | ALM.exe -Add -Application -Name:ExampleApp - Path:C:\Windows\System32\TestApp.exe - Arguments:"-t" -Event: USER_LOGOFF |
| Deleting an application node from ExampleApp application. | ALM.exe -Remove -Application -Name: ExampleApp |

NOTE:

- You must provide unique names to add a new application entry to the ApplicationLaunchConfig.xml using ALM.exe.
- Only three execution event values USER_LOGOFF, SVC_STARTUP, and ON_SHUTDOWN, are supported in the ALM application. You can add only one of these values to each event.

xData Cleanup Manager

xData Cleanup Manager (xDCM) version 1.0 prevents extraneous information from being stored on the local disk. xDCM can be used to automatically clean up directories used to temporarily cache the information. A clean up is triggered on either service startup, user logoff, or system shutdown.

It also enables you to configure multilevel logs which are essential for troubleshooting. You can clean up files, folders, and enable or disable xDCM using Application Programming Interface (API). You can also add or remove configuration nodes from the xDCM configuration file using command-line interface.

NOTE:

- Existing NetXclean.ini configurations are ported to new xDataCleanupConfig.xml.
- Content in the xData Cleanup Manager are cleaned by default.

xDCM CLI tool

You can use the xDCM CLI tool to add or remove configuration nodes from xDCM configuration file XdataCleanupConfig.xml. This tool is available at the installation path of the xDCM application. By default, the tool is available at %systemdrive%\Program Files \xDCM.

Configuration of nodes using xDCM

You can use the following options and parameters to configure application nodes in XdataCleanupConfig.xml:

Table 9. Options to configure nodes

| Option | Description |
|--------|---|
| Add | Option to add a folder cleanup node. |
| Remove | Option to delete a folder cleanup node. |

Table 10. Parameters to configure nodes

| Parameter | Values |
|---|---|
| CleanupType: <type of the clean up node> | Folder File Registry |
| Name: <name of the clean up node> | [Folder/File/Registry name] |
| Path: <path of the clean up node> | [Folder/File/Registry path] |
| PathExclusions: <paths to be excluded from deletion (Path1,Path2)/NULL> | [Path/NULL] |
| Event: <event to execute the command> | USER_LOGOFF SVC_STARTUP ON_SHUTDOWN |
| CleanType: <type of clean up> | DIR_DELETE DIR_EMPTY |
| CleanFrom: <type of memory> | Disk Overlay |

Examples to configure nodes using xDCM

Table 11. Examples to configure nodes using xDCM

| Scenario | Command |
|--|--|
| Adding a folder cleanup node in XdataCleanupConfig.xml under DiskCleanup element. | XDCM.exe -Add -CleanupType:Folder -Name:Notepad -Path:C:\Windows\Security -PathExclusions:"C:\Windows\Security\database, C:\Windows\logs" -Event: USER_LOGOFF -CleanType:DIR_EMPTY -CleanFrom:Disk |
| Deleting a file cleanup node under OverlayCleanup element Notepad in XdataCleanupConfig.xml. | XDCM.exe -Remove -CleanupType:File -Name:Notepad -CleanFrom:Overlay |

NOTE:

- If you log off from the thin client when UWF is disabled, the folder cleanup node is used by ClientServiceEngine service to clean up the contents inside the directory C:\Windows\Security. Also, when the contents of this directory is deleted, the contents in the folders C:\Windows\Security\database and C:\Windows\logs are deleted as they are added in the excluded paths.
- You must provide unique names to add a new application entry to the XdataCleanupConfig.xml using XDCM.exe.
- When you are running the command to add an entry, the folder path is compared with the existing entries. If the path is already available, only the exclusion paths are added to the existing folder entry.

Capturing logfiles

You can configure DebugLog.xml file to collect different types of logs for an application. You can modify the log levels to obtain specific type of logs. The logs files are created at C:\Windows\Logs\

 **NOTE:** By default, no logs are created for an application.

Configuration of DebugLog XML file

You can use the Debug Configuration Editor (DCE) console application to configure the debug configuration XML file. This tool can be used to commit, exclude, or modify the debug configuration file.

To commit, exclude, or modify the debug configuration file, enter the following commands on the Debug Configuration Editor:

- To commit the file and obtain the logfiles—`DebugConfigEditor.exe -CommitLog -Path "DebugLog.xml"`. This command commits the file present in the path that is mentioned in `Debug.xml`.
- To exclude the collection of logs from a folder mentioned in the `Debug.xml`—`DebugConfigEditor.exe -ExcludeLog -Path "DebugLog.xml"`.
- To configure the `Debug.xml` file to collect different types of logs—`DebugConfigEditor.exe -UpdateConfig -Path "DebugLog.xml" -LogPath "Path of Log File" -LogFileName "Name of log File" -LogLevel "logLevel"`.


The following table describes the different LogLevel values that can be used:

Table 12. LogLevel values

| Value | Description |
|-------|--------------------------------------|
| 0 | Logs are not captured. |
| 1 | Error logs are captured. |
| 2 | Warning logs are captured. |
| 3 | Error and warning logs are captured. |
| 4 | Information logs are captured. |
| 7 | All logs are captured. |

Saving files and using local drives

Thin clients use an embedded operating system with a fixed amount of disk space. Dell recommends you to save files that you want to keep on a server rather than on a thin client.

 **CAUTION:** Be careful of application settings that write to the drive C, which resides in disk space. By default, these applications write cache files to the drive C on the local system. If you must write to a local drive, change the application settings to use the drive Z. The default configuration settings that are mentioned in [Managing Users and Groups with User Accounts](#) minimize writing to the drive C for factory-installed applications.


drive Z

Drive Z is the on-board volatile memory (Dell Wyse RAM Disk) of the thin client. It is recommended that you do not use this drive to save data that you want to retain.

For information about using the Z drive with roaming profiles, see [Participating in Domains](#).

drive C

Drive C is the on-board non-volatile flash memory. Dell recommends that you avoid writing to drive C. Writing to drive C reduces the free disk space. If the free disk space on drive C is reduced under 500 MB, the thin client becomes unstable.

 **NOTE:** Dell recommends that 500 MB of disk space is left unused. If the free disk space is reduced to 500 MB, the thin client image is irreparably damaged and it is necessary for you to contact an authorized service center to repair the thin client.

Enabling the Unified Write Filter protects the disk from damage and presents an error message if the cache is overwritten. However, if this message occurs you are unable to flush files of the Unified Write Filter cache and any thin client configuration changes still in cache is lost. Items that are written to the Unified Write Filter cache or directly to the disk if the Unified Write Filter is disabled during normal operations include:

- Favorites
- Created connections

- Delete/edit connections

Mapping network drives

About this task

Administrators can map network drives. To map the network drive and retain the mappings after the thin client device is restarted, see *Map a network drive* at <https://support.microsoft.com>.



Participating in domains

You can participate in domains by joining the thin client device to a domain or by using roaming profiles.

About this task

To join a domain, see

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > System**.
The **System** window is displayed.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.
The **System Properties** dialog box is displayed.
4. Click **Change** option to change the domain or workgroup.
 - a) Click **Domain**.
The **Computer Name/Domain Changes** dialog box is displayed.
 - b) Enter the domain of your choice.
 - c) Click **OK**.
5. To join a thin client device to a domain, click **Network ID**.
The **Join a Domain or Workgroup** wizard is displayed. On the first page of the wizard, select the option that describes your network.
 - Business Network—Click this option if your thin client is a part of business network and you use it to connect to other clients at work.
 - a. Click **Next**.
 - b. Select the option according to your company's network availability on a domain.
If you select the option **Network with a domain**, then enter the following information:
 - User name
 - Password
 - Domain nameIf you select the option **Network without a domain**, then enter **Workgroup**, and then click **Next**.
 **NOTE: You can click Next even if you do not know the workgroup name.**
 - c. To apply the changes, you must restart the computer. Click **Finish**.
 **NOTE: Before restarting your computer, save any open files and close all programs.**
- Home Network—Click this option if your thin client is a home client and it is not a part of a business network. To apply the changes, you must restart the computer. Click **Finish**.

 **CAUTION: Exercise caution when joining the thin client device to a domain as the profile downloaded at logon could overflow the cache or flash memory.**

When joining the thin client device to a domain, the Unified Write Filter should be disabled so that the domain information can be permanently stored on the thin client device. The Unified Write Filter should remain disabled through the next restart as information is written to the thin client on the restart after joining the domain. This UWF is important when joining an Active Directory domain. For details on disabling and enabling the Unified Write Filter, see [Before Configuring your Thin Client](#).

To make the domain changes permanent, complete the following:

- a) Disable the Unified Write Filter.
- b) Join the domain.
- c) Restart the thin client.
- d) Enable the Unified Write Filter.

 **NOTE:**

If you use the Write Filter Enable icon to enable the Write Filter, the thin client restarts automatically.

Next steps

Using Roaming Profiles

You can participate in domains by writing roaming profiles to the C drive. The profiles must be limited in size, and it is not retained when the thin client device is restarted. For successful downloading and proper functioning, there must be sufficient disk space available for roaming profiles. Sometimes, it may be necessary to remove software components to free space for roaming profiles.

Using the Net and Tracert utilities

Net and Tracert utilities are available for administrative use. For example, determining the route took by packets across an IP network.


For more information on these utilities, go to www.microsoft.com.

Managing Users and Groups with User Accounts

To create and manage user accounts and groups, and configure advanced user profile properties, use the **User Accounts** window. By default, a new user is only a member of the **Users** group and is not locked down. As an administrator, you can select the attributes and profile settings for users.

This section provides quick-start guidelines on:


- Creating User Accounts
- Editing User Accounts
- Configuring User Profiles

 **NOTE:** For detailed information on using the User Accounts window, click the Help icon and examples links provided throughout the wizards. For example, you can use the Windows Help and Support window to search for items such as user profiles and user groups. Obtain links to detailed steps on creating and managing these items.

Creating user accounts

Only administrators can create user accounts locally or remotely through VNC. However, due to local flash or disk space constraints, the number of additional users on the thin client device should be kept minimum.

About this task

 **CAUTION:** To permanently save the information, ensure that you disable the Unified Write Filter (UWF).

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > User Accounts**.
3. On the **User Accounts** window, click **Manage another account**.
The **Manage Accounts** window is displayed.
4. Click **Add new user** in PC settings.
The **PC settings** wizard starts. Use this wizard to create a user account.
5. After creating the standard users and administrators, these users will appear in the **Manage Accounts** window. See **Step 3**.

Editing user accounts

Prerequisites

Open the **User Accounts** window as described in [Managing User Accounts](#).

About this task

To edit the default settings of a standard user or administrator account:

Steps

1. On the **User Accounts** window, click **Manage another account**.
The **Manage Accounts** window is displayed.
2. To change as required, select **User**.
The **Change an Account** window is displayed. Now make the desired changes using the links provided.

Configuring user profiles

Prerequisites

Open the **User Accounts** window as described in [Managing User Accounts](#).

About this task

CAUTION:

- **By default, all application settings are set to cache to C drive. Dell recommends that you cache to the RAM Disk Z drive as is preset in the account profiles to avoid overflowing the Unified Write Filter cache.**
- **It is recommended that other applications available to new and existing users be configured to prevent writing to the local file system because of the limited size of the disk space. It is recommended that care be exercised when changing configuration settings of the factory-installed applications.**

To configure the default admin and user profiles stored on the thin client:

Steps

1. On the **User Accounts** window, click **Configure Advanced User Profile Properties**.
The **User Profiles** dialog box is displayed.
2. Use the command buttons such as **Change Type**, **Delete**, and **Copy to** as described in the Microsoft documentation provided throughout the wizards.

Changing the computer name of a thin client

Administrators can change the computer name of a thin client. The computer name information and the Terminal Services Client Access License (TSCAL) are preserved regardless of the Unified Write Filter state (enabled or disabled). This maintains the specific computer identity information and facilitates the image management of the thin client.

About this task

To change the computer name of a thin client device, see

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > System**.
The **System** window is displayed.
3. In the **Computer name, domain, and workgroup settings** section, click **Change Settings**.
The **System Properties** dialog box is displayed.
4. Click **Change** to rename the computer name.

5. In the **Computer Name** window, type the name for the thin client device in the **Computer name** field, and click **OK**.
6. In the Confirmation dialog box, click **OK** to restart for applying the changes.
7. Click **Close**, and then click **Restart Now** to apply the changes.

System administration

To maintain your thin client device environment, you can perform local and remote system administration tasks. The tasks include:

- [Accessing thin client BIOS settings](#)
- [Unified Extensible Firmware Interface \(UEFI\) and secure boot](#)
- [Using Wyse Management Suite](#)
- [Ports and slots](#)
- [Using Tight VNC \(Sever and Viewer\) to shadow a thin client](#)

Accessing thin client BIOS settings

About this task

To access the thin client BIOS settings, do the following:

Steps

1. During system start-up, press F2 when you see a Dell logo. The **BIOS Setup** screen is displayed.
2. Change the BIOS settings as required.
3. Save the changes and exit.

Unified Extensible Firmware Interface and secure boot

Unified Extensible Firmware Interface (UEFI) is a standard firmware interface designed to improve software interoperability and address limitations of BIOS. UEFI is designed to replace Basic Input Output System (BIOS).

Secure Boot is a feature on UEFI-based clients that help increase the security of a client by preventing unauthorized software from running on a client during the boot sequence. It checks whether each software has a valid signature, including the operating system (OS) that is loaded during booting.

The thin client device is enabled with UEFI and Secure Boot. Due to this feature, you cannot boot from USB keys if you do not enter the BIOS, disable Secure Boot, change the boot mode to Legacy, and enable the **Boot from USB** option.

Booting from DOS USB key

About this task

The following table provides guidelines to boot from a DOS USB key on the supported thin client devices:

Example

Table 13. Booting from a DOS USB key

| Thin clients | Guidelines to boot the thin client |
|--|--|
| <ul style="list-style-type: none"> • Wyse 5020 Thin Client with Win10 IoT (D90Q10) • Wyse 7020 Thin Client with Win10 IoT (Z90Q10) • Wyse 7020 Accelerated Graphics Thin Client with Win10 IoT (Z90QQ10) • Wyse 5060 Thin Client | <p>To boot the thin client from a DOS USB key, do the following:</p> <ol style="list-style-type: none"> 1. During system start up, press <code>Delete</code> when you see a Wyse logo. The BIOS Setup screen is displayed. |

| Thin clients | Guidelines to boot the thin client |
|--------------|---|
| | <ol style="list-style-type: none"> 2. Set the Secure Boot to Disabled. 3. Set the Boot Mode to Legacy. 4. Set the Boot from USB to Enabled. 5. Save the changes and exit. 6. From the pop-up menu, select your USB key, and boot as Normal. |

Creating bootable UEFI USB key

About this task

To create a bootable UEFI USB key, do the following:

Steps

1. Obtain an executable UEFI shell.
2. Save the file as `bootx64.efi` on your client.
3. Format the USB key with `FAT32`.
4. In the USB key, create the `\efi\boot` directory.
5. Copy the `bootx64.efi` file to the `\efi\boot` directory on the USB key.
The bootable UEFI USB key is created.

Using Dell Wyse Management Suite

Wyse Management Suite is the next generation management solution that lets you centrally configure, monitor, manage, and optimize your Dell Wyse thin clients. The new Suite makes it easier to deploy and manage thin clients with high functionality and performance, and ease of use. It also offers advanced feature options such as cloud versus on-premises deployment, manage-from-anywhere using a mobile application, enhanced security such as BIOS configuration and port lockdown. Other features include device discovery and registration, asset and inventory management, configuration management, operating system and applications deployment, real-time commands, monitoring, alerts, reporting, and troubleshooting of endpoints.

For more information about Dell Wyse Management Suite, go to dell.com/support/manuals.

NOTE: To register the devices that run Windows 10 IoT Enterprise operating system to Wyse Management Suite, see *Registering Windows Embedded Standard Thin Clients to Wyse Management Suite by using Wyse Device Agent* at dell.com/support/manuals.

Ports and slots

The thin client device has many ports and slots. For information on the ports and slots on the thin client device at your workplace, see the respective Quick Start Guide at dell.com/support.

To provide the services through the ports, install the appropriate drivers or software on the thin client device.

NOTE:

- You can install other services and add-ons that are available from the Dell website for free or for a licensing fee.
- You can configure the thin client device to use Bluetooth-enabled peripherals. For more information, see [Configuring Bluetooth connections](#).

TightVNC—server and viewer

To configure or reset a thin client device from a remote location, use TightVNC—server and viewer. TightVNC is primarily intended for support and troubleshooting purposes.

Install TightVNC locally on the thin client device. After installation, it allows the thin client to be shadowed, operated and monitored from a remote device.

TightVNC Server starts automatically as a service upon thin client device restart. The initialization of TightVNC Server can also be controlled by using the Services window by this procedure.

To open **TightVNC Server** window:

1. Log in as an Administrator.
2. Click **Start Menu > TightVNC > TightVNC Server**.

NOTE:

- **TightVNC Viewer is available from TightVNC website.**
- **TightVNC is included in WDM software as a component.**
- **TightVNC Viewer must be installed on a shadowing or remote machine before use.**
- **If you want to permanently save the state of the service, ensure that you flush the files of the Unified Write Filter during the current system session.**

TightVNC—Pre-requisites

Before TightVNC server installation on a remote machine, to access a thin client device you must know the following:

- IP address or valid DNS name of the thin client device to shadow, operate or monitor.
- Primary password of the thin client device to shadow, operate or monitor.

NOTE:

- **To obtain the IP address of the thin client device, move the pointer over the TightVNC icon in the taskbar,**
- **To configure TightVNC server, the default password is DELL.**

Using TightVNC to shadow a thin client

About this task

TightVNC Server starts automatically as a service upon thin client startup. The TightVNC Server service can also be stopped and started by using the Services window.

Steps

1. Log in as an administrator.
2. Go to **Start > Control Panel > Administrative Tools > Services**, and then select **TightVNC Server**.
3. You may also use the TightVNC Server features in **Start > TightVNC**.


To shadow a thin client from a remote machine:

- a) On a remote machine on which TightVNC Viewer is installed, open the **New Tight VNC Connection** dialog box.
- b) Enter the IP address or valid DNS name of the thin client that is to be shadowed or operated or monitored.
- c) Click **OK**.
The **VNC Authentication** dialog box is displayed.
- d) Enter the **Password** of the thin client that is to be shadowed; this is the Primary Password of the thin client that is to be shadowed.
- e) Click **OK**.

The thin client that is to be shadowed or operated or monitored is displayed for the administrator in a separate window on the remote machine. Use the mouse and keyboard on the remote machine to operate the thin client just as you would if you were operating it locally.

Configuring TightVNC server properties on the thin client

Steps

1. To open the **TightVNC Server Configuration (offline)** dialog box, go to **Start > TightVNC > TightVNC Server — Offline Configuration**.
The **TightVNC Server Configuration (offline)** dialog box is displayed.
 2. In the **Server** tab, set the **Primary password**. Use this password while shadowing the thin client. Default primary password is `wyse`.
 3. In the **Server** tab, select the following check boxes:
 - Accept incoming connections
 - Require VNC authentication
 - Enable file transfers
 - Hide desktop wallpaper
 - Show icon in the notification area
 - Serve Java Viewer to web clients
 - Use mirror driver if available
 - Grab transparent windows
 4. Retain the following check boxes blank:
 - Block remote input events
 - Block remote input on local activity
 - No local input during client sessions
 5. In the **Main server port** box, select or type 5900.
 6. In the **web access port** box, select or type 5800.
 7. In the **Screen polling cycle** box, select or type 1000.
 8. Click **OK**.
-  **NOTE:** For security purposes, it is recommended that the primary password be changed immediately upon receipt of the thin client and it is for administrator use only.

Network architecture and server environment

This section contains information about the network architecture and enterprise server environment needed to provide network and session services for your thin client. It includes:

- [Understanding how to configure your network services](#)
- [Using Dynamic Host Configuration Protocol \(DHCP\)](#)
- [DHCP Options](#)
- [Using Domain Name System \(DNS\)](#)
- [About Citrix Studio](#)
- [About VMware Horizon View Manager Services](#)

Understanding how to configure your network services

Network services provided to thin clients can include DHCP, FTP file services, and DNS. You can configure, design, and manage your network services depending on the availability in your environment.

You can configure your network services using:

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)

Using Dynamic Host Configuration Protocol

A thin client is initially configured to obtain its IP address and network configurations from a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server provides the IP address or DNS name of the FTP server and the FTP root-path location of software in `Microsoft.msi` form to access the IP address and network configurations through the DHCP upgrade process.

DHCP is recommended to configure and upgrade thin clients as it saves time and efforts needed to complete these processes locally on multiple thin clients. If a DHCP server is not available, fixed IP addresses can be assigned and it must be entered locally for each device.

A DHCP server can also provide the IP address of the WMS server.

DHCP options

The DHCP options listed in the following table are accepted by the thin clients.

Table 14. DHCP options

| Option | Description | Notes |
|--------|-----------------------------------|---|
| 1 | Subnet Mask | Required |
| 3 | Router | Optional but recommended. It is not required unless the thin client must interact with servers on a different subnet. |
| 6 | Domain Name Server (DNS) | Optional but recommended |
| 12 | Hostname | Optional |
| 15 | Domain Name | Optional but recommended |
| 43 | Vendor Class Specific Information | Optional |
| 50 | Requested IP | Required |

| Option | Description | Notes |
|--------|---|---------------------------------------|
| 51 | Lease Time | Required |
| 52 | Option Overload | Optional |
| 53 | DHCP Message Type | Required |
| 54 | DHCP Server IP Address | Recommended |
| 55 | Parameter Request List | Sent by thin client |
| 57 | Maximum DHCP Message Size | Optional (always sent by thin client) |
| 58 | T1 (renew) Time | Required |
| 59 | T2 (rebind) Time | Required |
| 61 | Client identifier | Always sent |
| 155 | Remote Server IP Address or name | Optional |
| 156 | Logon User Name used for a connection | Optional |
| 157 | Domain name used for a connection | Optional |
| 158 | Logon Password used for a connection | Optional |
| 159 | Command Line for a connection | Optional |
| 160 | Working Directory for a connection | Optional |
| 163 | SNMP Trap server IP Address list | Optional |
| 164 | SNMP Set Community | Optional |
| 165 | Remote Desktop Connection startup published applications | Optional |
| 168 | Name of the server of the virtual port | Optional |
| 165 | Wyse Management Suite server URL option tag | Optional |
| 166 | MQTT server URL option tag | Optional |
| 167 | Wyse Management Suite CA Validation server URL option tag | Optional |
| 199 | Wyse Management Suite Group Token server URL option tag | Optional |

 **NOTE:** For more information on configuring a DHCP server, see www.microsoft.com.

Using Domain Name System

Thin client devices accept valid Domain Name System (DNS) names registered on a DNS server available to the enterprise intranet. The thin client device sends a query to DNS server on the network to translate the name into the corresponding IP address. DNS allows hosts to be access by their registered DNS names rather than their IP address.

Every Windows DNS server in Windows Server 2000 and later includes Dynamic DNS (DDNS) and every server registers dynamically with the DNS server. For DHCP entry of DNS domain and server location information, see [Using Dynamic Host Configuration Protocol \(DHCP\)](#).

About Citrix Studio

Citrix Studio is a software program that enables you to configure and manage your personalized desktops and applications. It provides an easy end-user computing experience across all devices and networks while delivering optimal performance, better security, and improved personalization.

 **NOTE:** For more information about installing and configuring the Citrix Studio, go to [Citrix Website](#).

Citrix Studio consists of various wizards that allows you to perform the following tasks:

- Publish virtual applications
- Create groups of server or desktop operating systems
- Assign applications and desktops to users
- Grant user access to resources
- Assign and transfer permissions
- Obtain and track Citrix licenses
- Configure StoreFront

All available Virtual Desktop Applications (VDA) are listed in the Studio. From the VDA list, select the application you would like to publish. Information displayed in the Studio is received from the Broker Service in the Controller.

About VMware Horizon View Manager

VMware View is an enterprise-class virtual desktop manager that securely connects authorized users to centralized virtual desktops. It provides a complete, end-to-end solution that improves control and manageability and provides a familiar desktop experience. Client software securely connects users to centralized virtual desktops, back-end physical systems, or terminal servers.

 **NOTE:** For more information, on installing and configuring View Manager, go to [VMware Website](#).

VMware View includes the following key components:

- **View Connection Server**—A software service that acts as an intermediate for client connections by authenticating and then directing incoming remote desktop user requests to the appropriate virtual desktop, physical desktop, or terminal server.
- **View Agent**—A software service that is installed on all guest virtual machines, physical systems, or terminal servers. View Manager manages this software. The agent provides features such as the Remote Desktop Connection monitoring, virtual printing, remote USB support, and single sign-on.
- **View Client**—It is a locally installed software application that communicates with View Connection Server, to allow users to connect to their desktops using Microsoft Remote Desktop Connection.
- **View Portal**—This component is similar to View Client but provides a View user interface through a web browser. It is supported on multiple operating systems and browsers.
- **View Administrator**—This component provides the View administration through a web browser. View administrators use it to do the following:
 - Manage configuration settings.
 - Manage virtual desktops and entitlements of desktops of the Windows users and groups.

View Administrator also provides an interface to monitor log events and is installed with View Connection Server.

- **View Composer**—To allow View Manager to rapidly deploy multiple linked clone desktops from a single centralized base image, **View Composer** software service is installed on the Virtual Center server.

Installing firmware using USB Imaging Tool

Firmware installation is the process of installing the Windows 10 IoT Enterprise firmware on your thin client.

Use the Dell Wyse USB Imaging Tool version 3.2.0 to install the Windows 10 IoT Enterprise image on your thin client. For information about installation instructions, see the *Dell Wyse USB Imaging Tool version 3.2.0 User's Guide* at <https://downloads.dell.com/wyse/>.

Frequently asked questions

How to install Skype for Business

To install Skype for business on your thin clients, do the following:

1. Log in as an administrator.
2. Disable Unified Write Filter.
3. Download the Skype for Business stand-alone (64-bit) from <https://support.microsoft.com>.
4. Double-click the .exe file, and click **Run**.
5. After the installation is complete, click **Close**.
6. Launch Skype for business.
7. On the license agreement screen, click **Accept**.
8. Enable Unified Write Filter.

For more information, see *Install Skype for Business* at <https://support.office.com>.

How to set up a smart card reader

To set up a smart card reader, do the following:

1. Log in as an administrator.
2. Disable Unified Write Filter.
3. Download your preferred smart card application.
4. Extract the file to your local drive.
5. Connect the smart card reader with the smart card, and click **Setup**.
6. After the installation is complete, install the server certificate if you want to establish a connection for Citrix or VMWare setup.
7. Enable Unified Write Filter.
8. Connect to your preferred VDI session such as Citrix, VMware, or RDP.

How to use USB Redirection

USB Redirection enables you to connect an external device into a USB port on your thin client and access the device using a remote desktop or application.

You can configure USB Redirection in a Citrix Virtual Apps and Desktops (formerly Citrix XenDesktop) environment. For more information, see *Citrix Generic USB Redirection Configuration Guide* at support.citrix.com.

You can also configure options to use and manage USB devices in a View virtual desktop session. For more information, see *USB Device Redirection, Configuration, and Usage in View Virtual Desktops* at www.vmware.com

How to capture and push Windows 10 IoT Enterprise operating system image

You can capture and push Windows 10 IoT Enterprise operating system image using any of the following methods:

- Wyse Management Suite
- Microsoft System Center Configuration Manager (SCCM)
- USB Imaging Tool

For information about Wyse Management Suite and SCCM, see the respective guides at <https://support.dell.com/manuals>.

For information about USB Imaging Tool, see *Dell Wyse USB Imaging Tool User's Guide* at <https://downloads.dell.com/wyse>.

Troubleshooting

Keyboard customization issues

To customize the keyboard language that is not supported by default, do the following:

1. Go to `C:\Windows\system32\oobe`.
2. Delete the `oobe.xml` file and the related subdirectories.
3. Customize the `sysprep.xml` file manually and set the keyboard, locales, and so on, to the respective language.
4. Deploy the `.xml` file manually, or by using SCCM or Custom Sysprep.

All preferences for keyboard, locale, time zone, countries, and so on, are applied.

Resolving memory issues

To troubleshoot **Out of memory** error in Dell Wyse Windows Embedded thin clients, use one of the following tools to identify and adjust your memory requirements:

- Windows Task Manager
- Unified Write Filter
- File Explorer

 **NOTE:** The name of the error dialog box helps you to identify the source of the memory issue.

Using Windows Task Manager

1. Log in as an administrator.
2. Press `Ctrl+Alt+Delete`.
3. Click **Task Manager**.
The **Task Manager** window is displayed.
4. Click **More details**.
5. Click the **Performance** tab, and analyze your system memory resources.
6. Close the programs that are using more memory.

Using Unified Write Filter


1. Log in as an administrator.
2. Double-click the UWF icon in the system tray.
3. Configure the **Amount of RAM to be used for FBWF cache (MB)** option.

Using File Explorer

You can use File Explorer to verify the size of your Z: (RAMDisk) drive. You must refresh the application to view the updated values.

Blue screen error or BSOD issues

A blue screen error or BSOD with error code `CRITICAL_PROCESS_DIED` is observed on Wyse 5070 thin client with Apacer Solid-State Drives running Windows 10 IoT Enterprise version 10.03.06.10.18.00. To resolve this issue, you must disable the link power management mode for storage devices that are connected to the thin client using an AHCI interface.

 **NOTE:** This issue is resolved in Windows 10 IoT Enterprise image builds later than version 10.03.06.10.18.00, and hence you are not required to apply the registry entry manually.

To disable the link power management mode using a registry file, do the following:

1. Log in as an administrator.
2. Disable Unified Write Filter.

The system restarts.

3. Log in as an administrator again.
4. Open Notepad and type the following syntax:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\storahci\Parameters\Device]
"SingleIO"=hex(7):2a,00,00,00
"NoLPM"=hex(7):2a,00,00,00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-f91c70521c60\DefaultPowerSchemeValues\381b4222-f694-41f0-9685-ff5bb260df2e]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-f91c70521c60\DefaultPowerSchemeValues\8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-f91c70521c60\DefaultPowerSchemeValues\1841308-3541-4fab-bc81-f71556f20b4a]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
```

5. Save the file as a .reg file.

6. Click **Start**.

7. Type cmd in the search field.

8. Right-click **Command Prompt**.

9. Click **Run as administrator**.

The **User Account Control** window is displayed.

10. Click **Yes**.

The elevated command prompt window is displayed.

11. Run the command `reg import <file path of the registry file>`.

12. Enable Unified Write Filter.

WiFi settings configured from Wyse Management Suite are not persistent across multiple Wyse 5070 thin clients

When you configure a WiFi connection on a Wyse 5070 Thin Client, it connects to a specific wireless network (SSID) without asking for the password. When the same configuration is exported to Wyse Management Suite and deployed to other Wyse 5070 Thin Clients, the configuration is applied and you are prompted to enter a password to connect to the same wireless network. To make the WiFi settings persistent, do the following:

Steps

1. Connect the Wyse 5070 Thin Client to the wireless network.
2. Run `DWirelessProfileEditor.exe` file.
The **Wireless Profile Password Editor** window is displayed.
3. Browse to the destination path to save the profile as an xml file and click **Save**.
4. Click the **Export WiFi Profiles** button in the **Wireless Profile Password Editor** window.
5. From the **Profiles** drop-down list, select the profile to deploy the configuration.

6. Clear the **Password** field, and enter the password again.

7. Click **Change Password**.

 **NOTE: Do not click the Export WiFi Profiles button again.**

8. Close the **Wireless Profile Password Editor** window.

9. Log in to Wyse Management Suite.

10. Go to **Apps & Data > File Repository > Inventory**.

11. Click **Add File**.

12. Browse to the xml file.

13. From the **Type** drop-down list, select **Windows Wireless Profile**.

14. Enter the description.

15. Select the **Override existing file** option if you want to overwrite the present configuration.

16. Click **Upload**.

17. Go to **Groups & Configs > Edit Profiles > WES > Network**.

18. Click **Configure this item**.

19. From the **Windows Wireless Profiles** drop-down list, select the uploaded file.

20. Click **Save & Publish**.