

Dell Wyse Latitude 5280 Mobile Thin Client

User Guide



Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

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

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

© 2017 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Welcome to Wyse Latitude 5280 mobile thin client

Dell Latitude 5280 is an affordable commercial-class mobile thin client that delivers relevant features to small and medium-sized businesses (SMBs). Target customers are across multiple verticals such as finance, federal, commercial, and education. Latitude 5280 mobile thin client supports Windows 10 IoT Enterprise (WIE10).



Hardware installation

Dell Wyse Latitude 5280 mobile thin client hardware installation

For more information on the hardware installation, see Dell Wyse Latitude 5280 mobile thin client Quick Start Guide.

Accessing thin client BIOS settings

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

- 1 When the system starts, press the **F2** key.
The **BIOS Setup** screen is displayed.
- 2 Change the BIOS settings as required.

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

Logging in to the Wyse Latitude 5280 mobile thin client

Whatever you view during the turn on or during the reboot of thin client device depends on the configurations done by the administrator. After creating user account, an administrator can configure a user account where a user can either automatically log in or may require user credentials to log in.

 **NOTE:**

- Ensure that you disable the Unified Write Filter (UWF) before changing a password on the thin client and enable the UWF after changing a password on the thin client.
- To change the password, hold CTRL+ALT+DEL key combination, and then click **Change a password**. However, this feature is not applicable for the **User** accounts.



Displays

Connecting to monitor

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

- HDMI port
- VGA port

For more information on configuring a dual monitor display, see [Configuring dual monitor display](#)

Configuring dual monitor display

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

To open the **Screen Resolution** window:

- 1 Log in as an administrator.
- 2 From **Start** menu, click **Control Panel > Display > Change Display Settings**.

The **Screen Resolution** window is displayed. For detailed instructions on how to configure the screen resolution, go to www.microsoft.com.

For more information about setting up multiple monitors, refer [Dell documentation](#).

Networks

Using Dynamic Host Configuration Protocol (DHCP)

A thin client is configured to obtain its IP address and network configurations from a DHCP server. The DHCP server provides the IP address or DNS name of the FTP server and the FTP root-path location of the software in Microsoft.msi. This can be used to access the FTP server by using the DHCP upgrade process.

It is recommended that you configure and upgrade thin clients by using DHCP, as it saves time and effort to complete the processes locally on multiple thin clients. If a DHCP server is not available, fixed IP addresses can be assigned, which must be entered locally for each thin client.

A DHCP server provides the IP address of the WDM server. For more information on remote administration, see [WDM software for remote administration](#)

Using Domain Name System (DNS)

Thin client devices accept valid DNS names registered on a DNS server that is available to the enterprise intranet. The thin client device sends a query to the DNS server on the network to resolve hostnames into IP addresses. DNS allows hosts to be accessed by using the registered DNS names.

The Windows DNS server in Windows 2000 and later versions includes Dynamic DNS (DDNS), and each server registers dynamically with the Windows DNS server. For information on DHCP entry of DNS domain and server location, see [Using Dynamic Host Configuration Protocol \(DHCP\)](#).



Peripherals

Configuring and using peripherals

The thin client contains the following ports and slots:

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

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

NOTE:

- You can install other services and add-ons that are available from the Dell website for free or for a licensing fee.
- For more information, see [Dell support site](#).
- You can configure the thin client device to use Bluetooth enabled Peripherals. For more information, see [configuring Bluetooth connections](#).

Configuring Bluetooth connections

You can use your thin client device with other Bluetooth enabled devices, if they have the Bluetooth capability.

NOTE:

To retain your settings, disable the UWF and configure NetXClean.

To configure your thin client for Bluetooth connections:

- 1 Log in as an administrator.
- 2 Click **Start Menu > Control Panel > Device Manager**.
The **Device Manager** window is displayed.
- 3 Expand **Bluetooth Radios**, and double-click any **Bluetooth** icon.

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

To add another Bluetooth-enabled device to the thin client device:

- a In the **control panel**, click **Devices and Printers**.

b Click **Add a Device**.

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

To turn on Bluetooth on the Bluetooth-enabled device, refer to the device documentation and follow the instructions. When the thin client identifies the device, select the device.

4 Click **Next** and follow the instructions in the wizard.



Power state

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

- 1 On the taskbar, click **Start Menu**.
- 2 From the **Start** menu, click **Power** and select any of the options:
 - **Sleep**— Your thin client starts up faster, as this mode uses very less power.
 - **Shut down**— Preferred for orderly closing of the operating system.
 - **Restart**—The thin client device is turned off and turned on instantly.

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

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

Software

Configuring connections locally

When you log in to your mobile thin client as a User, the Windows desktop displays following notable features:

- Citrix Receiver
- Remote Desktop connection
- vWorkspace connection
- VMware Horizon client
- Ericom Connect-WebConnect client

Configuring Citrix Receiver session services

Citrix Receiver is a server based on computing technology that separates the logic of an application from its user interface. The Citrix Receiver client software installed on the thin client device allows you to interact with the application GUI, while all the application processes are executed on the server.

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

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

To install the software, refer to the documentation accompanying the software. Make sessions and applications available to the thin client devices that share the server environment.

 **NOTE:**

If you use a Windows 2003/2008 Server or Citrix XenApp 5.0 with Windows Server 2008, a Terminal Services Client Access License (TSCAL) server must also be accessible on the network. The server grants a temporary license, which expires after 120 days. After the temporary license expires, you must purchase and install the TSCALs on the server.

To configure a Citrix Receiver session:

- 1 Log in as an administrator.
- 2 Access the Citrix Server by using one of the following options:
 - From the **Start Menu**, click **Citrix Receiver**.
 - Double-click the **Citrix Receiver** icon on the desktop.

After you log in to the Citrix Server, the **Add Account** window is displayed.

- 3 In the **Add Account** window, enter the Server IP address, and then click **Next**.
- 4 For secure connections, enter Fully Qualified Domain Name (FQDN); for non-secure connections, enter the IP address.
- 5 Enter the user credentials, and click **Log on**.

You can add an account by providing the IP address, and you can view the details of the Citrix Receiver.

- 6 Click **Yes**, and then click **Next**.



The Virtual desktop of the Citrix Receiver is displayed.

- 7 In the **Virtual desktop** window, click **Add Apps (+) > All Applications**.

You can select or clear the application check boxes. The selected applications are displayed on the virtual desktop.

- 8 On the virtual desktop, click **Settings** to:

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

Configuring the Remote Desktop Connection session services

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

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

NOTE: If you use a Windows 2003/2008 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, you must purchase and install the TSCALs on the server. You cannot make a connection without a temporary or permanent license.

To configure a **Remote Desktop Connection**:

- 1 Log in as a user or administrator.
- 2 From the **Start** menu, click **Remote Desktop Connection**, or double-click the **Remote Desktop Connection** icon on the desktop.

The **Remote Desktop Connection** window is displayed.

- 3 In the **Computer** box, enter the computer or the domain name.

- 4 For advanced configuration options, click **Show Options**.

- In the **General** tab, you can enter the logon credentials, edit or open an existing RDP connection, or save a new RDP connection file.
- 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.
- 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.
- In the **Experience** tab optimize the performance of your remote session based on the connection quality.

NOTE:

If you find that the Unified Write Filter cache is filling up, disable the Bitmap caching in the **Experience** tab.

- In the **Advanced** tab, select the action that should be taken when the server authentication fails and configure settings for connection through Remote Gateway.

- 5 Click **Connect**.

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

The remote desktop is displayed with the connection bar on the top if you have selected the **Display the connection bar when I use the full screen** check box in step 3 b.

Configuring vWorkspace connection

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

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

To configure a vWorkspace connection:

- 1 Log in as a user or administrator.
- 2 from the **Start** menu, click **Dell Wyse vWorkspace**, or double-click the **vWorkspace** icon on the desktop.
The **vWorkspace** window is displayed.
- 3 In the **vWorkspace** window, enter the vWorkspace Server IP, or your registered email address or website address, and then press **Enter**.

NOTE: To retrieve your connector configuration from the vWorkspace server, enter the **Username**, **Password**, and **Domain credentials** and then select the **Save Credentials (encrypted)** check box if you want to save your login credentials.

- 4 Select your preferred vWorkspace Farm location from the following options:
 - Inside Office
 - Outside Office
- 5 Click **Connect**.
- 6 In the **Login Credentials** dialog box, enter the following credentials to connect to the vWorkspace Farm:
 - Username
 - Password
 - Domain

If you are successfully connected, then the **vWorkspace Farm** screen is displayed.

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

Configuring vWorkspace Farm

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

- 1 To view the configuration options available, click **vWorkspace Farm**.
- 2 To configure your vWorkspace Farm settings, click the **Settings** icon .
 - a To allow auto connect to the specified configuration upon startup, select the **Automatically connect to this configuration on startup** check box
 - b From the drop-down list, select the location where you want to deploy the vWorkspace Farm. The available options are:
 - Always prompt for location.
 - Use Location Inside Office
 - Use Location Outside Office
 - c In the **Display settings** section, configure the following options:
 - From the **Screen resolution** drop-down list, select your preferred screen resolution for your vWorkspace session.
 - Select the following check boxes as per your requirements:



- Use all my monitors for the remote session
- Display connection bar
- Pin connection bar

d In the **Device settings** section, configure the following options:

- Select the following check boxes as per your requirements:
 - Play audio
 - Use USB devices
 - Use microphone
- To select additional devices and resources on your computer that you want to use in your remote session, click **More Devices**.

- 3 Click **OK** to save your settings.
- 4 Click the **Delete** icon, if you want to delete the configured vWorkspace Farm.
- 5 To view the Name, Type, and Timestamp of your vWorkspace Farm, click the **Info** icon.

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

The upper pane of the **vWorkspace Farm** page contains the following options (not mandatory) for advanced configuration.

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

Connecting to a virtual desktop by using VMware Horizon Client

VMware Horizon Client is a locally installed software application that communicates between View Connection Server and thin client OS. It provides access to centrally hosted virtual desktops from your thin clients.

VMware session services can be made available on the network after you install the VMware Horizon 6. It provides virtualized or hosted desktops and applications through a single platform to end users.

To connect to a virtual desktop by using VMware Horizon:

- 1 Log in as a user or administrator.
- 2 Access the **VMware Horizon client** window by using one of the following options:
 - From the **Start Menu**, click **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, do the following as per your requirements:
 - 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 provided field.
 - c Click **Connect**.
 - d In the **Login** dialog box, enter the user name and login password in the respective boxes.

e From the **Domain** drop-down list, select the domain where the server is located.

f Click **Login**.

The VMware Horizon Client connects to the selected desktop. After connection is established, the list of published desktops are displayed.

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

For more information, refer to the VMware Horizon Client documentation on www.vmware.com.

 **NOTE:**

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

To access 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 any of the following options based on your requirements:

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

Using Ericom Connect-WebConnect client

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

• To access Ericom Connect-WebConnect Client as a stand-alone:

a Log in as a user or administrator.

b From the **Start Menu**, click **Ericom Connect-WebConnect client** or double-click the **Ericom Connect-WebConnect client** icon on the desktop.

The **Ericom AccessPad** login window is displayed.

c In the **Ericom AccessPad** Login window, enter your login credentials, and click **Login**.

The **DELL – Ericom Application Zone** window is displayed.

 **NOTE:** By default, the Ericom AccessPad login window is displayed in English (US). To set the UI to your preferred language, click the Globe icon in the lower-right corner of the window, and select your preferred language from the drop-down list.

d In the **DELL – Ericom Application Zone** window, the **Blaze demo server**, **RDP demo server**, **Ericom server**, and **Paint** applications are displayed.

Double-click any of these applications to access them.

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

e To create a shortcut on your desktop window, click **Options > Create a shortcut on Desktop** in the **DELL – Ericom Application Zone** window.

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

• To access the Ericom Connect-WebConnect client through a web browser:

a Double-click the **Internet Explorer** icon.

The **Internet Explorer** web page is displayed.

b To access the Ericom Power Term Emulation, enter the URL <http://serverIP/FQDNWebConnect6.0/AppPortal/Index.asp>.
The **PowerTerm WebConnect Application Portal** page is displayed.

c In the **PowerTerm WebConnect Application Portal** page, enter the login credentials and also specify the domain name, then click **Login**.

d After you Log in, Published desktops and applications such as the **Blaze demo server**, **RDP demo server**, and **Paint** are displayed.
Double-click any of these applications to access them on a new web page.

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



- e To end the Ericom Power Term WebConnect session, click **Logout** on the left side of the **PowerTerm WebConnect Application Portal** page.

Management interface

WDM software for remote administration

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

WDM provides the following important features:

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

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

Configuring Wyse Device Agent (WDA) settings

Wyse Device Agent enables you to configure/register the client to connect to Wyse Device Manager (WDM) / Cloud client Manager (CCM) server and performs auto discovery for searching the available management server in the order of WDM and CCM.

The following are three types of registrations in WDA:

- Auto Discovery
- WDM Registration
- CCM Registration

Auto Discovery

The **Auto Discovery** option in the WDA UI enables WDA to search the available management servers and register the thin client on the respective server in the order of WDM and CCM.



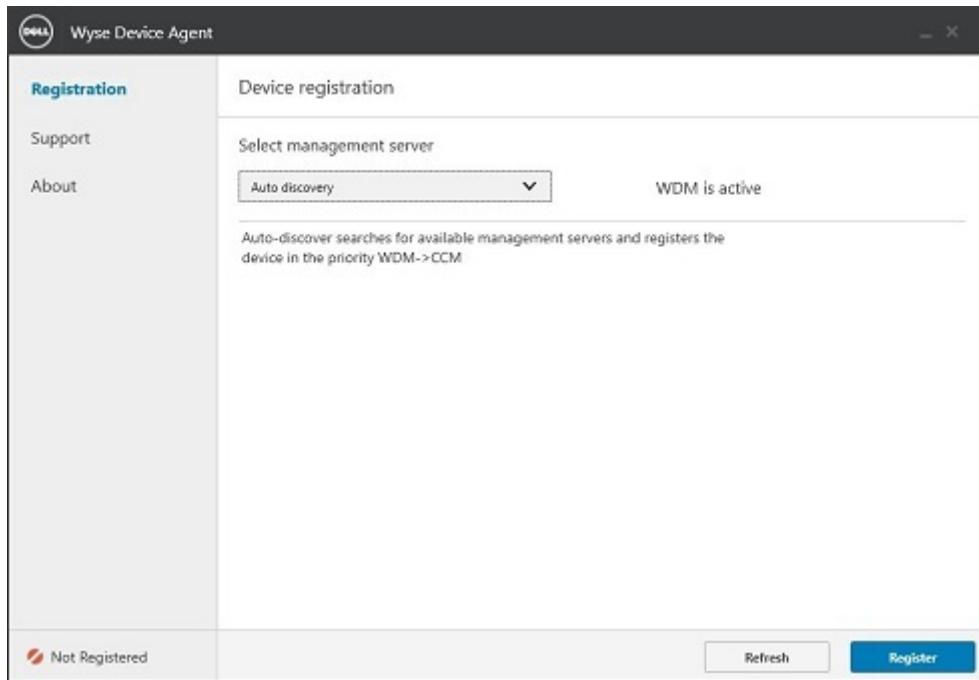


Figure 1. Auto discovery

The **Auto Discovery** option searches in the order of WDM and CCM and gets connected to the management server that is available.

Configuring WDM by using WDA

- 1 In the WDA UI, enter the IP address or FQDN of the WDM server.

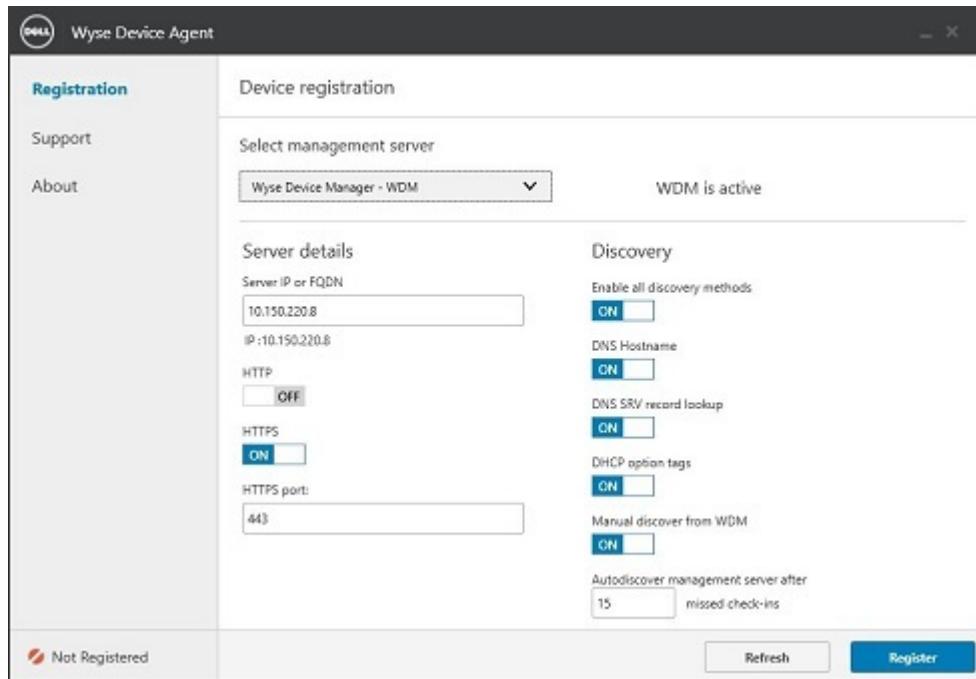


Figure 2. Device registration

- 2 To enable or disable the required type of server, click the **On/Off** button.
- 3 Enter the WDM server port number in the **HTTPS port** field. The default value is 443.

NOTE: Whenever Client is registered to a WDM server, all the details that are configured for discovery are taken from that WDM server.

- 4 To connect with WDA Management Server, enable any of the following WDA discovery options:
 - Enable all discovery methods.
 - DNS Hostname
 - DNS SRV record lockup
 - DHCP option tags
 - Manual discover from WDM.
- 5 To automatically discover the management, set the time interval in the **Autodiscover management server after** field.
- 6 Click **Register**.

Configuring CCM by using WDA

- 1 From the **Select management server** drop-down list, select **Cloud Client Manager-CCM**.

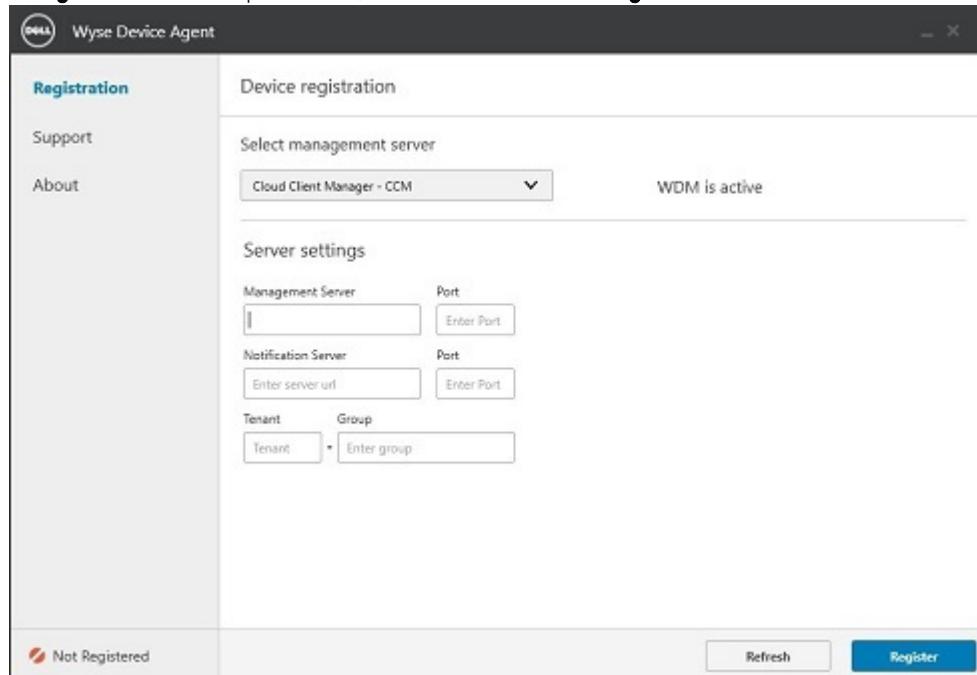


Figure 3. Device registration

- 2 In the **Server settings** section, do the following:
 - In the **Management Server** field, enter the IP address of the CCM management server; in the **Port** field, enter the CCM server port number.
 - In the **Notification Server** field, enter the MQTT server url; in the **Port** field, enter the MQTT server port number.
 - In the **Group** field, enter the group token of the CCM management server.
- 3 Click **Register**.

System specifications

The following table provides the specification of the Wyse Latitude 5280 mobile thin client:

Table 1. System specifications

Features	Latitude 5280
Processor type	Intel Kaby Lake i5 processor
Chipset	Integrated with the processor
Flash and memory	8 GB (DDR4L, 2133 MHz) RAM 128 GB M.2 SSD
Storage	128 GB M.2 SSD
Display	12.5" (16:9) HD panel eDP 1.3 1920 x 1080 FHD resolution
Graphic solutions	· Intel HD Graphics 620
Multimedia	Front facing HD camera (supports Windows 10 face recognition) Integrted digital microphone (dual array) Integrated ave Maxx Audio Pro audio Microsoft Skype for Business Logo Two stereo speakers
Ports, slots, and chassis	HDMI (1.4) ports Universal audio jack Multimedia/flash card reader (SD 4.0) 3 x USB 3.0 1 x USB Type-C Bluetooth 4.x
Connectivity options	10/100/1000Mbps Ethernet through RJ45 WiFi 802.11 a/b/g/n/ac WWAN Cat6 2CA for three US Carriers on (Verizon, AT&T, and Sprint) and three Japanese carriers (Softbank, KDDI, Docomo) through M.2 IPv6 ITES compliant USB-C dock support

Features	Latitude 5280
	Bluetooth BT 4.x through WLAN card
I/O	1 x VGA 1 x DisplayPort 1 x USB 2.0 2x USB 3.0 Media card reader 1.3-megapixel camera
Operating Systems	<ul style="list-style-type: none"> Windows 10 IoT Enterprise Redstone 64-bit
BIOS	UEFI BIOS
AC adapter	45 W AC adapter
Weight	3.0 lbs
Dimensions	21.4 x 305.15 x 211.3 mm



Troubleshooting

Enhanced Pre-Boot System Assessment (ePSA) diagnostics

The ePSA diagnostics (also known as system diagnostics) performs a complete check of your hardware. The ePSA is embedded with the BIOS and is launched by the BIOS internally. The ePSA diagnostics provides a set of options for particular devices or device groups, enabling you to:

- Run tests automatically or in an interactive mode
- Repeat tests
- Display or save test results
- Run thorough tests to introduce additional test options to provide extra information about the failed device(s)
- View status messages that inform you if tests are completed successfully
- View error messages that inform you of problems encountered during testing

△ CAUTION: Use the system diagnostics that comes with your software to test only your computer. Using this program with other computers may cause invalid results or error messages.

○ NOTE: Some tests for specific devices require user interaction. Always ensure that you are present at the computer terminal when the diagnostic tests are performed.

Running the ePSA diagnostics

- 1 Start up the computer.
- 2 As the computer boots, press the F12 key.
- 3 On the boot menu screen, select the **Diagnostics** option.
The **Enhanced Pre-boot System Assessment** window is displayed.
- 4 Click the arrow key at the bottom left corner.
The Diagnostics front page is displayed.
- 5 Press the arrow in the lower-right corner to go to the page listing.
The detected items are listed.
- 6 To run a diagnostic test on a specific device, press Esc and click **Yes** to stop the diagnostic test.
- 7 Select the device from the left pane and click **Run Tests**.
If there are any issues, error codes are displayed, note the error code and validation number and contact Dell.