Windows 10 IoT Enterprise LTSC 2021

Administrator's Guide

September 2023
Rev. A01

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.

Contents

1

Introduction

OptiPlex thin clients that run the Windows 10 IoT Enterprise LTSC 2021 operating system provide access to applications, files, and network resources. The applications and files are made available on machines hosting Remote Desktop Connection and VMware Horizon Client session.

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

To activate your Windows 10 operating system offline by using **Activate by Phone** option, see Activating Windows 10 Offline.

NOTE:

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

Technical support

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

About this guide

This guide is intended for thin client administrators running Windows 10 IoT Enterprise LTSC 2021. It provides information and detailed system configurations to help you design and manage a Windows 10 IoT Enterprise environment.

Supported thin clients

The following are the list of thin clients that run the Windows 10 IoT Enterprise LTSC 2021 operating system:

- OptiPlex All-in-One 7410
- Latitude 3440
- Latitude 5440
- OptiPlex Micro Plus 7010

2

Getting started

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

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

NOTE: You can also use Microsoft Endpoint Configuration Manager and VMware Workspace One to manage your thin clients.

Automatic and manual login

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

For more information, see Managing Users and Groups with user accounts.

NOTE:

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

When you start the thin client, you are logged in to the user desktop by default.

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

- **Administrators**—The default username is **`Admin`** and the default case-sensitive password is **`Admin#<Service tag of the device>`**.
- **Users**—The default username is **`User`** and default case-sensitive password is **`User#<Service tag of the device>`**.
- **Customized User**—Log in to your thin client by entering the user credentials which you have set for the customized user account.

NOTE: For information about how to find the service tag of the device, see *Find the Service Tag of Your Dell Thin Client* at https://www.dell.com/support.

Before configuring your thin clients

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

Grouping Applications into Desktops

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

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

Connecting to a printer or an external device

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

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

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

Connecting to a monitor

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

- HDMI port
- DisplayPort
- Type-C port

For more information about configuring multiple monitor display, see Configuring multi-monitor display.

3

Accessible applications

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

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

Using VMware Horizon Client to connect to virtual desktop

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

About this task

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

Steps

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

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

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

      The VMware Horizon Client connects to the selected desktop. After connection is established, the list of published desktops is displayed.
   f. Right-click the particular application or the desktop icon, and then click **Launch** to connect to that application or desktop.

   For more information, see VMware Horizon Client.

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

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

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

Citrix Workspace App

Citrix Workspace app is preinstalled on your thin clients. You can also install Citrix Workspace app on the thin client to access your applications and desktops using Citrix Virtual Apps and Desktops from a remote client device. Citrix Workspace app provides access from your desktop, Start menu, Citrix Workspace user interface, and web browsers. You can use Citrix Workspace app on domain and non-domain joined thin clients.

Citrix Workspace is a cloud-based enterprise app store that provides secure and unified access to apps, desktops, and content (resources) from anywhere on any device. These resources can be Citrix DaaS, content apps, local and mobile apps, SaaS and Web apps, and browser apps. For more information, see Citrix Workspace App.

StoreFront is an on-premises enterprise app store that aggregates applications and desktops from Citrix Virtual Apps and Desktops sites into a single easy-to-use store for users. For more information, see StoreFront documentation.

Adding store URL to Citrix Workspace App

Provide users with the account information that they require to access virtual desktops and applications using the following:

- Providing users with account information to enter manually
- Configuring email-based account discovery
- Adding store through Command Line Interface
- Provisioning file
- Using the Group Policy Object administrative template

For more information, see Citrix Workspace App for Windows.

Provide users with account information to enter manually

Upon successful installation of Citrix Workspace app, you are required to enter an email or server address to access the apps and desktops. When you enter the details for a new account, Citrix Workspace app verifies the connection. On successful verification, Citrix Workspace app prompts you to log in to the account.

To set up accounts manually, be sure to distribute the information that is required to connect to the virtual desktops and applications.

- To connect to a Workspace store, provide the Workspace URL.
- To connect to a StoreFront store, provide the URL for that server. For example, https://servername.company.com.
- To connect through Citrix Gateway, first determine whether a user must see all configured stores or only the store with remote access enabled for a particular Citrix Gateway.
  - To present all configured stores, provide users with the Citrix Gateway fully qualified domain name.
  - To limit access to a particular store, provide users with the Citrix Gateway fully qualified domain name and the store name in the form- CitrixGatewayFQDN?MyStoreName:

For example, if a store named SalesApps has remote access enabled for server1.com and a store named HRApps has remote access enabled for server2.com, the user must enter as follows-

- server1.com?SalesApps to access SalesApps or
- server2.com?HRApps to access HRApps. CitrixGatewayFQDN?MyStoreName feature requires a new user to create an account by entering a URL and is not available for email-based discovery.

For more information, see Citrix workspace documentation.

Configuring remote desktop connection session services

Prerequisites

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

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

About this task

To configure a remote desktop connection:

Steps

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

Azure Virtual Desktop

A virtual desktop allows users to access their desktop and applications from anywhere on any kind of endpoint device, while IT organizations can deploy and manage these desktops from a centrally located data center.

To launch the client after installation, use the **Start** menu and search for **Remote Desktop**.

About Azure Virtual Desktop

- Azure Virtual Desktop (classic)—Azure Virtual Desktop (classic) environment
- Azure Virtual Desktop—What is Azure Virtual Desktop?

Use a user account

Steps

1. Select Subscribe from the main page.
2. Sign in with your user account when prompted.

Results

The resources that are grouped by workspace appear in the **Connection Center**.

NOTE: The Windows client automatically defaults to Azure Virtual Desktop (classic). However, if the client detects additional Azure Resource Manager resources, it adds them automatically or notifies the user that they are available.

Use a specific URL

Steps

1. Select **Subscribe with URL** from the main page.
2. In the **Email or Workspace URL** field:
   - For Workspace URL, use the URL provided by your admin.
   - For email, use your email address.

     The client finds the URL associated with your email, provided your admin has enabled email discovery.
3. Select **Next**.
4. Sign in with your user account when prompted.
   The resources that are grouped by workspace appear in the **Connection Center**. For more information, see Azure virtual desktop documentation.

Amazon WorkSpaces

Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users, known as WorkSpaces. WorkSpaces eliminates the need to procure and deploy hardware or install complex software. You can quickly add or remove users as your needs change. Users can access their virtual desktops from multiple devices or web browsers. For more information, see Amazon WorkSpaces.

Connect to Workspace

About this task

To connect to Workspace, complete the following procedure:

Steps

1. The first time that you run the client application, you are prompted for your registration code, which is contained in your welcome email. The WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. To enter a different registration code, launch the client application, and then choose **Change Registration Code** at the bottom of the login page.
2. Enter your username and password in the login screen and choose **Sign In**. If your WorkSpaces administrator has enabled multifactor authentication for your organization's WorkSpaces, you are prompted for a passcode to complete your login. Your WorkSpaces administrator provides more information about how to obtain your passcode.

3. If your WorkSpaces administrator has not disabled the Keep me logged in feature, you can select the **Keep me logged in** check box at the bottom of the login screen to save your credentials securely so that you can connect to your WorkSpace while the client application remains running. Your credentials are securely cached up to the maximum lifetime of your Kerberos ticket.
   After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

Manage your Login Information (5.0+ clients only)

About this task

You can view your registration code and what Region your Workspace is in. You can specify whether you want the WorkSpaces client application to save your current registration code, and you can assign a name to your Workspace. You can also specify if you want Amazon WorkSpaces to keep you logged in to a Workspace until you quit or your login period expires. To manage your login information for a Workspace, do the following:

Steps

1. In the WorkSpaces client application, go to `Settings > Manage Login Information`.
2. In the **Manage Login Information** dialog box, you can see the registration code and Region information for your WorkSpace.
3. If you want the WorkSpaces client to remember your current registration code, select the **Remember Registration Code** check box. This step is optional.
4. Under **Saved registration codes**, select the WorkSpace that you want to name.
5. In the **WorkSpace name** box, enter a name for the WorkSpace.
6. If you want WorkSpaces to keep you logged in until you quit or your login period expires, select the **Keep me logged in** check box. This step is optional.
7. Choose **Save**.
   For more information, see Amazon Workspace documentation

Zoom Meetings optimization for VDI

A VDI server is a shared hardware resource for multiple users at one time. VDI hardware which can support multiple virtual desktops generally cannot sustain the processing demands of video conferencing on top of its other processing requirements.

The Zoom VDI Client and plug-in addresses this issue by removing most media-processing demands from the VDI server, and instead redirecting them to the plug-in, which processes the media using its own hardware resources on the local machine. Zoom creates an optimized experience by sending independent data streams to both the VDI Client and plug-in, allowing each component to focus on the responsibilities it does best.

Prerequisites for Zoom Meetings optimization

Organizations using Citrix XenDesktop or VMware Horizon server published desktop, or Windows Remote Desktop Citrix Workspace, VMware Horizons, AVD client, or Windows remote desktop client

NOTE: Citrix Workspace app from Microsoft store is not supported.

In the optimized experience, the VDI Client primarily focuses on rendering an empty placeholder of the Zoom meeting, containing only a blank screen of the meeting content and the meeting toolbar buttons. The VDI Client also maintains in-meeting data, like the participant list, through its direct connection to the Zoom meeting, and processes any screen sharing of the local user's desktop.

Direct Optimization

Similarly, in the Direct Optimization experience, the plug-in assists the VDI Client by performing the other half of the VDI Client's work. The plug-in also has a direct connection with the Zoom meeting to receive the meeting video, audio, and content, which is and then layered on top of the VDI Client's meeting content placeholder image.

The VDI Client and plug-in create a synchronized experience together by rendering the Zoom meeting in layers, superimposing the plug-in's media on top of the VDI Client's Zoom placeholder. The plug-in and VDI Client coordinate efforts, using the VDI software provider's existing virtual channel.

The Zoom Cloud maintains two separate data streams to both the VDI desktop and the plug-in. In a Direct Optimized mode, the following occurs.

- The plug-in receives data streams for video, audio, and inbound content directly from the cloud.
- The VDI desktop receives and displays general meeting data—like the participant information—in the Zoom Client placeholder while also uploading any local screen-sharing content.
- The plug-in and VDI desktop communicate with each other using the VDI vendor's virtual connection, signaling where to place and render the on-screen media between the two layers.

For information about troubleshooting your Zoom Meetings optimization for VDI, see the Deployment and Installation Guide.

Cisco Jabber Softphone for VDI Solutions

Cisco Jabber Softphone for VDI (JVDI) is the Unified Communications solution offered by Cisco for virtual deployments. It supports audio conferencing and instant messaging on the Hosted Virtual Desktops (HVD). The Cisco Jabber Softphone for VDI software offloads the audio processing from the virtual desktop servers to the thin client. All audio and video signals are routed directly between the endpoints without entering the HVD environment.

Cisco Jabber Softphone for VDI enables you to make and receive calls using the Cisco Unified Communications application. Cisco Jabber Softphone for VDI consists of the following two components:

- Cisco JVDI Agent
- Cisco JVDI Client

Cisco JVDI Agent is the JVDI connector that runs on the Citrix desktop or server. Cisco JVDI client is the JVDI package that runs on the thin client. The Jabber client that runs on the Citrix server handles the authentication, and the media processing is achieved on the thin client.

Setting up the Cisco Jabber Softphone for VDI Solutions

About this task

This section describes how to install and use the Cisco Jabber Softphone for VDI solutions.

Steps

1. Cisco Jabber Softphone for VDI solutions is part of Dell application store.
   To download latest Cisco Jabber VDI software, go to Cisco Jabber VDI download.
2. On the Virtual desktop, install Cisco JVDI Agent. Double-click the file and follow the installation wizard steps.
3. On the Virtual desktop, install Cisco Jabber.
   For information about the installation procedure, see the installation guide.
4. Install the `JVDI.pkg` on the thin client using Wyse Management Suite.
5. Log in to the virtual desktop, and sign in to Cisco Jabber using your user credentials.
   When you log in for the first time, do the following:
   a. On the Cisco Jabber interface, click **Advanced Settings**.
   b. Select your account type as **Cisco Communications Manager 9 or later**.
   c. Enter the login server address.

   NOTE: If the **Use my computer for calls** option is selected, Cisco Jabber is automatically registered with Cisco Unified Communications Manager. This option enables Jabber to work as a Softphone, and use the microphone or speaker that is connected to the thin client for phone calls.

Using Cisco Jabber

Use the Cisco Jabber application to perform the following tasks:

- Start an audio call.
- Answer the call.
- Hold or resume the call.
- Stop the video.
- Mute or unmute the audio.
- Turn on or turn off the self-view.
- Enter or exit the full screen.
- Merge the calls.
- Audio conferencing.
- Transfer the call.
- Play voice mail.
- Forward the call to voicemail.
- Forward the call to another number.
- Forward voice messages directly.
- Use the Device Selector menu to switch between headsets.
- Use the Device Selector menu to switch between cameras.
- Set up secure phone capabilities.
- Answer the call on multiple phone devices (Shared Line feature).

For information about troubleshooting your Cisco Jabber, see the Deployment and Installation Guide for Cisco Jabber Softphone for VDI.

Cisco Webex App for VDI

The Webex App VDI solution optimizes the audio and video for calls and meetings. The users can access Webex App from a remote virtual desktop (Citrix or VMware) environment using a thin client, such as a lightweight personal computer or laptop. For calls, the media goes directly between users and avoids traversing the data center. For meetings, media goes between the Webex cloud and the user's thin clients without another client in the middle. Without optimization, Webex App messaging works as-is in a Virtual Desktop Infrastructure (VDI) environment. The full Webex App experience also includes calling and meetings, which requires video and audio media processing.

Due to a limitation known as the hairpin effect, calling, meeting, and accompanying video capability are not supported without optimization. The additional bandwidth that is required for calls and video creates a bottleneck at the data center because the media flows from one user to the data center back to another user. As a result of this unoptimized media path and the lack of access to peripherals such as device speakers, microphone, and camera, the user experience is not ideal.

To fix the issue of the hairpin effect, the Webex App VDI plug-in extends the Cisco collaboration experience to virtual deployments so that users can use the full messaging, meeting, and calling functionality that the Webex App provides.

To reduce latency and to enhance media quality, the VDI plug-in optimizes the media workflows by streaming media directly between users on thin client endpoints, and leverages the hardware of the thin client machines to handle media processing. This media path does not go through the hosted virtual desktops (HVDs). The result is a stable and full-featured calling and meeting experience for your VDI users.

In this architecture, the Webex App is installed on the HVD in your VDI environment and required VDI plugins are installed on the user's thin client (typically a lightweight system, like a repurposed laptop or desktop).

Windows-based thin client, users access the Webex App on the HVD from a remote virtual desktop environment. With supported versions of Webex App, users can use all the integrated messaging, meetings, and calling on Webex App functionality on their thin client. Also, you can integrate Webex App VDI with a Unified CM or Webex Calling environment, so that users can use supported call features. You can also deploy the full featured meetings experience by installing the Webex App Meetings VDI plug-in.

For information about troubleshooting your Cisco Webex App for VDI, see the Deployment and Installation Guide.

Wyse Easy Setup

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

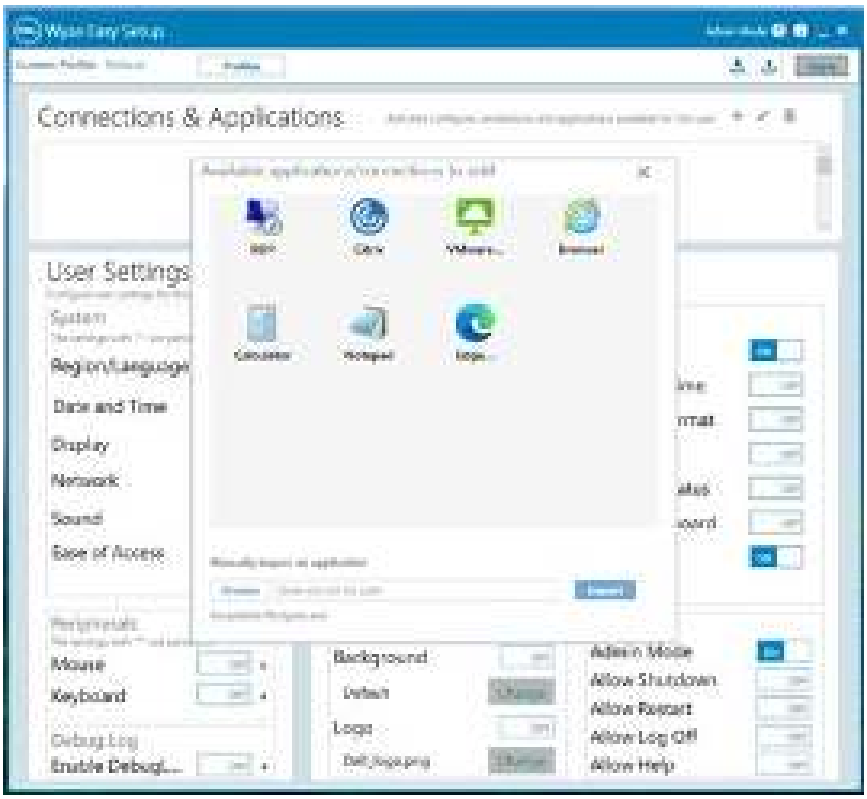
Wyse Easy Setup enables you to:

- Create a dedicated browser-focused client by configuring the Internet Explorer and Chromium Edge settings.

- Configure multiple broker connections such as Citrix, VMware, Azure Virtual Desktop (AVD), and Remote Desktop Protocol (RDP).
- Configure a device to create a dedicated application for a particular line of business.

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

Admin Mode - Import locally available Application



About this task

To add a locally available application, follow the steps that are given below:

Steps

1. Click **Browse** and provide the location of the binary of the application.
2. Then select **Import**.
3. The application is now added in the available application/connection list.

Admin Mode - Configure Control Panel Items

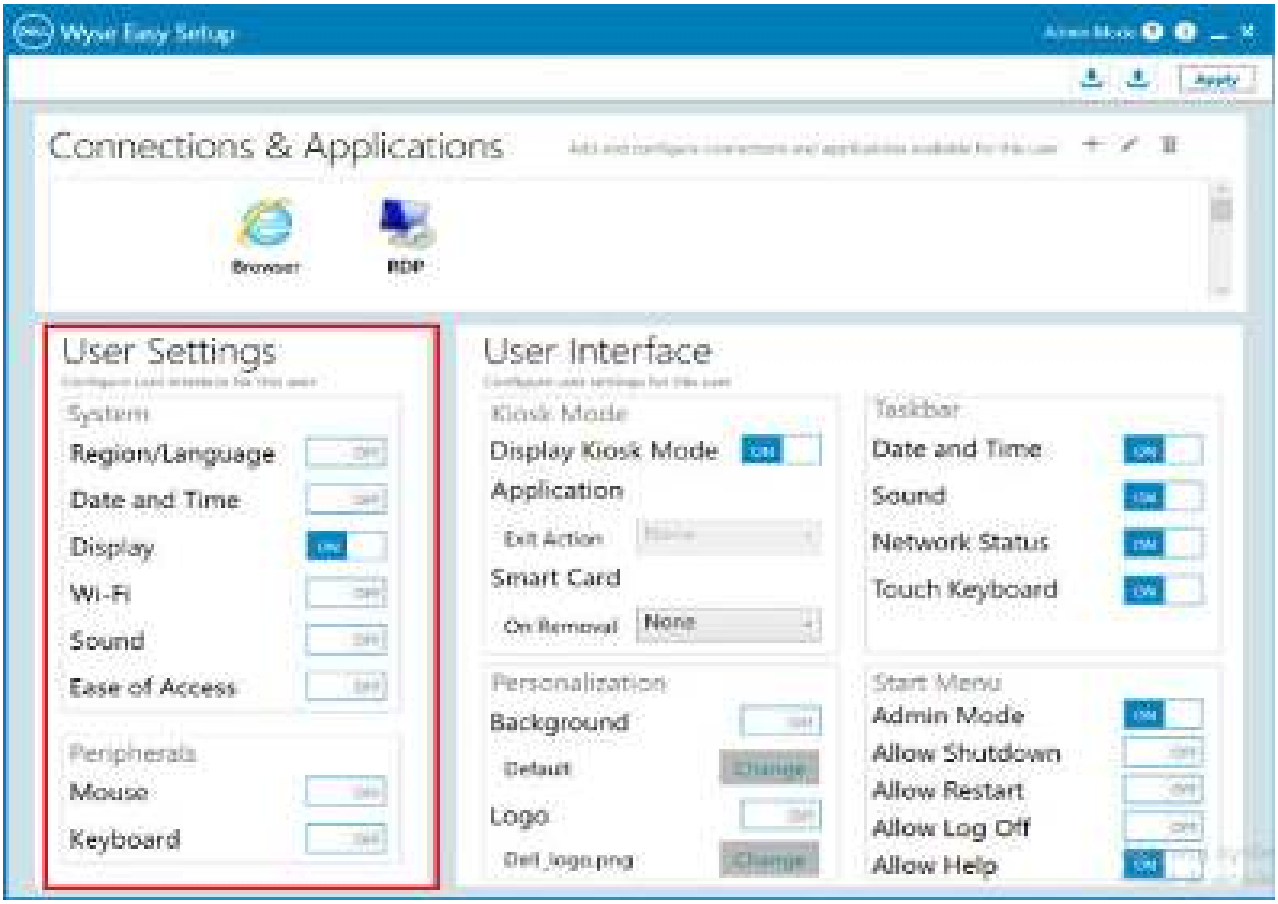


Figure 1. Admin Mode

- This feature enables the user to configure control panel items.
- These settings are applied to both **Windowed Mode** and **KIOSK mode**.
- If these settings are configured and applied, only the selected control panel item settings are displayed inside the control panel.
- The user's control panel is empty, If none of the settings are applied.

Admin Mode - Import/Export

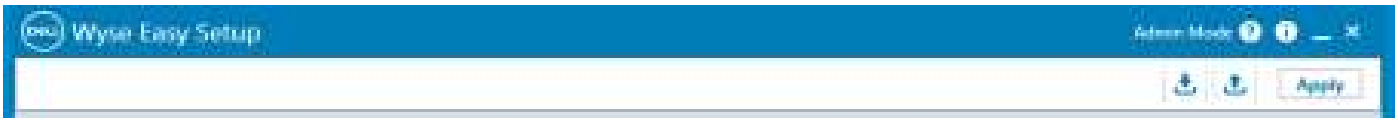


Figure 2. Admin Mode - Import/Export

Import: This mode can be used to import local configurations (JSON file) which can then be applied to the current machine by clicking **Apply**. The user must select source folder and the file that is to be taken as input.

Export: This mode can be used to export current machine configurations to an external JSON file. The user can select the destination folder and filename for the output file.

User Mode - Main UI shell

Figure 3. User Mode - Main UI shell

Configuring Wyse Easy Setup Settings - with Wyse Management Suite

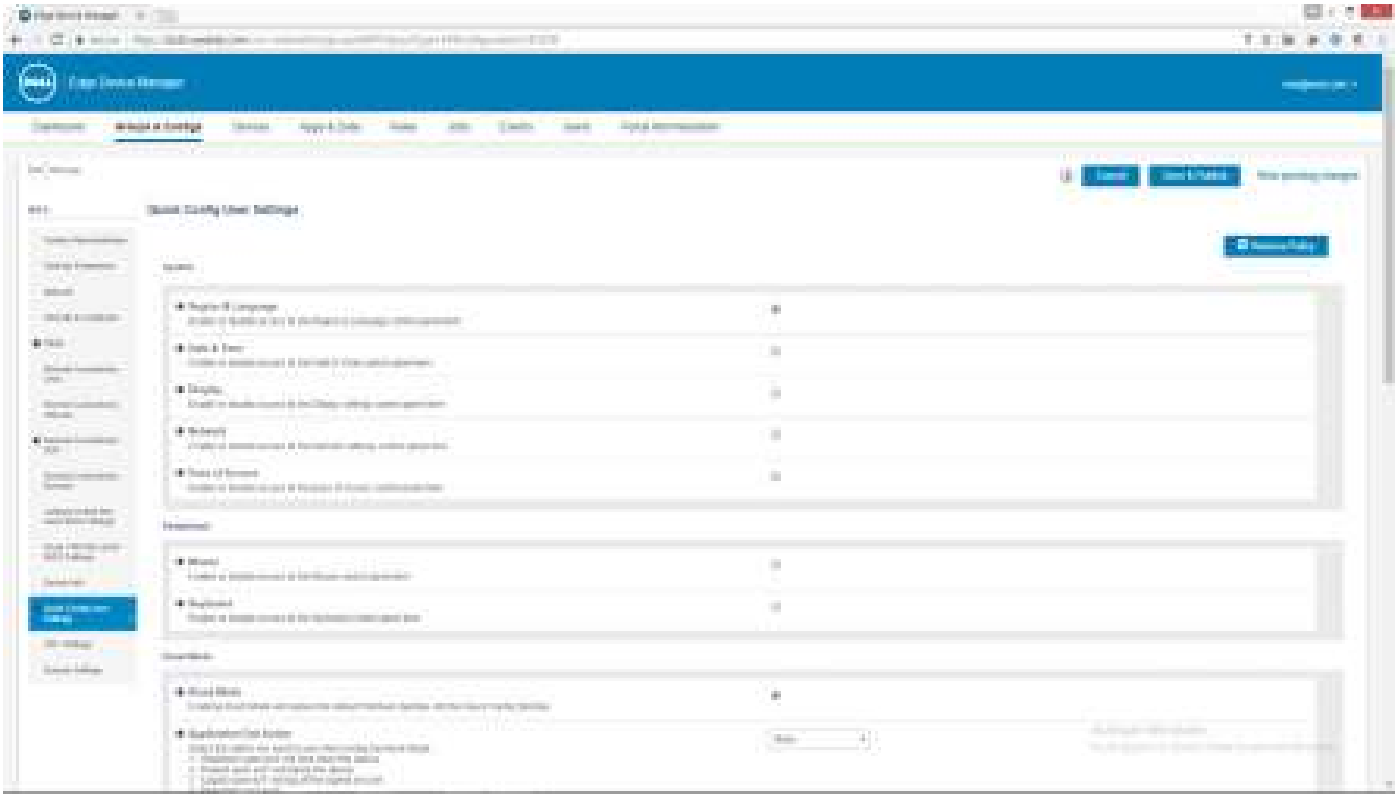


Figure 4. Configuring Wyse Easy Setup Settings - with Wyse Management Suite

All the settings that are made through Admin mode of Wyse Easy Setup can be done through Wyse Management Suite - Edge Device Manager.

Overlay Optimizer

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

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

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

4

Administrative features

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

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

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

Using Administrative tools

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

Configuring component services

To access and configure the component services, event viewer, and local services use the **Component Services** console. For more information, see Administrative Tools in Windows 10.

Formatting existing partition

To format a partition or volume on a hard disk, the Unified Write Filter must be disabled and you must be log in as an administrator. For information about formatting an existing partition, see *Create and format a hard disk partition* at https://support.microsoft.com/.

Viewing events

To view monitoring and troubleshooting messages from Windows and other programs, use the Event Viewer window. In the Component Services console, click the **Event Viewer** icon from the **Console Root** tree. The summary of all the logs of the events that have occurred on your computer is displayed. For more information, see Event Viewer.

NOTE: Event logs are lost on reboot because of Write Filter.

Managing services

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

Steps

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

   For more information, see Component Services Administration.

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

Configuring wireless local area network settings

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

Using custom fields

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

About this task

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

Steps

1. Log in as an administrator.
2. Go to **Start** > **Dell Thin Client Application**.
   The **Dell Thin Client Application** window is displayed.
3. On the left navigation bar, click **Custom Fields**.
4. Enter the custom field information in the custom field boxes, and click **Apply**.
   The custom field information is transferred to the Windows registry which is then available to the WMS server.

   CAUTION: To permanently save the information, ensure that you disable/enable the Unified Write Filter (UWF). For more information, see Before configuring your thin client.

   NOTE: After installing the latest e-support image, **Dell Thin Client Application** will be removed. Instead use **Dell Application Control Center** for any Dell Thin Client application functionalities.

Enabling auto logon

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

About this task

To enable/disable auto logon:

Steps

1. Log in as an administrator.
2. Go to **Start** > **Dell Thin Client Application**.
   The **Dell Thin Client Application** window is displayed.
3. On the left navigation bar, click **Auto Logon**.
4. To start with the admin logon page, enter `Admin` in the **Default User Name** field.

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

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

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

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

Viewing and configuring Microsoft Endpoint Configuration Manager components

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

About this task

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

Steps

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

Next steps

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

Microsoft Endpoint Configuration Manager

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

For more information, see Managing Windows-based Dell Wyse and OptiPlex Thin Clients using Microsoft Endpoint Configuration Manager

Devices and printers

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

Prerequisites

CAUTION: To refrain from cleaning up your settings, disable/enable the Unified Write Filter (UWF) and configure Application Launch Manager and xData Cleanup Manager.

About this task

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

Steps

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

Adding printers

About this task

To add a printer to the thin client:

Steps

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

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

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

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

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

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

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

Adding devices

About this task

To add a device to the thin client:

Steps

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

Configuring multi-monitor display

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

About this task

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

Steps

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

   For information about setting up multiple monitors, see How to Set up Multiple Monitors in Windows 10.

Managing audio and audio devices

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

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

Using sound dialog box

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

About this task

To open the **Sound** dialog box:

Steps

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

   The **Sound** dialog box is displayed.

2. Use the following tabs, and configure the sound related settings:
   - **Playback**—Select a playback device and modify the settings.
   - **Recording**—Select a recording device and modify the settings.
   - **Sounds**—Select an existing or modified sound theme for events in Windows or programs.
   - **Communications**—Click an option to adjust the volume of different sounds when you are using your thin client to place or receive telephone calls.
3. Click **Apply**, and click **OK**.

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

Additional language support

You can add additional languages to your Windows 10 IoT Enterprise operating system.

Steps

1. Log in as an administrator.
2. Disable Unified Write Filter.
3. Enable **Windows Update** by deleting the `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU` registry.
4. Restart the thin client.
5. Log in as an administrator.
6. Go to **Start** > **Settings** > **Time & Language** > **Region & Language** > **Add Language**.
7. Select the available language pack and click **Install**.
   The language pack is displayed in the **Region & Language** window.
8. Select the language pack and click **Options**.
9. Click **Download** and install the language packs.
10. Go to `C:\Windows\Setup\Tools`.
11. Right-click `LanguageConfig.exe` and click **Run as Administrator**.
12. Select the language and click **Apply**.
13. Restart the device.
    The device is ready for Golden Image support.

Setting region

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

About this task

To select your regional formats, do the following:

Steps

1. Log in as an administrator.
2. Go to **Start** > **Control Panel** > **Region**.
   The **Region** dialog box is displayed.
3. In the **Formats** tab, select the language, date, and time.
   To customize the formats, do the following:
   a. Click **Additional Settings**.
      The **Customize Format** window is displayed.
   b. Customize the settings, and click **OK**.
4. Click **Apply**, and then click **OK**.
5. In the **Location** tab, select a particular location to display additional information such as news and weather.
6. In the **Administrative** tab, change the language to be displayed in programs that do not support Unicode, and copy the settings.

Managing user accounts

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

About this task

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

Steps

1. Log in as an administrator.
2. Go to **Start** > **Control Panel** > **User Accounts**.
   For more information about using the **User Accounts** window, see Managing user and groups with user accounts.

Using Windows Defender

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

About this task

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

Steps

1. Log in as an administrator.
2. Go to **Start** > **Control Panel** > **Windows Defender**.
   The **Windows Defender** window is displayed. In the **Home** tab, select a scan option, and click **Scan Now**.

Example

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

Next steps

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

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

NOTE: For more details on using the task scheduler for alternate timing, refer the support page.

Windows Defender Advanced Threat Protection

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

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

C-A-D tool

The C-A-D tool enables administrators to map the Ctrl+Alt+Del key combination of VDI applications to display the Ctrl+Alt+Del screen of the VDI application. If the C-A-D tool is enabled, you can use Ctrl+Alt+Del key combination for all VDI applications. Also, you can use Win+L and Ctrl+Alt+Delete key function in the remote session such as Remote Desktop, Citrix, and VMware sessions.

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

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

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

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

Wyse Device Agent

Wyse Device Agent (WDA) is a unified agent for all thin client management solutions. Installing WDA on a thin client makes it manageable by Dell Wyse Management Suite (WMS).

Viewing and exporting operating system image manifest files

About this task

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

Table 1. Manifest files

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

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

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

Viewing and exporting operating system image current manifest information

Steps

1. Log in as an administrator.
2. Go to **Start** > **Control Panel** > **Dell Wyse Software Manifest Utilty**.
3. Click **Export Support Data**.
   The data is exported to the default path `C:/Users/Public/Public Documents/Wyse`.
   NOTE:
   You can also export the data to a custom folder by selecting **Custom Path** and browsing to the required folder.
4. Click **SupportData folder** to view the apps, drivers, and QFE folders that were exported.
   Each folder will contain an XML file with the requested data.

Viewing operating system image factory manifest information

Steps

1. Log in as an administrator.
2. Go to `C:\Windows\Setup\Tools`.
   The `BuildContent` folder contains the factory manifest of the thin client.
3. View the information of the operating system image manifest.
   - To view the information of the installed products in the factory at the time of shipment, go to **Apps** > **InstalledProducts xml file**.
   - To view the information of the QFEs installed in the factory at the time of shipment, go to **Qfe** > **QFE xml file**.

- To view the information of the currently installed drivers manifest information, go to **Drivers** > **Drivers xml file**.

Example

NOTE:

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

5

Additional administrator utility and settings information

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

Automatically launched utilities

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

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

  NOTE: While the Dell Wyse Write Filter icons and functionality are currently supported, it is recommended that you use the UWF as described in the Microsoft documentation available at navigate to the Unified Write Filter documentation.
- **Application Launch Manager**— The Application Launch Manager (ALM) version 1.0 enables you to start any application based on pre-defined events such as service startup, user log off or system shutdown in session zero. The application also allows you to configure multi-level logs which is essential for easy troubleshooting.
- **xData Cleanup Manager**— xData Cleanup Manager (xDCM) version 1.0 keeps extraneous information from being stored on the local disk. xDCM can be used to automatically clean-up directories used for temporary caching of information. Clean-up is triggered on either service startup, user logoff, or system shutdown. It does the clean-up invisibly to the user and is completely configurable.
- **VNC Server**—After you log in to your thin client, the Windows VNC Server utility starts automatically. VNC allows a thin client desktop to be accessed remotely for administration and support. For more information, see Using Tight VNC to Shadow a thin client.

Utilities affected by log off, restart, and shut down

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

- **Unified Write Filter**—After you turn on the system, the Unified Write Filter utility starts automatically. It is recommended that you use the UWF as described in the Microsoft documentation. For more information, see the support page and navigate to the Unified Write Filter documentation.
- **Application Launch Manager**— The Application Launch Manager (ALM) version 1.0 enables you to start any application based on pre-defined events such as service startup, user log off or system shutdown in session zero. The application also allows you to configure multi-level logs which is essential for easy troubleshooting.
- **xData Cleanup Manager**— xData Cleanup Manager (xDCM) version 1.0 keeps extraneous information from being stored on the local disk. xDCM can be used to automatically clean-up directories used for temporary caching of information. Clean-up is triggered on either service startup, user logoff, or system shutdown. It does the clean-up invisibly to the user and is completely configurable.
- **Power Management**—A Monitor Saver turns off the video signal to the monitor, allowing the monitor to enter a power-saving mode after a designated idle time. To access the power settings, go to **Start** > **Control Panel** > **Power Options**.
- **Wake-on-LAN**—This feature discovers all thin clients connected to your LAN, and enables you to wake them by clicking a button. For example, to perform image updates and remote administration functions on devices that have been shut down or are on standby. To use this feature, the thin client power must be turned on.

Unified Write Filter

About this task

Unified Write Filter (UWF) is a sector-based write filter that protects your storage media. UWF redirects the write attempts to a virtual overlay, and intercepts the write attempts to the protected volume. This improves the stability, reliability of the device

thereby reducing the wear on write media, such as solid-state drives. In UWF, overlay is a virtual storage space that saves changes made on the protected volume. If the file system attempts to modify a protected sector, UWF will copy the sector from the protected volume to the overlay, and the overlay is updated. If an application tries to read from that sector, UWF returns the data from the overlay, so that the system appears to have written to the volume, while the volume remains unchanged. For more information, see the Unified Write Filter documentation.

CAUTION: Failure to keep the Write Filter turned on (except for regular maintenance or Application/Driver installs or upgrades) will prematurely wear out your Flash/SSD storage and invalidate your warranty.

Next steps

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

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

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

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

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

Using Unified Write Filter

About this task

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

Steps

1. Log in as an administrator.
   If automatic login to a user desktop is enabled, log off from the user desktop and log in as an administrator.
2. To disable the Unified Write Filter, double-click the **Dell Wyse WF Disable** icon on the desktop.
   This icon disables the filter and reboots the system.

3. Configure the thin client device as per your requirements.
4. After you configure the thin client device, to enable the Unified Write Filter, double-click the **Dell Wyse WF Enable** icon on the desktop.
   This icon enables the filter and reboots the system. Your configurations on the thin client device are now saved, and they persist after you reboot the thin client.

Next steps

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

You can add specific files or folders on a protected volume to a file exclusion list to exclude those files and folders from being filtered by UWF. When a file or folder is in the exclusion list for a volume, all writes to that file or folder bypass UWF filtering, and are written directly to the protected volume and persist after the device restarts.

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

Running Unified Write Filter command–line options

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

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

Table 2. Running Unified Write Filter command–line options

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

Table 2. Running Unified Write Filter command–line options (continued)

Command-line options	Description
`uwfmgr overlay get-config`	This command-line displays configuration settings for the Unified Write Filter overlay. Displays information for both the current and the next session.
`uwfmgr registry /?`	This command-line displays configuration settings for exclusions of registry keys.

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

CAUTION:

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

Enabling and disabling the Write Filter using the desktop icons

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

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

Setting Write Filter controls

To view and manage UWF control settings, use the **Unified Write Filter Control** dialog box. To open the dialog box:

1. Log in to the admin profile.
2. Disable the **Unified Write Filter Control**.
3. Launch the DACC by **run as administrator**.

   DACC window is displayed.

4. Click **Write Filter Manager**.
5. **Write Filter Dashboard** and **Commits & Exclusion** options are be listed under **Write Filter Manager**.

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

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

- **Write Filter Dashboard**
- **Write Filter Status** —Shows the status of the **Unified Write Filter**. The status may either be Enabled or Disabled.
- **Enable UWF**—Allows you to enable the **Unified Write Filter** and prompts you to restart the thin client device. To save the changes, restart the thin client. After the system restarts to enable the Unified Write Filter, the Unified Write Filter status icon in the desktop notification area turns green.
- **Disable UWF**—Allows you to disable the **Unified Write Filter** and prompts you to restart the thin client device. To save the changes, restart the thin client. After disabling the Unified Write Filter, the **Unified Write Filter** status icon in the desktop notification area turns red, and the **Unified Write Filter** remains disabled after the system restarts.
- **Amount of RAM used for UWF Cache**— Shows the amount of RAM allocated to the Unified Write Filter cache for the current session in Megabytes (MB).
- **Write Filter Settings**

- Amount of RAM to be used for UWF Cache -Shows the amount of RAM that is to be used as the Unified Write Filter cache for the next session in MB. This value must be in the range of 256 MB to 2048 MB. There is an extra check to ensure that this value does not exceed 50% of the Total Available RAM.

- **Write Filter Threshold Settings**
  - Warning Threshold (%)-Shows the UWF cache percentage value at which a Low Memory warning message is displayed to the user for the current session. Shows the UWF cache percentage value at which a Low Memory warning message is displayed to the user. The default value is 80, minimum value is 50, maximum value is 80.
  - Critical Threshold (%)-Shows the UWF cache percentage value at which a Critical Memory warning message is displayed to the user. Shows the UWF cache percentage value at which a Critical Memory warning message is displayed to the user. Once the memory level crosses the warning level 2, system automatically restarts. (Default value = 90, Minimum value = 55, Maximum value = 90).
- **Commits and Exclusion**

1. **File Manager**
   - Current Session
     - **File/Directory Path**— Allows you to add and remove a file or directory, to or from the exclusion list for the next session.
     - This retrieves the list of files or directories that are written through in the current session, and the title of the pane is shown as Current Session Exclusion List. The Next Session retrieves the list of files or directories that are written through for the next session, and the title of the pane is shown as Next Session Exclusion List. The system does not restart the thin client, and the changes are not committed until an administrator restarts the thin client device manually.
   - Commit a file
     - **File Path**—Allows you to add, remove, and commit files to the underlying media. The system does not restart the thin client device. The changes are committed immediately.

       NOTE: If the file is not committed, delete a file path from the list.
2. **Registry Manager**
   - Current Session
     - **File/Directory Path**— Allows you to add and remove a Registry key path, to or from the exclusion list for the next session.
     - This retrieves the list of Registry key paths that are written through in the current session, and the title of the pane is shown as Current Session Exclusion List. The Next Session retrieves the list of Registry key path that are written through for the next session, and the title of the pane is shown as Next Session Exclusion List. The system does not restart the thin client, and the changes are not committed until an administrator restarts the thin client device manually.
     - Commit a Registry
       - **Registry Key Path**—Allows you to add, remove, and commit files to the underlying media. The system does not restart the thin client device. The changes are committed immediately.

         NOTE: If the Registry Key path is not committed, delete a Registry Key path from the list.
     - Current Session Exclusion List
       - **File/Directory Path**—Allows you to add and remove a file or directory, to or from the exclusion list for the next session. This retrieves the list of files or directories that are written through in the current session, and the title of the pane is shown as Current Session Exclusion List. The Next Session retrieves the list of files or directories that are written through for the next session, and the title of the pane is shown as Next Session Exclusion List. The system will not restart the thin client, and the changes are not committed until an administrator restarts the thin client device manually.

Application Launch Manager

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

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

ALM Command Line Interface tool

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

Configuration of nodes using ALM

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

Table 3. Options to configure nodes

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

Table 4. Parameters to configure nodes

Parameter	Values
`Name:`<name of the application>	[Application name]
`Path:`<path of the application>	[Application path]
`Arguments:`< specify the configuration information when the application is launched>	[Argument]

`Event:`<event to execute the command>	`USER_LOGOFF`
	`SVC_STARTUP`
	`ON_SHUTDOWN`
	`USER_LOGIN`

Examples to configure nodes using xDCM

Table 5. Examples to configure nodes using xDCM

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

NOTE:

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

xData Cleanup Manager

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

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

NOTE:

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

xDCM Command Line Interface tool

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

Configuration of nodes using xDCM

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

Table 6. Options to configure nodes

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

Table 7. Parameters to configure nodes

Parameter	Values

`CleanupType:`<type of the clean up node>	`Folder`
	`File`
	`Registry`

`Name:`<name of the clean up node>	[Folder/File/Registry name]
`Path:`<path of the clean up node>	[Folder/File/Registry path]
`PathExclusions:`<paths to be excluded from deletion (Path1,Path2)/NULL>	[Path/NULL]

`Event:`<event to execute the command>	`USER_LOGOFF`
	`SVC_STARTUP`
	`ON_SHUTDOWN`

`CleanType:`<type of clean up>	`DIR_DELETE` `DIR_EMPTY`
`CleanFrom:`<type of memory>	`Disk` `Overlay`

Examples to configure nodes using xDCM

Table 8. Examples to configure nodes using xDCM

Scenario	Command
Adding a folder cleanup node in `XdataCleanupConfig.xml` under **DiskCleanup** element.	`XDCM.exe -Add -CleanupType:Folder -Name:Notepad -Path:C:\Windows\Security -PathExclusions:"C:`

Table 8. Examples to configure nodes using xDCM (continued)

Scenario	Command
	`\Windows\Security\database, C:\Windows\logs" -Event: USER_LOGOFF -CleanType:DIR_EMPTY -CleanFrom:Disk`
Deleting a file cleanup node under **OverlayCleanup** element **Notepad** in `XdataCleanupConfig.xml`.	`XDCM.exe -Remove -CleanupType:File -Name:Notepad -CleanFrom:Overlay`

NOTE:

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

Capturing logfiles

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

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

Configuration of DebugLog XML file

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

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

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

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

Table 9. LogLevel values

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

Mapping network drives

About this task

Administrators can map network drives. To map the network drive and retain the mappings after the thin client device is restarted, see Map a network drive.

Participating in domains

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

About this task

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

Steps

1. Log in as an administrator.
2. Go to **Start** > **Control Panel** > **System**.
   The **System** window is displayed.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.
   The **System Properties** dialog box is displayed.
4. Click **Change** option to change the domain or workgroup.
   a. Click **Domain**.
      The **Computer Name/Domain Changes** dialog box is displayed.
   b. Enter the domain of your choice.
   c. Click **OK**.
5. To join a thin client device to a domain, click **Network ID**.
   The **Join a Domain or Workgroup** wizard is displayed. On the first page of the wizard, select the option that describes your network.
   - Business Network—Click this option if your thin client is a part of business network and you use it to connect to other clients at work.
     a. Click **Next**.
     b. Select the option according to your company's network availability on a domain.
        If you select the option **Network with a domain**, then enter the following information:
        - User name
        - Password
        - Domain name

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

        NOTE: You can click **Next** even if you do not know the workgroup name.
     c. To apply the changes, you must restart the computer. Click **Finish**.
        NOTE: Before restarting your computer, save any open files and close all programs.
   - Home Network—Click this option if your thin client is a home client and it is not a part of a business network. To apply the changes, you must restart the computer. Click **Finish**.

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

   To make the domain changes permanent, complete the following:

   a. Disable the Unified Write Filter.
   b. Join the domain.
   c. Restart the thin client.

d. Enable the Unified Write Filter.

NOTE:

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

Next steps

Using Roaming Profiles

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

Managing Users and Groups with User Accounts

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

This section provides quick-start guidelines on:

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

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

Creating user accounts

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

About this task

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

Steps

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

Editing user accounts

Prerequisites

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

About this task

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

Steps

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

Configuring user profiles

Prerequisites

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

About this task

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

Steps

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

Changing the computer name of a thin client

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

About this task

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

Steps

1. Log in as an administrator.
2. Go to **Start** > **Control Panel** > **System**.
   The **System** window is displayed.
3. In the **Computer name, domain, and workgroup settings** section, click **Change Settings**.
   The **System Properties** dialog box is displayed.
4. Click **Change** to rename the computer name.
5. In the **Computer Name** window, type the name for the thin client device in the **Computer name** field, and click **OK**.
6. In the Confirmation dialog box, click **OK** to restart for applying the changes.
7. Click **Close**, and then click **Restart Now** to apply the changes.

Removing language and feature on demand packages

Prerequisites

Perform the following steps to remove language and feature on demand packages:

NOTE: These steps must be performed from the admin account with the **Unified Write Filter** disabled.

Steps

1. Start a command prompt with administrator privileges.
2. Run the following command:`dism /online /get-packages | find /I "Client-Language"`.

3. See **Language Code** table to identify the languages installed.
4. Once a language has been identified, find all the associated packages with that language.
5. Run `dism /online /get-packages | find /I "<Language Abbreviation>"`
6. Run the following commands to remove all **French-language** feature packages:

   ```
   dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-Speech-fr-fr-Package~31bf3856ad364e35~amd64~~10.0.14393.0" /norestart

   dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-TextToSpeech-fr-fr-Package~31bf3856ad364e35~amd64~~10.0.14393.0" /norestart

   dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-OCR-fr-fr-Package~31bf3856ad364e35~amd64~~10.0.14393.0" /norestart

   dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-Handwriting-fr-fr-Package~31bf3856ad364e35~amd64~~10.0.14393.0" /norestart

   dism /online /remove-package /packagename:"Microsoft-Windows-LanguageFeatures-Basic-fr-fr-Package~31bf3856ad364e35~amd64~~10.0.14393.0" /norestart
   ```

   NOTE: Not all the languages include the **LanguageFeatures-Speech** package. If the selected language includes the **LanguageFeatures-Speech** package, then that package must be removed.

   NOTE: Double byte character languages (Chinese Simplified, Chinese Traditional, Japanese, and Korean) include the following **Feature On Demand** packages that must be removed, if the following languages are removed from the system:

   - Chinese Simplified

     ```
     Microsoft-Windows-LanguageFeatures-Fonts-Hans-Package~31bf3856ad364e35~amd64~~10.0.14393.0
     ```

   - Chinese Traditional

     ```
     Microsoft-Windows-LanguageFeatures-Fonts-Hant-Package~31bf3856ad364e35~amd64~~10.0.14393.0
     ```

     ```
     Microsoft-Windows-InternationalFeatures-Taiwan-Package~31bf3856ad364e35~amd64~~10.0.14393.0
     ```

   - Japanese

     ```
     Microsoft-Windows-LanguageFeatures-Fonts-Jpan-Package~31bf3856ad364e35~amd64~~10.0.14393.0
     ```

   - Korean

     ```
     Microsoft-Windows-LanguageFeatures-Fonts-Kore-Package~31bf3856ad364e35~amd64~~10.0.14393.0
     ```

   These packages are not dependent on any other packages, hence these can be removed at any time.

   NOTE: You must remove the **LanguageFeatures-Basic** package.

   NOTE: A list of supported **Windows 10 IoT Enterprise Language** packages are found in the following table **Windows 10 IoT Enterprise Language Packages**.

7. Once the **LanguageFeature** packages are removed, remove the **Client-LanguagePack**.

   ```
   start /b /wait dism /online /remove-package /packagename:"Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~fr-FR~10.0.14393.0" /norestart
   ```

8. Repeat the steps to remove all the unused languages from the system.
9. After removing the unused languages, reboot the system.
10. After the system reboots, log in into the admin account and run the `OSComponentCleanup` utility.
11. Enable **Unified Write Filter**.

Language codes

Following are the list of language codes:

Table 10. Language codes

Language	Abbreviation
English	EN-US
Chinese Simplified	ZH-CN
Chinese Traditional	ZH-TW
Danish	DA-DK
Dutch	NL-NL
Finnish	FI-FI
French	FR-FR
French Canadian	FR-CA
German	DE-DE
Italian	IT-IT
Japanese	JA-JP
Korean	KO-KR
Norwegian	NB-NO
Portuguese Brazilian	PT-BR
Russian	RU-RU
Spanish	ES-ES
Swedish	SV-SE

Adding languages to LTSC 2021

Prerequisites

- These steps must be performed from the admin account with the **Unified Write Filter** disabled.
- A network connection is required to install localized language packages from Microsoft.

Steps

1. Open the **Windows Settings** and click **Time & Language**.
2. In the left pane, click **Language**.
3. Under **Preferred languages**, click **Add a language**.
4. In the search field, type the required language that must be added to the system and select the language, and then click **Next**.
5. Check the **Set as my Windows display language** check box and click **Install**.

   NOTE: The display language can be changed from the Windows display language drop-down menu.
6. Verify all the installed language packages before proceeding.

   NOTE: Verifying the installed packages may take several minutes and are dependent upon the number of languages that are installed in the system. Also, it depends on the network bandwidth and the response time from Microsoft source installation servers.

7. To verify all the packages that are installed, open a command prompt with administrator privileges, and run the following commands. Only proceed when all **Client-LanguagePackages** are displayed along with the language-specific feature on-demand packages for SNMP components.

   ```
   dism /online /get-packages | find /i "-Language"
   ```

   ```
   dism /online /get-packages | find /i "SNMP"
   ```

8. Remove **Language Experience** appx packages.

   NOTE: If you do not remove **Language Experience** appx packages, an error is displayed when the **Windows Sysprep** is performed.

9. Open PowerShell, run `Get-AppxPackage -AllUsers "*LanguageExperience*" | Remove-AppxPackage -AllUsers` command.
10. Verify all the language experience appx packages have been removed by running `Get-AppxPackage -AllUsers "*LanguageExperience*"` command.
    This command returns no output.
11. Open **Administrative Language Settings** and click **Change System Locale** under **Language for non-Unicode Programs**.
12. Select the added language under **Current System Locale** drop-down menu and click **OK**.
13. Now click **Copy Settings** under **Welcome screen and new user accounts**, check **Welcome screen and system accounts** and **New user accounts** check boxes and click **OK**.
14. Restart the device.

Windows 10 IoT enterprise language packages

These are the list of supported localized language packages on Wyse Windows Thin Client systems:

Table 11. English

Language packages
Microsoft-Windows-Client-LanguagePack-Package-en-US
Microsoft-Windows-LanguageFeatures-Basic-en-us-Package
Microsoft-Windows-LanguageFeatures-Handwriting-en-us-Package
Microsoft-Windows-LanguageFeatures-OCR-en-us-Package
Microsoft-Windows-LanguageFeatures-Speech-en-us-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-en-us-Package

Table 12. Chinese Simplified

Language packages
Microsoft-Windows-Client-LanguagePack-Package-zh-CN
Microsoft-Windows-LanguageFeatures-Basic-zh-cn-Package
Microsoft-Windows-LanguageFeatures-Handwriting-zh-cn-Package
Microsoft-Windows-LanguageFeatures-OCR-zh-cn-Package
Microsoft-Windows-LanguageFeatures-Speech-zh-cn-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-zh-cn-Package
Microsoft-Windows-LanguageFeatures-Fonts-Hans-Package

Table 13. Chinese Traditional

Language packages
Microsoft-Windows-Client-LanguagePack-Package-zh-TW

Table 13. Chinese Traditional (continued)

Language packages
Microsoft-Windows-LanguageFeatures-Basic-zh-tw-Package
Microsoft-Windows-LanguageFeatures-Handwriting-zh-tw-Package
Microsoft-Windows-LanguageFeatures-OCR-zh-tw-Package
Microsoft-Windows-LanguageFeatures-Speech-zh-tw-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-zh-tw-Package
Microsoft-Windows-LanguageFeatures-Fonts-Hant-Package
Microsoft-Windows-InternationalFeatures-Taiwan-Package

Table 14. Danish

Language packages
Microsoft-Windows-Client-LanguagePack-Package-da-DK
Microsoft-Windows-LanguageFeatures-Basic-da-dk-Package
Microsoft-Windows-LanguageFeatures-Handwriting-da-dk-Package
Microsoft-Windows-LanguageFeatures-OCR-da-dk-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-da-dk-Package

Table 15. Dutch

Language packages
Microsoft-Windows-Client-LanguagePack-Package-nl-NL
Microsoft-Windows-LanguageFeatures-Basic-nl-nl-Package
Microsoft-Windows-LanguageFeatures-Handwriting-nl-nl-Package
Microsoft-Windows-LanguageFeatures-OCR-nl-nl-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-nl-nl-Package

Table 16. Finnish

Language packages
Microsoft-Windows-Client-LanguagePack-Package-fi-FI
Microsoft-Windows-LanguageFeatures-Basic-fi-fi-Package
Microsoft-Windows-LanguageFeatures-Handwriting-fi-fi-Package
Microsoft-Windows-LanguageFeatures-OCR-fi-fi-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-fi-fi-Package

Table 17. French

Language packages
Microsoft-Windows-Client-LanguagePack-Package-fr-FR
Microsoft-Windows-LanguageFeatures-Basic-fr-fr-Package
Microsoft-Windows-LanguageFeatures-Handwriting-fr-fr-Package
Microsoft-Windows-LanguageFeatures-OCR-fr-fr-Package
Microsoft-Windows-LanguageFeatures-Speech-fr-fr-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-fr-fr-Package

Table 18. French Canadian

Language packages
Microsoft-Windows-Client-LanguagePack-Package-fr-CA
Microsoft-Windows-LanguageFeatures-Basic-fr-ca-Package
Microsoft-Windows-LanguageFeatures-OCR-fr-ca-Package
Microsoft-Windows-LanguageFeatures-Speech-fr-ca-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-fr-ca-Package

Table 19. German

Language packages
Microsoft-Windows-Client-LanguagePack-Package-de-DE
Microsoft-Windows-LanguageFeatures-Basic-de-de-Package
Microsoft-Windows-LanguageFeatures-Handwriting-de-de-Package
Microsoft-Windows-LanguageFeatures-OCR-de-de-Package
Microsoft-Windows-LanguageFeatures-Speech-de-de-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-de-de-Package

Table 20. Italian

Language packages
Microsoft-Windows-Client-LanguagePack-Package-it-IT
Microsoft-Windows-LanguageFeatures-Basic-it-it-Package
Microsoft-Windows-LanguageFeatures-Handwriting-it-it-Package
Microsoft-Windows-LanguageFeatures-OCR-it-it-Package
Microsoft-Windows-LanguageFeatures-Speech-it-it-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-it-it-Package

Table 21. Japanese

Language packages
Microsoft-Windows-Client-LanguagePack-Package-ja-JP
Microsoft-Windows-LanguageFeatures-Basic-ja-jp-Package
Microsoft-Windows-LanguageFeatures-Handwriting-ja-jp-Package
Microsoft-Windows-LanguageFeatures-OCR-ja-jp-Package
Microsoft-Windows-LanguageFeatures-Speech-ja-jp-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-ja-jp-Package
Microsoft-Windows-LanguageFeatures-Fonts-Jpan-Package

Table 22. Korean

Language packages
Microsoft-Windows-Client-LanguagePack-Package-ko-KR
Microsoft-Windows-LanguageFeatures-Basic-ko-kr-Package
Microsoft-Windows-LanguageFeatures-Handwriting-ko-kr-Package
Microsoft-Windows-LanguageFeatures-OCR-ko-kr-Package

Table 22. Korean (continued)

Language packages
Microsoft-Windows-LanguageFeatures-TextToSpeech-ko-kr-Package
Microsoft-Windows-LanguageFeatures-Fonts-Kore-Package

Table 23. Norwegian

Language packages
Microsoft-Windows-Client-LanguagePack-Package-nb-NO
Microsoft-Windows-LanguageFeatures-Basic-nb-no-Package
Microsoft-Windows-LanguageFeatures-Handwriting-nb-no-Package
Microsoft-Windows-LanguageFeatures-OCR-nb-no-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-nb-no-Package

Table 24. Portuguese Brazilian

Language packages
Microsoft-Windows-Client-LanguagePack-Package-pt-BR
Microsoft-Windows-LanguageFeatures-Basic-pt-br-Package
Microsoft-Windows-LanguageFeatures-Handwriting-pt-br-Package
Microsoft-Windows-LanguageFeatures-OCR-pt-br-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-pt-br-Package

Table 25. Russian

Language packages
Microsoft-Windows-Client-LanguagePack-Package-ru-RU
Microsoft-Windows-LanguageFeatures-Basic-ru-ru-Package
Microsoft-Windows-LanguageFeatures-Handwriting-ru-ru-Package
Microsoft-Windows-LanguageFeatures-OCR-ru-ru-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-ru-ru-Package

Table 26. Spanish

Language packages
Microsoft-Windows-Client-LanguagePack-Package-es-ES
Microsoft-Windows-LanguageFeatures-Basic-es-es-Package
Microsoft-Windows-LanguageFeatures-Handwriting-es-es-Package
Microsoft-Windows-LanguageFeatures-OCR-es-es-Package
Microsoft-Windows-LanguageFeatures-Speech-es-es-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-es-es-Package

Table 27. Swedish

Language packages
Microsoft-Windows-Client-LanguagePack-Package-sv-SE
Microsoft-Windows-LanguageFeatures-Basic-sv-se-Package
Microsoft-Windows-LanguageFeatures-Handwriting-sv-se-Package

Table 27. Swedish (continued)

Language packages
Microsoft-Windows-LanguageFeatures-OCR-sv-se-Package
Microsoft-Windows-LanguageFeatures-TextToSpeech-sv-se-Package

Imaging using Dell Application Control Center

Dell Wyse thin clients that run the Windows 10 IoT Enterprise 2021 LTSC operating system can be imaged using Dell Application Control Center (DACC). The below procedures are followed to perform imaging:

- USB Imaging
- Wyse Management Suite Imaging

USB imaging using DACC

Steps

1. Image the device with the latest Windows 10 IoT Enterprise LTSC 2021 image.
2. Log in to the administrator's account and disable UWF.
3. Install the latest DAS bundle that deploys DACC by default.
4. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.
5. Go to **Imaging section** > **Image Settings**.
6. Select **Imaging Source** as **USB** from the drop-down list.
7. **Set Host Name Calculation** feature as **Enable Feature** or **Disable Feature** under **Host Name Calculation** based on your requirement.

   NOTE: Host Name Calculation is a client behavior that is configurable and allows resetting the hostname to **Windows Embedded Standard <MAC address>**.

   - To get the hostname calculation to occur for the local or the target client to which the captured golden image is to be pushed, follow the below steps:
     a. Clear **Enable Feature** under **Host Name Calculation** option to reset the hostname of the client to **Windows Embedded Standard <MAC address>**.
     b. The hostname of the machine you are capturing the image from must be set as **`MINWITHNET`** for hostname calculation to occur.

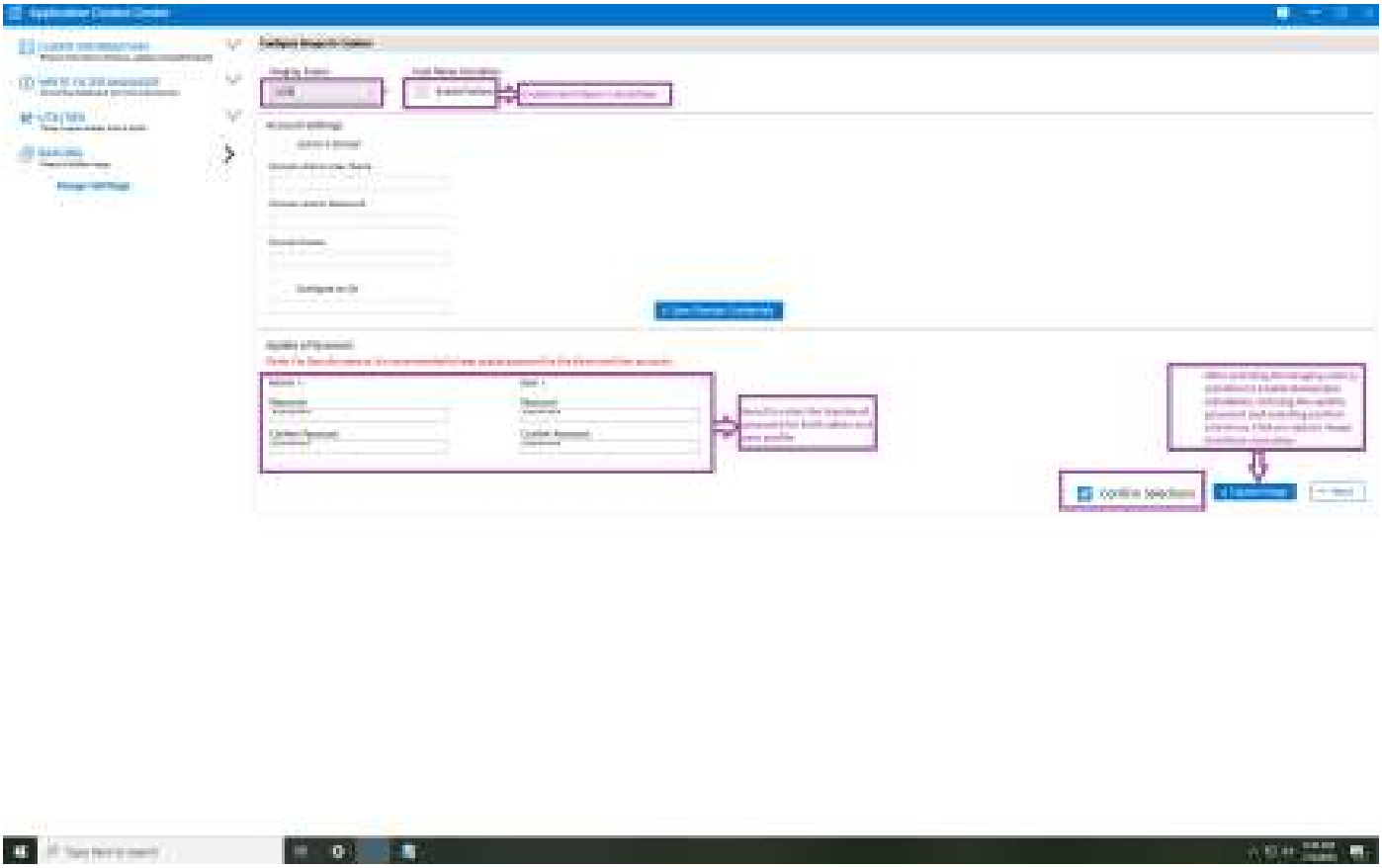


Figure 5. Clear Enable Feature

- If you do not want the hostname calculation to occur for the target client to which the captured golden image is pushed, follow the below step:
  a. Select **Enable Feature** under **Disable Host Name Calculation**.

     This process notifies the underlying subsystem to not reset the hostname to **Windows Embedded Standard <MAC address>**.

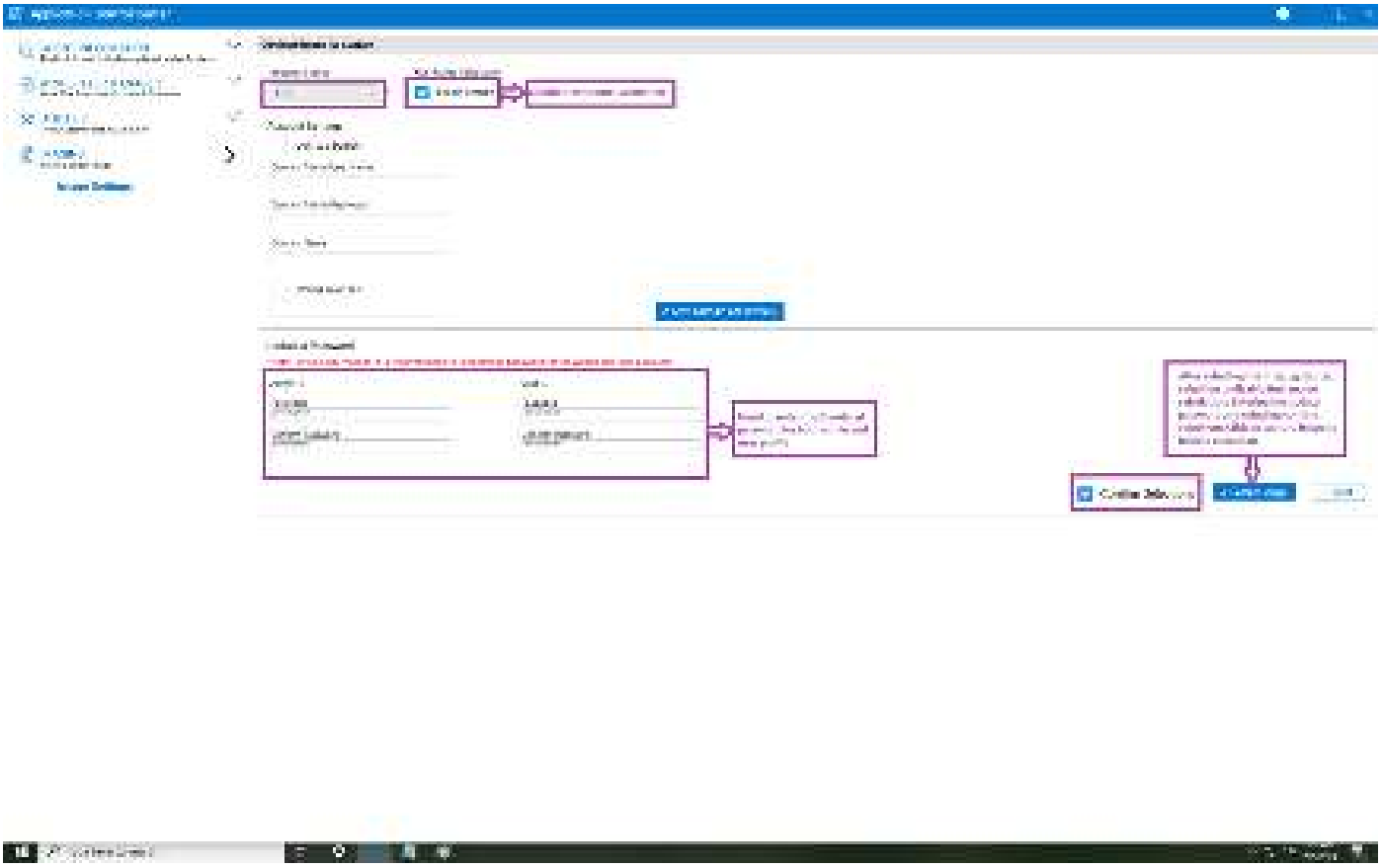


Figure 6. Select Enable Feature

8. Select the **Confirm Selections** check box and click **Capture Image**.

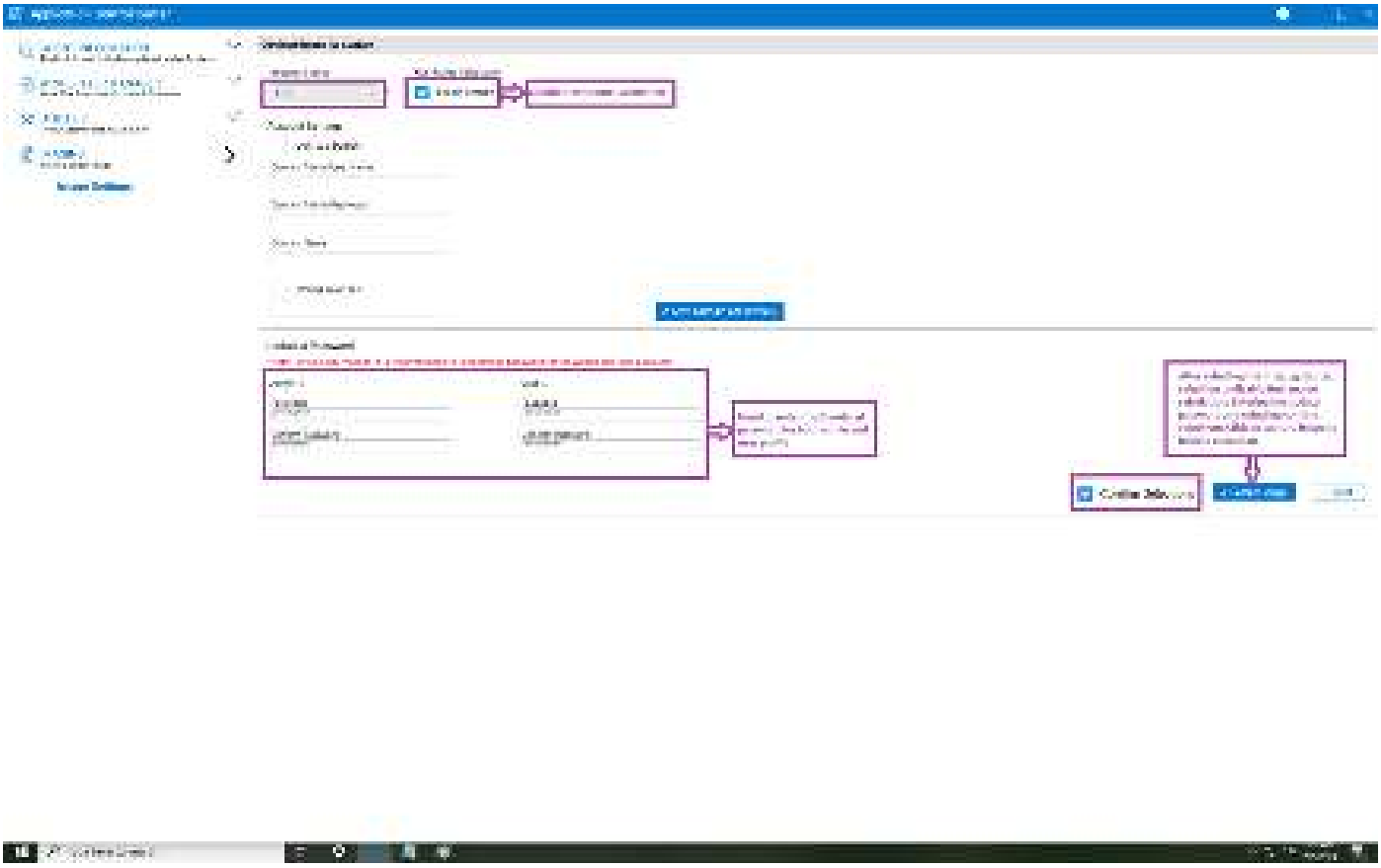


Figure 7. Confirm Image for Capture in Application Control Center

A window confirming USB imaging is displayed.

9. Click **Ok** to initiate the precustom Sysprep process.
   The device shuts down after the precustom Sysprep process is complete.
   NOTE: Connect the USB drive that is configured for USB imaging before you power on the device.
10. Power on the device and press **F12** when the one-time boot menu is displayed.
11. Select the **USB** option and boot the device using the configured USB drive.
12. Click the icon under **Pull device image under USB drive** in the **Dell Wyse USB Imaging Tool** window.
13. Click **Ok** to initiate the Image Pull process.
    Once the image pull completes, a message stating the image pull was successful is displayed.
14. Remove the USB drive and click **Restart**.
    The USB drive is ready with the golden image that can be used to deploy on another device.

Wyse Management Suite imaging using DACC

Steps

1. Image the device with the latest Windows 10 IoT Enterprise LTSC 2021 image.
2. Log in to the administrator's account and disable UWF.
3. Install the latest DAS bundle that deploys DACC by default.
4. Register the device to Wyse Management Suite server by following the steps below:
   a. Go to system tray.
   b. Click the **WDA** icon.
   c. Select **WMS** from the management server drop-down list and register the device by providing valid inputs.
5. Log in to the Wyse Management Suite server when the device is registered.
6. Click **Devices** and select your registered device after logging in to the Wyse Management Suite server.

7. Select **Pull OS Image** option from **More Actions** drop-down list.
   Pull OS Image window is displayed.
8. Enter **Name of image**, **File repository path**, **Pull type**, and **Default options** .
9. Click **Prepare for Image Pull**.
   Image Pull Request from System Admin window is displayed on the registered device.
10. Click **Pull now** to capture image without running custom Sysprep.
11. Click **Pull after sysprep** for capture image by running custom Sysprep.
12. Right-click the **Application Control Center** shortcut icon on the desktop and select **Run as administrator**.
13. Go to **Imaging section** > **Image Settings**.
14. Select **Imaging Source** as **USB** from the drop-down list.
15. Set the **Host Name Calculation** feature as **Enable Feature** or **Disable Feature** under **Disable Host Name Calculation** based on your requirement.

    NOTE: Host Name Calculation is a client behavior that is configurable and allows resetting the hostname to **Windows Embedded Standard <MAC address>**.

- To get the hostname calculation to occur for the local or the target client to which the captured golden image is to be pushed, follow the below steps:
  a. Clear **Enable Feature** under **Disable Host Name Calculation** option to reset the hostname of the client to **Windows Embedded Standard <MAC address>**.
  b. The hostname of the machine you are capturing the image from must be set as **`MINWITHNET`** for hostname calculation to occur.

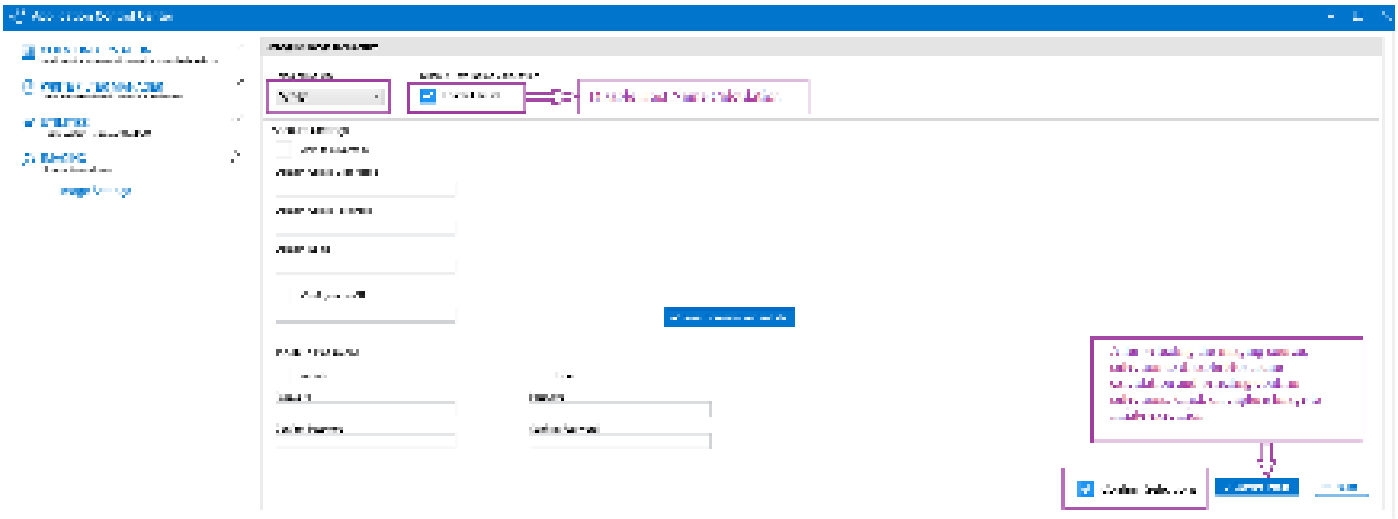


Figure 8. Clear Enable Feature

- If you do not want the hostname calculation to occur for the target client to which the captured golden image is pushed, follow the below step:
  a. Select **Enable Feature** under **Host Name Calculation** .

  This process notifies the underlying subsystem to not reset the hostname to **Windows Embedded Standard <MAC address>**.

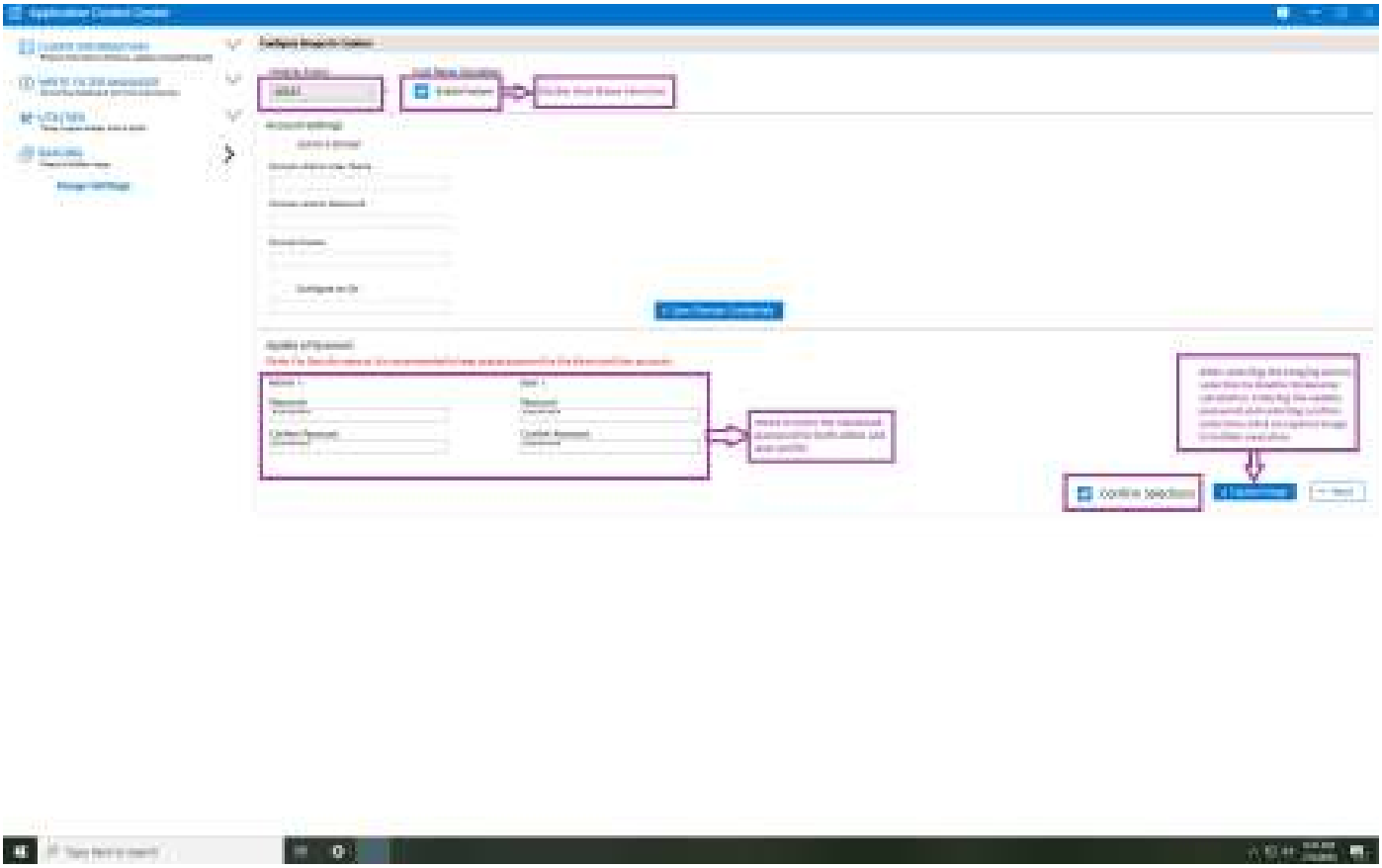


Figure 9. Select Enable Feature

16. Select the **Confirm Selections** check box and click **Capture Image**.

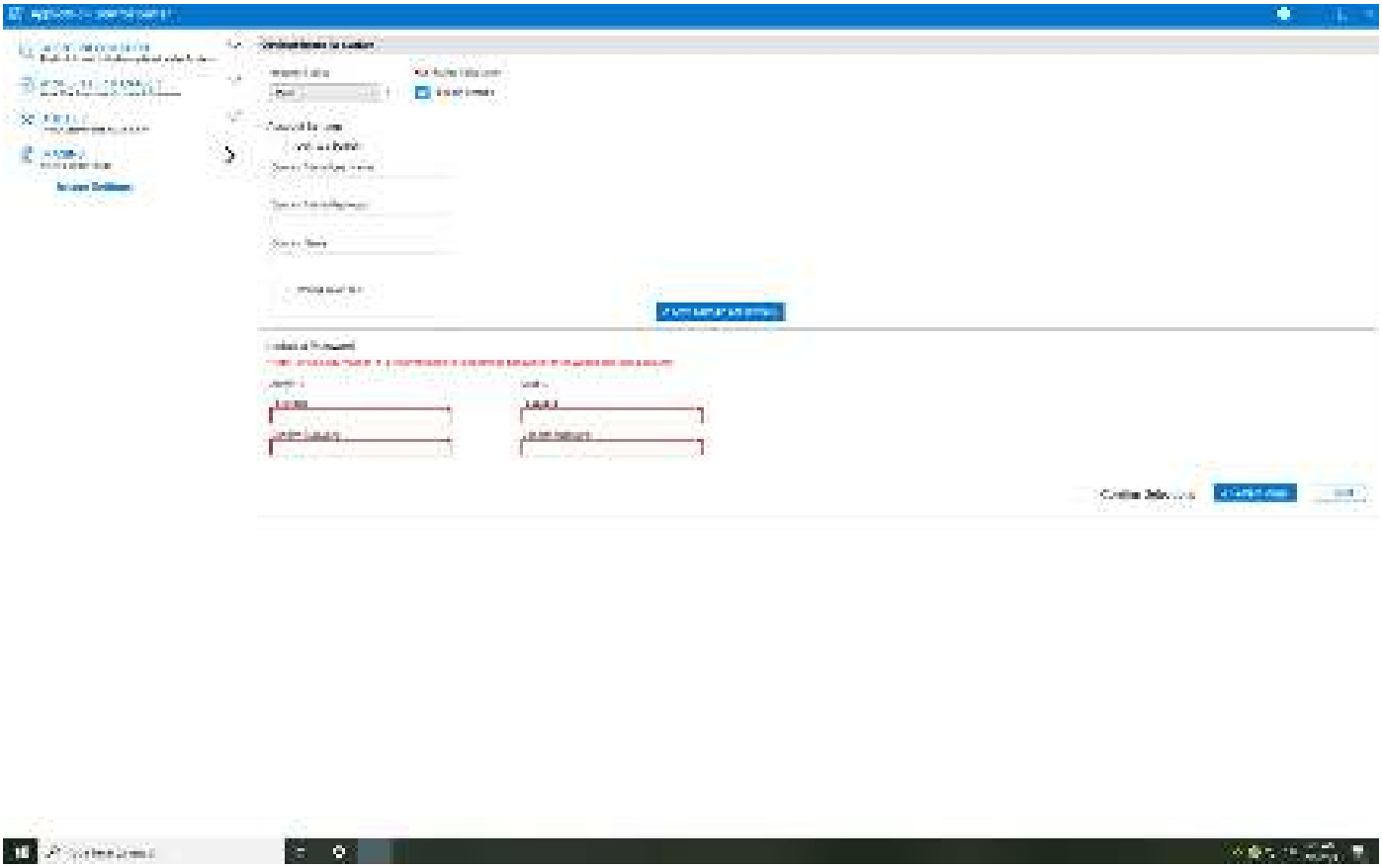


Figure 10. Confirm Image for Capture in Application Control Center

The device shuts down after the precustom Sysprep process is complete.

17. Power on the device.
    The device uploads the image to the Wyse Management Suite server.

6

System administration

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

Accessing thin client BIOS settings

About this task

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

Steps

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

Unified Extensible Firmware Interface and secure boot

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

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

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

Using Dell Wyse Management Suite

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

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

NOTE:

Dell Cloud Client Manager (CCM) is re-envisioned as Wyse Management Suite and provides new features, functionalities with major product level enhancements to CCM R14. For more information, see Wyse Management Suite Release Notes at dell.com/support/manuals. Existing customers can continue to manage their thin clients as before, and take advantage of the new features introduced in this release.

TightVNC—server and viewer

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

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

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

To open **TightVNC Server** window:

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

NOTE:

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

TightVNC—Pre-requisites

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

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

NOTE:

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

Using TightVNC to shadow a thin client

About this task

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

Steps

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

   To shadow a thin client from a remote machine:

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

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

Configuring TightVNC server properties on the thin client

Steps

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

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

Uninstall procedure for TightVNC versions 2.x

Steps

1. Log in as an Administrator (or as a user with similar permissions).
2. Disable **Unified Write Filter**.
3. Log in as administrator after the reboot.
4. If TightVNC Server is running, close it. If it is running but does not appear on the tray icon, select **Process Manages**, locate all tvnserver.exe process, and shut down each of them.
5. If TightVNC Server was registered as a system service, unregister it. To do that, locate tvnserver.exe file under `\Program Files\TightVNC` (or wherever TightVNC was installed), and type in the command line: `tvnserver.exe -remove`.
6. Remove the `\Program Files\TightVNC directory` (or wherever TightVNC was installed).
7. Remove all TightVNC shortcuts from the Start\All Programs menu.
8. Remove the settings from the registry . The settings can be found in `HKEY_LOCAL_MACHINE\Software\TightVNC` and/or `HKEY_CURRENT_USER\Software\TightVNC`.
9. Enable **Unified Write Filter**.

7

Network architecture and server environment

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

Understanding how to configure your network services

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

You can configure your network services using:

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

Using Dynamic Host Configuration Protocol

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

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

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

DHCP options

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

Table 28. DHCP options

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

Table 28. DHCP options (continued)

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

NOTE: For more information on configuring a DHCP server, see support site.

Using Domain Name System

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

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

About Citrix Studio

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

NOTE: For more information about installing and configuring the Citrix Studio, go to Citrix Website.

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

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

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

About VMware Horizon View Manager

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

NOTE: For more information, on installing and configuring View Manager, go to VMware Website.

VMware View includes the following key components:

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

  View Administrator also provides an interface to monitor log events and is installed with View Connection Server.
- **View Composer**—To allow View Manager to rapidly deploy multiple linked clone desktops from a single centralized base image, **View Composer** software service is installed on the Virtual Center server.

8

Frequently asked questions

How to set up a smart card reader

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

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

How to use USB Redirection

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

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

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

Using Wyse Management Suite

Prerequisites

If you are using Wyse Management Suite 1.3 remote repository, then Recovery/ Recovery + OS pull templates are not available in the repository. You must upgrade Wyse Management Suite to 1.4 to access the templates.

Steps

1. Go to the **Windows Embedded Standard** or **ThinLinux** device page.
2. Select **Pull OS Image** option, from the **More Actions** drop-down list.
3. Enter or select the following details:
   - **Name of Image**—Provide a name for the image. To replace the image with a similar name and the image files that are not completed successfully, click **Override name**.
   - **File repository**—From the drop-down list, select the file repository to where the image is uploaded. There are two types of file repositories:
     - Local repository
     - Remote Wyse Management Suite repository
   - **Pull Type**—Select either **Default** or **Advanced** based on your pull type requirement.
     - When the **Default** pull type is selected, the following options are displayed:
       - Compress
       - OS
       - BIOS
     - When the **Advanced** pull type is selected, a drop-down list for selecting the template is displayed. Select any template which is available by default.

NOTE: You can use custom templates by editing the existing or default templates.

4. Click **Prepare for Image Pull**.

Results

When the **Pull OS Image** command is sent, the client device receives an image pull request from the server. An image pull request message is displayed on the client side. Click either of the following options:

- **Pull after sysprep**—The device restarts, and logs in to the operating system in a disabled state. Run the custom sysprep. After the custom sysprep is complete, the device boots to Merlin operating system and the image pull operation is performed.
- **Pull now**—The device boots to the Merlin operating system and the image pull operation is performed.

9

Troubleshooting

Keyboard customization issues

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

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

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

Resolving memory issues

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

- Windows Task Manager
- Unified Write Filter
- File Explorer

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

Using Windows Task Manager

1. Log in as an administrator.
2. Press Ctrl+Alt+Delete.
3. Click **Task Manager**.

   The **Task Manager** window is displayed.
4. Click **More details**.
5. Click the **Performance** tab, and analyze your system memory resources.
6. Close the programs that are using more memory.

Using Unified Write Filter

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

CADMAP tool interfering with published application shortcut keys

The Winlockworkstation.exe add-on must be pushed using Wyse Management Suite or Microsoft Endpoint Configuration Manager. This feature enables you to use WIN+L key combination in remote sessions. You can enable or disable the WIN+L key combination in local sessions using WinLock Workstation application.

You can also use /WE or /WD parameters to enable or disable the WIN+L key combination.

In VDI sessions, WIN+L functionality works as configured on the server. On closing VDI sessions, the WIN+L functionality retains the user configured state that is pushed from server using the Winlockworkstation.exe add-on.