Dell Enhanced Microsoft Windows Embedded Standard 7 P — 64 Bit

Administrator’s Guide for OptiPlex 9020M

Notes, cautions, and warnings

✎ NOTE: A NOTE indicates important information that helps you make better use of your computer.

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

Copyright © 2015 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2015 - 06

Rev. A00

Contents

1

Introduction

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

Other locally installed software permits remote administration of the Optiplex 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 Optiplex client supports Microsoft Silverlight and Microsoft NET Framework 3.5 or later versions. For more information about Silverlight and Framework, go to www.microsoft.com.

About this Guide

This guide is intended for administrators of Optiplex Client running Dell Enhanced Microsoft Windows Embedded Standard 7 Professional. It provides information and detailed system configurations to help you design and manage a WES7P client environment. Depending on your hardware and software configurations, the figures you see may be different than the example figures shown in this guide.

This guide supplements the standard Microsoft Windows Embedded Standard 7 documentation supplied by Microsoft Corporation. It explains the differences, enhancements, and additional features provided by Dell with the Optiplex client. It does not attempt to describe the standard features found in Microsoft Windows Embedded Standard 7.

Windows Embedded Standard 7 help can be accessed from the Microsoft Help and Support website at support.microsoft.com/default.aspx .

Supported Product

This guide is intended for **Dell OptiPlex 9020M client**.

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, software downloads, registration, warranty extensions/RMAs, reference manuals, and so on, visit www.dell.com/wyse/support. If you still need help, you can call Customer Support at 877-459-7304, Extension: 5137801. Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

.

2

Getting Started

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

To get started using your Optiplex client see:

- Logging On, see Logging On
- Using your Desktop, see Using Your Desktop
- Before Configuring Your Optiplex clients, see Before Configuring Your Optiplex Clients
- Connecting to a Printer, see Connecting to a Printer
- Connecting to a Monitor, see Connecting to a Monitor
- Logging Off, see Logging Off

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 Optiplex client in your environment, see Using Dynamic Host Configuration (DHCP).

Important:

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

Logging On

The initial display that you see when you turn on your Optiplex client or during the reboot of your Optiplex 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 Dell Wyse Winlog.

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

Using Your Desktop

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

For viewing your desktop, you must log in to your Optiplex 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** — Full Administrator taskbar.
- **Connection Icons**— Connection icons such as VMware Horizon Client, Citrix Receiver, Remote Desktop Connection, Ptstart, and vWorkspace AppPortal.
- **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 administrators.
- **Administrator system tray icons**.

  For more options, see 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**— Full User taskbar.
- **Connection Icons**— Connection icons such as VMware Horizon Client, Citrix Receiver, Remote Desktop Connection, Ptstart, and vWorkspace AppPortal.
- **Start Menu** — Click the **Start** button to open the **start** menu for users.
- **User System Tray**.

  For more options. see Notable User Features.

Before Configuring Your Optiplex Client

File Based Write Filter Utility and NetXClean Utility are meant to protect your Optiplex clients. These utilities prevent your Optiplex 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 Optiplex client.

Connecting to a Printer

To connect a local printer to your Optiplex 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 Optiplex client model, with proper monitor cables, splitters or adapters you can connect to a monitor using the following:

- A VGA (analog) monitor port
- A Display(digital) port

For more information on configuring dual display settings, see Dual Monitor Display.

Logging Off

To log off the Optiplex client:

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 Optiplex client.
   - **Sleep**— This mode enables the power-saving state and allows the Optiplex 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 Optiplex client by either of the ways: using the Windows Security window.
   - From the **Start** menu, click **log off** if you want to log off your Optiplex client.
   - Press CTRL+ALT+DEL to open the **Windows Security** window, and then click **log off**.

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

3

Notable User Features

When you log in to your Optiplex client as a User, the Windows desktop displays certain notable extended features in the **Programs** menu.

You can perform the following activities:

- To browse the internet, use Internet Explore; Using the Internet Explorer.
- View Client Information; see Viewing Client Information.
- Configure Citrix Receiver session services; see Using the Citrix Receiver.
- Ericom — PowerTerm Session Manager, see Using the Ericom PowerTerm Terminal Emulation..
- Ericom Power Term WebConnect, see Using Ericom Power Term WebConnect.
- Remote Desktop Connections, see Configuring a Remote Desktop Connection Session Services.
- To connect to a virtual desktop, use VMware Horizon View Client; see Using the VMware Horizon Client.
- Configure vWorkspace connections; see Using the vWorkspace AppPortal.

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 in the Optiplex client Administrator desktop.
- Click the **Start** button on the taskbar, click **All Programs**, and then click **Internet Explorer** on the Programs Menu.

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 modified the settings. If you require more browser resources, you can access another browser through an ICA, RDP, VMware, or Dell vWorkspace session.

Viewing Client Information

Use the **Client Information** dialog box to view information about the Optiplex client. To open the **Client Information** dialog box, perform either of the ways mentioned here:

- Click the Client Information Quick Launch icon on the taskbar on the Optiplex client Administrator desktop.

- Click the **Start** button on the taskbar, click **All Programs**, and then click **Dell Wyse Client Information** on the Programs Menu.

To view the Optiplex client information, click the following tabs:

1. **General** — Displays the following device information:
   - Website
   - Product Name
   - Product ID
   - Version
   - Windows Embedded Version
   - Ethernet MAC Address
   - IP Address
   - Serial Number
   - Terminal H/W Rev — The related information is displayed as **N/A**
   - CPU Type
   - CPU Speed in MHz
   - Flash Capacity
   - RAM Capacity
   - System Partition
   - User Name
   - OS Activation Status
2. **Installed Modules**— Displays the list of applications that are installed on the Optiplex client.
3. **WDM Packages** — The tab is displayed blank because this feature is not supported on Optiplex client.
4. **QFEs** — Displays the list of Microsoft QFEs (previously known as hot fixes) applied to the Optiplex Client.
5. **Copyrights/Patents** — Displays copyrights and patents information.

Using the Citrix Receiver

Use the **Citrix Receiver** window to access your hosted applications from your desktop or a Web interface. To open the **Citrix Receiver** window, perform either of the ways mentioned here:

- On the Optiplex 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 the Ericom-PowerTerm Terminal Emulation

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

- **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 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**.

Using Ericom PowerTerm WebConnect

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 Ericom PowerTerm WebConnect window, 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 on 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 the **Internet Explorer** icon in the taskbar on Optiplex Client Administrator’s 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 on 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.

Configuring a Remote Desktop Connection Session Services

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 Optiplex 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 Optiplex clients. The Span version can be used when extending a single session to two monitors for dual-monitor.

Using VMware Horizon Client

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 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.

Using the vWorkspace AppPortal

Use the **vWorkspace AppPortal** window to access your hosted applications from your desktop or a Web interface. To open the **vWorkspace AppPortal** window, perform either of the ways mentioned here:

- On an Optiplex client Administrator desktop, double-click the **AppPortal** icon.
- On the taskbar, click **Start** → **All Programs** → **Quest Software** → **vWorkspace Connector for Windows** → **AppPortal**.

1. To add a In the **vWorkspace** dialog box, enter your vWorkspace Server Name, URL, or file path for the connection, and then click **OK**.
2. Enter the your credentials, and then click **Login**.
3. Select a desktop from the list, and then click **Connect**. vWorkspace connects to the selected desktop. After connection is established, the client window is displayed.

To manually set up a vWorkspace configuration, see Setting Up a vWorkspace Configuration Manually .

Setting up a vWorkspace Configuration Manually

To manually set up a vWorkspace Configuration:

1. In the **vWorkspace AppPortal** window, click **Actions** on the toolbar, and then click **Manage configurations**.

   The **New Configuration** dialog box is displayed.
2. In the **New Configuration** dialog box, use the following guidelines to set up a vWorkspace Configuration:
   a. In the **Select Configuration** tab, click the **create new configuration** button if you want to create new configuration, and tehn click **Next**.

      If you want to make changes in an existing configuration, click the **Modify existing configuration** button.

   b. In the **Connectivity** tab, click the plus symbol, enter the name or IP address of the server in the box, and then click **OK**.
   c. Click **Next**.
   d. In the **Firewall/Proxy Traversal** tab, enter the firewall or proxy information, and then click **Next**.
   e. In the **Credentials** tab, specify the credentials for the respective configuration, and then click **Next**.
   f. In the **Display** tab, configure the Display settings and Color Settings as per your requirement, and then click **Next**.

      You can set the appearance of application and desktop windows by selecting the appropriate options.

   g. In the **Local Resources** tab, configure the settings for the remote audio, keyboard and other peripheral devices, and then click **Next**.
   h. In the **Experience** tab, select the appropriate options for optimized performance, and then click **Next**.
   i. Use the **Password Management** tab to manage the domain password through AppPortal.
   j. In the **Desktop Integration** tab, configure the settings for Optiplex client shortcuts and file type associations, and then click **Next**.
   k. Use the **Auto-Launch** tab to configure the applications to start automatically.
   l. Click **Finish**.

   The New configuration with your preferred settings is added to the Configurations section in vWorkspace AppPortal window.
3. Click the new configuration of your choice.

   The **Logon Credentials** dialog box is displayed.
4. Enter the username, password, and domain to log in.

NOTE: You can use the **Quest vWorkspace Remote Desktop Connection** window to access your vWorkspace desktop and applications. To open this window, on the taskbar, click **Start** → **All Programs** → **Quest Software** → **vWorkspace Connector for Windows** → **Remote Desktop Connection**.

vWorkspace Options for Additional Configurations

Control Panel has the following vWorkspace options for additional configurations:

- vWorkspace Enhanced Audio
- vWorkspace Universal Printer Client

NOTE: For more information on using vWorkspace, see your software version's documentation.

Using the vWorkspace Enhanced Audio

Use the **vWorkspace Enhanced Audio** window to configure general vWorkspace audio input/output settings and log options for troubleshooting purposes.

To open the **vWorkspace Enhanced Audio** window, on the start menu, click **Control Panel** → **vWorkspace Enhanced Audio**.

vWorkspace Enhanced Audio enables you to redirect your audio devices to RD Session Hosts and hosted desktops to use with applications involving dictation and for certain VOIP applications. These settings are disabled by default.

Using the vWorkspace Universal Printer Client

Use the **vWorkspace Universal Printer Client** window to configure the following available options:

- vWorkspace printer options
- Bandwidwith control options
- Log options for troubleshooting purposes

The vWorkspace Universal Printer client properties apply to auto-created client printers, and not to printers assigned by the vWorkspace Management Console.

For example, the Auto-create network printers option creates a printer mapping for each network printer defined on the client device.

4

Notable Administrator Features

This chapter explains the features included in the Control Panel. To open **Control Panel**, click **Start Control Panel**.

The following administrator features include:

- Using Administrative Tools
- Using TPM and BitLocker
- CAD Tool
- Configuration Manager (SCCM)
- Dell Wyse RAMDisk
- Dell Wyse Winlog
- Connecting to a printer or an external device
- Dual Monitor Display
- Region and Languages
- Sounds and Audio Devices
- User Accounts
- Windows Defender

NOTE:

1. An administrator 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 optiplex clients and to persist after the device reboot.
2. Additional software features are available for the download. For more information, refer release notes of the latest build and contact Technical Support.

Important: **Intel Smart Connect Chipset** application is included in the build, as it is a part of on board BIOS component. However, this feature is not supported in this build.

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 Root** folder. 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 Optiplex client, use the **Services** window. To open Services window, go to **Start** Menu, **Control Panel Administrative Tool Services**.

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

   NOTE: Make sure the File Based 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 Optiplex client restart, to ensure that the Optiplex client configuration is saved disable the Unified Write Filter (UWF). Be sure to enable the UWF later. For more information, see Before Configuring your Optiplex Clients .

Tip:

You can use the **Winlog** dialog box, go to **Control Panel** → **Dell Wyse Winlog**) to disable Auto Log. You can easily log on as an administrator when you need to restart your Optiplex client. For more information, see Dell Wyse Winlog.

To use TPM and BitLocker:

1. Ensure that the TPM-supported client is running the latest WE8S build, that also supports TPM.
2. Log in as an Administrator.
   a. Enter the BIOS. On the BIOS configuration pane, click the **Security** tab and under TPM Support, enable TPM. For more information, see Accessing Optiplex Client BIOS Settings.

      The TPM Configuration pane appears.

   b. Select **TPM Configuration** and press **Enter**.
   c. Under Change TPM Status, press **Enter** and select **Enabled and Activate**.
   d. 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. Click the Services icon in the Component Services console to start the Services.msc, double-click **HAgent** in the Name list of the Services window of the Component Services console to open the **HAgent Properties** dialog box, set the Startup type to **Manual**, and then click the **Stop** button to stop the HAgent service.
5. On the Windows desktop, click **Start** → **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 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 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** → **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.
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. To use this click**Start** → **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.

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.

If TPM is not enabled, initialized and owned, then the following dialog box displays when BitLocker is turned on.

CAD Tool

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

The Mapped keys for different VDI applications supported by CAD Tool are shown here:

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

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.

Configuration Manager

To view and configure the Dell SCCM components installed on your Optiplex client, use the **Configuration Manager Properties**.

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

For more information, refer Dell SCCM Guide at http://www.dell.com/wyse/manuals

Dell Wyse RAMDisk

RAMDisk 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 RAMDisk:

- Browser Web page cache
- Browser history
- Browser cookies
- Browser cache
- Temporary Internet files
- Print spooling

- User/system temporary files

To configure the RAMDisk size, go to **Start** → **Control Panel** → **RAMDisk**. After the changes made in the size of the RAMDisk, restart the Optiplex 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 Optiplex client reboot. For more information, see Before Configuring Your Optiplex Clients.

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

Dell Wyse Winlog

By default, Automatic logon to a user desktop is enabled. Auto login changes can be made in the **Winlog Settings** window. To open **Winlog Settings** window, go to **Start** → **Control Panel** → **Dell Wyse Winlog**

The following changes can be made in the **Dell Wyse Winlog** window:

- To enable or disable Auto Logon
- To change the Default User Name
- To change the Default Password
- To change the Default Domain

Connecting to a Printer or an External Device

To connect a parallel printer to your Optiplex 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 Optiplex 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 Optiplex client. For more information, see Adding Devices.

Adding Printer

To add a printer to the Optiplex 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 Optiplex 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 Optiplex 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 Optiplex 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 Optiplex 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 Optiplex client only.

For more information, refer http://www.microsoft.com.

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

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

Setting the Region and Language

Use the **Region and Language** dialog box to select your keyboard language.

To open the **Region and Language** dialog box, on the **Start** menu, click **Control Panel**, and then click **Region and Language**.

Select your preferred keyboard language from the available language options.

Important: The default language is **English (United States)**.

Third-party applications, Dell applications, and Microsoft names remain in English.

Sounds and Audio Devices

Use the **Sound** dialog box to manage your audio devices.

To view the **Sound** dialog box, On the Start Menu, click **Control Panel** → **Sound**.

Use the following tabs to configure the sound settings:

- **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 to Managing Users and Groups with User Accounts.

Windows Defender

To scan your Optiplex client 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**.

5

Additional Administrator Utility and Settings Information

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

It discusses:

- Automatically Launched Utilities
- Utilities Affected by Log Off, Restart, and Shut Down
- Using the File Based Write Filter (FBWF)
- Understanding the NetXClean Utility
- Saving Files and Using Local Drives
- Mapping Network Drives
- Participating in Domains
- Using the WinPing Diagnostic Utility
- Using the Net and Tracert Utilities
- Managing Users and Groups with User Accounts
- Changing the Computer Name of an Optiplex client

Automatically Launched Utilities

The following utilities are automatically started:

- **File Based Write Filter** — Upon system start, the File Based Write Filter utility tray is automatically started. It provides a secure environment for Optiplex client computing by protecting the Optiplex client from undesired disk 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 started. NetXClean is a clean-up utility that keeps extraneous information from being stored on the local disk. If you want to keep certain profile configurations 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 Optiplex client logon, the Windows VNC Server utility is automatically started. VNC allows an Optiplex client desktop to be accessed remotely for administration and support. See Using TightVNC (Server and Viewer) to Shadow an Optiplex client..

Utilities Affected by Log Off, Restart, and Shut Down

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

- **File Based Write Filter cache** — If you make changes to system configuration settings and want them to persist after a reboot, you must flush the files of the File Based Write Filter cache during the current system session. Otherwise, the new settings will be lost when the Optiplex client is shut down or restarted. The File Based Write Filter cache contents are not lost when you simply log off and on again as the same or different user; that is, you can flush the files of the File Based Write Filter cache after the new logon and still retain the changes. For instructions on flushing, see Before Configuring Your Optiplex Clients. For detailed information about the File Based Write Filter, see Using the File Based Write Filter (FBWF)

  NOTE: A user cannot flush the files of the File Based Write Filter cache; this is a local or remote administrator function.

- **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, see Before Configuring Your Optiplex Clients and Understanding the NetXClean Utility.
- **Power Management** — A Monitor Saver turns off the video signal to the monitor, allowing the monitor to enter a power-saving mode after a designated idle time. Power settings are available in **Start** → **Control Panel** → **Power Options**.
- **Wake-on-LAN** — This standard Windows Embedded Standard feature discovers all optiplex clients in your LAN, and enables you to wake them up by clicking a button.
- NOTE: Wake on LAN feature will not work by default for laptop clients; you must enable the feature in the bios. In addition, for a laptop client, only S3 mode is supported the S5 mode is not supported.
- **Optiplex 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. The local time utility can be set to synchronize the optiplex client clock to a time server automatically at a designated time, or manually.

  NOTE:

  Correct time should be maintained as some applications require access to local optiplex 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 Optiplex client computing by protecting the client from undesired disk writes. By preventing excessive disk write activity, the File Based Write Filter also extends the life of the Optiplex client. It gives the appearance of read-write access to the disk by employing a cache to intercept all disk writes and returning success to the process that requested the I/O.

The intercepted disk writes stored in cache are available as long as the Optiplex client remains active but are lost when the Optiplex client is restarted or turned off. To preserve selected changes, the selected files of the cache can be transferred to the disk on demand by 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 disk 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 color indicates that the File Based Write Filter is enabled and red color 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 Optiplex client if the cache is more than eighty percent full. 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 Technical support for help.

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

- Running File Based Write Filter Command Line Options
- Enabling and Disabling the File Based Write Filter Using the Desktop Icons
- Setting the File Based Write Filter Controls

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 configure the File Based Write Filter Control settings:

1. Double-click the **Write Filter** icon on the notification area of the administrator taskbar.

The **Dell Wyse File Based Write Filter Control** dialog box is displayed.

2. Use the following guidelines to configure the File Based Write Filter Controls:

   a. FBWF Status section 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 (MB)**— Shows 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 section includes:

      - **Amount of RAM to be used for FBWF Cache (MB)**— Shows 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 section includes following options that allows you to improve the effectiveness of cache memory:

        – Cache Compression

        – Cache Preallocation

        – None

   c. FBWF Warning Settings section 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 Optiplex client. If you do not restart the Optiplex client, the changes made will not be saved until the Optiplex 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 Optiplex client. If you do not restart the Optiplex client, the changes made will not be saved until the Optiplex 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 all the FBWF Cache Settings, Advanced Cache Settings, and the FBWF Warning Settings to their default values.
g. File Commit section 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 Optiplex 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. This 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. If it 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 Optiplex client and the changes are not committed until an administrator restarts the Optiplex client manually.

Understanding the NetXClean Utility

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

NetXClean prevents unwanted or trash files from building up and filling the free space in the disk. The NetXClean utility is particularly important when multiple users have log-on rights to an Optiplex client, as disk 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

Saving Files and Using Local Drives

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

Saving Files

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

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

Drive Z

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

For RAMDisk configuration information, see Dell Wyse RAMDisk.

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

Drive C

Drive C is the on-board non-volatile flash memory. 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 under 3 MB, the Optiplex 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 Optiplex client image will be irreparably damaged and it will be necessary for you to contact an authorized service center to repair the Optiplex client.

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

- Favorites
- Created connections

- Delete/edit connections

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

Mapping Network Drives

Users and administrators can map network drives. However, to retain the mappings after the Optiplex 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 Optiplex client to a domain or by using roaming profiles.
Joining a Domain

1. Log in as an administrator.
2. On the **Start** menu, click **Control Panel** → **System.**

   The **System window** is displayed.
3. In the **Computer name**, **domain and workgroup settings** section, click **Change** Settings.

   The **System Properties** dialog box is displayed.
4. Click **Change** option to change the domain or workgroup.

   a. Click **Domain** option.

      The **Computer Name/Domain** Changes dialog box is displayed.

   b. Enter the domain of your choice.

   c. Click **OK**.
5. To join an Optiplex client to a domain, click **Network ID**.

   The **Join a Domain or Workgroup** wizard is displayed. On the first page of the wizard, select any of the following options that describes your network.

   - Business Network — Click this option if your optiplex client is a part of business network and you use it to connect to other clients at work.

1. Click **Next**.
2. Select the option according to your company’s network availability on a domain.

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

   – User Name

   – Password

   – Domain Name

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

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

- Home network — Click this option if your optiplex client is a home client and its not a part of a business network.

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.

Use the following guidelines:

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** to create and manage user accounts, create and manage groups, and configure advanced user profile properties.

To view the **User Accounts** window, click **Start** → **Control panel** → **User Accounts**.

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 example links provided throughout the wizards. Use 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 disk space constraints, the number of additional users on the Optiplex client should be kept to a minimum.

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

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 the box.
   b. If you want to create **Administrator account** , select the administrator check box, and then enter the name in the 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 Optiplex 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 an Optiplex Client

Administrators can change the computer name of an Optiplex 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 Optiplex client.
To change the computer name of an 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 Optiplex 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 Optiplex client environment.

It includes

- Restoring Default Settings
- Accessing Optiplex Client BIOS Settings
- Configuring and Using Peripherals
- Using TightVNC (Server and Viewer) to Shadow an Optiplex Client

Restoring Default Settings

Depending on the default settings you want to restore on the Optiplex client, you can use the BIOS to restore default values for all the items in the BIOS setup utility For more information, see Accessing Optiplex client BIOS Settings

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

Accessing Optiplex Client BIOS Settings

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

1. During the start-up, press the **F2** key.
   The **BIOS** Settings dialog box is displayed.
2. Change the BIOS Settings as required.

Configuring and Using Peripherals

The Optiplex client has only the **USB port** available on it.

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

TightVNC (Server and Viewer)

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

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

TightVNC Server starts automatically as a service upon Optiplex 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 Menu Toolbar** → **Programs** → **TightVNC** → **TightVNC Server (Service Mode)**

NOTE:

- TightVNC Viewer is available from TightVNC website.
- 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.

TightVNC (Server and Viewer) — Pre-requisites

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

- IP address or valid DNS name of the Optiplex client to be shadow, operate or monitor. For more information, see Viewing Client Information.
- Primary password of the Optiplex client to shadow, operate or monitor. For more information, see Configuring TightVNC Server Properties on the Optiplex Client.

NOTE:

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

Using TightVNC to Shadow an Optiplex Client

TightVNC Server starts automatically as a service upon 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 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 optiplex 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 client that is shadowed, and then click **OK**.

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

The Optiplex 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 just as you would if you were operating it locally.

Configuring TightVNC Server Properties on the Optiplex Client

To Configure the TightVNC Server Properties on the Optiplex 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**. Use this password while shadowing the Optiplex client.

   Default Primary 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 Optiplex Client.

A

Using Dynamic Host Configuration Protocol (DHCP)

This appendix contains the DHCP options you can use with your Optiplex client. A Optiplex client is initially configured to obtain its IP address and network configurations from a DHCP server, new Optiplex client or a Optiplex 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 Optiplex client is recommended and saves you the time and effort needed to complete these processes locally on multiple Optiplex 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 Optiplex 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 Optiplex client.

57	Maximum DHCP Message Size.	Optional. Always sent by Optiplex 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 ptiplex 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.
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.