Dell Wyse Management Suite

Version 1.3 Administrator's 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.

Contents

Introduction to Wyse Management Suite

Wyse Management Suite is the next generation management solution that enables you to centrally configure, monitor, manage, and optimize your Dell Wyse thin clients. It also offers advanced feature options such as cloud as well as on-premises deployment, manage-from-anywhere option by using a mobile application, enhanced security such as BIOS configuration and port lockdown. Other features include device discovery and registration, asset and inventory management, configuration management, operating system and applications deployment, real-time commands, and monitoring, alerts, reporting, and troubleshooting of endpoints.

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

Editions

Wyse Management Suite is available in the following editions:

- **Standard (Free)**—The Standard edition of the Wyse Management Suite is available only for an on-premise deployment. You do not require a license key to use the Standard edition. The Standard edition is suitable for small and medium businesses.

- **Pro (Paid)**—The Pro edition of Wyse Management Suite is available for both on-premise and cloud deployment. You require a license key to use the Pro edition. It provides subscription-based licensing. With the Pro solution, organizations will be able to adopt a hybrid model and float licenses between on-premises and cloud. The Pro on-premise edition is suitable for small, medium, and large businesses. For a cloud deployment, the Pro edition can be managed on non-corporate networks (home office, third party, partners, mobile thin clients, and so on). The Pro edition of the Wyse Management Suite also provides:

  - A mobile application to view critical alerts, notifications, and send commands in real time.

  - Enhanced security through two-factor identification and Active Directory authentication for role-based administration.

  - Advanced app policy and reporting

   ⓘ **NOTE:**
    - Cloud services are hosted in the US and Germany. Customers in countries with data residency restrictions may not be able to take advantage of the cloud-based service.

    - Licenses can be floated easily between cloud and on-premise installation.

For more information on the features supported in Standard and Pro editions, see the Feature matrix.

The Wyse Management Suite Web console supports internationalization. On the lower-right corner of the page, from the drop-down menu, select any one of the following languages:

- English
- French
- Italian
- German
- Spanish
- Chinese
- Japanese

What is new in this release?

The following new features are introduced in this release:

- Added support for Teradici device management.
- Added support for Dell Wyse Easy Setup version 1.2.
- Added support for enhanced ThinOS policy settings.
- Added support for alert notifications from specific groups.
- Added support for enhanced installer with Teradici EMSDK.
- Added support for Teradici devices in the mobile application.

ⓘ **NOTE: Only Wyse Management Suite private cloud supports Teradici.**

Getting started with Wyse Management Suite

This section provides information about the general features to help you get started as an administrator and manage thin clients from the Wyse Management Suite software.

Topics:

- Logging in to Wyse Management Suite on public cloud
- Prerequisites to deploy Wyse Management Suite on private cloud
- Functional areas of management console
- Configuring and managing thin clients

Logging in to Wyse Management Suite on public cloud

To log in to the Wyse Management Suite console, you must have a supported web browser installed on your system. For a list of supported web browsers, see Supported web browsers. To log in to the Wyse Management Suite console, do the following:

1   Access the public cloud (SaaS) edition of the Wyse Management Suite by using one of the following links:
    - **US datacenter**—us1.wysemanagementsuite.com/ccm-web
    - **EU datacenter**—eu1.wysemanagementsuite.com/ccm-web

    ⓘ **NOTE: When you log in to the Wyse Management Suite console for the first time, or if a new user is added, or if a user license is renewed, the Terms and Condition page is displayed. Read the terms and conditions, select the respective check boxes, and click Accept.**

2   Enter your user name and password.
3   Click **Sign In**.

ⓘ **NOTE:**

- You receive your login credentials when you sign up for the Wyse Management Suite trial on www.wysemanagementsuite.com or when you purchase your subscription. You can purchase the Wyse Management Suite subscription from the Dell Sales team or from your local Dell partner. For more details, see www.wysemanagementsuite.com.

- Dell recommends to change your password after logging in for the first time.

- The default user names and passwords for additional administrators are created by the Wyse Management Suite account owner.

- An externally accessible repository must be installed on a server with a DMZ while using the pro edition of Wyse Management Suite on the public cloud. Also, the fully qualified domain name (FQDN) of the server must be registered in the public DNS.

Changing your password

To change the login password, click the account link in the upper-right corner of the management console, and then click **Change Password**.

Logging out

To log out from the management console, click the account link at the upper-right corner of the management console, and then click **Sign out**.

Prerequisites to deploy Wyse Management Suite on private cloud

Table 1. Prerequisites

Properties	Wyse Management Suite server		Wyse Management Suite software repository
	For 10,000 or less devices	**For 50,000 or less devices**	
Operating system	Windows Server 2012 R2 or Windows Server 2016 Supported language pack—English, French, Italian, German, and Spanish		Windows Server 2012 R2 or Windows Server 2016
Minimum disk space	40 GB	120 GB	120 GB
Minimum memory (RAM)	8 GB	16 GB	16 GB
Minimum CPU requirements	4 cores	4 cores	4 cores
Network communication ports	The Wyse Management Suite installer adds Transmission Control Protocol (TCP) ports 443, 8080, and 1883 to the firewall exception list. The ports are added to access the Wyse Management Suite console and to send the push notifications to the thin clients. · TCP 443—HTTPS communication · TCP 8080—HTTP communication (optional) · TCP 1883—MQTT communication · TCP 3306—MariaDB (optional if remote) · TCP 27017—MongoDB (optional if remote) · TCP 11211—Memcache · TCP 5172, 49159—EMSDK (optional for Teradici devices)		The Wyse Management Suite repository installer adds TCP ports 443 and 8080 to the firewall exception list. The ports are added to access the operating system images and application images that are managed by Wyse Management Suite.
Supported browsers	· Microsoft Internet Explorer version 11 · Google Chrome 58.0 and later versions · Mozilla Firefox 52.0 and later versions · Microsoft Edge browser on Windows—English only		

ⓘ **NOTE:**

- **WMS.exe** and **WMS_Repo.exe** must be installed on two different servers. You must install the Wyse Management Suite remote repository for the public cloud. For private cloud, you must install the Wyse Management Suite remote repository and local repository. For more information, see Accessing file repository.
- The software can be installed on a physical or a virtual machine.
- It is not necessary that the software repository and the Wyse Management Suite server have the same operating system.

Functional areas of management console

The Wyse Management Suite console is organized into the following functional areas:

- The **Dashboard** page provides information about the current status on each functional area of the system.
- The **Groups & Configs** page employs a hierarchical group policy management for device configuration. Optionally, subgroups of the global group policy can be created to categorize devices according to corporate standards. For example, devices may be grouped based on job function, device type, and so on.

- The **Users** page enables local users and users imported from the Active Directory to be assigned global administrator, group administrator, and viewer roles to log in to Wyse Management Suite. Users are given permissions to perform operations based on the roles assigned to them.
- The **Devices** page enables you to view and manage devices, device types, and device-specific configurations.
- The **Apps & Data** page provides management of device applications, operating system images, policies, certificate files, logos, and wallpaper images.
- The **Rules** page enables you to add, edit, and enable or disable rules such as auto grouping and alert notifications.
- The **Jobs** page enables you to create jobs for tasks such as reboot, WOL, and application or image policy that need to be deployed on registered devices.
- The **Events** page enables you to view and audit system events and alerts.
- The **Portal Administration** page enables you to configure various system settings such as local repository configuration, license subscription, active directory configuration, and two-factor authentication.

Configuring and managing thin clients

Configuration management—Wyse Management Suite supports a hierarchy of groups and subgroups. Groups can be created manually or automatically based on rules defined by the system administrator. You can organize the groups based on the functional hierarchy, for example marketing, sales, and engineering, or based on the location hierarchy, for example, country, state, and city.

> (i) NOTE:
> In the Pro edition, you can add rules to create groups. You can also assign devices to an existing group depending on the device attributes such as subnet, time zone, and location.

You can also configure the following:

- Settings that apply to all devices in the tenant account which are set at the Default Policy group. These settings are the global set of parameters that all groups and subgroups inherit from. The settings that are configured at lower-level groups take precedence over the settings that were configured at the parent or higher-level groups.

  For example,
  – Configure the policies for default policy group (parent group). After configuring the policies, check the custom group (child group) policies. Same set of policies are applied to child group as well. Configuration in Default Policy Group settings are the global set of parameters that all groups and subgroups inherit from parent group.
  – Configure different settings for the custom group. The custom group receives both the payloads, but devices in the Default policy Group does not receive the payload configured for custom policy group.
  – Configure different settings for the custom group. The settings that are configured at lower-level groups take precedence over the settings that were configured at the parent or higher-level groups.
- Settings that are specific to a particular device which can be configured from the **Device Details** page. These settings, like lower-level groups, take precedence over the settings configured in the higher-level groups.

When you create and publish the policy, the configuration parameters are deployed to all the devices in that group including the subgroups.

After a policy is published and propagated to the devices, the settings are not sent again to the devices until you make any change. New devices that are registered, receive the configuration policy that is effective for the group to which it was registered. This includes the parameters inherited from the global group and intermediate level groups.

Configuration policies are published immediately, and cannot be scheduled for a later time. Few policy changes, for example display settings, may force a reboot.

Application and operating system image deployment—Applications and operating system image updates can be deployed from the **Apps & Data** tab. Applications are deployed based on the policy groups.

> (i) NOTE: Advanced application policy allows you to deploy an application to the current and all subgroups based on your requirement. Operating system images can be deployed to the current group only.

Wyse Management Suite supports standard and advanced application policies. A standard application policy allows you to install a single application package. The device restarts during installing an application. You need to reboot the device before and after each application

installation. With an advanced application policy, multiple application packages can be installed with only two reboots. This feature is available only in the Pro edition. Advanced application policies also support execution of pre-and-post installation scripts that may be needed to install a particular application.

You can configure standard and advanced application policies to be applied automatically when a device is registered with Wyse Management Suite or when a device is moved to a new group.

Deployment of application policies and operating system images to thin clients can be scheduled immediately or later based on the device time zone or any other specified time zone.

Inventory of devices—This option can be located by clicking the **Devices** tab. By default, this option displays a paginated list of all the devices in the system. You can choose to view a subset of devices by using various filter criteria, such as groups or subgroups, device type, operating system type, status, subnet, and platform or time zone.

To navigate to the **Device Details** page for that device, click the device entry listed on this page. All the details of the device are displayed.

The **Device Details** page also displays all the configuration parameters that are applicable to that device, and also the group level at which each parameter is applied.

This page also enables to set configuration parameters that are specific to that device by enabling the **Device Exceptions** button. Parameters configured in this section override any parameters that were configured at the groups and/or global level.

Reports—You can generate and view canned reports based on the predefined filters. To generate canned reports, click the **Reports** tab on the **Portal Admin** page

Mobile application—You can receive alert notifications and manage devices using the mobile application—**Dell Mobile Agent** available for the Android devices. To download the mobile application and the **Dell Mobile Agent Getting Started Guide**, click the **Alerts and Classification** tab on the **Portal Admin** page.

Wyse Management Suite dashboard

The **Dashboard** page enables you to view the status of a system, and the recent tasks that are performed within the system. To view a particular alert, click the link in the **Alerts** section. The **Dashboard** page also allows you to view the device summary.

Figure 1. Dashboard

Topics:

- View alerts
- View the list of events
- View the device status
- Change user preferences
- Access online help
- Change your password
- Log out

View alerts

The **Alerts** section displays the summary of all the alerts. This section has the following attributes:

- **Devices Not Checked In**
- **App Compliance**
- **Other Device Alerts**

To view the detailed list of all the alerts, do the following:

1 Click **Dashboard**.

The alerts summary is displayed.

2 Click **View All Alerts**.

The **Events** page is displayed with list of all the alerts.

View the list of events

The **Events** section displays the summary of events that have occurred in the last few days.

To view the detailed list of all the events, do the following:

1 Click **Dashboard**.

The events summary is displayed.

2 Click **View All Events**.

The **Events** page is displayed with list of all the events.

View the device status

The **Display** section provides the summary of device statuses. The **Summary** section displays the device count based on the following device status category:

· **Compliant**
· **Pending**
· **Unmanaged**
· **Non-Compliant**

To view the detailed list of all the devices, do the following:

1 Click **Dashboard**.

The devices summary is displayed.

2 Click **View All**.

The **Devices** page is displayed with list of all the registered devices.

Change user preferences

To change the user preferences, such as alert notification, policy settings, and page size, do the following:

1 On the upper-right corner of the **Dashboard** page, click the login drop-down menu.

2 Click **User Preferences**.

The **User Preferences** window is displayed.

3 Click **Alerts**, and select the appropriate check boxes to assign an alert type—Critical, Warning or Info—for notifications from your emails and mobile applications.

4 Click **Policies**, and select the **Ask me if I want to use the ThinOS Wizard mode** check box to display the **Select ThinOS Configuration Mode** window every time you configure the ThinOS policy settings.

5 Click **Page size**, and enter a number from 10 to 100 in the **Number Of Items Per Page** text box. This option enables you to set the number of items displayed on each page.

Access online help

To access the Wyse Management Suite manuals, do the following:

1 On the upper-right corner of the **Dashboard** page, click the login drop-down menu.

2 Click **WMS Help**.

The **Support for Wyse Management Suite** page is displayed.

Change your password

To change your password, do the following:

1   On the upper-right corner of the **Dashboard** page, click the login drop-down menu.
2   Click **Change Password**.
    The **Change Password** window is displayed.
3   Enter the current password.
4   Enter the new password.
5   Reenter the new password for confirmation.
6   Click **Change Password**.

Log out

To log out from the management console, do the following:

1   On the upper-right corner of the **Dashboard** page, click the login drop-down menu.
2   Click **Sign out**.

Managing groups and configurations

The **Groups & Configs** page enables you to define policies that are required to configure your devices. You can create sub groups of the global group policies and categorize devices based on your requirements. For example, devices may be grouped based on job functions, device type, and so on.
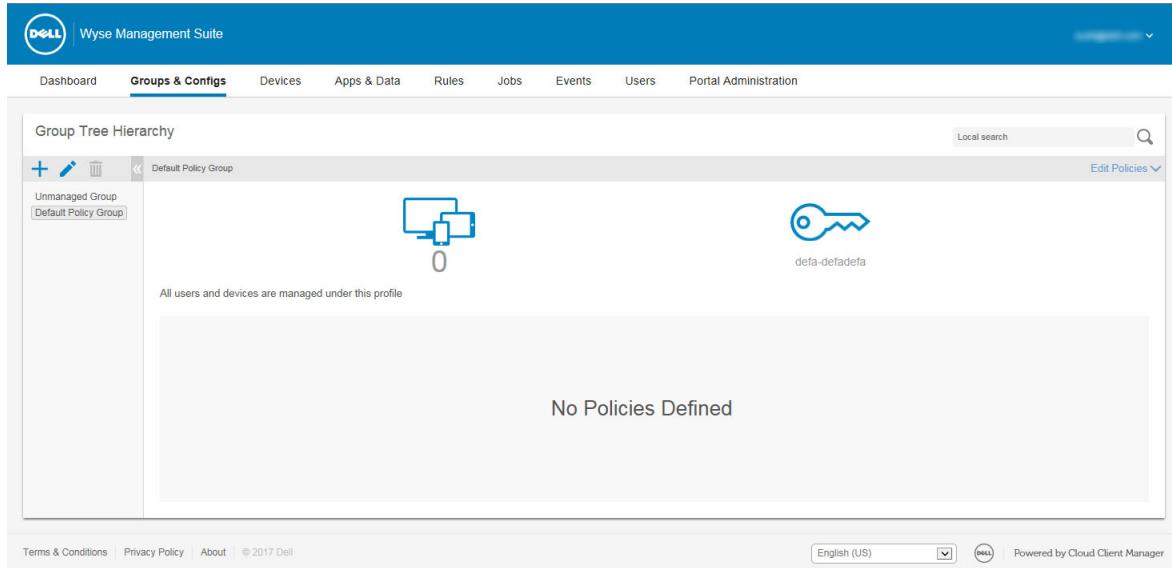
Figure 2. Groups and configuration

For each group, you can define policies for the following operating systems:

· **ThinOS**
· **WES**
· **Linux**
· **ThinLinux**
· **Teradici**
· **Wyse Software Thin client**

Devices inherit policies in the order that they are created. The settings configured in a default policy group are applied as default settings in all the policies listed in the **Default Policy Group**. In a group, all users and devices present in that group have **Default Policy Group** as their default setting.

On the **Device Details** page, you can create an exception for a device in the group to have a subset of policies that are different from the group default.

The configuration for a particular asset with details of where configurations are set—Global, Group, and the Device levels—are displayed on the page. The option to create exceptions is available on the page. The **Exception** settings are applicable only for that selected devices. For more details, see Configuring device level policy.

> ⓘ **NOTE:**
> - When you modify the lower-level policies, a bullet symbol is displayed next to the policy. This symbol indicates that the policy is an override to a higher-level policy. For example, System Personalization, Networking, Security, and so on.
> - When you modify policies, an asterisk (*) is displayed next to the policy. This symbol indicates that there are unsaved or unpublished changes. To review these changes before publishing them, click the **View pending changes** link.

If a policy configuration has to be prioritized between the different levels, then the lowest-level policy takes precedence.

After you configure the policy settings, thin clients are notified about the changes. Changes take effect immediately after configuring the thin clients.

> ⓘ **NOTE: Certain settings, such as BIOS configuration for Windows Embedded Standard require a restart for the changes to take effect. However, most of the settings on ThinOS, you must restart the device for the changes to take effect.**

The policies are enforced in the following precedence:

- Global
- Group
- Device

Topics:

Add a group

To add a group, do the following:

1. On the **Groups & Configs** page, click the ➕ icon.
2. In the **Add New Group(s)** dialog box, enter the **Group Name** and **Description**.

   > ⓘ **NOTE: To change the name and description of a group, use Active Directory.**

3. In the **Registration** tab, select the **Enabled** check box under Group Token.
4. Enter the group token.

   > ⓘ **NOTE: The devices can be registered to a group by entering the group token which is available on the device registration screen.**

5. In the **Administration** tab, you can select the name of group admin(s), who should manage this group. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box. To move one group from the **Assigned Group Admins** to **Available Group Admins**, do vice versa.
6. Click **Save**.

   The group is added to the list of available groups on the **Groups & Configs** page.

Edit a group

To edit a group, do the following:

1 On the **Groups & Configs** page, click the ✎ icon.
2 In the **Editing Default Policy group** dialog box, edit the group information such as **Group Name** and **Description**.
3 In the **Registration** tab, edit the group token.

   ⓘ NOTE: **The devices can be registered to a group by entering the group token which is available on the device registration screen.**

4 Click **Save**.

Remove a group

As an administrator, you can remove a group from the group hierarchy. To remove a group, do the following:

1 In the **Groups & Configs** page, under **Group Tree Hierarchy**, click the 🗑 icon.

   A warning message indicating that this action removes one or more groups from the group tree hierarchy is displayed.

2 Click **Remove Group**.

   ⓘ NOTE: **When you remove a group from the group hierarchy, all users and devices that belong to the deleted group are moved to a selected group.**

Edit an unmanaged group

Devices that belong to the unmanaged group do not use licenses or receive configuration or application-based policies. To add devices to an unmanaged group, use the unmanaged group device registration key as part of auto registration or manual device registration. To edit an unmanaged group, do the following:

1 Click **Edit group**.

   The **Editing Unmanaged Group** page is displayed. The **Group Name** displays the name of the group.

2 Enter the following details:
   - **Description**—Displays a brief description of the group.
   - **Group Token**—Select this option to enable group token.

3 Click **Save**.

   ⓘ NOTE: **For a public cloud, the group token for an unmanaged group must be enabled to register devices. For a private cloud, the group token for an unmanaged group is automatically enabled.**

Configure a global level policy

To configure a global level policy, do the following:

1 In the **Groups & Configs** page, from the **Edit Policies** drop-down menu, select a device type.

   The policy settings of the respective device type are displayed.

2 Select the policy setting you want to configure, and then click **Configure this item**.

3 Click **Save and Publish**.

Configure a group level policy

To configure a group level policy or multilevel group polices, do the following:

1   In the **Groups & Configs** page, go to a group where you want to configure the policy, and click **Edit Policies**.
2   From the drop-down menu, select the device type you want to configure.
    The policy settings of the device type are displayed.
3   Select a policy setting and then click **Configure this item**.
4   Click **Save and Publish**.

Configure a device level policy

To configure a device level policy, do the following:

1   In the **Devices** page, click the device you want to configure.
    The **Device Details** page is displayed.
2   In the **Device Configuration** section, click **Create/Edit Exceptions**.

Edit the ThinOS policy settings

To edit the ThinOS policy settings, do the following:

1   Click **Groups & Configs**.
    The **Groups & Configs** page is displayed.
2   Click the **Edit Policies** drop-down menu.
3   Click **ThinOS**.
    The **Select ThinOS Configuration Mode** window is displayed.
4   Select your preferred mode to configure the policy settings. The available modes are:
    · Wizard Mode
    · Advanced Configuration Mode

    ⓘ NOTE: **To set the ThinOS Advanced Configuration as the default mode, select the check box.**
5   After configuring the policy settings, click **Save and Publish**.

ThinOS—Wizard mode

Use this page to configure the most frequently used parameters for the ThinOS devices. To configure the policy settings, do the following:

1   Select **Wizard** as the mode of configuration.
2   The following are the available policy settings on the **ThinOS—Wizard mode** page.

Figure 3. ThinOS—Wizard mode

- Setup Security
- Setup Keyboard and Display
- Setup Visual Experience
- Setup Timezone
- Setup General Settings
- Setup Broker

- Click **Next** to go to policy settings.
- Click **Back** to view the previous policy settings.
- Click **Cancel** to go back to the **Groups & Configs** page.
- Click **Save & Publish** to save the changes.
- Click **Continue** to go to ThinOS advanced configuration mode.

Configuring setup security settings

Use this page to configure the thin client security settings, such as user privilege and certificate installation.

(i) **NOTE:**

- Certificate assignment can be managed at global level, group level, or device level. When you select the **auto-install certificates** option, the list of certificates uploaded on the **File Repository Inventory** page is loaded.
- For automating certificates deployments, select the certificates to be automatically installed on thin clients.

Table 2. Configuring Privilege Settings

Option	Description
Privilege level	Select this option to define the default privilege level during system boot. From the drop-down menu, select any one of the following levels: • None—Disables all the system setting option. • High—Disables the connectivity settings except local customization.

Option	Description
	• Low—All settings are enabled on the local client.
Show Display Settings (8.5+)	Select this option to configure the display settings. From the drop-down menu, select a group to set the configuration access.
Allow lock down	Select this option to save the privilege level to the device so that the privilege level is also used when there is no network connection or when the configuration could not be fetched from the server. This is applicable is the privilege level is high.
Enable Keyboard and Mouse Settings (8.5+)	Select this option to configure the keyboard and mouse settings.
Enable Admin mode	Select this option to access the admin mode by entering the **Administrator User Name** and **Administrator Password**. This option can be enabled only if the privilege level is set to low or none.
Encrypted Credentials (8.5+)	Select this option to encrypt the login credentials.
Show Admin Mode button (8.5+)	Select this option to display local admin mode button on the sign-on Window.
Auto-install certificates	Select this option to automatically install the certificates. Once you select this option, the list of certificates in the file repository are displayed. Select the preferred certificate.
Enable VNC	Select this option to enable Virtual Network Computing (VNC) shadowing. VNC shadowing is the process which allows you to remotely share the same session as the user, see what the user sees, and assist with applications or session specific issues.
VNC Password	Enables you to set the VNC password. The password can contain a maximum of 16 characters.
Encrypt Password (8.5+)	Select this option to encrypt the password.

Configuring keyboard and display settings

Use this page to configure the thin client monitor display settings, such as resolution, and dual monitor.

Table 3. Configuring Keyboard Settings—ThinOS 8.5+

Option	Description
Keyboard Layout	Select the layout and language of the keyboard from the drop-down list.

Table 4. Configuring Monitor Display Settings

Option	Description
Enable Dual Monitor	Select the check box to enable dual monitor functionality.
Dual Monitor Mode	Select this option to select the monitor mode. From the **Display Monitor Mode** drop-down menu, select either **Mirror Mode** or **Span Mode**.

Option	Description
Auto detect monitors (8.5+)	Select the check box to detect the total number of monitors connected to the system. ⓘ **NOTE: If you select both the Auto detect monitors (8.5+) and Enable Dual Monitor option, then the configuration settings remain the same for both the single and dual monitor setup.**

Configuring visual experience

Use this page to configure the thin client visual experience settings, such as desktop display (Classic or Zero Launchpad) and session functionality.

Table 5. Configuring desktop appearance

Option	Description
Desktop Wallpaper	Displays only the images that are uploaded to the file repository. When you select this check box, the wallpaper file and the wallpaper layout drop-down menus are displayed.
Company Logo	Displays the logo on the device login screen. When you select this check box, the **Logo File** drop-down menu is displayed. You can upload the logo file from the file repository inventory.

Table 6. Configuring visual experience

Option	Description
Classic Desktop vs Zero Launchpad	Select this option to define the desktop experience. ⓘ **NOTE: Zero Launchpad is recommended for ThinOS Lite/ Xenith devices, and for full screen sessions. Classic Desktop is recommended for seamless applications.**
Enable Logon Main Menu (8.5+)	Select this option to enable the logon main menu.
Action after all session exit	Select this option to define the action after you close the last active session. From the drop-down menu, select any one of the following options: • None • Sign-off automatically • Shut down the system automatically • Restart the system automatically
Shutdown / Restart counter	Enter the seconds to wait before system restart. The valid values are 0–60.

Configuring timezone

Use this page to configure the thin client settings, such as time servers, and time zone.

Table 7. Timezone

Option	Description
Manually Set Time Zone	Select this option to override the system preference menu of the device with the time zone settings.
Date Format (8.5+)	Select the required date format.
Time Format (8.5+)	Select the required time format.
Time Servers	Enter the list of time servers to synchronize local time separated by a semicolon.

Configuring general settings

Use this page to configure the thin client firmware upgrade settings, such as live upgrade, firmware update logic, and platform firmware mappings.

> (i) NOTE:
>
> - Remote firmware imaging from the cloud is supported with the ThinOS firmware version 8.0_037 or later.

Table 8. Configuring Sign-on settings

Option	Description
Domain List (8.5+)	Enter the list of domains to sign-in to the broker server. Separate the names by a semi-colon.

Table 9. Firmware upgrade

Option	Description
Disable Live Upgrade	Live Upgrade enables the thin client immediately after download and applies the new firmware based on defined policies. If you prefer that the thin client should only check for new firmware on each boot, then disable the Live Upgrade feature.
Define desired platform or firmware mappings	This option maps the specific firmware versions to different platform types. To map a platform type to a specific firmware version, do the following: 1 From the **Platform Type** drop-down menu, select a platform. 2 From the **Firmware to auto-deploy** drop-down menu, select a firmware version. The list of platform types and the number of firmware versions currently uploaded to the **File Repository Inventory** page are displayed.

Table 10. Configuring local resources

Option	Description
Map SmartCards	Select this option to redirect the smart cards into the remote session.
Enable USB Redirection	Select this option to enable USB redirection on the devices. From the drop-down menu, select your preferred option.
Exclude disk devices	Select this option to exclude the disk devices.
Exclude audio devices	Select this option to exclude the audio devices.
Exclude printer devices	Select this option to exclude the printer devices.
Exclude video devices	Select this option to exclude the video devices.

Configuring broker settings

Use this page to configure the thin client remote connection and broker settings, such as addresses and credentials for brokers, such as, Citrix, Microsoft, VMware, and vWorkspace.

Table 11. Configuring broker server

Option	Description
Select the broker you are using	Select this option to establish a broker connection for a published desktop. From the drop-down menu, select any one of the following options: · Citrix · Microsoft · vWorkspace · VMware
Broker Server	Enter the broker server host name or IP address.
Citrix custom store name	Enter the citrix store name for the citrix StoreFront connection. This option is applicable only for Citrix.
Sessions to connect automatically	Select this option to automatically connect to the session. ⓘ NOTE: **The name of the desktop or application is case sensitive. Use a semicolon to separate the multiple sessions which must be initialized automatically.**
Reconnect At Logon	From the drop-down menu, select your preferred option. You can reconnect to both disconnected and active sessions. This option is applicable only for Citrix.
Security Mode	Select this option to set a security mode. From the drop-down menu, select your preferred option. This option is applicable only for VMware
Protocol	Select this option to choose a protocol. From the drop-down menu, select your preferred option. This option is applicable only for VMware.
Enable vWorkspace Gateway	Select this option to enable vWorkspace gateway functionality. This option is applicable only for vWorkspace.

ThinOS—Advanced mode

Use this page to configure the advanced policy settings for the ThinOS devices. To configure the advanced policy settings, do the following:

1 Select **Advanced Configuration** as the mode of configuration.

2 The following are the available policy settings on the **ThinOS** page.
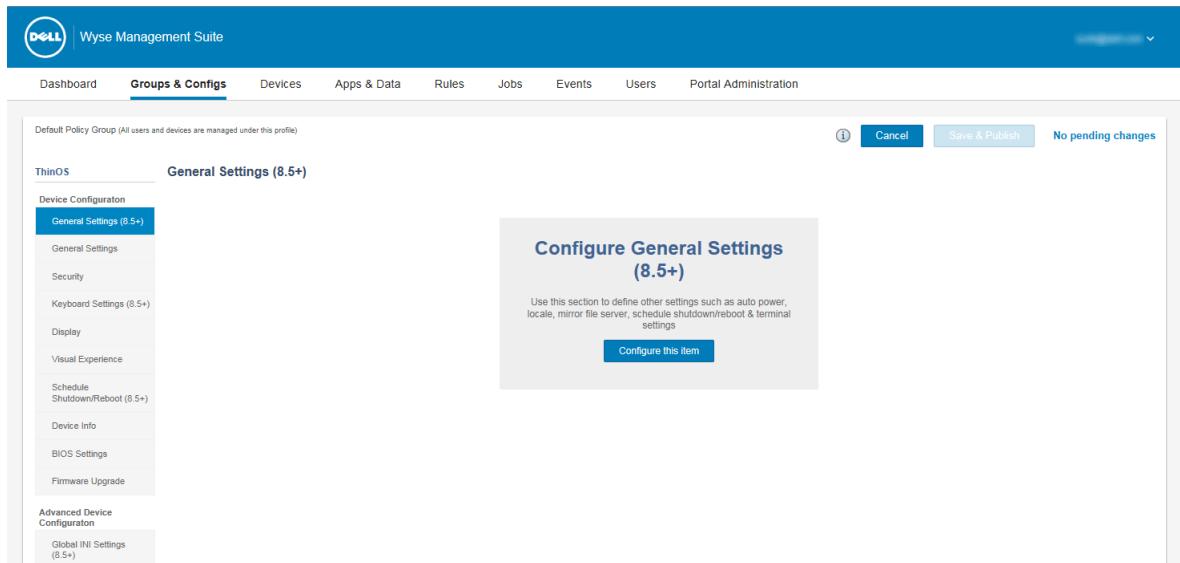
Figure 4. ThinOS—Advanced mode

- · **Device Configuration**
- · **Advanced Device Configuration**
- · **Remote Connection (Legacy)**
- · **Remote Connection (8.5+)**
- · **Printers (8.5+)**
- · **Network Settings (8.5+)**

3 Click **Save & Publish** to save your changes.

4 Click **Remove Policy** to go back to the **ThinOS** page.

5 Click **Cancel** to go back to the **Groups & Configs** page.

Configuring general settings

Use the **General Settings** page to configure the thin client general settings, such as auto power settings, local settings, mirror file server settings, and terminal settings for ThinOS 8.5 and later version devices.

Table 12. Configuring general settings

Option	Description
Auto Power	The **Auto Power** check box specifies about how the system starts when the power is first applied to the unit.

Table 13. Configuring keyboard options

Option	Description
Load the language file	Select this option to install the language files on ThinOS devices.
System Language	Select this option to set the language for the system. From the drop-down list, select your preferred option.
Locale file name	Select this option to select the certificate to install on the device. From the drop-down list, select the certificates added in the file repository.
Font file name	Select this option to select the font file to install on the device. From the drop-down list, select the font files added in the file repository.

Table 14. Configuring mirror file server

Option	Description
Mirror File Server	If the **FileServer** is offline, this setting allows you to store a local copy of the configuration in cache.

Table 15. Configuring terminal settings

Option	Description
Terminal Name	Enter the terminal name. You can also use the system variables to automate renaming multiple devices.
Terminal Reboot	If this setting is enabled, the system is forced to restart after the terminal name is changed. Restart the system to view the changes.
Inactive	Select this option to restart or shut down the system depending on the option you have selected from the **Action after All Sessions Exit** drop-down list in the **Visual Experience** policy setting for the ThinOS devices. Enter the time value in minutes. The range of inactive time is 0–480 seconds.
No Session Timer	Select this option to restart or shut down the system depending on the option you have selected from the **Action after All Sessions Exit** drop-down list in the **Visual Experience** policy setting for the ThinOS devices. Enter the time value in minutes. The range of inactive time is 0–480. ⓘ **NOTE: This setting only applies if the Inactive value is set to 0.**

Table 16. Configuring audio settings for ThinOS 8.6 and later versions

Option	Description
Configure Audio settings	Select this option to configure the audio settings.
Analog Audio Jack pop-up	Select this option to display the audio selection message when you plug in the analog headset.
Mute	Select this option to enable or disable the mute option. From the drop-down list, select one of the following option: · No mute · Mutes audio · Mutes audio and system beep

Option	Description
	• Mutes system beep
Microphone Volume	Select the option to set microphone volume levels. From the drop-down list, select one of the following option: • High • Middle • Low
Microphone Mute	Select this option to mute the microphone.
Disable Audio over display port	Select this option to disable the audio over the display port.
Microphone boost	From the drop-down list, select the preferred option. The available options are: • Yes—Enables the OnBoard microphone boost. • No—Disables the OnBoard Microphone boost. • 1,2,3,4—Increases the decibel value of the mic.
Playback Buffering Cache	From the drop-down list, select the preferred option. This option allows you configure ThinOS audio playback minimum buffering amount in ten millisecond units. This option can be used when network bandwidth is not large enough to play the audio smoothly. The available options are: • 1—ThinOS buffers at least 10 ms of audio data when playing audio. • 50—ThinOS buffers at least 500 ms (0.5s) of audio data when playing audio.
EnableSpeaker	Select this option to enable the internal loud speaker.
Playback Device	Enter the playback device name.
Recording Device	Enter the recording device name.
Mic Gain Device	Enter the device name on which you want the mic gain.
Mic Gain Level	Enhances the mic gain by number of times the specified value.
Volume	From the drop-down list, select the level of the volume.

Table 17. Configuring mouse settings for ThinOS 8.6 and later versions

Option	Description
Configure Mouse settings	Select this option to configure the mouse settings.
Mouse Speed	From the drop-down list, select the mouse speed is sufficient.
Mouse Swap	Select this option to enable the mouse swap buttons.
Touch Screen Drag	Select this option to enable the drag option on the touch screen.
Invert Scroll Wheel	Select this option to invert the mouse scroll wheel.
Big Cursor	Select this option to increase the local mouse to twice as normal one.
Disable	Select this option to disable the mouse pointer on the screen.

Configuring general settings

Use **General Settings** page to configure the ThinOS thin client settings, such as sign-on settings, and time zone.

Table 18. Configuring sign-on settings

Option	Description
Default user name	Enter the default user name for the local sign-on screen.
Default Password	Enter the default password for the local sign-on screen.
Domain Name	Enter the default domain name for the local sign-on screen. ⓘ **NOTE: You can enter multiple domain names separated by a comma with a maximum of 31 characters.**
Remember last user name at logoff	Select this option to store the user name when you log off the system. From the drop-down list select the preferred option. ⓘ **NOTE: The user name is not stored if the system is restarted or the system is turned off.**
Disable Domain Field (8.5+)	Select the check box to disable the domain field option on the sign-on window.
Domain List (8.5+)	Enter the list of domains mentioned on the sign-on window. Use a semi-colon to separate the domain name.
Remember last user name and/or domain at reboot/shutdown	Select this option to store the user name or domain when the system is restarted or turned off.

Table 19. Configuring timezone settings

Option	Description
Manually Set TimeZone	Select the check box to override the system preference menu settings. From the **Timezone** and **Enable Daylight Savings** drop-down menu, select your preferred option.
Date Format (8.5+)	From the **Date Format (8.5+)** drop-down menu, select the appropriate format.
Time Format (8.5+)	From the **Time Format (8.5+)** drop-down menu, select the appropriate format.
Time Servers	Enter the list of time servers to synchronize local time separated by a semi-colon.

Configuring security settings

Use the **Security Settings** page to configure the ThinOS thin client security settings, such as sign on settings, privilege settings, the G-key reset, and so on.

Table 20. Configuring sign on settings

Option	Description
Require domain login	From the **Require domain login** drop-down menu, select the preferred option.
Disable guest user	Select the check box to disable the local guest user account.
Require reentering password	Select the check box to enter the password again while signing in.
Require smartcard	From the **Require smartcard** drop-down menu, select the preferred option.

Table 21. Configuring privilege settings

Option	Description
Privilege level	Select this option to define the default privilege level during system boot. From the drop-down menu, select any one of the following levels: · None—Disables all the system setting menus. · High—Disables the connectivity settings, but the local customization is enabled. · Low—All settings are enabled on the local client.
Show Display Settings (8.5+)	Select this option to configure the display settings. From the drop-down menu, select a group to set the configuration access.
Enable Keyboard and Mouse Settings (8.5+)	Select this option to configure the keyboard and mouse settings.
Disable Date and Time Settings (8.5+)	Select this option to configure the date and time settings.
Network location to upload (8.5+)	Enter the location to upload the network trace, network capture, and log files.

Table 22. Configuring administrator mode

Option	Description
Enable Admin mode	Select the check box to enable the admin mode. When privilege level is **low** or **none**, you can access the admin mode by entering the user name and password.
Encrypted Credentials (8.5+)	Select the check box to encrypt the credentials.
Show Admin Mode button (8.5+)	Select the check box to display the admin mode option on the sign on window.

Table 23. Configuring general settings

Option	Description
Enable the Gkey reset	Select this option to reset the factory settings of the device. While restarting the system, press the G key to reset the factory settings.
Enable Trace	Select this option to trace the files. This parameter enables the ICA or RDP trace mode and the trace file is created in the directory.
Remove Certificate (8.5+)	Select this option to remove the certificate.
Delete Certificate (8.5+)	Select this option to delete the certificate. Enter the certificate name which you want to delete.
Auto-install Certificates	Select this option to install the certificate automatically.
Disable ThinPrint Service	Select this option to disable the **ThinPrint** service.
Encrypt local Flash	Select this option to configure the local settings, and set the user credentials. Select this check box if you want to encrypt local flash.
Disable VNC Shadowing	Select this option to disable the VNC shadowing.
Fast Disconnect Key	Select this option to use the fast disconnect key. ⓘ NOTE: **To disconnect from the Citrix sessions, press the F12 key.**

Table 24. Configuring security policy

Option	Description
Security Policy (8.5+)	From the **Security Policy (8.5+)** drop-down menu, select the global security mode for SSL connection.
Secured Network Protocol (8.5+)	Select this option to secure the network protocol. The unsecure network protocols are disabled.
TLS Minimum Version (8.5+)	Select this option to choose the minimum version of SSL connection for the ThinOS devices.
TLS Maximum Version (8.5+)	Select this option to choose the maximum version of SSL connection for the ThinOS devices.
DNS File Server Discover (8.5+)	Select this option to discover the DNS file server.

Table 25. Configuring VNC settings

Option	Description
Enable VNC	Select this option to enable VNC shadowing.
VNC Password	Enter the VNC password with a maximum of 16 characters.
Encrypt Password (8.5+)	Select this option to encrypt the password.
Max Concurrent VNC (8.5+)	From the drop-down menu, select the maximum number of concurrent VNC connections.
Zlib Compression (8.5+)	Select the check box to enable the Zlib compression.
Prompt user on start	Select this option to perform the shadowing process on the terminal.

Option	Description
Query user timeout	Enter the total amount of time in seconds to accept or reject the shadowing session. The range is 10–600 seconds.
Promt user on end	Select the check box to notify the end of a remote shadowing session.
View only	Select the check box to disable the keyboard or mouse events on the system during a shadowing session.
Force 8–bit	Select this option to configure the display settings. Select the check box to use 8–bit per pixel.

Table 26. Configuring WDM services

Option	Description
Disable WDM Services	Select this option to disable the WDM service.
Quick Mode (8.5+)	Select this option to speed up the boot time for the ThinOS devices.

Configuring keyboard settings

Use the **Keyboard Settings** page to configure the keyboard layouts, and the behavior of keyboard shortcuts for ThinOS 8.5 and later version devices.

Table 27. Configuring keyboard settings

Option	Description
Character Set	Select this option to set an appropriate character set. From the drop-down list, select your preferred character set.
Keyboard Layout	Select this option to set an appropriate keyboard layout. From the drop-down list, select your preferred keyboard layout.
Keyboard Repeat Delay	Select this option to set the time that a key can be pressed without repeating the letter as input. From the drop-down list, select the option based on your preference.
Keyboard Repeat Rate	Select this option to set the repeat rate for your keyboard. The repeat rate is the speed at which the key input repeats itself when you press and hold down the key on your keyboard. From the drop-down list, select one of the following options based on your preference: · Slow · Normal · Fast
Key Sequence	Select the check box to enable the key sequence.
Ctrl-Alt-Del	Press the **Ctrl-Alt-Del** keys to lock the system.
Ctrl-Alt-Up	Press the **Ctrl-Alt-Up** keys to switch the session between fullscreen and window mode.
Ctrl-Alt-Down	Press the **Ctrl-Alt-Down** keys to switch between task selection.
Ctrl-Alt-Left	Press the **Ctrl-Alt-Left** keys to lock the system.
Ctrl-Alt-Right	Press the **Ctrl-Alt-Right** keys to lock the system.

Option	Description
Win + L	Press the **Win+L** keys to lock the system.
Alt-Tab	Press the **Alt-Tab** keys to lock the system.

Configuring display settings

Use the **Display Settings** page to configure the ThinOS thin client monitor display settings, such as resolution, rotation, color depth, and dual monitor.

Table 28. Configuring monitor display settings

Option	Description
Enable Dual Monitor	Select the check box to enable dual monitor functionality.
Dual Monitor Mode	Select this option to select the monitor mode. From the **Display Monitor Mode** drop-down menu, select either **Mirror Mode** or **Span Mode**.
Main Screen	Select this option to access the main screen. From the **Main Screen** drop-down menu, select either **Screen 1** or **Screen 2**.
Alignment	Select this option to align the monitor screen. From the **Alignment** drop-down menu, select your preferred option.
Layout—ThinOS 8.5+	Select this option to select either **Landscape** or **Portrait** layout.
Taskbar—ThinOS 8.5+	Select this option to select the placement of the taskbar on the screen. From the **Taskbar (8.5+)** drop-down menu, select either **MainScreen** or **WholeScreen**.
Auto detect monitors—ThinOS 8.5+	Select the check box to detect the total number of monitors connected to the system. ⓘ **NOTE: If you select both Auto detect monitors (8.5+) and the Enable Dual Monitor option, then the configuration settings remain the same for both the single and dual monitor setup.**
Desktop Color Depth	Select this option to set the color depth for your desktop. From the **Desktop Color Depth** drop-down menu, select either **16-bit** or **32-bit**.

Table 29. Configuring primary monitor settings

Option	Description
Monitor Resolution	Select this option to set the resolution for your monitor. From the drop-down menu, select the appropriate resolution for your monitor.
Monitor Rotation	Select this option to define the rotation. From the drop-down menu, select the appropriate rotation direction.
Monitor Refresh Rate—ThinOS 8.5+	Select this option to set the refresh rate for your monitor. From the drop-down menu, select the appropriate refresh rate for your monitor.

Table 30. Configuring secondary monitor settings

Option	Description
Monitor Resolution (8.5+)	Select this option to set the resolution for your monitor. From the drop-down menu, select the appropriate resolution for your monitor.
Monitor Rotation (8.5+)	Select this option to define the direction—Left, Right, or None—to enable the rotation. From the drop-down menu, select the appropriate rotation direction.
Monitor Refresh Rate (8.5+)	Select this option to set the refresh rate for your monitor. From the drop-down menu, select the appropriate refresh rate for your monitor.

Table 31. Configuring screen saver settings

Option	Description
Screen saver (8.5+)	Enter the screen saver time in minutes.
Lock the terminal (8.5+)	Select this option to set the terminal in lock state when the screen saver time is activated. From the **Lock the terminal (8.5+)** drop-down menu, select the any one of the following options: · 0–Disabled · 1–Unlock with password only and wallpaper is displayed · 2–Unlock with password only and a black screen is displayed · 3–Unlock with user name and password only and a black screen is displayed
Screen Saver Type (8.5+)	Select this option to specify which screen saver to use. From the **Screen Saver Type (8.5+)** drop-down menu, select the preferred option.
Sleep (8.5+)	Select this option to specify the time interval in minutes to stop the soft screen saver and turn off the monitor. From the **Sleep (8.5+)** drop-down menu, select the preferred option.

Configuring visual experience settings

Use the **Visual Experience** page to configure the ThinOS thin client visual experience settings, such as desktop theme and behavior after session exit.

Table 32. Configuring desktop appearance

Option	Description
Desktop Color (8.6+)	Enter the background color of the local desktop.
Desktop Wallpaper	Displays only the images that are uploaded to the file repository. When you select this check box, the following options are displayed: · Disable wallpaper · Enable wallpaper · Dell default wallpaper (8.6+) · Wyse default wallpaper (8.6+)

Option	Description
	ⓘ NOTE: When you select the Enable wallpaper option, the wallpaper file and wallpaper layout is displayed.
Company Logo	Displays the logo on the device login screen. When you select this check box, the **Logo File** drop-down menu is displayed. You can upload the logo file from the file repository inventory.
EULA at login	Displays the end-user license agreement at each login. When you select this check box, the **EULA file** drop-down menu is displayed. By using this option, you can upload a plain text file.

Table 33. Configuring visual experience

Option	Description
Classic Desktop vs Zero Launchpad	Select this option to define the desktop experience. ⓘ NOTE: Zero Launchpad is recommended for ThinOS Lite or Xenith devices, and for full screen sessions. Classic Desktop is recommended for seamless applications.
Prevent toolbar from closing unless mouse focus moves away	Select this check box if you want to prevent the toolbar from closing unless mouse focus moves away.
Disable Home Icon	Select this option to disable the home icon.
Enable Logon Main Menu (8.5+)	Select the check box to enable the main menu screen on the desktop when you log in to the system.
Enable the Zero toolbar activation in left margin	Select this option to select any one of the following options to activate the Zero toolbar: · No · On mouse over after specified seconds · Only after clicking
Toolbar Disable Mouse	Select the check box to disable the mouse functionality when the zero toolbar option is enabled.
Toolbar Click (8.5+)	Select the check box to enable the toolbar click option when the zero toolbar option is enabled.
Number of seconds before toolbar is activated	Select this option to set the time (in seconds) before the toolbar is activated. Select one of the following timings based on your preference: · 0.5 seconds · 1 second · 1.5 seconds · 2 seconds
Action after all session exit	Select this option to define the action after you close the last active session. From the drop-down menu, select any one of the following options: · None · Sign-off automatically · Shut down the system automatically

Option	Description
	• Restart the system automatically.

Schedule shutdown or reboot settings

Use the **Schedule Shutdown/Reboot (8.5+)** page to configure a scheduled restart or shutdown for ThinOS 8.5 and later version devices.

Table 34. Schedule shut down or reboot

Option	Description
Scheduled Reboot	Select the check box to specify the time or day to schedule a system restart.
Scheduled Shutdown	Select the check box to specify the time or day to schedule a system shutdown.
Idle Time	Enter the Idle time. The system restarts in an active session when the value of the Idle time is set to 10 minutes.
Reboot/Shutdown Time	Enter the time when the system must restart or shut down. Set the time in 24-hour format.
Reboot/Shutdown End	Enter the time to stop the system restart or shut down process. Set the time in 24-hour format.
Days	Select the check box to specify the days when you want to restart or shut down the system.

Configuring device information

Use the **Device Info** page to set the ThinOS device details.

Table 35. Configuring device information

Option	Description
Location	Enter the device location.
Contact	Enter the device contact.
Custom 1 to 3	Enter the custom values.

Configuring BIOS settings

Use the **BIOS Settings** page to configure the BIOS settings of ThinOS thin clients.

Table 36. System configuration

Option	Description
Enable Audio	Select this check box to enable the audio device.

Table 37. Configuring security settings

Option	Description
Admin Setup Lockout	Select this option to prevent others from entering the setup when an admin password is set.

Table 38. Configuring administrator password settings

Option	Description
Enable Admin Password	Select this check box to enable the BIOS administrator password.
Admin Password	Enter the new BIOS administrator password. This option is available only if you select the **Enable Admin Password** check box.

Table 39. Configuring auto-on settings

Option	Description
Auto On Time	From the drop-down list, set the time of the day that you want the system to turn on automatically.

Table 40. Configuring USB

Option	Description
Enable Rear-Left Dual USB 2.0 Ports	Select this check box to enable the device attached to this port. If you select this check box, the device is available to the operating system. However, if the USB port is disabled, the operating system cannot detect the device attached to this port. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.
Enable Front USB Ports	Select this check box to enable the device attached to this port. If you select this check box, the device is available to the operating system. However, if the USB port is disabled, the operating system cannot detect the device attached to this port. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.
Enable USB Boot Support	Select this check box to enable the USB boot setup. Allows you to boot any type of USB mass storage devices.

Table 41. Configuring power management settings

Option	Description
AC Recovery	From the drop-down list, select an option to specify how the system must behave when the AC power is restored.
Wake On LAN	From the drop-down list, select an option to allow the thin client to power up from the OFF state. You can trigger a thin client to power up from the off state by using a LAN signal.
Wake On USB	Select this option to to enable USB devices to wake the system from OFF state or from the hibernate state.

Table 42. Reboot schedule

Option	Description
Reboot Option	Some BIOS settings requires the system to restart. From the drop-down list, select one of the following options: • Reboot immediately—The system restarts immediately. • Reboot later—Select the **Reboot Hour** and **Reboot Minute** to set the system restart time. • Do not reboot—The system does not restarts.

Configuring firmware upgrade

Use the **Firmware Upgrade** page to configure the ThinOS thin clients firmware upgrade settings, such as live upgrade, firmware update logic, local firmware check preferences, and platform firmware mappings.

Table 43. Configuring firmware upgrade

Option	Description
Disable Live Upgrade	This parameter automatically installs the new firmware on the thin client based on the defined policies immediately after you restart the thin client. To check for new firmware on each restart, disable this option.
Firmware Update Logic	This parameter determines how the thin client behaves when the new firmware is published from the management console. From the drop-down menu, select any one of the following options: • Do not update—Thin client ignores the firmware versions assigned to the management policies. • New firmware only—Thin client updates the firmware only when a newer version is assigned to the management policy. • Any different firmware—Thin client updates the firmware to the version assigned by the management policy—even if the version is lower than the current image on device.
Skip Local Firmware Check	Select this option to enable the thin client to bypass the local file server checks for the firmware updates. ⓘ **NOTE: Dell recommends that you enable this option if you define a firmware on the management console. It leads to an endless restart as the thin client applies differing images, if you have firmware policies in the management console and firmware on a local file server.**
Verify Signature	Select the check box to verify the signature.
Enable BIOS Upgrade	Select this option to enable the BIOS upgrade process.
Select BIOS File	Select this option to choose the BIOS file which is uploaded in the file repository. From the drop-down menu select the BIOS file.
Define desired platform or firmware mappings	This option maps the specific firmware versions to different platform type. To map a platform type to a specific firmware version, do the following: 1 From the **Platform Type** drop-down menu, select a platform.

Option	Description
	2 From the **Firmware to auto-deploy** drop-down menu, select a firmware version. The list of platform types and the number of firmware versions currently uploaded to the **File Repository Inventory** page are displayed.

Configuring device settings

Use the **Device Settings** page to configure the mouse, keyboard, monitor, time zone, printers, audio, and network settings for ThinOS 8.6 and later versions.

Table 44. Device Settings Preference

Option	Description
Device Settings Managements	From the drop-down list, select the preferred option. The available options are: • Disable manual override—Select this option to disable manual overriding for all the devices with Wyse Management Suite configurations. • Enable all manual overrides—Select this option to manually override all the devices with client configurations. • Enable selective manual overrides—Select this option to manually override the selected devices with specific client configurations.
Monitor	Select this option to manually override the monitor settings. This option is applicable if you have selected the **Enable selective manual overrides** option.
Mouse	Select this option to manually override the mouse settings. This option is applicable if you have selected the **Enable selective manual overrides** option.
Keyboard	Select this option to manually override the keyboard settings. This option is applicable if you have selected the **Enable selective manual overrides** option.
Timezone	Select this option to manually override the time zone settings. This option is applicable if you have selected the **Enable selective manual overrides** option.
Printer	Select this option to manually override the printer settings. This option is applicable if you have selected the **Enable selective manual overrides** option.
Audio	Select this option to manually override the audio settings. This option is applicable if you have selected the **Enable selective manual overrides** option.
Network	Select this option to manually override the network settings, such as WLAN or static IP. This option is applicable if you have selected the **Enable selective manual overrides** option.

Configuring global INI settings

Use the **Global INI settings** page to configure global INI settings for ThinOS 8.5 and later version devices.

Table 45. Configuring global INI settings

Option	Description
Global INI	From the drop-down list, select your preferred option. A **global.ini** file contains the global parameters for all the devices. The parameters can be existing **wnos.ini** or a newly created .INI file which is uploaded to the file repository.

Configuring central configuration settings

Use the **Central Configuration** page to specify a file server where the ThinOS thin clients checks for configuration and image updates.

Table 46. Central configuration

Option	Description
File Server/Path	Enter the full path of folder that contains the **wnos** file. Supported protocols include ftp, http, and https. The default protocol is ftp.
User	Enter the user name to access the file server.
Password	Enter the password to access the file server.

Configuring advanced settings

Use the **Advanced Settings** page to configure additional settings which are ThinOS thin client specific INI parameters or to disable the local INI check. Dell recommends that you do not include the INI parameters for policies which are already configured in other options. Password encoding and encryption are not applied to password parameters.

Table 47. Configuring advanced settings

Option	Description
No Global INI	If selected, the global INI parameter from the file server is not downloaded.
	Enter the INI parameter from line 1 to line 20 for the thin clients.

Configuring remote connections

Use the **Remote Connections** page to configure the ThinOS thin clients remote connection settings, such as addresses and credentials for broker and direct connections.

Table 48. Configuring connection broker settings

Option	Description
Select Broker	Select this option to establish a broker connection for published desktop. From the drop-down menu, select any one of the following options:

Option	Description
	· None · Citrix · Microsoft · vWorkspace · VMware ⓘ NOTE: ThinOS Lite/Xenith devices support the Citrix broker connection.
Manually define direct RDP connections	Select this option to define the RDP connections manually. When you select this option, the **Direct Connections (RDP)** box is displayed.
Broker Server	Enter the broker server host name or IP address.
Citrix StoreFront	Select this option to enable the Citrix StoreFront based layout of published applications and desktops on the device. This option is applicable only for Citrix.
Display on Desktop	From the drop-down list, select an option that you want to display on the desktop. This option is applicable only for Citrix.
Automatically Connect to sessions	Select this option to automatically connect to the session. This option is applicable only for Citrix, VMware, and vWorkspace.
Use recommended settings for settings	Select this option to choose the recommended settings. This option is applicable only for Citrix.
Manually define direct RDP connections	Select this option to define the RDP connections manually. If you select this option, the **Direct Connection** box is displayed.
Configure TS Gateway	Select this option to configure the TS gateway. If you select this option, the **TS Gateway Settings** table is displayed. This option is applicable only for Microsoft.
Security Mode	Select this option to set a security mode. This option is applicable only for VMware.
Protocol	Select this option to choose a protocol. This option is applicable only for VMware.

Table 49. Configuring Direct connections (RDP)

Option	Description
Connection Name	Enter the name of the connection.
Host Name or IP Address	Enter the host name or IP address of the connection.
Auto Start	Select this option to restart the connection automatically.
Reconnect After Disconnect	Select this option to reconnect the connection automatically after the connection is disconnected.
User Name	Enter the user name for remote login.
Password	Enter the password for remote login.
Domain Name	Enter the domain name for remote login.

Option	Description
Color depth	Select this option to set the color depth. From the drop-down list, select the color depth for remote login.
Session Window Behavior	Select this option to set the session window behavior. From the drop-down list, select whether the remote connection should be started in the window mode or full screen mode. ⓘ NOTE: **The Zero launchpad mode only supports full screen sessions and the window mode is launched on a single screen. The full screen spans between both the monitors.**
Audio Playback	This option helps you to manage audio settings in the remote session. From the drop-down menu, select any one of the following options based on your preference: • Play locally • Play on remote computer • Do not Play

Table 50. Session behavior defaults

Option	Description
Font Smoothing	Select this option to enable font smoothing. Font smoothing is a method to obtain sharper fonts in low resolution screens.
Advanced RDP protocol features	Select this option to configure the features of an RDP protocol.
Default color depth for connections	Select this option to set the color depth for your connection. From the drop-down list, select a color depth for remote login.
Session Window Behavior	Select this option to set the session window behavior. From the drop-down list, select whether the remote connection should be started in the window mode or full screen mode. This option is applicable only for Citrix. ⓘ NOTE: **The Zero launchpad mode only supports the full screen sessions, and the window mode is launched on a single screen. The full screen spans between two monitors.**
USB Redirection Technology	Select this option to enable USB redirection. USB redirection is a technology that Select this option to access the USB devices that are connected to the thin client from within a remote desktop or application. This option is applicable only for Citrix.
Audio quality	Select this option to set the audio quality. This option is applicable only for Citrix.
Map USB disks to	From the drop-down list, select the disk space to assign to the USB. This option is applicable only for Citrix.
Enable Seamless Mode	Select this option to set the seamless mode. A **seamless** interface is the joining of two computer programs so that they appear to be one program with a single user interface. This option is applicable only for Citrix.
Hide taskbar in Seamless Mode	Select this option to hide the taskbar in seamless mode. This option is applicable only for Citrix.

Table 51. Configuring HDX protocol settings

Option	Description
Improve KB over high latency	From the drop-down list, select the preferred option that improves KB over high latency.
Improve Mouse over high latency	From the drop-down list, select the preferred option that improves mouse over high latency.
Auto-connect	From the drop-down list, select and enable the preferred option to connect the remote connection automatically. • Multimedia redirection • Enable Session Reliability • Enable progressive Display • Enable ICA Ping • Offscreen support

Table 52. Configuring peripheral behavior

Option	Description
Auto-connect selected local	Select this option to automatically connect the following peripherals: • Printers • Serials • Smartcards • Sound
Enable USB storage disks	Select this option to enable USB storage disks. From the drop-down menu, select any one of the following options: • No • Yes (Read or write) • Yes (Read-only)
Enable USB Redirection	Select this option to enable the USB redirection. From the drop-down menu, select any one of the following options: • No • Yes, redirect all USB devices • Yes, but exclude some devices ⓘ NOTE: You also have an option to exclude disk, printer, audio, and video devices.
Mouse Queue timer	Select this option to set the mouse queue timer in an ICA or RDP session. The range of the mouse queue timer is 0–99.

Table 53. Configuring additional settings

Option	Description
Maximum Bitmap Cache	To set the maximum bitmap cache for your RDP session, enter a number from 128 to 1024.
4 pixel Aligned Session Width	Select this option to enable the 4-pixel aligned session width.
Automatically reconnect sessions at logon?	Select this option to enable the thin client to automatically reconnect the session at login. This option is applicable only for Citrix.
Automatically reconnect from button menu?	Select this option to enable the thin client to automatically reconnect the session from the button menu. This option is applicable only for Citrix.
Account Self-service server	Enter the server details.
Access Gateway authentication method	From the drop-down list, select the method to access the gateway authentication.
Use HTTP for browsing	Select this option to enable HTTP for browsing. This option is applicable only for Citrix.
Alternate address via firewall	Select this option to enable an alternate address through firewall. This option is applicable only for Citrix.
System Menu	Select this option to set the system menu. This option is applicable only for Citrix.
Disable Reset VM	Select this option to disable the VM reset. This option is applicable only for Citrix.
Show 32–bit icons for the first of connections	Enter the 32-bit icons for the first set of connections. This option is applicable only for Citrix.

Configuring global session settings—ThinOS 8.5 and later versions

Use the **Global session settings** page to configure VDI global settings for ThinOS 8.5 and later version devices.

Table 54. Configuring local resources settings

Option	Description
Map Printers	Select this option to automatically connect the local printers when the session starts.
Map Serials	Select this option to automatically connect the local serials when the session starts.
Map SmartCards	Select this option to redirect the smartcards to the remote session.
Map Sound	Select this option to enable the local system sound when the session starts.
Map Disks	Select this option to enable map disks. You can automatically connect the USB drives for ICA and RDP connections when the session starts.
Disks Read Only	Select this option to enable read-only disks.

Option	Description
Enable USB Redirection	Select this option to redirect the USB drives to the remote session. From the drop-down list, select your preferred option. If **Exclude some devices** option is selected, you can exclude the following devices from the session: • Exclude disk devices • Exclude audio devices • Exclude printer devices • Exclude video devices
Display on desktop (8.6+)	From the drop-down list, select your preferred option.
Enable Whitelist or Disable Blacklist	Use this option to enable whitelist or disable blacklist. By default, **Do not enable whitelist or blacklist** is selected. ⓘ NOTE: **The device restarts when you enable this option.** The following options are displayed when you select **Enable whitelist** or **Enable blacklist**: • Class • USB Class • Vendor ID

Table 55. Configuring advanced settings

Option	Description
Reconnect After Disconnect	Select this option to reconnect the connection automatically after the connection is disconnected.
Multi-Monitor	Select this option to enable the multi-monitor support. The height and width of the session desktop is similar to the local virtual desktop size.
Turn Compression off	Select this option to compress the file size and to reduce the time required to download the files.
Optimize for low link speed	Select the check box to optimize session settings for low link speed.
Full Screen Mode	Select this option to set the connection window in the full screen mode.
Fast Disconnect Key	Select this option to use the fast disconnect key. ⓘ NOTE: **To disconnect from the sessions, press the F12 key.**

Configuring USB redirection settings

Universal Serial Bus (USB) redirection is a technology that enables you to plug an external device into a USB port on the endpoint and access the device from within a remote desktop or application. You can configure the USB to redirect automatically to a particular device. Use the **USB redirection settings** page to force redirect the USB connected devices to the remote session for ThinOS 8.5 and later version devices.

Table 56. USB redirection settings

Option	Description
Force Redirect	Enter the force redirect device ID.
Force Local	Enter the force local device ID.
Redirect Type	From the drop-down list, select the redirection type. ⓘ NOTE: **If PCoIP or Blast connection type is selected, then do not select any value.**
Interface Redirect	Select this option to enable the interface redirection option.

Configuring third party authentication settings

Use **Third party authentication** settings page to configure Single Sign-On (SSO) authentication settings for ThinOS 8.5 and later version devices.

Table 57. Configuring authentication settings

Option	Description
Authentication Mode	Select this option to specify the authentication mode. From the drop-down menu, select any one of the following options: • Imprivata • Caradiam • SecureMatrix • HealthCast

Table 58. Configuring RF-ID settings

Option	Description
Rf-Id Disable Beep	Select this option to disable RFID beep. Radio-Frequency Identification—RFID is the use of radio waves to read and capture information stored on a tag attached to an object. A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader. RFID authentication provides a quick access to a system to perform short tasks, you can use fast user identification through radio-frequency identification (RFID).
Disable Keystroke	Select this option to disable keystroke functionality. A keystroke is a single press of a key on a keyboard. Each key press is a keystroke. The keyboard is used as an input port for sending signals.
Set Card Type	Select this option to set the card type. **RFID** cards contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader which is also known as an interrogator.
Disable Initialization	Select this option to disable the RFID authentication.
Disable LED	Select this option to disable the LED.

Table 59. Configuring imprivata settings

Option	Description
Imprivata OneSign Server	Enter the host name or the IP address with optional TCP port number or URLs of the imprivata OneSign server.
Kiosk Mode	Select this option to enable the kiosk mode. If enabled, then different OneSign user can unlock the client desktop.
Enable Windows Authentication	Select this option to enable Windows authentication. If enabled, the OneSign sign fails. Sign in to the predefined broker with Windows credentials.
Auto-Access	From the drop-down menu, select your preferred option.
Net BIOS Domain Name	Select this option to enable the Net BIOS domain name option. If enabled, the Net BIOS domain name is listed in the imprivata domain list.
Suspend Action	From the drop-down menu, select your preferred option. If you select 0, then lock the terminal, and if you select 1, then sign off the terminal.
Disable HotKey	Select this option to disable the HotKey functionality.
Disable Prompt To Enroll	Select this option to disable the prompt to enroll option. If disabled, then ThinOS system does not prompt to enroll their security answers after OneSign sign on.
Security Mode	From the drop-down menu, select your preferred option. The security mode species the SSL certification validation policy.

Table 60. Configuring Caradigm settings

Option	Description
SSO CM Server	Enter the name of the Single Sign-On (SSO) and Context Management (CM) server. You can use single sign-on authentication with Web or desktop applications. The server authenticates the user information.
Default Group Name	Enter the name of the default group name.
Enable LogOff	Select this option to enable the logoff functionality.
Caradigm Security Mode	From the drop-down menu, select your preferred option. This option helps the health care providers to quickly and securely log in to the clinical applications.
Caradigm LogLevel	From the drop-down menu, select your preferred option. **Caradigm LogLevel** allows separation of the software that generates messages, the system that stores the messages, and the software that reports and analyzes the messages. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.
Disable Manual Logon	Select this option to disable the manual logon functionality.

Table 61. Configuring SecureMatrix settings

Option	Description
Secure Matrix Server	Enter the secure matrix server details. You can manage admin access, enforce password policies, and add multifactor authentication for an extra layer of security.

Table 62. Configuring HealthCast settings

Option	Description
HealthCast Server	Enter the name of the HealthCast server. You can use single sign-on authentication with Web or desktop applications. The server authenticates the user information.
HealthCast Security Mode	From the drop-down menu, select your preferred option. HealthCast solution provides secure access and unparalleled speed to virtual desktops, and clinical desktops, convenient fast-user switching, automated workflow, unique proximity badge features, optional PIN, remote access solutions with second factor authentication, and roaming sessions which allows immediate re-access to the work at any computer.
HealthCast LogLevel	From the drop-down menu, select your preferred option. **HealthCast LogLevel** allows separation of the software that generates messages, the system that stores the messages, and the software that reports and analyzes the messages. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.
Client Certificate	From the drop-down menu, select your preferred option. The certificates are uploaded to the file repository.

Configuring citrix broker connection settings

Use the **Citrix Broker** connection settings page to configure the citrix broker connection settings for ThinOS 8.5 and later version devices.

Table 63. Configuring basic settings

Option	Description
Broker Server	Enter the broker server host name or IP address.
Citrix custom store name	Enter the custom store name for your Citrix StoreFront connection.
Account Self-service server	Enter the server details.
Citrix StoreFront Style	Select this option to enable the Citrix StoreFront based layout of published applications and desktops on the device.
Password Expiry Notification	Select this option to enable the password expire notification. When the password is about to expire, a warning message is displayed with the number of days remaining to change the password.
Display on Desktop	From the drop-down list, select an option that you want to display on the desktop.

Option	Description
Use recommended settings for settings	Select this option to configure the recommended settings. For more information, hover the mouse on the **Information (i)** icon.
Automatically reconnect from button	Select this option to enable the thin client to automatically reconnect the session from the button menu.
Sessions to connect automatically	Select this option to automatically connect to the session.
RequestIconDataCount	Enter the number of icons. The icons are 32–bit color icons.
Reconnect At Logon	From the drop-down menu, select your preferred option. You can reconnect to both disconnected and active sessions.

Table 64. Configuring NetScaler gateway authentication

Option	Description
NetScaler Gateway Authentication	Select this option to enable the NetScaler Gateway authentication functionality.
User name	Enter the user name for the authentication purpose.
Password	Enter the password for the authentication purpose.
Domain	Enter the domain name for the authentication purpose.

Table 65. Configuring multi logon settings

Option	Description
Multi Farm	Select this option to support the servers which are part of different farms.
Multi Domain	Select this option to enable the multi domain functionality.
Multi Logon	Select this option to enable the multi login functionality.
Sequential Domain	Select this option to choose the domains in sequential order which are listed in the DomainList option.

Configuring citrix HDX connection settings

Use the **Citrix HDX Settings** page to define VDI global settings for citrix connections for ThinOS 8.5 and later version devices.

Table 66. Configuring basic settings

Option	Description
Audio quality	Select this option to set the audio quality.
Enable Seamless Mode	Select this option to set the seamless mode.
Multimedia Redirection	Select this option to redirect multimedia.
Map USB disks to	From the drop-down list, select the disk space to assign to the USB.

Option	Description
Session Window Behavior	Select this option to define whether the remote connection should be launched in a full screen mode. Select either **Full Screen** or **Window mode**. ⓘ NOTE: **Zero launchpad mode only supports full screen sessions. Window mode starts on a single screen while the full screen session spans across both monitors.**
Session Reliability	Select this option to enable the ICA session reliability.
Alternate address via firewall	Select this option to enable an alternate address through firewall.
Browsing Protocol Type	Select this option to choose the protocol type. From the drop-down list, select your preferred option.
USB Redirection Technology	Select this option to enable USB redirection. USB redirection is a technology that allows you to access the USB devices that are connected to the thin client from within a remote desktop or application.

Table 67. Configuring multimedia settings

Option	Description
HDXFlashUseFlashRemoting	Select this option to specify whether to use HDX Flash Redirection or not.
HDXFlashEnableServerSideContentFetching	Select this option to specify whether to use server side content fetching or not.
EnableRTME	Select this option to start the RTME service.
FlipByTimer	Select this option to choose the screen refresh method.

Configuring VMware broker connection settings

Use the **VMware Broker** connection settings page to configure the VMware broker connection settings ThinOS 8.5 and later version devices.

Table 68. Configuring basic settings

Option	Description
Broker Server	Enter the broker server host name or IP address. ⓘ NOTE: **You must specify between HTTP:// or HTTPS://.**
Security Mode	Select this option to set a security mode.
Protocol	Select this option to specify the display protocol. The server default protocols are All, RDP, PCoIP or Blast.
Sessions to connect automatically	Select this option to automatically connect to the session. ⓘ NOTE: **The name of the desktop or application is case sensitive. Use a semicolon to separate the multiple sessions which must be initialized automatically.**

Configuring VMware settings

Use the **VMware Settings** page to configure the VDI global settings for PCoIP connections on ThinOS 8.5 and later version devices.

Table 69. Basic settings

Option	Description
USB Redirection Technology	Select this option to enable USB redirection. USB redirection is a technology that allows you to access the USB devices that are connected to the thin client from within a remote desktop or application. You can either select VMware PCoIP or Wyse Thin Client Extensions (TCX) USB redirection. ⓘ NOTE: **If you select the TCX USB Redirection option, you require an additional TCX Server Suite.**
Show Disconnect Message	Select this option to see the disconnect message. A disconnect message is displayed when the USB device is removed from the system.
Show Reconnect Message Time	Enter the reconnect message time.
Resume Timeout	Enter the resume timeout.

Configuring Microsoft broker connection settings

Use the **Microsoft Broker** connection settings page to configure the Microsoft broker connections for ThinOS 8.5 and later version devices.

Table 70. Configuring basic settings

Option	Description
Broker Server	Enter the broker server host name or IP address. ⓘ NOTE: **You must specify between HTTP:// or HTTPS://.**
Sessions to connect automatically	Select this option to automatically connect to the session. ⓘ NOTE: **Name of the desktop or application is case sensitive. Use a semi-colon to separate the multiple sessions which must be initialized automatically.**

Configuring Microsoft RDP connection settings

Use the **Microsoft RDP Settings** page to configure the Microsoft RDP connection settings for ThinOS 8.5 and later version devices.

Table 71. Configuring basic settings

Option	Description
Enable NLA	Select this option to enable Network Level Authentication. User authentication is required to establish a connection with the server.
Enable Recording	Select this option to enable recording.

Table 72. Configuring RDP8 settings

Option	Description
Bitmap Codec RemoteFX	Select this option to enable the RemoteFX Bitmap Codec option. The default value is yes. Dell recommends that you select **No** for Wyse 3010 thin clients and Wyse 3020 thin clients.
Enable TS MM	Select this option to enable multimedia redirection for terminal server.
Force Span	Select this option to enable the force span of the view. If you enable the span option, the remote desktop becomes a rectangle which equals to the area of your local monitors.
RemoteFX graphic channel	Select this option to enable RemoteFX graphic channel.
UDP Traffic Channel	Select this option to enable RDP 8 UDP traffic channel. The default value is yes.
Video Optimized VOR	Select this option to enable RDP 8 video optimized redirection. The default value is yes.

Table 73. Configuring advanced settings

Option	Description
USB Redirection Technology	Select this option to enable USB redirection. USB redirection is a technology that allows you to access the USB devices that are connected to the thin client from within a remote desktop or application. You can either select VMware PCoIP or Wyse Thin Client Extensions (TCX) USB redirection. ⓘ **NOTE: If you select the TCX USB Redirection option, you require an additional TCX Server Suite.**
Color Depth	Select this option to configure the features of an RDP protocol.
Maximum Bitmap Cache	To set the maximum bitmap cache for your RDP session, enter a number from 128 to 1024.
4 Pixel Aligned Session Width	Select this option to enable the 4 pixel aligned session width.
Auto-Detect Network	Select this option to automatically detect the terminal server gateway.

Option	Description
Enable RDP H.264	Select this option to enable the H.264 encoding process for the RDP connections.

Configuring vWorksapce broker connection settings

Use the **vWorksapce Broker** connection settings page to configure the vWorksapce broker connection settings for ThinOS 8.5 and later version devices.

Table 74. Configuring basic settings

Option	Description
Broker Server	Enter the broker server host name or IP address. ⓘ **NOTE: You must specify between HTTP:// or HTTPS://.**
Enable vWorkspace Gateway	Select this option to enable vWorkspace gateway functionality.
Sessions to connect automatically	Select this option to automatically connect to the session. ⓘ **NOTE: The name of the desktop or application is case sensitive. Use a semicolon to separate the multiple sessions which must be initialized automatically.**

Configuring AWS broker connection settings

Use the **AWS Broker** connection settings page to configure the AWS broker connection settings for ThinOS 8.5 and later version devices.

Table 75. Configuring basic settings

Option	Description
Broker Server	Enter the broker server host name or IP address. ⓘ **NOTE: You must specify between HTTP:// or HTTPS://.**
Security Mode	Select this option to specify the client connectivity if it cannot verify a secure connection to the server.
Sessions to connect automatically	Select this option to automatically connect to the session. ⓘ **NOTE: The name of the desktop or application is case sensitive. Use a semicolon to separate the multiple sessions which must be initialized automatically.**

Configuring direct RDP connection settings

Use the **Direct RDP Connection** settings page to configure the RDP connections which can be accessed ThinOS 8.5 and later version devices.

Table 76. Configuring basic settings

Option	Description
Connection Name	Enter the name of the connection with a maximum of 38 characters.
User Name	Enter the user name for the application login.
Host Name or IP Address	Enter the host name or IP address of the connection.
Start Command	Enter the string of commands which must be executed after logging in to the server.
Password	Enter the password for the application login. ⓘ NOTE: **The password is not encrypted. Dell recommends that you do not specify the password. You are prompted to enter the password when the connection is created.**
Domain Name	Enter the domain name for Windows network with a maximum of 19 characters.
Auto Start	Select this option to restart the connection automatically.
Reconnect After Disconnect	Select this option to reconnect the connection automatically after the connection is disconnected.

Table 77. Configuring local resources

Option	Description
Map Printers	Select this option to automatically connect the local printers when the session starts.
Map Serials	Select this option to automatically connect the local serials when the session starts.
Map SmartCards	Select this option to redirect the smartcards to the remote session.
Map USB drives	Select this option to automatically map the USB drive when the session starts.
Map local disk drives	Select this option to automatically map the local disk drives when the session starts.

Table 78. Configuring session settings

Option	Description
Audio Playback	This option helps you to define how audio must be played in the remote session. From the drop-down menu, select any one of the following options: • Do not Play

Option	Description
	• Play Locally • Play on remote
RDP Audio Recording	Select this option to record the audio remotely.
Default color depth for the connections	Select this option to define the screen color depth of the connection.

Table 79. Configuring advanced settings

Option	Description
Connection Display	Select this option to set the screen resolution on the remote desktop.
Turn Compression off	Select this option to compress the files and to reduce the time required to download the files.
Auto-Detect Network	Select this option to automatically detect the terminal server gateway.
Mouse Queue timer	To set the mouse queue timer in an ICA or RDP session, enter a number from 0 to 99.
Session Window Behavior	Select this option to define whether the remote connection should be launched in a full-screen mode. Select either **Full Screen** or **Window mode** based on your preference. ⓘ **NOTE: Zero launchpad mode only supports full screen sessions. Window mode starts on a single screen while the full screen session spans both monitors.**

Table 80. Configuring terminal gateway settings

Option	Description
Use Terminal Server Gateway	Select this option to specify the Windows terminal server login details. If enabled, enter the following details: • RD host name or IP address • RD user name • RD password • RD domain name

Configuring direct ICA connection settings

Use the **Direct ICA Connection** settings page to configure the ICA connections which can be accessed on the ThinOS 8.5 and later version devises.

Table 81. Configuring basic settings

Option	Description
Connection Name	Enter the name of the connection with a maximum of 38 characters.
User Name	Enter the user name for the application login.
Password	Enter the password for the application login. ⓘ **NOTE: The password is not encrypted. Dell recommends that you do not specify the password. You are prompted to enter the password when the connection is created.**
Domain Name	Enter the domain name for Windows network with a maximum of 19 characters.
Auto Start	Select this option to restart the connection automatically.
Reconnect After Disconnect	Select this option to reconnect the connection automatically after the connection is disconnected.

Table 82. Configuring connection settings

Option	Description
Host or Application	From the drop-down list, select your preferred option.
Host Name or IP Address	Enter the host name or IP address of the connection.
Browser IP	Enter the list of IP addresses or DNS registered names.
Encryption	Select this option to set an encryption level. From the drop-down menu, select your preferred option.
Resolution	Select this option to set the resolution for your monitor. From the drop-down menu, select the appropriate resolution for your monitor. ⓘ **NOTE: If you select an unsupported resolution, the device ignores the setting.**

Table 83. Configuring local resources

Option	Description
Map Printers	Select this option to automatically connect the local printers when the session starts.
Map Serials	Select this option to automatically connect the local serials when the session starts.
Map SmartCards	Select this option to redirect the smartcards to the remote session.

Table 84. Configuring logon settings

Option	Description
Logon Mode	Select this option to select the log in mode.
Start Command Application	Enter the start command application.
Start Command Working Directory	Enter the start command working directory.

Table 85. Configuring session settings

Option	Description
Audio Quality	Select this option to set the audio quality.
Alternate address via firewall	Select this option to enable an alternate address through the firewall.
Session Reliability	Select this option to enable the ICA session reliability.
Optimize For Low Speed Link	Select the check box to optimize session settings for low link speed.
Font Smoothing	Select this option to enable font smoothing. Font smoothing is a method to obtain sharper fonts in low resolution screens.
Session Window Behavior	Select this option to define whether the remote connection should be launched in a full-screen mode. Select either **Full Screen** or **Window mode** based on your preference. (i) **NOTE: Zero launchpad mode only supports full screen sessions. Window mode starts on a single screen while the full screen session spans both monitors.**

Configuring global printer settings

Use the **Global Settings** page to configure global printer settings for ThinOS 8.5 and later version devices.

Table 86. Configuring default printer settings

Option	Description
Default Printer	Select this option to set a printer as a default printer.
PrinterMap settings	The files uploaded to **Apps and data** > **File repository** > **Inventory** are displayed. From the drop-down menu, select the mapping file.

Configuring printer settings

Use the **Printer** settings page to configure a new printers for ThinOS 8.5 and later version devices.

Table 87. Configuring printer select

Option	Description
Printer Type	From the drop-down menu select the printer type. The following are the types of printer: • Local printer

Option	Description
	· LPD printer · SMB printer
Local Printer	From the drop-down menu select the local printer connection.

Table 88. Configuring printer settings

Option	Description
Name	Enter the name of the shared printer.
LocalName	This option is applicable only for LPD printer. Enter the name of the printer.
Host	This option is applicable only for local LPD printer. Enter the IP address of the LPD service host.
Queue	This option is applicable only for LPD printer. Enter the queue name of the printer.
Username	This option is applicable only for SMB printer. Enter the user name.
Password	This option is applicable only for SMB printer. Enter the password.
Domain	This option is applicable only for SMB printer. Enter the domain name.
Printer ID	Enter the printer ID. The printer ID specifies the windows print driver name. The default printer ID is **Generic/Text Only**. This value is case-sensitive.
Class	Enter the class in the provided field. The following options are the predefined classes: · PCL4 · PCL5 · PS · TXT
Enabled	Select the check box to enable the printer.
EnableLPD	This option is applicable only for local printer and SMB printer. Select the check box to enable the LPD service.

Configuring WLAN global settings

Use the **WLAN Global Settings** page to configure WLAN global settings for ThinOS 8.5 and later version devices.

Table 89. Configuring WLAN global settings

Option	Description
Roam Sensitivity	Select this option to choose the sensitivity level of wireless roaming.
Disable Band	From the drop-down menu, select the preferred option. The **Disable Band** configuration is used to disable 2.4G or 5G 802.11 band. The default value is **Do not disable any band**.
Prefer Band	From the drop-down menu, select the preferred option.

Option	Description
	The **Prefer Band** configuration is used to set the priority of wireless connection band, and to select the 2.4G or 5G access point to connect. The default value is **Do not prefer any band**.
DisableN	Select the check box to disable the 802.11n mode.
Disable WLAN	Select this option to disable the wireless functionality. From the drop-down menu, select the preferred option. If you select the **EnetUp** option from the drop-down menu, when the ethernet is up and running, the wireless is disabled.

Configuring WLAN connections

Use the **WLAN Connections** page to configure the thin client WLAN connections for ThinOS 8.5 and later version devices.

Table 90. Configuring authentication settings

Option	Description
Security Type	Select this option to specify the authentication method. From the drop-down menu, select any one of the following options: • Open • Open(WEP) • SharedKey • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise
Encryption	This option is applicable only for Open(WEP), SharedKey, WPA-Personal, and WPA-Enterprise. From the drop-down menu, select your preferred option.
Web Key 1,2,3, and 4	This option is applicable only for Open(WEP) and SharedKey. From the drop-down menu, select your preferred option.
WPA Key	This option is applicable only for WPA-Personal and WPA2-Personal. Enter the WPA key in the provided field.
Network Type	This option is applicable only for WPA-Personal, WPA-Enterprise, WPA2-Personal, and WPA2-Enterprise. From the drop-down menu, select your preferred option.

Table 91. Configuring basic settings

Option	Description
SSID	Enter the name of the Service Set Identifier (SSID) connection.
Mode	From the drop-down menu, select the type of mode based on your requirement.

Table 92. Configuring IEEE 802.1X settings for WPA-Enterprise and WPA2-Enterprise

Option	Description
EAP Type	From the drop-down menu, select your preferred option.
FAST Type	This option is applicable only for EAP-FAST[8.3]. From the drop-down menu, select your preferred option.
LEAP user name	This option is applicable only for EAP-LEAP. Enter the leap user name in the provided field.
LEAP Password	This option is applicable only for EAP-LEAP. Enter the leap password in the provided field.
Server Validate	This option is applicable only for EAP-TLS and EAP-PEAP. Select the check box to validate the sever connection.
Server Check	This option is applicable only for EAP-TLS and EAP-PEAP. Select the check box to check the sever connection.
Server Name	This option is applicable only for EAP-TLS and EAP-PEAP. Enter the server name.
Client Certificate Filename	This option is applicable only for EAP-TLS. Enter the client certificate file name.
PrivateKey Client Certificate Password	This option is applicable only for EAP-TLS. Enter the private key client certificate password in the provided field.
TLS Authentication Type	This option is applicable only for EAP-TLS. From the drop-down menu, select your preferred option.
PEAP TLS Version	This option is applicable only for EAP-TLS. From the drop-down menu, select your preferred option.
PEAP Type	This option is applicable only for EAP-PEAP. From the drop-down menu, select your preferred option.
EAP Identity	This option is applicable only for EAP-PEAP and EAP-FAST[8.3]. Enter the EAP identity.
user name	This option is applicable only for EAP-PEAP and EAP-FAST[8.3]. Enter the user name.
Password	This option is applicable only for EAP-PEAP and EAP-FAST[8.3]. Enter the password.
Hide Domain	This option is applicable only for EAP-PEAP and EAP-FAST[8.3]. Select the check box to hide the domain.
Domain	This option is applicable only for EAP-PEAP and EAP-FAST[8.3]. Enter the domain name.
Enable Single Signon	This option is applicable only for EAP-PEAP and EAP-FAST[8.3]. Select the check box to enable the single sign on functionality.

Configuring LAN connections

Use the **LAN Connections (8.6+)** page to configure the LAN connections for ThinOS 8.6 and later version devices.

Table 93. Configuring IEEE 802.1X settings

Option	Description
Network Type	From the drop-down list, select the preferred option. The system automatically restarts and the changes to network type are applied.
Ethernet Speed	From the drop-down list, select the preferred option. The selected option is stored in the non-volatile memory. The system automatically restarts and the changes to Ethernet speed are applied.
Enable IEEE802.1x Authentication	Select this option to enable IEEE802.1x authentication. IEEE 802.1X is an IEEE standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to the devices with LAN or WLAN.
EAP Type	From the drop-down menu, select your preferred option. The available options are: • **Light weight extensible authentication protocol (EAP-LEAP)**—This is an authentication protocol used in wireless networks and point-to-point connections. LEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control. • **Transport Layer Security (EAP-TLS)**—It provides client and server authentication. It is often used for wireless networking and it is one of the stronger forms of authentication for both the wireless client and server. • **Protected Extensible Authentication Protocol (EAP-PEAP)**—It is a protocol that captures the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. It provides client and server authentication. • **Flexible Authentication via Secure Tunneling (EAP-FAST[8.3])**—It is used in wireless networks and point-to-point connections to perform session authentication. The purpose of EAP-FAST[8.3] is to replace the Lightweight Extensible Authentication Protocol (LEAP). LEAP is a wireless authentication protocol that contains known security vulnerabilities when used with weak passwords. EAP-FAST addresses these vulnerabilities by performing authentication over a TLS tunnel, which is established using a Protected Access Credential (PAC).
FAST Type	From the drop-down menu, select your preferred option. This option is applicable only for EAP-FAST[8.3].
LEAP user name	Enter the leap user name in the provided field. This option is applicable only for EAP-LEAP.
LEAP Password	Enter the leap password in the provided field. This option is applicable only for EAP-LEAP.
Server Validate	Select this check box if you want the system to validate the server connection. This option is applicable only for EAP-TLS and EAP-PEAP.

Option	Description
Server Check	Select the check box to check the sever connection. This option is applicable only for EAP-TLS and EAP-PEAP.
Server Name	Enter the server name. This option is applicable only for EAP-TLS and EAP-PEAP.
Client Certificate Filename	Enter the client certificate file name. This option is applicable only for EAP-TLS.
PrivateKey Client Certificate Password	Enter the private key client certificate password in the provided field. This option is applicable only for EAP-TLS.
TLS Authentication Type	From the drop-down menu, select your preferred option. This option is applicable only for EAP-TLS.
PEAP TLS Version	From the drop-down menu, select your preferred option. This option is applicable only for EAP-TLS.
PEAP Type	From the drop-down menu, select your preferred option. This option is applicable only for EAP-PEAP.
EAP Identity	Enter the EAP identity. This option is applicable only for EAP-PEAP and EAP-FAST[8.3].
user name	Enter the user name. This option is applicable only for EAP-PEAP and EAP-FAST[8.3].
Password	Enter the password. This option is applicable only for EAP-PEAP and EAP-FAST[8.3].
Hide Domain	Select the check box to hide the domain. This option is applicable only for EAP-PEAP and EAP-FAST[8.3].
Domain	Enter the domain name. This option is applicable only for EAP-PEAP and EAP-FAST[8.3].
Enable Single Signon	Select the check box to enable the single sign on functionality. This option is applicable only for EAP-PEAP and EAP-FAST[8.3].

Configure SCEP Settings

Use the **SCEP Settings (8.6+)** page to configure the SCEP settings for ThinOS 8.6 and later versions.

Table 94. Configuring SCEP 8.6+ settings

Option	Description
SCEP Auto Enroll	Select this option to enable automatic certificate enrolment by using the environment's SCEP server.
Auto Renewal	Select this option to enable automatic certificate renewal. The thin client tries to renew the requested certificates manually or automatically through SCEP. The renewal initiated after half of the valid period of the existing certificate is expired.
Install CA Certificates	Select this option to install the Root CA's certificate as a trusted certificate.
Country	Enter the country name. The country name must have only two letters in uppercase.

Option	Description
State	Enter the state name.
Location	Enter the location name.
Organization	Enter the organization name.
Organization Unit	Enter the organization unit name.
Common Name	Enter the common name such as, $TN.dellwyse.com. You can use the terminal name as part of the common name.
Email	Enter the e-mail address.
Key Usage	Select the preferred key usage option.
Key Length	From the drop-down list, select the key length of the client certificate in bits.
Subjective Alternative Name	Enter the alternate name for the client certificate. It is a list of names such as, e-mail addresses, IP addresses, URLs, and DNS, where you must use a semicolon (;) as a delimiter.
Request URL	Enter the service URL of the SCEP server.
CA Certificate Hash Type	From the drop-down list, select the hash value used to verify the certificate authenticity.
CA Certificate Hash	Enter the MD5 hash value to verify the CA authenticity.
Enrolment Password	Enter the enrolment password.
Encrypt Enrolment Password	Select the check box to enable the encryption for the enrolment password.
SCEP Administrator URL	Enter the SCEP administrator URL.
SCEP User	Enter the SCEP administrator user name.
SCEP User password	Enter the SCEP administrator user password.
Encrypt SCEP User Password	Select this option to set the password. Enter the SCEP administrator user encrypted password which is received from **https://scep.dellwyse.com/CertSrv/mscep_admin**.
SCEP User Domain	Enter the SCEP user domain.

Configure proxy Settings

Use the **Proxy (8.6+)** page to configure the proxy settings for ThinOS 8.6 and later version devices.

Table 95. Configuring proxy 8.6+ settings

Option	Description
Proxy Settings	Select the check box to enable the proxy settings which are saved in the non-volatile memory.
Applist	This list provides the information about which application uses the configured proxy.
Enabe proxy protocol with Global, Http, Https, and Socks5	From the drop-down list, select the proxy protocol with Global, Http, Https, and Socks5. If you select **Yes** from the **Enabe proxy**

Option	Description
	protocol with Global, Http, Https, and Socks5 drop-down list, then enter the **Server Name**, **User Name**, **Password**. To check if the password is encrypted or not, select the **Encrypt** option.

Edit the Windows Embedded Standard policy settings

To edit the Windows Embedded Standard (WES) policy settings, do the following:

1 Click **Groups & Configs**.

The **Groups & Configs** page is displayed.

2 Click the **Edit Policies** drop-down menu.

3 Click **WES**.

The **WES** page is displayed. The Windows Embedded Standard thin client policy settings include the following options:

- System Personalization
- Desktop Experience
- Network
- Security and Lockdown
- Other settings
- Remote Connections Citrix
- Remote Connections VMware
- Remote Connections RDP
- Remote Connections Browser
- Latitude mobile thin client BIOS settings
- Wyse 7040 thin client BIOS settings
- Device Info
- Wyse Easy Setup
- VNC settings
- Domain settings
- BIOS WES 5070 settings

4 After configuring the policy settings, click **Save and Publish**.

Configuring system personalization

Use the system personalization page to configure the thin client settings, such as display, keyboard, mouse, time zone, and audio options for Windows Embedded Standard devices.

Table 96. Configuring display options

Option	Description
Enable Dual Monitor	Select this option to enable the dual monitor functionality. If selected, the **Display Mode** option is available.
Display Mode	From the drop-down list, select one of the following options: • Duplicate these displays • Extend these displays If you select **Extend these displays**, the following options are available:

Option	Description

	• **Monitor Resolution (Secondary)**—Select this option to set the resolution for your monitor. From the drop-down menu, select the appropriate resolution that suits your monitor type.
	 • **Display Identifier (Secondary)**—Select this option to set an identifier for your monitor. From the drop-down menu, select an appropriate monitor identification number.
	 • **Monitor Rotation (Secondary)**– Select this option to set an orientation options for your monitor. From the drop-down menu, select one of the display orientation options based on your preference:
	   – Landscape
	   – Portrait
	   – Landscape—flipped
	   – Portrait—flipped
	 • **Enable Multi Monitor**—Select this option to enable the multi monitor setting.
	 • **Multi Monitor Support**—From the drop-down list, select monitor resolution, monitor rotation, refresh rate, color depth, span position, display identifier, and remove.

Monitor Resolution (Primary)	Select this option to set the resolution for your monitor. From the drop-down menu, select the appropriate resolution that suits your monitor type.
Display Identifier (Primary)	Select this option to set a display identifier for your monitor. From the drop-down menu, select an appropriate monitor identification number.
Monitor Rotation (Primary)	Select this option to set an orientation options for your monitor. From the drop-down menu, select one of the display orientation options based on your preference: • Landscape • Portrait • Landscape—flipped • Portrait—flipped

Table 97. Configuring keyboard options

Option	Description
Language	Select this option to choose one or more input languages for your keyboard. From the drop-down menu, select your preferred keyboard input language.
Default Keyboard Layout	Select this option to set an appropriate keyboard layout. From the drop-down menu, select your preferred keyboard layout.
Blink Rate	Select this option to set the speed at which the cursor (insertion point) blinks to make it more visible, or less visible—depending on your requirement. From the drop-down menu, select your preferred cursor blink rate.
Keyboard Preferences	Select this option to set the keyboard hotkeys.
Keyboard Repeat Delay	Select this option to set the duration of time that a key can be pressed without repeating the letter as input. From the drop-down menu, select one of the following options based on your preference: • Short

Option	Description
	· Medium Short · Medium Long · Long
Keyboard Repeat Rate	Select this option to set the repeat rate for the keyboard, which is the speed at which the key input repeats itself when you press and hold down the key on the keyboard.
Menu Access	Select this option to enable the menu access keys on your keyboard.
MS Gina Keyboard Layout	Select this option to view the **Keyboard Selection** screen on the Windows login screen. MS Gina Keyboard Layout feature allows to choose desired language and keyboard layout in the Windows devices on the login screen. For example, If the Windows credential is in Non-English and the keyboard attached to the Windows system is English. You cannot enter the credentials as there is no option to change or select the language and keyboard layout on the Windows login screen. You can configure the desired languages, substitute languages and keyboard layout along with **MS Gina Keyboard Layout** from the Wyse Management Suite server. When you apply the language or keyboard settings, MS Gina Keyboard layout is displayed on the Windows login screen. You can change or select desired language and keyboard layout from the Windows login screen. ⓘ NOTE: **The Windows login screen is displayed when the auto logon setting is disabled. To Apply MS Gina Keyboard Layout settings from the Wyse Management Suite server, you must disable and enable the Write Filter option. The Windows system restarts twice.**
Substitute Keyboard Layouts	Select this option to choose one or more input languages for your keyboard. From the drop-down list, select your preferred keyboard input languages.
Enable C-A-D mapping	Select this option to enable the C-A-D map setting. The local Ctrl +Alt+Del key combination is used to map the remote sessions. This setting is applicable to the following broker connections: · Citrix · Remote Desktop Protocol (RDP) · VMware

Table 98. Configuring mouse, basic mouse, mouse pointer, and mouse vertical options

Option	Description
Mouse Speed	Select this option to specify the speed of the mouse pointer when moving the mouse device.
Left-handed Mouse	Select this option to swap the left and right-click mouse buttons.
Click Lock	Select this option to use the highlight or drag function without holding down the mouse button.

Option	Description
	To set the **Click Lock Time** parameter, from the drop-down menu, select the appropriate time for the mouse button to be held down before the click is locked.
Double Click Speed	Select this option to set the time interval between two consecutive mouse clicks. From the drop-down menu, select your preferred option.
Find Mouse Pointer	Select this option if you want to find the mouse pointer when it is not in motion. ⓘ NOTE: You can press the `Ctrl` key on your keyboard to locate the mouse pointer when it is not in motion.
Hide Mouse Pointer	Select this option to hide the mouse pointer when it is stationary. ⓘ NOTE: To locate the mouse pointer when it is stationary, press the `Ctrl` key.
Pointer Trail Length	Select this option to define the length of the pointer trail when the mouse pointer is in motion.
Snap Mouse Pointer	Select this option to automatically move the mouse pointer to the default button in a dialog box.
Scroll Lines	Select this option to define the number of lines scrolled at a time using vertical scrolling on your mouse.

Table 99. Configuring time zone options

Option	Description
Time Servers (NTP Servers)	Select this option to view the time servers to enable local time synchronization. Enter the NTP servers separated by commas.
Timezone Name	Select this option to set the time zone for your device. From the drop-down menu, select your preferred time zone.

Table 100. Configuring audio options

Option	Description
Audio Mute	Select this option to mute the audio of your device.
Audio Volume	Select this option to adjust the audio volume of your device. From the drop-down menu, select your preferred volume option.
Microphone Mute	Select this option to mute your microphone.
Microphone Volume	Select this option to adjust the volume of your microphone. From the drop-down menu, select your preferred volume option.

Configuring desktop experience

Use this page to configure the thin client settings, such as desktop wallpaper, and desktop color for Windows Embedded Standard devices.

Table 101. Configuring desktop experience

Option	Description

Desktop Wallpaper	Select this option to set a wallpaper for your desktop.
	After you enable the desktop wallpaper option, do the following:
	
	• From the **Wallpaper File** drop-down list, select a wallpaper for your desktop.
	
	   ⓘ **NOTE:**
	   Select a wallpaper only from the list of images uploaded to the file repository.
	
	• From the **Wallpaper Layout** drop-down list, select any of the following layouts for your desktop wallpaper:
	
	   – Center
	   – Tile
	   – Stretch
	   – Fill

Desktop Color	Select this option to define a background color for your local desktop.

Configuring network settings

Use this page to configure the network settings for the Windows Embedded Standard devices.

Table 102. Configuring network settings

Option	Description
Radio State	Select this option to enable the wireless radio state. ⓘ **NOTE:** This option is similar to turning the device ON or OFF.
Windows Wireless Profiles	Select this option to set a Windows wireless profile. From the drop-down menu, select your preferred Windows wireless profile. ⓘ **NOTE:** Select a profile only from the list of wireless profiles uploaded to the file repository.

Configuring security and lockdown settings

Use this page to configure the security and lockdown settings.

Option	Description
Install Certificates	Select this option to view the certificates that are uploaded to the file repository.
Disable USB Storage Device Access	Select this option to disable the USB mass storage device access for non-administrator users.
Disable Print Screen	Select this option to disable the print screen functionality for non-administrator users.
Disable Task Manager	Select this option to disable the task manager access for non-administrator users.
Disable USB Storage Write	Select this option to disable **Write Access** to USB storage for all users.
Disable Imaging Device Access	Select this option to disable the device access for all users.
Disable Printer Device Access	Select this option to disable the printer access for all users.
Disable Smart Card Reader Device Access	Select this option to disable the smart card reader device access for all users.
Disable Media Device Access	Select this option to disable the USB media device access for all users.

Option	Description
Configure Autologon	From the drop-down list, select any one of the following options: • **Do not manage autologon** • **Disable autologon** • **Enable autologon**

Option	Description
Change Local admin Password	Select the check box to change the Windows password for the local administrator account. The system automatically restarts twice.
Local admin Password	Enter the Windows password for the local administrator account. The password must be a minimum of 8 and a maximum of 32 characters.

Table 106. Configuring Windows user password settings

Option	Description
Change Local User Password	Select the check box to change the Windows password for the local user account.
Local User Password	Enter the Windows password for the local user account. The password must be a minimum of 8 and a maximum of 32 characters.

Configuring other settings

Use this page to configure the thin client settings, such as power, shared drive, and clock settings for Windows Embedded Standard devices.

Table 107. Configuring appliance mode

Option	Description
Appliance Mode	Select this option to set an appropriate mode for the appliance. Appliance mode option starts the application in a Kiosk mode and with no access to the desktop or other applications. You can come out of the appliance mode using the configured keys. For example, Ctrl+Shift+A. From the drop-down menu, select any of the following options: • Off • Generic • VMware View • Citrix • Internet Explorer • RDP

Table 108. Configuring power settings

Option	Description
Device Power Plan	Select this option to choose a power plan for your device. From the drop-down menu, select either of the following options: • Balanced • Power Saver

Table 109. Configuring power settings on battery

Option	Description
Device Sleep Plan	Select this option to set the time after which your device goes to sleep mode. From the drop-down menu, select a delay time.
Dim Display	Select this option to set the time after which the display is dimmed. From the drop-down menu, select a delay time.
Turn Off Display	Select this option to set the time after which the display is turned off. From the drop-down list, select a delay time.

Table 110. Configuring power settings when plugged-in

Option	Description
Device Sleep Plan	Select this option to set the time after which your device goes to sleep mode. From the drop-down menu, select a delay time.
Dim Display	Select this option to set the time after which the display is dimmed. From the drop-down menu, select a delay time.
Turn Off Display	Select this option to set the time after which the display is turned off. From the drop-down menu, select a delay time.

Table 111. Configuring shared drives

Option	Description
Shared Drive	Select this option to add a shared drive to your device. Click **Add Shared Drive**. Enter the share name, remote drive path, user name, and password for the shared drive. ⓘ NOTE: **To delete a shared drive from the list, select the shared drive that you want to remove and click Remove.**

Table 112. Configuring clock settings

Option	Description
Clock1	Select this option to configure Clock 1 on your device. After you enable Clock1, set the **Display Name** for the clock. From the drop-down menu, select the **Time Zone** for Clock 1.
Clock2	Select this option to configure Clock 2 on your device. After you enable Clock 2, set the **Display Name** for the clock. From the drop-down menu, select the **Time Zone** for Clock 2.

Configuring remote connection settings—Citrix

Use this page to configure the Citrix connection settings, such as display, server options, and flash redirection for the Windows Embedded Standard devices.

Table 113. Basic options

Option	Description
Connection Name	Select this option to set a name for connection identification.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start the session after you log in.
Connection Type	Select this option to set a connection type. From the drop-down menu, select any of the following options: • Citrix XenApp • Citrix XenDesktop • Citrix Gateway • Citrix StoreFront

Option	Description
Citrix Server FQDN or IP address	Select this option to list the Citrix servers. Enter the list of ICA browsers separated by commas for the connection.
Published Applications	Select this option to specify a published application that you want to start.
Single Sign On	Select this option to enable the single sign-on feature for the connection. If you enable single sign-on, use your Windows login credentials to connect to the Citrix server.
Username	Select this option to define a user name for the Citrix connection, if single sign-on is disabled.
Password	Select this option to define a password for the Citrix connection, if single sign-on is disabled.
Domain Name	Select this option to define a domain name for the Citrix connection.
Window Size	Select this option to specify the window size for the Citrix connection. From the drop-down menu, select a window size.
Screen Color Depth	Select this option to define the screen color depth for the Citrix connection. • Default • Better Speed 16–Bit • Better Appearance 32–Bit
Auto Reconnect	Select this option to automatically restore the connection, if the connection is dropped.
Audio Quality	Select this option to choose the audio quality for the Citrix connection. From the drop-down menu, select any of the following options: • Default User Audio Setting • High Definition • Optimized for Speech • Low Bandwidth • Off
User Key Combos Passthrough	Select this option to specify a window to apply the Windows user key combinations. • Default User Key Combos Passthrough • On the local desktop • On the remote desktop • In full screen desktops only

Table 114. Application display

Option	Description
Desktop Display	Select this option to view the Citrix connection on your desktop. After you enable this option, specify the **Desktop Folder Name** for the connection.
Start Menu Display	Select this option to enable the start menu display on the connection desktop.

Option	Description
	After you enable this option, specify the **Start Menu Display Folder** for the connection.
System Tray Display	Select this option to display the Citrix connection icon in the notification area.

Table 115. Server options

Option	Description
Logon Method	Select this option to choose a logon method for your Citrix connection. • Default Logon Method • Prompt Logon Method

Table 116. Advanced settings

Option	Description
Disable Full Screen Pop-up	Select this option to disable the full screen pop-up warning.
Logon—Connect to Active and Disconnected Sessions	Select this option to connect to the active and disconnected sessions after you log in.
Menu—Connect to Active and Disconnected Sessions	Select this option to connect to active and disconnected sessions.
Reconnect from Menu	Select this option to reconnect to the existing sessions from the client menu.

Table 117. Flash redirection

Option	Description
Use Flash Remoting	Select this option to render the flash content on the client device instead of the remote server.
Enable Server-Side Content Fetching	Select this option to download the content to the server and send it to the user device.
Use Server HTTP Cookies	Select this option to synchronize the client-side HTTP cookies with the server-side.
URL Rewriting Rules for Client-Side Content Fetching	Select this option to add rules that redirect the user devices to other servers for client-side fetching. Click **Add Item**, and enter the content rule name and content rule value. ⓘ NOTE: **To delete an item from the list, select the item you want to remove, and click Remove.**

Configuring remote connection settings—VMware

Use this page to configure the VMware connection settings for the Windows Embedded Standard devices.

Table 118. Configuring remote connections—VMware

Option	Description
Connection Name	Select this option to define the name to identify the connection.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start after you log in.
VMware Server Address	Select this option to enter the server address of the VMware connection.
Protocol	Select this option to choose the protocol for the VMware connection. From the drop-down menu, select either of the following options: · PCOIP · RDP · Blast
Login as Current User	Select this option to enable the single sign-on feature for the connection. If you enable the **login as current user** option, use your Windows login credentials to connect to the VMware server.
Username	Select this option to define a user name for the VMware connection, if single sign-on is disabled.
Password	Select this option to define a password for the VMware connection, if single sign-on is disabled.
Domain Name	Select this option to define a domain name for the VMware connection.
Security Mode	Select this option to specify the client connectivity if it cannot verify a secure connection to the server.
Fullscreen Mode	Select this option to set the VMware connection window in full screen mode. If you do not select the fullscreen mode, from the drop-down menu, select the **Window Size**.
Display Fullscreen Drop Down Menu Bar	Select this option to display the **Fullscreen** drop-down menu for your connection.
Automatically Launch This Desktop	Select this option to specify a published desktop to start upon a successful connection.
Auto Reconnect	Select this option to automatically reconnect, if the connection is dropped.
Broker	Select this option to define the hostname or IP address of the **View Connection** broker.
Broker History	Select this option to specify the previously used hostname or IP address of the **View Connection** broker.

Configuring remote connection settings—RDP

Use this page to configure the RDP connection settings, such as RD Gateway, display, and local resources settings for the Windows Embedded Standard devices.

Table 119. Configuring basic settings

Option	Description
Connection Name	Select this option to define the name to identify the connection.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start after you log in.
Server Address	Select this option to enter the server address of the connection.
Single Sign On	Select this option to enable the single sign-on feature for the connection. If you enable the **login as current user** option, use your Windows login credentials to connect to the server.
Username	Select this option to define a user name for the connection, if single sign-on is disabled.
Password	Select this option to define a password for the connection, if single sign-on is disabled.
Domain Name	Select this option to define a domain name for the connection.
Auto Reconnect	Select this option to enable the connection to automatically reconnect, if the connection is dropped.

Table 120. Configuring RD gateway

Option	Description
Use RD Gateway settings	Select this option to configure the settings for RD Gateway. After you enable the option, enter the **RD Server** name for the gateway. From the **RD Gateway Logon Method** drop-down menu, specify the credentials to validate the connection with the RD Gateway: • Ask for password NTLM • Smartcard • Allow me to select later • From the **RD Gateway Usage Method** drop-down menu, select any of the following ways to use a remote desktop server: • Do not use RD Gateway server—All IP addresses • Use RD Gateway server settings • Use RD Gateway server settings for Non-Local IP addresses only • Use default settings • Local IP addresses only

Table 121. Configuring display settings

Option	Description
Fullscreen	Select this option to set the connection window in the full screen mode. After the full screen mode is enabled, from the drop-down menu, select the window size.
Display Connection Bar	Select this option to display the connection bar in the fullscreen mode.
MultiMonitor Support	Select this option to enable the multi-monitor support.
Screen Color Depth (in bits)	Select this option to define the screen color depth of the connection. • RDP 15–Bit High Color • RDP 16–Bit High Color • RDP 24–Bit True Color • RDP 32–Bit Highest Quality

Table 122. Configuring other settings—Experience

Option	Description
Connection Speed To Optimize the Performance	Select this option to specify the connection speed to optimize the performance.
Desktop Background	Select this option to enable the desktop background for the connection.
Visual Styles	Select this option to enable the visual styles for the connection.
Font Smoothing	Select this option to enable font smoothing for the connection.
Persistent Bitmap Caching	Select this option to enable persistent bitmap caching for the connection.
Desktop Composition	Select this option to enable the desktop composition for the connection.
Disable Cursor Setting	Select this option to disable the cursor setting for the connection.
Show Window Contents While Dragging	Select this option to display the window contents while dragging the window.
Menu and Window Animation	Select this option to enable menu and window animation in the connection.
Use Redirect Server Name	Select this option to enable the usage of redirect server name.
If Server Authentication Fails	Select this option to specify the action that must be taken when the server authentication fails. • Connect and don't warn me • Do not connect • Warn me

Table 123. Configuring local resources

Option	Description
Redirect Clipboard	Select this option to use the local clipboard of the device in the remote connection.
Redirect COM Ports	Select this option to use the local COM (serial) ports of the device in the remote connection.
Redirect DirectX	Select this option to redirect DirectX on the client computer and make it available in the remote connection.
Redirect Drives	Select this option to use the local drives of the device in the remote connection.
Redirect POS Devices	Select this option to use the Point of Service devices, such as bar code scanners and magnetic readers of the device in the remote connection.
Forward All Printers	Select this option to use the local printer of the device in the remote connection.
Redirect Smart Card	Select this option to use the local smart cards of the device in the remote connection.
Enable RemoteFX USB Device Redirection	Select this option to enable or disable the RemoteFX USB device redirection.
Enable the redirection of USB drives that are plugged in later	Select this option to enable or disable the redirection of the USB drives from the RDP session.
Enable the redirection of Other supported Plug and Play devices	Select this option to enable or disable the redirection of other plug and play devices.

Configuring remote connection settings—Browser

Use this page to configure the browser connection settings, such as IE proxy and favorites, for the Windows Embedded Standard devices.

Table 124. Basic settings

Option	Description
Connection Name	Select this option to define a name to identify the connection.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start after you log in.
URL	Select this option to specify the default URL for the browser.
Internet Zone Security Level	Select this option to make the security settings for Internet Explorer in the internet zone.
Local Zone Security Level	Select this option to make the security settings for Internet Explorer in the local zone.
Trusted Zone Security Level	Select this option to make the security settings for Internet Explorer in the trusted sites.
Restricted Zone Security Level	Select this option to make the security settings for Internet Explorer in the restricted sites.

Table 125. Internet Explorer (IE) favorites and trusted site settings

Option	Description
IE Favorite	Select this option to add your favorite and trusted sites. Perform the following steps to add your favorite and trusted sites: 1 Click **Add Site**, and enter the folder name, URL, and description. 2 Click **Create Shortcut** to create a shortcut for the site. 3 Click **Remove** to delete a site from the list. ⓘ **NOTE:** URL must begin with Https:// when the **Trusted Sites** check box is selected.
Require Server Verification (https:) for all sites in the zone	Select this option to enable a server verification for all sites in the zone.

Table 126. Internet Explorer—IE proxy settings

Option	Description
Enable Proxy	Select this option to configure proxy for the browser.

Table 127. Firewall

Option	Description
Domain Firewall	Select this option to enable the domain firewall.
Private Firewall	Select this option to enable the private firewall.
Public Firewall	Select this option to enable the public firewall.

Table 128. Aero—valid for Windows Embedded Standard 7

Option	Description
Aero	Select this option to enable the Aero feature for the browser. ⓘ **NOTE:** This feature is available only for Windows Embedded Standard 7

Configuring Latitude mobile thin client BIOS settings

Use this page to define the BIOS settings of Latitude mobile thin clients.

Table 129. System configuration

Option	Description
Serial Port 1	Select this check box to determine how the serial port on the docking station operates. This option enables you to avoid resource conflicts between devices by disabling or remapping the address of the port.

Option	Description
	• **Disabled**: Port is disabled. • **COM1**: Port is configured at 3F8h with IRQ 4. • **COM2**: Port is configured at 2F8h with IRQ 3. • **COM3**: Port is configured at 3F8h with IRQ 4. • **COM4**: Port is configured at 2F8h with IRQ 3.
Sound Device	Select this check box to enable the sound device.
Microphone	Select this check box to enable the microphone.
Speaker	Select this check box to enable the speakers.

Table 130. USB configuration

Option	Description
External USB Ports	Select this check box to enable the device attached to this port. The device is also made available to the operating system. If a USB port is disabled, operating system cannot detect any device attached to the port.

Table 131. Configuring wireless settings

Option	Description
EnableBluetooth	Select this check box to enable Bluetooth.
WLAN/GPS	Select this check box to enable WLAN/GPS.
Wireless LAN	Select this check box to enable wireless LAN.

Table 132. Configuring security settings

Option	Description
Admin Setup Lockout	Select this check box to prevent users from entering **Setup** when the admin password is set.

Table 133. Admin password settings

Option	Description
Enable Admin Password	Select this check box to enable the BIOS administrator password. Successful changes to this password take effect immediately.
Admin Password	Enter the new BIOS admin password. This option is available only if you select the **Enable Admin Password** check box.

Table 134. Configuring power management settings

Option	Description
Wake On LAN	Enable this option to power on the device from the Wyse Management Suite console. To perform this action, run the Wake On LAN (WOL) command on the **Devices** page.
Wake on AC	Enable this option to automatically boot the device after power is restored—following a power failure.

Table 135. Configuring auto-on settings

Option	Description
Auto On	From the drop-down list, set the time of the day you want the system to turn on automatically.

Table 136. Configuring reboot schedule

Option	Description
Reboot Option	Some BIOS settings requires the system to restart. From the drop-down list, select one of the following options: • Reboot immediately—The system restarts immediately. • Reboot later—Select the **Reboot Hour** and **Reboot Minute** to set the system restart time. • Do not reboot—The system does not restarts.

Configuring Wyse 7040 thin client BIOS settings

Use this page to configure the BIOS settings of Wyse 7040 thin clients.

Table 137. System configuration

Option	Description
Sound Device	Select this check box to enable the sound device.
Microphone	Select this check box to enable the microphone.
Speaker	Select this check box to enable the speakers.

Table 138. Configuring security settings

Option	Description
Admin Setup Lockout	Select this check box to prevent users from entering **Setup** when the Admin password is set.

Table 139. Configuring administrator password settings

Option	Description
Enable Admin Password	Select this check box to enable the BIOS administrator password. Successful changes to this password take effect immediately.
Admin Password	Enter the new BIOS admin password. This option is available only if you select the **Enable Admin Password** check box.

Table 140. Configuring auto-on settings

Option	Description
Auto On	From the drop-down list, set the time of day you want the system to turn on automatically.

Table 141. Configuring reboot schedule

Option	Description
Reboot Option	Some BIOS settings requires the system to restart. From the drop-down list, select one of the following options: • Reboot immediately—The system restarts immediately. • Reboot later—Select the **Reboot Hour** and **Reboot Minute** to set the system restart time. • Do not reboot—The system does not restarts.

Table 142. USB configuration

Option	Description
Enable Front USB Ports	Select this check box to enable the device attached to this port. If you select this check box, the device is made available to the operating system also. However, if the USB port is disabled, the operating system cannot detect any device attached to this port.
Enable Rear USB Ports	Select this check box to enable the device attached to this port. If you select this check box, the device is made available to the operating system also. However, if the USB port is disabled, the operating system cannot detect any device attached to this port.

Table 143. Configuring power management settings

Option	Description
Wake on AC	From the drop-down list, select an option to specify how the system must behave when AC power is restored after an AC power loss. The available options are: • Off • Last • On
Wake On LAN	From the drop-down list, select an option to allow the thin client to power up from the off state. You can trigger a thin client to power up from the off state by using a LAN signal or a wireless LAN signal.

Configuring device information

Use the **Device Info** page to set the device details.

Table 144. Configuring device information

Option	Description
Location	Enter the device location.
Contact	Enter the device contact.
Custom 1 to 3	Enter the custom values.

Configuring Wyse Easy Setup settings

Use the **Wyse Easy Setup** page to configure the Wyse Easy Setup settings for the control panel and the user interface.

Table 145. Configuring system

Option	Description
Region & Language	Enables the user to access the region and language option in the control panel.
Date & Time	Enables the user to access the date and time option in the control panel.
Display	Enables the user to access the display option in the control panel.
Network	Enables the user to access the network option in the local system control panel.
Ease of Access	Enables the user to access the easy of access option in the control panel.

Table 146. Configuring peripherals

Option	Description
Mouse	Enables the user to access the mouse option in the control panel.
Keyboard	Enables the user to access the keyboard option in the control panel.

Table 147. Configuring Kiosk mode

Option	Description
Kiosk Mode	Select this option to replace the default Windows desktop with the Wyse easy setup desktop, Wyse easy setup remote connections, and Wyse easy setup applications.
Applications	Enter the details to register a new application.
Application Exit Action	From the application exit action drop-down list, select any one of the following options: · Shutdown upon Exit · Restart upon Exit · Logout upon Exit · Persistent upon Exit This setting is applicable when you have configured at least one of the remote connections.
Smart Card On Removal	From the smart card on removal drop-down list, select any one of the following options: · Restart upon removing the smart card · Logout upon removing the smart card

Option	Description
	- Shutdown upon removing the smart card - LockScreen upon removing the smart card

Table 148. Personalization

Option	Description
Background	From the drop-down menu, select the preferred graphic image. The image should be uploaded to the file repository and displayed as a wallpaper.
Logo	From the drop-down list, select the logo files which are uploaded in **Apps & Data** > **File Repository** > **Inventory**.

Table 149. Configuring taskbar

Option	Description
Date & Time	Enables the user to set the date and time option on the Wyse Easy Setup shell or custom desktop.
Sound	Enables the user to set the sound parameters in the Wyse Easy Setup shell or custom desktop.
Network	Enables the user to view the network option on the Wyse Easy Setup shell or custom desktop.
Touch Keyboard	Enables the user to view the touch keyboard on the Wyse Easy Setup shell or custom desktop.

Table 150. Configuring Start menu

Option	Description
Allow Shutdown	Enables the user to shut down the system on the Wyse Easy Setup shell or custom desktop.
Allow Restart	Enables the user to restart the system on the Wyse Easy Setup shell or custom desktop.
Allow Log off	Enables the user to log off the system on the Wyse Easy Setup shell or custom desktop.

Configuring VNC settings

Use this page to configure the VNC settings.

Table 151. Configuring VNC

Option	Description
Enable VNC	Select this option to enable the VNC Server.
VNC User Prompt	If you select this option, you must accept or decline the VNC shadowing

Option	Description
VNC User Required Password	Select this option to set the VNC password.
VNC Primary Password	Select this option to change the VNC password. Enter the new password with a maximum of eight characters.
VNC View-only Password	Enables you to work on view-only mode if you login using this password.

Configuring domain settings

Read the instructions provided on the screen to add the Windows Embedded Standard 7, Windows Embedded 8 Standard or Windows 10 IoT Enterprise device to the corporate Active Directory domain.

Table 152. Configuring domain settings

Option	Description
Domain or Workgroup	From the drop-down list, select the preferred option.
Domain or Workgroup Name	Enter the FQDN of the domain.
User Name	Enter the user name. The account should have **Add to domain** option.
Password	Enter the password.
Account OU	Enter the location of the organizational unit where the computer object should be created.
Auto Login	Select the check box to display the Windows login screen.

Configuring BIOS settings for Wyse 5070 thin client with Windows 10 IoT Enterprise

Use the BIOS settings page to configure the BIOS settings for Wyse 5070 thin client and Wyse 5070 Extended thin client with Windows 10 IoT Enterprise.

Table 153. System configuration

Option	Description
Enable Audio	Select this check box to enable the audio device.
Enable Microphone	Select this check box to enable the microphone.
Enable Internal Speaker	Select this check box to enable the internal speaker.
Parallel Port	From the drop-down list, select the option to determine how the parallel port on the docking station operates. · **Disabled**: Port is disabled. · **AT**: Port is configured for IBM AT compatibility. · **PS2**: Port is configured for IBM PS2 compatibility. · **ECP**: Port is configured for extended capability port protocol.

Option	Description
	ⓘ NOTE: This option is available for Wyse 5070 Extended thin client when the add-on card is installed.
Serial Port 1	From the drop-down list, select the option to determine how the serial port on the docking station operates. This option allows you to avoid resource conflicts between devices by disabling or remapping the address of the port. • **Disabled**: Port is disabled. • **COM1**: Port is configured at 3F8h with IRQ 4. • **COM2**: Port is configured at 2F8h with IRQ 3. • **COM3**: Port is configured at 3F8h with IRQ 4. • **COM4**: Port is configured at 2F8h with IRQ 3.

Table 154. USB configuration

Option	Description
Enable Front USB Ports	Select this check box to enable the operating system to detect the devices attached to the front USB port. However, if the USB port is disabled, the operating system cannot detect the device attached to the front USB ports. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.
Front port Top	Select this option to enable the top USB port on the front of the thin client.
Front port Top Medium	Select this option to enable the top middle USB port on the front of the thin client.
Front port Bottom Medium	Select this option to enable the bottom middle USB port on the front of the thin client.
Front port Bottom	Select this option to enable the bottom USB port on the front of the thin client.
Enable Rear USB Ports	Select this check box to enable the operating system to detect the devices attached to the back USB port. However, if the USB port is disabled, the operating system cannot detect the device attached to the back USB ports. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.
Rear port Top Left	Select this option to enable the top left USB port on the back of the thin client.
Rear port Top Right	Select this option to enable the top right USB port on the back of the thin client.
Rear port Bottom Left	Select this option to enable the bottom left USB port on the back of the thin client.
Rear port Bottom Right	Select this option to enable the bottom right USB port on the back of the thin client.

Table 155. Configuring security settings

Option	Description
Enable Admin Setup Lockout	Select this option to prevent others from entering the setup when an administrator password is set.

Table 156. Configuring power management settings

Option	Description
Wake On LAN	From the drop-down list, select any option to allow the thin client to power up from the OFF state. You can trigger a thin client to power up from the OFF state by using a LAN signal.
AC Recovery	From the drop-down list, select any option to specify how the system operates when the AC power is restored.

Table 157. Configuring wireless settings

Option	Description
WLAN/WiGig	Select this check box to enable the internal wireless devices.
Bluetooth	Select this check box to enable Bluetooth devices.

Table 158. Configuring auto-on settings

Option	Description
Auto On Time	From the drop-down list, set the time of the day you want the system to turn on automatically.

Table 159. Reboot schedule settings

Option	Description
Reboot Option	Some BIOS settings require the system to restart. From the drop-down list, select one of the following options: - Reboot immediately—The system restarts immediately. - Reboot later—Select the **Reboot Hour** and **Reboot Minute** to set the system restart time. - Do not reboot—The system does not restarts.

Edit the Linux policy settings

To edit the Linux policy settings, do the following:

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **Linux**.
   The **Linux** page is displayed. The Linux thin client policy settings include the following options:
   - System Personalization
   - Desktop Experience

- Login Experience
- Network
- Security
- Central Configuration
- Other settings
- VDI Global Settings
- Remote Connection Citrix
- Remote Connection VMware
- Remote Connections RDP
- Remote Connections Browser
- Advanced

4   After configuring the policy settings, click **Save and Publish**.

Configuring system personalization

Use the **system personalization** page to configure system personalization.

Table 160. Configuring system personalization

Option	Description
Monitor Resolution (Primary)	Select this option to set the monitor resolution. From the drop-down menu, select your preferred monitor resolution.
Monitor Rotation	Select this option to define the orientation of the monitor. From the drop-down list, select either **Vertical** or **Horizontal** based on your preference.

Enable Dual Monitor	Select this option to enable the dual monitor functionality. When you select this check box, the following options are displayed:
	
	• Mirror Mode—Display is mirrored.
	• Span Mode—Display is spanned. From the drop-down list, select one of the options:
	  – On Left
	  – On Right
	  – Bottom
	  – Top

Layout	Select this option to set the keyboard layout of the thin client. From the drop-down menu, select your preferred option.
System Language	Select this option to set the language for the system. From the drop-down list, select your preferred option.
Mouse Speed	Select this option to specify the speed of the mouse pointer when moving the mouse. The range of mouse speed is 0–6.
Left-handed Mouse	Select this option to set the mouse orientation to the left position. If this check box is not selected, the mouse orientation is set to the right position.
Time Zone	Select this option to set the time zone based on your location. From the drop-down menu, select your preferred time zone.

Option	Description
Time Format	Select this option to choose the time format. From the drop-down menu, select either 12–hour or 24-hour format.
Time Servers (NTP Servers)	Select this option to list the time servers. Time severs allow the NTP server to synchronize the time.
Audio Volume	Select this option to set the audio volume of the thin client. The range of the audio volume is 0–100.
Audio Mute	Select this option to set the thin client to mute mode.
Microphone Volume	Select this option to set the microphone volume of the thin client. The range of the microphone volume is 0–100.
Microphone Mute	Select this option to set the microphone to mute mode.

Configuring desktop experience

Use the **Desktop experience** page to configure the desktop settings, such as desktop wallpaper, wallpaper layout, and the desktop shortcut keys.

Table 161. Configuring desktop experience

Option	Description
Desktop Wallpaper	Select this option to change the default wallpaper.
Wallpaper File	Select this option to choose your preferred wallpaper. Images uploaded to the file repository are displayed.
Wallpaper Layout	Select this option to set the wallpaper Layout. From the drop-down menu, select your preferred wallpaper layout. The default wallpaper layout is **center**.
Hot Keys	Select this option to disable the hot keys for the following actions: • Close current active window • Minimize current active window • Maximize/Unmaximize current active window • Unmaximize current active window • Resize current active window • Move current active window • Mouse Button Modifier • Show Panel Main Menu • Show Panel Main Menu list • Display Run Command window • Activate Screensaver • Show Desktop • Switch between open windows • Toggle current active window between full screen and normal mode • Display menu options for current window • Print screen—Take a screenshot

Configuring login experience settings

Use this page to configure the settings, such as auto login, login banner message, and passwords for admin, thin user, and root users.

Table 162. Configuring login experience settings

Option	Description
Auto Login	Select this option to enable the thin client to automatically log in without any user intervention. Use the **Auto Login Username** option to select the default login user.
Auto Login Username	Select the **Auto Login** check box to define the default user for auto login. From the drop-down menu, select your preferred option. · admin · thinuser · guest
Enable Banner on Login window	Select this option to configure a banner message in the login screen. The **Banner Message** option is displayed when you select the **Enable Banner on Login window** check box. Enter a customized text in the box displayed on the login screen.
Root Password	Enter the password if you want to change the root password.
Admin Password	Enter the password if you want to change the admin password.
Thinuser Password	Enter the password if you want to change the thinuser password.
Guest Password	Enter the password if you want to change the guest password.

Configuring network settings

Use this page to configure the network settings.

Table 163. Configuring network settings

Option	Description
Wireless Connection Name	Enter the name of the connection.
SSID	Enter the name of the Service Set Identifier (SSID) connection.
Security Mode	From the drop-down menu, select the type of security mode based on your requirement. Enter the security mode details in the respective fields.

Configuring security settings

Use this page to configure the security options.

Table 164. Configuring security settings

Option	Description
Password Encryption Algorithm	Select this option to choose the password encryption algorithm. From the drop-down menu, select any of the following options: · Base-64 · AES · Plain-Text The default value is **Base-64**.
Enable Gkey Reset	By default, the Gkey reset feature is enabled. The factory reset of the device can be performed when the G key is pressed during device boot-up.
Install Certificates	Select this option to choose the certificate which you want to install on the device. From the drop-down menu, select the certificates which are added in the file repository.
Enable SSH	Select this option to enable Secure Shell (SSH) on the device.
Allow "root" SSH login	Select this option to enable the root SSH login.
Enable VNC Server	Select this option to enable the VNC Server.
Require User to enter password	Select this option to set the VNC password.
VNC Password	Select this option to enter the VNC password.
Prompt user on VNC session start	Select this option to enable a popup message for accepting the incoming VNC connection request.

Configuring central configuration settings

Use this page to enter the file server, firmware server, root path, and the corresponding user credentials.

Table 165. Configuring central configuration settings

Option	Description
File Server Path	Enter the full path of the folder that contains the **wlx** folder. Supported protocols include ftp, http, and https. The default protocol is ftp.
File Server Username	Enter the user name to access the file server.
File Server Password	Enter the password to access the file server.
Root Path	This root path is used to access files on the server. The directory name **/wlx** is appended to the root path entry before use. If root path is not provided, **/wyse** is considered.
Firmware Server/ Path	Enter the full path of folder that contains the firmware images. Supported protocols include ftp, http, and https.

Option	Description
	The default protocol is ftp.
Firmware Server Username	Enter the user name to access the firmware server.
Firmware Server Password	Enter the password to access the firmware server.
Firmware Root Path	This root path is used to access the firmware images on the server. The directory name **/wtx** is appended to the root path entry before use. If the root path is not provided, **/wyse** is considered.

Configuring other settings

Use this page to configure the other options.

Table 166. Configuring other settings

Option	Description
Auto Power-On	Select this option to enable the system to boot up when power is restored without waiting for the user to press the power button.
Power Button Action	From the drop-down menu, select any one of the option to specify the default action to be performed when you press the power button. · Interactive · Restart · Shutdown · None
DHCP Vendor ID	Select this option to change the DHCP Vendor ID. The default Vendor ID is **wyse-5000**.
Browser Homepage	Select this option to change the browser homepage. Enter the URL address of your choice to set the browser homepage.

Configuring VDI global settings

Use this page to configure the global settings for Citrix and VMware View clients.

Table 167. Configuring Citrix general settings

Option	Description
ICA Browsing Protocol	Select this option to set the default browsing protocol.
Browser IP	Enter the browser IP address.
Store Name	Select this option to specify the store name.
Domain Name	Enter the domain name.

Option	Description
PN Desktop Setup (Show All Application)	Select this option to enable the PN desktop setup. When this option is enabled, all the published applications are displayed on the desktop.
Enable Multimedia Redirection (MMR)	Select this option to enable the Multimedia Redirection.
Enable H.264 Decoding Support	Select this option to enable the H.264 decoding support for the ICA connections.
HDX Webcam Frame Rate	Select this option to set the preferred frame rate for the HDX Webcam.
HDX Webcam Image Width	Select this option to set the width of image request from the HDX Webcam.
HDX Webcam Image Height	Select this option to set the height of image request from the HDX Webcam.
Audio Bandwidth Limit	Select this option to set the bandwidth used for audio input. From the drop-down menu, select any one of the following options: · Low · Medium · High
Enable UDP Audio	Select this option to enable the transport of audio data through UDP.
Flash Redirection Policy	Select this option to set the Flash Redirection policy. From the drop-down menu, select either allow or deny the Flash Redirection policy.
Transparent Key Passthrough	Select this option to determine how the mapping of certain key combinations is used when connecting to ICA sessions. From the drop-down menu, select any one of the following options: · Local · Remote · Full Screen Only
Use Alternate Address	Select this option to use an alternate IP address from the ICA master browser to pass firewalls.
ICA Proxy Type	Select this option to choose the proxy type for the ICA connection. The default value is **None**.

Table 168. Configuring Citrix USB redirection settings

Option	Description
Allow USB Redirection of devices plugged in before ICA Session start	Select this option to set the ICA Desktop Appliance Mode. This option allows the USB redirection of the devices plugged in before the ICA session starts.
Enable USB Redirection	Select this option to enable the Citrix USB redirection to all the devices.

Option	Description
	You can specify which devices and device families can be allowed or denied through the USB redirection policy in to the Citrix sessions.

Table 169. Configuring Citrix drive mapping

Option	Description
Enable ICA Dynamic Drive Mapping	Select this option to enable the Double ICA Dynamic Drive Mapping. If this option is disabled, you can add the individual drives for various drive types. As a result, only individual drives are redirected in to the ICA session.

Table 170. Configuring VMware USB redirection

Option	Description
Enable USB Redirection	Select this option to enable VMware USB Redirection to all the devices. You can specify which devices and device families can be allowed or denied through the USB redirection policy in to the VMware sessions.

Configuring remote connection settings—Citrix

Use this page to create a Citrix broker connection. Configuration settings for the Citrix connection vary based on the connection type.

Table 171. Configuring remote connection settings

Option	Description
Connection Name	Select this option to enter a name to identify the connection.
Auto Launch Connection on Logon	Select this option to automatically launch the connection after you log in.
Connection Type	Select this option to set a connection type. From the drop-down menu, select any one of the following options: • Server Connection • Published Application • Store Front
Citrix Server FQDN or IP Address	Select this option to enter the IP address or FQDN of the Citrix server. This option is displayed when you select the connection type as **Published Application** or **Storefront**.
Published Application	Select this option to specify a published application to start. This option is displayed when you select the connection type as **Published Application** or **Storefront**.
Connection Server	Select this option to enter the IP address or FQDN of the Citrix connection server.

Option	Description
Username	Enter the user name.
Password	Enter the password.
Domain Name	Enter the domain name.
Store Name	Enter the store name of the Citrix server. This option is displayed when you select the connection type as **Published Application** or **Storefront**.
Browsing Protocol	Select this option to set a browsing protocol for the secure and non-secure connections. From the drop-down list, select either of the following options: · http · https
Low Bandwidth	Select this option to set the slow bandwidth optimization.
Enable Sound	Select this option to enable sound.
SmartCard Login	Select this option to enable the smart card login feature for ICA connection.
Encryption Level	Select this option to set an encryption level. From the drop-down menu, select any one of the following encryption levels: · Basic · RC5 (128–bit – Log in Only) · RC5 (40–bit) · RC5 (56–bit) · RC5 (128– bit)
Windows Size	Select this option to set a window size. From the drop-down menu, select any one of the following options: · Default · Seamless · 640 x 480 · 1024 x 768 · 800 x 600 · 1280 x 1024 · 1600 x 1200 · Full Screen
Screen Color Depth	Select this option to set a screen color depth. From the drop-down menu, select any one of the following options: · 64K · 256 · 16M
Auto Reconnect	Select this option to enable the thin client to reconnect to the Citrix session automatically.

Option	Description
Delay before trying to reconnect	Select this option to set the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Configuring remote connection settings—VMware

Use this page to create a VMware View broker connection.

Table 172. Configuring remote connection VMware

Option	Description
Connection Name	Select this option to enter a name to identify the connection.
Auto Launch Connection On Logon	Select this option to automatically launch the connection after you log in.
VMWare Server Address	Enter the hostname or the IP address of the VMware View server.
VMWare Server Port Number	Enter the port number of the host.
Use Secure Connection (SSL)	Select this option to use the SSL connection.
Protocol	Select this option to set **PCOIP** or **RDP** as protocol.
Enable NLA	Select this option to enable Network Level Authentication. When the **RDP** option is set as protocol, this option is displayed.
Username	Enter the user name
Password	Enter the password.
Domain Name	Enter the domain name.
Interactive Mode	Select this option to enable the User Interactive mode.
Lock the Server URL / Host field	Select this option to lock the server URL.
Security Mode	Select this option to set the security mode. From the drop-down menu, select any one of the following options: · Never connect to untrusted servers · Warn before connecting to untrusted servers · Do not verify server identity certificates.
Fullscreen Mode	Select this option to view the remote session in the fullscreen mode.
Window Size	Select this option to set a window size. From the drop-down menu, select any one of the following options: · Use all monitors · Full Screen · Large Screen · Small Screen

Option	Description
	• 1024 x 768 • 800 x 600 • 640 x 480
Disable Fullscreen drop down menu bar	Select this option to disable the drop-down menu in the fullscreen mode.
Automatically launch this Desktop	Select this option to specify the name of the published desktop to automatically launch upon successful connection.
Auto Reconnect	Select this option to enable the thin client to reconnect to the VMware session automatically.
Delay before trying to reconnect	Enter the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Configuring remote connection settings—RDP

Use this page to create an RDP broker connection.

Table 173. Configuring remote connection settings—RDP

Option	Description
Connection Name	Select this option to enter the name to identify the connection.
Auto Launch Connection on Logon	Select this option to automatically launch the connection after you log in.
Server Address	Enter the server name or the IP address.
SmartCard Login	Select this option to enable the smart card authentication.
Use Network Level Authentication (NLA)	Select this option to enable the Network Level authentication.
Username	Enter the user name.
Password	Enter the password.
Domain Name	Enter the domain name.
Window Size	Select this option to set a window size. From the drop-down menu, select any one of the following options: • Default • 640 x 480 • 1024 x 768 • 800 x 600 • 1280 x 1024 • 1600 x 1200 • Full Screen

Option	Description
Forward All Printers	Select this option to forward all the printers to the remote connection.
Auto Reconnect	Select this option to enable the thin client to reconnect to the RDP session automatically.
Delay before trying to reconnect	Enter the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Drive Mapping	Select this option to map drives on the RDP session. Click the **Add Drive Mapping** button, and enter the following details:
	
	• Drive Letter—From the drop-down menu, select the drive letter.
	• Drive Type—Select any one of the following drive types:
	  – USB Disk or Memory Stick
	  – USB CD ROM
	  – USB Floppy

Use RD Gateway settings	Select this option to use the RD gateway settings. The **RD Server**, and the **Use Remote Desktop credentials for RD Gateway** options are displayed.
RD Server	Select this option to specify the RD gateway host address.
Use Remote Desktop Credentials for RD Gateway	Select this option to use the remote desktop credentials for the RD gateway. When you clear the check box, the **RD Username**, **RD Password**, and **RD Domain Name** options are displayed.
RD Username	Enter the RD user name for the RD gateway login.
RD Password	Enter the RD password for the RD gateway login.
RD Domain Name	Enter the RD domain name for the RD gateway login.

Configuring remote connection settings—Browser

Use this page to configure the remote connections browser.

Table 174. Configuring remote connection settings—Browser

Option	Description
Connection Name	Enter the name to identify the connection.
Auto launch Connection on Logon	Select this option to automatically launch the connection during login.
URL	Enter the starting URL.
Kiosk Mode	Select this option to enable the kiosk mode.
Window Size	Select this option to set a window size. From the drop-down menu, select the size of the window of your choice.

Option	Description
Auto Reconnect	Select this option to enable the thin client to reconnect the browser automatically.
Delay before trying to reconnect	Enter the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Configuring advanced settings

Configurations can be applied to the Linux client device by providing the INI parameters in the **Advanced** option. Dell recommends that you do not include the INI parameters for policies which are already configured in other options. Password encoding and encryption are not applied to password parameters.

Table 175. Configuring advanced settings

Option	Description
No Global INI	If selected, the global INI parameter from the file server is not downloaded. Enter the INI parameter from line 1 to line 20 for the thin clients.

Edit the ThinLinux policy settings

To edit the ThinLinux policy settings, do the following:

1 Click **Groups & Configs**.

The **Groups & Configs** page is displayed.

2 Click the **Edit Policies** drop-down menu.

3 Click **ThinLinux**.

The **ThinLinux** page is displayed. The ThinLinux thin client policy settings include the following options:

- System Personalization
- Desktop Experience
- Login Experience
- Network
- Security
- Central Configuration
- Other settings
- VDI Global Settings
- Remote Connections Citrix
- Remote Connections VMware
- Remote Connections RDP
- Remote Connections Browser
- Advanced Settings
- Device Info
- BIOS ThinLinux 3040 Settings
- BIOS ThinLinux 5070 Settings

4 After configuring the policy settings, click **Save and Publish**.

Configuring system personalization

Use the **System Personalization** page to configure the system personalization.

Table 176. Configuring display settings

Option	Description
Monitor Resolution—Primary	Select this option to set the monitor resolution. From the drop-down menu, select your preferred monitor resolution.
Monitor Rotation	Select this option to define the orientation of the monitor. From the drop-down list, select either vertical or horizontal based on your preference. ⓘ **NOTE: The horizontal and vertical (Rotate to right) options are only available for Wyse Management Suite server UI.**
Enable Dual Monitor	Select this option to enable the dual monitor functionality. If you select this check box, the following options are displayed: • Display Mode—Use this option to set the Display mode. • Monitor Resolution (Secondary)—From the drop-down menu, select your preferred monitor resolution. • Span Position—Display is spanned. From the drop-down menu, select any one of the following options: 　– On Left 　– On Right 　– Bottom 　– Top
Enable Multi Monitor	Select this option to enable multi-monitor settings.
Monitor Resolution (Third)	From the drop-down list, select the monitor resolution for the third monitor. ⓘ **NOTE:** 　• Windows Embedded Standard multi-monitor—No limitations. 　• ThinLinux multi-monitor— Dell Wyse 5070 extended thin client supports multi-monitor functionality when more than four monitors are connected.
Span Position	Display is spanned. From the drop-down, select one of the options: • Right • Left • Bottom • Top
Select number of monitors to be Supported.	From the drop-down list, select the number of monitors to be supported. ⓘ **NOTE: If you select more than three monitors, then the monitor resolution setting and monitor rotation setting is common for all the monitors. Dell Wyse 5070 extended thin client supports multi-monitor functionality when more than four monitors are connected.**

Table 177. Configuring keyboard settings

Option	Description
Layout	Select this option to set the keyboard layout of the thin client. From the drop-down menu, select your preferred option.

Table 178. Configuring language settings

Option	Description
System Language	Select this option to set the language for the system. From the drop-down list, select your preferred option.

Table 179. Configuring mouse settings

Option	Description
Mouse Speed	Select this option to specify the speed of the mouse pointer when moving the mouse. The range of mouse speed is 0–6.
Left-handed Mouse	Select this option to swap the mouse button between left-click and right-click.

Table 180. Configuring time zone settings

Option	Description
Time Zone	Select this option to set the time zone based on your location. From the drop-down menu, select your preferred time zone.
Time Format	Select this option to select the time format. From the drop-down menu, set the time format to either 12–hour or 24-hour format.
Time Servers (NTP Servers)	Select this option to list the time servers. Time severs allow the NTP server to synchronize the time. Multiple servers are allowed, and the server names must be separated by commas.

Table 181. Configuring audio settings

Option	Description
Audio Volume	Select this option to set the audio volume of the thin client. The range of the audio volume is 0–100.
Audio Mute	Select this option to set the thin client to mute mode.
Microphone Volume	Select this option to set the microphone volume of the thin client. The range of the microphone volume is 0–100.
Microphone Mute	Select this option to set the microphone to mute mode.

Configuring desktop experience

Use this page to configure the desktop settings, such as desktop wallpaper, wallpaper layout, and the desktop shortcut keys.

Table 182. Desktop experience

Option	Description
Desktop Wallpaper	Select this option to change the default wallpaper.
Wallpaper File	Select this option to select your preferred wallpaper. Images uploaded to the file repository are displayed.
Wallpaper Layout	Select this option to set the wallpaper layout. From the drop-down menu, select your preferred wallpaper layout. The default wallpaper layout is **center**.

Hot Keys—Select any of the following check boxes to disable the hot keys and their respective functionality:

Configure hot keys for following actions:

- Minimize current active window
- Maximize/Unmaximize current active window
- Unmaximize current active window
- Resize current active window
- Move current active window
- Show Desktop
- Switch between open windows
- Toggle current active window between full screen and normal mode
- Print screen (Take a screenshot), you can select the check box to enable or disable the print screen option.

Configuring login experience

Use this page to configure the settings, such as auto login, login banner message, and passwords for admin, thin user, and root users.

Table 183. Configuring login experience

Option	Description
Auto Login	Select this option to enable the thin client to automatically log in without any user intervention.
Enable Banner on Login window	Select this option to configure a banner message in the login screen.
Banner Message	The **Banner Message** option is displayed when you select the **Enable Banner on Login window** check box. Enter a customized text in the box displayed on the login screen.
Root Password	Enter the password if you want to change the root password
Thinuser Password	Enter the password if you want to change the thinuser password

Configuring network settings

Use this page to configure the network settings.

Table 184. Configuring network settings

Option	Description
Wireless Connection Name	Enter the name of the connection
SSID	Enter the name of the Service Set Identifier (SSID) connection.
Security Mode	From the drop-down menu, select the type of security mode based on your requirement. Enter the security mode details in the respective fields.

Configuring security settings

Use this page to configure the security policy settings.

Table 185. Configuring general settings

Option	Description
Enable Gkey Reset	By default, the Gkey reset feature is enabled. The factory reset of the device can be performed when the G key is pressed during device boot.
Install Certificates	Select this option to choose the certificate which you want to install on the device. From the drop-down menu, select the certificates which are added in the file repository.

Table 186. Configuring SSH settings

Option	Description
Enable SSH	Select this option to enable Secure Shell (SSH) on the device.
Allow "root" SSH login	Select this option to enable the root SSH login.

Table 187. Configuring VNC settings

Option	Description
Enable VNC Server	Select this option to enable the VNC Server.
Require User to enter Password	Select this option to set the VNC password.
VNC Password	Select this option to enter the VNC password.
Prompt user on VNC session start	Select this option to enable a popup message for accepting the incoming VNC connection request.

Configuring central configuration settings

Use this page to enter the file server, firmware server, root path, and the corresponding user credentials.

Table 188. Configuring central configuration settings

Option	Description
File Server/ Path	Enter the full path of the folder that contains the **wlx2** folder. Supported protocols include ftp, http, and https. The default protocol is ftp.
File Server Username	Enter the user name to access the file server.
File Server Password	Enter the password to access the file server.
Root Path	This root path is used to access files on the server. The directory name **/wlx2** is appended to the root path entry before use. If root path is not provided, **/wyse** is considered.
Enable Delayed Update	Select this option to enable the background image or the add-ons upgrade or downgrade process.
Delayed Update Server / Path	Enter the full path of the folder that contains the firmware images. Supported protocols include ftp, http, and https. The default protocol is ftp.
Delayed Update Server Username	Enter the user name to access the delayed update server.
Delayed Update Server Password	Enter the password to access delayed update server.
Delayed Update Mode	Select this option to set the update mode for delayed update process.
Reset to factory defaults	Select this option to set the device to the factory default condition after the imaging process.
Allow base image downgrade	Select this option to enable the base image downgrade.

Configuring other settings

Use this page to configure the other options.

Table 189. Configuring other settings

Option	Description
Auto Power-On	Select this option to enable the system to boot when power is restored without waiting for the user to press the power button.
Power Button Action	From the drop-down menu, select any one of the options: • Interactive • Restart • Shutdown

Option	Description
	· None The options define the action to be taken when you press the power button.
DHCP Vendor ID	Select this option to change the DHCP Vendor ID. The default Vendor ID is **wyse-5000**.
Browser Homepage	Select this option to change the browser homepage. Enter the URL address of your choice to set the browser homepage.

Configuring VDI global settings

The following VDI Global Settings can be configured under ThinLinux Policy Settings. In the VDI Global Settings you can set the Global settings for Citrix and VMWare View.

Table 190. Configuring Citrix general settings

Option	Description
ICA Browsing Protocol	Select this option to set the default browsing protocol.
ICA PAM Login	Select this option to configure the PAM login.
Browser IP	Enter the browser IP address.
Store Name	Specify the store name.
Domain Name	Enter the domain name.
PN Desktop Setup (Show All Applications)	Select this option to enable the PN desktop setup. When this option is enabled, all the published applications are displayed on the desktop.
Enable Multimedia Redirection (MMR)	Select this option to enable the Multimedia Redirection.
Enable H.264 Decoding Support	Select this option to enable the H.264 decoding support for the ICA connections.
HDX Webcam Frame Rate	Select this option to set the preferred frame rate for the HDX Webcam.
HDX Webcam Image Width	Select this option to set the width of image request from the HDX Webcam.
HDX Webcam Image Height	Select this option to set the height of image request from the HDX Webcam.
Audio Bandwidth Limit	Select this option to set the bandwidth used for audio input. From the drop-down menu, select any one of the following options: · Low · Medium · High

Option	Description
Enable UDP Audio	Select this option to enable the transport of audio data through UDP.
Flash Redirection Policy	Select this option to either allow or deny Flash Redirection Policy.
Transparent Key Passthrough	Select this option to determine how the mapping of certain key combinations is used when connecting to ICA sessions. From the drop-down menu, select any one of the following options: · Local · Remote · Full Screen Only
Use Alternate Address	Select this option to use an alternate IP address from the ICA master browser to pass firewalls.
ICA Proxy Type	Select this option to choose the proxy type for the ICA connection. The default value is **None**.

Table 191. Configuring Citrix USB redirection settings

Option	Description
Allow USB Redirection of devices plugged in before ICA Session start	Select this check box for ICA Desktop Appliance Mode. This option allows USB redirection of the devices that were plugged in before ICA session start.
Enable USB Redirection	Select this option to enable Citrix USB redirection to all the devices. You can specify which devices and device families can be allowed or denied in to the Citrix sessions.

Table 192. Configuring Citrix Drive mapping settings

Option	Description
Enable ICA Dynamic Drive Mapping	Select this option to enable the ICA Dynamic Drive Mapping. If this option is disabled, you can add the individual drives for various drive types. As a result, only individual drives are redirected in to the ICA session.
Map all drives to a single share name (WyseUSB)	Select this option to redirect all the USB device contents in the ICA session under a single directory—Wyse USB.

Table 193. Configuring VMware USB redirection settings

Option	Description
Enable USB Redirection	Select this option to either allow or deny USB redirection policy in to the VMware sessions.

Configuring remote connection settings—Citrix

Use this page to create a Citrix broker connection. Configuration settings for the Citrix connection vary based on the connection type.

Table 194. Configuring remote connection settings—Citrix

Option	Description
Connection Name	Select this option to enter a name to identify the connection.
Auto Launch Connection on Logon	Select this option to automatically launch the connection after you log in.
Connection Type	Select this option to set a connection type. From the drop-down menu, select any one of the following options: • Server Connection • Published Application • Store Front
Connection Server	Select this option to enter the IP address or FQDN of the Citrix server.
Citrix Server FQDN or IP address	Select this option to enter the Citrix server FQDN or IP address. This is applicable for Published Application and StoreFront connection type.
Published Application	Select this option to specify a published application to start. This is applicable for Published Application and StoreFront connection type.
Store Name	Enter the store name. This is applicable for Published Application and StoreFront connection type.
Username	Enter the user name.
Password	Enter the password.
Domain Name	Enter the domain name.
Browsing Protocol	Select this option to set a browsing protocol for the secure and non-secure connections. From the drop-down list, select either of the following options: • http • https
Low Bandwidth	Select the check box for low bandwidth optimization.
Enable Sound	Select the check box to enable sound.
SmartCard Login	Select the check box to enable smart card login for ICA connection.
Encryption Level	Select this option to set an encryption level. From the drop-down menu, select any one of the following encryption levels: • Basic • RC5 (128–bit – Log in Only) • RC5 (40–bit) • RC5 (56–bit) • RC5 (128– bit)
Windows Size	Select this option to set a window size. From the drop-down menu, select any one of the following options:

Option	Description
	• Default • Seamless • 640 x 480 • 1024 x 768 • 800 x 600 • 1280 x 1024 • 1600 x 1200 • Full Screen
Screen Color Depth	Select this option to set a screen color depth. From the drop-down menu, select any one of the following options: • 64K • 256 • 16M
Auto Reconnect	Select this option to enable the thin client to reconnect to the Citrix session automatically.
Delay before trying to reconnect	Select this option to set the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Configuring remote connection settings—VMware

Use this page to create a VMware View broker connection.

Table 195. Configuring remote connection settings—VMware

Option	Description
Connection Name	Select this option to enter a name to identify the connection.
Auto Launch Connection On Logon	Select this option to automatically launch the connection after you log in.
VMWare Server Address	Enter the hostname or the IP address of the VMware View server.
VMWare Server Port Number	Enter the port number of the host.
Use Secure Connection (SSL)	Select this option to use the SSL connection.
Protocol	Select this option to set **PCOIP**, **RDP**, or **Blast** as protocol.
Username	Enter the user name.
Password	Enter the password.
Domain name	Enter the domain name.
Enable NLA	Select this option to enable Network Level Authentication. When the **RDP** option is set as protocol, this option is displayed.
Username	Enter the user name when the PCoIP protocol is selected.

Option	Description
Password	Enter the password when the PCoIP protocol is selected.
Domain Name	Enter the domain name.
Interactive Mode	Select this option to enable the User Interactive mode.
Lock the Server URL / Host field	Select the check box to lock the server URL.
Security Mode	Select this option to set the security mode. From the drop-down menu, select any one of the following options: • Never connect to untrusted servers • Warn before connecting to untrusted servers • Do not verify server identity certificates.
Fullscreen Mode	Select this option to view the remote session in the fullscreen mode.
Window Size	Select this option to set a window size. From the drop-down menu, select any one of the following options: • Use all monitors • Full Screen • Large Screen • Small Screen • 1024 x 768 • 800 x 600 • 640 x 480
Disable Fullscreen Drop Down Menu Bar	Select this option to disable the drop-down menu in the fullscreen mode.
Automatically Launch This Desktop	Select this option to specify the name of the published desktop to automatically launch upon successful connection.
Auto Reconnect	Select this option to enable the thin client to reconnect to the VMware session automatically.
Delay before trying to reconnect	Enter the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Configuring remote connection settings—RDP

Use this page to create an RDP broker connection.

Table 196. Configuring remote connection settings—RDP

Option	Description
Connection Name	Select this option to enter the name to identify the connection.
Auto Launch Connection on Logon	Select this option to automatically launch the connection after you log in.

Option	Description
Server Address	Enter the server name or the IP address.
SmartCard Login	Select this option to enable the smart card authentication.
Use Network Level Authentication (NLA)	Select this option to enable the Network Level authentication.
Username	Enter the user name.
Password	Enter the password.
Domain Name	Enter the domain name.
Window Size	Select this option to set a window size. From the drop-down menu, select any one of the following options: • Default • 640 x 480 • 1024 x 768 • 800 x 600 • 1280 x 1024 • 1600 x 1200 • Full Screen
Forward All Printers	Select this option to forward all the printers to the remote connection.
Auto Reconnect	Select this option to enable the thin client to reconnect to the RDP session automatically.
Delay before trying to reconnect	Enter the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.
Map all drives to a single share name—WyseUSB	Select this option to map all the devices to a single shared name—WyseUSB.

Table 197. Configuring RD gateway settings

Option	Description
Use RD Gateway settings	Select this option to use the RD gateway settings. The **RD Server** and the **Use Remote Desktop credentials for RD Gateway** options are displayed.
RD Server	Select this option to specify the RD gateway host address.
Use Remote Desktop credentials for RD Gateway	Select this option to use the remote desktop credentials for the RD gateway.

Configuring remote connection settings—Browser

Use this page to configure the Remote connections browser.

Table 198. Configuring remote connection settings—Browser

Option	Description
Connection Name	Enter the name to identify the connection.
Auto launch Connection on Logon	Select this option to automatically launch the connection during login.
URL	Enter the starting URL.
Kiosk Mode	Select this option to enable the kiosk mode.
RC Disable Panel in kiosk mode	Select this option to disable the RC panel in the kiosk mode.
Window Size	Select this option to set a window size. From the drop-down menu, select the size of the window of your choice.
Auto Reconnect	Select this option to enable the thin client to reconnect the browser automatically.
Delay before trying to reconnect	Enter the time in seconds to delay the reconnection attempt. When you select the **Auto Reconnect** check box, this option is displayed.

Configuring advanced settings

Configurations can be applied to the ThinLinux client device by providing the INI parameters in the **Advanced** option. Dell recommends that you do not include the INI parameters for policies which are already configured in other options. The password encoding and encryption are not applied for the password parameters.

Table 199. Configuring advanced settings

Option	Description
No Global INI	If selected, the global INI parameter is not downloaded from the file server. Enter the INI parameter from line 1 to line 20 for the thin clients.

Configuring device information

Use the **Device Info** page to set the device details.

Table 200. Configuring device information

Option	Description
Location	Enter the device location.
Contact	Enter the device contact.
Custom 1 to 3	Enter the custom values.

Configuring Wyse 3040 thin client BIOS settings

Use this page to configure the BIOS settings of Wyse 3040 thin clients.

Table 201. Configure general settings

Option	Description
Device Notes	Enter the device notes in the provided field. For example, property ownership tag.

Table 202. Configure system settings

Option	Description
Enable UEFI Network Stack	Select this check box to enable UEFI Network Stack. The networking protocols are installed and the pre-OS and early OS networking features are made available to use any enabled NICs.
Integrated NIC	From the drop-down list, select the preferred option.
Audio	Select this option to enable the audio device.

Table 203. Configure USB settings

Option	Description
Enable USB Boot Support	Select this check box to enable the USB boot setup. Allows you to boot any type of USB Mass Storage Devices.
Enable Front USB Ports	Select this check box to enable the device attached to this port. If you select this check box, the device is made available to the operating system also. However, if the USB port is disabled, the operating system cannot detect any device attached to this port. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.
Enable Rear-Left Dual USB 2.0 Ports	Select this check box to enable the device attached to this port. If you select this check box, the device is made available to the operating system also. However, if the USB port is disabled, the operating system cannot detect any device attached to this port. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.

Table 204. Configure wireless settings

Option	Description
Wireless Device Enable	Select the check box to enable internal wireless devices.

Table 205. Configure security settings

Option	Description
UEFI Capsule Firmware Update	Select the check box to update the BIOS through UEFI capsule firmware update.

Table 206. Configure BIOS Admin password settings

Option	Description
Enable Admin Password	Select this check box to enable the BIOS administrator password. Successful changes to this password take effect immediately.
Admin Password	Enter the new BIOS administrator password. This option is available only if you select the **Enable Admin Password** check box.

Table 207. Configure power management settings

Option	Description
USB Wake Support	Select the check box to allow the thin client to power up from the off state.
Wake On LAN	From the drop-down list, select an option to allow the thin client to power up from the off state. You can trigger a thin client to power up from the off state by using a LAN signal or a wireless LAN signal.
AC Recovery	From the drop-down list, select an option to specify how the system must behave when the AC power is restored.

Table 208. Configure auto-on settings

Option	Description
Auto On	From the drop-down list, set the time of day you want the system to turn on automatically.

Table 209. Configure post behavior settings

Option	Description
Numlock LED	Select the check box to turn on the NumLock LED light when the systems restarts.
Keyboard Errors	Select the check box to display the keyboard related errors when the systems restarts.
Fastboot	From the drop-down list, select an option to increase speed of the restart process.
Extend BIOS POST Time	From the drop-down list, select a delay time to see the post status messages.

Table 210. Configure reboot schedule

Option	Description
Reboot Option	Some BIOS settings requires the system to restart. From the drop-down list, select one of the following options: · Reboot immediately—The system restarts immediately. · Reboot later—Select the **Reboot Hour** and **Reboot Minute** to set the system restart time. · Do not reboot—The system does not restarts.

Configuring BIOS settings for Wyse 5070 thin client with ThinLinux

Use the **BIOS** settings page to configure the BIOS settings for Wyse 5070 thin client with ThinLinux.

Table 211. Configure general settings

Option	Description
Device Notes	Enter the device notes in the provided field. For example, property ownership tag.

Table 212. Configure system settings

Option	Description
Enable Audio	Select this check box to enable the audio device.
Enable UEFI Network Stack	Select this check box to enable **UEFI Network Stack**. For the enabled NICs, the networking protocols are installed, and the pre-OS and early OS networking features are available.
Integrated NIC	From the drop-down list, select the preferred option. This option controls the on-board LAN controller. • **Disabled**: The internal LAN is disabled and is not visible to the operating system if it does not have an IP address. • **Enabled**: The internal LAN is enabled. • **Enabled w/PXE**: The internal LAN is enabled with PXE boot. ⓘ **NOTE: Dell recommends not to disable the integrated NIC and integrated NIC 2.**
Parallel Port	From the drop-down list, select the option to determine how the parallel port on the docking station operates. • **Disabled**: Port is disabled. • **AT**: Port is configured for IBM AT compatibility. • **PS2**: Port is configured for IBM PS2 compatibility. • **ECP**: Port is configured for extended capability port protocol. ⓘ **NOTE: This option is available for extended chassis when the add-on card is installed.**
Serial Port 1	From the drop-down list, select the option to determine how the serial port on the docking station operates. This option enables you to avoid resource conflicts between devices by disabling or remapping the address of the port. • **Disabled**: Port is disabled. • **COM1**: Port is configured at 3F8h with IRQ 4. • **COM2**: Port is configured at 2F8h with IRQ 3. • **COM3**: Port is configured at 3F8h with IRQ 4. • **COM4**: Port is configured at 2F8h with IRQ 3.

Table 213. Configure USB settings

Option	Description
Enable USB Boot Support	Select this check box to enable the USB boot setup. Allows you to boot any type of USB Mass Storage Devices.
Enable Front USB Ports	Select this check box to enable the device attached to the front USB port. If you select this check box, the device is detected by the operating system. However, if the USB port is disabled, the operating system cannot detect the device attached to the front USB port. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.
Enable Rear USB Ports	Select this check box to enable the device attached to this back USB port. If you select this check box, the device is detected by the operating system. However, if the USB port is disabled, the operating system cannot detect the device attached to the back USB port. ⓘ NOTE: The USB keyboard and the mouse always work in the BIOS setup irrespective of this setting.

Table 214. Configure security settings

Option	Description
Enable UEFI Capsule Firmware Update	Select the check box to update the BIOS through UEFI capsule firmware update.
Enable admin Setup Lockout	Select this check box to prevent others from entering the setup when an administrator password is set.

Table 215. Configure power management settings

Option	Description
Wake On LAN	From the drop-down list, select an option to allow the thin client to power up from the OFF state. You can direct the thin client to power up from the OFF state by using a LAN signal.
AC Recovery	From the drop-down list, select an option to specify how the system should operate when the AC power is restored.
USB Wake Support	Select the check box to allow the thin client to power up from the OFF state.

Table 216. Configure post behavior settings

Option	Description
Enable Numlock LED	Select the check box to turn on the NumLock LED light when the system restarts.
Enable Keyboard Errors Detection	Select the check box to enable the system to display keyboard related errors at restart.
Fastboot	From the drop-down list, select an option to increase the speed of the restart process.

Option	Description
Extend BIOS POST Time	From the drop-down list, select a delay time to see the post status messages.

Table 217. Configure wireless settings

Option	Description
WLAN/WiGig	Select this check box to enable the internal wireless devices.
Bluetooth	Select this check box to enable Bluetooth devices.

Table 218. Configure BIOS administrator password

Option	Description
Enable administrator Password	Select this check box to enable the BIOS administrator password. If you change this password, the changes are applied immediately.
administrator Password	Enter the new BIOS administrator password. This option is available only if you select the **Enable administrator Password** check box.

Table 219. Configure auto-on settings

Option	Description
Auto On Time	From the drop-down list, set the time of the day that you want the system to turn on automatically.

Table 220. Configure reboot schedule settings

Option	Description
Reboot Option	Some BIOS settings require the system to restart. From the drop-down list, select one of the following options: • Reboot immediately—The system restarts immediately. • Reboot later—Select the **Reboot Hour** and **Reboot Minute** to set the system restart time. • Do not reboot—The system does not restart.

Editing Teradici policy settings

To edit the Teradici policy settings, do the following:

1 Click **Groups & Configs**.

The **Groups & Configs** page is displayed.
2 Click the **Edit Policies** drop-down menu.
3 Click **Teradici**.

The **Teradici** page is displayed. The Teradici thin client policy settings contain the following options:

- Timezone
- Language
- Company Logo
- Video
- Power

- Security
- Firmware upgrade
- Remote Connection

4   Click **Save and Publish**.

Configuring time zone settings

Use the **Time zone** page to configure the time zone settings for Teradici thin client.

Table 221. Configure time zone settings

Option	Description
Enable NTP	Select the check box to enable the Network Time Protocol (NTP) feature.
NTP Server	Select this option to enter the NTP hostname. The hostnames must be either IP addresses or FQDNs.
Query Interval	Enter the query response interval in minutes, hours, days, or weeks. Query response interval is the maximum amount of time that can pass between the time the router sends a query and receives a response from the host.
Time zone	From the drop-down list, select the time zone of the system.
Enable DayLight Savings	Select the check box to enable the Daylight Saving Time (DST) feature.

Configuring language settings

Use the **Language** page to configure the language settings.

Table 222. Configure language settings

Option	Description
Language	From the language drop-down list, select the language for Object Storage Device (OSD) user interface.
Keyboard Layout	From the keyboard layout drop-down list, select the layout for the OSD.

Configuring company logo settings

Use the **Company Logo** page to configure the company logo settings.

Table 223. Configuring company logo settings

Option	Description
Logo file	From the drop-down list, select the required logo file. The Teradici OSD logo files located in the **File Repository Inventory** page are loaded.

Option	Description
	ⓘ **NOTE: The logo image must be a 24 bitmap which does not exceed 256 resolutions by 24 resolutions. Any other image with different properties is not displayed or is displayed incorrectly.**
Use logo for view banner	Select the check box against the logo banner that you want to be displayed.

Configuring video settings

Use the **Video** page to configure the video settings.

Table 224. Configure video settings

Option	Description
Minimum Image Quality	Enables you to change the image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, select **Reduced** to enable higher frame rates. Select towards Perception-Free to enable higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the Minimum Image Quality parameter. Note: The Maximum Initial Image Quality must be greater than or equal to the Minimum Image Quality.
Maximum Image Quality	Select towards Reduced to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Select towards Perception-Free to produce higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of the screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. Note: The Maximum Initial Image Quality must be greater than or equal to the Minimum Image Quality.
Enable local cursor	When enabled, the Tera2PCoIP Zero Client always shows the local cursor. When disabled, the local cursor is only shown when the host requests it or a locally-terminated mouse is connected.

Configuring power settings

Use the **Power** page to configure the power settings.

Table 225. Configure power settings

Option	Description
OSD Screen Saver Timeout	This is the period of inactivity in the device. You can enter the time in seconds. After the time is entered, the device sets the attached

Option	Description
	displays to low power mode. The range is 10–9999. Enter the time as 0 to disable this option. ⓘ NOTE: **This feature is applicable only when the device is not in the session.**
Display Suspend Timeout	This is the period of inactivity in the device. You can enter the time in seconds. After the time is entered, the device sets the attached displays to low power mode. The range is 10–14400. Enter the time as 0 to disable this option. ⓘ NOTE: **This feature applicable only when the device is in the session.**

Configuring security settings

Use the **Security** page to configure the security settings.

Table 226. Upload certificate

Option	Description
Certificates	Select the required check box to upload the certificate. Clear the check box to delete an uploaded certificate. The list of certificates uploaded on the **File Repository Inventory** page is displayed. The certificates are deleted after you restart the device. You can only upload **.pem** files.

Table 227. USB device authorization

Option	Description
Authorized/Unauthorized Devices based on Class	From the **Status**, and the **Device Class** drop-down list, select your preferred option. You can authorize or unauthorize a USB device based on class. Click the **Add Class** option to add more classes. Click the **–** icon to remove a class.

Table 228. Advanced configuration

Option	Description
Enable Administrative Web Interface	Select the check box to enable the management console interface. If enabled, the PCoIP management console cannot access or manage the Tera2 PCoIP zero client.
Enable Wake-On-LAN	Select the check box to enable the thin client to power up from the off state. You can trigger a thin client to power up from the off state by using a LAN signal.
Enable Power On After Power Loss	Select the check box to enable the thin client to power up from the off state when the power is supplied.
Remember Username	Select the check box to populate the last entered user name automatically.
Security Settings	From the drop-down list, select the preferred option. The available options are:

Option	Description
	• Low • Medium • High

Table 229. Administrator password

Option	Description
Administrator Password	Enter a new administrative password for Administrative Web Interface (AWI), and local OSD interface.

Upgrading firmware settings

Use the **Firmware Upgrade** page to upgrade the firmware settings.

Table 230. Upgrading firmware settings

Option	Description
Enable live upgrade	Select this option to enable the live upgrade process. This feature allows you to download and apply the firmware immediately after downloading. The system automatically restarts and the changes to **Enable live upgrade** are applied. If you disable this feature, the firmware is downloaded to the system but not installed. The system waits till next restart to apply the firmware.
Firmware to auto-deploy	The list of firmware files uploaded on the File Repository Inventory page is loaded. From the drop-down list select the firmware file to upgrade the thin client. The security level must be set to **High Security Environment**.

Configuring remote connection settings

Use the **Remote Connection** page to configure the remote connection settings.

Table 231. Remote Connection

Option	Description
Session Connection Type	From the drop-down list, select the connection type. The available connection types are: • View Connection Server • PCoIP Connection Server Based on the selected connection type, the configuration option changes.
Mode	From the drop-down list, select the session type. The available session types are: • Basic • Auto-Logon • Kiosk

Option	Description
	• Imprivata OneSign
Host Name or IP Address	Enter the DNS name or IP Address. This option is applicable when the connection type is **View Connection Server** and the session types are **Basic**, **Auto-Logon**, and **Kiosk**.
Server URI	Enter the Uniform Resource identifier (URI) for the **PCoIP Connection Manager**. The address must be in the following format: https://[hostname]|[IP Address] This option is applicable when the connection type is **PCoIP Connection Server**, and the session types are **Basic** or **Auto-Logon**.
Logon Username	Enter the username of the client. The username must be a maximum of 128 characters. This option is applicable when the connection types are **View Connection Server** or **PCoIP Connection Server**, and the session type is **Auto-Logon**.
Logon Password	Enter the password of the client. The password must be a maximum of 128 characters. This option is applicable when the connection types are **View Connection Server** or **PCoIP Connection Server**, and the session type is **Auto-Logon**.
Logon Domain Name	Enter the domain name of the thin client. The domain name must be a maximum of 256 characters. This option is applicable when the connection types are **View Connection Server** or **PCoIP Connection Server**, and the session type is **Auto-Logon**.
Username Type	From the drop-down list, select the type of username. The username must match the device name in the view connection server. This option is applicable when the connection type is **View Connection Server** and the session type is **Kiosk**.
Password	Enter the password to protect the kiosk virtual machine. The password must match the device password in the view connection server. This option is applicable when the connection type is **View Connection Server** and the session type is **Kiosk**.
Bootstrap URL	Enter the bootstrap URL which is used to find an initial OneSign server in a OneSign authentication deployment. This option is applicable when the connection type is **View Connection Server** and the session type is **Imprivata OneSign**.

Table 232. Advanced options

Option	Description
Use Secure Connection (SSL)	Select this option to use the SSL connection. This option is applicable when the connection type is **View Connection Server** and the session types are **Basic**, **Auto-Logon**, and **Kiosk**.
Always connect to this server at startup	Select this to option to automatically connect to the server. This option is applicable when the connection type is **View Connection Server** and the session types are **Basic**, **Auto-Logon**, and **Kiosk**.
Auto launch if only one desktop	Select this option and enter the credentials to connect to a provisioned desktop or application. This option is applicable when

Option	Description
	the connection type is **View Connection Server** and the session types are **Basic**, **Auto-Logon**, and **Kiosk**.
OneSign Pool Name Mode	From the drop-down list, select the preferred option. This option is applicable when the connection type is **View Connection Server** and the session type is **Imprivata OneSign**
Pool Name to Select	Enter the pool name. If the list includes the entered pool name, the client immediately starts a session with that pool. This option is applicable when the connection type is **View Connection Server** and the session type is **Imprivata OneSign**
OneSign Appliance Verification	From the drop-down list, select the type of verification performed on the certificate provided by the OneSign appliance server. This option is applicable when the connection type is **View Connection Server** and the session type is **Imprivata OneSign**
Direct To View Address	Enter the address to use when you are unable to reach the OneSign server. The address must be in the following format: **https://[hostname]|[IP Address]** This option is applicable when the connection type is **View Connection Server** and the session type is **Imprivata OneSign**
Certificate Check Mode	From the drop-down list, select the level of verification performed on the certificate provided by the connection server. This option is applicable when the connection type is **PCoIP Connection Server**.
Certificate Check Mode Lockout	Select this option if required. This option is applicable when the connection type is **PCoIP Connection Server**.
Enable Session Disconnect Hotkey	Select the check box to enable this feature. You can press the `Ctrl+Alt+F12` hotkey sequence to display the **Zero Client Control Panel** screen. You can disconnect the current session on the workstation or power off the workstation. This option is applicable when the connection type is **PCoIP Connection Server**.

Table 233. Available Broker Servers

Option	Description
Server Type	From the drop-down list, select the server type. The available connection types are: • View Connection Server • PCoIP Connection Server
Cache Mode	From the drop-down list, select the preferred option.
Broker Servers	Click **Add Server** option to add the broker connection.

Edit the Wyse Software Thin Client policy settings

To edit the Wyse Software Thin Client policy settings, do the following:

1 Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2 Click the **Edit Policies** drop-down menu.
3 Click **Wyse Software Thin Client**.
   The **Wyse Software Thin Client** page is displayed. The Wyse Software thin client policy settings include the following options:

- System Personalization
- Desktop Experience
- Network
- Security and Lockdown
- Other Settings
- Remote Connections Citrix
- Remote Connections VMware
- Remote Connections RDP
- Remote Connections Browser
- Device Info
- Wyse Easy Setup (2.0+)
- VNC Settings
- Domain Settings

4 After configuring the policy settings, click **Save and Publish**.

Configuring system personalization

Use this page to configure the thin client display settings, such as resolution, color depth, dual monitor, time zone, mouse, and audio options for Wyse software devices.

Table 234. Configuring display options

Option	Description
Enable Dual Monitor	Select this option to enable the dual monitor functionality.
Monitor Resolution (Primary)	Select this option to set the resolution of your monitor. From the drop-down menu, select the appropriate resolution.
Display Identifier (Primary)	Select this option to set a display identifier for your monitor. From the drop-down menu, select an appropriate monitor identification number.
Monitor Rotation (Primary)	Select this option to set an orientation for your monitor. From the drop-down menu, select one of the following options based on your preference: - Landscape - Portrait - Landscape—flipped - Portrait—flipped

Table 235. Configuring keyboard options

Option	Description
Language	Select this option to select one or more input languages for your keyboard. From the drop-down menu, select your preferred keyboard input language.
Keyboard Layout	Select this option to set an appropriate keyboard layout. From the drop-down menu, select your preferred keyboard layout.
Blink Rate	Select this option to set the speed at which the cursor (insertion point) blinks to make the cursor more visible, or less visible—

Option	Description
	depending on your requirement. From the drop-down menu, select your preferred cursor blink rate.
Keyboard Preferences	Select this option to set the keyboard hotkeys.
Keyboard Repeat Delay	Select this option to set the time that a key can be pressed without repeating the letter as input. From the drop-down menu, select one of the following options based on your preference: · Short · Medium Short · Medium Long · Long
Keyboard Repeat Rate	Select this option to set the repeat rate for your keyboard, which is the speed at which the key input repeats itself when you press and hold down the key on your keyboard.
Menu Access	Select this option to enable the menu access keys on your keyboard.
MS Gina Keyboard Layout	Select this option to view the **Keyboard Selection** screen on the Windows login screen. MS Gina Keyboard Layout feature allows to choose desired language and keyboard layout in the Windows devices on the login screen. For example, If the Windows credential is in Non-English and the keyboard attached to the Windows system is English. You cannot enter the credentials as there is no option to change or select the language and keyboard layout on the Windows login screen. You can configure the desired languages, substitute languages and keyboard layout along with **MS Gina Keyboard Layout** from the Wyse Management Suite server. When you apply the language or keyboard settings, MS Gina Keyboard layout is displayed on the Windows login screen. You can change or select desired language and keyboard layout from the Windows login screen. ⓘ NOTE: **The Windows login screen is displayed when the auto logon setting is disabled. To Apply MS Gina Keyboard Layout settings from the Wyse Management Suite server, you must disable and enable the Write Filter option. The Windows system restarts twice.**

Table 236. Configuring mouse settings

Option	Description
Mouse Speed	Select this option to specify the speed of the mouse pointer when moving the mouse device.
Left-handed Mouse	Select this option to swap the left and right-click mouse buttons.

Table 237. Configuring basic mouse options

Option	Description
Click Lock	Select this option to highlight or to drag the pointer without holding down the mouse button. To set the **Click Lock Time** Option, from the drop-down menu, select the appropriate time for the mouse button to be held down before the click is locked.
Double Click Speed	Select this option to set the time interval between two consecutive mouse clicks. From the drop-down menu, select your preferred option.

Table 238. Configuring mouse pointer option

Option	Description
Find Mouse Pointer	Select this option, if you want to find the mouse pointer when it is not in motion. ⓘ **NOTE:** You can press the `Ctrl` key on your keyboard to locate the mouse pointer when it is not in motion.
Hide Mouse Pointer	Select this option to hide the mouse pointer when it is stationary. ⓘ **NOTE:** To locate the mouse pointer when it is stationary, press the `Ctrl` key.
Pointer Trail Length	Select this option to define the length of the pointer trail when the mouse pointer is in motion.
Snap Mouse Pointer	Select this option to automatically move the mouse pointer to the default button in a dialog box.

Table 239. Mouse Vertical

Option	Description
Scroll Lines	Select this option to define the number of lines scrolled at a time using vertical scrolling on your mouse.

Table 240. Configuring Time Zone

Option	Description
Time Servers (NTP Servers)	Select this option to view the time servers to enable local time synchronization. Enter the NTP servers separated by a comma.

Table 241. Configuring Time zone options

Option	Description
Timezone Name	Select this option to set the time zone for your device. From the drop-down menu, select your preferred time zone.

Table 242. Configuring audio settings

Option	Description
Audio Mute	Select this option to mute the audio of your device.
Audio Volume	Select this option to adjust the audio volume of your device. From the drop-down menu, select your preferred volume option.
Microphone Mute	Select this option to mute your microphone.
Microphone Volume	Select this option to adjust the volume of your microphone. From the drop-down menu, select your preferred volume option.

Configuring desktop experience

Use this page to configure the thin client settings, such as desktop wallpaper, and desktop color for Wyse software devices.

Table 243. Configuring desktop experience

Option	Description
Desktop Wallpaper	Select this option to set a wallpaper for your desktop. After you enable the desktop wallpaper option, do the following: • From the **Wallpaper File** drop-down list, select a wallpaper for your desktop. (i) NOTE: Select a wallpaper only from the list of images uploaded to the file repository. • From the **Wallpaper Layout** drop-down list, select any of the following layouts for your desktop wallpaper: – Center – Tile – Stretch – Fill
Desktop Color	Select this option to define a background color for your local desktop.

Configuring network settings

Use this page to configure the network settings for the Wyse software devices.

Table 244. Configuring network settings

Option	Description
Radio State	Select this option to enable the wireless radio state. (i) NOTE: This option is similar to turning the device on or off.
Windows Wireless Profiles	Select this option to set a Windows wireless profile. From the drop-down menu, select your preferred Windows wireless profile.

Option	Description
	ⓘ **NOTE:** Select a profile only from the list of wireless profiles uploaded to the file repository.

Configuring security and lockdown settings

Use this page to configure the security and lockdown settings.

Table 245. Security and lockdown

Option	Description
Install Certificates	Select this option to view the certificates that are uploaded to the file repository.
Disable USB Storage Device Access	Select this option to enable or disable the USB mass storage device access for non-administrator users.
Disable Print Screen	Select this option to enable or disable the print screen functionality for non-administrator users.
Disable Task Manager	Select this option to enable or disable the task manager access for non-administrator users.

Configuring other settings

Use this page to configure the thin client settings, such as power, shared drive, and clock settings for Wyse software devices.

Table 246. Configuring appliance mode

Option	Description
Application Mode	Select this option to set an appropriate mode for the appliance. Appliance mode option starts the application in a Kiosk mode and with no access to the desktop or other applications. You can come out of the appliance mode using the configured keys. For example, Ctrl+Shift+A. From the drop-down menu, select any of the following options: · Off · Generic · VMware View · Citrix · Internet Explorer · RDP
Exit From Appliance Mode	Select this option to exit from the appliance mode by using a shortcut key.

Table 247. Power settings

Option	Description
Device Power Plan	Select this option to select a power plan for your device. From the drop-down menu, select either of the following options:

Option	Description
	· Balanced · Power Saver

Table 248. Power settings on battery

Option	Description
Device Sleep Plan (on battery)	Select this option to set the time after which your device goes to sleep mode. From the drop-down menu, select a delay time.
Dim Display (on battery)	Select this option to set the time after which the display is dimmed. From the drop-down menu, select a delay time.
Turn Off Display (on battery)	Select this option to set the time after which the display is turned off. From the drop-down list, select a delay time.

Table 249. Power settings when plugged-in

Option	Description
Device Sleep Plan (plugged-in)	Select this option to set the time after which your device goes to sleep mode. From the drop-down menu, select a delay time.
Dim Display (plugged-in)	Select this option to set the time after which the display is dimmed. From the drop-down menu, select a delay time.
Turn Off Display (plugged-in)	Select this option to set the time after which the display is turned off. From the drop-down menu, select a delay time.

Table 250. Configuring shared drives

Option	Description
Shared Drive	Select this option to add a shared drive to your device. Click **Add Shared Drive**. Enter the share name, remote drive path, user name, and password for the shared drive. ⓘ **NOTE: To delete a shared drive from the list, select the shared drive that you want to remove and click Remove.**

Table 251. Clock settings

Option	Description
Clock1	Select this option to configure Clock 1 on your device. After you enable Clock1, set the **Display Name** for the clock. From the drop-down menu, select the **Time Zone** for Clock 1.
Clock2	Select this option to configure Clock 2 on your device. After you enable Clock 2, set the **Display Name** for the clock. From the drop-down menu, select the **Time Zone** for Clock 2.

Configuring remote connection settings—Citrix

Use this page to configure the Citrix remote connection which can be accessed on the Wyse software thin client.

Table 252. Configuring basic options

Option	Description
Connection Name	Select this option to set a name for connection identification.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start the session after you log in.
Connection Type	Select this option to set a connection type. From the drop-down menu, select any of the following options: • Citrix XenApp • Citrix XenDesktop • Citrix Gateway • Citrix StoreFront
Citrix Server FQDN or IP address	Select this option to list the Citrix servers. Enter the list of ICA browsers separated by commas for the connection.
Published Applications	Select this option to specify a published application that you want to start.
Single Sign On	Select this option to enable the single sign on feature for the connection. If you enable single sign on, use your Windows login credentials to connect to the Citrix server.
Username	Select this option to define a user name for the Citrix connection, if single sign on is disabled.
Password	Select this option to define a password for the Citrix connection, if single sign on is disabled.
Domain Name	Select this option to define a domain name for the Citrix connection.
Window Size	Select this option to specify the window size for the Citrix connection. From the drop-down menu, select a window size.
Screen Color Depth	Select this option to define the screen color depth for the Citrix connection. From the drop-down menu, select any of the following options: • Default • Better Speed 16–Bit • Better Appearance 32–Bit
Auto Reconnect	Select this option to automatically restore the connection, if the connection is dropped.
Audio Quality	Select this option to select the audio quality for the Citrix connection. From the drop-down menu, select any of the following options: • Default User Audio Setting • High Definition • Optimized for Speech • Low Bandwidth

Option	Description
	• Off
User Key Combos Passthrough	Select this option to specify a window to apply the Windows user key combinations. • Default User Key Combos Passthrough • On the local desktop • On the remote desktop • In full screen desktops only

Table 253. Configuring application display settings

Option	Description
Desktop Display	Select this option to view the Citrix connection on your desktop. After you enable this option, specify the **Desktop Folder Name** for the connection.
Start Menu Display	Select this option to enable the start menu display on the connection desktop. After you enable this option, specify the **Start Menu Display Folder** for the connection.
System Tray Display	Select this option to display the Citrix connection icon in the notification area.

Table 254. Configuring server options

Option	Description
Logon Method	Select this option to choose a logon method for your Citrix connection. • Default Logon Method • Prompt Logon Method

Table 255. Configuring advanced settings

Option	Description
Disable Full Screen Pop-up	Select this option to disable the full screen pop-up warning.
Logon—Connect to Active and Disconnected Sessions	Select this option to connect to the active and disconnected sessions after you log in.
Menu—Connect to Active and Disconnected Sessions	Select this option to connect to active and disconnected sessions.
Reconnect from Menu	Select this option to reconnect to the existing sessions from the client menu.

Table 256. Configuring flash redirection

Option	Description
Use Flash Remoting	Select this option to render the flash content on the client device instead of the remote server.
Enable Server-Side Content Fetching	Select this option to download the content to the server and send it to the user device.
Use Server HTTP Cookies	Select this option to synchronize the client-side HTTP cookies with the server-side.
URL Rewriting Rules for Client-Side Content Fetching	Select this option to add rules that redirect the user devices to other servers for client-side fetching. Click **Add Item**, and enter the content rule name and content rule value. ⓘ **NOTE: To delete an item from the list, select the item you want to remove, and click Remove.**

Configuring remote connection settings—VMware

Use this page to configure the VMware remote connection which can be accessed on the Wyse software thin client.

Table 257. Configuring remote connection settings—VMware

Option	Description
Connection Name	Select this option to define the name to identify the connection.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start after you log in.
VMware Server Address	Select this option to enter the server address of the VMware connection.
Protocol	Select this option to choose the protocol for the VMware connection. From the drop-down menu, select either of the following options: · PCOIP · RDP · Blast
Login as Current User	Select this option to enable the single sign-on feature for the connection. If you enable the **login as current user** option, use your Windows login credentials to connect to the VMware server.
Username	Select this option to define a user name for the VMware connection, if single sign-on is disabled.
Password	Select this option to define a password for the VMware connection, if single sign-on is disabled.
Domain Name	Select this option to define a domain name for the VMware connection.
Security Mode	Select this option to specify the client connectivity if it cannot verify a secure connection to the server.
Fullscreen Mode	Select this option to set the VMware connection window in full screen mode.

Option	Description
	If you do not select the full screen mode, from the drop-down menu, select the **Window Size**.
Display Fullscreen Drop Down Menu Bar	Select this option to display the **Fullscreen** drop-down menu for your connection.
Automatically Launch This Desktop	Select this option to specify a published desktop to start upon a successful connection.
Auto Reconnect	Select this option to automatically reconnect, if the connection drops.
Broker	Select this option to define the host name or IP address of the **View Connection** broker.
Broker History	Select this option to specify the previously used host name or IP address of the **View Connection** broker.

Configuring remote connection settings—RDP

Use this page to configure the RDP remote connections which can be accessed on the Wyse software thin client.

Table 258. Configuring basic settings

Option	Description
Connection Name	Select this option to define the name to identify the connection.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start after you log in.
Server Address	Select this option to enter the server address of the connection.
Single Sign On	Select this option to enable the single sign-on feature for the connection. If you enable the **login as current user** option, use your Windows login credentials to connect to the server.
Username	Select this option to define a user name for the connection, if single sign-on is disabled.
Password	Select this option to define a password for the connection, if single sign-on is disabled.
Domain Name	Select this option to define a domain name for the connection.
Auto Reconnect	Select this option to enable the connection to automatically reconnect, if the connection is dropped.

Table 259. Configuring RD gateway settings

Option	Description
Use RD Gateway settings	Select this option to configure the settings for RD gateway. After you enable the option, enter the **RD Server** name for the gateway. Specify the credentials to validate the connection with the RD Gateway. From the **RD Gateway Logon Method** drop-down menu, select any one of the following: • Ask for password NTLM • Smartcard

Option	Description
	• Allow me to choose later From the **RD Gateway Usage Method** drop-down menu, select any of the following ways to use a remote desktop server: • Do not use RD Gateway server—All IP addresses • Use RD Gateway server settings • Use RD Gateway server settings for Non-Local IP addresses only • Use default settings • Local IP addresses only
Remote Desktop Gateway KDC Proxy	Select this option to configure the settings for KDC proxy. After you enable the option, enter the **KDC Proxy Name** name for the sever.

Table 260. Configuring display settings

Option	Description
Fullscreen	Select this option to set the connection window in the full screen mode. After the full screen mode is enabled, from the drop-down menu, select the window size.
Display Connection Bar	Select this option to display the connection bar in the full screen mode.
MultiMonitor Support	Select this option to enable the multi-monitor support.
Screen Color Depth (in bits)	Select this option to define the screen color depth of the connection. • RDP 15–Bit High Color • RDP 16–Bit High Color • RDP 24–Bit True Color • RDP 32–Bit Highest Quality

Table 261. Configuring other Settings—Local and Parameter

Option	Description
Remote Audio Play Back	Select this option to manage the audio playback in the remote connection.
Enable Remote Audio Recording	Select this option to record the audio remotely.
Apply Windows Keys	Select this option to apply Windows keys. From the drop-down menu, select the preferred option.
Start the Following Program on connection	Select this option to start the selected program as soon as the system is connected. After you enable the option, enter the **Program Path and File Name** and provide the folder details in **Start in Following Folder** field.
Prompt Credentials	Select this option to enter the credentials.
Negotiate Security Layer	Select this option to use the most secure layer that is supported by the client.

Option	Description
Enable Compression	Select this option to automatically compress the files to reduce the size of the files and to reduce the amount of time to download the files.
Enable Video Playback	Select this option to redirect the audio of the remote computer in a remote session, and provides an improved experience for video playback.
Enable Workspace Reconnect	Select this option to reconnect with the workspace.

Table 262. Configuring local resources

Option	Description
Redirect Clipboard	Select this option to use the local clipboard of the device in the remote connection.
Redirect COM Ports	Select this option to use the local COM (serial) ports of the device in the remote connection.
Redirect DirectX	Select this option to redirect DirectX on the client computer and the option is available in the remote connection.
Redirect Drives	Select this option to use the local drives of the device in the remote connection.
Redirect POS Devices	Select this option to use the Point of Service devices, such as bar code scanners and magnetic readers of the device in the remote connection.
Forward All Printers	Select this option to use the local printer of the device in the remote connection.
Redirect Smart Card	Select this option to use the local smart cards of the device in the remote connection.

Table 263. Configuring other settings—Experience

Option	Description
Connection Speed To Optimize the Performance	Select this option to specify the connection speed to optimize the performance.
Desktop Background	Select this option to enable the desktop background for the connection.
Visual Styles	Select this option to enable the visual styles for the connection.
Font Smoothing	Select this option to enable font smoothing for the connection.
Persistent Bitmap Caching	Select this option to enable persistent bitmap caching for the connection.
Desktop Composition	Select this option to enable the desktop composition for the connection.
Disable Cursor Setting	Select this option to disable the cursor setting for the connection.
Show Window Contents While Dragging	Select this option to display the window contents while dragging the window.
Menu and Window Animation	Select this option to enable menu and window animation in the connection.
Use Redirect Server Name	Select this option to enable the usage of redirect server name.

Option	Description
If Server Authentication Fails	Select this option to specify the action that must be taken when the server authentication fails. • Connect and don't warn me • Do not connect • Warn me

Configuring remote connection settings—Browser

Use this page to configure the remote connection browser which can be accessed on the Wyse software thin client.

Table 264. Configuring basic settings

Option	Description
Connection Name	Select this option to define a name to identify the connection.
Auto Launch Connection On Logon	Select this option to enable the connection to automatically start after you log in.
URL	Select this option to specify the default URL for the browser.
Internet Zone Security Level	Select this option to set the security settings for Internet Explorer in the Internet zone.
Local Zone Security Level	Select this option to set the security settings for Internet Explorer in the local zone.
Trusted Zone Security Level	Select this option to set the security settings for Internet Explorer in the trusted sites.
Restricted Zone Security Level	Select this option to set the security settings for Internet Explorer in the restricted sites.

Table 265. Configuring Internet Explorer (IE) favorites and trusted site settings

Option	Description
IE Favorite	Select this option to add your favorite and trusted sites. Perform the following steps to add your favorite and trusted sites: • Click **Add Site**, and enter the folder name, URL, and description. • Click **Create Shortcut** to create a shortcut for the site. • Click **Remove** to delete a site from the list. ⓘ NOTE: The URL must begin with https:// when the **Trusted Sites** check box is selected.
Require Server Verification (https:) for all sites in the zone	Select this option to enable a server verification for all sites in the zone.

Table 266. Configuring Internet Explorer (IE) proxy settings

Option	Description
Enable Proxy	Select this option to configure proxy for the browser.

Table 267. Configuring Firewall settings

Option	Description
Domain Firewall	Select this option to enable the domain firewall.
Private Firewall	Select this option to enable the private firewall.
Public Firewall	Select this option to enable the public firewall.

Table 268. Configuring Aero (Valid for Windows Embedded Standard 7) settings

Option	Description
Aero	Select this option to enable the Aero feature for the browser. (i) **NOTE:** This feature is available only for Windows Embedded Standard 7

Configuring device information

Use the **Device Info** page to set the device details.

Table 269. Configuring device information

Option	Description
Location	Enter the device location.
Contact	Enter the device contact.
Custom 1 to 3	Enter the custom values.

Configuring Wyse Easy Setup version settings

Use the **Wyse Easy Setup (2.0)** page to configure the Wyse Easy Setup settings for the control panel and the user interface.

Table 270. Configure system

Option	Description
Region & Language	Select this check box to access the region and language option in the control panel.
Date & Time	Select this check box to access the date and time option in the control panel.
Display	Select this check box to access the display option in the control panel.

Option	Description
Network	Select this check box to access the network option in the local system control panel.
Ease of Access	Select this check box to access the ease of access option in the control panel.

Table 271. Configure peripherals

Option	Description
Mouse	Select this check box to access the mouse option in the control panel.
Keyboard	Select this check box to access the keyboard option in the control panel.

Table 272. Configure Kiosk mode

Option	Description
Kiosk Mode	Select this check box to replace the default Windows desktop with the Wyse easy setup desktop, Wyse easy setup remote connections, and Wyse easy setup applications.
Applications	Enter the details to register a new application.
Application Exit Action	From the application exit action drop-down list, select any one of the following options: • Shutdown upon Exit • Restart upon Exit • Logout upon Exit • Persistent upon Exit This setting is applicable when you have configured at least one of the remote connections.
Smart Card On Removal	From the smart card on removal drop-down list, select any one of the following options: • Restart upon removing the smart card • Logout upon removing the smart card • Shutdown upon removing the smart card • LockScreen upon removing the smart card

Table 273. Configure personalization

Option	Description
Background	From the drop-down list, select the preferred graphic image. Note: Before you perform this step, you must upload the graphic images to the file repository.
Logo	From the drop-down list, select the logo files which are uploaded in **Apps & Data** > **File Repository** > **Inventory**.

Table 274. Configure taskbar

Option	Description
Date & Time	Select this option to set the date and time option on the Wyse Easy Setup shell or custom desktop.
Sound	Select this option to set the sound parameters in the Wyse Easy Setup shell or custom desktop.
Network	Select this option to view the network option on the Wyse Easy Setup shell or custom desktop.
Touch Keyboard	Select this option to view the touch keyboard on the Wyse Easy Setup shell or custom desktop.

Table 275. Configure Start menu

Option	Description
Allow Shutdown	Select this option to shut down the system on the Wyse Easy Setup shell or custom desktop.
Allow Restart	Select this option to restart the system on the Wyse Easy Setup shell or custom desktop.
Allow Log off	Select this option to log off the system on the Wyse Easy Setup shell or custom desktop.

Configuring VNC settings

Use this page to configure the VNC settings.

Table 276. Configuring VNC settings

Option	Description
Enable VNC	Select this option to enable the VNC Server.
VNC User Prompt	If you select this option, you must accept or decline VNC shadowing.
VNC User Required Password	Select this option to set the VNC password.
VNC Primary Password	Select this option to change the VNC password. Enter the new password with a maximum of eight characters.
VNC View-only Password	Enter the primary password. You cannot edit the password.

Configuring domain settings

Read the instructions provided on the screen to add the Wyse Software Thin Client device to the corporate Active Directory domain.

Table 277. Configuring domain settings

Option	Description
Domain or Workgroup	Select this option to choose the domain. From the drop-down list, select the preferred option.
Domain or Workgroup Name	Enter the FQDN of the domain.
User Name	Enter the user name. The account should have **Add to domain** option.
Password	Enter the password.
Account OU	Enter the location of the organizational unit where the computer object should be created.
Auto Login	Select the check box to display the Windows login screen.

Managing devices

This section describes how to perform a routine device management task by using the management console. To locate the inventory of the devices, click the **Devices** tab. You can view a subset of the devices by using various filter criteria, such as groups or subgroups, device type, operating system type, status, subnet, platform, or time zone.

To view the **Device Details** page of a particular device, click the device entry listed on the page. All the configuration parameters of the device and the group level at which each parameter is applied are displayed on the **Device Details** page.

You can set the configuration parameter that is specific to the device. Parameters configured in this section override any parameters that were configured at the groups and/or at the global level.

Figure 5. Devices

Topics:

- Methods to register devices to Wyse Management Suite
- Searching a device using filters
- Saving the current filter
- Querying the device status
- Locking the devices
- Restarting the devices
- Unregistering the devices
- Resetting to factory default settings
- Changing a group assignment
- Sending messages to devices
- Activating the devices
- Viewing device details
- Managing device summary
- Viewing system information
- Viewing device events
- Viewing installed applications
- Rename the thin client
- Configuring remote shadow connection

- Tagging devices
- Device compliance status
- Pulling Windows Embedded Standard or ThinLinux image
- Requesting a log file
- Troubleshooting your device

Methods to register devices to Wyse Management Suite

You can register a thin client to the Wyse Management Suite by using any of the following methods:

- Register manually through the User Interface provided by the Wyse Device Agent (WDA) on the device.
- Register automatically by configuring the appropriate option tags on the DHCP server.
- Register automatically by configuring the appropriate DNS SRV records on the DNS server.

ⓘ **NOTE:**

- For a public cloud, register a thin client by providing the Wyse Management Suite URL, and the group token for the group to which you want to register the device.
- For a private cloud, register a thin client by providing the Wyse Management Suite URL, and the group token (Optional for the group to which you want to register this device. Devices are registered to the unmanaged group, if the group token is not provided.

Registering ThinOS devices by using Wyse Device Agent

To register the ThinOS devices manually, do the following:

1. From the desktop menu, go to **System Setup** > **Central Configuration**.
   The **Central Configuration** window is displayed.
2. Click the **WDA** tab. The WDA service automatically runs after the client boot up process is complete.
   WMS is selected by default.
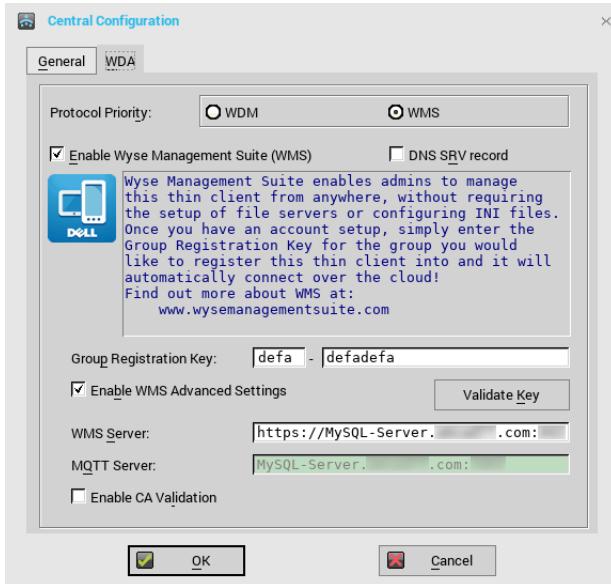
Figure 6. Central Configuration

3. Select the **Enable Wyse Management Suite** check box to enable Wyse Management Suite.

4   Enter the **Group Registration Key** as configured by your administrator for the desired group.

5   Select the **Enable WMS Advanced Settings** option, and enter the WMS server or MQTT server details.

6   Enable or disable CA validation based on your license type. For public cloud, select the **Enable CA Validation** check box, and for private cloud, select the **Enable CA Validation** check box if you have imported certificates from a well-known certificate authority into your Wyse Management Suite server.

> ⓘ **NOTE:**
>
> For the pro cloud version of Wyse Management Suite in USA, do not change the default WMS server and MQTT server details. For the pro cloud version of Wyse Management Suite in Europe, use the following:
> - CCM Server—eu1.wysemanagementsuite.com
> - MQTT Server—eu1-pns.wysemanagementsuite.com:1883

7   To verify the setup, click **Validate Key**. The device automatically restarts after the key is validated.

> ⓘ **NOTE: If the key is not validated, verify the credentials which you have provided. Ensure that ports 443 and 1883 are not blocked by the network.**

8   Click **OK**.

Device is registered on Wyse Management Suite console.

Registering Wyse Software Thin Client to Wyse Management Suite by using Wyse Device Agent

Prerequisites

Create a group to register a device to Wyse Management Suite.

Steps

1   Open the **Wyse Device Agent** application.

The **Wyse Device Agent** window is displayed.

2   Enter the device registration details.

3   From the **Management Server** drop-down list, select **Wyse Management Suite**.

4   Enter the server address and the port number in the respective fields.

5   Enter the group token. For a single tenant, the group token is an optional step.

6   Click **Register**.

After the registration is complete, the **Registered to Wyse Management Suite** message is displayed.

Registering Linux thin clients using Wyse Device Agent

> ⓘ **NOTE: Creating a group is a pre-requisite for registering the thin client to Wyse Management Suite. For information, see Add a group.**

1   Open the **Wyse Device Agent** (WDA) application.

The **Wyse Device Agent** window is displayed.

2   Enter the device registration details.

3   In the **Wyse Management Suite** tab, enter the Wyse Management Suite server address.

4   Enter the group token.

5   Click **Register**.

After the registration is complete, the **Registered to Wyse Management Suite** message is displayed.

Registering Wyse Embedded Standard Thin Clients to Wyse Management Suite by using Wyse Device Agent

Create a group in Wyse Management Suite to register a device.

1 Open the Wyse Device Agent application.

The Wyse Device Agent screen is displayed.

2 From the **Management Server** drop-down list, select **Wyse Management Suite**.

3 Enter the server address and the port number in the respective fields.

4 Enter the group token.

For a single tenant, the group token is an optional step.

5 Click **Register**.

Registering ThinLinux version 2.0 devices by using FTP INI method

Create a group to register in Wyse Management Suite.

1 Create a **wlx.ini** file. Enter the following parameter:

WMSEnable`=yes\no`

WMSServer`=https://FQDN of the WMS Server:Port <By default 443 is used>`

GroupRegistrationKey`=GroupToken present in WMS Server`

CAValidation`=True/False`

For example, to register the ThinLinux version 2.0 device to Wyse Management Suite (FQDN of the server is ServerFQDN.domain.com) having with the group token defa-defadefa, and with the CA Validation option enabled, enter the following INI parameter:

WMSEnable`=yes`

WMSServer`=https://ServerFQDN.domain.com:443`

GroupRegistrationKey`=defa-defadefa`

CAValidation`=True`

2 Place the wlx ini file in the wyse\wlx2 folder.

3 Go to **Settings** and switch to admin on the ThinLinux thin client.

4 Go to **Management > INI**.

5 Enter the FTP server URL.

6 Click **Save** and then restart the thin client.

7 Go to **Management > Wyse Device Agent**.

In the Wyse Device Agent tab, observe that the Wyse Management Server details are available in the respective field and the client entry can be seen in Wyse Management Server>Devices page.

Registering ThinLinux version 1.0 devices by using FTP INI method

Create a group to register in Wyse Management Suite.

1   Create a **wlx.ini** file. Enter the following parameter:
    WMSEnable=`yes\no`

    WMSServer=`https://FQDN of the WMS Server:Port <By default 443 is used>`

    GroupRegistrationKey=`GroupToken present in WMS Server`

    CAValidation=`True/False`

    For example, to register the ThinLinux version 1.0 device to Wyse Management Suite (FQDN of the server is ServerFQDN.domain.com) having with the group token defa-defadefa, and with the CA Validation option enabled, enter the following INI parameter:

    WMSEnable=`yes`

    WMSServer=`https://ServerFQDN.domain.com:443`

    GroupRegistrationKey=`defa-defadefa`

    CAValidation=`True`
2   Place the wlx ini file in the wyse\wlx folder.
3   Go to **Settings** and switch to admin on the ThinLinux thin client.
4   Go to **Management** > **INI**.
5   Enter the FTP server URL.
6   Click **Save** and then restart the thin client.
7   Go to **Management** > **Wyse Device Agent**.
    In the Wyse Device Agent tab, observe that the Wyse Management Server details are available in the respective field and the client entry can be seen in Wyse Management Server>Devices page.

Registering ThinOS devices by using the FTP INI method

Create a group to register in Wyse Management Suite.

1   Create a **wnos.ini** file. Enter the following parameter:
    CCMEnable=`yes/no` **CCMServer**=`FQDN of WMS Server` **GroupPrefix**=`The prefix of the Group Token` **GroupKey**=`The Group Key` **CAVAlidation**=`yes/no` **Discover**=`yes/no`

    For example, to register the ThinOS device to Wyse Management Suite (FQDN of the server is ServerFQDN.domain.com) having with the group token defa-defadefa, and with the CA Validation option enabled, enter the following INI parameter:

    CCMEnable=`yes` **CCMServer**=` is ServerFQDN.domain.com` **GroupPrefix**=`defa` **GroupKey**=`defadefa` **CAVAlidation**=`yes` **Discover**=`yes`
2   Place the `wnos.ini` file inside wnos folder of any FTP path.
3   Go to **Central Configuration** on the ThinOS device.
4   In the **General** tab, provide the FTP path in file servers or path till the parent folder.
5   Enter the FTP credentials if required. If FTP does not need credentials, username and password can be anonymous.

6   Click **OK**, and then restart the thin client.

7   Go to **Central Configuration** on the ThinOS device.

In the **Wyse Device Agent** tab, observe that the Wyse Management Server details are available in the respective field and the client entry can be seen in Wyse Management Server>Devices page.

Registering ThinLinux thin clients by using Wyse Device Agent

Create a group in Wyse Management Suite to register a device.

1   Open the Wyse Device Agent application.

The Wyse Device Agent screen is displayed.

2   Enter the device registration details.

3   In Wyse Management Suite, enter the Wyse Management Suite server details.

4   Enter the group token.

For a single tenant, the group token is an optional step.

5   Click **Register**. After the registration is complete, the confirmation message is displayed.

Registering devices by using DHCP option tags

You can register the devices by using the following DHCP option tags:

(i) **NOTE:**

For detailed instructions on how to add DHCP option tags on the Windows server, see Creating and configuring DHCP option tags.

Table 278. Registering device by using DHCP option tags

Option Tag	Description
Name—WMS **Data Type**—String **Code**—165 **Description**—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, **wmsserver.acme.com:443**, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. For links to register your devices in Wyse Management Suite in public cloud, see Getting started with Wyse Management Suite on public cloud.
Name—MQTT **Data Type**—String **Code**—166 **Description**—MQTT Server	This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, **wmsservername.domain.com: 1883**. To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example, US1:us1-pns.wysemanagementsuite.com EU1:eu1-pns.wysemanagementsuite.com
Name—CA Validation **Data Type**—String **Code**—167 **Description**—Certificate Authority Validation	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. By default, the CA validation is enabled in the public cloud. You can disable the CA validation in the public cloud as well. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.

Option Tag	Description
	Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.
Name—GroupToken **Data Type**—String **Code**—199 **Description**—Group Token	This tag is required to register the ThinOS devices with Wyse Management Suite on public or private cloud. This tag is optional to register the Windows Embedded Standard or ThinLinux devices with Wyse Management Suite on private cloud. If the tag is not available, then the devices are automatically registered to the unmanaged group during on-premise installation.

Registering devices by using DNS SRV record

DNS based device registration is supported with the following versions of Wyse Device Agent:

- Windows Embedded Systems—13.0 or later versions
- Thin Linux—2.0.24 or later versions
- ThinOS—8.4 firmware or later versions

You can register devices with the Wyse Management Suite server if DNS SRV record fields are set with valid values.

> (i) NOTE: For detailed instructions on how to add DNS SRV records on the Windows server, see Creating and configuring DNS SRV record.

The following table lists the valid values for the DNS SRV records:

Table 279. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name—_WMS_MGMT **Record FQDN**—_WMS_MGMT._tcp.<Domainname> **Record Type**— SRV	This record points to the Wyse Management Suite server URL. For example, **wmsserver.acme.com:443**, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. For links to register your devices in Wyse Management Suite in public cloud, see Getting started with Wyse Management Suite on public cloud. > (i) NOTE: Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite.
Record Name—_WMS_MQTT **Record FQDN**—_WMS_MQTT._tcp.<Domainname> **Record Type**—SRV	This record directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, **wmsservername.domain.com:1883**. > (i) NOTE: MQTT is optional for the latest version of Wyse Management Suite. To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example, US1—us1-pns.wysemanagementsuite.com EU1—eu1-pns.wysemanagementsuite.com
Record Name—_WMS_GROUPTOKEN	This record is required to register the ThinOS devices with Wyse Management Suite on public or private cloud.

URL/Tag	Description
Record FQDN—_WMS_GROUPTOKEN._tcp.<Domainname> **Record Type**— TEXT	This record is optional to register the Windows Embedded Standard or ThinLinux devices with Wyse Management Suite on private cloud. If the record is not available, then the devices are automatically registered to the unmanaged group during on-premise installation. ⓘ **NOTE: Group Token is optional for the latest version of Wyse Management Suite on private cloud.**
Record Name—_WMS_CAVALIDATION **Record FQDN**—_WMS_CAVALIDATION._tcp.<Domainname> **Record Type**—TEXT	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. By default, the CA validation is enabled in the public cloud. You can disable the CA validation in the public cloud as well. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. ⓘ **NOTE: CA Validation is optional for the latest version of Wyse Management Suite.**

Searching a device using filters

To search a device using filters, do the following:

1   From the **Configuration Groups** drop-down list, select either the default policy group or the groups which are added by an administrator.

2   From the **Status** drop-down list, select any one of the following options:

- **Registration**
  - Registered
  - Pre-registered
  - Not Registered
  - Compliant
  - Pending
  - Non-Compliant
- **Online Status**
  - Online
  - Offline
  - Unknown
- **Others**
  - Recently Added

3   From the **OS Type** drop-down list, select any one of the following operating systems:

- **Thin Client**
  - Linux
  - ThinLinux
  - ThinOS
  - WES
  - Teradici (Private cloud)
  - Wyse Software Thin Client

4   From the **OS Subtype** drop-down list, select a subtype for your operating system.

5   From the **Platform** drop-down list, select a platform.

6   From the **OS Version** drop-down list, select an OS version.

7   From the **Agent Version** drop-down list, select an agent version.

8   From the **Subnet** drop-down list, select a subnet.

9   From the **Timezone** drop-down list, select the time zone.

10   From the **Device Tag** drop-down list, select the device tag.

Saving the current filter

After selecting your required filter options, you can save the filters as a group. To save the current filter, do the following:

1   Enter the **Name** of the filter.

2   Provide a description for the filter in the **Description** box.

3   Select the check box to set the current filter as the default option.

4   Click **Save Filter**.

Querying the device status

To send a command to update the device information and status in the system, do the following:

1   Click **Devices**.

      The **Device** page is displayed.

2   Apply the filters to find the preferred device.

3   Select the check box of the device.

4   Click **Query**.

      An **Alert** window is displayed.

5   Click **Send Command** to send the query command.

Locking the devices

To lock the registered device, do the following:

1   Click **Devices**.

      The **Device** page is displayed.

2   Apply the filters to find the preferred device.

3   Select the check box of the device.

4   Click **Lock**.

      An **Alert** window is displayed.

5   Click **Send Command** to send the lock command.

Restarting the devices

To restart the registered device, do the following:

1   Click **Devices**.

      The **Device** page is displayed.

2   Apply the filters to find the preferred device.

3   Select the check box of the device.

4   Click **Restart**.

      An **Alert** window is displayed.

5   Click **Send Command** to send the restart command.

Unregistering the devices

To unregister the registered device, do the following:

1. Click **Devices**.

   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. Click **Unregister**.

   An **Alert** window is displayed.
5. Select the **Force Unregistration** check box.
6. Click **Send Command** to send the unregister command.

   ⓘ **NOTE:**
   - Force unregister option can be used to remove the device when there is no communication between the server and client. The device will be moved to unmanaged state and can be removed from the server entry.
   - Unregister and Force unregister actions can be performed by WES WDA UI also.

Resetting to factory default settings

To reset your ThinOS-based devices to factory default settings, do the following:

1. Click **Devices**.

   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Factory Reset**.

   An **Alert** window is displayed.
5. Enter the reason for the client reset.
6. Click **Send Command**.

Changing a group assignment

To change a group assignment, do the following:

1. Click **Devices**.

   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Change Group**.

   The **Change Group Assignment** window is displayed.
5. From the drop-down menu, select a new group for the device
6. Click **Save**.

Sending messages to devices

To send messages to devices, do the following:

1. Click **Devices**.

   The **Devices** page is displayed.
2. Apply the filters to find the preferred device.

3   Select the check box of the device.

4   From the **More Actions** drop-down menu, click **Send Message**.

The **Send Message** window is displayed.

5   Enter the message.

6   Click **Send**.

Activating the devices

If a device is turned off or in the sleep mode, and you want to activate the device, then do the following:

1   Click **Devices**.

The **Device** page is displayed.

2   Apply the filters to find the preferred device.

3   Select the check box of the device.

4   From the **More Actions** drop-down menu, click **Wake On LAN**.

An **Alert** window is displayed.

5   Click **Send Command**.

Viewing device details

To view the device details, do the following:

1   Click **Devices**.

The **Device** page is displayed.

2   Apply the filters to find the preferred device. For more information, see Searching a device using filters.

The preferred device list is displayed.

3   Click any one of the displayed devices.

The **Device Details** page is displayed.

Managing device summary

To view and manage information on the Notes, Group Assignment, Alerts, and Device Configuration, do the following:

1   Click **Devices**.

2   On the **Device Details** page, click **Summary** tab.

The device summary is displayed.

3   In the right pane, click **Add note**.

An **Add Note** window is displayed.

4   Type the message in the provided field and click **Save**.

5   In the right pane, click **Change Group Assignment**.

The **Change Group Assignment** window is displayed.

6   From the drop-down menu, select a new group for the device.

7   Click **Save**.

8   Click **Create/Edit exceptions** to create or edit a device level exception, and configure a particular device policy on the **Devices** page.

Viewing system information

To view the system information, do the following:

1   Click **Devices**.

The **Device** page is displayed.

2   Apply the filters to find the preferred device. For more information, see Searching a device by using filtersSearching a device using filters.

The preferred device list is displayed.

3   Click any one of the displayed devices.

The **Device Details** page is displayed.

4   Click **System Info**.

The system information is displayed.

Viewing device events

To view and manage information on the system events pertaining to a device, do the following:

1   Click **Devices**.

The **Device** page is displayed.

2   Apply the filters to find the preferred device. For more information, see Searching a device by using filtersSearching a device using filters.

The preferred device list is displayed.

3   Click any one of the displayed devices.

The **Device Details** page is displayed.

4   On the **Device Details** page, click **Events** tab.

The events on the device is displayed.

Viewing installed applications

To view the installed applications on the device, do the following:

1   Click **Devices**.

The **Device** page is displayed.

2   Apply the filters to find the preferred device. For more information, see Searching a device by using filters.

The preferred device list is displayed.

3   Click any one of the displayed devices.

The **Device Details** page is displayed.

4   Click **Installed Apps** tab.

The list of installed applications on the device is displayed.

This option is available for Windows Embedded Standard, Linux, and ThinLinux devices. The following are the attributes displayed on the page:

·   Name

·   Publisher

·   Version

·   Installed On

ⓘ **NOTE:**

The installed applications count increases or decreases based on the installation or uninstallation of the applications. The list is updated when the device checks-in or is queried next.

Rename the thin client

Use this page to change the host name of thin clients that run on Windows Embedded Standard, ThinLinux, and ThinOS operating systems. To change the host name, do the following:

1 On the **Devices** page, click the device.

2 From the **More options** drop-down list, select the **Change Host Name** option.

3 Enter the new host name when prompted.

   ⓘ **NOTE: Host name can only contain alphanumeric characters, and a hyphen.**

4 For Windows Embedded Standard devices, the **Reboot** drop-down list is included in the **Alert** window. To restart the system, select the **Reboot** option. If the **Reboot Later** option is selected, the device restarts at the configured time, and then the host name is updated.
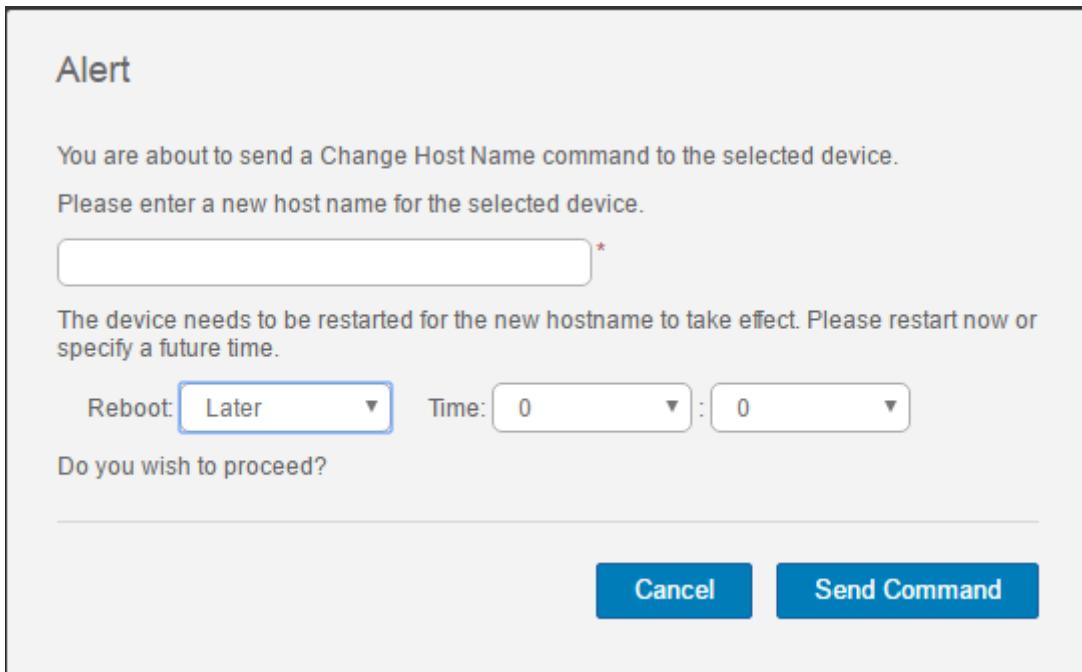
Figure 7. Alert

   ⓘ **NOTE: A ThinLinux device does not need to be restarted to update the host name.**

5 Click **Send Command**.

   A confirmation message is displayed.

Configuring remote shadow connection

Use this page to allow global and group administrators to access the Windows Embedded Standard, ThinLinux, and ThinOS thin client sessions remotely. This feature is applicable to only to private cloud and is available for both Standard and Pro licenses.

ⓘ **NOTE: Wyse Management Suite portal supports a maximum of five remote shadow sessions per tenant.**

1 On the **Devices** page, click the device.

2 From the **More options** drop-down list, select the **Remote Shadow (VNC)** option.
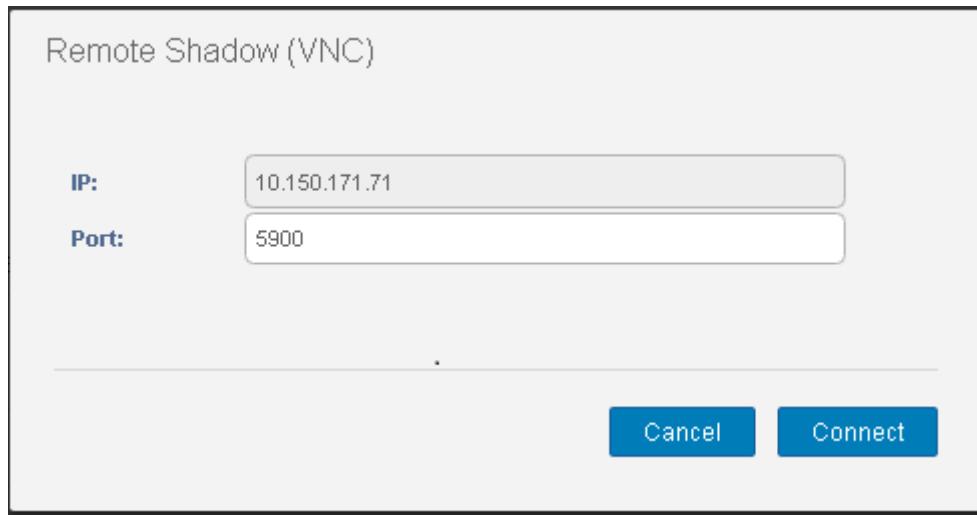
Figure 8. Remote Shadow(VNC)

The IP address and the port number of the target thin client is displayed in the **Remote Shadow (VNC)** dialog box.

ⓘ **NOTE: The default port number is 5900.**

3   Change the port number of the target thin client.(optional)

4   Click **Connect** to initiate a remote session to the target thin client.

Tagging devices

Wyse Management Suite enables you to identify a device or group of devices by using the **Tag Device** option.

1   Click **Devices**.

The **Device** page is displayed.

2   Apply the filters to locate the preferred device. For more information, see Searching a device by using filter.

The preferred device list is displayed.

3   Select one or more devices. From the **More Options** drop-down list, click **Tag Device**.

The **Set Device Tag** window is displayed.

4   Enter the preferred tag name.

5   Click **Set Tag**.

Device compliance status

By default, the following colors are displayed as the device status:

· Red—when the registered device has not been checked in for more than seven days.

· Gray—When you apply any configuration policy to the device.

· Green—When you apply all the configuration policies to the device.

The default value can be changed from 1 to 99 days.

The **Online Status** option is located next to the device name. The following colors are displayed in the online status:

· Red—When the device has not sent its heartbeat for more than three attempts .

· Gray—When the device has not sent its heartbeat for more than two attempts but less than three attempts.

· Green—When the device sends its heartbeat regularly.

Pulling Windows Embedded Standard or ThinLinux image

Use the Wyse Management Suite to pull an operating system or BIOS from a thin client. To perform the Windows Embedded Standard or ThinLinux image pull operation:

1   Go to the **Windows Embedded Standard** or **ThinLinux** device page.
2   Select **Pull OS Image** option, from the **More Actions** drop-down list.
3   Enter or select the following details:

  - **Name of Image**—Provide a name for the image. To replace the image with a similar name and the image files which are not completed successfully, click **Override name**.
  - **File repository**—From the drop-down list, select the file repository to where the image is uploaded. There are two types of file repository:
    – Local repository
    – Remote Wyse Management Suite repository
  - **Pull Type**—Select either **Default** or **Advanced** based on your pull type requirement.
    – When the **Default** pull type is selected, the following options are displayed:
      ◦ Compress
      ◦ OS
      ◦ BIOS
    – When the **Advanced** pull type is selected, a drop-down list for selecting the templates is displayed. Select any template which is available by default.

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

Figure 9. Pull OS image screen

4   Click **Prepare for Image Pull**.

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

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

  ⓘ NOTE: This option is applicable for Windows Embedded Standard devices.

- **Pull now**—The device boots to Merlin operating system and the image pull operation is performed.

ⓘ NOTE:

- Legacy on-premise gateway does not support the image pull operation. To use this feature, install the Wyse Management Suite repository.
- BIOS pull is not supported for Dell manufactured Windows Embedded Standard devices.
- To use CA Validation for imaging, follow the below steps:
  a   Ensure that the Wyse Device Agent and Merlin must be updated to the latest version on the device.
  b   Install the certificates to the thin clients where the OS image pull or push operation has to be performed.
  c   Enable the CA Validation from Wyse Management Suite server. For local repository, enable the CA Validation option from the setup page, and for Wyse Management Suite repository, enable the CA Validation option from the edit page.

  ⓘ NOTE: Do not install any certificates to the thin client, if you have already installed Well Known certificate to the Wyse Management Suite server and Wyse Management Suite repository.

Requesting a log file

To request a device log from Windows Embedded Standard, ThinOS and ThinLinux devices, do the following:

1 Go to the **Devices** page, and click a particular device.

   The device details are displayed.

2 Click the **Device Log** tab.

3 Click **Request Log File**.

4 After the log files are uploaded to the Wyse Management Suite server, click the **Click here** link, and download the logs.
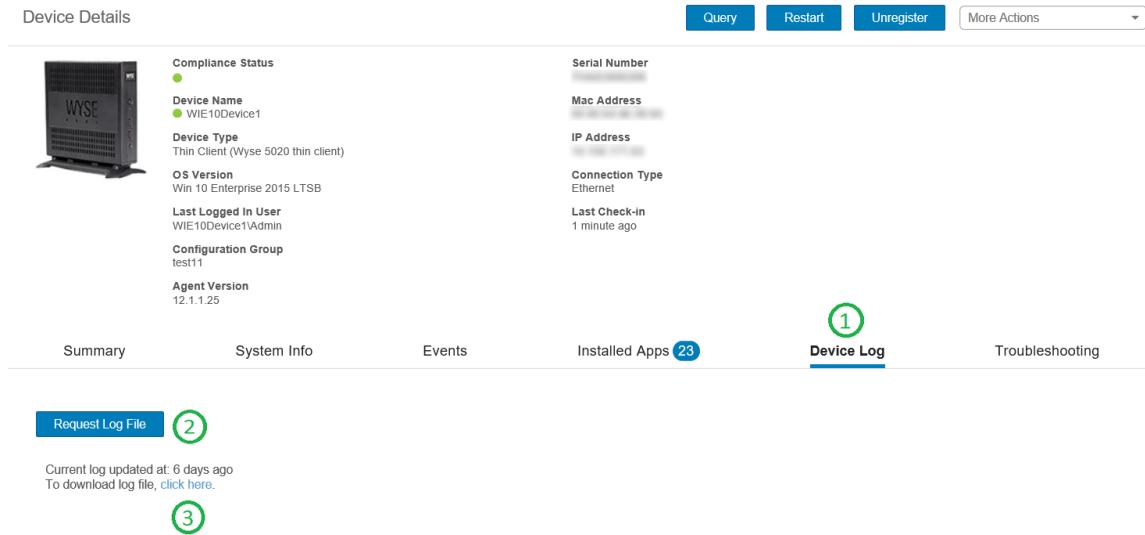
Figure 10. Log file pull

> ⓘ NOTE:
> - The device must be enabled to pull the log file.
> - The ThinOS device uploads the system logs.
> - The Windows Embedded Standard uploads Wyse Device Agent logs and Windows Event viewer logs.
> - Linux or ThinLinux uploads Wyse Device Agent logs and system logs.
> - Linux or ThinLinux uploads the log file in `.tar` format, if you are extracting the files on Windows system then you require 7zip or any other equivalent file.

Troubleshooting your device

To view and manage the troubleshooting information, do the following:

1 On the **Device Details** page, click **Troubleshooting** tab.

2 Click **Request Screen Shot**.

   You can capture the screen shot of the thin client with or without the client permission. If you select the **Require User Acceptance** check box then a message is displayed on the client. This option is applicable only for Windows Embedded Standard, Linux, and ThinLinux devices.

3 Click **Request Processes List**, to view the list of the processes running on the thin client.

4 Click **Request Services List**, to view the list of the services running on the thin client.

5 Click **Start Monitoring**, to access the performance metric console.

   On the **Performance metric** console, the following details are displayed:

   - Average CPU last minute.

- Average memory usage last minute.

Apps and data

This section describes how to perform routine device application tasks, operating system imaging, inventory management, and set policies by using the Wyse management console.

Figure 11. Apps and data

- Standard application policy—This policy allows you to install a single application package.
- Advanced application policy—This policy allows you to install multiple application packages.
- Image policy—This policy allows you to install the operating system.

Deployment of application policies and operating system images to the thin clients can be scheduled immediately or later, based on a specific time zone, or time zone that is configured on your device. For more information see Managing jobs.

Topics:

- Application policy
- Image policy
- Managing file repository

Application policy

Wyse Management Suite supports the following types of application inventories and application deployment policies:

- Configuring thin client application inventory
- Configuring Wyse Software thin client application inventory
- Creating and deploying standard application policy to thin clients
- Creating and deploying advanced application policy to thin clients
- Creating and deploying standard application policy to Wyse Software Thin Clients
- Creating and deploying advanced application policy to Wyse Software Thin Clients

Important notes for Windows based devices:

- Supports installation for windows based applications with extension .msi, .exe, .msu, .msp.

  Application with any other extension is downloaded to **%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA**

- For deploying .exe applications by using Wyse Management Suite, follow the silent installation method. You must enter the appropriate silent parameters if required. For example, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**
- Supports script deployments with file extensions .bat, .cmd, .ps1, .vbs.

  Script with any other extension is downloaded to **%sytemdrive%\wyse\WDA" Ex: "C:\wyse\WDA**.

- Any script which is pushed by using Wyse Management Suite should be non-interactive which means there is no user interaction required during the installation.
- In advanced application policy if there is a script/exe which returns value other than 0 then it is considered as a failure.
- In advanced application policy if pre-install fails then application installation is not continued.
- Any exe/scripts pushed by using standard application is reported as success with error code being updated in job status.
- For applications with extension msi/msu/msp standard error codes is reported. If application returns REBOOT_REQUIRED then device goes through one extra reboot.

Important notes for Linux devices:

- Supports installation for Linux based applications with extension .bin, .deb for ThinLinux 2.0 and .rpm for Thin Linux 1.0.
- Supports script deployments for ThinLinux devices with extensions .sh.
- In standard or advanced application policy if there is a script/deb/rpm which returns value other than 0 then it is considered as a failure.
- In advanced application policy if pre-install fails then app installation is not continued.

Configuring thin client application inventory

To configure the thin client inventory, do the following:

1. Click the **Apps and Data** tab.
2. In the left pane, go to **App Inventory** > **Thin Client**.
   Application details are displayed in the **Thin Client Inventory** window.
3. To add an application to the inventory, place the thin client application files in the **<repo-dir>\repository\thinClientApps** folder.
   Wyse Management Suite Repository sends metadata for all the files to the Wyse Management Suite server periodically.
4. To edit the application, do the following:
   a. Select the uploaded application from the list.
   b. Click **Edit App**.
      The **Edit Application** window is displayed.
   c. Enter the note.
   d. Click **Save**.

Configuring Wyse Software thin client application inventory

To configure the Wyse Software thin client inventory, do the following:

1 Click the **Apps and Data** tab.
2 In the left pane, go to **App Inventory** > **Wyse Software Thin Client**.
3 To add an application to the inventory, place the thin client application files in the **<repo-dir>\repository\softwareTcApps** folder.
   Wyse Management Suite Repository sends metadata for all the files to the Wyse Management Suite server periodically.

Creating and deploying standard application policy to thin clients

To deploy a standard application policy to thin clients, do the following:

1 In the local repository, go to **thinClientApps**, and copy the application to the folder.
2 Ensure that the application is registered by navigating to the **Apps & Data** tab and selecting **Thin Client** under **App Inventory**.

   ⓘ NOTE: **The App Inventory interface takes approximately two minutes to populate any recently added programs.**
3 Click **Apps & Data**.

   Apps & Data page is displayed.
4 In **App Policies**, click **Thin Client**.
5 Click **Add Policy**.

   Add Standard App Policy window is displayed.
6 Enter the **Policy Name**.
7 From the drop-down list, select the **Group**.
8 From the drop-down list, select the **Task**.
9 From the drop-down list, select the **OS Type**.
10 From the drop-down list, select the **Application**.
11 To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
12 Timeout displays a message on the client which gives you time to save your work before the installation begins. Specify the number of minutes the message dialog box should be displayed on the client.
13 To allow delay in implementation of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:
   • From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay the policy execution.
   • From the **Max delays** drop-down list, select the number of times (1–3) you can delay execution of the policy.
14 From the **Apply Policy Automatically** drop-down list, select any one of the following options:
   • Do not apply automatically— This options does not apply any policy automatically to the devices.
   • Apply the policy to new devices—This option automatically applies the policy to a registered device which belongs to a selected group or is moved to a selected group.
   • Apply the policy to devices on check in—This option is automatically applied to the device at check-in.

   ⓘ NOTE: **For Windows based devices, specify the silent installation parameters for .exe files to execute the application in the silent mode. For example, VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**
15 Click **Save** to create a policy.
   A message is displayed to allow the administrator to schedule this policy on devices based on group.
16 Select **Yes** to schedule a job on the same page.

17   The application policy job can run:

    a   **Immediately**—Server runs the job immediately.

    b   **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date/time of the device time zone.

    c   **On selected time zone**—Server creates one job to run at the date/time of the designated time zone.

18   To create the job, click **Preview** and schedules are displayed on the next page.

19   You can check the status of the job by navigating to the **Jobs** page.

Creating and deploying advanced application policy to thin clients

To deploy an advanced application policy to thin clients, do the following:

1   Copy the application and the pre/post install scripts (if necessary) to deploy to the thin clients. Save the application and the pre/post install scripts in the **thinClientApps** folder of the local repository or the Wyse Management Suite repository.

2   Go to **Apps&Data** > **AppInventory** and select **Thin Client** to verify if the application is registered.

3   Click **Thin Client** under **App Policies**.

4   Click **Add Advanced Policy**. The **Add Advanced App Policy** page is displayed.

5   To create an application policy, do the following:

    a   Enter the **Policy Name**.

    b   From the drop-down list, select the **Group**.

    c   Select the **Sub Groups** check box to apply the policy to sub groups.

    d   From the drop-down list, select the **Task**.

    e   From the drop-down list, select the **OS Type**.

    f   Click **Add app**, and select one or more applications under **Apps**. For each application, you can select a pre and post install script under **PreInstall**, **PostInstall**, and **Install Parameters**. If you want the system to reboot after the application is successfully installed, select **Reboot**. Click **Add app** and repeat the step to add multiple applications.

        ⓘ NOTE: **To stop the application policy at first failure, select Enable app dependency. If this option is not selected, failure of an application affects the policy implementation.**

    g   If you want to deploy this policy to specific operating system or platform, select **OS Subtype Filter** or **Platform Filter**.

    h   Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1–999 min)** box. Timeout displays a message on the client which gives you time to save your work before the installation begins.

    i   To allow delay in execution of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:

        •   From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay the policy execution.

        •   From the **Max delays** drop-down list, select the number of times (1–3) you can delay execution of the policy.

    j   From the **Apply Policy Automatically** drop-down list, select any one of the following options:

        •   Do not apply automatically— This options does not apply any policy automatically to the devices.

        •   Apply the policy to new devices—This option automatically applies the policy to a registered device which belongs to a selected group or is moved to a selected group.

        •   Apply the policy to devices on check in—This option is automatically applied to the device at check-in.

        ⓘ NOTE: **For Windows based devices, specify the silent installation parameters for .exe files to execute the application in the silent mode. For example, VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

    k   Select the **Skip write filter check** check box to skip the write filter cycles. This option is applicable for Windows Embedded Standard operating system devices and Wyse Software thin client devices.

6   Click **Save**. A message is displayed to allow administrators to schedule this policy on devices based on the group. Select **Yes** to schedule the application policy for devices immediately or at a scheduled date and time on the **App Policy Job** page.

The application policy job can run:

    a   **Immediately**—Server runs the job immediately.

    b   **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date/time of the device time zone.

    c   **On selected time zone**—Server creates a job that must be scheduled at the date and time of the designated time zone.

7   Click **Preview** and schedule on the next page to create the job.

8   You can check the status of the job by navigating to the **Jobs** page.

Creating and deploying standard application policy to Wyse Software Thin Clients

To deploy a standard application policy to Wyse Software Thin Clients, do the following:

1   In the local repository, go to **softwareTcApps**, and copy the application to the folder.

2   Ensure that the application is registered by navigating to the **Apps & Data** tab and selecting **Wyse Software thin client** under **App Inventory**.

    ⓘ **NOTE: The App Inventory interface takes approximately two minutes to populate any recently added programs.**

3   Click **Apps & Data**.

    Apps & Data page is displayed.

4   In **App Policies**, click **Wyse Software Thin Client**.

5   Click **Add Policy**.

    Add Standard App Policy window is displayed.

6   Enter the **Policy Name**.

7   From the drop-down list, select the **Group**.

8   From the drop-down list, select the **Task**.

9   From the drop-down list, select the **OS Type**.

10   From the drop-down list, select the **Application**.

11   To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.

12   Timeout displays a message on the client which gives you time to save your work before the installation begins. Specify the number of minutes the message dialog box should be displayed on the client.

13   To allow delay in execution of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:

    ·   From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay the policy execution.

    ·   From the **Max delays** drop-down list, select the number of times (1–3) you can delay execution of the policy.

14   From the **Apply Policy Automatically** drop-down list, select any one of the following options:

    ·   Do not apply automatically— This options does not apply any policy automatically to the devices.

    ·   Apply the policy to new devices—This option automatically applies the policy to a registered device which belongs to a selected group or is moved to a selected group.

    ·   Apply the policy to devices on check in—This option is automatically applied to the device at check-in.

    ⓘ **NOTE: For Windows based devices, specify the silent installation parameters for .exe files to execute the application in the silent mode. For example, VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

15   Click **Save** to create a policy.

    A message is displayed to allow the administrator to schedule this policy on devices based on group.

16   Select **Yes** to schedule a job on the same page.

17   The application policy job can run:

a **Immediately**—Server runs the job immediately.

b **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date/time of the device time zone.

c **On selected time zone**—Server creates one job to run at the date/time of the designated time zone.

18 To create the job, click **Preview** and schedules are displayed on the next page.

19 You can check the status of the job by navigating to the **Jobs** page.

Creating and deploying advanced application policy to Wyse Software Thin Clients

To deploy an advanced application policy to Wyse Software Thin Clients, do the following:

1 In the local repository, go to **softwareTcApps**, and copy the application to the folder.

2 Ensure that the application is registered by navigating to the **Apps & Data** tab and selecting **Wyse Software thin client** under **App Inventory**.

> ⓘ NOTE: The App Inventory interface takes approximately two minutes to populate any recently added programs.

3 Click **Apps & Data**.

   Apps & Data page is displayed.

4 Click **Wyse Software Thin Clients** under **App Policies**.

5 Click **Add Advanced Policy**. The **Add Advanced App Policy** page is displayed.

6 To create an application policy, do the following:

a Enter the **Policy Name**.

b From the drop-down list, select the **Group**.

c Select the **Sub Groups** check box to apply the policy to sub groups.

d From the drop-down list, select the **Task**.

e From the drop-down list, select the **OS Type**.

f Click **Add app**, and select one or more applications under **Apps**. For each application, you can select a pre and post install script under **PreInstall**, **PostInstall**, and **Install Parameters**. If you want the system to reboot after the application is successfully installed, select **Reboot**. Click **Add app** and repeat the step to add multiple applications.

> ⓘ NOTE: To stop the application policy at first failure, select Enable app dependency. If this option is not selected, failure of an application affects the policy implementation.

g If you want to deploy this policy to specific operating system or platform, select **OS Subtype Filter** or **Platform Filter**.

h Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1–999 min)** box. Timeout displays a message on the client which gives you time to save your work before the installation begins.

i To allow delay in execution of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:

- From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay the policy execution.
- From the **Max delays** drop-down list, select the number of times (1–3) you can delay execution of the policy.

j From the **Apply Policy Automatically** drop-down list, select any one of the following options:

- Do not apply automatically— This options does not apply any policy automatically to the devices.
- Apply the policy to new devices—This option automatically applies the policy to a registered device which belongs to a selected group or is moved to a selected group.
- Apply the policy to devices on check in—This option is automatically applied to the device at check-in.

> ⓘ NOTE: For Windows based devices, specify the silent installation parameters for .exe files to execute the application in the silent mode. For example, VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart

k   Select the **Skip write filter check** check box to skip the write filter cycles. This option is applicable for Windows Embedded Standard operating system devices.

7   Click **Save**. A message is displayed to allow administrators to schedule this policy on devices based on the group. Select **Yes** to schedule the application policy for devices immediately or at a scheduled date and time on the **App Policy Job** page.

The application policy job can run:

a   **Immediately**—Server runs the job immediately.

b   **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date/time of the device time zone.

c   **On selected time zone**—Server creates a job that must be scheduled at the date and time of the designated time zone.

8   Click **Preview** and schedule on the next page to create the job.

9   You can check the status of the job by navigating to the **Jobs** page.

Image policy

Wyse Management Suite supports the following types of operating system image deployment policies:

- Adding Windows Embedded Standard operating system and ThinLinux images to the repository
- Adding ThinOS firmware to the repository
- Adding Terdici firmware to the repository
- Creating Windows Embedded Standard and ThinLinux image policies.

Adding Windows Embedded Standard operating system and ThinLinux images to repository

Prerequisites

- If you are using Wyse Management Suite with cloud deployment, go to **Portal Administration** > **Console Settings** > **File Repository**. Click **Download version 1.3** to download the WMS_Repo.exe file and install the Wyse Management Suite repository installer. For more information, see Accessing file repository.
- If you are using Wyse Management Suite with on-premise deployment, the local repository is installed during Wyse Management Suite installation process.

To add an image to the repository folder on your system, do the following:

1   Copy the Windows Embedded Standard operating system images or ThinLinux images to the **<Repository Location>\repository \osImages\zipped** folder.

Wyse Management Suite extracts the files from the zipped folder and uploads the files in the **<Repository Location>\repository \osImages\valid** location. The image extraction may take several minutes depending upon the image size.

> (i) **NOTE: For ThinLinux operating system, download the merlin image, for example, 1.0.7_3030LT_merlin.exe, and copy in the <Repository Location>\Repository\osImages\zipped folder.**

The image is added to the repository.

2   Go to **Apps and data** > **OS image repository** > **WES/ThinLinux** to view the registered image.

Adding ThinOS firmware to repository

To add a operating system image to the ThinOS firmware repository, do the following:

1   In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS**.

2   Click **Add File**.

The **Add File** screen is displayed.

3   To select a file, click **Browse** and navigate to the location where your file is located.

4   Enter the description for your file.

5   Select the check box if you want to override an existing file.

6   Click **Upload**.

> ⓘ **NOTE:** The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy a firmware to a device or a group of devices, go to the respective device or group configuration page.

Adding Teradici firmware to repository

To add a operating system image to the Teradici firmware repository, do the following:

1   In the **Apps & Data** tab, under **OS Image Repository**, click **Teradici**.

2   Click **Add Firmware File**.

    The **Add File** screen is displayed.

3   To select a file, click **Browse** and navigate to the location where your file is located.

4   Enter the description for your file.

5   Select the check box if you want to override an existing file.

6   Click **Upload**.

> ⓘ **NOTE:** The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy a firmware to a device or a group of devices, go to the respective device or group configuration page.

Creating Windows Embedded Standard and ThinLinux image policies

To configure the Windows Embedded Standard image or ThinLinux image policies, do the following:

1   In the **Apps & Data** tab, under **OS Image policies**, click **WES / ThinLinux**.

2   Click **Add Policy**.

    The **Add WES/ ThinLinux Policy** screen is displayed.

3   In the **Add WES/ ThinLinux Policy** page, do the following:

    a   Enter a **Policy Name**.

    b   From the **Group** drop-down menu, select a group.

    c   From the **OS Type** drop-down menu, select an OS type.

    d   From the **OS Subtype Filter** drop-down menu, select an OS subtype filter.

    e   If you want to deploy an image to a specific operating system or platform, select either **OS Subtype Filter** or **Platform Filter**.

    f   From the **OS Image** drop-down menu, select an image file.

    g   From the **Rule** drop-down menu, select any one of the following rules that you want to set for the image policy:

    - Upgrade only
    - Allow downgrade
    - Force this version.

    h   From the **Apply Policy Automatically** drop-down menu, select one of the following option:

    - Do not apply automatically—The image policy is not applied automatically to a device registered with Wyse Management Suite.
    - Apply the policy to new devices—The image policy is applied to a new device registered with Wyse Management Suite.
    - Apply the policy to devices on check in—The image policy is applied to a new device on check in which is registered with Wyse Management Suite.

4   Click **Save**.

Managing file repository

This section allows you to view and manage the file repository inventories, such as wallpaper, logo, EULA text file, Windows wireless profile, and certificate files.

To add a new file, do the following:

1   In the **Apps & Data** tab, under **File Repository**, click **Inventory**.
2   Click **Add File**.
    The **Add File** screen is displayed.
3   To select a file, click **Browse** and navigate to the location where your file is located.
4   From the **Type** drop-down menu, select any one of the following options that suits your file type:
    - Certificate
    - Wallpaper
    - Logo
    - EULA text file
    - Windows Wireless Profile
    - INI File
    - Locale
    - Printer Mappings
    - Font

    ⓘ NOTE: **To view the maximum size and the supported format of the files that you can upload, click the information (i) icon.**
5   Select the check box if you want to override an existing file.

    ⓘ NOTE: **The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To assign the file, go to the respective device configuration page.**
6   Click **Upload**.

How to change wallpaper for all devices belonging to marketing group

To add a wallpaper to Wyse Management Suite repository, do the following:

1   Navigate to the **Apps & Data** tab.
2   In the navigation bar on the left pane, select **Inventory**.
3   Click the **Add File** button.
4   Browse and point to the image that you want to use as a wallpaper.
5   For type, select **Wallpaper**.
6   Enter the description and click **Upload**.

To change the configuration policy of a group by assigning a new wallpaper, do the following:

1   Select a policy group.
2   Click **Edit Policies**, and select **WES**.
3   Select **Desktop Experience** and click **Configure this item**.
4   Select **Desktop Wallpaper**.
5   From the drop-down list, select the wallpaper file.

6   Click **Save and Publish**.

Click **Jobs** to check the status of configuration policy. You can click the number next to the status flag in the **Details** column to check devices with their status.

7

Managing rules

This section describes how to add and manage the rules in the Wyse Management Suite console. The following filtering options are provided:

- **Registration**
- **Unmanaged Device Auto Assignment**
- **Alert Notification**

Topics:

Editing a registration rule

Configure the rules for unmanaged devices by using the **Registration** option.
To edit a registration rule, do the following:

1   Click **Rules**.

The **Rules** page is displayed.

2   Click **Registration** and select the unmanaged devices option.

3   Click **Edit Rule**.

The **Edit Rule** window is displayed.

You can view the following details:

- Rule
- Description
- Device Target
- Group

4   From the drop-down menu, select a target client to apply the **Notification Target** option and the time duration to apply the **Notification Frequency** option.

ⓘ NOTE: **The notification frequency can be configured for every 4 hours, every 12 hours, daily, or weekly basis to the target device.**

5   Enter the number of days until you want to apply the rule in the **Apply rule after (1–30 days)** box.

ⓘ NOTE: **By default, registration of an unmanaged devices are unregistered after 30 days.**

6   Click **Save**.

Creating unmanaged device auto assignment rules

To create rules for the unmanaged device auto assignment, do the following:

(i) **NOTE:** Make sure that you have installed the pro license version of Wyse Management Suite.

1 Click the **Rules** tab.
2 Select the **Unmanaged Device Auto Assignment** option.
3 Click the **Add Rules** tab.
4 Enter the **Name** and select the **Destination group**.
5 Click the **Add Condition** option and select the conditions for assigned rules.
6 Click **Save**.

The rule is displayed in the unmanaged group list. This rule is applied automatically and the device is listed in the destination group.

Editing unmanaged device auto assignment rule

To edit rules for the unmanaged device auto assignment, do the following:

1 Click the **Rules** tab.
2 Select the **Unmanaged Device Auto Assignment** option.
3 Select the rule and click the **Edit** option.
4 Enter the **Name** and select the **Destination group**.
5 Click the **Add Condition** option and select the conditions for assigned rules.
6 Click **Save**.

Disabling and deleting rule

To disable and delete the disabled rules for the unmanaged device auto assignment, do the following:

1 Click the **Rules** tab.
2 Select the **Unmanaged Device Auto Assignment** option.
3 Select a rule and click the **Disable Rule** option.
   The selected rule is disabled.
4 Select the disabled rule and click the **Delete Disabled Rule(s)** option.
   The rule is deleted.

Saving the rule order

If multiple rules are present, then you can change the order of a rule to be applied on the devices.
To change the order of a rule, do the following:

1 Click the **Rules** tab.
2 Select the **Unmanaged Device Auto Assignment** option.
3 Select the rule which you want to move and then move it to the top order.
4 Click **Save Rule Order**.

Adding a rule for alert notification

To add a rule for alert notification, do the following:

1 Click the **Rules** tab.
2 Select the **Alert Notification** option.
3 Click **Add Rule**.
   An **Add Rule** window is displayed.
4 From the **Rule** drop-down list, select a rule.
5 Enter the **Description**.
6 From the **Group** drop-down list, select the preferred option.

7   From the drop-down menu, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.

8   Click **Save**.

Editing an alert notification rule

To edit a rule for alert notification, do the following:

1   Click the **Rules** tab.

2   Select the **Alert Notification** option.

3   Click **Edit Rule**.

     An **Edit Rule** window is displayed.

4   From the **Rule** drop-down list, select a rule.

5   Enter the **Description**.

6   From the **Groups** drop-down list, select a group.

7   From the drop-down list, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.

8   Click **Save**.

Managing Jobs

This section describes how to schedule and manage jobs in the management console.

Figure 12. Jobs

In this page you can see jobs based on the following filtering options:

- **Configuration Groups**—From the drop-down menu, select the configuration group type.
- **Scheduled by**—From the drop-down menu, select a scheduler who performs the scheduling activity. The available options are:
  - Admin
    - App Policy
    - Image Policy
    - Device Commands
  - System
    - Publish Group Configuration
    - Others
- **OS Type**—From the drop-down menu, select the operating system. The available options are:
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
- **Status**—From the drop-down menu, select the status of the job. The available options are:
  - Scheduled
  - Running/In Progress
  - Completed
  - Cancelled

- – Failed
- **Detail Status**—From the drop-down menu, select the status in detail. The available options are:
  - – 1 or more failed
  - – 1 or more pending
  - – 1 or more In progress
  - – 1 or more cancelled
  - – 1 or more completed
- **More Actions**—From the drop-down menu, select the **Sync BIOS Admin Password** option. The Sync BIOS Admin Password Job window is displayed

Topics:

Sync BIOS admin password

From the **More Actions** drop-down menu, select the **Sync BIOS admin password** option. To synchronize the BIOS admin password, do the following:

1. Enter the password. The password must be a minimum of 4 and a maximum of 32 characters.
2. Select the **Show Password** check box to view the password.
3. From the **OS Type** drop-down menu, select your preferred option.
4. From the **Platform** drop-down menu, select your preferred option.
5. Enter the name of the job.
6. From the **Group** drop-down menu, select your preferred option.
7. Select the **Include All Subgroup** check box to include the subgroups.
8. Enter the description in the **Description** box.
9. Click **Preview**.

Searching a scheduled job by using filters

This section describes how to search a scheduled job and manage the jobs in the management console. To search a scheduled job by using filters, do the following:

1. Click **Jobs**.
   The **Jobs** page is displayed.
2. From the **Configuration Groups** drop-down menu, select either the default policy group or the groups which are added by an administrator.
3. From the **Scheduled by** drop-down menu, select a scheduler who performs the scheduling activity.
   The available options are:
   - Admin
     - – App Policy
     - – Image Policy
     - – Device Commands
   - System
     - – Publish Group Configuration

- Others

4   From the **OS Type** drop-down menu, select the operating system.

The available options are:

- ThinOS
- WES
- Linux
- Thin Linux
- Wyse Software Thin Client

5   From the **Status** drop-down menu, select the status of the job.

The available options are:

- Scheduled
- Running/In Progress
- Completed
- Cancelled
- Failed

6   From the **Detail Status** drop-down menu, select the status in detail.

The available options are:

- 1 or more failed
- 1 or more pending
- 1 or more In progress
- 1 or more cancelled
- 1 or more completed

7   From the **More Actions** drop-down menu, select the **Sync BIOS Admin Password** option.

The **Sync BIOS Admin Password Job** window is displayed. For more information see Sync BIOS Admin Password

Scheduling the image policy

Image policy is not a recurring job. Each command is specific to a device. To schedule an image policy, do the following:

1   On the **Jobs** page, click the **Schedule Image Policy** option.

The **Image Update Job** screen is displayed.

2   From the drop-down list, select a policy.

3   Enter the job description.

4   From the drop-down list, select the date or time.

5   Enter/select the following details:

- **Effective**—Enter the starting and ending date.
- **Start between**—Enter the starting and ending time.
- **On day(s)**—Select the days of the week.

6   Click the **Preview** option to view the details of the scheduled job.

7   Click the **Schedule** option to initiate the job.

Scheduling an application policy

Application policy is not a recurring job. Each command is specific to a device. To schedule an application policy, do the following:

1   On the **Jobs** page, click the **Schedule Application Policy** option.

The **App Policy Job** screen is displayed.

2   From the drop-down list, select a policy.

3   Enter the job description.

4   From the drop-down list, select the date or time.

5   Enter/select the following details:

- **Effective**— Enter the starting and ending date.
- **Start between**—Enter the starting and ending time.
- **On day(s)**—Select the days of the week.

6   Click the **Preview** option to view the details of the scheduled job.

7   On the next page, click the **Schedule** option to initiate the job.

Scheduling the device command job

To schedule a device command job, do the following:

1   On the **Jobs** page, click **Schedule device command job**.

The **Device Command Job** screen is displayed.

2   From the drop-down list, select a command.

Device command is a recurring job. On selected days of the week and at a specific time the commands are sent to the selected devices.

3   From the drop-down list, select the type of operating system.

4   Enter the name of the job.

5   From the drop-down list, select a group name.

6   Enter the job description.

7   From the drop-down list, select the date or time.

8   Enter/select the following details:

- **Effective**— Enter the starting and ending date.
- **Start between**—Enter the starting and ending time.
- **On day(s)**—Select the days of the week.

9   Click the **Preview** option to view the details of the scheduled job.

10   On the next page, click the **Schedule** option to initiate the job.

Managing Events

This section describes how to view all events and alerts in the management system using the management console. It also provides instructions on viewing an audit of events and alerts for system auditing purposes.

A summary of events and alerts is used to obtain an easy-to-read daily summary of what has happened in the system. The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

Figure 13. Events

Searching an event or alert by using filters

To search an event or alert by using filters, do the following:

1   Click **Events**.
    The **Events** page is displayed.

2   From the **Configuration Groups** drop-down menu, select either the default policy group or the groups which are added by an administrator.

3   From the **Events or Alerts** drop-down menu, select any one of the following options:
    - Events
    - Current Alerts
    - Alert History

4   From the **Timeframe** drop-down menu, select any one of the following operating systems:
    This option allows you to view the events which occurred in a particular timeframe. The available options in the drop-down menu are:
    - Today
    - Yesterday
    - This Week
    - Custom

5   From the **Event Type** drop-down menu, select any one of the following operating systems:
    All the events are classified under particular groups. The available options in the drop-down menu are:

- Access
- Registration
- Configuration
- Remote Commands
- Management
- Compliance

Searching an event or alert by using filters

To search an event or alert by using filters, do the following:

1   Click **Events**.

    The **Events** page is displayed.

2   From the **Configuration Groups** drop-down menu, select either the default policy group or the groups which are added by an administrator.

3   From the **Events or Alerts** drop-down menu, select any one of the following options:

- Events
- Current Alerts
- Alert History

4   From the **Timeframe** drop-down menu, select any one of the following operating systems:

    This option allows you to view the events which occurred in a particular timeframe. The available options in the drop-down menu are:

- Today
- Yesterday
- This Week
- Custom

5   From the **Event Type** drop-down menu, select any one of the following operating systems:

    All the events are classified under particular groups. The available options in the drop-down menu are:

- Access
- Registration
- Configuration
- Remote Commands
- Management
- Compliance

Viewing a summary of events

The **Events and Alerts** window displays all the events and alerts that have taken place in the system. Go to **Events** > **Summary**.

Viewing audit log

The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

1   Go to **Events** > **Audit**.

2   From the **Configuration Groups** drop-down list, select a group for which you want to view the audit log.

3   From the **Timeframe** drop-down list, select the time period to view the events that occurred during that time period.

Managing users

This section describes how to perform a routine user management task in the management console. The following are the two types of users:

- **Administrators**—Wyse Management Suite administrator can be assigned the role of a global administrator, group administrator, or viewer.
  - A Global Administrator has access to all the Wyse Management Suite functions.
  - A Group Administrator has access to all assets and functions for specific groups that are assigned to them.
  - A viewer has read-only access to all the data and can be assigned permissions to trigger the specific real-time commands, such as shutdown and restart.

  If you select administrator, you can perform any of the following actions:
  - Add Admin
  - Edit Admin
  - Activate Admin(s)
  - Deactivate Admin(s)
  - Delete Admin(s)
  - Unlock Admin(s)

Figure 14. Administrator

- **Unassigned Admins** —Users imported from the AD server are displayed on the **Unassigned admins** page. You can later assign a role to these users from the portal.

  For better and faster management of users, select the users of your choice based on the available filter options. If you select **Unmanaged Users**, you can perform any of the following actions:
  - Edit User
  - Activate User(s)
  - Deactivate User(s)
  - Delete User(s)

Figure 15. Unassigned admins

ⓘ | **NOTE: To import users from the CSV file, click Bulk Import.**

Topics:

- Adding a new admin profile
- Editing an admin profile
- Deactivating an admin profile
- Deleting an admin profile
- Editing a user profile
- Importing the CSV file

Adding a new admin profile

To add a new admin profile, do the following:

1   Click **Users**.
2   Click **Administrator(s)**.
3   Click **Add Admin**.
     The **New Admin User** window is displayed.
4   Enter your email ID and user name in the respective fields.
5   Select the check box to use the same user name as mentioned in the email.
6   Do one of the following:
     - If you click the **Personal Information** tab, enter the following details:
       – First name
       – Last name
       – Title
       – Mobile phone number
     - If you click the **Roles** tab, enter the following details:
       1   In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
            – Global Administrator
            – Group Administrator
            – Viewer

> (i) **NOTE: If you select the Administrator role as Viewer, the following administrative tasks are displayed:**
>   ◦ Query Device
>   ◦ Unregister Device
>   ◦ Restart/Shutdown Device
>   ◦ Change Group Assignment
>   ◦ Remote Shadow
>   ◦ Lock Device
>   ◦ Wipe Device
>   ◦ Send Message
>   ◦ WOL Device

2 In the **Password** section, do the following:

   a Enter the custom password.

   b To generate any random password, select the **Generate random password** radio button.

7 Click **Save**.

Editing an admin profile

To edit an admin profile, do the following:

1 Click **Users**.
2 Click **Administrator(s)**.
3 Click **Edit Admin**.

   The **Edit Admin User** window is displayed.

4 Enter your email ID and user name in the respective fields.

> (i) **NOTE: When you update the login name, you are forced to log out from the console. Log in to the console using the updated account login name.**

5 Do one of the following:

   • If you click the **Personal Information** tab, enter the following details:
     – First name
     – Last name
     – Title
     – Mobile phone number
   • If you click the **Roles** tab, enter the following details:
     1 In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
     2 In the **Password** section, do the following:

        a Enter the custom password.

        b To generate any random password, select the **Generate random password** radio button.

6 Click **Save**.

Deactivating an admin profile

Deactivating the admin profile prevents you from logging in to the console, and removes your account from the registered devices list. To deactivate an admin user, do the following:

1 Click **Users**.
2 Click **Administrator(s)**.
3 From the list, select a user and click **Deactivate Admin(s)**.

   An alert window is displayed.

4 Click **OK**.

Deleting an admin profile

Admin must be deactivated before you delete them. To delete an admin, do the following:

1   Click **Users**.
2   Click **Administrator(s)**.
3   Select the check box of a particular admin or admins which you want to delete.
4   Click **Delete Admin(s)**.

   An **Alert** window is displayed.
5   Enter a reason for the deletion to enable the **Delete** link.
6   Click **Delete**.

Editing a user profile

To edit a user profile, do the following:

1   Click **Users**.
2   Click **Unassigned Admins**.
3   Click **Edit User**.

   The **Edit Admin User** window is displayed.
4   Enter your email ID and user name in the respective fields.

   ⓘ **NOTE: When you update the login name, you are forced to log out from the console. Log in to the console using the updated account login name.**
5   Do one of the following:

   •   If you click the **Personal Information** tab, enter the following details:
      –   First name
      –   Last name
      –   Title
      –   Mobile phone number
   •   If you click the **Roles** tab, enter the following details:
      1   In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
      2   In the **Password** section, do the following:

         a   Enter the custom password.
         b   To generate any random password, select the **Generate random password** radio button.
6   Click **Save**.

Importing the CSV file

To import users from the CSV file, do the following:

1   Click **Users**.

   The **Users** page is displayed.
2   Select the **Unassigned Admins** option.
3   Click **Bulk Import**.

   The **Bulk Import** window is displayed.
4   Click **Browse** and select the CSV file.
5   Click **Import**.

Portal administration

This section contains a brief overview of your system administration tasks that are required to set up and maintain your system.

Figure 16. Portal admin

Topics:

- Adding the Active Directory server information
- Importing users to public cloud through active directory
- Alert classifications
- Creating an Application Programming Interface-API accounts
- Accessing file repository
- Configuring other settings
- Thin clients
- Managing Teradici configurations
- Enabling Two-Factor authentication
- Generating reports
- Enabling multi-tenant accounts
- Enabling custom branding
- Managing license subscription
- Managing system setup

Adding the Active Directory server information

To import Active Directory users on the Wyse Management Suite private cloud, do the following:

1   Log in to the Wyse Management Suite private cloud.
2   Navigate to **Portal Admin** > **Console Settings** > **Active Directory (AD)**.
3   Click the **Add AD Server Information** link.
4   Enter the server details such as **AD Server Name**, **Domain Name**, **Server URL**, and **Port**.
5   Click **Save**.
6   Click **Import**.
7   Enter the user name and password.

> ⓘ **NOTE: To search groups and users, you can filter them based on Search Base, and Group name contains options. You can enter the values as following:**
>
> - `OU=<OU Name>`, for example, `OU=TestOU`
> - `DC=<Child Domain>, DC=<Parent Domain>, DC=com`, for example, `DC=Skynet, DC=Alpha, DC=Com`
>
> **You can enter a space after a comma, but you cannot use single or double quotes.**

8   Click **Login**.
9   On the **User Group** page, click **Group name** and enter the group name.
10 In the **Search** field, type the group name you want to select.
11 Select a group.

The selected group is moved to the right pane of the page.

12 Click **Next**.
13 Click **Import Users**.

> ⓘ **NOTE: If you provide an invalid name or do not provide a last name, or provide any email address as name, then the entries cannot be imported into Wyse Management Suite. These entries are skipped during the user import process.**

The Wyse Management Suite portal displays a confirmation message with the number of imported active directory users. The imported active directory users are listed at **Users tab** > **Unassigned Admins**.

14 To assign different roles or permissions, select a user and click **Edit User**.

After you assign the roles to the active directory user, they are moved to the **Administrators** tab on the **Users** page.

Active directory users can log in to the Wyse Management Suite Management portal by using the domain credentials. To log in to the Wyse Management Suite portal, do the following:

1   Start the Wyse Management Suite management portal.
2   On the login screen, click the **Sign in with your domain credentials** link.
3   Enter the domain user credentials, and click **Sign In**.

The imported Active Directory users can be activated or deactivated on the **Users** page by using the global administrator login. If your account is deactivated, you cannot log in to the Wyse Management Suite Management portal.

> ⓘ **NOTE: To import the users using LDAPS protocol, complete the following steps:**
>
> 1   Import the AD Domain Server Root Certificate into Java Key Store Manually using the keytool. For example, **<C:\Program Files \DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe> -importcert -alias "WIN-O358EA52H8H" -keystore "<C:\Program Files\DELL \WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"**
> 2   Restart Tomcat service.

Configuring Active Directory Federation Services feature on public cloud

To configure Active Directory Federation Services (ADFS) on a public cloud, do the following:

1 On the **Portal Admin** page, under **Console Settings**, click **Active Directory (AD)**.
2 Enter the Wyse Management Suite details to ADFS. To know the location details on the ADFS server where you must upload the Wyse Management Suite xml files, hover the mouse over the **information (i)** icon.

> ⓘ NOTE: To download the Wyse Management Suite xml file, click the download link.

3 Set the Wyse Management Suite rules in ADFS. To know the custom claim rule details, hover the mouse over the **information (i)** icon.

> ⓘ NOTE: To view the Wyse Management rules, click the Show WMS Rules link. You can also download the Wyse Management Suite rules by clicking the link provided in the Wyse Management Suite Rules window.

4 To configure the ADFS details, click **Add Configuration**, and do the following:

> ⓘ NOTE: To allow tenants to follow the ADFS configuration, upload the ADFS metadata file.

   a To upload the XML file stored on your thin client, click **Load XML file**.

      The file is available at **https://adfs.example.com/FederationMetadata/2007–06/FederationMetadata.xml**.
   b Enter the details of the entity ID and X.509 signing certificate in the respective boxes.
   c Enter the ADFS login URL address and the ADFS logout URL address in the respective boxes.
   d To enable tenants to configure Single Sign-On by using ADFS, select the **Enable SSO login using ADFS** check box. This feature follows the Security Assertion and Markup Language (SAML) standard specification.
   e To validate the configuration information, click **Test ADFS Login**. This enables tenants to test their setup before saving.

   > ⓘ NOTE: Tenants can activate/deactivate SSO login by using ADFS.

5 Click **Save**.
6 After you save the metadata file, click **Update Configuration**.

> ⓘ NOTE:
> - Tenants can log in and log out by using their AD credentials configured from their ADFS. You must ensure that the AD users are imported to the Wyse Management Suite server. On the login page, click **Sign in** and enter your domain credentials. You must provide the email address of your AD user and sign in.
> - For more information about the ADFS documentation, go to Technet.microsoft.com/en-us/windowsserver/dd448613.

Importing users to public cloud through active directory

1 Download and install the file repository, see Accessing file repository. The repository must be installed by using the company network and must have the access to the AD server to pull the users.
2 Register the repository to public cloud. Once registered, follow the steps mentioned on the UI to import the users to Wyse Management Suite public cloud. You can edit the roles of the AD user after importing to Wyse Management Suite public cloud.
3 To setup ADFS on public cloud, see Configuring Active Directory Federation Services feature on public cloud.

Alert classifications

The Alert page categorizes the alerts as **Critical**, **Warning**, or **Info**.

> ⓘ NOTE: To receive alerts through e-mail, select the Alert Preferences option from the username menu displayed on the upper-right corner.

Select the preferred notification type such as, **Critical**, **Warning**, or **Info** for the following alerts:

- Device health alert
- Device not checked in

Creating an Application Programming Interface-API accounts

This section allows you to create secured Application Programming Interface (API) accounts. This service provides the ability to create special accounts.

To configure the external application service, do the following:

1 Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.
2 Select **External App Services** under **Console Settings**.
3 Select the **Add** tab to add an API service.

   The **Add External App Services** dialog box is displayed.
4 Enter the following details to add an external application service.

   - Name
   - Description
5 Select the **Auto Approve** check box.

   If you select the check box, approval from the global administrators is not required.
6 Click **Save**.

Accessing file repository

File repositories are places where **files** are stored and organized. Wyse Management Suite has two types of repositories:

- **Local Repository**—During the Wyse Management Suite private cloud installation, provide the local repository path in the Wyse Management Suite installer. After the installation, go to **Portal Admin** > **File Repository** and select the local repository. Click the **Edit** option to view and edit the repository settings.
- **Wyse Management Suite Repository**—Log in to Wyse Management Suite public cloud, go to **Portal Admin** > **File Repository** and download the Wyse Management Suite repository installer. After the installation, register the Wyse Management Suite repository to Wyse Management Suite Management server by providing the required information.

To use Wyse Management Suite repository, do the following:

1 Download the Wyse Management Suite repository from the public cloud console.
2 After the installation process, start the application.
3 On the Wyse Management Suite Repository page, enter the credentials to register the Wyse Management Suite repository to Wyse Management Suite server.
4 If you enable the **Register to Public WMS Management Portal** option, you can register the repository to Wyse Management Suite public cloud.
5 Click the **Sync Files** option to send the sync file command.
6 Click **Check In** and then click **Send Command** to send the device information command to the device.
7 Click the **Unregister** option to unregister the on-premises service.
8 Click **Edit** to edit the files.

   a From the drop-down list of **Concurrent File Downloads** option, select the number of files.
   b Enable or disable **Wake on LAN** option.
   c Enable or disable **Fast File Upload and Download (HTTP)** option.

      - When HTTP is enabled, the file upload and download occurs over HTTP.
      - When HTTP is not enabled, the file upload and download occurs over HTTPS.
   d Select the **Certificate Validation** check box to enable the CA validation for public cloud.

ⓘ **NOTE:**

- a When CA Validation from Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations such as, Apps and Data, Image Pull/Push is successful. If certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate Certificate Authority** under **Events** page. All the operations such as, Apps and Data, Image Pull/Push is not successful.
- b When CA Validation from Wyse Management Suite server is disabled, then the communication from server and client happens in secure channel without Certificate Signature validation.

e Add a note in the provided box.

f Click **Save Settings** .

Configuring other settings

You can use the following settings to enforce the **APNS Warnings**, **License Expiration Warnings**, and other **Self Service Legal Agreements**.

- **Dismiss License Expiration Warning on Dashboard page**—Select this check box to disable the warning for a license expiration from displaying on the **Dashboard** page.
- **Enable Advanced Dell Wyse Cloud Connect options in Android Settings policy configuration page (Note: Professional Tier Only)** —Select this option to enable Advanced Dell Wyse Cloud Connect options in the Android Settings policy configuration page.
- **Heartbeat interval**—Enter the time. The device sends heartbeat signal every 60 to 360 minutes.
- **Checkin interval**—Enter the time. The device sends full checking signal every 8 to 24 hours.
- **Not Checked In compliance alert**—Enter the number of days before a device triggers a **Not Checked In compliance alert**. The range is 1–99.

Thin clients

This section provides the following web links where you can download:

- Thin client operating system images—appservices.wyse.com/pages/serviceandsupport/support/downloads.asp
- Wyse Device Agent for Windows Embedded Standard thin clients—appservices.wyse.com/pages/serviceandsupport/support/downloads.asp
- Instructions for installing Wyse Device Agent on Windows Embedded Standard thin clients— support.wyse.com/OA_HTML

It also lists the groups and their corresponding registration tokens created for thin clients.

Managing Teradici configurations

To add a Teradici server, do the following:

1 In the **Portal Administration** tab, under **Console Settings**, click **Teradici**.

2 Click **Add Server**.

The **Add Server** screen is displayed.

3 Enter the **Server Name**. The port number is automatically populated.

4 Select the **CA Validation** check box to enable CA validation.

5 Click **Test**.

Enabling Two-Factor authentication

You must have at least two active global administrator users in the system.
Create two or more global administrators before proceeding to the task. To enable two factor authentication, do the following:

1 Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.

2 Click **Two Factor Authentication** under **Console Settings**.

3 You must select the check box to enable the two factor authentication.

> (i) **NOTE:** Administrators must verify the second authentication factor using one time passcodes to log in to the management portal.

4   You will receive a onetime passcode to your e-mail address. Enter one time passcode to verify.

By default, you have eight attempts to verify the one time passcode. If you fail to verify the passcode, the account will be locked. Only global administrators can unlock locked accounts.

Generating reports

To generate the reports, do the following:
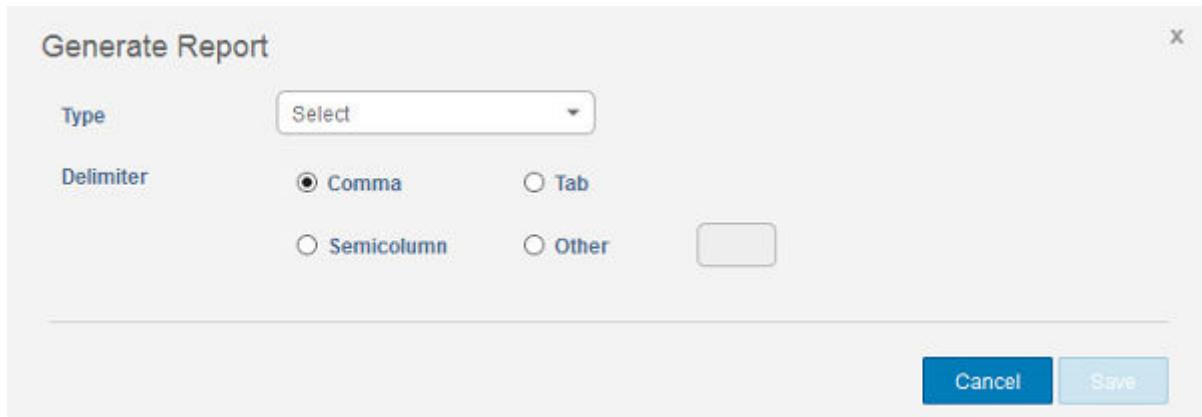
Figure 17. Generate report

1   Go to **Portal Admin** > **Reports**.
2   Click the **Generate Report** option.
     The **Generate Report** window is displayed.
3   From the **Type** drop-down list, select the type of the report.
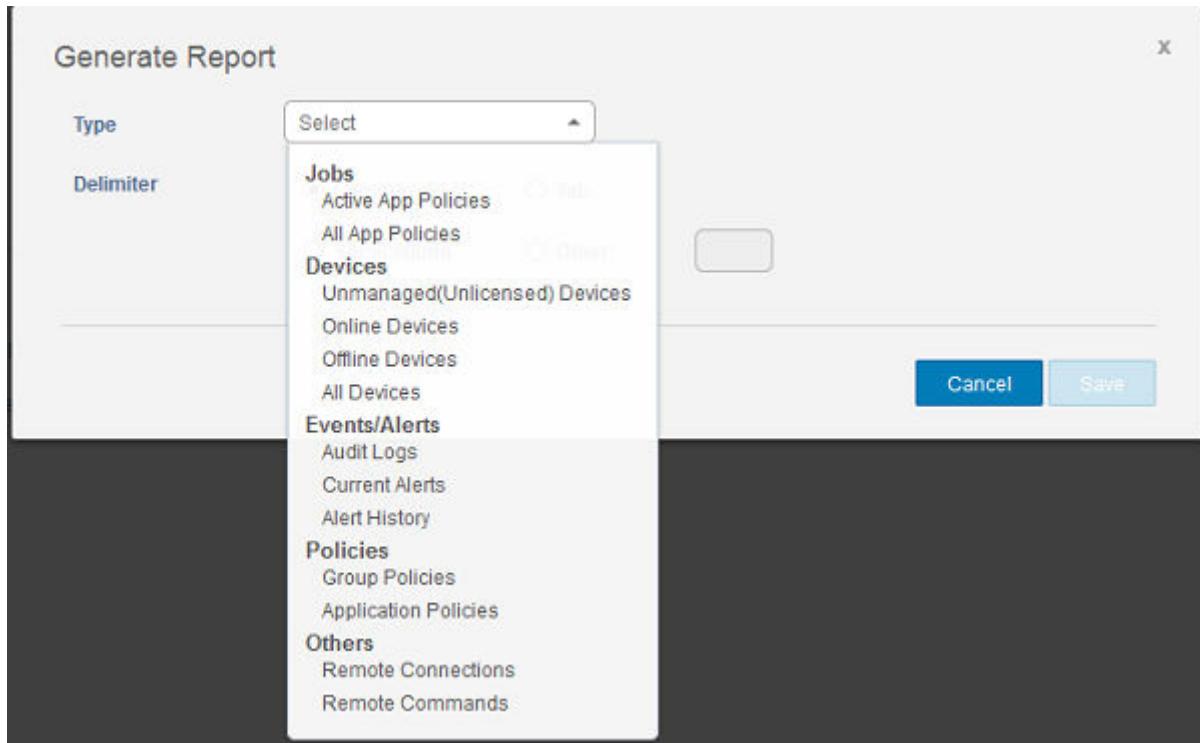
Figure 18. Types of report

4   From the **Groups** drop-down list, select the group.

5   Select the delimiter.

6   Click **Save**.

Enabling multi-tenant accounts

This section allows you to create an additional organization. You can manage the organizations independently. Each account must have its own license key and can set up its own set of admin accounts, policies, operating system images, application, rules, alerts, and so on. The high level operator creates these organizations.

To enable multi tenant accounts, do the following:

1   Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.

2   Select **Multi-Tenant** under **Console Settings**.

3   Select the check box to enable multi-tenant option.

4   Enter the following details:
    - User name
    - Password
    - Confirm password
    - Email

5   Click **Save Settings**.

Enabling custom branding

This option allows you to add the name of your company and its logo or brand. You can upload your own header logo, favicon, add a header title, and change header colors to customize the Wyse Management Suite portal.
To access and specify custom branding:

1   Go to **Portal Administrator** > **Account** > **Custom Branding**.
2   Click **Enable Custom Branding**
3   In **Header Logo**, click **Browser** and select and select the header logo image from the folder location.

    The maximum size of the header logo must be 500*50 pixels.
4   Enter the title under in **Title** option.
5   Select the **Display title in browser window/tab** check box to view the title in the browser.
6   Enter the color codes for **Header background color** and **Header text color**.
7   Click **Browse** and select the **Favicon**.

    The favicon appears in the browser address bar next to the website URL.

   ⓘ NOTE: You must save the images as .ico files only.
8   Click **Save Settings**.

Managing license subscription

This section allows you to view and manage the management console license subscription and its usage.
On the **Portal Admin** page, you can view the **Subscription** option. This page also provides the following information:

- **Registered Thin Client Devices**
- **Server information**
- **Import License (Private cloud)**
- **Export License for Private Cloud (Public cloud)**

Importing licenses from Wyse Management Suite Public Cloud

To import licenses from Wyse Management Suite Public Cloud to Wyse Management Suite Private Cloud, do the following:

1   Log in to Wyse Management Suite Private Cloud console.
2   Go to **Portal Administration** > **Accounts** > **Subscription**.
3   Enter the Wyse Management Suite Public Cloud details:
    - Username
    - Password
    - Data center
    - Number of TC seats
    - Number of Edge Gateway and Embedded PC seats
    - Number of Wyse Software Thin Client seats
4   Click **Import**.

   ⓘ NOTE: Wyse Management Suite Private Cloud must be connected to Wyse Management Suite public cloud.

Exporting licenses to Wyse Management Suite Private Cloud

To export licenses to Wyse Management Suite Private Cloud from Wyse Management Suite public cloud, do the following:

1 Log in to Wyse Management Suite public cloud console.
2 Go to **Portal Administration** > **Accounts** > **Subscription**.
3 Enter the number of thin client seats that must be exported to Wyse Management Suite Private Cloud.
4 Click **Export**.
5 Copy the generated license key.
6 Log in to Wyse Management Suite Private Cloud console.
7 Go to **Portal Administration** > **Accounts** > **Subscription**.
8 Enter the generated license key in the box.
9 Click **Import**.

Thin client licenses allocation

To allocate the thin client licenses between Wyse Management Suite Private Cloud and Wyse Management Suite Public Cloud account, do the following:

1 Log in to the Wyse Management Suite Public Cloud console.
2 Go to **Portal Administration** > **Accounts** > **Subscription**.
3 Enter the number of thin client seats.

   ⓘ **NOTE: The thin client seats should be manageable in the Public Cloud. The entered number of thin client seats must not exceed the number displayed in Manageable option.**

4 Click **Export**.

   ⓘ **NOTE: The number of Public Cloud licenses is adjusted based on the number of thin client seats exported to the Private Cloud.**

5 Copy the generated license key.
6 Log in to Wyse Management Suite Private Cloud console.
7 Go to **Portal Administration** > **Accounts** > **Subscription**.
8 Import the exported license key to the Private Cloud.

   ⓘ **NOTE: The license cannot be imported if it has insufficient thin client seats to manage the number of devices currently being managed in the Private Cloud. In this case repeat steps 3–8 to allocate the thin client seats.**

Managing system setup

This section provides the information about the following:

1 Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.
2 Click **Setup** under **Systems**.
3 Select the check box to perform server certificate validation for all device-to-server communication.
4 Enter the following details in the **Update SMTP for Email Alerts** area:

   · SMTP server
   · Send from address
   · Username
   · Password
   · Test address

Current Certificate: Select the **Certificate Validation** check box to enable the CA validation for private cloud. All the communication from the server and the client including file download, OS image download from Local Repo uses the certificate.

ⓘ **NOTE:** To Enable CA Validation for Remote Repo, Go to Portal Administration > File Repository > Select the Repository > Edit > Enable CA Validation > Save Settings.

ⓘ **NOTE:**

- 1 When CA Validation from Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations such as, Apps and Data, Image Pull/Push is successful. If certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate Certificate Authority** under **Events** page. All the operations such as, Apps and Data, Image Pull/Push is not successful.

  2 When CA Validation from Wyse Management Suite server is disabled, then the communication from server and client happens in secure channel without Certificate Signature validation.

5   Select the following options and enter the details:

- **Key/Certificate**: Upload HTTPS key/certificate file pair (only PEM format is supported).
- **PKCS-12**: Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is required for IIS pfx.

6   Click **Save**.

Configuring Wyse Easy Setup by using Wyse Management Suite

You can install and configure the Wyse Easy Setup software by using Wyse Management Suite.

Topics:

Installing Wyse Easy Setup

Prerequisites

- A minimum free disk space of 100 MB
- A minimum RAM disk size of 100 MB
- Microsoft Visual C++ Redistributable 2012 32–bit (x86) or 64–bit (x64)
- Microsoft .Net Framework 4.5 and above
- Wyse Device Agent version 14.0.0.237 and above

Steps

1 Log in to the Wyse Management Suite console.
2 Click **Apps & Data**.
3 In **App Policies**, click **Thin Client**.
4 Click **Add Policy**.
   The **Add Standard App Policy** window is displayed.
5 Enter the policy name.
6 Select the group, task, OS type, application, OS subtype filter, and platform filter from the corresponding drop-down list.
7 Enter /s in the **Installer Parameters** field.
8 Click **Save**.
9 Go to the **Jobs** page and schedule the job to start the silent installation of Wyse Easy Setup.

Deploying a Wyse Easy Setup configuration

Before deploying a configuration, ensure that the thin client is registered to Wyse Management Suite.

1 Log in to the Wyse Management Suite console.
2 Click **Groups & Configs**.
3 Select a group, and click **Edit Policies**.
4 Click **WES**.
5 Click **Wyse Easy Setup**.
6 After configuring the policy settings, click **Save and Publish**.

(i) **NOTE:**

- If the thin client is registered to Wyse Management Suite, all the local configurations deployed using the Wyse Easy Setup administrator shell are discarded. The remote configurations deployed using Wyse Management Suite are applied.
- If the thin client is unregistered from Wyse Management Suite, the configurations deployed through Wyse Management Suite are discarded. The local configurations deployed using the Wyse Easy Setup administrator shell are applied.

Configuring Wyse Converter for PCs by using Wyse Management Suite

You can install and configure the Wyse Converter for PCs software by using Wyse Management Suite.

Topics:

- Registering Wyse Software thin client to Wyse Management Suite
- Registering Wyse Software Thin Client to Wyse Management Suite by using Wyse Device Agent
- Registering devices by using DHCP option tags to Wyse Management Suite
- Registering Wyse Software thin clients by using DNS SRV record to Wyse Management Suite
- Configuring the Wyse Software thin client by using Wyse Management Suite

Registering Wyse Software thin client to Wyse Management Suite

You can register Wyse Software thin client with Wyse Management Suite by using any of the following methods:

- Register manually through the user interface provided by the Wyse Device Agent (WDA) on the device.
- Register automatically by configuring the appropriate option tags on the DHCP server.
- Register automatically by configuring the appropriate DNS SRV records on the DNS server.

Registering Wyse Software Thin Client to Wyse Management Suite by using Wyse Device Agent

Prerequisites

Create a group to register a device to Wyse Management Suite.

Steps

1   Open the **Wyse Device Agent** application.
    The **Wyse Device Agent** window is displayed.
2   Enter the device registration details.
3   From the **Management Server** drop-down list, select **Wyse Management Suite**.
4   Enter the server address and the port number in the respective fields.
5   Enter the group token. For a single tenant, the group token is an optional step.
6   Click **Register**.
    After the registration is complete, the **Registered to Wyse Management Suite** message is displayed.

Registering devices by using DHCP option tags to Wyse Management Suite

You can register the devices by using the following DHCP option tags:

Table 280. Registering device by using DHCP option tags

Option Tag	Description
Name—WMS **Data Type**—String **Code**—165 **Description**—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, **wmsserver.acme.com:443**, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. (i) **NOTE: Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite.**
Name—MQTT **Data Type**—String **Code**—166 **Description**—MQTT Server	This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, **wmsservername.domain.com: 1883**. To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example, US1—us1-pns.wysemanagementsuite.com EU1—eu1-pns.wysemanagementsuite.com
Name—CA Validation **Data Type**—String **Code**—167 **Description**—Certificate Authority Validation	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. By default, the CA validation is enabled in the public cloud. You can disable the CA validation in the public cloud as well. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.

Registering Wyse Software thin clients by using DNS SRV record to Wyse Management Suite

DNS based device registration is supported with the Wyse Device Agent: 13.0 or later versions. You can register devices with the Wyse Management Suite server if DNS SRV record fields are set with valid values. The following table lists the valid values for the DNS SRV records:

Table 281. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name—_WMS_MGMT **Record FQDN**—_WMS_MGMT._tcp.<Domainname> **Record Type**— SRV	This record points to the Wyse Management Suite server URL. For example, **wmsserver.acme.com:443**, where wmsserver.acme.com is the fully qualified domain name of the server where Wyse Management Suite is installed. (i) **NOTE: Do not use https:// in the server URL, or the thin client will not register under Wyse Management Suite.**
Record Name—_WMS_MQTT **Record FQDN**—_WMS_MQTT._tcp.<Domainname> **Record Type**—SRV	This record directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, **wmsservername.domain.com:1883**.

URL/Tag	Description
	ⓘ **NOTE: MQTT is optional for the latest version of Wyse Management Suite.** To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example, US1—us1-pns.wysemanagementsuite.com EU1—eu1-pns.wysemanagementsuite.com
Record Name—_WMS_CAVALIDATION **Record FQDN**—_WMS_CAVALIDATION._tcp.<Domainname> **Record Type**—TEXT	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. By default, the CA validation is enabled in the public cloud. You can disable the CA validation in the public cloud as well. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. ⓘ **NOTE: CA Validation is optional for the latest version of Wyse Management Suite.**

Configuring the Wyse Software thin client by using Wyse Management Suite

You can configure your Wyse Software thin client by using Wyse Management Suite 1.1 and later version if the device is converted to a thin client by using Wyse Converter for PCs. Before you configure the Wyse Software thin client, you must register it on Wyse Management Suite.

1   Log in to the Wyse Management Suite console.
2   Click **Groups & Configs** on the dashboard.
3   Select a group, and click **Edit Policies**.
4   Click **Wyse Software Thin Client**.
     The **Wyse Software Thin Client** page is displayed.
5   After configuring the options, click **Save and Publish**.

Teradici device management

The Teradici device management section provides the information about managing and discovering the teradici divices. The teradici management console uses SDK's to support management, configuration for tera devices. This is applicable only for Wyse Management Suite private cloud with pro license type. For more information on Teradici configuration policies, see Editing Teradici policy settings.

Topics:

• Discovering Teradici devices
• CIFS use case scenarios

Discovering Teradici devices

Prerequisites

• Install the latest version of Wyse Management Suite on Microsoft Windows 2012 Server or later versions. Threadx 5.x and 6.x devices works with the latest version of the operating system.
• Install and enable the **EMSDK** component.
• The FQDN of the Wyse Management Suite server must be available for **DHCP** or **DNS** configurations.
• `Cert.pem` must be placed in the default path **C:\Program Files\Dell\WMS\Teradici\EMSDK**. It is used to discover Threadx devices.

Manual discovery from the client

1   Go to, **https://<clientIP>**.
2   Accept the certificate warning message.
3   Enter the administrator password (default password is Administrator) and login.
4   Go to, **upload** > **certificate**. Select the `Cert.pem`file from the default path and click **Upload**.
5   Go to **Configuration** > **Management**. Click the **clear management state** button to register the device to the new Management Server.
6   Set the **manager discovery mode** to manual
7   Enter the **Endpoint Bootstrap Manager URL** in the following format **wss://<IP Address of the WMS server>**

   ⓘ **NOTE: If EMSDK is installed with custom port then provide Endpoint Bootstrap Manager URL in the following format wss://<IP Address:Custom port.**

8   Click **Apply**, and then click **Continue.**
9   The **management status** is displayed as Connected to the Endpoint server.

Adding the PCoIP endpoint vendor class to DHCP server

1   Log in to your DHCP server.
2   Right-click the DHCP server in the **SERVERS** pane, and select **DHCP Manager**.
3   Right-click the **IPv4** option, and then select **Define Vendor Classes**.
4   Click **Add** to add a new DHCP vendor class.
5   Enter the **PCoIP Endpoint** in the **Display name** field.

6 Enter the **PCoIP Endpoint** in the **ASCII** column as the Vendor ID.

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

Configuring DHCP options

1 Right-click the **IPv4** option, and the select **Set Predefined Options**.

2 Select **PCoIP Endpoint** as the **Option** class, and then click **Add**.

3 In the **Option Type** dialog box, enter the name as **EBM URI**, data type as **String**, code as **10**, and description as **Endpoint Bootstrap Manager URI**, and then click **OK**.

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

5 Expand the DHCP scope to which you want to apply the options.

6 Right-click the **Scope Options**, and then select **Configure Options**.

7 Click the **Advanced** tab, and then select the **PCoIP Endpoint** vendor class.

8 Select the **010 EBM URI** check box, and then enter a valid Management Console URI in the **String** field. Click **Apply**. This URI requires a secured WebSocket prefix, for example, **wss://<MC IP address>:[port number]**. 5172 is the MC's listening port . Entering this port number is an optional step.

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

10 Select **PCoIP Endpoint** as the **Option** class, and then click **Add**.

11 In the **Option Type** dialog, enter the name as **EBM X.509 SHA-256 fingerprint**, data type as **String**, code as **11**, and the description as **EBM X.509 SHA-256 fingerprint**, and then click **OK**.

12 Expand the DHCP scope to which you want to apply the options.

13 Right-click the **Scope Options**, and then select **Configure Options**.

14 Click the **Advanced** tab, and then select the **PCoIP Endpoint** vendor class.

15 Select the **011 EBM X.509 SHA-256 fingerprint** check box, and paste the SHA-256 fingerprint.

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

17 Go to the client web browser.

18 Go to **Configuration** > **Management**, and set the **manager discovery mode** to **Automatic**

19 The client is connected to the server which is mentioned in the DHCP server.

Creating the DNS SRV record

1 Log in to the **DNS server**.

2 Right-click the DNS server in the **SERVERS** pane, and the select **DNS Manager** from the context menu.

3 In **Forward Lookup Zones**, right-click the domain, and then select **Other New Records** from the context menu.

4 In the **Resource Record Type** dialog box, select **Service Location (SRV)** from the list, and click **Create Record**.

5 Set **Service** to **_pcoip-bootstrap**, protocol to **_tcp**, and **Port number** to **5172**, which is MC's default listening port. For **Host offering this service**, enter the MC's FQDN.

> ⓘ **NOTE: The MC's FQDN must be entered because the DNS specification does not allow an IP address in the SRV records.**

6 Click **OK**.

Adding a DNS TXT record

1   In **Forward Lookup Zones**, right-click the domain, and then select **Other New Records** from the context menu.

2   In the **Resource Record Type** dialog box, select the **Text (TXT)** from the list, and then click **Create Record**.

3   Enter the following details:

     a   In the **Record name** field, enter the host name of the Wyse Management Suite server offering the service. The FQDN field is populated automatically. This should match the FQDN of the Wyse Management Suite server.

     b   In the **Text** field, enter **pcoip-bootstrap-cert=** and then paste the Wyse Management Suite server certificate SHA-256 fingerprint.

4   Click **OK**.

5   Go to the client web browser.

6   The client is connected to the Wyse Management Suite server which is mentioned in the DNS server.

Creating SHA-256 fingerprint

1   Start the Mozilla Firefox.

2   Navigate to **Options Advanced** Tab

3   Click **Certificates** to view the certificates.

4   Under **Certificate Manager** , click **Authorities**, and the click **Import**.

5   Browse the certificate, and the click **View**.

6   Copy the **SHA-256** fingerprint.

CIFS use case scenarios

The following use cases are supported in Wyse Management Suite:

- When you select **Wyse Management Suite** as **Setup Type** while installing Wyse Management Suite private cloud.
  - CIFS configuration page is displayed. This page is required as we need to configure the shared folder.
    > ⓘ NOTE: **The Configure CIFS User Credentials option is disabled by default.**
- When you select **Teradici EMSDK** as **Setup Type** while installing Wyse Management Suite private cloud.
  - For CIFS credentials, you can use an existing account or create a new one.
- When you select both **Wyse Management Suite** and **Teradici EMSDK** as **Setup Type** while installing Wyse Management Suite private cloud.
  - CIFS configuration page is displayed. This page is required as we need to configure the shared folder.
    > ⓘ NOTE: **The Configure CIFS User Credentials option is disabled by default.**
  - For CIFS credentials, you can use an existing account or create a new one.
- When you install only EMSDK on a system which already has the EMSDK service installed.
  - If Teradici EMSDK is selected then a warning message is displayed when you click **Next** from the **Setup Type** page. The message is **The installer has detected that the Teradici EMSDK is already installed. The EMSDK will be updated if required**. No port number is required.
    - If **Configure CIFS User Credentials** option is selected (By default)
      - a   Stop the service.
      - b   Update the EMSDK service.

    c   Restart the service. It operates under the same pre-configured user.

- ○ If **Configure CIFS User Credentials** option is selected with **Use an existing user**option.
  - a   Stop the service.
  - b   Update the EMSDK service.
  - c   Update the service log on user to the one selected.
  - d   Restart the service. It operates under the same pre-configured user.
- ○ If **Configure CIFS User Credentials** option is selected with **Create a New User** option.
  - a   Stop the service.
  - b   Update the EMSDK service.
  - c   Update the service log on user to the newly created user.
  - d   Restart the service. It operates under the same pre-configured user.

- When you install both **Wyse Management Suite** and **Teradici EMSDK** on a system that has already the EMSDK service installed.
  - – Same as **When you install only EMSDK on a system which already has the EMSDK service installed** except that the **Configure CIFS User Credentials** option is selected by default and greyed out. You must enter CIFS credentials.

Troubleshooting Wyse Management Suite

Table 282. Troubleshooting

Issue	Workaround
Email alert notifications are not working.	Configure the SMTP server from the Wyse Management Suite server portal admin.
Wake on LAN is not working.	Enable the local or remote file repository.
Unknown file type warning message is displayed when you double click the WMS launch icon.	Check the security settings or UAC of the server. Ensure that all the Windows is updated with all the patches.
Unable to pull the thin client log file when ThinLinux device is not synchronized with NTP server.	Configure the device with a proper NTP server.
Error in syncing TC files alert message is displayed when you try to sync the file repository.	Ensure everyone has full permission to local repository and no user access message is displayed when you copy the image or applications to the local repository.
File download such as wallpaper, certificates fails for ThinOS when server is out of time sync.	Configure the device with proper NTP server.
ThinOS DHCP discovery fails when DNS SRV tags are available with blank values.	Remove the empty DNS tags.
Apply to new devices does not work for ThinOS app policies during registration.	Create a job to push the app policy.
After changing the hostname of the repository server, the repository UI does not open through desktop shortcut. After changing the hostname of the repository server, the certificate changes and you get the certificate error while opening the repository UI and self-signed certificate for CA validation also fails.	You must provide the updated hostname in the URL.
On Windows Embedded Standard devices, if the custom values are not set, groups are not created when you select custom values as group type. In the group structure, a level is missed.	Custom fields must have values before forming groups for Windows Embedded Standard devices.
Sync time command fails on Windows Embedded Standard devices.	No workaround available.
As part of RSP push, CU—Confirm User command always display **No user logged in** error even when a valid user is logged in to the thin client.	No workaround available.
The 404 error is displayed if the server is left ideal for 2 days.	The server restarts due to Windows. Restart all the Wyse Management Suite related services.
Wyse Management Suite server does not respond when the disk space is less than 300 MB.	Increase the storage space, and restart the Wyse Management Suite related services.

Issue	Workaround
When the agent registers with http, Wyse Management Suite sends the https URL and all the new agents switch to https.	Agents 12.x does not have this behavior since the agent does not understand the switching login.
No Supported sub Auth types error is displayed when you try to launch VNC session from Wyse Management Suite server after disabling the **VNC User required password** option.	Launch the VNC with **VNC User required password** option.
Add Policy and Add Advance Policy buttons become nonfunctional after application folders are removed.	Do not delete the repository folder.
Deleting inventory files manually from the physical path(c:\repository\data) does not remove the file from Wyse Management Suite UI—**File does not exist** error is displayed.	Do not delete the file from the repository folder manually.
ThinOS applications are installed twice when the applications are pushed with firmware.	The root disk is formatted when you upgrade or downgrade the **base.pkg**.
Import tool allows you to import RSP packages even if you delete any file (part1Image.img,vmlinuz,mbr and so on) from the RSP package on WDM repository.	Valid RDP packages must be present in Wyse Device Manager.
Wyse Management Suite displays a 404 error.	Verify if any java code is deleted by the antivirus software.
Window Embedded Standard app download fails.	App download authentication is required for Window Embedded Standard agent.
	If the app download fails with **https**, try with **http**. Ensure the firewall settings allows **http** port. The default port is 8080.
If the device is added to the domain during unregister or policy removal, the device reverts to the work group from the domain.	Set the default policy for domain settings, and push the policy.
RemoteFX USB redirection Policy does not get applied for USB mass storage devices.	Add the following registry entries to the device:
	1 Log in to device as an administrator and disable the Write Filter.
	2 Go to Run command and type `Regedit`.
	3 Go to **HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces**
	4 Add string registry key as `100` and set the value as for Mass Storage Device as follows:**{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}** for CD ROM : **{53F56308-B6BF-11D0-94F2-00A0C91EFB8B}**
	ⓘ | NOTE: **Flower brackets are mandatory.**
USB lock down configuration is not applied when you click the update button.	This issue is only for Wyse Software thin clients. Login again to apply the policy.
When you push SD command as part of RSP, Windows Embedded Standard client restarts instead of shutdown.	In Wyse Device Manager the device sends V02 message and goes to log off state. This is not supported for Wyse Management Suite.
Application installation fails when a policy is created from two different repository servers.	Ensure all the repositories are accessible by the device.
	Wyse Device Agent always tries the test download with the application created from the first repository server. If the test download fails the agent does not proceed further and an error report is sent to the server.

Issue	Workaround
You cannot perform RAW imaging using RSP through Wyse Management Suite.	To perform ThinLinux RAW imaging through Wyse Management Suite: 1 Create an FTP location. 2 Copy the RAW image to the FTP location. 3 Copy the RAW image file again from the Wyse Management Suite Repository. 4 Create a Standard App policy with RAW image by providing the FTP location, user name, and password as install parameters. 5 Schedule a policy job.
Wyse Management Suite server does not work after you install it with the remote database option on the same server where MongoDB is installed.	Delete the stratus database entry if present.
Wyse Management Suite server user interface does not load and log in to the server after installing the server.	The server hostname might contain underscore (_). Change the hostname without an underscore in it.
Wyse Device Agent registration fails after installing the server with custom ports.	Provide http/https prefix in the server field from the agent.
Static IP is not preserved on the thin client after an image push (Sysprep).	Assign a static IP to the thin client and restart the device.
Wyse Device Agent user interface shows **Service not running** or a blank screen when an upgrade or downgrade is performed for ThinLinux Wyse Device Agent.	Wait for few seconds until all the services are running.
Unable to import users with LDAPS configuration.	On the Wyse Management Suite server side do the following: 1 Import the AD domain server root certificate into Java Key Store manually by running the following command: **<C:\ProgramFiles\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe> -importcert -alias "WIN-O358EA52H8H" -keystore "<C:\ProgramFiles\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"** 2 Restart Tomcat services. In the Wyse Management Suite repository do the following: 1 Use the UI option to import the certificate to Java Keystore. 2 Restart Tomcat services.
Multi monitor option is not present for Wyse software thin client.	Multi monitor feature is not supported on Wyse Converter for PCs.
Wyse Management Suite upgrade from 1.0 to 1.1 does not work with external Mongo and embedded Maria database.	Upgrade directly to Wyse Management Suite 1.2.
Imaging through HTTP does not work.	Ensure HTTP is enabled manually. From Wyse Management Suite version 1.2 onwards, HTTP is disabled by default and admin must enable from the Tomcat manually. ⓘ NOTE: If the app download fails with **https**, try with **http**. Ensure the firewall settings allows **http** port. The default port is 8080.

Issue	Workaround
Mongo, Maria and Tomcat services are stopped after restarting the Wyse Management Suite server.	Windows defender service deletes the Wyse Management Suite related files. Check the defender service logs if any deleted files. Retrieve the deleted files.
VC++ package takes 20 minutes to install.	Ensure that the windows server is updated with the latest service packs and updates. Ensure that the Windows update is not in-progress while installing the Wyse Management Suite.
ThinLinux agent upgrade from 2.0.24 to 2.2.11 is not working.	ThinLinux devices with agent version 2.0.24 must be upgraded to 2.1.23 before upgrading to 2.2.11 since 2.0.24 agent does not install the **.tar** files.
Agent upgrade from 3.0.7 to 3.2.13 fails on the Wyse 3040 thin client with Thinlinux device.	Upgrade the agent to 3.0.10 version using package **wda3040_3.0.10-01_amd64.deb**. This package is bundled in Wyse Management Suite 1.2 installer and then upgrade to the latest WDA 3.2.13.
The threadx 6.x teradici devices fails to register to EMSDK after resetting the factory settings.	Connect the zero client to the NTP server before connecting to the end device, similar to using the DHCP option. You can also install a certificate with valid start date. The date must fall before the firmware date.
When Wyse Management Suite UI is installed with embedded Maria, remote mongo and database server is provided as localhost in remote mongo, then the **HTTP 404 Not Found** error is displayed.	Use local IP 127.0.0.1 or the server IP.
The image which is pulled by USB tool is not registered in Wyse Management Suite server.	Modify the image version to .rsp file and register to Wyse Management Suite.
Teradici server fails to sync, when IP address of the Wyse Management Suite server is changed (EMSDK in the same server) even after restarting the server.	Update the Teradici Server IP from the Portal > Administration > Teradici > Edit server.
When importing the groups and devices using WDM default Groups Types from the Import Tool, OS type is displayed twice.	Restart the import process from beginning.
When you select the Set up page after changing the Wyse Management Suite server IP address, the **Error:Error** message is displayed.	Restart the Wyse Management Suite services after changing the IP address.
After Wyse Management Suite fresh installation with custom port (well-known ports), not able to launch Web UI.	Dell recommends to use port 1024 or greater.
In ThinLinux version 2.0, **Media validation failed** error observed when you try to downgrade from 2.0.25 test build to 2.0.22/2.0.14(5070/3040) released builds.	Install the latest version of Merlin above 3.7.7.
After merlin upgrade, boot files are not copied under **/boot** folder	Uninstall and install the latest version of merlin.
Unable to login to the Wyse Management Suite server when all the accounts are locked and 2FA option is enabled	Set the TwoStepVerificationEnabled value to False (0) from the table stratus.tenant present in the MariaDB.

Installing or upgrading Wyse Device Agent

This section provides information about how to install or upgrade Wyse Device Agent on your thin clients, such as Windows Embedded Standard, Linux, and ThinLinux devices, by using Wyse Management Suite.

- **Windows Embedded Standard devices**—Wyse Device Agent version 14 can be downloaded from Dell support location and installed or upgraded on Windows Embedded Standard devices using any of the following methods:
    - Upgrading Wyse Device Agent using Wyse Management Suite application policy.
    - Installing Wyse Device Agent manually.
- **Linux and ThinLinux devices**—Wyse Device Agent can be installed or upgraded on Linux and ThinLinux devices by using Wyse Management Suite. For more information, see Installing or upgrading Wyse Device Agents on ThinLinux and Linux clients.

Topics:

- Upgrading Wyse Device Agent using Wyse Management Suite application policy
- Installing Wyse Device Agent manually
- Installing or upgrading Wyse Device Agents on ThinLinux and Linux clients

Upgrading Wyse Device Agent using Wyse Management Suite application policy

Dell recommends that you use the Wyse Management Suite application for upgrading Wyse Device Agent on devices. In the Wyse Management Suite private cloud setup, the latest Wyse Device Agent packages for Windows Embedded Standard are available in the local repository. If you are using a public cloud or a remote repository on a private cloud, copy the **WDA.exe** file to the **thinClientApps** folder in the repository. To upgrade Wyse Device Agent, do the following:

1   After the **WDA.exe** file is copied to the repository, go to the **Apps and Data** section, and create a normal application policy with this package.

> ⓘ NOTE: Advanced application policy is supported only from Wyse Device Agent 14.x onwards. Dell recommends that you use the normal application policy when upgrading Wyse Device Agent from 14.x. You can also use the advanced application policy for upgrading Wyse Device Agent from 14.x to latest versions.

2   Go to the **Jobs** page, and schedule a job to upgrade the Wyse Device Agent.

> ⓘ NOTE: For upgrading Windows Embedded Standard Wyse Device Agent from 13.x version to 14.x version, Dell recommends that you use HTTP as the repository protocol.

After a successful installation, the status is sent to the server.

Installing Wyse Device Agent manually

To install Wyse Device Agent manually, do the following:

1   Copy the **WDA.exe** file to the thin client.
2   Double-click the **WDA.exe** file.

> ⓘ NOTE:
> - Different Wyse Device Agent packages are available for each variant of Windows Embedded Standard.
> - A warning message is displayed when an older version of Wyse Device Agent or HAgent is installed on the device.

3   Click **Yes**.

4　In the **Group token** field, enter a group token. This is an optional field. To skip this step, click **Next**. You can enter the group token details later in the Wyse Device Agent User Interface.

5　From the **Region** drop-down list, select the region of the Wyse Management Suite public cloud server.

After successful installation, the Wyse Management Suite public cloud server automatically registers the device to the Wyse Management Suite console.

Installing or upgrading Wyse Device Agents on ThinLinux and Linux clients

To upgrade Wyse Device Agent and platform utility packages on Linux and ThinLinux clients from Wyse Management Suite server, do the following:

ⓘ | **NOTE: You can install or upgrade add-ons by using any of the following options:**

- Using INI parameters
- Add-ons Manager
- RPM commands

1　If you are using a public cloud or a remote repository on a private cloud, copy the RPM files to the **thinClientApps** folder of the repository. By default, the latest Wyse Device Agents and platform utility RPMs for Linux and ThinLinux clients are available in local repository.

2　Go to the **Apps and Data** page, and create two application policies—for platform utility add-on and Wyse Device Agent add-on.

ⓘ | **NOTE:**
- To upgrade these add-ons, use a normal policy. This is because the **Advanced App policy** function is supported only for Wyse Device Agent version 2.0.11 and 2.0.24 onwards on Linux and ThinLinux clients.
- You must install platform utility add-on and Wyse Device Agent add-on for Linux thin clients. You can install `wda_x.x.x.tar` file for ThinLinux thin clients.
- To install Wyse Device Agents on Dell Wyse 3040 thin clients with ThinLinux version 2.0, image version 2.0.14, and Wyse Device Agent version 3.0.7, you must install `wda3040_3.0.10-01_amd64.deb` file, and then install `wda_3.2.12-01_amd64.tar` file.

3　Go to the **Jobs** page and schedule a job to upgrade the platform utility add-on.

You must wait until the platform utility add-on is successfully installed on your thin client.

ⓘ | **NOTE: Install a platform utility add-on first, and then install a Wyse Device Agent add-on. You cannot install the latest Wyse Device Agents before installing the latest platform utility add-on.**

4　On the **Jobs** page, schedule a job to upgrade Wyse Device Agent on the client.

ⓘ | **NOTE: Linux client restarts after installing the Wyse Device Agent add-on version 2.0.11.**

Wyse Management Suite feature matrix

The following table provides information about the features supported for each subscription type:

Table 283. Feature matrix for each subscription type

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Highly scalable solution to manage thin clients	Free up to 10,000 devices	50,000 devices and more	1 million devices and more
License key	Not required	Required	Required
Group based management	Supported	Supported	Supported
Multi-level groups and inheritance	Supported	Supported	Supported
Configuration policy management	Supported	Supported	Supported
Operating system patch and image management	Supported	Supported	Supported
View effective configuration at device level after inheritance	Supported	Supported	Supported
Application policy management	Supported	Supported	Supported
Asset, inventory and systems management	Supported	Supported	Supported
Automatic device discovery	Supported	Supported	Supported
Real-time commands	Supported	Supported	Supported
Smart scheduling	Supported	Supported	Supported
Alerts, events and audit logs	Supported	Supported	Supported
Secure communication (HTTPS)	Supported	Supported	Supported
Manage devices behind firewalls	Limited*	Limited*	Supported
Mobile application	Not supported	Supported	Supported
Alerts using email and mobile application	Not supported	Supported	Supported
Scripting support for customizing application installation	Not supported	Supported	Supported
Bundle applications to simplify deployment and minimize reboots	Not supported	Supported	Supported

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Delegated administration	Not supported	Supported	Supported
Dynamic group creation and assignment based on device attributes	Not supported	Supported	Supported
Two-factor authentication	Supported	Supported	Supported
Active directory authentication for role based administration.	Not supported	Supported	Supported
Multi-tenancy	Not supported	Supported	Supported
Enterprise grade reporting	Not supported	Supported	Supported
Multiple repositories	Not supported	Supported	Supported
Enable/disable hardware ports on supported platforms	Not supported	Supported	Supported
BIOS configuration on supported platforms	Not supported	Supported	Supported

(i) **NOTE:** *The asterisk indicates that you can manage the devices by using Wyse Management Suite only in a secure firewall work environment. You cannot manage thin clients beyond the purview of the firewall settings.

Supported thin clients on Wyse management Suite

Table 284. Supported thin clients

Operating System	Device Type	Build number
Linux	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client	11.3.106 WDA version 2.0.11-00.1 and later Platform utility version 1.0.3-0.1 and later
ThinLinux	Wyse 5020 thin client Wyse 5060 thin client Wyse 7020 thin client Wyse 3030 LT thin client Wyse 3040 thin client	For Wyse 3040 thin client: 1.0.7.1 and other platforms-1.0.7 WDA version 2.2.10-00.01 and later Platform Utility version 1.2.3-0.3 and later
ThinLinux 2.0	Wyse 3040 thin client Wyse 5070 thin client Wyse 5070 Extended thin client	For Wyse 3040 thin client: 2.0.14.31318 WDA version 3.0.7 and later Platform Utility version 2.2.7-04 and later For Wyse 5070 thin client: 2.0.22.31472 WDA version 3.2.13–01 and later Platform Utility version 2.2.7-04 and later
Windows Embedded Standard 7 (WES7)	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 3030 thin client Wyse 7010 Extended thin client	7076 and 7077 WDA versions 14.2.0.x and later
Windows Embedded Standard 7P (WES7P)	Wyse 5010 thin client	7065, 7066, 7067 WDA versions 14.2.0.x and later

Operating System	Device Type	Build number
	Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 7010 Extended thin client	
	Wyse 7040 thin client	7065 WDA versions 14.2.0.x and later
	Latitude 3460 mobile thin client	7065 WDA versions 14.2.0.x and later
	Latitude E7270 mobile thin client	7065 WDA versions 14.2.0.x and later
	Wyse 5060 thin client	7067 WDA versions 14.2.0.x and later
Windows 10 IoT Enterprise (WIE10)	Wyse 5020 thin client	0A62
	Wyse 7020 thin client	0A63
	Latitude 3480 mobile thin client	0A64
	Latitude 5280 mobile thin client	10.03.06.05.18.00
	Wyse 5070 thin client	WDA versions 14.2.0.x and later
	Wyse 5070 Extended thin client	
Windows Embedded 8 Standard (WE8S)	Wyse 5010 thin client	930
	Wyse 7010 thin client	WDA versions 14.2.0.x and later
	Wyse 5020 thin client	
	Wyse 7020 thin client	
ThinOS	Wyse 5040 AIO	8.3 HF, 8.4
	Wyse 3010 thin client	Firmware version 8.5_108
	Wyse 3020 thin client	
	Wyse 5010 thin client (ThinOS, PCOIP)	
	Wyse 7010 thin client	
	Wyse 3030 LT thin client	
	Wyse 5060 thin client	
	Wyse 3040 thin client	
	Wyse 5070 thin client	

Operating System	Device Type	Build number
	Wyse 5070 Extended thin client	
Teradici	Wyse 5030 PCoIP zero client Wyse 7030 PCoIP zero client Wyse 5050 AIO	Threadx 5.x Threadx 6.x

D

Wireless profiles password editor

This Wireless profiles password editor is used to capture the wireless profiles and edit the passwords. The profiles are saved in an XML file. The same XML file can be used to configure the Wyse Management Suite through Cloud Client Manager.

ⓘ **NOTE:**
.NET Framework 4.5 must be installed to run this tool on any Windows operating system or Windows Embedded operating system.

Topics:

- Configuring windows wireless profile
- Configuring the Wireless Profiles Password Editor
- Limitations of Wireless Profiles Password Editor

Configuring windows wireless profile

To configure the windows wireless profile, do the following

1   Go to, **C:\Program files\Wyse\WDA\bin\<DWirelessProfileEditor.exe>**.
2   Right-click the .exe file and select the **Run as administrator** option.
    The **Wireless Profiles Password Editor** window is displayed.
3   Click **Browse** and select the location to save the new XML profile.
4   Click **Save**.
5   From the **Profiles** drop-down list, select the wireless network.
    Click **Change password** to change the password if required.
6   Click **Export WIFI Profiles** to save the profile.

    ⓘ **NOTE: The exported file can be imported from the Wyse Management Suite Apps & data inventory page to push it to the devices.**

Configuring the Wireless Profiles Password Editor

To configure the wireless profiles password editor, do the following:

1   Go to, **C:\Program files\Wyse\WDA\bin\<DWirelessProfileEditor.exe>**.
2   Right-click the .exe file and select the **Run as administrator** option.
    The **Wireless Profiles Password Editor** window is displayed.
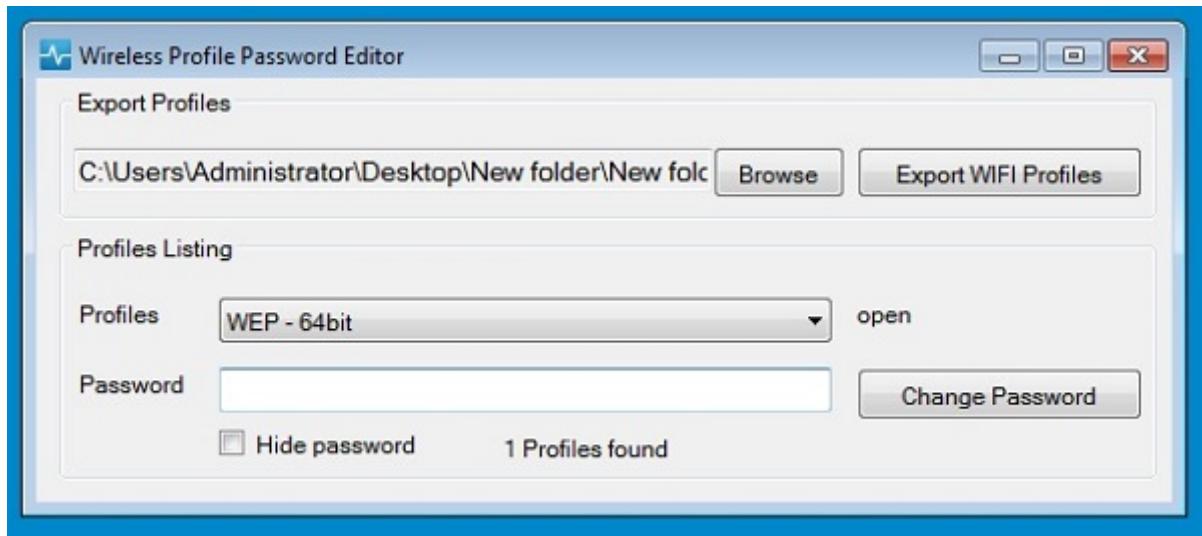
Figure 19. Wireless Profiles Password Editor

3   Click **Browse** and select the location to save the new XML profile.

4   Click the **Export WIFI Profiles** option.

The current wireless profile is exported to the **Profiles** tab. The current wireless connection password is populated in the **Password** tab.

5   Edit the password and click the **Change Password** option.

Changed password is encrypted and saved to the XML profile.

6   On the server side of Wyse Management Suite console, click **App & Data** tab. For more information see Managing file repository

Limitations of Wireless Profiles Password Editor

The following are the limitations of Wireless Profiles Password Editor:

· Passwords are valid only for the following authentication types:

– WPAPSK

– WPA2PSK

· Passwords do not exist for the following enterprise authentication profile types:

– WPA

– WPA2

Create and configure DHCP option tags

To create a DHCP option tag, do the following:

1   Open the Server Manager.
2   Go to **Tools**, and click **DHCP option**.
3   Go to **FQDN** > **IPv4** and right-click **IPv4**.
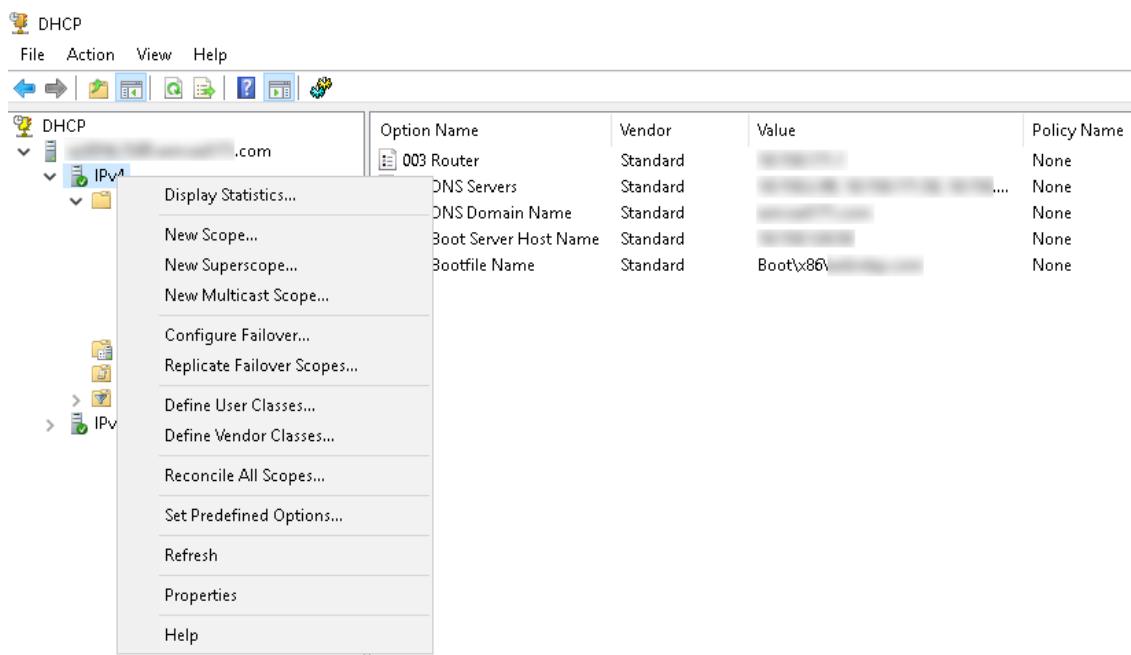
Figure 20. DHCP

4   Click **Set Predefined Options**.
    The **Predefined Options and Values** window is displayed.
5   From the **Option class** drop-down list, select the **DHCP Standard Option** value.
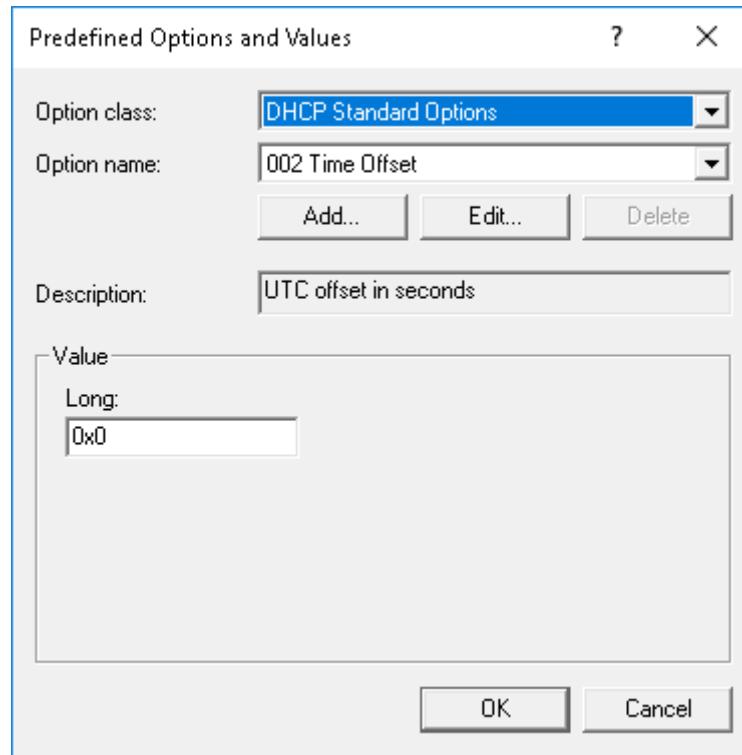
Figure 21. Predefined Options and Values

6   Click **Add**.
     The **Option Type** window is displayed.
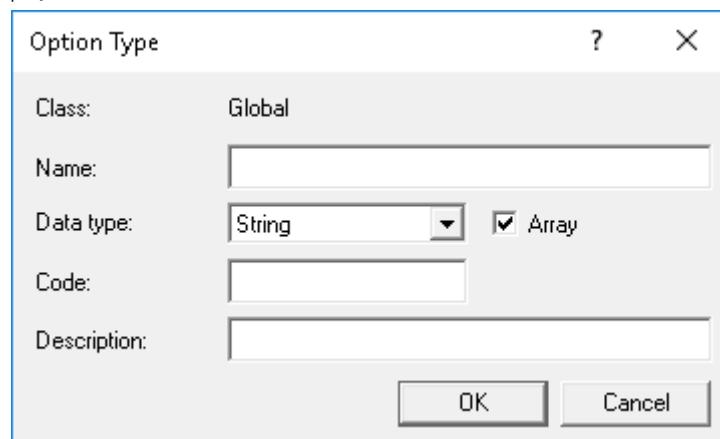
Figure 22. Option Type

The options must be either added to the server options of the DHCP server or scope options of the DHCP scope.

Configuring the DHCP option tags

- To create the 165 Wyse Management Suite server URL option tag, do the following:

  a   Enter the following values, and click **OK**.
       – Name—WMS
       – Data type—String
       – Code—165

    – Description—WMS_Server

b   Enter the following value, and then click **OK**.

    String—`WMS FQDN`

    For example, WMSServerName.YourDomain.Com:443
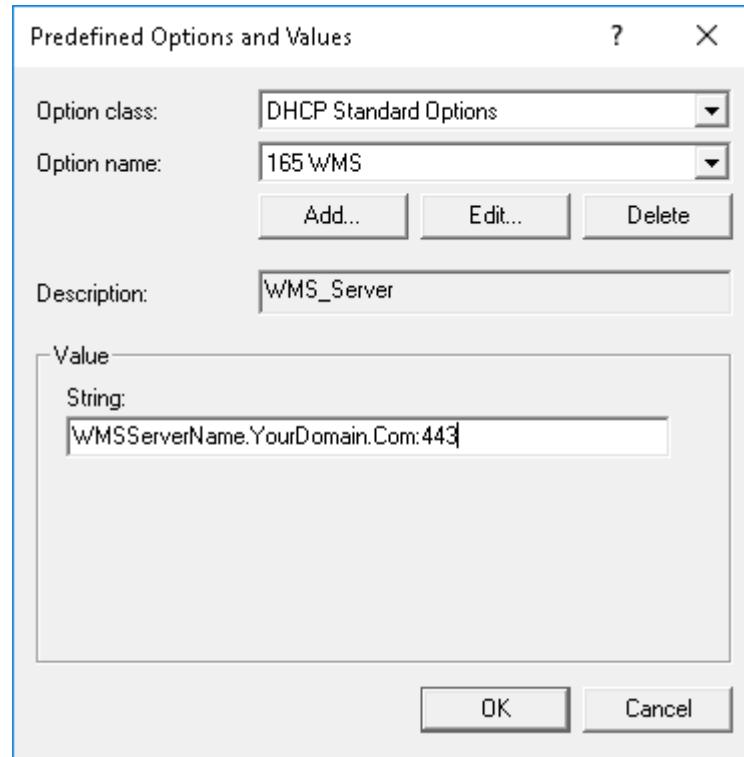
Figure 23. 165 Wyse Management Suite server URL option tag

- To create the 166 MQTT server URL option tag, do the following:

    a   Enter the following values, and click **OK**.
        – Name—MQTT
        – Data type—String
        – Code—166
        – Description—MQTT Server

    b   Enter the following value, and click **OK**.

        String—`MQTT FQDN`

        For example, WMSServerName.YourDomain.Com:1883
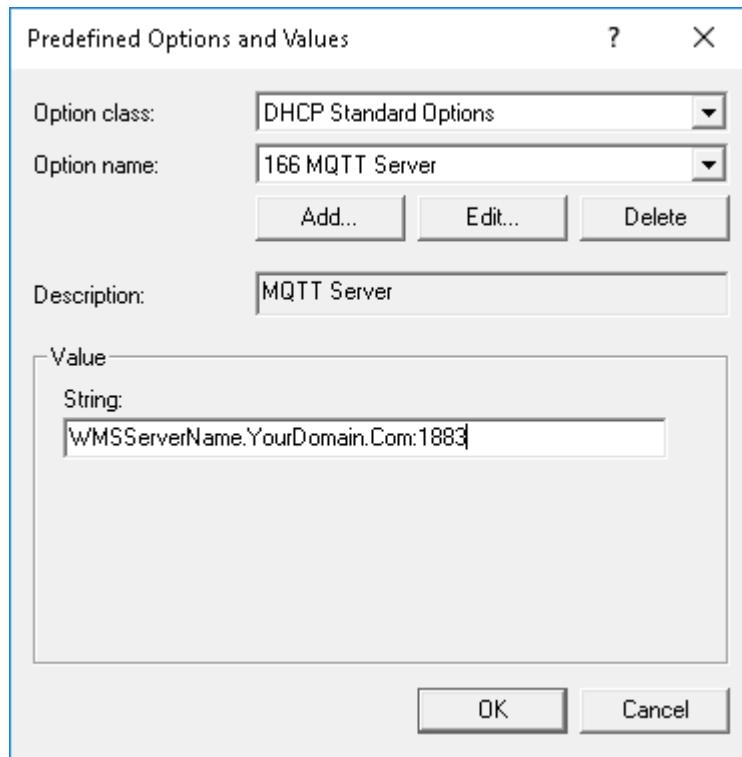
Figure 24. 166 Wyse Management Suite server URL option tag

• To create the 167 Wyse Management Suite CA Validation server URL option tag, do the following:

    a   Enter the following values, and click **OK**.
  – Name—CA Validation
  – Data type—String
  – Code—167
  – Description—CA Validation

    b   Enter the following values, and click **OK**.

      String—TRUE/FALSE
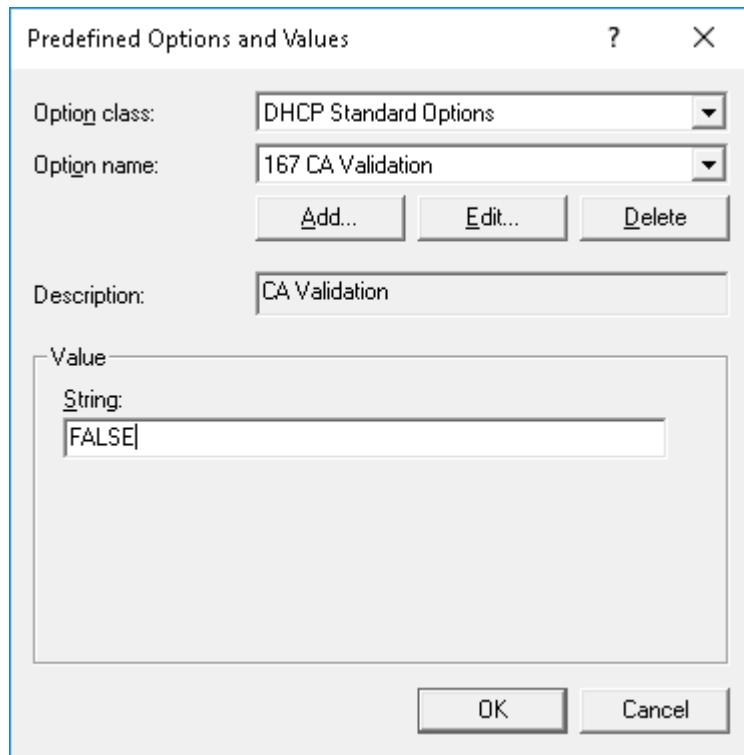
Figure 25. 167 Wyse Management Suite server URL option tag

- To create the 199 Wyse Management Suite Group Token server URL option tag, do the following:

  a Enter the following values, and click **OK**.
     - Name—Group Token
     - Data type—String
     - Code—199
     - Description—Group Token
  b Enter the following values, and click **OK**.

     String—defa-quarantine
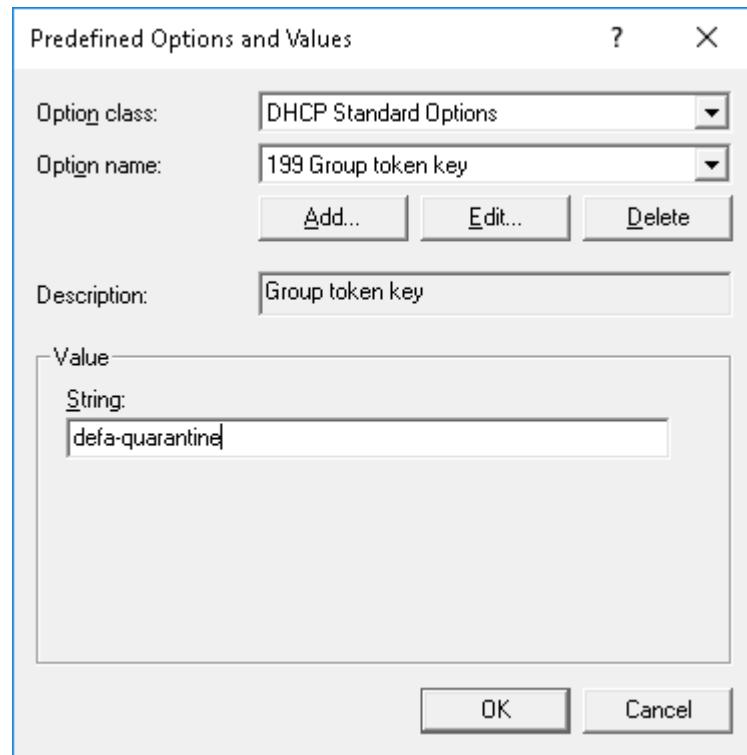
Figure 26. 199 Wyse Management Suite server URL option tag

Create and configure DNS SRV records

To create a DNS SRV record, do the following:

1. Open the Server Manager.
2. Go to **Tools**, and click **DNS option**.
3. Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** > **_tcp** and right-click the **_tcp option**.
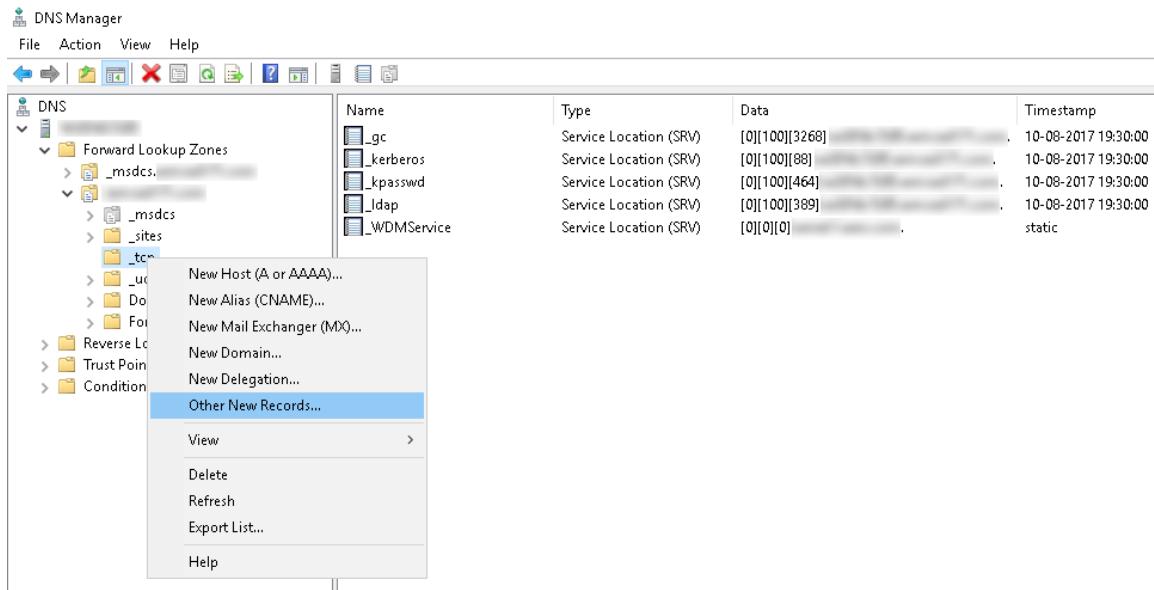

Figure 27. DNS manager

4. Click **Other New Records**.
   The **Resource Record Type** window is displayed.
5. Select the **Service Location (SRV)**, click **Create Record**, and do the following:
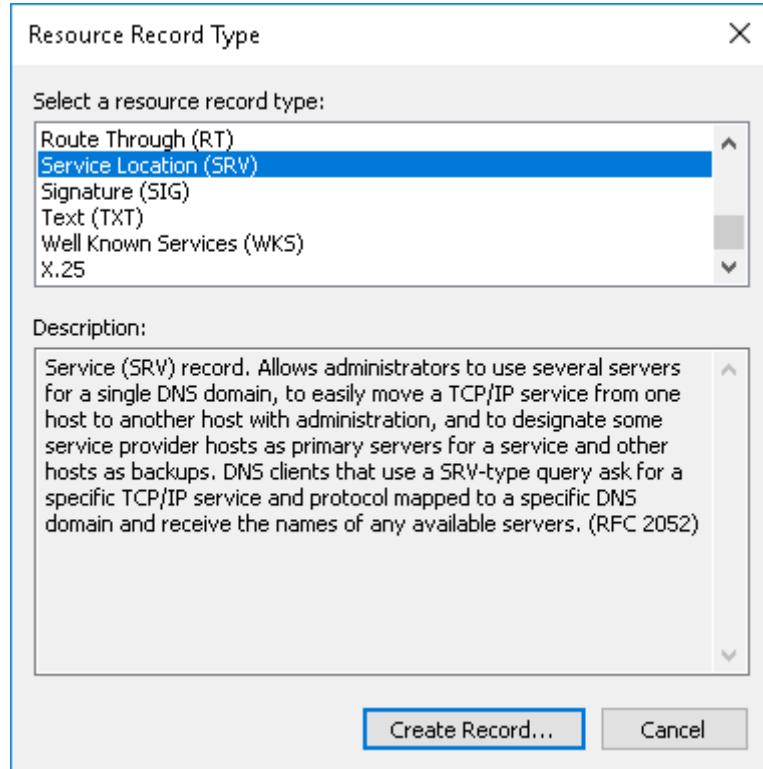
Figure 28. Resource Record Type

   a   To create Wyse Management Suite server record, enter the following details and click **OK**.

- Service—_WMS_MGMT
- Protocol—_tcp
- Port number—443
- Host offering this service—FQDN of WMS server
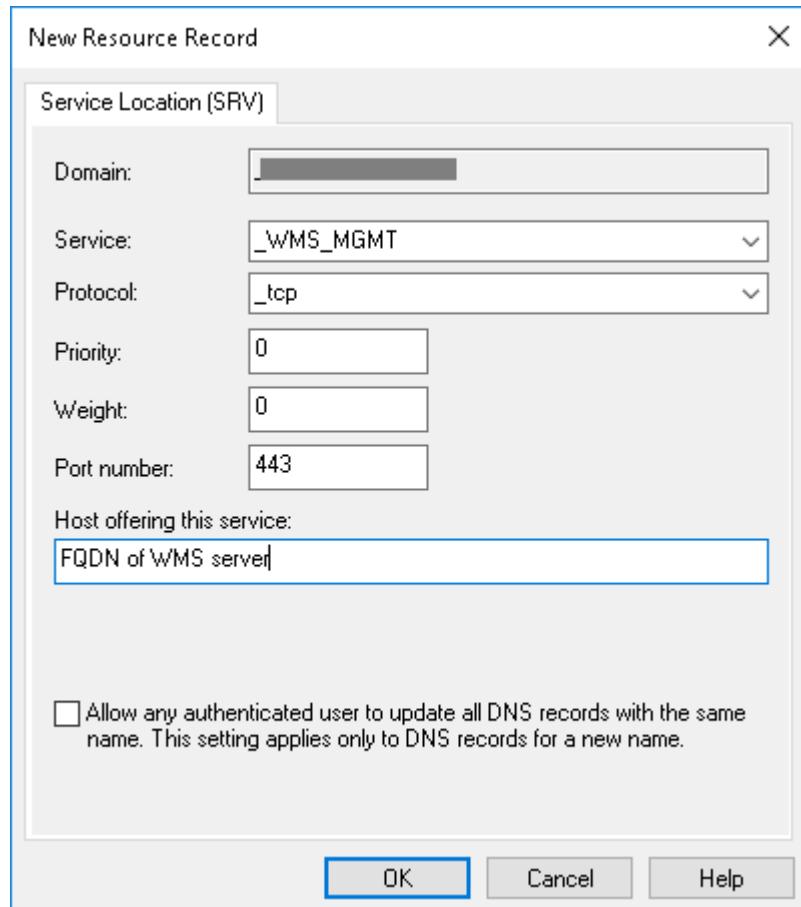
Figure 29. _WMS_MGMT service

b To create MQTT server record, enter the following values, and then click **ÓK**.

- Service—_WMS_MQTT
- Protocol—_tcp
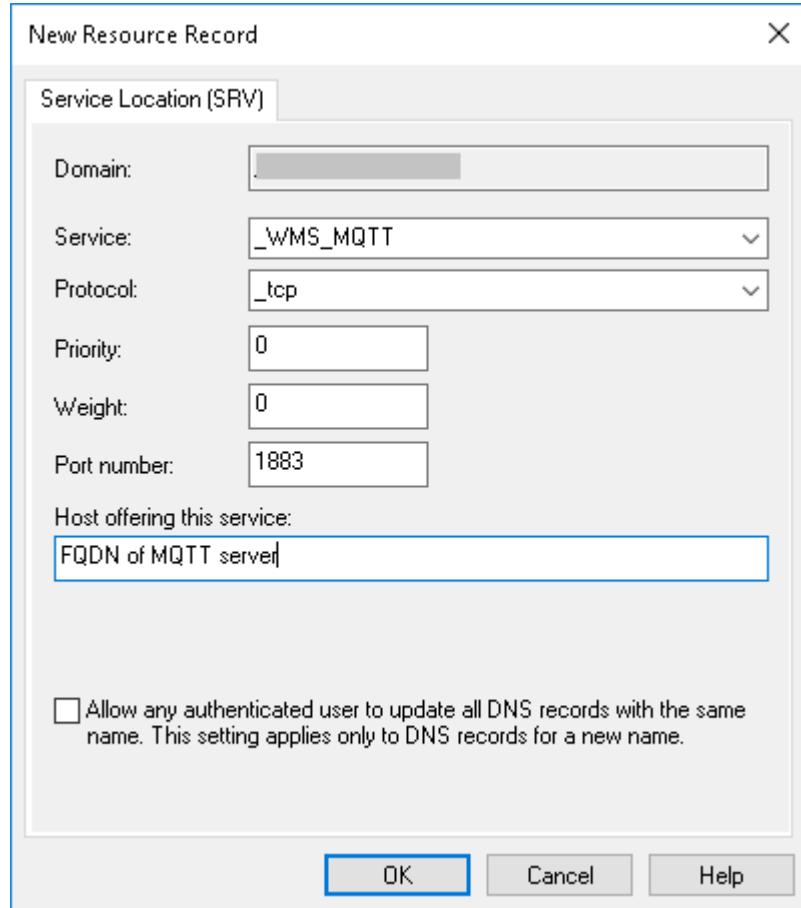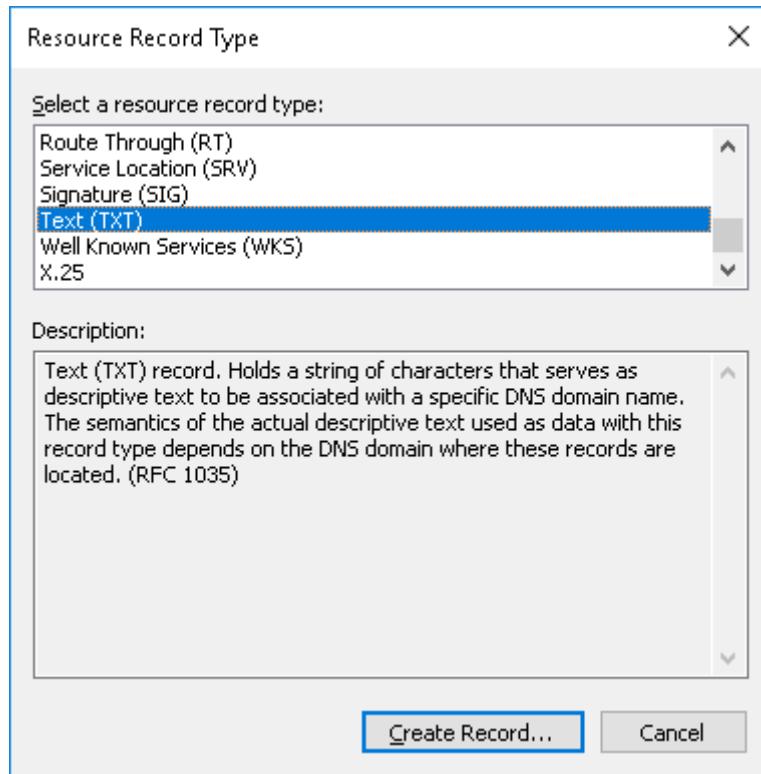- Port number—1883
- Host offering this service—FQDN of MQTT server

Figure 30. _WMS_MQTT service

6   Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** and right-click the domain.

7   Click **Other New Records**.

8   Select **Text (TXT)**, click **Create Record**, and do the following:

Figure 31. Resource Record Type

    a   To create Wyse Management Suite Group Token record, enter the following values, and click **OK**.

- Record name—_WMS_GROUPTOKEN
- Text—WMS Group token
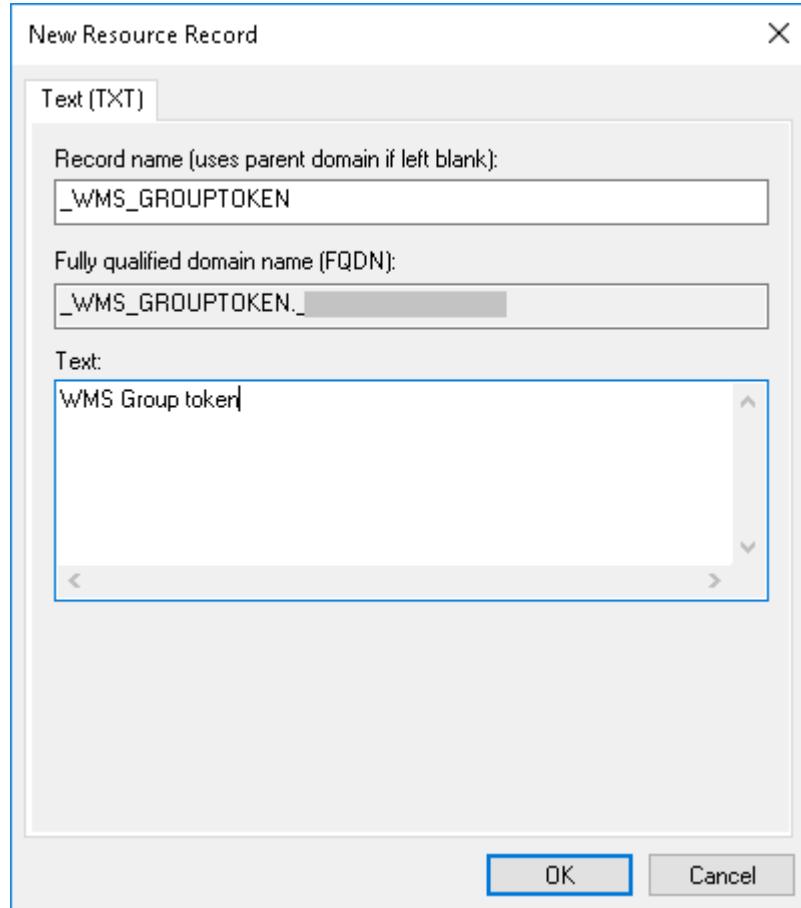
Figure 32. _WMS_GROUPTOKEN record name

b To create Wyse Management Suite CA validation record, enter the following values, and then click **OK**.
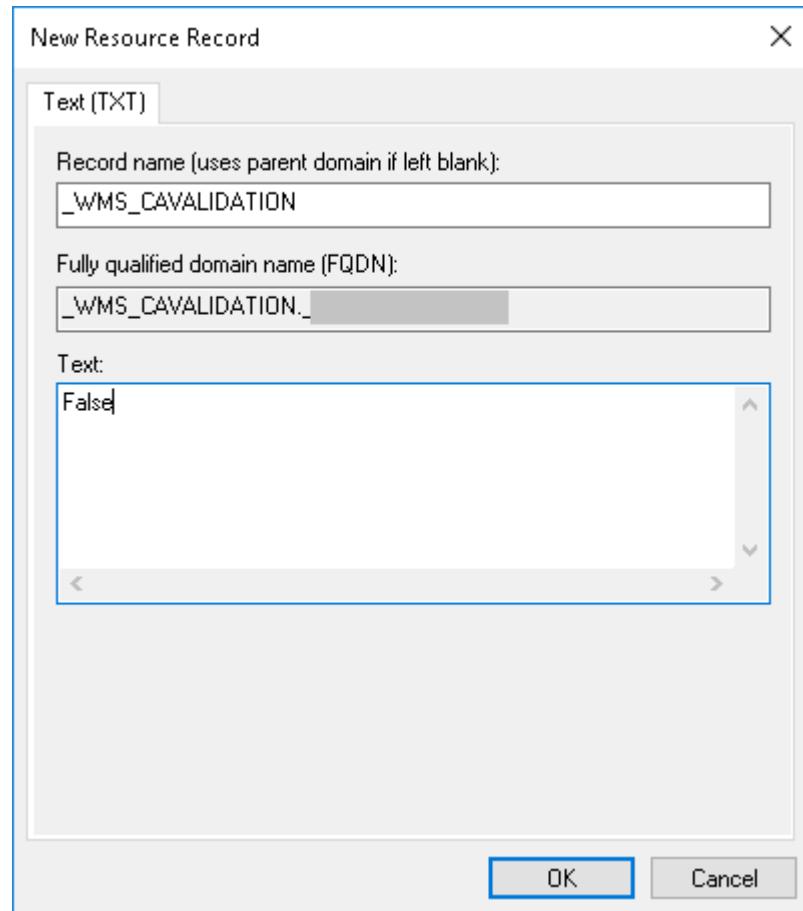
- Record name—_WMS_CAVALIDATION
- Text—TRUE/FALSE

Figure 33. _WMS_CAVALIDATION record name

Steps to change the host name to IP address

Steps to change the host name to IP address when host name resolution fails, to the following:

1   Open the DOS prompt in elevated Admin mode
2   Change the directory to `C:\Program Files\DELL\WMS\MongoDB\bin.`
3   Enter the command, `mongo localhost -username stratus -p --authenticationDatabase admin`
     Output—MongoDB shell version v3.4.10
4   Enter the password.
     Output—
     · connecting to: mongodb://127.0.0.1:27017/localhost
     · MongoDB server version: 3.4.10
5   Enter : use stratus
     Output—switched to db stratus
6   Enter the command, `> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, {$set : {'value' : "https://IP:443/ccm-web"}} )`
     Output—{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7   Enter the command, `> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})`
     Output—{ "_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }