Dell Wyse Enhanced Windows Embedded Standard 7P for Wyse 5060 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 - 01

Rev. A01

Contents

1

Introduction

Supported clients running Dell Wyse Enhanced Windows Embedded Standard 7P provide access to applications, files, and network resources within Citrix, Microsoft, VMware and Dell vWorkspace environments, and other leading infrastructures. The thin clientOptiplex client contains a full featured Internet Explorer browser and thin clientOptiplex client emulation software called Ericom — PowerTerm Session Manager.

Other locally installed software permits remote administration of the thin clientsOptiplex clients and provides local maintenance functions. Additional add-ons are available that support a wide range of specialty peripherals and features for environments that needs a secure Windows user interface with 32–bit and 64–bit Windows compatibility.

Your thin clientOptiplex client supports Microsoft Silverlight, Microsoft Message Queuing (MSMQ), Microsoft Lync VDI 2013 plug-in and Microsoft .Net Framework 3.5 or later versions. For more information about Microsoft software components, go to www.microsoft.com.

About this Guide

This guide is intended for administrators using Wyse 5060 thin clients that has Dell Wyse Enhanced Windows Embedded Standard 7P as the operating system. It provides information and detailed system configurations to help you design and manage a WES7P client environment.

Supported Platforms

This guide is intended for Wyse 5060 thin client running WES7P (64–bit).

Finding the Information You Need in this Guide

You can use either the Search window or Find toolbar to locate a word, series of words, or partial word in an active PDF document. For detailed information on using these features, refer to the Help in your PDF reader.

Technical support

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

2

Getting Started

This section describes the activities that you must perform to start using your thin clientOptiplex client:

To get started using your thin clientOptiplex client, see:

- Logging On.
- Using your Desktop.
- Before Configuring Your Thin Client.
- Connecting to a Printer.
- Connecting to a Monitor.
- Power State.

NOTE: While it can be used in environments without central configuration for basic connectivity needs, supported clients are designed to be centrally managed and configured using network and session services.

In general, we recommend you use central configuration to automatically push updates and enable any desired default configuration to all thin clientOptiplex client in your environment, see Using Dynamic Host Configuration (DHCP).

IMPORTANT:

To save any configurations you make on a thin clientOptiplex client to persist after a thin clientOptiplex client reboot, be sure to disable the File Based Write Filter before your configurations to the thin clientOptiplex client, and then enable the File Based Write Filter after your configurations. For more information, see Before Configuring Your Thin Client.

Logging On

The initial display that you see when you turn on your thin clientOptiplex client or during the reboot of your thin clientOptiplex client depends on the administrator configurations. After creating user account, an administrator can configure that particular user account to log in automatically or require manual login with user credentials. For more information, see Enabling Auto Logon.

For information about creating and managing user accounts, see Managing Users and Groups with User Accounts.

Automatic and Manual logon

For security reasons, automatic logon to a User desktop is enabled on the thin client by default.

To log in as a different user or administrator:

1 Click **Start Menu** > **Log off**, to log off the current desktop and hold the **Shift** key until the logon window is displayed.

2 Log in using one of the following options:

- **Administrators** — The default name is **Administrator** which is displayed automatically and default password is **DellCCCvdi**.
- **Users** — The default name is **User** which is displayed automatically and default password is **DellCCCvdi**.

IMPORTANT: Passwords are case-sensitive.

NOTE: As an administrator, you can use Auto Logon to configure your thin client to start with the Logon window so that you can simply log in as an administrator. For more information, see Enabling Auto Logon.

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

We recommend you change the default passwords of your thin client. To change a password:

1 Disable the File Based Write Filter before you change a password, and then enable it after your change. For more information, see Working with the File Based Write Filter Utility.

2 Log in as an Administrator, and then open **Windows Security** window by holding CTRL+ALT+DEL key combination.

3 Click **Change a Password**, and then use the **Change a Password** dialog box to specify your old password and new password.

Using Your Desktop

What you see after logging in to the thin clientOptiplex client depends on the configurations set by the Administrator.

For viewing your desktop, you must log in to your thin clientOptiplex client as Administrator or User.

If you log in as Administrator, the **Administrator Desktop** is displayed. You can find the following applications or elements on your desktop:

- **Taskbar** — Administrator taskbar.
- **Connection Icons**— Connection icons such as VMware Horizon Client, Citrix Receiver, Remote Desktop Connection, Ptstart, and vWorkspace.
- **File Based Write Filter icons** — FBWF Disable and FBWF Enable icons.
- **Right-Click Desktop menu** — Right-click on the desktop to view the desktop menu.
- **Start Menu** — Click the **Start** button to open the **start** menu for administrator.
- **Administrator system tray icons**.

  For more options. see Accessible Applications, and Notable Administrator Features.

In addition to the Standard Control Panel icons, an extended set of resources for configuring user preference settings and system administration are included in the Control Panel. To open the control panel, click the **Start** button, and then click **Control Panel**.

If you log in as User, the **User Desktop** is displayed. You can find the following applications or elements on your desktop:

- **Taskbar**— User taskbar.
- **Connection Icons**— Connection icons such as VMware Horizon Client, Citrix Receiver, Remote Desktop Connection, Ptstart, and vWorkspace.
- **Start Menu** — Click the **Start** button to open the **start** menu for user.
- **User System Tray**.

Before Configuring Your Thin ClientsOptiplex Client

File Based Write Filter Utility and NetXClean Utility are meant to protect your thin clientsOptiplex client. These utilities prevent your thin clientOptiplex client configurations from persisting after log off and restart. The local settings and profile configurations you set 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 clientOptiplex client.

IMPORTANT:
To help you to easily configure and manage multiple thin clients, use the Dell Wyse Device Manager (WDM) software.

Working with the File Based Write Filter Utility

The File Based Write Filter provides a secure environment for thin client Optiplex client computing by protecting the thin client Optiplex client from undesired flash memory writes. Changes made to the thin client Optiplex client configurations are lost when the thin client Optiplex client is restarted unless the files of the File Based Write Filter cache are cleared during the current system session.

Use the following guidelines to configure the File Based Write Filter Utility:

1 Log in as Administrator.

If automatic logon to a user desktop is enabled, you must log off the user desktop and log in as an administrator. For more information, see Logging On.

2 To disable the File Based Write Filter, double-click the **FBWF Disable** icon in red color on your desktop.

This disables the File Based Write Filter and reboots your Optiplex client thin client.

3 Configure the thin client Optiplex client as per your requirements.

4 After you configure the Optiplex client thin client, to enable the FBWF, double-click the **FBWF Enable** icon in green color on your desktop.

This enables the File Based Write Filter and reboots your Optiplex client thin client.

Your configurations on the thin client Optiplex client are saved and they will persist after a thin client device reboot.

For more information about the File Based Write Filter, see Using the File Based Write Filter.

Brief Introduction about NetXClean Utility

NetXClean is a clean-up that keeps extraneous information from being stored on the local disk. 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.

Connecting to a Printer

To connect a local printer to your thin clientOptiplex client, be sure you obtain and use the correct adapter cables. You also need to install the driver for the printer by following the printer driver installation instructions. For information on connecting to printers, see Connecting to a Printer or an External Device.

Connecting to a Monitor

Depending on your thin clientOptiplex client model, with proper monitor cables, splitters or adapters you can connect to a monitor using a **Display(digital) port**.

For more information on configuring dual display settings, see 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** button.

2 From the **Start** menu, point to the arrow next to the **log off** button, and then click any one of the following:

- **Restart**— To restart your thin clientOptiplex client.

- **Sleep**— This mode enables the power-saving state and allows the thin clientOptiplex client to quickly resume full power operations when you want to start working again.
- **Shut down**– Preferred for orderly closing of the operating system.

3 You can also log off the thin clientOptiplex client by any of the following ways:

- From the **Start** menu, click **log off** if you want to log off your thin clientOptiplex client.
- Press CTRL+ALT+DEL and then click **log off**.
- Press ALT+F4 to log off from the session.

NOTE: If automatic logon is enabled, the thin clientOptiplex client will immediately logs on to the default user desktop. We recommend you use Shut down button to turn off your thin clientOptiplex client.

3

Accessible Applications

When you log in to your thin clientOptiplex client, the Windows desktop displays certain notable features.

You can perform the following activities:

- Browse the internet using Internet Explorer, see Using the Internet Explorer.
- View Dell Thin Client Application, see Using the Dell Thin Client Application.
- Configure Citrix Receiver session services, see Using the Citrix Receiver.
- Use Ericom PowerTerm, see Using Ericom Power Term WebConnect.
- Use Ericom — PowerTerm Session Manager, see Using the Ericom PowerTerm Terminal Emulation.
- Configure Remote Desktop Connections, see Configuring a Remote Desktop Connection Session Services .
- Connect to a virtual desktop using VMware Horizon View Client, see Using the VMware Horizon Client.
- Configure vWorkspace connections, see Configuring a vWorkspace connection.

NOTE: Keyboard Caps Lock Indicator Application — Dell Keyboard driver software is included in the build. 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.

Using the Internet Explorer

Use **Microsoft Internet Explorer (64-bit)** for your browser needs. To open the Internet Explorer, perform either of the ways mentioned here:

- Click the Internet Explorer Quick Launch icon on the taskbar on the Thin ClientOptiplex client Administrator desktop.
- Click the **Start** button on the taskbar, click **All Programs**, and then from the Programs Menu, click **Internet Explorer**.

NOTE: The Internet Explorer has internet option settings that are preselected at the factory to limit writing to flash memory. These settings prevent exhaustion of the limited amount of flash memory available and you should not modify the settings. If you require more browser resources, you can access another browser through an ICA, RDP, VMware, or Dell vWorkspace session.

Using the Dell Thin Client Application

Use the Dell Thin Client Application to view the general information about the thin client device, System Shortcuts, Custom fields, RAM Disk, Auto Logon, CAD Map and Support information.

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

- **Administrator**— On the Administrator desktop, click **Start** > **All Programs** > **Dell Thin Client Application** to open the page.
- **User**— On the User desktop, click **Start** > **All Programs** > **Dell Thin Client Application** to open the page.

On the left pane of the **Dell Thin Client Application** page, 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.
- **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. For more information about using these options, see Notable Administrator 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.

Using the Citrix Receiver

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 either 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

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 access the Citrix Receiver session:

- On the Thin ClientOptiplex Client Administrator desktop, double-click the **Citrix Receiver** icon.
- Click the **Start** button on the taskbar, click **All Programs**, and then click **Citrix Receiver** on the Programs Menu.

For information about configuring the Citrix receiver, go to www.citrix.com, and then refer to *Citrix Documentation*.

Using Ericom PowerTerm WebConnect

Ericom PowerTerm WebConnect maximizes the value of Terminal Servers (RDS), Virtual desktops (VDI), Web applications, cloud services, and legacy host systems. For IT departments of all sizes, PowerTerm WebConnect streamlines the management and utilization of IT resources, while protecting past IT investments and significantly improving the end user-experience.
You can access the Ericom Power Term WebConnect either as a stand-alone application or on a network.

1 Accessing Ericom Power Term WebConnect as a stand-alone:
   a Log in as a user or administrator.
   b Double-click **PtStart** icon on the desktop.
   The **Ericom PowerTerm WebConnect** window is displayed.
   c Enter IP Address in the **Server Address** field, and click **OK**.
   When you start accessing it for the first time PtStart.exe file is generated and then Power Term WebConnect Login window is displayed. Else, Power Term WebConnect Login window is displayed.
   PtStart.exe file provides the details regarding the server IP address, the folder in which it is installed and the path to reach the folder.
   d In the Power Term WebConnect Login window, enter your credentials, and click **Login**.
   For example: User Name : **administrator@domain.com**.
   Password: ******
   DELL – Ericom Application Zone window is displayed.
   e 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.
   f To create a shortcut on your desktop, click **Options** > **Create a shortcut on Desktop** in the **DELL – Ericom Application Zone** window.

g To log out, click **File** > **Logout** in **DELL- Ericom Application Zone** window.

2 Accessing Ericom Power Term WebConnect through Web Browser :

a Click **Internet Explorer** icon in the taskbar on Thin Client Administrator desktop.

Internet Explorer web page is displayed.

b Enter the URL **http://serverIP/FQDNWebConnect6.0/AppPortal/Index.asp** to access the Ericom Power Term Emulation.

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.

For more information about Ericom Power Term WebConnect, see www.ericom.com/ericom-connect/enterprise/ and www.ericom.com/DOC/TECHNICALREFERENCES/PTWC_MANUAL.PDF.

Using the Ericom-PowerTerm Terminal Emulation

The following two options are available under the Ericom-PowerTerm Terminal Emulation to configure and manage your connections.

The PowerTerm InterConnect comprises of several robust terminal emulation applications supporting the host access, that needs large and small organizations. The PowerTerm InterConnect products provides fast and reliable access to data residing on the broadcast range of hosts, such as IBM Mainframe zSeries, IBM AS/400 iSeries, UNIX, OpenVMS, Tandem, and HP. It allows enterprises to standardize on a single host access solution.

- **PowerTerm Session Manager**
- **PowerTerm Terminal Emulation**

Use the **PowerTerm Session Manager** to manage your connections:

1 On the taskbar, click the **Start** button, and then click **All Programs**.

2 Click **Ericom-PowerTerm Terminal Emulation** on the Programs menu, and then click **PowerTerm Session Manager**.

Use the **PowerTerm Terminal Emulation** to configure your connection information.

1 On the taskbar, click the **Start** button, and then click **All Programs**.

2 Click **Ericom-PowerTerm Terminal Emulation** on the Programs menu, and then click **PowerTerm Terminal Emulation**.

The **TELNET : PowerTerm InterConnect for Thin ClientsOptiplex Clients** window is displayed.

3 Use the **Connect** dialog box to configure your connection information such as Session Type, Host Name, Terminal Name, Port number, Terminal Type, Terminal ID, Security type, Upon Connection Run settings, and Sessions List.

For more information about the Ericom — PowerTerm Terminal Emulation, go to www.dell.com/wyse/knowledgebase and then search for **Ericom PowerTerm**.

Configuring a 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.

Use the **Remote Desktop Connection** dialog box to establish and manage connections to remote applications.

To configure a Remote Desktop Connection:

1 Log in as user or administrator.
2 On the taskbar, click the **start** button, and then click **All Programs**.
3 Click **Remote Desktop Connection** on the Programs menu, and then click **Remote Desktop Connection**.

The **Remote Desktop Connection** dialog box is displayed.

You can also double-click the **Remote Desktop Connection** icon on the desktop to open the **Remote Desktop Connection** dialog box.

4 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, 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, from the drop-down list select the desired environment you want to apply the 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 **Programs** tab, to start a default program with the remote session, select the **Start the following program on connection** check box and specify the details.
   e In the **Experience** tab optimize the performance of your remote session based on the connection quality.

      NOTE: If you find that the File Based Write Filter cache is filling up, you can disable Bitmap caching in the Experience tab after clicking Show Options in the window.

   f In the **Advanced** tab, in the **Server Authentication** section, from the drop-down list, select the action you want the thin clientOptiplex client to perform when the server authentication fails.

      In the **Connect from anywhere** section, click **Settings** to configure the connection settings such as Remote Desktop Gateway server settings and logon settings when you are working remotely.

5 Click **Connect**.
6 Enter the login credentials for connecting to the remote session in the **Security** dialog box.

NOTE: The standard version (default) is used for a single monitor display, while the Span version can be used when extending a single session to two monitors for dual-monitor capable thin clientsOptiplex clients. The Span version can be used when extending a single session to two monitors for dual-monitor.

Using VMware Horizon Client

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.

Use the **VMware Horizon Client** window to connect to a virtual desktop . To open the **VMware Horizon Client** window, perform either of the ways mentioned here:

- On the taskbar, click **Start** > **All Programs** > **VMware** > **VMware Horizon Client**.
- Double-click the **VMware Horizon Client** icon on the desktop.

To use the VMware Horizon Client, follow the guidelines mentioned here:

1 To add a new server, click the **New Server** button or double-click the **Add Server** icon in the upper-left corner of the **VMware Horizon Client** window.

The **VMware Horizon Client** dialog box is displayed.

2 In the **VMware Horizon Client** dialog box, enter the host name or IP address of a View Connection Server in the Connection Server box, and then click **Connect**.

3 Enter your credentials, and then click **Login**.

4 Select a desktop from the list, and then click **Connect**. VMware Horizon Client connects to the selected desktop. After connection is established, you can view the client window.

For more information, go to www.vmware.com, and refer to the VMware Horizon View Client documentation.

NOTE:

For additional options, click the **options** icon in the upper-right corner of the **VMware Horizon Client** window. The available options are Help, Support information, About VMware Horizon Client, Configure SSL, and Hide the selector after launching an item.

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 taskbar, click **Start** > **All Programs** > **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.

4

Notable Administrator Features

This chapter explains the notable administrator features that are available for you to configure.

The administrator features include:

- Using Administrative Tools
- Using TPM and BitLocker
- CAD Tool
- Configuration Manager (SCCM)
- Dell Wyse RAMDisk
- Enabling Auto Logon
- Device Manager: Bluetooth Connections
- Connecting to a Printer or an External Device
- Display: Dual Monitor Display
- Display: Rotation
- Network and Sharing Center: Wireless Local Area Network (WLAN) Settings
- Realtek HD Audio Manager
- Setting Region and Language
- Sounds and Audio Devices
- User Accounts
- Windows Defender
- About Threat Defense
- Introduction to Unified Build

NOTE:

1. User is allowed to configure some of the features such as Dual Monitor in the **Display** settings. Only the Administrator can enable/disable the File Based Write Filter to configure the thin-clients and to persist after a thin-client reboot.
2. Additional software features are available for the download. For more information, refer release notes of the latest build and contact Technical Support.

Using Administrative Tools

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

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

- Configuring the Component services
- Viewing the Events
- Managing the Services

Configuring the 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 drop-down list to 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 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 clientOptiplex client, use the **Services** window. To open Services window, go to **Start** > **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. To go to Startup type, click **Properties** > **General tab** > **Startup Type**.

- 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.

CAUTION: During the thin client device restart, to ensure that the thin client configuration is saved disable the File Based Write Filter (FBWF). Be sure to enable the FBWF later. For more information, see Before Configuring Your Thin Clients.

NOTE:

You can use the **Auto Logon** dialog box, go to **Start** > **All Programs** > **Dell Thin Client Application** > **Auto Logon**) to disable Auto Logon feature. You can easily log in as an administrator when you restart your thin client device.

To use TPM and BitLocker:

1 Ensure that the TPM-supported client is running the latest WES7P build, that also supports TPM.
2 Enter the BIOS and then enable TPM. To enable TPM:
a On the BIOS configuration pane, click the **Security** tab. For more information on accessing the BIOS, see Accessing Thin Client BIOS Settings.

b Under TPM Support, select **Enabled** to enable the TPM.

c To save your changes, press the **F10** key.

3 Restart the client to the OS. Verify that the OS has a separate system partition which contains the files needed to start the client. By default the system partition is an active partition.

4 Launch the Services.msc (click the Services icon in the Component Services console), open the **HAgent Properties** dialog box (double-click **HAgent** in the Name list of the Services window of the Component Services console), set the Startup type to **Manual**, and then click the **Stop** button to stop the HAgent service.

5 On the Windows desktop, click **Start menu** > **Run**, type **Gpedit.msc** in the Open box, and then press the **Enter** key to open the Local Group Policy Editor window.

6 To open the Require additional authentication at startup window, go to **Local Computer Policy** > **Administrative Templates** > **Windows Components** > **BitLocker Driver Encryption** > **Operating System Drives** > **Require additional authentication at startup**.

7 In the Require additional authentication at startup section, select the Enabled option and clear/uncheck the **Allow BitLocker without a compatible TPM** option.

8 To open the Configure TPM platform validation profile window, go to **Local Computer Policy** > **Administrative Templates** > **Windows Components** > **BitLocker Driver Encryption** > **Operating System Drives** > **Configure TPM platform validation profile**.

9 In the Configure TPM platform validation profile section, select the **Enabled** option and clear/uncheck the **PCR4**, **PCR5**, **PCR8**, **PCR9** and **PCR10** validation profiles.

10 Once the above policies are set, force update the policies using the gpupdate/force command or reboot the client.

11 On the Windows desktop, click **Start menu** > **Run**, type **tpm.msc** in the Open box, and then press the **Enter** key to open the TPM Administration window (or you can click **Start** > **Control Panel** > **BitLocker Drive Encryption** > **TPM Administration**) where you can verify that the **Initialize TPM** option is enabled; if this option is disabled, then clear the TPM by using the **Clear TPM** option, reboot the client, and then repeat this step to verify that the **Initialize TPM** option is enabled. In some of the clients, TPM is initialized by default.

12 After verifying that the **Initialize TPM** option is enabled, click **Initialize TPM**, and then reboot the client.

13 After reboot, TPM will be initialized and it involves enabling and taking ownership of TPM.

14 Now you can use the Turn On BitLocker link to turn on the BitLocker C drive encryption in the BitLocker Drive Encryption Properties dialog box (Click **Start menu** > **Control Panel** > **BitLocker Drive Encryption** icon).

> **NOTE:**
> Whenever TPM is to be initialized, the client must be restarted because the security hardware must be initialized. Since the security hardware must be initialized, a BIOS screen immediately displays prompting the user for confirmation.

Upon accepting, the security hardware is initialized. Then the TPM ownership must be taken by providing a password. It is recommended that once a TPM is initialized, it is best not to change the state or disable it. Leaving the TPM initialized is not an issue with Imaging, as Imaging is independent of TPM.

The options available for BitLocker Drive Encryption depend on the policy set. Since the Allow BitLocker without a compatible TPM is not set/selected, the following BitLocker startup preferences are displayed when TPM is enabled, initialized and owned.

CAD Tool

The CAD Tool allows administrators to map the Ctrl+Alt+Del key combination to VDI applications to display the Ctrl+Alt+Del screen of the VDI application. Use the Ctrl+Alt+Del key combination instead of the following key combinations to display the Ctrl+Alt+Del screen of the respective VDI application.

- Citrix: **Ctrl+F1**
- Dell vWorkspace: **Ctrl+Alt+End**
- RDP: **Ctrl+Alt+End**
- VMView: **Ctrl+Alt+Insert**

NOTE: The limitations of CAD Tool are:

- The CAD tool does not work for Xen Desktop in a Citrix session, but works only for Citrix Xen applications.
- This does not work with VMware View Version 3.3.0 Build 2507564

.

System Center Configuration Manager

To view and configure the Microsoft SCCM components installed on your thin clientOptiplex client, use the **Configuration Manager Properties**.

To open **Configuration Manager Properties** dialog box, go to **Start** > **Control Panel** > **Configuration Manager**.

For more information, refer the SCCM Guide for managing Dell Wyse thin clients at www.dell.com/wyse/manuals.

Dell Wyse Custom Fields

To enter the configuration strings used by the WDM Software, use the **Dell Wyse Custom Field** dialog box. The configuration strings gives you the information regarding the location, user, administrator, and so on.

Click **OK** to copy the custom field information that is entered to the Windows Registry.

NOTE: For details on using Custom Field information, see the WDM documentation available at downloads.dell.com/wyse/WDM/.

Dell Wyse RAM Disk

RAM Disk is volatile memory space used for temporary data storage. It is the Z drive shown in the **My Computer** console. 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, go to **Start** > **All Programs** > **Dell Thin Client Application** > **RAM Disk**. After the changes made in the size of the RAM Disk, restart the thin clientOptiplex client for the changes to be saved. To permanently save the changes, make sure the files of the File Based Filter cache have been cleared during the recent system session before the thin clientOptiplex client reboot.

NOTE: The default RAM Disk size may vary depending on the thin clientOptiplex client and size of the installed memory. The minimum RAM Disk size can be set is 2 MB. The maximum RAM Disk size can be set is 1024 MB. Usually, the default value is set to 512 MB.

Enabling Auto Logon

By default, Automatic logon to a user desktop is enabled. Auto login changes can be made in the **Auto Logon Settings** window. To open **Auto Logon Settings** window, go to **Start** > **All Programs** > **Dell Thin Client Application** > **Auto Logon**

The following changes can be made in the **Auto Logon** window:

- Enable or disable Auto Logon
- Change the Default User Name
- Change the Default Password
- Change the Default Domain

Device Manger: Bluetooth Connections

You can access Bluetooth- enabled devices in your thin-client device, if your thin-client has optional Wireless Bluetooth capability.

1 To manage an existing Bluetooth device :
   a Go to **Start** > **Control Panel** > **Device Manager**
   b Click **Bluetooth Radios**.
   c To manage an existing Bluetooth device, double-click on the **Bluetooth icon**

   You can update drivers using the **Driver** tab

2 To add Bluetooth- enabled device:
   a Go to **Start** > **Control Panel** > **Devices and Printers**

   Devices and Printers window is displayed
   b Click **Add a Device**.
   c Turn on the Bluetooth — enabled devcie and ensure that the device is discoverable.
   d When the device is discoverable by the thin-client device, click **Next** and follow the wizard.

NOTE: Be sure to disable the File Based Write Filter and to configure NetXClean to refrain from clearing up your settings. For more information, see Before Configuring Your Thin Client

Connecting to a Printer or an External Device

To connect a parallel printer to your thin clientOptiplex client device through a USB port, make sure that you have a USB -to-parallel printer adapter cable. You also need to install the driver for the printer by following the printer driver installation instructions.

To connect to the printer, you add the printer to the thin clientOptiplex client by using the Add Printer wizard. For more information see Adding Printer.

If you want to connect to an external device, you add the device to the thin clientOptiplex client. For more information, see Adding Device.

Adding Printer

To add a printer to the thin clientOptiplex 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 Printer** wizard, click **Add a Printer**.

   A universal print driver is installed on the thin clientOptiplex client to support text-only printing to a local printer. 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 View** applications can be achieved through printer drivers on the servers.

   Printing to a local printer from Citrix Receiver, Remote Desktop Connection, or VMware Horizon View 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 clientOptiplex 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 Device

To add a device to the thin clientOptiplex 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 clientOptiplex client.

Display: Dual Monitor Display

To configure the dual monitor settings, go to **Start** > **Control Panel** > **Display** > **Change Display Settings**. The configurations are made in the **Screen Resolution** window and it is applicable for Dual-Monitor capable thin clientsOptiplex client only.

For more information, refer www.microsoft.com.

For more information on Multi-Display, Multi-Touch and Dual-Monitor Supported thin-client devices, refer www.dell.com/wyse/knowledgebase.

TIP: While configuring Dual-Monitor settings, set the same screen resolution for both the monitors.

Display: Rotation

To configure the display rotation feature, do the following:

1 On the taskbar, click **Start** > **All Programs** > **AMD Catalyst Control Center** > **AMD Catalyst Control Center**.
The **AMD Catalyst Control Center** window is displayed.
2 In the upper-right corner of the window, click **Preferences**.
3 From the drop-down menu, click **Hotkeys**.
The **Hotkeys Manager** dialog box is displayed.
4 Select the **Enable Hotkeys feature** check box.
5 From the **List Hotkeys** drop-down list, select **Creating and Arranging Desktops**.
The available Hotkeys actions that can be configured are listed.
6 Select the preferred rotation action check box for which you want to assign the Hotkey, and then click **Edit**.
The **Edit Hotkeys** dialog box is displayed.
7 From the drop-down list, select the modifier keys to associate with Hotkey.
8 Use the keyboard arrow buttons to associate with the selected modifier keys.

NOTE: White space Character cannot be used as a Hotkey.

9 Click **OK** to activate the Hotkey feature.

For more information, go to answers.microsoft.com/en-us/windows/forum/windows_7-desktop/how-torotate-screen-in-windows-7-by-a-shortcut/55fca2a8-c34f-41f6-81ba-ce44e7127aeb?auth=1.

Network and Sharing Center: Wireless Local Area Network (WLAN)Settings

If Dell Wyse supported WLAN hardware modules are installed on the thin client, clicking the **Network and Sharing Center** icon in the Control Panel allows you to:

1 **Manage Wireless Networks** (click the **Manage Wireless Networks** link):

- Add —Click **Add** to open and use the wizard to add a wireless network to edit an existing wireless network, right-click it, and then select **Properties** to open and use the **Network Properties** dialog box.
- Adapter Properties —Click **Adapter Properties** to open and use the properties dialog box for the wireless adapter.
- Profile Types —Click **Profile Types** to open and use a dialog box to the enable or disable the ability to create Per User Profiles.
- Network and Sharing Center - Click **Network Sharing Center** to return to the **Network and Sharing Center** dialog box provides network settings, and gives access to network settings.

2 **Change Adapter Settings** click the **Change Adapter Settings** link:

- Click **Organize** to open the list of options you can use to organize your network connections.
- Select a connection to display the list of command buttons you can use to view the status, connect to, enable, disable, diagnose, rename, and change thesettings of the connection.

3 **Change Advanced Sharing Settings** (click the Change Advanced Sharing Settings link): Select the network profile settings you want for each of your networks.

Realtek HD Audio Manager

To manage your audio and audio devices, go to **Realtek HD Audio Manager** dialog box. Use the **Volume** icon in the taskbar to adjust the volume. Click the **Volume** icon to open the master volume control. Power speakers are recommended.

Setting Region and Language

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

1 Log in as an Administrator.

2 On the taskbar, click **Start** > **Control Panel** > **Region and Language**.

The **Region and Language** 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 **Keyboards and Languages** tab, you can change your keyboard or input language and install or uninstall languages that Windows can use to display text and where supported recognize speech and handwriting.

6 In the **Administrative** tab, you can change **system locale** and **copy settings**.

Sounds and Audio Devices

To manage your audio devices, go to **Sound** dialog box.

The following configurations can be made in the following tabs:

- **Playback** : Select a playback device to modify its settings. After the changes are made, click **Apply**.

- **Recording** : Select a recording device to modify its settings. After the changes are made, click **Apply**.
- **Sounds** : A sound theme is a set of sounds applied to events in Windows and programs. You can select an existing scheme or save one you have modified. After the changes are made, click **Apply**.
- **Communications** : Windows can automatically adjust the volume of different sounds when you are using your PC to place or receive phone calls.

  Select any one of the radio button as per your requirement, when Windows detects communication activity:

  - Mute all other sounds
  - Reduce the volumes of other sounds by 80%
  - Reduce the volumes of other sounds by 50%
  - Do nothing

Volume can also be adjusted using the **Volume** icon in the system tray of the taskbar. Powered speakers are recommended.

User Accounts

To manage users and groups, go to **Start** > **Control Panel** > **User Accounts**.

The following tasks can be performed in the User Accounts window:

- Change your password
- Remove your password
- Change your picture.

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

Windows Defender

To scan your Optiplex client thin clients and protect against spyware and malware, click **Scan Now** in the **Window Defender** window. To open **Windows Defender** window, go to **Start** > **Control Panel** > **Windows Defender**.

To configure and manage the anti-spyware and anti-malware software settings, click **Options** in the **Tools and Settings** console. To open **Options** console, go to **Start** > **Control Panel** > **Windows Defender** > **Tools** > **Options**.

NOTE:

Windows Defender Auto Update

- This auto update feature is provided for Windows defender to update on every second Sunday of the month. By default. this auto update is set at 1:00 A.M. However. reboot has to be done manually or an Administrator has to initiate reboot from management server every month on the second Sunday after 30 minutes from the auto update start time, to reflect defender updates.
- The auto update process runs in background and notification on the auto update progress is not displayed on the screen.

About Threat Defense

Dell Data Protection | Threat Defense (powered by Cylance) is an advanced threat prevention solution deployed to prevent damage that malware causes to thin client. This solution stops malicious files, and other malicious active scripts from getting executed. The threat prevention solution can be centrally managed using cloud-based console. Constant internet connection is not required and this solution protects your thin client from malware attacks even when you are offline. For more information about Threat Defense, refer to the Dell Data Protection - Threat Defense Administrator Guide.

Introduction to Unified Build

The WES7P v9.07 unified build is a 64-bit image that supports English (en-US) and the following languages:

- German—de-DE

- Spanish—es-ES
- French France—fr-FA
- French Canadian—fr-CA
- Italian—it-IT
- Japanese—ja-JP
- Korean—ko-KR
- Chinese Simplified—zh-CN
- Chinese Traditional—zh-TW
- Portuguese Brazilian—pt-BR

Imaging Support using WDM/USB

Use WDM or USB imaging tool to *image* the Wyse 5060 thin clients running WES7P unified build.

Unified build contains the language metadata in the Merlin partition. Imaging the unified build results in the same MUI language that is available in Merlin. To change the language, do the following:

1 Click **Start** > **Computer** > **C:** > **Windows** > **Setup** > **Tools**.

The **LanguageConfig** application is available in the Tools folder.

2 Double-click the **LanguageConfig** application.

The **Language Config** window is displayed.

3 Select any one of the following languages as per your requirement and then click **Apply**.

- German—de-DE
- Spanish—es-ES
- French France—fr-FA
- French Canadian—fr-CA
- Italian—it-IT
- Japanese—ja-JP
- Korean—ko-KR
- Chinese Simplified—zh-CN
- Chinese Traditional—zh-TW
- English—en-US
- Portuguese Brazilian—pt-BR

4 Run Sysprep or push the unified build again to reflect the language changes. Changing the language writes the language metadata to the Merlin partition. The thin client boots up with the desired language that you have selected in the tool.

5

Additional Administrator Utility and Settings Information

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

It discusses:

Automatically Launched Utilities

The following utilities are automatically started:

- **File Based Write Filter** — Upon system start, the File Based Write Filter utility is automatically launched. It provides a secure environment for thin client computing by protecting the thin client from undesired flash memory writes. The active (green) or inactive (red) status of the filter is indicated by the color of the File Based Write Filter status icon in the system tray of the taskbar. See Using the File Based Write Filter (FBWF)
- **NetXClean** — Upon system start, the NetXClean utility is automatically launched. 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 for example, 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 launched. VNC allows a thin client desktop to be accessed remotely for administration and support. See Using TightVNC (Server and Viewer) to Shadow an 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 Optiplex client:

- **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 details about NetXClean, Brief Introduction about 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** > **Control Panel** > **Power Options**.

- **Wake-on-LAN** — This standard Windows Embedded Standard 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.
- **Thin Client Time** —After power off, clock time will not be lost as long as the power source remains on. Clock time will be lost, if the power source is off and a battery is not installed.

NOTE:

Correct time should be maintained as some applications require access to local thin client time. Use the Date and Time dialog box **Start** > **Control Panel** > **Date** and **Time** or by clicking the time area in the taskbar and then clicking the Change date and time settings link to edit the time and date as needed.

Using the File Based Write Filter (FBWF)

The File Based Write Filter provides a secure environment for thin clientOptiplex client computing by protecting the thin clientOptiplex client from undesired flash memory writes flash memory is where the operating system and functional software components reside. By preventing excessive flash write activity, the File Based Write Filter also extends the life of the thin clientOptiplex client. It gives the appearance of read-write access to the flash by employing a cache to intercept all flash writes and returning success to the process that requested the I/O.

The intercepted flash writes stored in cache are available as long as the thin clientOptiplex client remains active but are lost when the thin clientOptiplex client is restarted or switched off. To preserve selected changes, the selected files of the cache can be transferred to the flash manually using Commit in the File Based Write **Filter Control** dialog box; alternatively, if the files affected by the changes are not known, the changes can be made after disabling the File Based Write Filter using the **File Based Write Filter Control** dialog box, and then re-enabling the File Based Write Filter, For more information, see Setting the File Based Write Filter Controls.

The File Based Write Filter can be controlled either through the command line (fbwfmgr) or by double-clicking the File Based Write Filter icon in the Administrator system tray. The File Based Write Filter can flush specified files to the flash from cache only up to the point when the commit is performed; if more writes are performed on the files that have been flushed, then these files must be flushed/committed again if the additional changes also need to be preserved.

The File Based Write Filter can also be enabled/disabled through the command line or through the File Based Write Filter Enable/Disable desktop icons. The status (enabled/disabled) of the File Based Write Filter is displayed by the File Based Write Filter status icon in the system tray green indicates that the File Based Write Filter is enabled and red indicates that the File Based Write Filter is disabled.

NOTE:

- Contents of the File Based Write Filter cache should never be flushed if it is eighty-percent or more full. The Administrator should periodically check the status of the cache and restart the thin clientOptiplex client if the cache is more than eighty percent full. Note that alternatively an administrator can configure the client to reboot if the FBWF cache is 90 percent or more full. By default the client is configured to reboot if the FBWF cache usage exceeds 90 percent.
- A Terminal Services Client Access License (TSCAL) is always preserved regardless of File Based Write Filter state (enabled or disabled). If you want to have other registry settings preserved regardless of File Based Write Filter state, contact support for help as described in **Technical Support.**

WARNING: It is highly recommended that Windows write filter is kept enabled during normal use of thin clients. It should be disabled only by administrators while making necessary changes. Extended use with write filters turned off can reduce the life of your flash drive. It is a good practice to have write filters enabled to ensure device security.

This section provides the following information on using the File Based Write Filter:

Changing Passwords with the File Based Write Filter

On Microsoft Windows based machines, account passwords are regularly changed with the domain controller for security purposes. The same password process is applicable for a thin clientOptiplex client if the thin clientOptiplex client is a member of such a domain. With the File Based Write Filter enabled, a thin clientOptiplex client will successfully make this password change with the domain controller. However, since the File Based Write Filter is enabled, the next time the thin clientOptiplex client is booted it will not retain the new password. In such cases, you can use the following options:

- Disable the machine account password change on the thin clientOptiplex client by setting the **DisablePasswordChange** registry entry to a value of 1.
- Disable the machine account password change on the Windows based server by using the Microsoft documentation for the operating system.

  For example, on Windows 2003 Server, set the RefusePasswordChange registry entry to a value of 1 on all domain controllers in the domain instead of on all workstations. Clients will still attempt to change their passwords every 30 days, but the change will be rejected by the server.

NOTE: If you set the RefusePasswordChange registry entry in the Windows 2003 Domain Controller to a value of 1, the replication traffic will stop, but not the thin clientOptiplex client traffic. If you also set the DisablePasswordChange registry entry to a value of 1 in the thin clientOptiplex client, both thin clientOptiplex client and replication traffic will stop.

Running File Based Write Filter Command–Line Options

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

Use the following guidelines for the command–line option for the File Based Write Filter. You can also use the **commands** if you open Command Prompt window by entering command in the Run box:

- **fbwfmgr**

  With no arguments — Displays the File Based Write Filter configuration for the current session and the next.
- **fbwfmgr /enable**

  Enables the File Based Write Filter after the next system restart. The File Based Write Filter status icon is green when the File Based Write Filter is enabled.
- **fbwfmgr /disable**

  Disables the File Based Write Filter after the next system restart. The File Based Write Filter status icon remains red while disabled.
- **fbwfmgr /commit C: <file_path>**

  Commits the changes made to the file to the underlying media. Note that there is a single space between volume name and file_path. The file path must be an absolute path starting with \.

  For example, to commit a file **C:\Program Files\temp.txt** the command would be fbwfmgr **/commit C: \Program Files\temp.txt.**
- **fbwfmgr /restore C: <file_path>**

  Discards the changes made to the file, that is, it restores the file to its original contents from the underlying media. The file path must be an absolute path starting with \. If the file was deleted, it will be recovered.
- **fbwfmgr /addexclusion C: <file_or_dir_path>**

Adds the file or the directory to the exclusion list of the volume. That is, the file or directory is removed from the protection of the File Based Write Filter. The exclusion will take effect after the next system reboot. The file or directory path must be an absolute path starting with \.

- **fbwfmgr /removeexclusion C: <file_or_dir_path>**

  Removes the file or the directory from the exclusion list of the volume. That is, the file or directory is included within the protection of the File Based Write Filter. The removal of the exclusion will take effect after the next system reboot. The file or directory path must be an absolute path starting with \.

- **fbwfmgr /overlaydetail**

  Displays the list of files and directories that are modified, along with the size of memory used by the File Based Write Filter to cache the modified data of the file or directory and the number of open handles to it.

Enabling and Disabling the File Based Write Filter Using the Desktops Icons

For convenience, use the File Based Write Filter enable and disable icons present on the administrator desktop.

- **File Based Write Filter Enable Icon (Green)**— Double-clicking this icon enables the File Based Writer Filter. This Utility is similar to running the fdwfmgr /enable the command line option as described in Running File Based Write Filter Command Line Options. Also, double-clicking this icon immediately restarts the system and enables the File Based write Filter. The File Based Write Filter status icon in the system tray is green when the File Based Write Filter is enabled.
- **File Based Write Filter Disable Icon (Red)**— Double-clicking this icon allows you to disable the File Based Write Filter. This utility is similar to running the fbwfmgr / disable command line option as described in Running File Based Write Filter Command Line Options. However, double-clicking this icon immediately restarts the system and disables the File Based Write Filter. The File Based Write Filter remains disabled and can only be enabled using the File Based Write Filter Enable icon or through the command line as described in Running File Based Write Filter Command Line Options. The File Based Write Filter status icon in the system tray remains red while the File Based Write Filter is disabled.

Setting the File Based Write Filter Controls

Use the **File Based Write Filter Control** dialog box to view and manage your control settings
To view and manage File Based Write Filter control settings, use the File Based Write Filter Control dialog box.

1 To open the dialog box, double-click the FBWF icon in the notification area of the administrator taskbar.
  The **File Based Write Filter** dialog box is displayed.
2 Use the following guidelines setup the Write Filter Controls.
  a FBWF Status area includes:
    - **Current Status** — Shows the status (Enabled or Disabled) of the File Based Write Filter.
    - **Boot Command** — Shows the status of the Boot Command. FBWF_ENABLE means that the FBWF is enabled for the next session; and FBWF_DISABLE means that the FBWF is disabled for the next session.
    - **RAM used by FBWF** — Shows the amount of RAM used (in Kilobytes and Percentage) that is being used by the File Based Write Filter. If **Current Status** is Disabled, RAM Used by FBWF is always zero (0).
    - **Amount of RAM used for FBWF Cache** — Shows (in MB) the amount of RAM (in MB) that is used as File Based Write Filter cache for the current session.
    - **Cache Setting** — Shows the cache setting for the current session.
    - **Warning #1 (percent)** — Shows the FBWF cache percentage value at which a Low Memory warning message is displayed to the user for the current session.
    - **Warning #2 (percent)** — Shows the FBWF cache percentage value at which a Critical Memory warning message is displayed to the user, along with another message display counting down the number of seconds before automatic rebooting will occur for the current session.

- **Reboot Time Delay (in seconds)** — Shows the number of seconds that will lapse before system reboot in the Warning #2 (percent) case of cache overflow for the current session.

b FBWF Cache Settings area includes:

- **Amount of RAM to be used for FBWF Cache** — Shows (in MB) the amount of RAM (in MB) that is to be used as File Based Write Filter cache for the next session. This value should be in the range of 16 MB to 1024 MB. There is an additional check that this value should not exceed 1/3 of Total Available RAM.
- Advanced Cache Settings area includes options to allow you to improve the effectiveness of cache memory (**Cache Compression**, **Cache Preallocation**, or **None**).

c FBWF Warning Settings area includes:

- **Warning #1 (%)** — Shows the FBWF cache percentage value at which a Low Memory warning message is displayed to the user; Default value = 85, Minimum value = 50, Maximum value = 90.
- **Warning #2 (%)** — Shows the FBWF cache percentage value at which a Critical Memory warning message is displayed to the user, along with another message display counting down the number of seconds before automatic rebooting occur; Default value = 90, Minimum value = 55, Maximum value = 95.
- **Reboot Time Delay (in seconds)** — Shows the number of seconds that will lapse before system reboot in the **Warning #2 (%)** case of cache overflow.

d **Enable FBWF** — Allows you to enable the File Based Write Filter and prompts you to restart the thin clientOptiplex client. If you do not restart the thin clientOptiplex client, the changes made will not be saved until the thin clientOptiplex client is restarted. After the system restarts to enable the File Based Write Filter, the File Based Write Filter status icon in the desktop system tray turns green.

e **Disable FBWF** — Allows you to disable the File Based Write Filter and prompt you to restart the thin clientOptiplex client. If you do not restart the thin clientOptiplex client, the changes made will not be saved until the thin clientOptiplex client is restarted. After disabling the File Based Write Filter, the File Based Write Filter status icon in the desktop system tray turns red and the File Based Write Filter remains disabled after the system restarts.

f **Defaults** — Allows you to reset the FBWF Cache Settings area, Advanced Cache Settings area, and the FBWF Warning Settings area to their default values.

g File Commit area includes:

- **File Path** — Allows you to add, remove and commit files to the underlying media, delete a file path from the list if the file is not to be committed. The system will not restart the thin clientOptiplex client. The changes are committed immediately.

h 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 retrieves the list of files or directories that are write through in the current session; the title of the pane is shown as Current Session Exclusion List or the Next Session retrieves the list of files or directories that are write through for the next session; the title of the pane is shown as Next Session Exclusion List. The system will not restart the thin clientOptiplex client and the changes are not committed until an administrator restarts the thin clientOptiplex client manually.

Understanding the NetXClean Utility

NetXClean keeps extraneous information from being stored in flash memory. 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 garbage files from building up and filling the free space in the flash for example, if a flush of some files in the File Based Write Filter cache puts junk in flash directories that must be kept clean. The NetXClean utility is particularly important when multiple users have log-on rights to a thin clientOptiplex client, as memory space can be quickly used by locally stored profiles and temporary caching of information.

NetXClean TweakUI 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 will not delete the following profiles:

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

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

CAUTION: Be careful of application settings that write to the C drive, which resides in flash memory 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 RAMDisk) of the thin clientOptiplex client. It is recommended that you do not use this drive to save data that you want to retain.

For RAM Disk configuration information, see Dell Wyse RAM Disk.

For information about using the Z drive with Roaming profiles, see Participating in Domains.

Drive C and Flash

Drive C is the on-board non-volatile flash memory. It is recommended 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 to 90 percent of the total disk space, then thin clientOptiplex 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 clientOptiplex client image will be irreparably damaged and it will be necessary for you to contact an authorized service center to repair the thin clientOptiplex client.

The File Based Write Filter (if enabled) displays an error message if the cache is overwritten. However, if this message occurs you will be unable to flush files of the File Based Write Filter cache and any thin clientOptiplex client configuration changes still in cache will be lost. Cache is disabled when FBWF is turned off. Items that are written to the File Based Write Filter cache or directly to the flash if the File Based Write Filter is disabled during normal operations including:

- Favorites
- Created connections
- Delete/edit connections

Mapping Network Drives

Users and administrators can map network drives. However, to retain the mappings after the thin clientOptiplex client is restarted, complete the following:

1 Log in as an administrator.
2 On the **Start** menu, click **Computer.**
The **Computer window** is displayed.
3 Click the **Computer** button in the menu bar.
A ribbon with **command buttons** is displayed.
4 Click **Map Network Drive** button in the ribbon.
The Map Network Drive dialog box is displayed.
5 Select the drive letter from the Drive drop-down list, and type or browse for the folder you want to connect to.
6 Select the **Reconnect** at logon check box.
7 Flush the files of the File Based Write Filter cache during the current system session.
Since a User log-on account cannot flush the files of the File Based Write Filter cache, the mappings can be retained by logging off the user account (do not shut down or restart the system), logging back on using an administrator account, and then flushing 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.

Participating in Domains

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

1 Log in as an administrator.
2 Click **Start** > **Control Panel** > **System**.
The **System** window is displayed.
3 In the **Computer name, domain and workgroup settings** section, click **Change Settings**.
The **System Properties** dialog box is displayed.
4 Click **Change** option to change the domain or workgroup.
a Click the **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 clientOptiplex client 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
  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.
- Home Network—To apply the changes, you must restart the computer, and then click **Finish**.

NOTE: Before restarting your computer, save any open files and close all programs.

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 File Based Write Filter should be disabled so that the domain information can be permanently stored on the thin client. The File Based 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 FBWF is especially important when joining an Active Directory domain. For details on disabling and enabling the File Based Write Filter, see Before Configuring Your Thin Clients.

To make the domain changes permanent, complete the following:

a Disable the File Based Write Filter.

b Join the domain.

c Restart the thin client.

d Enable the File Based Write Filter.

NOTE: If you use the File Based Write Filter Enable icon to enable the File Based 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 the NetXClean utility, see Understanding the NetXClean Utility.

Using Roaming Profiles

Roaming profile works in any client any where and is not necessary to use the same client. 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 flash space available for roaming profiles. Sometimes, it may be necessary to remove software components to free space for roaming profiles. But Dell does not recommend you to remove any software components.

Using the WinPing Diagnostic Utility

WinPing is used to start the Windows Packet Internet Groper (PING) diagnostic utility and view the result of echo request sent to a network host.
To open the Dell Wyse WinPing dialog box:

WinPing is a diagnostic tool that sends an echo request to a network host. The host parameter is either a valid host name or an IP address. If the host is operational and on the network, it responds to the echo request. The default is to send three echo requests and then stop if

no response is detected. WinPing sends one echo request per second, calculates round-trip times and packet loss statistics, and displays a brief summary upon completion.

1 Click **Start** > **Run**.
2 Enter the WinPing in the **Open** box, and then click **OK**
The **Dell Wyse WinPing** dialog box is displayed.

a Enter a valid IP address in the IP address box.
b In the **Retries** box, type or select the number of echo requests you want to send out to the network lost.
c Click **Ping**.
WinPing sends one echo request per second, calculates round-trip times and packet loss statistics, and displays a brief summary under the Status section on the dialog box upon completion.

Using the Net and Tracert Utilities

Net and Tracert utilities are available for administrative use, for example, to determine the route taken by packets across an IP network.

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

Managing Users and Groups with User Accounts

Use the **User Accounts** window (**Start** > **Control Panel** > **User Accounts**) to create and manage user accounts, create and manage groups, and configure advanced user profile properties. By default, a new user is only a member of the Users group and is not locked down. As the 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 click the help icon in the User Accounts window to search for items such as user profiles and user groups and 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/disk space constraints, the number of additional users on the thin clientOptiplex client should be kept to a minimum.

NOTE: To permanently save the information, be sure to disable the File Based Write Filter (FBWF).

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 **Create a new user account**.
a If you want to create **Standard account**, select the standard user check box, and then enter the name in box.
b If you want to create **Administrator account** , select the administrator check box, and then enter the name in box.
c Click **Create account**.

Editing User Accounts

To edit the default settings of a Standard User or Administrator account, click on the account you want to modify in the **Manage Accounts** window and then make your changes.
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

To configure the Default, Admin and User profiles stored on the thin clientOptiplex client:

1 Click **Start** > **Control Panel** > **User accounts**.
The **User Accounts window** is displayed.
2 Click **Configure Advanced User Profile Properties.** and use the following guidelines:
a **Change Type** — To change the profile stored on the computer.
b **Delete**— To delete the profile
c **Copy To** — To copy the Profile.

Changing the Computer Name of a thin clientan Optiplex client

Administrators can change the computer name of a thin clientOptiplex client. The computer name information and the Terminal Services Client Access License (TSCAL) are preserved regardless of the File Based Write Filter state that is either enabled or disabled. This maintains the specific computer identity information and facilitates the image management of the thin client Optiplex client.
To change the computer name of a thin client Optiplex client:

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** tab to rename the computer name.
5 In the computer name window, type the name for the thin clientOptiplex client in the Computer name box, and then 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

This chapter contains local and remote system administration information to help you perform the routine tasks needed to maintain your thin client environment.

It includes

- Restoring Default Settings.
- Accessing Thin Client BIOS Settings.
- Imaging Devices with the Dell Wyse USB Imaging Tool.
- Configuring and Using Peripherals.
- Using TightVNC (Server and Viewer) to Shadow a Thin Client.
- WDM Software for Remote Administration.

Restoring Default Settings

Depending on the default settings you want to restore on thethin clientOptiplex client, you can:

- Use the BIOS to restore default values for all the items in the BIOS setup utility For more information, see Accessing Thin Client BIOS Settings.
- Re-image the thin client to restore all factory default settings using the Dell Wyse USB Imaging Tool or WDM, For more information, see Imaging Devices with the Dell Wyse USB Imaging Tool, and WDM Software for Remote Administration.

NOTE: For any information on re-imaging the Optiplex client, refer to *SCCM documentation*.

Preparing to Re-image

The thin client can only be returned to factory defaults by re-imaging the thin client, the same process used when upgrading the firmware. The re-imaging process requires:

- **A clean image** — Go to www.dell.com/wyse/downloads, select the active product download you need images are device dependent; be sure to select the correct model you want to re-image, and then download the files. Note that these files are normally in a compressed (.zip) format and will need to be extracted or executed, if in .exe format before use.
- **Imaging software** — Dell provides two imaging software products to re-image your thin client:
  - Dell Wyse USB Imaging Tool —recommended for smaller environments.
  - Dell Wyse Device Manager (WDM)—recommended for larger environments.

Accessing Thin ClientOptiplex Client BIOS Settings

While starting a thin clientOptiplex client, a Dell logo is displayed for a short period.

1 During the start-up, press the **DelF2** key.
  The **BIOS** Settings dialog box is displayed.
2 When prompted, enter **Fireport** as the password.
3 Change the BIOS Settings as required.

NOTE: To access the Boot Menu screen, during the system restart, press the P key. The P key functionality is valid only if you enable the Popup menu option in the BIOS settings.

Imaging Devices with the Dell Wyse USB Imaging Tool

Dell Wyse USB Imaging Tool provides a simple USB imaging solution to help IT and Customer Service staff quickly and easily image supported devices.

Using the tool's flexible Windows utility, users can easily:

- Configure a USB key to copy or pull firmware from a source device. You can later push to other target devices.
- Configure a USB key to update or push firmware that you include on the USB key to target devices to upgrade firmware.
- Create replicate or duplicate USB keys containing the original contents for simultaneous usage on target devices by users in several locations at the same time.

Configuring and Using Peripherals

The thin client has USB ports available on it.

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

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 the **Dell Wyse Support Site**.
- You can configure the thin client device to use Bluetooth- enabled Peripherals. For more information, see Device Manager Bluetooth Connections.

Using TightVNC to Shadow a Optiplex ClientThin Client

TightVNC Server starts automatically as a service upon thin client Optiplex 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.**

- You may also use the TightVNC Server features in **Start** > **All Programs** > **TightVNC Server (Service Mode)**

3 To shadow a Optiplex client thin client from a remote machine use the following guidelines:

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 shadowed or operated or monitored.

c Click **OK**.

The **VNC Authentication** dialog box is displayed.

d Enter the Password of the Optiplex clientthin client that is shadowed, and then click **OK**.

This is the Primary Password of the Optiplex client thin client that is shadowed.

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

TightVNC (Server and Viewer) — Pre-requisites

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

- IP address or valid DNS name of the thin clientOptiplex client to be shadow, operate or monitor. For more information, see Using the Dell Thin Client Application.
- Primary password of the thin clientOptiplex client 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 clientOptiplex client, move the pointer over the TightVNC icon in the taskbar.
- To configure TightVNC Server, the Default primary password is DELL.

TightVNC (Server and Viewer)

To configure or reset a thin clientOptiplex client from a remote location, use TightVNC (Server and Viewer). TightVNC is primarily intended for support and troubleshooting purposes.

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

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

- To open TightVNC Server window, click **Start** > **All Programs** > **TightVNC** > **TightVNC Server (Service Mode)**

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 File Based Write Filter during the current system session.

Configuring TightVNC Server Properties on the Thin ClientOptiplex Client

To Configure the TightVNC Server Properties on the Thin ClientOptiplex Client.

1. To open the **TightVNC Server Configuration (offline)** dialog box, click **Start** > **Program** > **TightVNC Server (Application Mode)** > **TightVNC Server** > **Offline Configuration.**

   TightVNC Server Configuration (offline) dialog box is displayed.
2. In the **Server tab**, set the **Primary password** or **View-only password**. Use this password while shadowing the thin clientOptiplex client.

   Default password is **DELL**.
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 In the **Server tab** , 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, it is highly recommended that the Primary Password be changed for administrator use only immediately upon receipt of the Thin ClientOptiplex Client.

WDM Software for Remote Administration

WDM servers provide network management services to the thin client complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot, rename, automatic device check-in support, Wake-On-LAN, change device properties, and so on With WDM you can manage all of your network devices from one simple-to-use console

For local custom fields that can be accessed by WDM, see Dell Wyse Custom Fields.

7

Using Dynamic Host Configuration Protocol (DHCP)

This appendix contains the DHCP options you can use with your thin clientOptiplex client. A thin clientOptiplex client is initially configured to obtain its IP address and network configurations from a DHCP server, new thin clientOptiplex client or a thin clientOptiplex client reset to default configurations. A DHCP server can also provide the IP address or DNS name of the file server and the root-path location of software in Microsoft .msi form for access through the DHCP upgrade process. Using DHCP to configure and upgrade thin clientOptiplex client is recommended and saves you the time and effort needed to complete these processes locally on multiple thin clientOptiplex client, if a DHCP server is not available, fixed IP addresses can be assigned and must be entered locally for each device.

For more information on configuring a DHCP server see documentation on the Microsoft web site at www.microsoft.com.

DHCP Options

Option	Description	Notes
1	Subnet Mask.	Required.
3	Router.	Optional but recommended. It is not required unless the thin clientOptiplex client must interact with servers on a different subnet.
6	Domain Name Server (DNS).	Optional but recommended. Can be either an IP address or a string such as MyDNSServer.com.
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 clientOptiplex client.
57	Maximum DHCP Message Size.	Optional. Always sent by thin clientOptiplex client.
58	T1 (renew) Time.	Required.
59	T2 (rebind) Time.	Required.
61	Client identifier.	Always sent.

161	File server list.	**Optional string**. Can be either the name or the IP address of the File server where the updated thin clientOptiplex client image is stored. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to also be the file server.
162	Root path to the file server. (FTP/HTTP/HTTPS).	Optional string.
163	SNMP Trap server IP Address list.	Optional.
164	SNMP Set Community.	Optional.
165	RDP startup published applications.	Optional.
166	Ericom - PowerTerm Session Manager Mode.	Optional.
167	Ericom - PowerTerm Session Manager ID.	Optional.
168	Name of the server for the virtual port.	Optional.
183	Defines the protocol to be used for downloading the WCM configuration file to the client and any custom items in the folder from the server specified in DHCP Option 195. Valid protocols are FTP, HTTP, and HTTPS. The default protocol is FTP.	Depending on your protocol use either of the following values: • FTP use: **FTP** • HTTP use: **HTTP** • HTTPS use: **HTTPS**.
184	Server Username.	**Optional string.** This is the username to use when authenticating to the server specified in Option 195.
185	Server Password.	**Optional string.** Password to use when authenticating to the server specified in Option 195. If the server allows Anonymous log in, you can leave this option blank.
195	Server (FTP/HTTP/HTTPS).	Optional IP Address or string. Can be either the IP Address or the fully qualified domain name (FQDN) of the Repository server. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to be the server.
196	Default WCM configuration path (FTP/HTTP/HTTPS).	**Optional string**. The relative directory starting from the root directory must be given. If 196 is not defined and is left blank: • FTP: For FTP, the default WCM configuration path is **c:\intpub\ftproot\\Wyse\WES7P.**

		• HTTP or HTTPS: For HTTP or HTTPS, the default WCM configuration path is the path specified by the virtual directory in IIS; usually wwwroot. For example, C:\inetpub\wwwroot\Wyse\WES7. **NOTE: For custom WCM configuration paths use only one of the following string values where Finance is your custom defined pathfor DHCP Option 196:** • FTP custom example: C:\inetpub\ftproot\Wyse\WES7\Finance • HTTP custom example: C:\inetpub\ftproot\Wyse\WES7\Finance • HTTPS custom example: C:\inetpub\ftproot\Wyse\WES7\Finance