Dell Wyse 3030 LT
User Guide

Regulatory Model: N06D
Regulatory Type: N06D001

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.

2016 - 07

Rev. A00

1

Welcome to Dell Wyse 3030 LT thin client

Dell Wyse 3030 LT thin client enhances the user's multimedia experience with its integrated graphics engine and provides multiple connectivity choices for an excellent virtual desktop solution. These thin clients have a dual core Intel 1.6GHz processer, which delivers high performance experience to the end users and allows easy deployment of ready to connect to Citrix, Microsoft, VMware, and Dell vWorkspace. The 3030 LT has various configuration options which support a wide variety of interfaces and peripherals. Wyse 3030 LT thin clients are ideal choice for virtual desktop environments because of easy deployment and management across remote sites.

About this guide

This guide is intended for Wyse 3030 LT thin clients running either Dell Wyse ThinLinux or Dell Wyse ThinOS. It provides hardware specifications and OS specific configurations to help you work with Wyse 3030 LT thin clients.

Dell Wyse external references

This section provides links to technology related support and self-service sites for **Dell Wyse Thin Clients**.

- Dell reference guides — User, Administrator, Quick Start Guide, and related documentation
- Dell Wyse Technology End User License Agreement
- Dell service and support — Latest software images
- Dell Wyse Device Manager — Information about Dell remote management software
- Dell and the Environment — Information about Dell compliance with RoHS and with the Waste Electrical and Electronic Equipment (WEEE)
- Dell and e-Recycling — Information about recycling and reuse of Dell products
- Dell product registration — Register your product

2

Installation and setup

This section describes about the following topics:

- Wyse 3030 LT thin client hardware setup.
- Wyse 3030 LT thin client BIOS configuration.

Wyse 3030 LT thin client hardware installation

For more information on the hardware installation, see ***Dell Wyse 3030 LT thin client Quick Start Guide***.

Accessing thin client BIOS settings on Wyse ThinOS

After starting your thin client you will see a Dell logo for a short period of time. During this period you can press and hold the **Delete** key to enter the BIOS with **Fireport** as the password to make necessary modifications. For example, you can use the F7 key to use Optimized Defaults (load optimal default values for all the items in the BIOS setup utility).

Accessing thin client BIOS settings on Wyse ThinLinux

This section describes about the 3030 LT thin client BIOS settings.

How to invoke BIOS settings and select boot source

The standard BIOS features and boot options are common to all platforms with the following boot options:

- Boot from **HardDisk** –Boots from the internal SSD storage.
- Boot from **USB** – Boots the USB storage from any of the USB ports (this option is disabled by default).
- Boot from **PXE** – Boots from the network through PXE.
- Boot from **CLOUD** – Not supported by ThinLinux.

The following are the BIOS Hot Key functions while booting:

- **P-Key** – The key invokes to the boot selection menu. It is used to select or alter the temporary boot order.
- **Del-key** – The key invokes to the BIOS settings. The BIOS settings is protected by a password and the default password is **Fireport**.

3

Logging on to the Wyse 3030 LT thin client

This section includes the following topics:

- Logging on to the Wyse 3030 LT running ThinOS.
- Logging on to the Wyse 3030 LT running ThinLinux.

Logging on to the Wyse 3030 LT running ThinOS

What you see after logging on to the server depends on the administrator configurations.

- **Users with a Classic Desktop** - will see the classic ThinOS desktop with full taskbar, desktop, and Connect Manager familiar to ThinOS users. This option is the default out-of-the-box experience and is recommended for terminal server environments with published applications and for backward compatibility with ThinOS 6.x versions.
- **Users with a Zero Desktop** - will see the Zero Desktop with the Zero Toolbar showing the assigned list of connections from which to select. This option is recommended for VDI and any full-screen only connections.

In any desktop case, you can select the desktop option you want (Classic Desktop or Zero Desktop) and create the connections you need using the Visual Experience tab on the **Remote Connections** dialog box.

To open the **Remote Connections** dialog box, perform one of the following tasks:

- **Classic Desktop** — Click User Name , and then select **System Setup** → **Remote Connections**.

  NOTE: User Name is the user who is logged-on and is located at the lower-left pane of the taskbar
- **Zero Desktop** — Click the **System Settings** icon on the Zero Toolbar, and then select **Remote Connections**.

Logging on to the Wyse 3030 LT running ThinLinux

On your initial configuration, Dell recommends that you connect by using a wired connection by plugging in the network connected Ethernet cable to your thin client.

After you turn on your thin client, you are automatically logged in to the local **thinuser** account. By default, the password of the thinuser account is set to **thinuser**.

NOTE: In cases where a GDM login is needed (for example, AD/Domain login, PNAgent login and so on), the auto-login option can be turned off through the GUI or by using the INI.

Admin mode enables you to perform system administration tasks such as adding or removing connections and setting up specific device settings. To enter into the **Admin** mode, click the **Switch to Admin** button from **Setting application** screen to admin mode and then enter the default root password in the **Password Needed** window. The default root password is **admin**.

4

Displays

This section provides information about the multiple monitor configurations.

Multiple monitor configurations

Wyse 3030 LT thin clients running ThinOS

Depending on your thin client model, connections to monitors can be made using either a DisplayPort, or a proper Dell monitor cables/splitters/adapters.

For information about configuring dual head display settings, see Configuring the Dual Head display setting on ThinOS.

Wyse 3030 LT thin clients running ThinLinux.

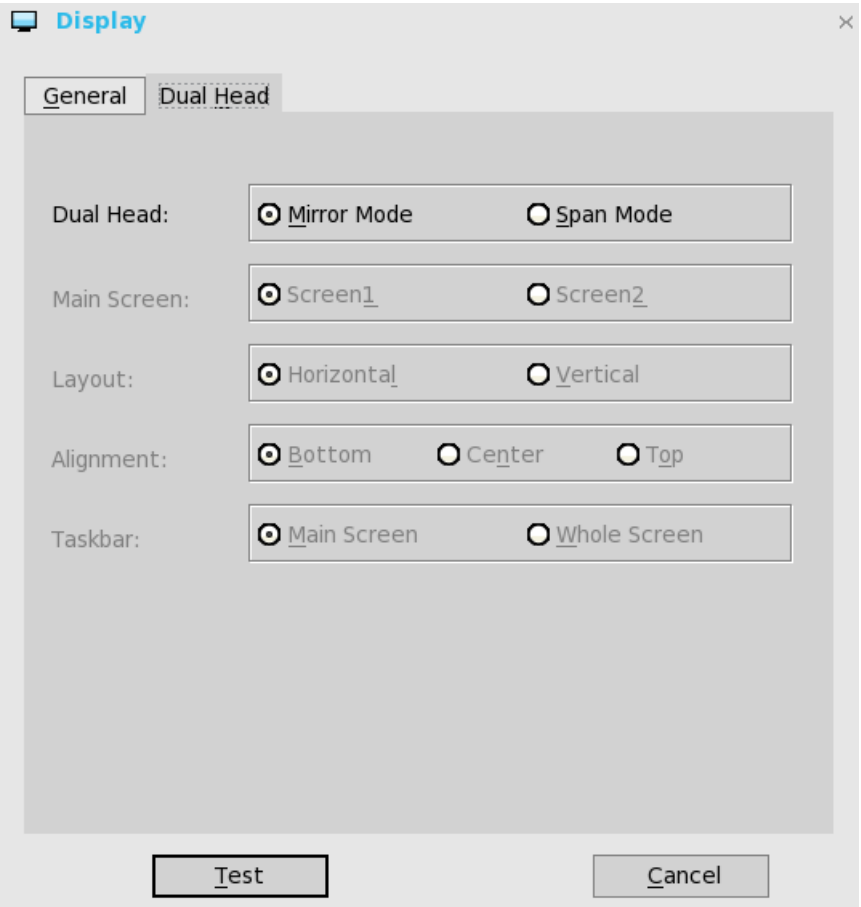
In a Dual-monitor configuration, if both monitors are connected, then by default, the monitors are in span mode. The primary monitor is on the left (monitor 1) and the secondary monitor is on the right (monitor 2). The resolutions of the monitors are auto detected by the system by analyzing the monitor's capabilities.

For information about configuring dual head display settings, see Customizing your display on ThinLinux.

Configuring dual Head display settings on Wyse ThinOS

To configure the Dual head display settings:

1. From the desktop menu, click **System Setup**, and then click **Display**.
   The **Display** dialog box is displayed.
2. Click **Dual Head** tab, and use the following guidelines:



This feature is applicable for supported Dual Monitor Capable Thin Clients Only.

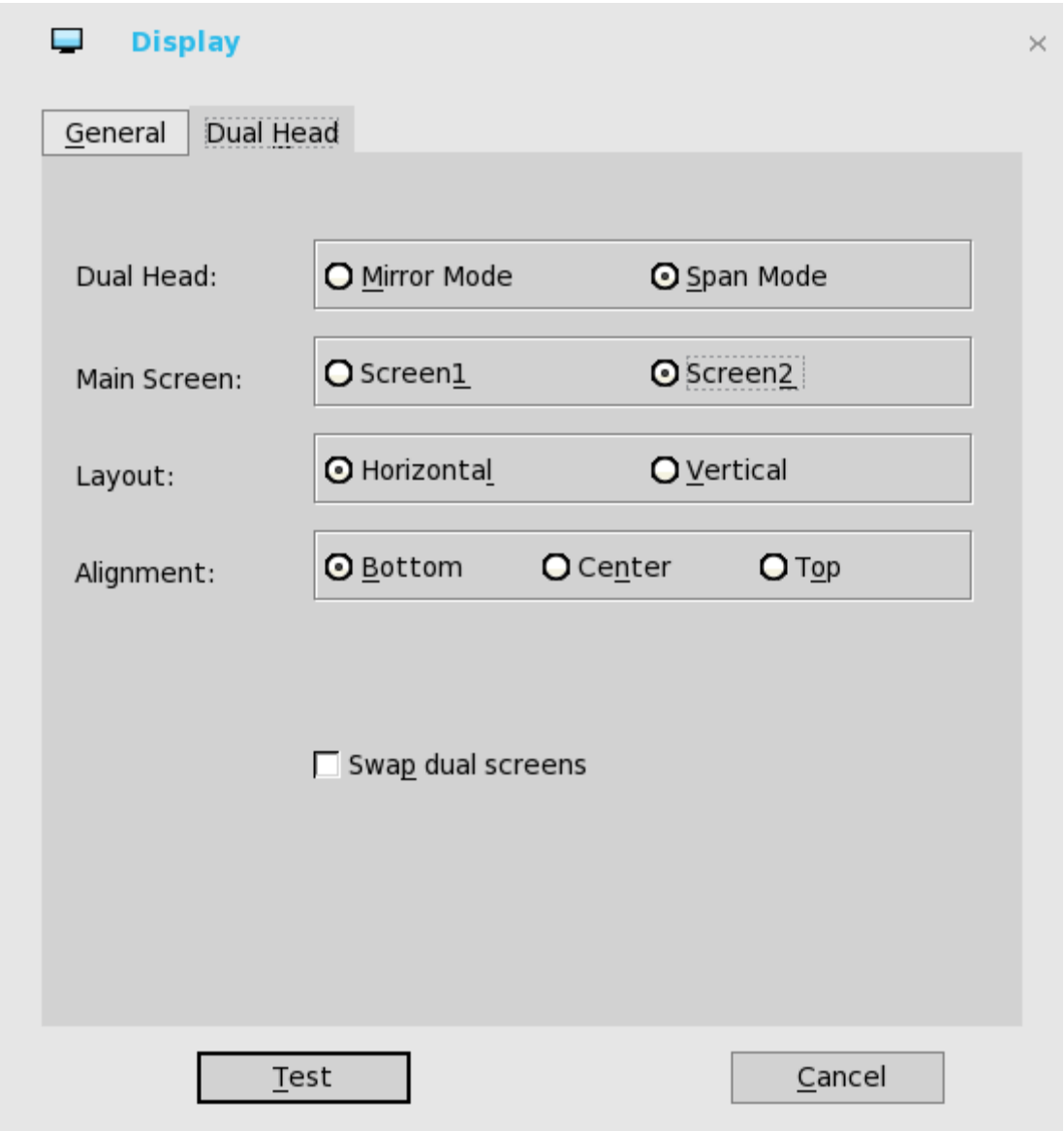
a. Select **Mirror Mode** option from **Dual Head** to have the two monitors work in a matching state, or **Span Mode** to have the two monitors work separately second is extended from first.
b. Select which of the two monitors you want to be the main screen - **Screen1** or **Screen2** from **Main Screen** option. The other screen is extended from the main screen.
c. Select how you want the two monitors to be oriented to each other through the **Layout** option.

   Horizontal—where you move between the monitors from the left and right of the screens.

   Vertical—where you move between the monitors from the top and bottom of the screens.
d. **Alignment**—Select how you want the monitors to be aligned **Bottom**, **Center**, or **Top**.

   Bottom means that screens are bottom-aligned in a horizontal orientation; Center means that screens are center-aligned; Top means screens are top-aligned in a horizontal orientation.
e. **Taskbar (Classic Desktop Only)**—Select under which screen you want the Taskbar to appear **Whole Screen** or **Main Screen**

   Gamma Supported Monitors Only—Use the Gamma Setup tab to adjust the saturation values for Red, Green, and Blue on VGA connected monitors supporting ggamma settings, if you feel the default settings are too light. The Gamma Setup tab is disabled once you click **Save+Exit**. You can enable it again by setting gamma={1-100} ggamma={1-100} bgamma={1-100} in the Resolution INI parameter. For more information, see *Dell Wyse ThinOS INI Guide*.



For Swap dual screens, when you set Main Screen to Screen2, an extra check box is displayed at the bottom of the tab that allows you to swap dual screens. If you clear the check box, the Screen1 is usually the left one or the top one in dual display. When you set Main Screen to Screen2, the main screen is changed to the right screen or bottom screen. If you select the **swap dual screens** check box, you are able to set Main Screen to Screen2, but still have it at the left side or the top side, which is considered more user friendly.

Customizing your display on ThinLinux

By default, the **Customize your display** screen is available in both User mode and Admin mode. Any changes to display preferences made through this screen is saved and available for the built-in thinuser. In a **Dual-monitor** configuration, if both monitors are connected, then by default, the monitors are in extended mode. The **primary monitor** is on the left (monitor 1) and the **secondary monitor** is on the right (monitor 2). The resolutions of the monitors are auto detected by the system by analyzing the monitor's capabilities.

1. Click the **Display** tab.
   The **Customize Your Display** page is displayed.

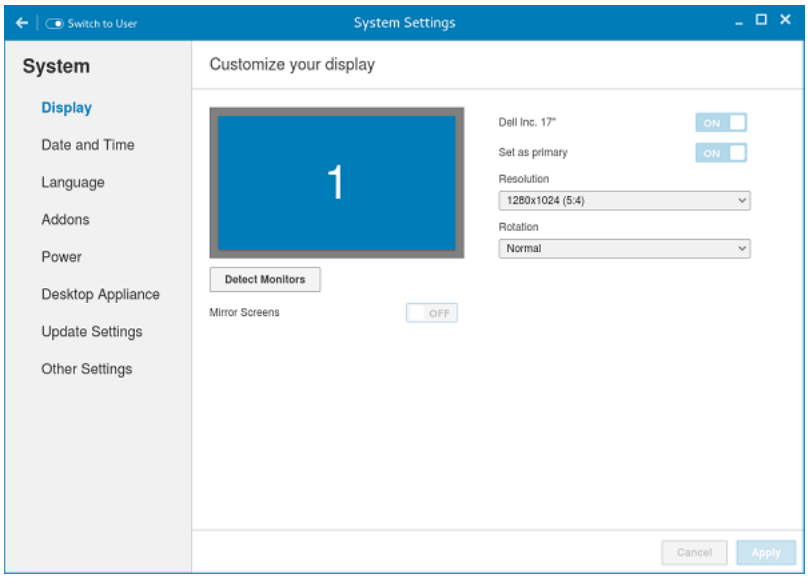


Figure 1. Display Settings

2. Select the preferred **Resolution** from the drop-down list.
3. Select the **Rotation** type from the drop-down list.
   - Normal
   - Right
   - Left
   - Upside-down
4. Click the **ON/OFF** button to switch between dual display and mirror mode in a dual monitor configuration.
5. Click the **ON/OFF** button to enable the **Set as primary** option. This option allows you to set the selected monitor as primary.
6. Click the **ON/OFF** button to enable the **Monitor On/Off** option. This option allows you to switch off and switch on the preferred monitor in a dual monitor configuration.

5

Networks

This section describes about the network configurations of Wyse 3030 LT running either ThinOS or ThinLinux.

- For network configurations on ThinOS, see Configuring the network settings on ThinOS.
- For network configurations on ThinLinux, see Configuring the network settings on ThinLinux.

Configuring the network settings on ThinOS

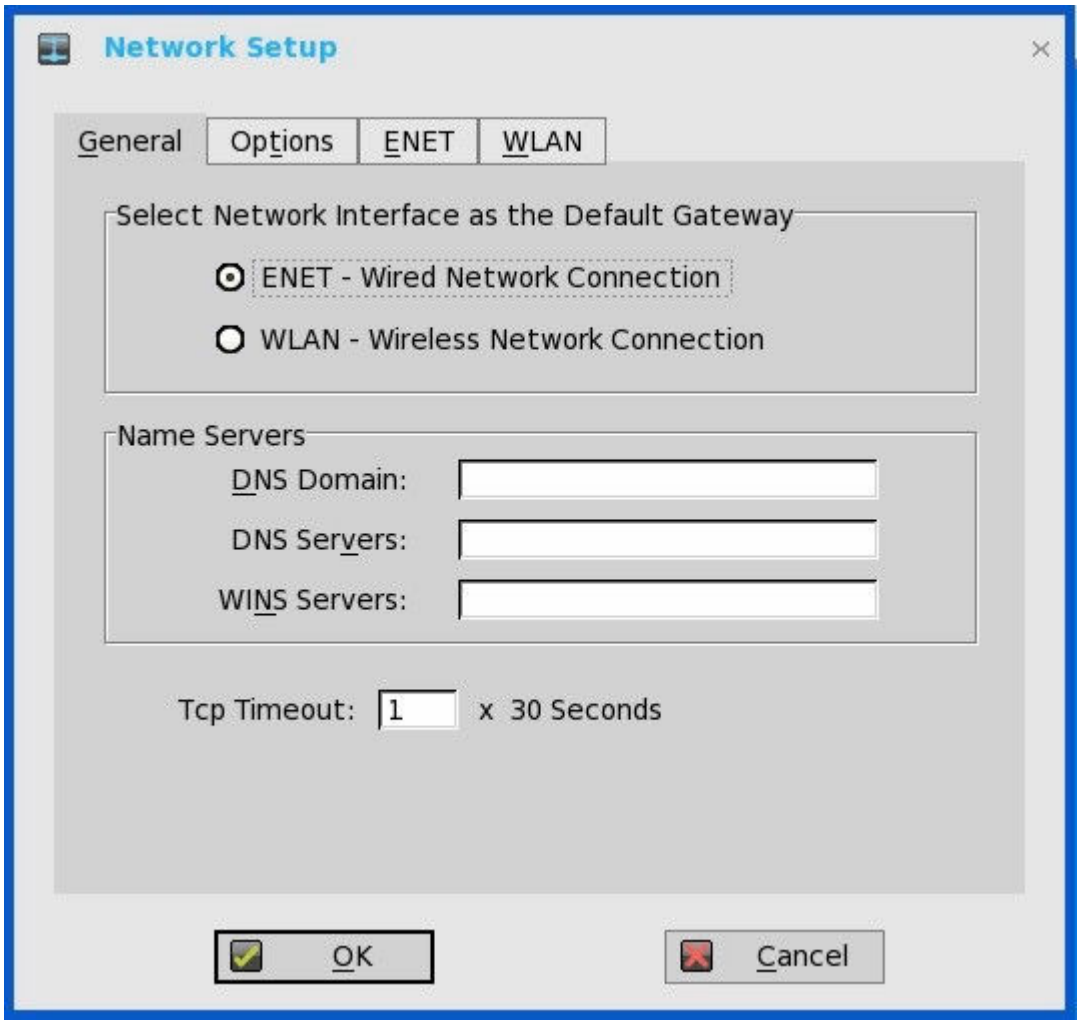
To configure the network settings use the following options:

- Configuring the General settings.
- Configuring the Options settings.
- Configuring the ENET settings.
- Configuring the WLAN settings.

Configuring general settings

To configure the general network settings:

1. From the desktop menu, click **System Setup**, and then click **Network Setup**.
   The **Network Setup** dialog box is displayed.



2. Click the **General** tab, and use the following guidelines:
   a. To set the default gateway, select the type of network interface from the available options.
      1. **Single Network support**—Either wireless or wired network is connected.
         - **ENET**—Click this option, if you want set up the Ethernet Wired Network Connection.
         - **WLAN**—Click this option, if you want set up the Wireless Network Connection.
         - If the user use wireless network after selecting ENET connection or wired network after selecting WLAN connection, then the system log "WLAN: Set default gate way xxx.xxx.xxx.xxx"for first case and"ENET: Set default gate way xxx.xxx.xxx.xxx" for second case are printed to ensure that the UI setting reflects the actual usage.

         NOTE: The User Interface (UI) will not be changed automatically.
      2. **Dual Network support** — Both wireless and wired networks are connected. The default gateway is determined by the UI settings.
   b. Enter the URL address of the DNS Domain in the **DNS Domain** box.
   c. Enter the IP address of the DNS Server in the **DNS Server** box.

   Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. Enter the DNS Domain and the network address of an available DNS Server. The function of the DNS Domain entry is to provide a default suffix is used in name resolution. The values for these two boxes may be supplied by a DHCP server. If the DHCP server

supplies these values, they replace any locally configured values. If the DHCP server does not supply these values, the locally configured values are used.

NOTE: You can enter up to 16 DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server, and the rest are secondary DNS servers or backup DNS servers.

d. Enter the IP address of the WINS Server in the **WINS Server** box.

Use of WINS is optional. Enter the network address of an available WINS name server. WINS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it is used to make the connection. These entries can be supplied through DHCP, if DHCP is used. DNS and WINS provide essentially the same function, name resolution. If both DNS and WINS are available, the thin client attempts to resolve the name using DNS first and then WINS.

You can enter two WINS Server addresses (primary and secondary), separated by a semicolon, comma, or space.

e. Enter the digit multiplier of 30 seconds in the **TCP Timeout** box to set the time-out value of a TCP connection. The value must be **1** or **2** which means the connection time-out value is from 1x30= 30 seconds to 2x30= 60 seconds. If the data for connecting to the server is not acknowledged and the connection is time out, setting the time-out period retransmits the sent data and again tries to connect to the server until the connection is established.

3. Click **OK** to save the settings.

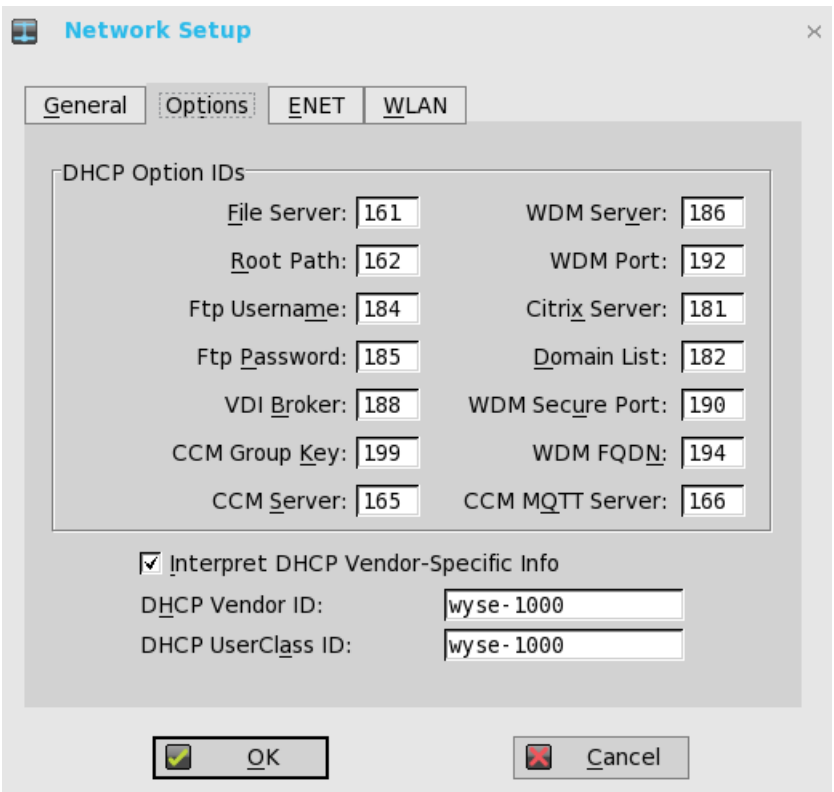
Configuring the DHCP Options Settings

To configure the options settings:

1. From the desktop menu, click **System Setup**, and then click **Network Setup**.

   The **Network Setup** dialog box is displayed.

2. Click the **Options** tab, and use the following guidelines:



a. **DHCP Option IDs** — Enter the supported DHCP options. Each value can only be used once and must be between **128** and **254**.

b. **Interpret DHCP Vendor-Specific Info** — Select this check box for automatic interpretation of the vendor information.

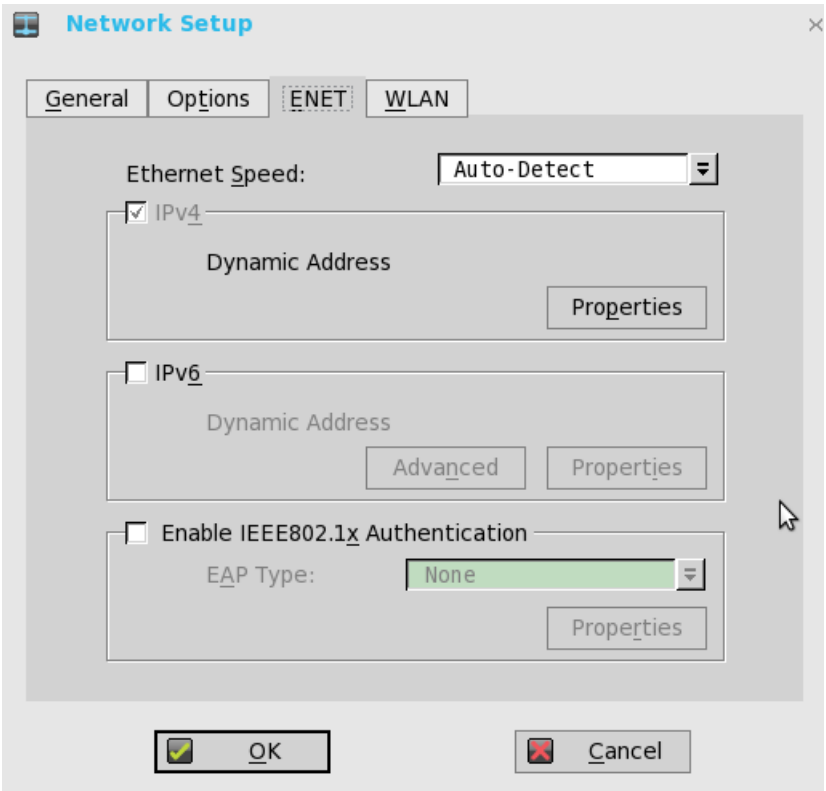
c. **DHCP Vendor ID** — Shows the DHCP Vendor ID when the dynamically allocated over DHCP/BOOTP option is selected.
d. **DHCP UserClass ID** — Shows the DHCP UserClass ID when the dynamically allocated over DHCP/BOOTP option is selected.

3. Click **OK** to save the settings.

Configuring ENET settings

To configure the ENET settings:

1. From the desktop menu, click **System Setup**, and then click **Network Setup**.
   The **Network Setup** dialog box is displayed.
2. Click the **ENET** tab, and use the following guidelines:



a. **Ethernet Speed**—Normally the default (**Auto-Detect**) should be selected, but another selection can be made if automatic negotiation is not supported by your network equipment. The selections include **Auto-Detect**, **10 MB Half-Duplex**, **10 MB Full-Duplex**, **100 MB Half-Duplex**, **100 MB Full-Duplex**, and **1 GB Full-Duplex**.
   The **10 MB Full-Duplex** option can be selected locally at the device, however, this mode may need to be negotiated through **AutoDetect**.
b. The **IPV4** check box is selected by default. Click **Properties** to set various options supported by IPV4.
   - **Dynamically allocated over DHCP/BOOTP**—Selecting this option enables your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server using DHCP options to provide information. Any value provided by the DHCP server replaces any value entered locally on the Options tab, however, locally entered values are used if the DHCP server fails to provide replacement values.
   - **Statically specified IP Address**—Select this option to manually enter the IP Address, Subnet Mask, and Default Gateway:
     - **IP Address**—Must be a valid network address in the server environment. The network administrator must provide this information.

- **Subnet Mask**—Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices: Same subnet or other subnet. If the location is other subnet, messages sent to that address must be sent through the Default Gateway, whether specified through local configuration or through DHCP. The network administrator must provide this value.
- **Default Gateway**—Use of gateways is optional. Gateways are used to interconnect multiple networks—routing or delivering IP packets between them. The default gateway is used for accessing the internet or an intranet with multiple subnets. If no gateway is specified, the thin client can only address other systems on the same subnet. Enter the address of the router that connects the thin client to the internet. The address must exist on the same subnet as the thin client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.

c. Select the **IPV6** check box, and then click **Advanced** to select various IPV6 supported setting options from the available check boxes.

d. Click **properties**, and use the following guidelines:

- **Wait DHCP**—Selecting this option enables your thin client to wait for IPV6 DHCP before the sign-in, if not selected the system waits for IPV4 DHCP if enabled.
- **Dynamically allocated over DHCP/BOOTP**—Selecting this option enables your thin client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server, using DHCP options, to provide information. Any value provided by the DHCP server replaces any value entered locally on the **Options tab**, however, locally entered values are used if the DHCP server fails to provide replacement values.
- **Statically specified IP Address**—Select this option to manually enter the IP Address, Subnet Mask, and Default Gateway.
  - **IP Address**—Must be a valid network address in the server environment. The network administrator must provide this information.
  - **Subnet Mask**—Enter the value of the subnet mask. For more information, see various options supported by IPV4 in this section.
  - **Default Gateway**—Use of gateways is optional. For more information, see various options supported by IPV4 in this section.
- **DNS Servers**—Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS is used to make the connection. Enter the network address of an available DNS Server. The value for this box may be supplied by a DHCP server. If the DHCP server supplies this value, it replaces any locally configured value. If the DHCP server does not supply this value, the locally configured value is used.

e. Select the check box to enable IEEE802.1x Authentication.

- **EAP Type**—If you have enabled the **Enable IEEEE 802.1x authentication** check box, select the EAP Type option you want—**TLS**, **LEAP** or **PEAP**.
- **TLS**—If you select the **TLS** option, click **Properties** to open and configure the **Authentication Properties** dialog box.
  - Select the **Validate Server Certificate** check box because it is mandatory to validate your server certificate.

    NOTE:
    The CA certificate must be installed on the thin client. Also note that the server certificate text field supports a maximum of approximately 127 characters, and supports multiple server names.
  - If you select the **Connect to these servers** check boxes, the box is enabled where you can enter the IP address of server.
  - Click **Browse** to find and select the Client Certificate file and the Private Key file you want.

The following kinds of server names are supported—all examples are based on the Cert Common name **company.dell.com**

NOTE:

Using only the FQDN, that is Company.wyse.com does not work. You must use one of the options—note that *.dell.com is the most common option as multiple authentication servers may exist: Servername.dell.com

*.dell.com

*dell.com

*.com

f. **LEAP**—If you select the **LEAP** option, click **Properties** to open and configure the **Authentication Properties** dialog box. Be sure to use the correct Username and Password for authentication. The maximum length for the username or the password is 64 characters.

g. **PEAP**—If you select the **PEAP** option, click **Properties** to open and configure the **Authentication Properties** dialog box. Be sure to select either **EAP_GTC** or **EAP_MSCHAPv2**, and then use the correct Username, Password, and Domain. Validate Server Certificate is optional.

NOTE:

The server certificate text box for LEAP and PEAP supports a maximum of approximately 127 characters, and supports multiple server names.

h. To configure the EAP-GTC, enter the username only. The password or PIN is required when authenticating.

To configure EAP-MSCHAPv2, enter the username, password, and domain.

Important: The domain/username in the username box is supported, but you must leave the domain box blank.

The CA certificate must be installed on the thin client, and the server certificate is forced to be validated. When EAP-MSCCHAPV2 is selected in EAP type in the **Authentication Properties** dialog box (for PEEP IEEE802.1x authentication), an option to hide the domain is available for selection. Username and Password boxes are available for use, but the **Domain** text box is disabled.

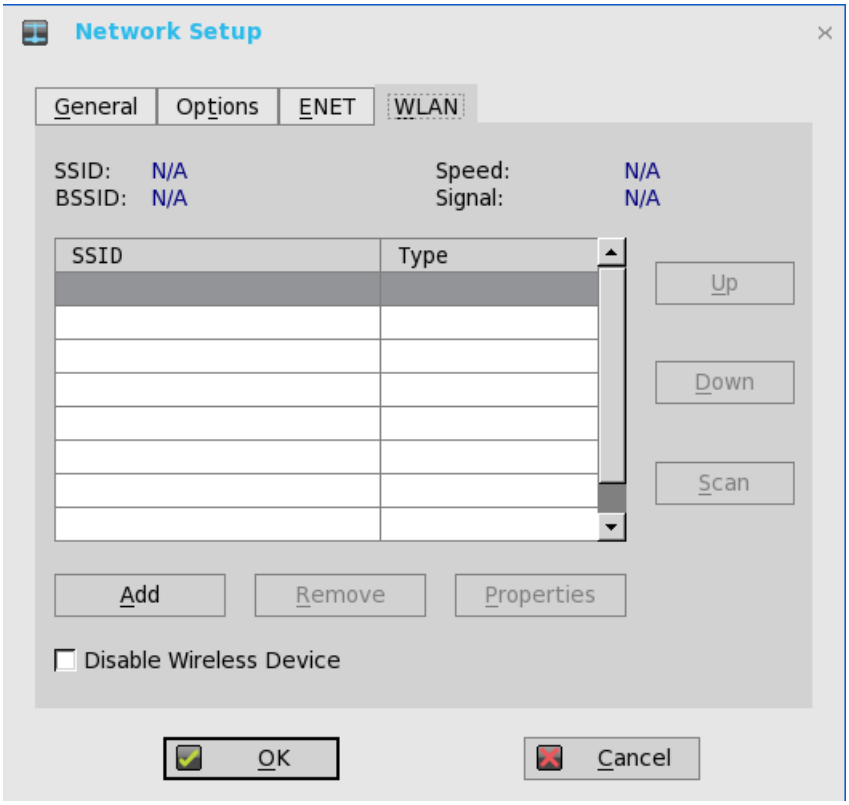
3. Click **OK** to save the settings.

Configuring the WLAN Settings

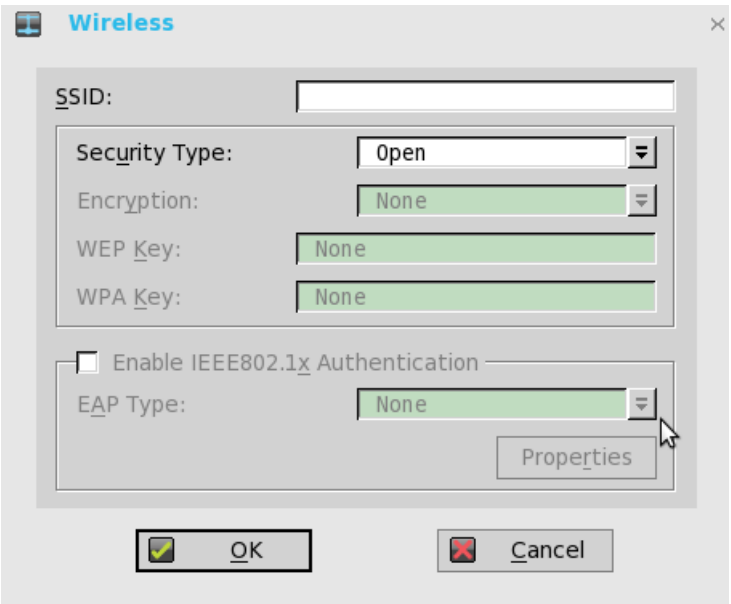
1. From the desktop menu, click **System Setup**, and then click **Network Setup**.

   The **Network Setup** dialog box is displayed.

2. Click the **WLAN** tab, and use the following guidelines:



a. **Add**— Use this option to add and configure a new SSID connection.
   You can configure the SSID connection from the available security type options.



b. After you configure the SSID connection, the added SSID connection is listed on the page of the **WLAN** tab.
c. **Remove** — Use this option, if you want to remove a SSID connection by selecting the SSID connection from the list.
d. **Properties** — Use this option to view and configure the authentication properties of a SSID connection that is displayed in the list.
e. Select the **Disable Wireless Device** check box, if you want to disable a wireless device.

3. Click **OK** to save the settings.

Configuring the network settings on ThinLinux

On the **System Settings** page, click the **Network** tab to view the **Network Settings** page.

1. Click the **Network** icon.

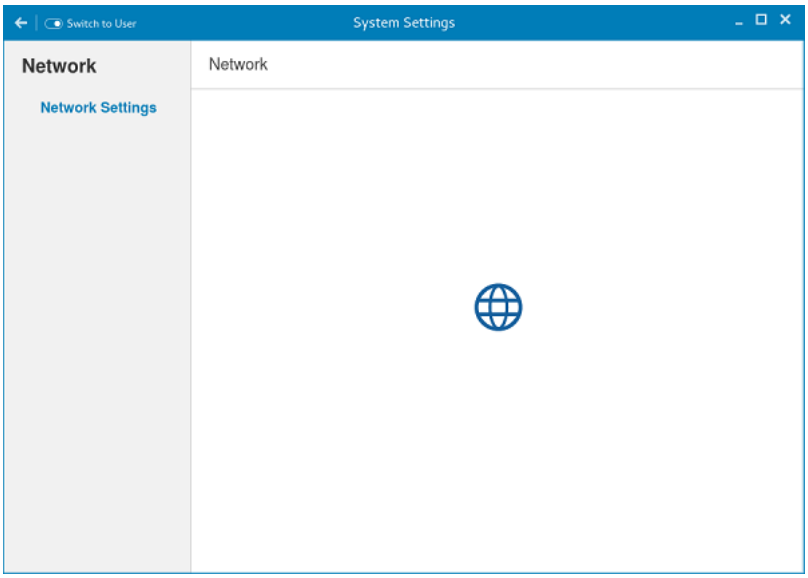


Figure 2. Network Settings

2. The **Network settings** page is displayed. In the left-pane, the following tabs are available for you to configure.
   - Wi-Fi
   - Wired
   - Network proxy

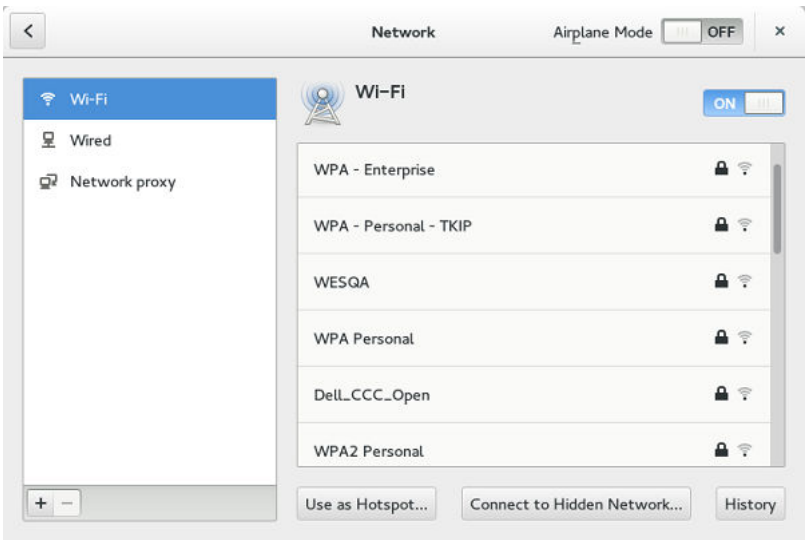


Figure 3. Network Settings page

Configuring wired network connection settings

To configure the wired connection settings, perform the following steps:

1. Click the **Wired** tab. The following attributes are displayed if the network cable is connected to your thin client and wired connection is established.
   - IP Address
   - Hardware Address
   - Default Route
   - DNS

   NOTE: After the network is disconnected, only hardware address and last used information are displayed.
2. On the lower-right corner of the page, click the **Settings** icon to configure the Wired Network connections.
   a. In the **Details** tab, the following attributes are displayed.
      - IP Address
      - Link Speed
      - Hardware Address
      - Default Route
      - DNS
3. Click the **Security** tab to configure the 802.1x security settings.
   a. Click the **ON** button to enable the 802.1x Security for your network connection.
   b. From the **Authentication** drop-down list, select the type of authentication you want to set for your network connection. The available options are:
      - MDS
      - TLS
      - FAST
      - Tunneled TLS
      - Protected EAP (PEAP)
   c. If the authentication type is selected as **MD5,** you must configure the following options.

Parameter	Description
Username	Enter the **Username** for the network connection.
Password	Enter the **password** you want to set for the connection.
Ask for this password every time	If this check box is selected, you will be prompted to enter the password every time when you connect to the network.
Show Password	Select this check box if you want to allow the user to view the hidden password.

   d. If the authentication type is selected as **TLS,** you must configure the following options.

Parameter	Description
Identity	Enter your Identity.
User certificate	Select the User certificate from the list or upload your personal certificate stored locally. To upload your personal certificate, click the **Folder** icon, and then browse to the location where you have stored the certificate.

Parameter	Description
CA Certificate	Select the CA certificate from the list or upload your CA certificate stored locally. To upload your CA certificate, click the **Folder** icon, and then browse to the location where you have stored the certificate.
Private key	Select the private key from the list or upload your private key stored locally. To upload your private key, click the **Folder** icon, and then browse to the location where you have stored the certificate.
Private key password	Enter the password that you want to set for the private key.
Show Password	Select this check box if you want to allow the user to view the hidden password.

e. If the authentication type is selected as **FAST,** you must configure the following options.

Parameter	Description
Anonymous identity	Enter the username you want to set for Anonymous Authentication Identity.
PAC provisioning	Select this check box to enable the PAC provisioning authentication. From the drop-down list, select any of the following PAC provisioning options: **Anonymous** – Select this option to establish a secure anonymous TLS communication with the client and provide it with a PAC. **Authenticated** – Select this option to enable a secure server-side authentication and provide the client with a proxy auto-config (PAC) file. **Both** – Select this option if you want to allow both Anonymous and Authenticated PAC provisioning.
PAC file	Select the PAC file from the list or upload your CA certificate stored locally. To upload your PAC file, click the **Folder** icon, and then choose the certificate from the location where you have stored the certificate.
Inner authentication	From the drop-down list, select the inner authentication method you want to set. The available options are GTC and MSCHAPv2.
Username	Enter the **Username** for the network connection.
Password	Enter the **password** you want to set for the connection.
Ask for this password every time	If this check box is selected, you will be prompted to enter the password every time when you connect to the network.

Parameter	Description
Show Password	Select this check box if you want to allow the user to view the hidden password.

f. If the authentication type is selected as **Tunneled TLS**, you must configure the following options.

Parameter	Description
Anonymous identity	Enter the username that you want to set for Anonymous Authentication Identity.
CA certificate	Select the CA certificate from the list or upload your CA certificate stored locally. To upload your CA certificate, click the **Folder** icon, and then browse to the location where you have stored the certificate.
Inner authentication	From the drop-down list, select the inner authentication method that you want to set. The available options are GTC and MSCHAPv2.
Username	Enter the Username for the network connection.
Password	Enter the password that you want to set for the connection.
Ask for this password every time	If this check box is selected, you will be prompted to enter the password every time when you connect to the network.
Show Password	Select this check box if you want to allow the user to view the hidden password.

g. If the Authentication type is selected as **Protected EAP (PEAP)**, you must configure the following options.

Parameter	Description
Anonymous identity	Enter the username you want to set for Anonymous Authentication Identity.
CA certificate	Select the CA certificate from the list or upload your CA certificate stored locally. To upload your CA certificate, click the **Folder** icon, and then browse to the location where you have stored the certificate.
PEAP version	Select the PEAP version type you want to use for EAP authentication. The available options are: • Automatic • Version 0 • Version 1
Inner authentication	From the drop-down list, select the inner authentication method that you want to set. The available options are GTC and MSCHAPv2.
Username	Enter the **Username** for the network connection.

Parameter	Description
Password	Enter the **password** that you want to set for the connection.
Ask for this password every time	If this check box is selected, you will be prompted to enter the password every time when you connect to the network.
Show Password	Select this check box if you want to allow the user to view the hidden password.

4. Click the **Identity** tab and configure the following settings:

   NOTE: Only Administrators are allowed to authenticate these settings by entering the admin password in the root privilege authentication dialog box after a particular setting is changed or configured.

   a. **Name**— Specifies the default name of the wired connection. If you want to set your preferred name for the connection, enter the name and then click **Apply**.
   b. **MAC Address**— Specifies the MAC address of the network connection.
   c. **Cloned Address**— Specifies the IP address that is cloned by the router.
   d. **Maximum transmission unit (MTU)**— Specifies the size (in bytes) of the largest protocol data unit that the protocol layer can pass onwards.
   e. **Connect automatically**— Select this check box to automatically connect to the network after you plug-in the network wire.
   f. **Make available to other users**— Select this check box if you want to allow other users to configure these settings.

5. Click the **IPv4** tab and do the following:
   a. Enable the **IPv4** button to configure the IPv4 settings.
   b. From the **Addresses** drop-down menu, select the type of IPv4 configuration. The available options are:
      - Automatic (DHCP)
      - Manual
      - Link-Local Only
   c. If **Automatic (DHCP)** option is selected, you must configure the following options.

Parameter	Description
DNS	Enable the **Automatic** button, if you want the thin client to automatically fetch the DNS Server.
Server	Specifies the IP address of the DNS Server. Click the **+** icon to add a new DNS server to the list.
Routes	Enable the **Automatic** button to turn on the automatic IPv4 routing.
Address	Specifies the Router IP address.
Netmask	Specifies the Netmask. Netmask is used to divide an IP address into subnets and specify the network's available hosts.
Gateway	Specifies the IP address of the default Gateway.
Metric	Specifies the Metric value for the network connection.

Parameter	Description
Use this connection only for resources on its network	Select this check box, if you want to allow the wired connection only for resources on its network.

d. If **Manual option** is selected, you must specify the IP address, Netmask IP and Gateway IP along with the parameters mentioned in Table 1: Automatic (DHCP).
e. If **Link-Local Only** option is selected, the DNS and Routes options are disabled. This is applicable only for communications within the host link or the host domain.

6. Click the **IPv6** tab and do the following:
   a. Enable the **IPv6** button to configure the IPv6 settings.
   b. From the **Addresses** drop-down menu, select the type of IPv6 configuration. The available options are:
      - Automatic
      - Automatic, DHCP only
      - Manual
      - Link-Local Only

      The IPv6 configuration is similar to configuring the IPv4 Settings. For IPv4 configuration, see the IPv4 settings in this section.
7. Click the **Reset** tab and do the following:
   a. Click **Reset** to reset the settings for your network connection, including passwords. However, the previous network is displayed as a preferred network.
   b. Click **Forget** to remove all details relating to this network that you do not want to automatically connect to.
8. Click **Apply** to save your configured settings.

NOTE: Click the Add Profile tab to add a new network profile. On the right pane, you must configure the following options:

- Security
- Identity
- IPv4
- IPv6

The configuration of all these tabs are similar to **Wired Network connections configurations** described in this section.

Audio

This section provides the information about the **Wired** audio and **Bluetooth** audio.

Wired audio

The wired audio supports the following options:

- Combo jack audio (3.5mm jack)
- Stereo headphone
- Mono microphone

NOTE: The audio is also supported through the display port.

Bluetooth audio

- Wireless and Bluetooth M.2 card module (option) on PCI-E.
- USB interface - Bluetooth 4.0

7

Peripherals

Wyse 3030 LT thin client running ThinLinux.

On the **System Settings** page, click the **Peripherals** icon. The following tabs are displayed on the left pane of the System Settings page.

- Keyboard
- Mouse
- Printers
- Sound

The following tables describes about the tested peripherals:

Keyboard

Table 1.

Model	Type
Dell KB813	Integrated Smart card reader
USB: WYSE HID Keyboard KU8933	Keyboard
Dell KB212-B	Keyboard
Dell KG-1089	Keyboard
Dell KB522	Business Multimedia Keyboard
Logitech K120	Keyboard

Mouse

Table 2.

Model	Type
Dell MS111-P	Mouse
Dell MG-1090	Mouse
Wyse Mouse MO42UOA	Mouse
Logitech M525-C	Wireless Mouse
Logitech M100	Mouse

Web Cameras

Table 3.

Model	Type
Logitech	Pro 9000
Logitech	HD Pro C920
MS Life cam	HD3000

Printer

Table 4.

Model	Type
Inkjet Printer	Canon MG2420
Inkjet Printer (WI-FI)	Canon MG3520
Color Printer	Dell C1660w
Multifunction Color Printer	Dell B1165nfw/B2375dfw
Mono Printer	Dell B2360D

Wyse 3030 LT thin client ThinOS

This section describes the tested peripherals of Wyse 3030 LT thin client running ThinOS.

The following table describes about the tested peripherals:

Table 5. Keyboard/mouse

Keyboard/mouse
Dell KB212-B /Mouse N889
Dell Keyboard KB113p
Dell Keyboard KB212-B
Dell Keyboard KB522
Dell Keyboard KB813 (Smartcard reader)
Dell Laser USB 6-Button Mouse
Dell Optical Wireless Mouse – WM123
Space Mouse Pro

Keyboard/mouse
KSI 1700 Keyboard
Logitech Media Keyboard K200/Mouse B100
Logitech T400 Zone Touch Mouse
Dell Wireless Bluetooth Travel Mouse – WM524
Dell WM713 Bluetooth
ThinkPad Compact Bluetooth Keyboard
Logitech K480 Bluetooth keyboard

Table 6. USB Webcam

USB Webcam
Logitech C920 HD Pro Webcam
Logitech C930e HD Webcam
Logitech C270 HD Webcam
Logitech BCC950 Conference Cam
Logitech HD Webcam C310
Logitech C525 HD Webcam
Logitech USB Webcam 9000
Microsoft LifeCam 3.0 Cinema
Microsoft LifeCam HD-3000

Table 7. Printer

Printer
Dell B1265dnf Multifunction Laser Printer
Dell B2375dnf Mono Laser Multifunction Printer
Dell B2360d Laser Printer

Table 8. Others

Others
Elo Touch Screen Serial
Prolific USB-to-Serial converter U232-P9V2

8

Setting power states

Wyse 3030 LT thin client running ThinOS.

Use the Shutdown dialog box to select the available option you want:

- Classic Desktop — Click **Shutdown** in the Connect Manager or Desktop Menu.
- Zero Desktop — Click the **Shutdown** icon on the Zero Toolbar.

Wyse 3030 LT thin client running ThinLinux.

The **Power** Setting page enables you to set Monitor Sleep mode.

In the Turn off screen after box, select the idle time from the drop down list. The monitor is turned off after the specified idle time.

NOTE: ThinLinux supports the display turn off and by default it is set for 4 minutes of idle time to comply with Energy Star category. If you select never option from the drop down list, it corresponds to idle time of 0 minutes.

9

Software

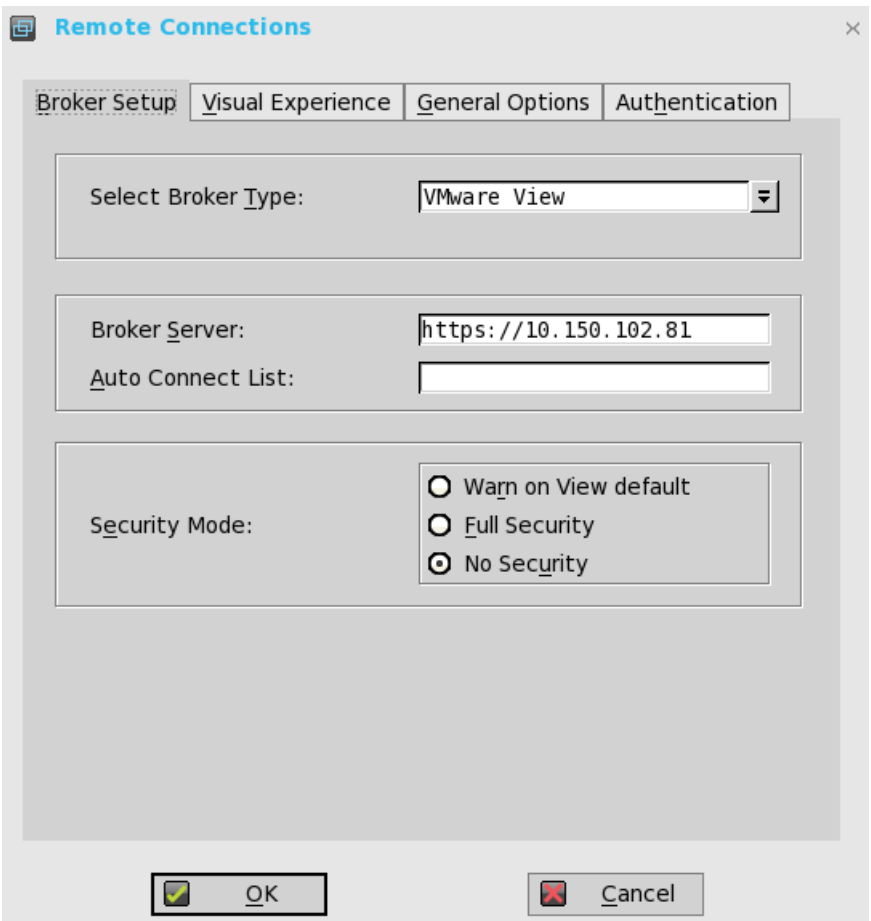
This section describes about establishing and configuring the virtual broker connections for 3030 LT thin clients running either ThinOS or ThinLinux.

- For configuring the virtual broker connection on ThinOS, see Configuring the broker setup on ThinOS.
- For configuring the virtual broker connection on ThinLinux, see Configuring connections locally on ThinLinux.

Configuring broker setup on ThinOS

To configure the Broker setup:

1. From the desktop menu, click **System Setup**, and then click **Remote Connections**.
   The **Remote Connections** dialog box is displayed.



2. Select the **Broker type** from the drop-down list.
   a. If you select **None** from the list, click either of the following connection protocols:
   b. If you select the **Citrix Xen**, use the following guidelines:

- Select the check box to enable the **StoreFront style**.
- **Broker Server**— Enter the IP address of the Broker Server.
- Select the check box to enable automatic reconnection at logon.

  NOTE:
  If you enable the automatic reconnection, you are able to select from the reconnection options. Click either of the options where you can connect to the disconnected sessions only or connect to both active and disconnected sessions.
- Select the check box to enable automatic reconnection from the button menu.

  NOTE: If you enable the automatic reconnection, you are able to select from the reconnection options. Click either of the options where you can connect to the disconnected sessions only or connect to both active and disconnected sessions.
- **Account Self-service Server**— Enter the IP address of the Account self-service server.
- **XenApp**—Use this option, if you want to set default settings to **XenApp**.
- **XenDesktop**—Use this option, if you want to set default settings to **XenDesktop**.

c. If you select the **VMware View**, use the following guidelines:
- **Broker Server**—Enter the IP address of the Broker server.
- **Security Mode**

  —Use this option to select the Security Mode. The available options are **Warn on View default, the Full security,** and **No security**.

d. If you select the **Microsoft**, enter the IP address of the Broker Server in the **Broker Server** box, and then click **OK** to save the settings.

e. If you select **Dell vWorkspace**, use the following guidelines:
- **Broker Server**—Enter the IP address of the Broker Server.
- Select the check box to enable vWorkspace Gateway.
- **vWorkspace Gateway**—Enter the IP Address of the vWorkspace Gateway.

f. If you select **Other**, you must enter the IP address of the Broker server in the **Broker Server** box.

3. Click **OK** to save the settings.

Configuring connections locally on ThinLinux

On the **System Settings** page, click the **Connections** icon. The Connections page contains the following tabs:

- Citrix
- VMware

NOTE: The description names for all the connections can not be edited once you create the connection.

Configuring and managing Citrix connections

The **Citrix Connections** page enables you to create and manage the Citrix connections both locally and globally.

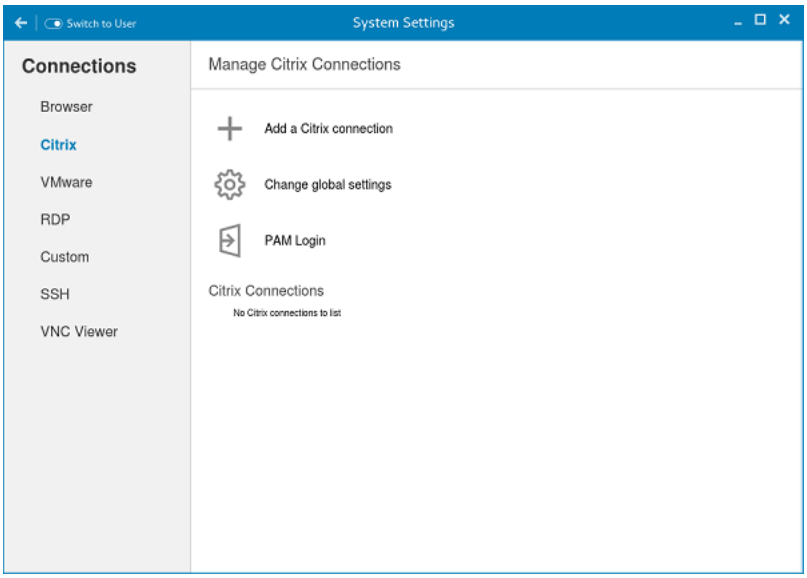


Figure 4. Citrix connection settings

To configure the local **Citrix** settings:

1. Click the **+** icon to add a new **Citrix Connection**.

   The **Citrix Connections** page is displayed.
2. Enter the name of the **Citrix connection** for which you specify the Server URL address.
3. From the **Connection Type** drop-down list, select any of the following connection types:
   - Server
   - Published Application
   - Storefront
4. Click **Save** to save the changes.

Configuring and managing VMware connections

The **VMware connections** page enables you to create and manage the View client 3.5 connections.

To configure the VMware Settings, complete the following task:

1. Click the **+** icon to add a new VMware Connection.

   The **VMware Connections** page is displayed.

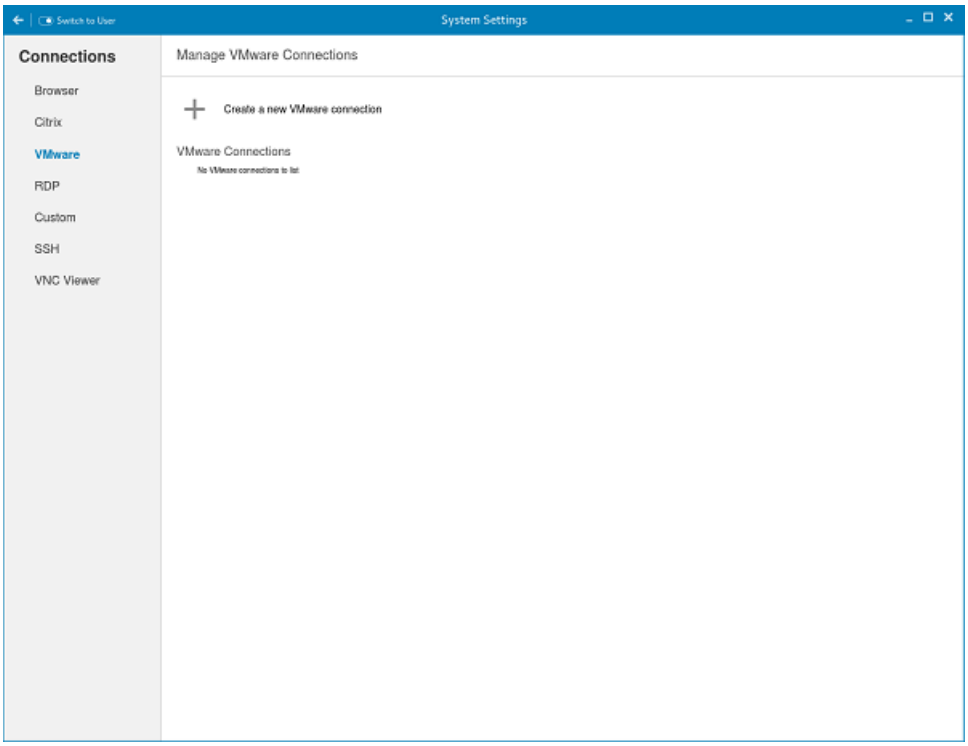


Figure 5. VMware connections settings

2. Enter the name of the **VMware connection**.
3. Configure the following options in the **Login** tab:

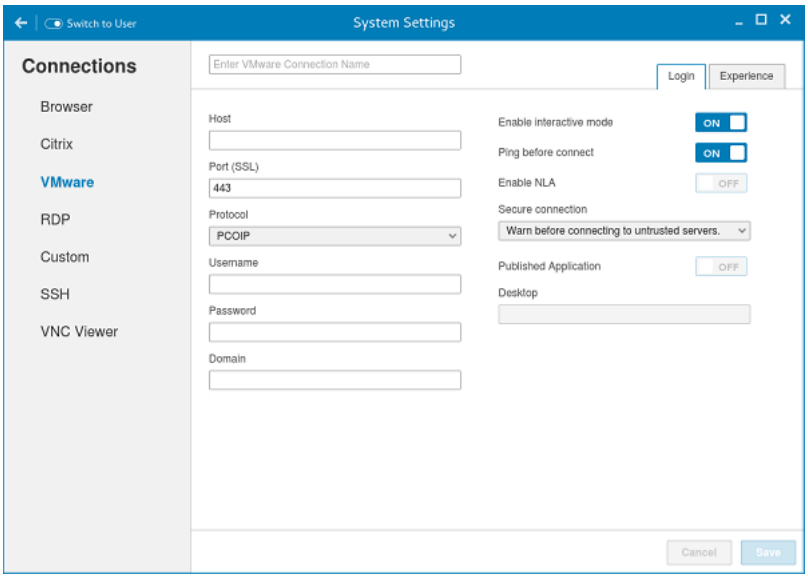


Figure 6. VMware login settings

Parameter	Description
Host	Enter the host name or **IP address** or **FQDN** of the Horizon of the VMware View Server.
Port	Enter the port number of the host.

Parameter	Description
Protocol	From the drop-down list, select the specific protocol.
Username	Enter the User ID that is used to log in to the remote Horizon server.
Password	Enter the password that is used to log in to the remote Horizon server.
Published Application	Click the **ON/OFF** button to enable or disable this option. If enabled, specify the Published Application name. If disabled, specify the Published desktop name.
Enable interactive mode	Click the **ON/OFF** button to enable or disable this option. If enabled, then after a successful connection to the server, it displays all the published application and desktop icons. You can start the applications or desktop sessions based on your choice. If disabled, then the Published Applications option is enabled in the Login tab. Selecting that option enables you to directly start the application or desktop that you specify.
Ping before connect	Click the **ON/OFF** button to enable or disable this option. If enabled, it pings the connection is checked in server IP/ FQDN before connecting to a session.
Enable NLA	Click the **ON/OFF** button to enable or disable this option. Enable the Network Level Authentication (NLA), if NLA is enabled on your remote computer. Your remote computer requires NLA user authentication before you establish a full Remote Desktop connection and the login screen is displayed.
Secure connection	Click the Secure Preferences tab and select any of the options that determine how the client should proceed when it cannot verify that your connection to the server is secure.
Domain	Enter the Domain name. It is used to log in the remote Horizon server.
Desktop	If interactive mode is disabled, you can specify Published desktop name.
Application	If interactive mode is disabled, you can specify the Published application name.

4. The following options must be configured in the **Experience** tab:

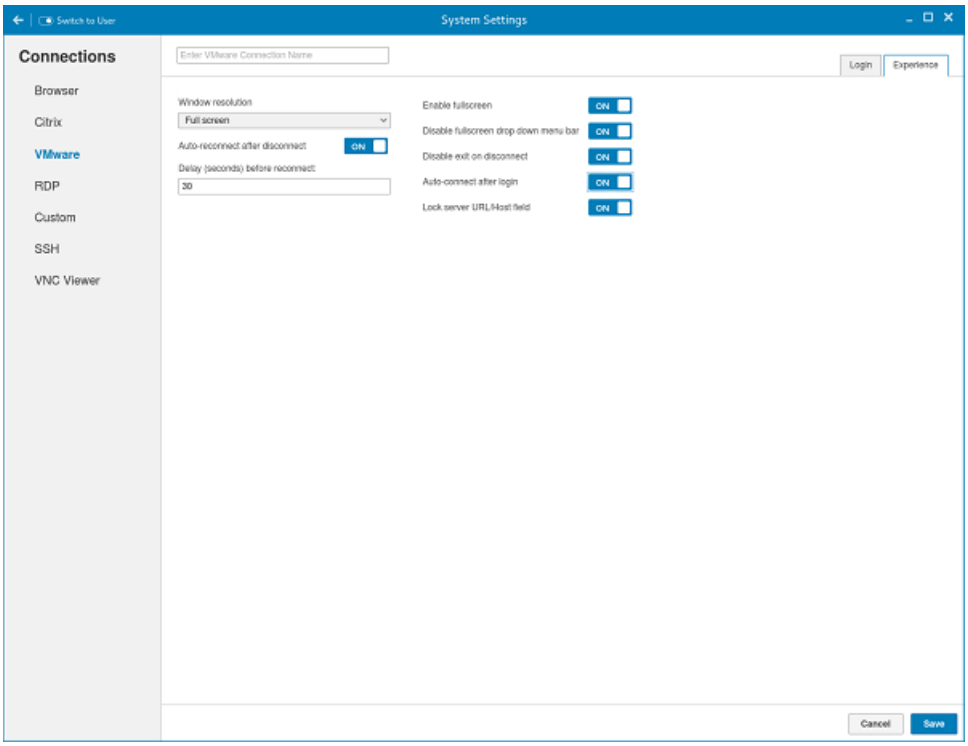


Figure 7. VMware experience settings

Parameter	Description
Windows resolution	Select the Windows resolution that you want to get the best display on your monitor. The available resolutions are: Use All Monitors Full Screen Large Screen Small Screen 1024X768 800X600 640X480
Auto-Reconnect after disconnect.	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically re-established after you disconnect from the session.
Delay (seconds) before reconnect.	Select the amount of time in seconds to delay the reconnection attempt after a disconnection occurs.
Enable fullscreen	Click the **ON/OFF** button to enable or disable this option. Select this option to view the remote session in full screen mode in all the monitors.
Disable fullscreen drop-down menu bar	Click the **ON/OFF** button to enable or disable this option.

Parameter	Description
	Select this option to disable the drop-down menu bar in the full screen mode.
Disable exit on the disconnect	Click the **ON/OFF** button to enable or disable this option. Select this option if you do not want the Horizon server to retry connecting if there is a connection error. You can typically select this option if you use kiosk mode.
Auto-connect after login.	Click the **ON/OFF** button to enable or disable this option. Select this option to reconnect automatically after a disconnection occurs.
Lock server URL/Host field	Click the **ON/OFF** button to enable or disable this option.

5. Click **Save** to save the settings.

10

Wyse Management Interface

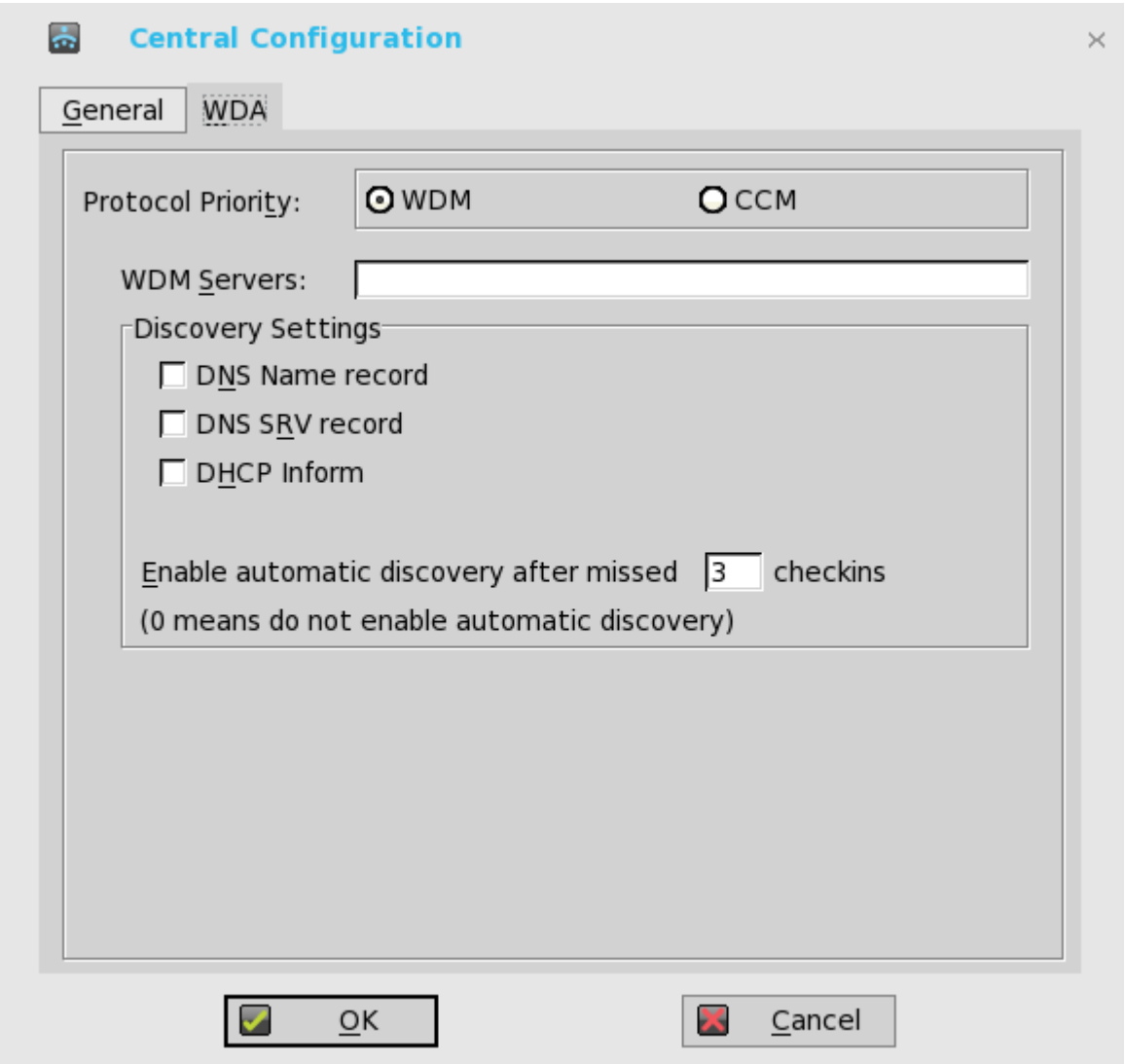
This section describes about the Wyse Management Interface of 3030 LT running either ThinOS or ThinLinux.

- For WDA settings on ThinOS, see Configuring the WDA settings on ThinOS.
- For WDA settings on ThinLinux, see Configuring the WDA settings on ThinLinux

Configuring the WDA settings on ThinOS

Use this tab to configure the WDM and CCM settings.
To configure the WDA settings, do the following:

1. From the desktop menu, click **System Setup**, and then click **Central Configuration**.
   The **Central Configuration** dialog box is displayed.
2. Click **WDA**, and use the following guidelines.
   WDM is selected by default. WDA service automatically runs after the client boot up.

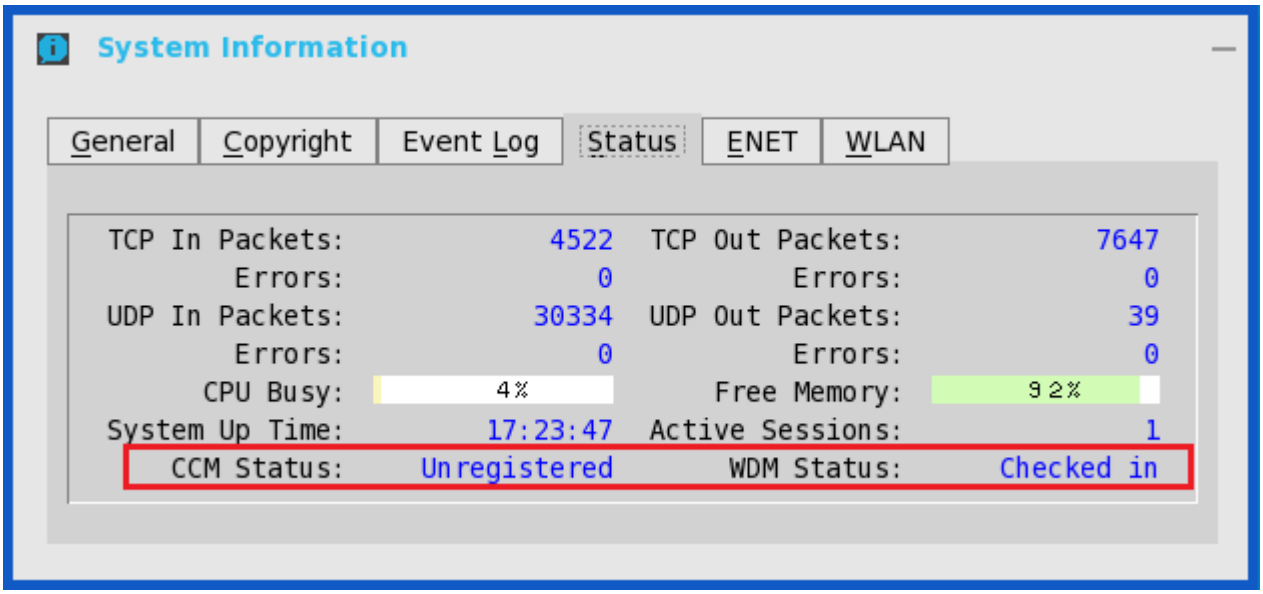


If the first discovery, for example, the WDM service is not successful, then it seeks for the next priority, for example, CCM service. This continues till a discovery is successful. If all discoveries fail, then it is started again automatically after a fixed time (24 hours).

a. **WDM Servers** — Enter the IP addresses or host names, if WDM is used. Locations can also be supplied through user profiles, if user INI profiles are used.
b. **DNS Name Record** — (Dynamic Discovery) Allows devices to use the DNS host name lookup method to discover a WDM Server.
c. **DHCP Inform** — (Dynamic Discovery) Allows devices to use DHCP Inform to discover a WDM Server.
d. **Enable Automatic Discovery After Missed Check-ins** — Select the number of missed check-ins after which you want the auto discovery options enabled.

3. Click **OK** to save the settings.

Service checked in status is displayed in System Information.

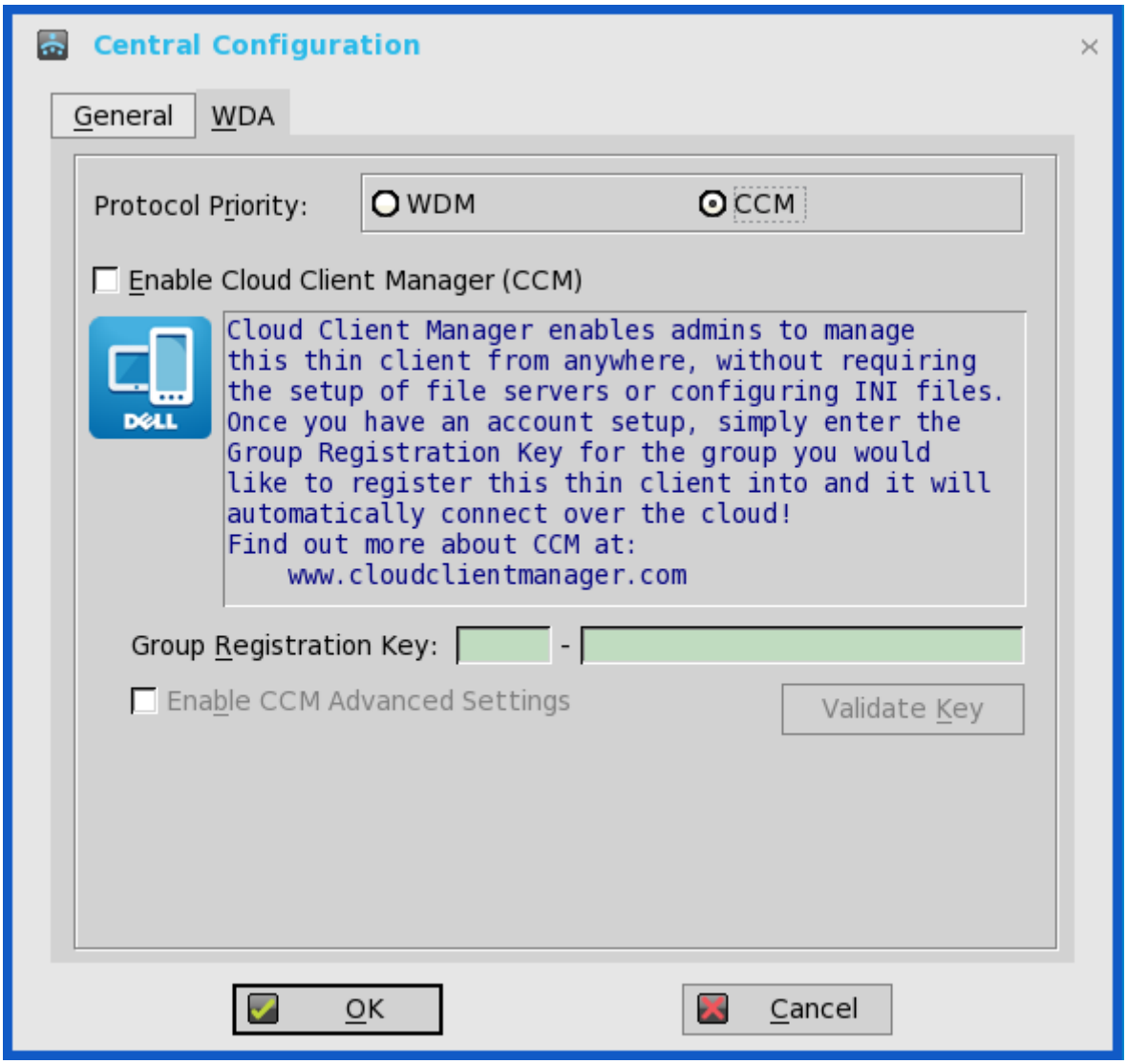


The following is the INI parameter for this feature:

`WDAService={yes(default),no}Priority ={WDM(default),CCM,"WDM;CCM","CCM;WDM"}`

To configure the CCM settings, do the following:

1. Click **CCM**, and use the following guidelines.
    a. **Enable Cloud Client Manager (CCM)** — Select the check box to enable the Cloud Client Manager(CCM).



b. **Group Registration Key** — Enter the **Group Registration Key** as configured by your cloud Client Manager administrator for the desired group.

NOTE: If you enable the Cloud Client Manager (CCM), make sure that you have entered the Group Registration Key and enabled the CCM Advanced Settings.

2. Click **OK** to save the settings.

Configuring the WDA settings on ThinLinux

The Wyse Device Agent (WDA) on the ThinLinux device supports only the features of Cloud Client Manager (CCM) device management solution. Wyse Device Agent is for configuring the CCM (Cloud Client Manager) client settings and registering a ThinLinux device into CCM and it is available only for admin user.

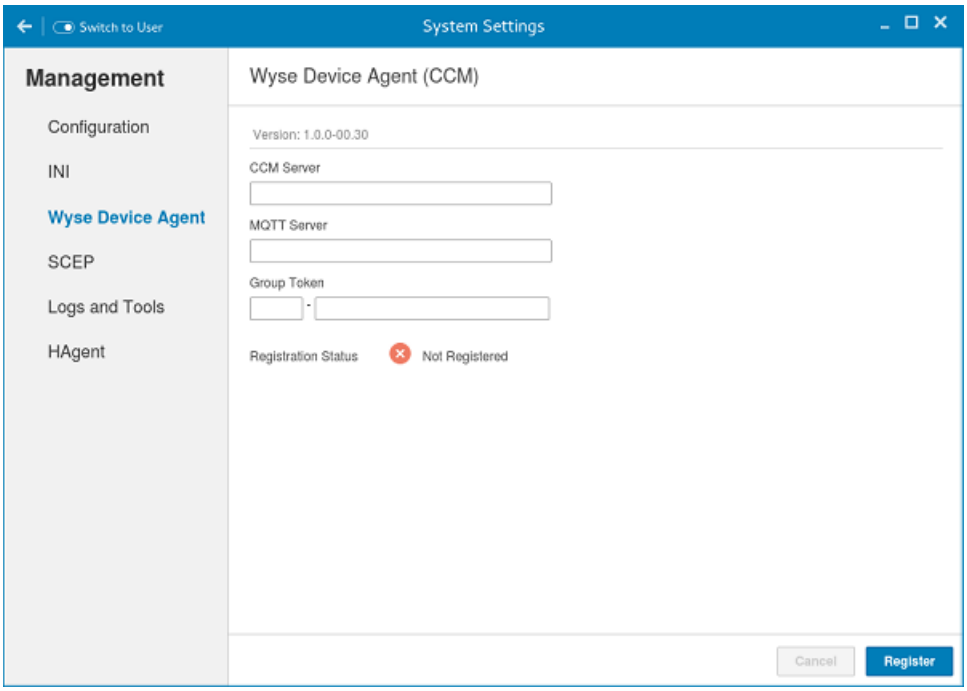


Figure 8. Wyse Device Agent (CCM)

If the device is not registered to a CCM server, the **Wyse Device Agent** screen shows the registration status as **Not Registered**.

1. In the **CCM Server** input box, enter the URL of CCM server you want to connect to.
2. In the **MQTT Server** input box, enter the IP address or hostname of Message Queue Telemetry Transport (MQTT) server.
3. In the Group Token input boxes, enter your group registration key to manage your ThinLinux device. This is a unique key for registering your thin client device. Thin clients can be directly registered to Groups directly and must have a Group Registration Key enabled to perform this action.
4. Do one of the following options:
   - Click **Register** to register your thin client on CCM server. When your thin client is successfully registered, the status is shown as Registered with green color icon next to the Registration Status label, and caption of Register button changes to Unregister.
   - Click **Unregister**, if you want to remove your thin client from the CCM management system. If Unregister fails, a dialog box for Force Unregister confirmation is displayed. Click **Yes** to forcefully unregister your device which is managed by CCM. When you perform Register or Unregister or Force Unregister from Agent screen, the applet should not be closed until Registration Status. After successful registration, you can access the CCM management server screen where you can view and manage Device Asset Details, Real-Time commands, and Troubleshooting information of your registered thin client.

Directing the Thin Client to CCM Server:

- To direct your thin client to CCM server, you must provide CCM/MQTT server details and Group registration Key. These details is discovered by Wyse Device Agent using any of the following ways:
  - DHCP Scope options
  - Using INI parameter
  - Using the Wyse Device Agent screen
- Directing the thin client to CCM Server using DHCP Scope options. The CCM/MQTT server details and Group Registration Key that are required for CCM registration can be obtained by querying the DHCP server with following option tags:
  - 199 – Scope option for Group Token (type = String, value = CCM-group-key).
  - 165 – Scope option for CCM server.
  - 166 – Scope option for MQTT server.

- Directing the thin client to CCM Server using INI parameters, INI syntax for CCM configuration:

  – CCMEnable={yes,no} CCMServer=<CCM Server URL> GroupRegistrationKey=<tenant code-group code> MQTTServer=<MQTT server>[:<MQTT port>]

  NOTE:

  When INI discovery method is used for registering the device, if you want to unregister the device, you must delete the INI parameters and restart the device first and then unregister the device. Else you have to perform the unregister process twice. For more information, see *ThinLinux INI Guide* .

11

System specifications

Table 9. Brand/Sub-brand/Model Number/Chassis description/Series Level/Category Type

Feature	Specification
CPU	Dual-core Intel Celeron N2807, 1.58 GHz processor
Operating System	Wyse ThinOS and Wyse ThinLinux.
Memory	4GB Flash eMMC 2GB RAM DDR3L; 1,333 MT/s data transfer rate
I/O peripheral support	1x SuperSpeedUSB 3.0 (front), 3 x high-speed USB 2.0 (two front, one rear) 2 x DisplayPort(optional VGA, DVI or HDMI adapter sold separately)
Networking	10/100/1000 Base-T Gigabit Ethernet. (RJ45) Wireless 802.11 a/b/g/n/ac dual band, dual antenna (option)
Display	DisplayPort: Up to 2560 x 1600 x 24 @ 60Hz
Audio	Universal audio jack: 1/8-inch mini, 16-bit stereo output, mono input Internal mono speaker
Dimensions	Height 7.37in (187mm) x Width 1.15in (29mm) x Depth 4.61in (117 mm)
Weight	2.34kg (5.2 lbs)
Mountings	Vertical feet, standard. Optional VESA mounting bracket
Wireless Network Security	Security protocols supported for both wireless and 802.1x network based authentication: EAP-TLS; EAP-LEAP; EAP-PEAP, EAP-MSCHAPv2, EAP-GTC; WEP; WPA Personal; WPA2 Personal; WPA Enterprise; WPA2 Enterprise
Device Security	Built-in Kensington security slot (lock and cable sold separately)
Power	Worldwide auto-sensing 100-240 VAC, 50 – 60Hz 30W, 12V DC

Feature	Specification
	EuPcompliant power adapter
Temperature range	Operating, Vertical position range is 32 degree Celsius to 104 degree Fahrenheit (10 to 40 degree Celsius) Storage is 14 degree Celsius to 140 degree Fahrenheit (-10 to 60 degree Celsius)
Humidity	20% to 80% condensing and 10% to 95% non-condensing
Regulatory and Environmental	For more information on complete listing of declarations and certifications, see Dell's regulatory and compliance home page at dell.com/regulatory_compliance

12

Troubleshooting your system

You can troubleshoot your system using indicators like diagnostic lights, and error messages during the operation of the device.

Diagnostic power LED codes

Table 10. Diagnostic power LED codes

Power LED light status	Possible cause	Troubleshooting steps
At first power apply :No LED light up briefly	Both power LED and activity LED come up briefly and then turn off.	• Check AC power, call your utility company • Check AC power cord is plug-in • Check DC plug is plug into the unit
At first power apply : Both LED stay ON	Both power LED and activity LED come up briefly and then turn off	• Logic board defect • BIOS malfunctioning • Abnormal power source
Push power button the LED does not turn	• Power LED should come up in steady BLUE • Activity LED should turn on in steady AMBER	• Logic board defect • Power button defect • Mechanical assembly misalign cause miss actuation
LED comes up normally but it will not display.	It will come up with BIOS screen in few seconds	• Incompatible monitor • Defect logic board • Malfunction dongle (if used) • Defect cable or connector
Distorted display	It should have normal viewable display.	• Incompatible monitor • Incompatible dongle (if used) • Not supported display mode • Bad connection on display output • Logic board defect