Dell Wyse Windows 10 IoT Enterprise for Latitude 5280 Mobile Thin Client

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.

2017 - 08

Rev. A00

Contents

1

Introduction

Dell Wyse thin clients running Microsoft Windows 10 IoT Enterprise provide access to applications, files, and network resources. It is made available on machines hosting Citrix Receiver, Microsoft Remote Desktop Connection, the VMware Horizon client session and Dell Wyse vWorkspace services. 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 specialty peripherals and features for environments needing a secure Windows user interface with 64-bit Windows compatibility. Your thin client device supports Microsoft Silverlight, Microsoft Lync VDI 2013 plug-in, and Microsoft .Net Framework 4.6 or later versions. For more information, see www.microsoft.com.

Session and networks services available and accessed on enterprise networks, a direct intranet connection or from a remote location using a secure gateway from Citrix, Microsoft, VMware, or Dell Wyse vWorkspace.

Technical support

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

2

Getting started

This section describes the activities that you can perform to start using your thin client device. You can also find information related to the available desktop features. When you boot your thin client device for the first time, the user desktop is displayed by default. You can log in to the thin client device as a user or an administrator. Administrator can configure a user account to log on automatically or manually by entering the login credentials.

To get started using your thin client device, see:

- Automatic and manual Logon
- Before configuring your thin clients
- Using your desktop
- Using the Start Menu
- Using the Search Box
- Using Action Center
- Grouping applications into desktops
- Connecting to a printer or an external device
- Connecting to monitor
- Power state

Logging on

Whatever we view during the turn on or during the reboot of thin client device depends on the administrator's configuration. After creating user account, an administrator can configure a user account to log on automatically or require manual logon with user credentials.

For more information, see Managing Users and Groups with User Accounts.

NOTE:

- Be sure to disable the Unified Write Filter (UWF) before you change a password on the thin client, and then enable the UWF after your change. For more information, see Before configuring your thin clients.
- To change the password, hold CTRL+ALT+DEL key combination, and then click **Change a password**. However, this feature is not applicable for **User** accounts.

Automatic and manual login

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

IMPORTANT: The Windows icon on the taskbar is the start menu button.

To log in as a different user or administrator:

1 Click **Start Menu** > **User icon** > **Sign Out** to log out from the current desktop.

2 Click anywhere on the lock screen to view the **logon** window.

3 You can view the user accounts list on the left-lower corner of your screen. Click the preferred user account and then enter the logon credentials.

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

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

Before configuring your thin clients

Unified Write Filter Utility and NetXClean Utility are meant to protect your thin clients. These utilities prevent your thin client configurations from persisting after you log out and restart. The local settings and profile configurations you change are removed by utilities. These utilities prevent undesired flash memory writes and clean-up extraneous information from being stored on the local disk.

However, there are instances where administrators want configurations to persist even after logoff and restarting a thin client.

Before configuring your thin clients, see

- Using the Unified Write Filter (UWF).
- Understanding the NetXClean Utility.

NOTE: To configure and manage multiple thin clients, see Dell Cloud Client Computing.

Working with Unified Write Filter utility

Unified Write Filter (UWF) is a sector-based write filter that you must use to protect your storage media. UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay.

WARNING: 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.

For more information about UWF, browse **Unified Write Filter** on www.microsoft.com.
The Dell Wyse Write Filter (WF) guidelines are given below:

1 Log in as an administrator.
If automatic logon 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 will persist after a thin client device reboot.

For more information, see Using the Unified Write Filter (UWF).

Brief introduction about NetXClean utility

NetXClean is a clean-up utility that runs in the background and removes extraneous information from the RAM drive before it can be flushed to local storage. If you want to retain certain profile configurations such as printers, monitors and other peripherals, be sure to configure NetXClean in order to refrain from cleaning up explicitly declared profiles.

For more information, see Understanding the NetXClean utility.

Using your desktop

Based on admin configurations, you are able to view the thin client desktop after logging on.

The **Thin Client Admin Desktop** typically consists of the following:

- **Admin Taskbar** — It includes,
  - The Start Menu button
  - The Search box
  - Quick Launch Bar icons
  - Task View
  - Notification area in the extreme right of the taskbar

    NOTE: On the extreme right of the task bar, click the New notifications icon to open the Action Center window. For more information about the Action Center, see Using Action Center.
- **Standard Desktop Icons** — It includes
  - Citrix Receiver
  - Dell Thin Client Application
  - Ericom Connect WebConnect Client
  - Internet Explorer
  - PowerTerm Terminal Emulation
  - Remote Desktop Connection
  - VMware Horizon Client
  - vWorkspace
  - Dell Wyse WF Disable
  - Dell Wyse WF Enable

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, click **Start Menu** > **Control Panel**. For more information, see Notable features.

Using the Start Menu

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.

To open the Start Menu:

1 Log in as an Admin.

2 Click the **Start Menu** button in the lower-left corner of the screen.

NOTE: You can also open the Start menu by pressing the Windows logo key on your keyboard.

3 From the Start Menu, you can use the following options to navigate through the available applications or configure the settings:

- **Settings**—Use this option to open the **Settings** window and configure some common Windows settings. The available settings are:
  - **System** — To configure the Display, Notifications, apps and power settings.
  - **Devices** — To configure the bluetooth, printer, camera, and other peripheral settings.
  - **Network and Internet** — To configure the Wi-Fi, airplane mode, Ethernet and VPN settings.

- **Personalization** — To configure the Background, lock screen and colors settings.
- **Accounts** — To configure your account settings.
- **Time and Language** — To configure the speech, region and date settings.
- **Ease of Access** — To configure the Narrator, magnifier and high contrast settings.
- **Privacy** — To configure the location and camera settings.
- **Update and Security**— To configure the Windows update settings.

- **Power** — You can sleep, restart or turn off your thin client. For more information, see Power State.
- **List of applications** —Click the Start Menu button to view full list of your applications and programs.

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

Using the Search Box

Use the search box on the taskbar to look for applications, files or settings on your Windows.
The Search box helps you find things and information on your Windows. To use the Search box:

1 Type what you are searching for in the search box on the taskbar.
You can 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.
2 Click the result to open the application or file you searched for.

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 puts important notifications from Windows and your applications right 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 screen to the right, or by selecting the **close** button.
- **Quick Action icons**: Quick Action icons allow you to access **All Settings** and applications you are likely to use often, from Bluetooth to VPN. When you open action center you will see all your available quick actions. Select the **Expand** option to see the settings and applications such as Location, Quiet hours, Brightness, Bluetooth, VPN, Battery saver, project, and connect, which are used more often.

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 quickly configure some common 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 through a USB-to-parallel adapter interfaced printers to your thin client device using a USB port. Follow your printer's USB installation instructions before connecting to a USB port.

NOTE:

To connect to the printer, you 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, you add the device to the thin client device. For more information, see Adding devices.

Connecting to monitor

The Latitude 5280 mobile thin client can connect to external monitors using either or both of the following ports:

- HDMI port
- VGA port

For more information on configuring a dual monitor display, see Configuring dual monitor display.

Power state

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

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 orderly closing of the operating system.
- **Restart**–The thin client device is turned off and turned on instantly.

You can also use the power state options by pressing the ALT+F4 key combination, and then selecting your preferred option from the drop-down list.

NOTE: If automatic logon is enabled, the thin client will immediately log on to the default user desktop.

3

Accessible applications

When you log in to your thin client as an Administrator or a User, the Windows desktop displays certain notable extended features in the Start menu.

You can perform the following tasks:

- To browse the Internet, use Internet Explorer, see Browsing the Internet with Internet Explorer.
- View client information, see Using the Dell Thin Client Application.
- Configure Citrix Receiver session services, see Configuring Citrix Receiver Session Services.
- Configure remote desktop connections, see Configuring Remote Desktop Connection Session Services.
- Configuring the VMware Horizon Client, see Using VMware Horizon Client to connect to a Virtual Desktop.
- Use Ericom–Powerterm Terminal Emulation, see Using Ericom PowerTerm Terminal Emulation.
- Use Ericom Connect-WebConnect Client, see Using Ericom Connect-WebConnect Client.
- Configure vWorkspace connections, see Configuring a vWorkspace Connection.
- Use Microsoft Lync Vdi 2013 plug-in, see Microsoft Lync Vdi 2013 plug-in.
- Use Adobe flash player, see Adobe Flash Player.
- Use Windows media player, see Windows Media Player.

NOTE: Keyboard Caps Lock Indicator Application — Dell Keyboard driver software (KM632) is included in this release. This software provides 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. Again, if you press the Caps Lock key to disable the Caps Lock feature, the unlock symbol is displayed on the desktop.

Browsing the internet with Internet Explorer 11

To open Internet Explorer 11, do either of the following:

- From the **Start Menu**, click **Windows Accessories**, and then click **Internet Explorer**.
- Double-click the **Internet Explorer** icon on the desktop.

NOTE:

- Internet Explorer has internet option settings that are preselected at the factory to limit writing to disk. These settings prevent exhaustion of the limited amount of disk space available and you should not modify these settings.
- The protected mode status of the internet Explorer is **Off**. This is because User Access Control (UAC) is enabled by default. However, UAC notifies you before changes are made to your client, that you require administrator-level permission. The Unified Write Filter (UWF) contained in the build continues to protect your system. For more information, see Before Configuring your thin clients.
- Internet Explorer (IE) cache settings are 100 MB. Temporary internet files, cache, history locations are set to drive C instead of drive Z to support IE 11 completely.

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 Logon, System Shortcuts, and Support information.

To access the **Dell Thin Client Application** page:

On the Admin/User desktop, click **Start menu** > **Dell Thin Client Application** to open the page. 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 following thin client device information.
  - Under the **Product Info** category, the following attributes are listed:
    - Product Name
    - Product ID
    - Model Name
    - Product Version
    - Windows Embedded Version
    - Manufacturer
    - Hardware Rev
    - OS Name
    - Serial Number
    - Website
    - Localized Language
    - Product Activation Status
  - Under the **CPU** category, the following attributes are listed:
    - Name
    - Speed
    - Address Width
    - Data Width
  - Under the **Memory/Storage** category, the following attributes are listed:
    - RAM Memory
    - Flash
    - System Partition
  - Under the **BIOS** category, the following attributes are listed:
    - Version
    - Manufacturer
  - Under the **Network** category, the following attribute is listed:
    - MAC (IP Address)
  - Under the **User** category, the following attributes are listed:
    - User
    - Domain
- **QFE**— Displays the list of Microsoft QFEs (previously known as hot fixes) applied to the thin client device.
- **Installed Products** — Displays the list of applications that are installed on the thin client device.
- **WDM Packages** — Displays the list of WDM Packages that have been applied to the thin client. For more information, see WDM software for Remote Administration .
- **Copyrights/Patents** — Displays copyrights and patents information.

When logged 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 Energy Star complaint is also displayed on the Dell Thin Client Application page.

For more information about using these options, see Notable features. In the **About and Support** tab, you can view the information related to the Application Version, Support Directory, Export support data and HTML view.

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 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 allows the user to interact with the application GUI, while all of the application processes are executed on the server.

Citrix Receiver session services can be made available on the network using Windows 2008/2012 Server with Terminal Services and one of the following installed:

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

To install the software, use the instructions accompanying them. Make sessions and applications available to the thin client devices sharing the server environment.

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

To configure a Citrix Receiver session:

1. Log in as an admin.
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 and then click **Next**.
   - For secure connections, enter Fully Qualified Domain Name (FQDN).
   - For non-secure connections, enter the IP address.
4. Enter the user credentials and then click **Log on**.
   You can add an account by providing the IP address and you can view the details of the Citrix Receiver.
5. Click **Yes** and then click **Next**.
   The Virtual desktop of the Citrix Receiver is displayed.
6. In the Virtual desktop window, click **Add Apps (+)** > **All Applications**.
   You can select or clear the application check -boxes. The selected applications are displayed on the virtual desktop.
7. On the virtual desktop, click **Settings** to:

- Refresh
- Add or Delete Server account
- Log-off

Configuring the Remote Desktop Connection session services

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

To install the software, use the instructions accompanying them. Make sessions and applications available to the thin client devices sharing the server environment.

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

To configure a **Remote Desktop Connection**:

1 Log in as a user or 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.
For advanced configuration options, click **Show Options**.

a In the **General** tab, you can enter the logon 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 you find that the Unified Write Filter cache is filling up, you can disable 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.

4 Click **Connect**.

5 Enter the login credentials for connecting to the remote session 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** option in step 3 b.

Using VMware Horizon Client to connect to a virtual desktop

VMware Horizon Client is a locally installed software application that communicates between View Connection Server and thin client OS. It provides access to centrally hosted virtual desktops from your thin clients.
VMware session services can be made available on the network after you install the VMware Horizon 6. It provides virtualized or hosted desktops and applications through a single platform to end users.
To connect to a virtual desktop, use the **VMware Horizon Client** window.

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

1 Log in as a user or 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 desktop is displayed.

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

For more information, refer to VMware Horizon Client documentation on 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. We recommend that you do not change this setting unless instructed to do so by your system administrator.

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

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

Configuring a vWorkspace connection

vWorkspace is a concept in which the desktop environment of a computer is separated from the physical computer and hosted as a virtual workspace on multiple environments, such as a virtual desktop infrastructure (VDI), terminal servers, and/or blade PCs running in a data center.

Workspace virtualization helps group and deliver a list of applications or desktops together as a single complete virtual workspace. It isolates and centralizes an entire computing workspace. vWorkspace provides flexible, location and platform independent access by delivering virtual workspace from multiple virtualization platforms.

To configure a vWorkspace connection:

1 Log in as a user or administrator.
2 On the **Start Menu**, click **Dell Wyse vWorkspace**, or double-click the **vWorkspace** icon on the desktop.
The **vWorkspace** window is displayed.
3 In the **vWorkspace** window, enter the vWorkspace Server IP, or your registered email address or website address, and then press **Enter**.
4 To retrieve your connector configuration from vWorkspace server, provide the Username, Password, and Domain credentials. Select the **Save Credentials (encrypted)** check box if you want to save your login credentials.
5 Select your preferred vWorkspace Farm location from the following options:
- Inside Office
- Outside Office

6 Click **Connect**.
7 In the **Login Credentials** dialog box, enter the following credentials to connect to the vWorkspace Farm:
- Username
- Password
- Domain

The **vWorkspace Farm** screen is displayed.

For more information about managing your vWorkspace connection, go to documents.software.dell.com/vworkspace.

Configuring vWorkspace Farm

After you log in to the vWorkspace Farm by using the login credentials, the vWorkspace Farm page is displayed. Use this page to configure the vWorkspace Farm.

1 Click **vWorkspace Farm** to view the configuration options available.
If you are successfully connected to the vWorkspace Farm, then the status of the connection is displayed in green color.
2 Click the **Settings** icon to configure your vWorkspace Farm settings.
   a Select the **Automatically connect to this configuration on startup** check box to allow auto-connect to the specified configuration upon startup.
   b From the drop-down list, select your location where you want to deploy the vWorkspace Farm. The available options are:
      - Always prompt for location
      - Use Location Inside Office
      - Use Location Outside Office
   c Under the **Display settings** section, the following options can be configured.
      - From the **Screen resolution** drop-down list, select your preferred screen resolution for your vWorkspace session.
      - Select the following check boxes as per your requirements:
         - Use all my monitors for the remote session
         - Display connection bar
         - Pin connection bar
   d Under the **Device settings** section, the following options can be configured.
      - Select the following check boxes as per your requirements:
         - Play audio
         - Use USB devices
         - Use microphone
      - Click **More Devices** to select additional devices and resources on your computer that you want to use in your remote session.
3 Click **OK** to save your settings.

4 Click the **Delete** icon, if you want to delete the configured vWorkspace Farm.
5 Click the **Info** icon to view the Name, Type, and Timestamp of your vWorkspace Farm.

The applications available on your vWorkspace Farm are listed in the **My Applications** area.

Additional configuration icons are displayed in the upper pane of the vWorkspace page.

1 Click the **Log Off** icon, if you want to log out from the vWorkspace Farm.
2 Click the **+** icon to add a new vWorkspace Farm.
3 Click the **Refresh** icon to refresh the application set.
4 Click the **Change Password** icon, if you want to change the password for your vWorkspace Farm.
5 Click the **Options** icon to access the following options:
   - Search (Ctrl+F)
   - Status Bar
   - Always on top
   - Hide when minimized
   - About

Using Ericom Connect-WebConnect client

You can access the Ericom Connect-WebConnect client either as a stand-alone application or on a network.

1 Accessing Ericom Connect-WebConnect Client as a stand-alone:
   a Log in as a user or administrator.
   b From the **Start Menu**, click **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.
   c In the **Ericom AccessPad** Login window, enter your credentials, and click **Login**.
   For example: User Name: **administrator@domain.com**.
   Password: ******
   DELL – Ericom Application Zone window is displayed.

   NOTE: By default, the Ericom AccessPad login window is displayed in English (US) language. 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.

   d In the **DELL – Ericom Application Zone** window, published applications such as **Blaze demo server**, **RDP demo server**, **Ericom server** and **Paint** are displayed.
   Double-click any of these to access them.
   You can also add your own applications from the server site.
   e To create a shortcut on your desktop, click **Options** > **Create a shortcut on Desktop** in the **DELL – Ericom Application Zone** window.
   f To log out, click **File** > **Logout** in **DELL- Ericom Application Zone** window.
2 Accessing the Ericom Connect-WebConnect client through Web Browser:
   a Double-click the **Internet Explorer** icon.
   The Internet Explorer web page is displayed.
   b Enter the URL **http://serverIP/FQDNWebConnect6.0/AppPortal/Index.asp** to access the Ericom Power Term Emulation.
   The **PowerTerm WebConnect Application Portal** page is displayed.
   c In the **PowerTerm WebConnect Application Portal** page, enter the credentials and also specify the domain name, then click **Login**.
   For example: Username: **administrator**
   Password: *****

Domain Name

d After you Log in, Published Desktops and Applications such as **Blaze demo server**, **RDP demo server** and **Paint** are displayed.

Double-click any of these to access them on a new web page.

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

e Click **Logout** on the left side of **PowerTerm WebConnect Application Portal** page to end the Ericom Power Term WebConnect session.

Using Ericom PowerTerm Terminal Emulation

To manage your connections, use **PowerTerm Session Manager**.

1 To open **TELNET : PowerTerm InterConnect for thin clients** window, do either of the following:

- Double-click on **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, in the left pane under **Session Type** select **TELNET** to configure the connection of your choice.

For more information, see Ericom-PowerTerm documentation at Dell Wyse Support Site.

Microsoft Lync VDI 2013 plug-in

Microsoft Lync VDI 2013 plug-in enables you to experience audio, and video in peer-to-peer calls and conference calls, when using Microsoft Lync 2013 in a Virtual Desktop Infrastructure (VDI) environment.

For more information, see www.technet.microsoft.com/en-us/library/jj204683.aspx.

Adobe Flash Player

Adobe Flash Player is the standard for delivering high-impact, and rich web content. The designs, animation, and application user interfaces are deployed immediately across all the browsers, and platforms to ensure a rich web experience.

For more information, go to http://www.adobe.com/software/flash/about/

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, rip music from CDs, sync digital media files to a portable device, and shop for digital media content from online stores. For more information, go to support.microsoft.com/en-us/help/17615/windows-media-player-12.

4

Notable features

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

To log in as an Admin, see Automatic and manual logon. When you log in to your thin client device as an Admin, you can access certain notable extended features in the Control Panel.

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

You can perform the following functions as an Admin:

- Use the Administrative Tools. See Using the administrative tools.
- Use the BitLocker Drive Encryption. See Using TPM and BitLocker.
- Use custom fields. See Using custom fields.
- Configure the RAM disk size. See Configuring RAM disk Size.
- Enabling auto logon. See Enabling auto logon.
- Accessing system shortcuts. See Using system shortcuts.
- View and configure SCCM components. See Viewing and configuring SCCM components.
- Add devices and printers. See Adding devices and Adding printers.
- Configure dual monitor display. See Configuring dual monitor display.
- Manage audio and audio devices. See Using the sound dialog box.
- Setting region and select language preferences. See Setting region and Language preferences.
- Manage user accounts. See Managing users and groups with user accounts.
- Scan and protect your computer against spyware and malware. See Using Windows Defender.
- Use Windows Defender Advanced Threat Protection (ATP), see Windows Defender Advanced Threat Protection (ATP)
- Use CAD tool, see CAD tool.
- Configure Wyse Device Agent (WDA), see Wyse Device Agent.
- Configure Citrix HDX RealTime Media Engine, see Citrix HDX RealTime Media Engine.

Using Administrative tools

To access the Administrative Tools window, on the taskbar, click **Start Menu** > **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

To access and configure the Component Services, Event Viewer and Local Services use the **Component Services** console

1 Log in as an administrator.
2 On the **Start** menu, click **Control Panel** > **Administrative Tools**.
3 From the Administrative Tools list, select **Component Services**.
4 In the **Component Services** console, select Component Services, Event Viewer, or Local Services from the **Console Root** tree and configure.

Viewing the events

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.

Managing the services

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

1 In the **Component Services** console, click the **Services** icon from the console tree.
The list of services is displayed.
2 Right-click on any of the service of your choice. You can perform Start, Stop, Pause, Resume and Restart operations.
You can select Startup type from the drop-down list:
- Automatic (Delayed Start)
- Automatic
- Manual
- Disabled

NOTE: Make sure the Write Filter is disabled while managing the services.

Using TPM and BitLocker

A TPM is a microchip designed to provide basic security-related functions, primarily involving encryption keys. BitLocker Drive Encryption (BDE) is a full disk encryption feature which is designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm in CBC mode with a 128 bit key, combined with the Elephant diffuser for additional disk encryption-specific security not provided by AES.

Windows 10 does not support sysprep on a BitLocker encrypted device. Because of 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 related script that handles TPM. 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 located at C:\Windows\setup\tools\. This 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.

To use TPM and BitLocker, do the following:

1 Enable TPM from the BIOS menu.
2 Modify the TPM related part of the script, based on the imaging solution.
3 Uncomment the below lines and update the pin for TPM encryption in the Custom FICore imaging method in C:\Windows\Setup\CustomSysprep\Modules\Post_CustomSysprep.psm1

- #cd C:\windows\setup\Tools\TPM\
- #.\TPM_enable.ps1 -pin 1234

4 Uncomment the below lines and update the pin for TPM encryption for SCCM push in **C:\Windows\Setup\ConfigMgrSysprep \Modules\Admin_ConfigMgrSysprep.psm1**

- #cd C:\windows\setup\Tools\TPM\
- #.\TPM_enable.ps1 -pin 1234

5 Uncomment the below lines and update the pin for TPM encryption in Non-Factory environment (WDM,WSI, USB Imaging solution) in `Post_CustomSysprep.psm1`

- #cd C:\windows\setup\Tools\TPM\
- #.\TPM_enable.ps1 -pin 1234

NOTE:

If the client is encrypted previously, then do the following to clear the TPM.

1 Enter the BIOS mode.

2 In TPM configuration, set the **Change TPM Status** to **Clear**, and then apply the settings.

3 Reboot the device, and enter the BIOS mode again.

4 Set the **Change TPM Status** to **Enable and Activate**.

Configuring Bluetooth connections

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

NOTE:

To retain your settings, disable the Unified Write Filter (UWF) and configure NetXClean. For more information, see Before Configuring your thin clients.

To configure your thin client for Bluetooth Connections:

1 Log in as an Admin.

2 Click **Start Menu** > **Control Panel** > **Device Manager**.

The **Device Manager** window is displayed.

3 Expand **Bluetooth Radios** and double-click any Bluetooth icon. For example, double-click **Generic Bluetooth Radio** to manage the existing Bluetooth device. You can also update the drivers in the **Update** tab.

To add another Bluetooth-enabled device to the thin client device, use the **Add a Device** wizard.

a To open the **Devices and Printers** window, click the **Devices and Printers** icon in Control Panel.

b Click **Add a Device**.

The **Add a Device** wizard is displayed.

4 Refer to the device documentation and follow the instructions to turn on Bluetooth on the Bluetooth-enabled device. When the device is discovered by the thin client device, select the device. Click **Next** and follow the wizard.

Configuring wireless local area network settings

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

1 Log in as an Admin.

2 On the **Start** menu, click **Control Panel** > **Network and Sharing Center** > **Setup a new connection or network**. You can also select the **Open network and sharing session** on the taskbar appeared on the Thin Client Administrator Desktop.

3 In the **Setup a new connection or network** window, select Manually Connect to Wireless Network, and then click **Next**.

4 In the dialog box, enter the following:

- Network Name
- Security type
- Encryption type
- Security key: Depending on the authentication the security key is entered.

5 Select the **Start this connection automatically** check box.

6 On the taskbar, select the **Open network and sharing session** and the name of the network which you entered is displayed.

7 Select **Connect**.

8 You can also view the network available and directly connect from the **Open network and sharing session** on the task bar of the Thin Client Administrator Desktop.

Using custom fields

To enter configuration strings for use by the WDM software, use the **Custom Fields** dialog box. The configuration strings can contain information such as location, user, administrator and so on.
To enter the information for use by the WDM server:

1 Log in as an Admin.

2 On the **Start Menu**, click **Dell Thin Client Application**.
The Dell Thin Client Application window is displayed.

3 On the left navigation bar, click **Custom Fields**.

4 Type 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 server.

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

NOTE:
For details on Custom Field information, see the WDM documentation.

Configuring the RAM disk size

RAM disk is a volatile memory space used for temporary data storage. It makes up the Z drive in the **This PC** window. 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 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:

1 Log in as an Administrator.

2 On the **Start Menu**, click **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 box, 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, make sure you disable the Unified Write Filter (UWF). For more information, see Before Configuring your thin clients.

NOTE:

The default RAM size is 8 GB. The minimum size of the RAM disk is 2 MB and can be expanded to 1024 MB. The recommended size of the RAM disk is between 10 percent and 20 percent of the installed RAM.

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.
To enable/disable Auto Logon:

1 Log in as an Administrator.

2 On the **Start** menu, click **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 box. By default, the **Enable Auto Logon** check box is selected.

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

NOTE:

- To permanently save the information, be sure to disable/enable the Unified Write Filter (UWF). For more information, see Before Configuring your thin clients.
- If auto logon 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 admin or user account.

System shortcuts

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

1 Log in as an Admin.

2 On the **Start Menu**, click **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 shortcut links to access the respective folders/files/applications.

Viewing and configuring SCCM components

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

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

1 Log in as an Admin.

2 On the **Start** menu, click **Control Panel** > **Configuration Manager**.

The **Configuration Manager Properties** dialog box is displayed.

For more information on how to use the **Configuration Manager Properties** dialog box, see *Dell Wyse SCCM Administrator's Guide*.

System Center Configuration Manager (SCCM) Client LTSB 2016

Microsoft SCCM helps you to empower the use of devices and applications which needs to be productive, while maintaining corporate compliance and control. It accomplishes 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 makes 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-premise, from a single administrative console. For more information, see *Dell Wyse SCCM Administrator's Guide*.

Devices and Printers

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

CAUTION: To refrain from cleaning up your settings, disable/enable the Unified Write Filter (UWF) and configure NetXClean. For more information, see Before Configuring your thin clients.

To add a device or a printer to the thin client:

1 Log in as an Admin.

2 On the **Start** menu, click **Control Panel** > **Devices and Printers**.

The **Devices and Printers** window is displayed.

Adding printers

To add a printer to the thin client:

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 according to 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

To add a device to the thin client:

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 dual monitor display

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

1 Log in as an Admin.
2 On the **Start** menu, click **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, refer to Dell documentation.

Managing audio and audio devices

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

Using the sound dialog box

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

1 On the **Start Menu**, click **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 its settings.
- **Recording**— Select a recording device and modify its 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:

- We recommend powered speakers.
- You can also adjust the volume using the **Volume** icon in the notification area of the task bar.

Setting region

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

1 Log in as an Administrator.
2 On the **Start Menu**, click **Control Panel** > **Region**.
The **Region** dialog box is displayed.
3 In the **Formats** tab, you can format the language, date and time.
a Further to make additional formats, click **Additional Settings**.
The **Customize Format** window is displayed.
Numbers, Currency, Time and Date are formatted.
b Click **OK** after customizing.
4 In the **Location** tab, you are provided with additional content for a particular location such as news and weather.
5 In the **Administrative** tab, you can change **system locale** and **copy settings**.

Managing user accounts

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

1 Log in as an Admin.
2 On the **Start** menu, click **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.
To open the **Windows Defender** window:

1 Log in as an Admin.
2 On the **Start** menu, click **Control Panel** > **Windows Defender**.
The **Windows Defender** window is displayed. On the **Home** tab, select a scan option and click **Scan Now**. To configure and manage your thin client device, you can use antimalware software settings in the Settings tab.

Windows Defender is anti-spyware software that is included with Windows and runs automatically when you turn on. Using of antispyware 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.

CAD tool

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

The following are the mapped keys for different VDI applications supported by CAD tool:

- Citrix: `Ctrl+F1`
- Dell vWorkspace: `Ctrl+Alt+End`
- RDP: `Ctrl+Alt+End`

NOTE: The limitation of CAD tool is:

- The CAD tool does not work for Xen Desktop in a Citrix session, but works only for the Citrix Xen applications.

The CAD tool is disabled by default in this build. To enable, do the following:

1. Log in to system using Admin account.
2. Disable the Write Filter.
3. Launch command prompt in elevated mode.
4. **cd c:\windows\system32**
5. Run **DWKBFilterMon.exe** and reboot.
6. Enable the Write Filter.

Wyse Device Agent (WDA)

WDA is a unified agent for all thin client management solutions. Installing the WDA on a thin client makes it manageable by Dell Wyse Device Manager (WDM), and Dell Cloud Client Manager (CCM). For more information, refer to the latest *Dell Wyse Device Agent Release Notes*.

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 interoperates with other Microsoft Lync endpoints running natively on devices.

For more information, see Citrix documentation.

Windows Defender Advanced Threat Protection (ATP)

Windows Defender 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 work side by side with third-party security solutions and anti-malware products. For more information, see Windows Defender Advanced Threat Protection

5

Additional administrator utility and settings information

This chapter provides additional information about utilities and settings available for administrators.
It discusses:

- Automatically launched utilities
- Utilities affected by log Off, restart, and shut down
- Using Unified Write Filter
- Understanding the NetXClean utility
- 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 are automatically started upon system start or successful thin client logon:

- **Unified Write Filter:** Upon system start, the Unified Write Filter utility is automatically started. 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. See Using the Unified Write Filter (UWF).

  NOTE: While the Dell Wyse WF (Write Filter) icons and functionality are currently supported, we recommend you use the UWF as described in Microsoft documentation. see www.microsoft.com and navigate to the Unified Write Filter documentation.

- **NetXClean Utility:** Upon system start, the NetXClean utility is automatically started. NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. If you want to keep certain profile configurations such as for printers, be sure to configure NetXClean to refrain from cleaning up any number of explicitly declared profiles. See Understanding the NetXClean Utility.
- **VNC Server:** Upon successful thin client logon, the Windows VNC Server utility is automatically started. VNC allows a thin client desktop to be accessed remotely for administration and support. See Using Tight VNC (Server and Viewer) 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:** Upon system start, the Unified Write Filter utility is automatically started. We recommend you use the UWF as described in Microsoft documentation. See www.microsoft.com and navigate to the Unified Write Filter documentation.
- **NetXClean Utility:** NetXClean is a clean-up utility that keeps extraneous information from being stored on the flash memory. Clean-up is triggered automatically on restart, shut-down, or user log-off. If you want to keep certain profile configurations, for example, printers,

be sure to configure NetXClean to refrain from cleaning up any number of explicitly declared profiles. For more information about NetXClean, see Before configuring your thin clients and Understanding the NetXClean utility.

- **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. Power settings are available in **Start Menu** > **Control Panel** > **Power Options**.
- **Wake-on-LAN:** This feature discovers all thin clients in your LAN, and enables you to wake them up by clicking a button. This feature allows WDM software. 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 remain on.

Unified Write Filter (UWF)

Upon system start, the Unified Write Filter utility is automatically started.

UWF File Folder exclusions:

- 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

UWF Registry Exclusions

- 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

Unified Write Filter (UWF) details: You can use Unified Write Filter (UWF) to protect your storage media. UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. This UWF improves the reliability and stability of your device and reduces the wear on write-sensitive media, such as flash memory media like solid-state drives. In UWF, an overlay is a virtual storage space that saves changes made to the underlying protected volumes. UWF intercepts all modifications to any sector on a protected volume. A sector is the smallest unit that can be changed on a storage volume. Any time the file system attempts to modify a protected sector, UWF instead copies the sector from the protected volume to the overlay, and then modifies the overlay instead. If an application attempts to read from that sector, UWF returns the data from the overlay instead, so that the system maintains the appearance of having written to the volume, while the volume remains unchanged.

CAUTION:

- It is recommended that Write Filter is enabled during normal use of thin clients. It disables only by administrator while making necessary changes. Extended use with write filters disabled can reduce the life of your flash drive. It is a good practice to enable write filter to ensure device security.

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 Command Prompt window with elevated privilege by entering command in the **Run** box:

- **uwfmgr**

  With no command-line options— Displays the command help.
- **uwfmgr filter enable**

  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.
- **uwfmgr filter disable**

  Disables the Unified Write Filter after the next system restart. The Unified Write Filter status icon remains red while disabled.
- **uwfmgr file commit C: <file_path>**

  Commits changes to a specified file to overlay for a Unified Write Filter-protected volume. Administrator-level permissions are required to use this command.

  The <file> parameter must be fully qualified, including the volume and path. UWFMGR.EXE 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 C:\Program Files\temp.txt the command would be `uwfmgr commit C: \Program Files\temp.txt`.
- **uwfmgr file add-exclusion C: <file_or_dir_path>**

  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 dir `HKLM\SYSTEM\WPA`, the command is `UWFmgr.exe registry add-exclusion HKLM \SYSTEM\WPA`.
- **uwfmgr file remove-exclusion C: <file_or_dir_path>**

  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.
- **uwfmgr overlay get-config**

  Displays configuration settings for the Unified Write Filter overlay. Displays information for both the current and the next session.
- **uwfmgr registry /?**

  Displays configuration settings for exclusions of registry keys.

TIP: 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 the following: `uwfmgr help volume`.

CAUTION:

- Administrators should use file security to prevent undesired usage of these commands.
- Do not attempt to flush 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 through 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 allows you to disable the Unified Write Filter. This utility is similar to running the uwfmgr filter disable command-line option. However, double-clicking this icon immediately restarts the system. The Unified Write Filter status icon in the notification area of the taskbar remains red while the Unified Write Filter is disabled.

Setting the 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.

To configure the UWF control settings, use the following guidelines:

- UWF Status area includes:
  - **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 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 area includes:
  - **Amount of RAM to be used for UWF Cache** — Shows the amount of RAM that is to be used as 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 area includes:
  - **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. Restart the thin client device, to save the changes. 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 prompt you to restart the thin client device. Restart the thin client device, to save the changes. 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 includes:
  - **File Path** — Allows you to add, remove and commit files to the underlying media. The system will not restart the thin client device. The changes are committed immediately.

    TIP: Delete a file path from the list, if the file is not committed.
- Current Session Exclusion List area includes:
  - **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.

Understanding the NetXClean utility

NetXClean keeps extraneous information from being stored in disk. NetXClean clean-up is triggered by either a service startup or a user log off. It runs in the background and performs the clean-up invisibly and no user input is necessary.

NetXClean prevents unwanted or trash files from building up and filling the free space in the disk. The NetXClean utility is particularly important when multiple users have log-on rights to an thin client, as disk space can be quickly used by locally stored profiles and temporary caching of information.

NetXClean Tweak UI functions includes clearing:

- Run history at log-on
- Document history at log-on
- Find Files history at log-on
- Find Computer history at log-on
- Internet Explorer history at log-on
- Selected Items Now
- Last User at log-on

NetXClean purges selected directories, files, and profiles. It uses a configuration file to determine which directories and files to purge and what not to purge. To select different directories and files to purge, you must select them in the configuration file.

NOTE: NetXClean purge selections are made by the manufacturer and should not be changed without manufacturer supervision.

Regardless of the configuration file selections, NetXClean does not clean any of the following directories or their parent directories:

- Windows directory
- Windows System subdirectory
- Current directory in which the service is installed

NetXClean does not delete the following profiles:

- Administrator
- All Users
- Default User
- The profile of the last user who logged on

NOTE: NetXClean Utility does not have any dependency on Unified Write Filter (UWF).

NetXClean Utility work flow across multiple User Profiles

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

1 Log in as an Admin.

2 In `netxclean.ini`, specify the profile specific values which you want the NetXClean Utility to perform.

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

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

Saving files and using local drives

Administrators need to know the following information about local drives and saving files.

Saving Files

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

CAUTION: Be careful of application settings that write to the C drive, which resides in disk space in particular, those applications which by default write cache files to the C drive on the local system. If you must write to a local drive, change the application settings to use the Z drive. The default configuration settings mentioned in Managing Users and Groups with User Accounts minimize writing to the C drive 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. We recommend that you avoid writing to drive C. Writing to drive C reduces the free disk space. If the free disk space on C drive is reduced under 3 MB, the thin client will become unstable.

NOTE: We highly recommend that 3 MB of disk space is left unused. If the free disk space is reduced to 2 MB, the thin client image will be irreparably damaged and it will be 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 will be unable to flush files of the Unified Write Filter cache and any thin client configuration changes still in cache will be 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

For information on the role of NetXClean in keeping the disk space clean, see Understanding the NetXClean Utility.

Mapping network drives

Administrators can map network drives. However, to retain the mappings after the thin client device is restarted, complete the following:

1 Log in as an administrator.

2 On the task bar, click the search icon and then enter `This PC`.

This PC desktop application is displayed in **Best Match** area on the result page.

3 Right-click **This PC**, and then click **Map network drive**.

The Map Network Drive dialog box is displayed.

4 Select the drive letter from the Drive drop-down list, and type or browse for the folder you want to connect to.

5 Select the **Reconnect at logon** check box.

6 Empty the files of the Unified Write Filter cache during the current system session.

Since a User logon account cannot flush the files of the Unified Write Filter cache, the mappings can be retained by logging off from the user account. The system must not shut down or restart, logging back on using an administrator account, and then removing the files of the cache.

TIP: A remote home directory can also be assigned by using a user manager utility or by other means known to an administrator.

7 Click **Finish** to complete the network drive mapping.

Participating in domains

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

Joining a Domain

1 Log in as an administrator.

2 On the **Start** menu, click **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** option.

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.

  1 Click **Next**.

  2 Select the option according to your company's network availability on a domain.

  If you select the option — Network with a domain, then you must enter the following information:

  - User name
  - Password
  - Domain name

  If you select the option — Network without a domain, then you may enter the **Workgroup**, and then click **Next**.

  NOTE: You can click Next even if you do not know the workgroup name.

3 To apply the changes, you must restart the computer. Click **Finish**.

IMPORTANT: 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 especially 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 restart happens automatically. By default, the NetXClean utility purges all but selected profiles on the system when the thin client device starts up or when the user logs off. For information on NetXClean utility, see Understanding the NetXClean Utility.

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. In some cases, 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

TIP: 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 new 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.

CAUTION: To permanently save the information, be sure to disable the Unified Write Filter (UWF).

1 Log in as an administrator.

2 On the **Start** menu, click **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

Open the **User Accounts** window as described in Managing User Accounts.
To edit the default settings of a standard user or administrator account:

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

Open the **User Accounts** window as described in Managing User Accounts.

CAUTION:

- By default, all application settings are set to cache to C drive. It is highly recommended 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:

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.
To change the computer name of a thin client device:

1 Log in as an admin.
2 On the **Start** menu, click **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** tab to rename the computer name.
5 In the Computer Name window, type the name for the thin client device in the Computer name box and Click **OK**.
6 In the Confirmation dialog box, click **OK** to restart for applying the changes.
7 Click **Close**, and then **Restart Now** to apply the changes.

6

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 (UFEI) and Secure Boot
- Using Dell Wyse Management Suite
- WDM software for remote administration
- Ports and slots
- Using Tight VNC (Sever and Viewer) to shadow a thin client

Accessing thin client BIOS settings

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

1 During the start-up, press the `F2` key.
The **BIOS Setup** screen is displayed.
2 Change the BIOS settings as required.

NOTE: To access boot menu, press the `F12` key.

Unified Extensible Firmware Interface (UEFI) 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 helps 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 being loaded during booting.

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

Booting from a DOS USB key

To boot from a DOS USB Key:

1 Press the `F2` key to enter the BIOS setup.
2 Set the **Secure Boot** to **Disabled**.
3 Click **Advanced Boot Options** and select the **Enable Legacy Option ROMs** check box.
4 Click **Boot Sequence** and set the Boot List option to **Legacy**.
5 Click **System Configuration** > **USB Configuration**, and select the **Enable USB Boot Support** check box.
6 Save the changes and exit.

7 During start up, press the F12 key and then select USB stick in boot menu.

Booting from a UEFI USB key

To boot from a UEFI USB key:

1 Press the F2 key to enter the BIOS setup.
2 Set the **Secure Boot** to **Disabled**.
3 Click **System Configuration** > **USB Configuration**, and select the **Enable USB Boot Support** check box.
4 Save the changes and Exit.
5 During start up, press the F12 key and then select USB stick in boot menu.

NOTE: Windows 10 IoT Enterprise (WIE10) x64 boots, if secure boot is set to Disabled. However for security purposes, this is not recommended.

Creating a Boot disk UEFI USB key

1 Obtain a UEFI shell executable. You can download the unsigned reference shell from: Sourceforge Download Center.
2 Save the file as: **bootx64.efi**
3 Format the USB Stick with **FAT 32**
4 In the USB Key, create the directory: **\efi\boot**
5 Copy the file **bootx64.efi** to the directory **\efi\boot** on the USB Key.

Using Dell Wyse Management Suite

Dell Wyse Management Suite is the next generation management solution for Dell Wyse thin clients that offers advanced feature options, such as Cloud versus On-premises deployment, manage-from-anywhere using Mobile Application. Enhanced security features, such as BIOS configuration and port lockdown are part of Wyse Management Suite. Additional features include Device Discovery and Registration, Asset and Inventory management, Configuration management, Operating systems and Applications deployment, Real-time commands, Monitoring, Alerts, Reporting, and Troubleshooting.

For more information about Wyse Management Suite, refer to Dell Wyse Management Suite Version 1.0 Administrator's Guide.

NOTE: Dell Cloud Client Manager (CCM) has been rebranded as Wyse Management Suite. Wyse Management Suite includes several major enhancements to CCM R14. For more information, see Dell Wyse Management Suite Release Notes. Existing customers can continue to manage their thin clients as before, and take advantage of the new features introduced in the Wyse Managment Suite release.

WDM software for remote administration

WDM software enables you to configure, monitor and manage Dell Wyse endpoint devices.

WDM provides the following important features:

- Remote shadow
- Reboot
- Shutdown
- Boot
- Automatic device check-in support
- Wake-On-LAN
- Change device properties

From a single console, you can easily issue software images, patches, updates and add-ons and manage all aspects of remote cloud clients to ensure peak user productivity.

Ports and Slots

The thin client device has many ports and slots available on it such as:

- VGA port
- Security lock
- AC power
- RJ45 port
- HDMI port
- DisplayPort or USB 3.0 over Type-C port
- USB 3.0 port
- Headphone jack
- uSIM card slot (optional)
- uSD card reader

To provide the services through the ports, install the appropriate software for the thin client device.

NOTE:

- You can install other services and add-ins that are available from the Dell website for free or for a licensing fee.

  For more information, see Dell support site.
- 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, be sure to flush the files of the Unified Write Filter during the current system session.

TightVNC (server and viewer) — 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 be shadow, operate or monitor. For more information, see Using the Dell Thin Client Application
- Primary password of the thin client device to shadow, operate or monitor. For more information, see Configuring TightVNC Server Properties on the Thin Client.

NOTE:

- To obtain the IP address of the administrator's thin client device, move the pointer over the TightVNC icon in the taskbar,
- To configure TightVNC Server, the default primary password is DELL.

Using TightVNC to shadow a thin client

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.

1 Log in as an administrator.
2 Click **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 will be 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

1 To open the **TightVNC Server Configuration (offline)** dialog box, click **Start Menu** > **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 poling cycle** box, select or type 1000.

8 Click **OK**.

NOTE: For security purposes, we recommend that the Primary password to be changed immediately upon receipt of the thin client and it is for administrator use only.

7

Establishing a server environment

This section contains information on 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. Configuring your network services depends on the availability in your environment, designing and managing it.

You can configure your network services using:

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

Using Dynamic Host Configuration Protocol (DHCP)

A thin client is initially configured to obtain its IP address and network configurations from a 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 for access 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 must be entered locally for each device.

A DHCP server can also provide the IP address of the WDM server. For more information, WDM software for Remote Administration.

DHCP options

The DHCP options listed in Table 1 are accepted by the thin clients.

Table 1. 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
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
186	WDM sever IP	IP addresses of WDM Server. If tag 194 is specified, then defining this tag is not necessary.
190	WDM secure port	Optional number, word, or two-bytes array. Specifies to use HTTPS to communicate with WDM instead of HTTP
192	WDM server port	Specifies HTTP (non-secure) communication with WDM.
194	WDM server FQDN	Optional. If this tag is specified, then defining tag 186 is not mandatory.

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

Using Domain Name System (DNS)

Thin client devices accept valid 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 for name to IP resolution. DNS allows hosts to be access by their registered DNS names rather than their IP address.

Every Windows DNS server in Windows 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 Remote Desktop Connection monitoring, virtual printing, remote USB support and single sign-on.
- **View Client**: It is 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**: A 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**: A component provides View administration through a web browser. View administrators use it to do the following:

- Make configuration settings.
- Manage virtual desktops and entitlements of desktops of 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.