

Windows 10 IoT Enterprise

Thin Client

Administrator Guide

Copyright © 2004-2018 VXL Instruments Limited. All Rights Reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the part of the manufacturer. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer.

Registered trademarks are properties of their respective owners. Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Every effort has been made to make this guide as complete and as accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity with respect to loss or damages arising from the use of information contained in this guide.

Last Updated: February, 2018

Version: Windows 10 IoT/AG-07-18

Table of Contents

1 Getting Started 1

Logging On 1

Automatic Logon 1

Manual Logon 2

Local Drives 2

Drive C 2

Drive Z 3

User and Administrator Desktop 3

User Desktop 3

Administrator Desktop 3

2 UWF (Unified Write Filter) 4

UWF Notification 4

UWF Configuration 4

3 Configuration 6

User Accounts and Profiles 6

Configure User Name and Password 7

System Date and Time 7

Wired Network Configuration 8

Wireless Network Configuration 8

Configuring Printers 9

Region and Location 10

Installing applications 10

Configuring application to cache on the RAM drive 10

4 Remote VDI Applications 11

Citrix Receiver with Citrix Online plug-in 11

VMware Horizon View Client 11

Remote Desktop Protocol Client 12

5 Remote Management Agent 13

Fusion Universal Device Management Support 13

6 Applications Support 14

Microsoft Applications 14

Windows Media Player 14
Windows Firewall 14
Internet Explorer 14
Microsoft Silverlight 14
Thin Client Administrative Applications 15
Thin Client Applets 15
Client information 15
Autologon Manager 16
Unified Write Filter (UWF) 17
USB Device Controller 17
Performance Warning Settings 18
RAM Drive Manager 19
Windows Connection Manager 20
7 Device Maintenance 21
Restoring to Factory Defaults 21
Accessing the Thin Client BIOS 21
Accessing the Boot Options menu 21
Installing 3rd Party Applications 22
8 Access Technical Support 23
Technical Support 23
Software Downloads 23
SSD Usage and Warranty 23
WES Customization 23
Microsoft support website (Documentation for Microsoft software) 23
Activation in Windows 10 23
Volume Activation for Windows 10 23
VMware support website (Documentation for VMware software) 23
Citrix support website (Documentation for VMware software) 23
Glossary 24
Index 25
Revision History 26

1 Getting Started

Windows 10 IoT Enterprise is the latest, powerful operating system from Microsoft.

Thin client series with Windows 10 IoT Enterprise has power users with an exceptional user experience together with excellent security and compatibility with leading industry desktop virtualization solutions including the latest Microsoft Remote Desktop Connection, VMware Horizon View and Citrix Receiver. Thin clients provide the flexibility, connectivity, security, multimedia, and peripheral capabilities that make them ideal for most mainstream business use.

This administrator guide provides information and instructions to use the thin client with the Windows 10 IoT Enterprise operating system. It is assumed that you will log on to Windows as an administrator when configuring the operating system or using administrative applications as discussed in this guide.

Logging On

There are two user accounts by default:

- **Administrator**

Allows you to make permanent system configurations, such as user account management or app installations

- **User**

Cannot make permanent changes to the system and is for end-user operation

By default, a Windows 10 IoT thin client is automatically logged on to the locked-down User account when Windows starts. So you must switch to the Administrator account manually using the default password Administrator.

To switch back to the User account, use the default password User.

Automatic Logon

The administrator can use from **Start > Thin Client Applets > Auto Logon Manager** to enable/disable auto logon and change the auto logon user name, password, domain name.

Only the Administrator has the privileges to change auto logon properties.

Automatic Log on allows a user to log on without entering the user name and password. This type of log on is useful when using the thin client as a public access computer or any computer that does not require user access rules. For example: A school library computer.

To enable automatic log on:

1. Turn on the thin client.
2. Log on as an ***Administrator***.
3. Click Start > Thin Client Applets > Autologon Manager. The Autologon Manager window appears.
4. In the **Username** field, enter a user name. This will be the default user name.

5. In the **Password** field, enter a password. This will be the default user password.
6. In the **Domain Name** field, enter a domain name.
7. Check Enable Autologon.
8. Click **OK**.
9. Restart the thin client. The User is automatically logged on.

To disable Autologon:

1. Turn on the thin client.
2. Log on as the ***Administrator***.
3. Click Start > Thin Client Applets > Autologon Manager. The Autologon Manager window appears.
4. Uncheck Enable Autologon.
5. Click **OK**.
6. Restart the thin client.

Manual Logon

You have to manually log on to Windows 10 IoT thin client if the AutoLogon is disabled.

To log on manually:

1. Turn on the thin client. The list of Logon profile appears.
2. Give a sign out. The Administrator and User accounts will be displayed.
3. Select an account.
4. In the **Password** field, enter the valid password.
5. Click **OK**.

Note: The default user name and password for the User account is **User** and default user name and password for the Administrator is **Administrator**

Local Drives

Drive C

Drive C is flash drive. This is the physical drive where the operating system and apps are installed. This drive is protected by Unified Write Filter (UWF) by default

Caution: If the available free space on the flash drive drops below 10%, the thin client becomes unstable.

Drive Z

RAM drive)—this is a virtual drive created using RAM. This drive behaves like a physical drive, but it is created at system startup and destroyed at system shutdown. You can configure the size of this drive with RAMDRIVE Manager

VXL recommends that you do not use this drive to save data that you want to retain after a reboot.

Note: VXL recommends that you save files that you want to retain on a server rather than on the thin client. Many applications by default write cache files on the Drive C in the local system. Save the application settings on Drive Z if you want to store it on a local drive.

Caution: The thin client uses an embedded operating system with a fixed flash memory capacity.

User and Administrator Desktop

When the Windows 10 IoT thin client turned on, a client's start-up screen looks like a generic Windows 10 start-up screen is noticed.

The Windows 10 IoT desktop application provides easy access to the thin client application and other client configuration options.

This chapter provides you an overview of the functions and features of the User and Administrator desktops.

User Desktop

The User desktop will have limited access to the **Control Panel** and **System Settings**. Following features are denied to access in the User account:

- Local drive access
- Device Manager
- Programs and Features
- System
- Mouse right click
- Run menu
- Administrative control panel applets

Administrator Desktop

The Administrator desktop gives you unrestricted access to the **Control Panel** and desktop settings.

2 UWF (Unified Write Filter)

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

This improves the reliability and stability of the device and reduces wear on write-sensitive media, such as flash memory media like solid-state drives.

With UWF, you can do stateless operations by creating a protected OS image, and you reduce the wear on flash media. UWF supports RAM and disk-based overlays. Both types of overlay discard all changes on restart. UWF also provides the ability to perform dynamic protection, which means adding and removing volumes at run time

Windows 10 IoT includes Unified Write Filter Manager. You can enable, disable and configure write filter using the UWF Manager application.

Note: Overlay cache will be cleared only by system restart, not either with logoff or switch user condition**.**

Caution: Its highly recommend to Turn On the UWF. It's highly recommended to disable the Windows Page File feature.

The use of the above features results in lower-endurance flash drives, premature wearing of the flash drive, decreased performance, and a decrease in the lifespan of the thin client.

UWF Notification

The UWF notification icon is located in the Windows notification area. The following status can be seen on the notification icon:

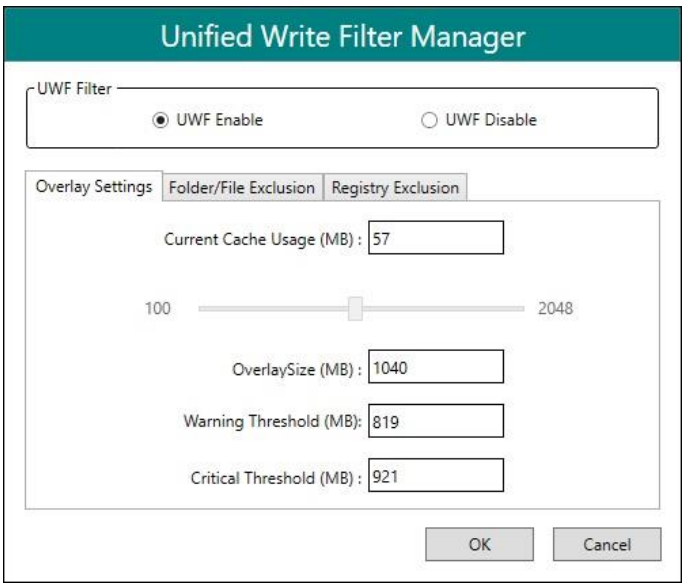
Icons appearance on tray:

- UWF enable → 
- UWF Disable → 

UWF Configuration

To access the UWF Manager Application:

1. Log on as an Administrator.
2. Click Start > Thin Client Applets > UWF Manager
3. **UWF Manager** Screen appears.



The tasks can be perform in this application include the following:

- Disable or enable UWF (Operation requires a system reboot)
- View information about UWF and the overlay cache
- Edit the exclusion list to add or remove files, folders and Registries
- Set the overlay cache threshold
- Set the cache usage at which warning and critical messages each display

Note: When the UWF overlay cache is filled up and reaches the critical threshold, the system will reboot.

3 Configuration

This chapter provides you with the information on following contents

- User Accounts and profiles
- Configuration user name and password
- System date and time
- Wired network configuration
- Wireless network configuration
- Region and Location
- Installing Applications
- Configuring apps to cache on the RAM drive

User Accounts and Profiles

This topic provides you with the information to create new user accounts. You can create multiple user accounts on Windows 10 IoT thin client. Every user account has a corresponding profile associated with it. The user profile stores desktop preferences, themes, screensavers etc.

A new user's profile is based on the Default User profile template, which includes policies similar to the factory-defined Administrator account. The new user profile will have a default membership with the local Users group. If the Default User profile settings are changed from those set at the factory, the changed settings are automatically applied to any newly created user profile - local or domain.

Any local domain account (created or cached) logged into the device prior to changes made to the default User profile are unaffected by these changes, only accounts logged in or cached after the changes have been made, have the new settings.

⚠**Caution:** Because of the limited size of flash memory, VXL recommends that you configure other applications available to the new and existing users to prevent writing to the local file system. VXL also recommends that you exercise extreme care when changing configuration settings of the factory-installed applications.

To create a new user:

- Log on as an Administrator.
- Right-click **Start > Control Panel > User Accounts > Manage another Accounts**. The User Accounts window appears.
- Click Make changes to my account in PC settings. The Manage Accounts window appears.
- The **PC Settings** window appears.

Notes:

- All child user events and records of a child account will be monitored by the Administrator account.
- The newly created account will be automatically added to the Users group.

To edit user account:

Right-click Start > Control Panel > User Accounts

To change a User profile to an Administrator:

Right-click Start > Control Panel > User Accounts

- Click Manage another account.
- Click on the Account that you want to grant administrative privileges.
- Click Change the account type. Select Standard or Administrator account type and click Change Account Type.

Configure User Name and Password

It is recommended that you change password in the first log in, for security reasons. You can change the password only when you are logged in as an administrator. To change the user name and password:

- Log on as an Administrator.
- Press Ctrl+Alt+Delete. The Windows Security dialog box appears.
- Click Change Password.
- Enter the Old password.
- Enter the New password.
- Re-enter the password in the Confirm password field and Press the Enter key.

System Date and Time

You can either set time manually or configure it to synchronize with a timeserver at designated times.

Note: The Windows Time service is stopped by default. To start the service Right-click **Start > Control Panel > Administrative Tools > Date and Time**

We recommended that the thin client time be synchronized with the server as some thin client applications may require access to the thin client time.

To set date and time:

- Right-click **Start > Control Panel**.
- Double-click Date and Time. The Date and Time dialog box appears.
- Click Change date and time… to change the current date and time.
- Click Change time zone… to set the current time zone.

Note: Set the time, date and time zone on first reboot.

- To synchronize thin client time with the Time Server:
- Click Internet Time.
- Click Change settings…The Internet Time Settings window appears
- Select Synchronize with an Internet timeserver.
- From the Server drop-down list, select a timeserver of the given choice.
- Click Update now to synchronize the thin client time with the timeserver. The clock was successfully synchronized message appears and click OK.

Wired Network Configuration

Thin client is automatically connected to the available wired network. You can turn on or off network sharing based on your preference.

To access Wired Network:

- On the System Tray, click Network and Sharing. The Networks window appears.
- Right-click on the connection to turn sharing on or off. The Do you want to turn on sharing… message appears.
- Click yes to turn on sharing within your network.
- Click No to turn off sharing within your network

Wireless Network Configuration

You can configure and access the wireless networks in your range if the wireless LAN hardware feature is present in your thin client model. To configure your client to connect to the wireless network:

On the system tray, click Network and Sharing. The Networks window appears.

- Select a connection from the list of wireless connections available.
- Select Connect automatically to automatically connect to this network when you log on to Windows10 IoT.
- Click Connect.
- In the Enter the network security key field, enter the security key.

Note: If you are connecting to an unsecure network, the connection will not prompt you to enter a network security key.

Click **Next**. You are successfully connected to your chosen wireless network.

Note: A few thin client models allow you to connect a wireless LAN dongle. You can follow the same preceding instructions to configure your client to connect to the wireless network.

Configuring Printers

Depending on the available ports, the thin client can provide connectivity for USB, serial, parallel and PCI devices if appropriate software and drivers are installed.

A generic universal print driver is installed on the thin client to support text-only printing to a locally connected printer. To print full text and graphics to a locally connected printer, install the driver provided by the manufacturer and follow the manufacturer's instructions.

Note: The Write Filters should be disabled or **Commit** the files in cache using the Unified Write Filter Manger before you install the driver.

You can print to network printers from ICA and RDP applications through print drivers on the servers.

Note: Downloading and using printer driver requires free flash memory. In some cases, you may have to remove software components to free up memory for the printer driver.

Printing to a locally connected printer from an ICA or RDP session using the print drivers of the server produces full text and graphics functionality from the printer. To do this, you must install the print driver on the server and the text-only driver on the thin client, the following section provides instructions to add printers.

Follow these steps to add a printer using the text-only print driver:

1. Connect the printer to the appropriate thin client port.
2. Right-click Start > Control Panel > Devices and Printers.
3. Select Add a Printer. The Add Printer wizard appears.
4. Click **The Printer that I want isn't listed** to add a local printer. The wizard will search and display the available network printers.
5. Select Add a Local printer or network printer with manual settings and Click Next.
6. From the **Use and existing port** drop-down list, select a printer port. For example, USB
7. From the **Manufacturer** list select your printer's manufacturer and from the **Printers** list, select the model of your printer and select have disk and Click **Next**.
8. Select the correct Printer in the list and Click **Next**.
9. Select **Do Not Share this Printer** if you do not intend to share this printer with other network users.
10. Select Share this printer so that others on your network can find and use it to enable network discovery of this printer and Click Next.
11. Click **Print a test page** to print a sample print page.
12. Click **Finish**.
13. The printer is successfully added and ready to use.

Region and Location

The region and keyboard language will be set to default when you first start your Windows 10 IoT thin client. You can edit these settings based on your location and language. The default keyboard and language option is US English. To edit your region and language:

- Right-click Start > Control Panel.
- Double-click **Region**. Click the **Formats** tab, Select the keyboard format, date and time formats
- Click the **Home location** tab drop-down list. Select your location.
- Click **Copy Settings** to copy your international settings to your welcome screen, system accounts and new user account.
- Click **Change system locale,** to change the display of text in application that does not use Unicode.

Installing applications

To install an application:

- Disable UWF (requires a system restart).
- Perform the installation.

Note: If the installation process requires a system restart, you should perform that restart before proceeding to the next step

- Enable UWF (requires a system restart).
- When installing apps, it might be necessary to temporarily change some environmental variables to point to the flash drive (C :) instead of the RAM drive (Z :). The RAM drive might be too small for the temporary files cached during the installation of some apps.

Configuring application to cache on the RAM drive

You should configure apps that cache temporary files to cache on the RAM drive (Z:) to reduce the amount of write operations to the flash drive (C:). By default, the following items are cached on the RAM drive:

- Temporary user, system, and print spooling files
- Temporary Internet files (copies of websites and media saved for faster viewing)
- Website cookies, caches, and databases (stored by websites to save preferences or improve website performance)
- Browsing history

4 Remote VDI Applications

Citrix Receiver with Citrix Online plug-in

The Citrix Receiver is used to access the Citrix Presentation Server. This application allows you to place icons on the start menu or the desktop. The Citrix Receiver can be used to connect to Citrix XenApp / Presentation Server and to access hosted applications from a web interface.

The Citrix Online plug-in is used to access hosted applications or virtual desktop.

To access the Citrix Receiver:

Double-click **Citrix Receiver** icon shortcut present on desktop.

For more information on the Citrix Online Plug-in / Citrix Receiver, visit: http://support.citrix.com/proddocs/topic/receiver/rec-receiver-and-plugins.html

VMware Horizon View Client

VMware Horizon View Client is a key component of VMware Horizon View; it is an enterprise class desktop management solution, which streamlines the management, provisioning and deployment of virtual desktops. Users can securely and easily access virtual desktops hosted on VMware infrastructure, terminal servers, blade PCs or even remote physical PCs through VMware Horizon View Client.

VMware Horizon Client with PCoIP delivers a high performance desktop experience even over high latency and low bandwidth connections. The View Client with Local Mode enables end-users to enjoy secure, offline access to desktops applications and data regardless of network availability. Since desktops are tied to users' identities and not devices, desktops follow the user from device to device for ultimate freedom and mobility.

For additional information and to obtain the latest VMware View client, contact VMware or see: http://www.VMware.com/products/view

Remote Desktop Protocol Client

Remote Desktop Protocol Client allows you to establish a connection to a Windows Terminal Server. You can use the RDP client to access remote applications.

For more information about the RDP client software, visit:

http://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx

The Microsoft RDP client can be used to connect to a legacy terminal server or to a remote desktop.

The Microsoft RDP Client application on the thin client accesses Microsoft Terminal Services.

You can make Microsoft RDP available on the network using any of the following services:

- Microsoft Windows 2003 / 2008 / 2012 Server with Terminal Services installed
- Microsoft Windows Server 2003 / 2008 / 2012

To connect to a remote desktop:

- Double-click the RDP icon on the desktop.
- In the **Computer** field, enter the IP address/name of the remote computer.
- Click **Connect**.

5 Remote Management Agent

Fusion Universal Device Management Support

Fusion UDM (Universal Device Manager) Premium delivers enterprise-class device management – big-company power on a small-company budget.

Fusion UDM Professional - comprehensive device management for everyone

Fusion UDM Professional eases the transition to new virtualized environment by providing a universal management console for all thin clients running Microsoft Windows Embedded, VXL Gio6 Linux or other third party vendor Windows Embedded OS devices. Fusion UDM Professional comes as standard and is free of cost when supplied with VXL devices. For non-VXL devices a small perpetual license cost is due.

Management Suite (FUDM) is web based remote management application for managing client devices.

Fusion UDM provides features for centralized remote administration, monitoring, management, control, configuration, maintenance, up-gradation with MIS reports. This feature rich software gives administrators the ability to perform operations on multiple clients using a single point interface.

All administrative activities of clients can be managed using FUDM. One can organize the clients in groups which allows administrator to apply common settings to multiple clients by applying them to group.

To evaluate please click on the link below

http://www.vxl.net/software/fusion-udm-professional

6 Applications Support

Microsoft Applications

Windows Media Player

The Windows Media Player software is capable of playing various audio and video formats. This version has improved security and performance.

To access Windows Media Player:

1. In the Search field, type windows media player.
2. Click Windows Media Player.

For more information about the Windows Media Player visit:

http://windows.microsoft.com/en-us/windows/windows-media-player

Windows Firewall

The Windows Firewall provides basic firewall features to secure your computer from illegal access.

To configure the Windows Firewall:

Right-click Start > Control Panel > Windows Firewall

For more information about the Windows Firewall visit:

http://windows.microsoft.com/en-IN/windows-8/windows-firewall-from-start-to-finish

Internet Explorer

The latest version of the Microsoft Internet Explorer is installed on your local flash storage. The **Internet Options** has been tweaked to prevent exhaustion of the limited flash memory available.

It is recommended that you do not modify the Internet Options.

To access Internet Explorer:

1. In the Search field, type internet explorer.
2. Click Internet Explorer.

For more information about Internet Explorer, visit:

http://support.microsoft.com/find-solutions/internet-explorer/internet-explorer-11/

Microsoft Silverlight

Microsoft Silverlight is used to stream media over a network. Silverlight can also be used to represent multimedia presentations, graphics and animation.

For more information about Microsoft Silverlight, visit:

http://www.microsoft.com/silverlight/

Thin Client Administrative Applications

Thin Client Applets

The applets associated with this Windows 10 IoT are available from the Thin Client Applets tool located in **Start Menu**. This tool provides access to the various different applets that are used to manage the behavior of Windows 10 IoT.

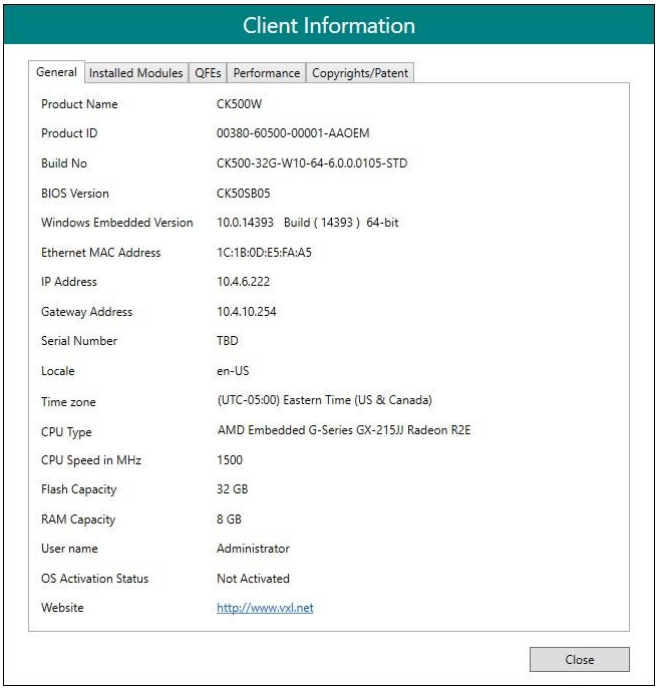


Client information

The Client Information option allows you to view the client, hardware and software information.

To access the Client Information,

- Click on **Start > Thin Client Applets** > **Client Information**.
- The Client Information Window Appears



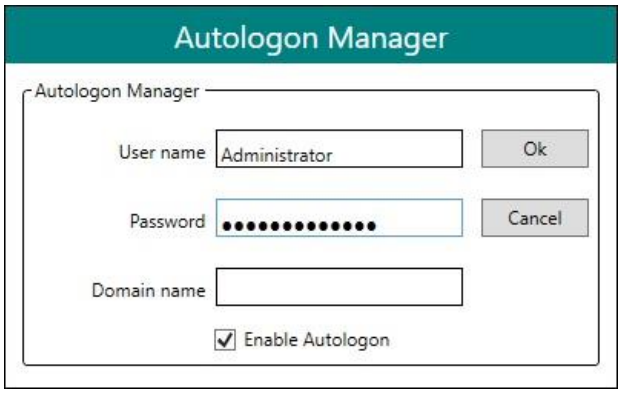
Autologon Manager

By default, a Windows 10 IoT based thin client is automatically logged on to the locked-down User account. The administrator can use the **Auto Logon Manager** in the **Thin Client Applet** from **Start Menu** to enable/disable auto logon and change the auto logon user name, password, and domain. Only the Administrator has the privileges to change auto logon properties.

Automatic Log on allows a user to log on without entering the user name and password. This type of log on is useful when using the thin client as a public access computer or any computer that does not require user access rules. For example: A school library computer.

To enable automatic logon:

1. Turn on the thin client.
2. Log on as an *Administrator*.
3. Click **Start > Thin Client Applets > Autologon Manager**. The Autologon Manager window appears.



4. In the **Username** field, enter a user name. This will be the default user name.
5. In the **Password** field, enter a password. This will be the default user password.
6. In the **Domain Name** field, enter a domain name.
7. Check **Enable Autologon**.
8. Click **OK**.
9. Restart the thin client. The User is automatically logged on.

To disable Autologon:

1. Turn on the thin client.
2. Log on as the *Administrator*.
3. Click **Start > Thin Client Applets > Autologon Manager**. The Autologon Manager window appears.
4. Uncheck **Enable Autologon**.
5. Click **OK**.
6. Restart the thin client.

Unified Write Filter (UWF)

- For information on Unified Write Filter **Refer Chapter No.2**

USB Device Controller

By default, Windows 10 IoT based thin client automatically enables all the USB peripherals. The administrator can use the **USB Device Controller** in the **Thin Client Applets** to enable as well as disable peripherals which uses interface as USB. Only the *Administrator* has the privileges to change USB device states.

USB Device Controller helps the user to protect their computer from unauthorized attempts to access devices through USB port.

To enable and disable peripherals:

1. Turn on the thin client.
2. Log on as an *Administrator*.
3. Click **Start > Thin Client Applets > USB Device Controller**. The USB Device Controller window appears.



4. Check or uncheck the devices which has to be enabled or disabled.
5. To revert back the changes click on **Revert** button.
6. Make changes and click **Apply** button.

   Scenario 1: If *Human Interface Devices* is disabled.

   1. "Disabling Human Interface Device, will disable USB Keyboards and mice. Do you want to proceed now?" message window will appear.



2. If user clicks '***Yes***', Human Interface Devices will be unchecked. **Restart** the Thin client
3. If user clicks '***No'***, all the changes will be reverted back. Return to USB Device Controller window.

Scenario 2: If any other devices are checked or unchecked and human interface devices state is not changed. **Restart** the thin client.

Note: For more information, refer MSDN link

https://web.archive.org/web/20170713151209/https://msdn.microsoft.com/en-us/library/windows/hardware/ff538820(v=vs.85).aspx

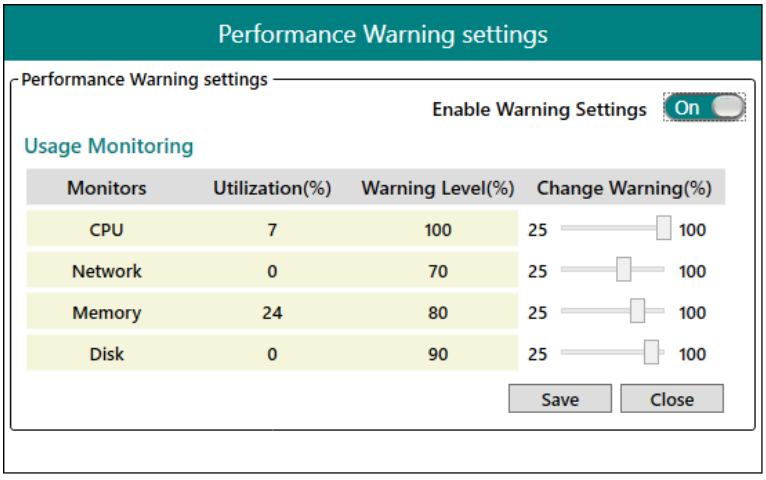
Performance Warning Settings

By using Performance Warning Settings application, you can Enable, Disable and configure Warning Settings.

By default, Warning settings will be in off Condition. Performance Warning Settings provides a visual display of real-time information about hardware Recourses (CPU, Network, Memory and Disk). In addition the Administrator privileged user can set Warning levels. Utilizations are updated in regular Interval of time. Notifications will popup if any of the monitor utilization exceeds warning level once the warning settings is enabled.

To **Enable** the *Performance Warning Settings:*

1. Log on as an Administrator.
2. Click Start > Thin Client Applets > Performance Warning settings. The Performance Warning settings window appears.



3. Click Enable Warning Settings to On Condition.
4. User can change the warning levels of CPU, Network, Memory and Disk.
5. Click **Save** to save the Changes.
6. If any one of the Monitor Utilization exceeds the warning levels, Notification window will appear.

To **Disable** Performance Warning Settings:

1. Log on as an *Administrator*.
2. Click Start > Thin Client Applets > Performance Warning settings. The Performance Warning settings window appears.
3. Click Enable Warning Settings to off Condition.
4. Click **Save** to save the Changes**.**

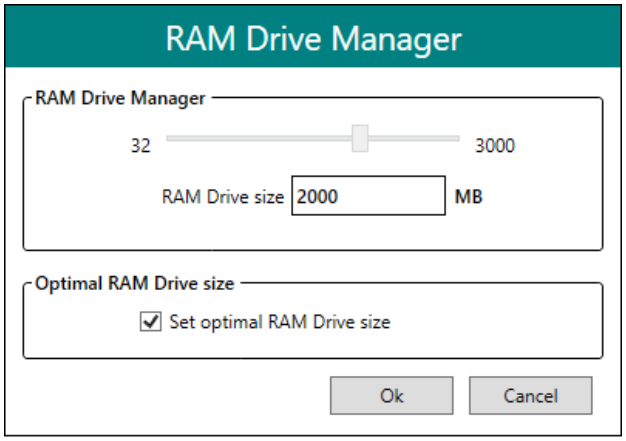
RAM Drive Manager

RAM Disk Manager allows you to configure the size of the RAM Disk drive (Z :)

- By default, the size of the RAM Disk drive is set to 256 MB.
- The maximum size of the RAM Disk drive allowed as follows,
    - For the Installed RAM of less than 3GB, RAM Disk Drive Size allowed maximum up to 500MB and the Optimal RAM Disk Drive Size will set to 350MB
    - For the Installed RAM of 3GB to 4GB, RAM Disk Drive Size allowed maximum up to 2000MB and the Optimal RAM Disk Drive Size will set to 1000MB
    - For the Installed RAM of 4GB and above, RAM Disk Drive Size allowed maximum up to 3000MB and the Optimal RAM Disk Drive Size will set to 2000MB

To set the *RAM Drive Size:*

1. Turn on the thin client.
2. Log on as an *Administrator*.
3. Click **Start > Thin Client Applets > RAM Drive Manager**. The RAM Drive Manager window appears.



4. To set the **RAM Drive size (MB)** change the slider value.
5. To use Optimal RAM Drive size, Check the **Set optimal RAM Drive size** to set the optimal RAM Drive size. After set the optimal RAM Drive Size, you can't able to change the Slider value.
6. Click **OK**, to save the RAM Drive size reboot is required.

Windows Connection Manager

Windows Connection Manager (WCM) is an application that is used to configure Windows based terminals and other supported devices with a kiosk type environment that allows easier access to virtual desktop connections. WCM enables administrative users to configure and control connections such as Citrix, VMware, RDP, and Internet Explorer (IE), while also linking them to user profiles.

The WCM enables the administrators to create a configuration file (.INI file) and a preferences file (.REG file) which can be deployed to WES7, WE8S and Win 10 IoT thin clients, as well as other supported Windows devices.

The administrator, using WCM, can automate the log on experience for users so that end-user interaction is minimized. WCM configures connections within the thin client based on the user logon information detailed within the .INI file together with any preferred display modes specified in the .REG file.

Ref WCM User Admin Guide for More details

7 Device Maintenance

This section of the guide deals with the maintenance aspects of the thin client. Some of these are performed locally on the device and some of them using FUDM.

Restoring to Factory Defaults

There are times when you may wish to place the thin client back to its factory settings. This can be achieved by use of the USB Reflash Tool. This tool allows you to re-image the SSD within the thin client using the default factory shipped OS.

To perform this task, you will first need to contact support at **http://www.vxl.net/support** and raise a ticket requesting the USB Reflash Tool and the default OS image. For licensing compliance, we will also need you to provide the serial number of the thin client together with the model and build number of the OS you require.

Once you have received the email with the instructions to download the tool and OS image file, please follow the detailed instructional guide within the package so you can image the device without any problems.

Please also ensure that you have a reliable Internet connection as some image files can be quite sizeable.

You can also re-image a WIN10-IoT thin client using FUDM and the image file. Please be aware that imaging multiple devices at the same time can have an adverse effect on network bandwidth as the images are quite sizeable.

Accessing the Thin Client BIOS

In order to access the thin client BIOS please power down the unit and then switch it back on. Repeatedly press the F1 key as soon as you power on.

Important: Do not change any settings in the BIOS that you are not sure about. Doing so may make your system inoperable.

Accessing the Boot Options menu

When you need to boot the thin client from a device other than the in-built SSD, you will need to access the Boot Options menu. This is done by repeatedly pressing the F10 key. This will display a choice of connected devices you can boot from.

Installing 3rd Party Applications

If required, you can install 3rd party applications on the WIN10-IoT thin client. To do this manually, you will need to:

- Logon as Administrator
- Disable Write Filter and reboot
- Logon as Administrator once more
- Install the application for all users
- Configure it if required
- Enable the Write Filter
- Reboot to complete the installation

You can also perform this task using FUDM. The option to install applications is located in **Device Settings > Software Deployment > Software and Patch Install/Uninstall**

8 Access Technical Support

Technical Support

Obtain support on range of thin-client hardware and its software solutions

http://www.vxl.net/support

Software Downloads

Find documentation for hardware and software, plus obtain security patches and request firmware updates for thin-client hardware.

http://www.vxl.net/support/downloads

SSD Usage and Warranty

http://www.vxl.net/support/ssd-usage-and-warranty

WES Customization

http://vxlsupport.me/

Microsoft support website (Documentation for Microsoft software)

http://support.microsoft.com

Activation in Windows 10

http://windows.microsoft.com/en-us/windows-10/activation-in-windows-10

Volume Activation for Windows 10

https://technet.microsoft.com/en-us/library/mt269358(v=vs.85).aspx

VMware support website (Documentation for VMware software)

http://www.vmware.com/support

Citrix support website (Documentation for VMware software)

http://www.citrix.com/support

Glossary

Keywords	Description
Client	A desktop computer or workstation that is capable of obtaining information and applications from a server
Dynamic Host Configuration Protocol (DHCP)	A protocol used by network administrators to centrally manage and automate the assignment of IP addresses in a network. Without DHCP, a fixed IP address needs to be assigned manually to each computer in the network. The method used to translate Internet domain names into IP addresses.
Domain Name System (DNS)	A domain name is a meaningful and easy-to-remember 'handle' for an IP address. The DNS method is based on DNS servers, which contain pre-defined and maintainable lists of domain names and IP addresses. Without this system, users would have to always remember and use IP addresses to access network computers or to browse the Internet.
Fusion UDM	A web-based device management software that provides expert management and intelligent insight of VXL's Windows Embedded thin and zero client devices.
Internet Timeserver	A time server is a server computer that reads the actual time from a reference clock and distributes this information to its clients using a computer network. The time server may be a local network time server or an internet time server
Unicode	An international encoding standard for use with different languages and scripts, by which each letter, digit, or symbol is assigned a unique numeric value that applies across different platforms and programs.
Windows Terminal Server	Remote Desktop Services in Windows Server 2008 R2, previously known as Terminal Services in Windows Server 2008 and previous versions, is one of the components of Microsoft Windows that allows a user to access applications and data on a remote computer over a network, using the Remote Desktop.

Index

A

autologon · 2

C

Citrix Presentation Server · 11

Citrix Receiver · 11

Citrix XenApp/Presentation Server · 11

Client Information · 15

Control Panel · 3

D

Default User · 6

desktop settings · 3

I

Internet Time · 8

P

print driver · 9

R

Remote Desktop Protocol · 12

S

start-up screen · 3

V

VMware Horizon Client · 11

Revision History

Version	Change Details	Authors/ Reviewers	Date
Windows 10 IoT/AG-01-18	Document creation	Girish / Ramu, Mohan	04/01/2018
Windows 10 IoT/AG-07-18	Document update	Girish / Ramu	15/02/2018