

Dell Wyse Management Suite

Version 1.0 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.

Chapter 1: Introduction to Wyse Management Suite.....	7
Chapter 2: Getting started with Wyse Management Suite.....	8
Logging in to Wyse Management Suite on public cloud.....	8
Getting started with Wyse Management Suite on private cloud.....	9
Prerequisites to deploy Wyse Management Suite on private cloud.....	9
Functional areas of management console.....	10
Configuring and managing thin clients.....	10
Chapter 3: Wyse Management Suite dashboard.....	12
Chapter 4: Managing groups and configurations.....	13
Configuring global level policy.....	14
Configuring group level policy.....	14
Configuring device level policy.....	14
Group tree hierarchy.....	15
Adding a group.....	15
Editing a group.....	15
Removing a group.....	15
Unmanaged group.....	16
Configuring ThinOS policy settings.....	16
ThinOS—Wizard mode.....	17
ThinOS—Advanced mode.....	21
Configuring Windows Embedded Standard policy settings.....	49
Configuring system personalization.....	50
Configuring desktop experience.....	53
Configuring network settings.....	53
Configuring security and lockdown settings.....	53
Configuring other settings.....	54
Configuring remote connection settings—Citrix.....	55
Configuring remote connection settings—VMware.....	57
Configuring remote connection settings—RDP.....	58
Configuring remote connection settings—Browser.....	61
Latitude mobile thin client BIOS settings.....	62
Wyse 7040 thin client BIOS settings.....	63
Configuring device information.....	65
Configuring Wyse Easy Setup settings.....	65
Configuring VNC settings.....	66
Configuring domain settings.....	66
Configuring Linux policy settings.....	67
System personalization.....	67
Desktop experience.....	68
Login experience.....	69
Network	70

Security.....	70
Configuring central configuration settings.....	71
Other settings.....	71
VDI global settings.....	72
Remote connection—Citrix.....	73
Remote connection—VMware.....	75
Remote connection—RDP.....	76
Remote connection—Browser.....	77
Configuring advanced settings.....	78
Configuring ThinLinux policy settings.....	78
System personalization.....	79
Desktop experience.....	81
Login experience.....	81
Network.....	82
Configuring security settings.....	82
Central configuration.....	83
Other settings.....	83
VDI Global Settings.....	84
Remote connection—Citrix.....	85
Remote connection—VMware.....	87
Remote connection—RDP.....	88
Remote connection—Browser.....	89
Advanced settings.....	90
Configuring device information.....	90
Configuring Wyse 3040 thin client BIOS settings.....	90
Configuring Wyse Software thin client policy settings.....	92
Configuring system personalization.....	93
Configuring desktop experience.....	96
Configuring network settings.....	96
Configuring security and lockdown settings.....	97
Configuring other settings.....	97
Configuring remote connection settings—Citrix.....	98
Configuring remote connection settings—VMware.....	100
Configuring remote connection settings—RDP.....	101
Configuring remote connection settings—Browser.....	104
Configuring device information.....	105
Configuring VNC settings.....	105
Configuring domain settings.....	106
Chapter 5: Managing devices.....	107
Using filters.....	107
Save current filter.....	108
Registering devices into Wyse Management Suite.....	108
Registering ThinOS thin clients through WDA User Interface.....	109
Registering Windows Embedded Standard thin clients through Wyse Device Agent User Interface..	109
Registering Linux thin clients through Wyse Device Agent User Interface.....	109
Registering devices by using DHCP option tags.....	110
Registering devices by using DNS SRV record.....	111
Viewing and managing device details.....	112
Pulling Windows Embedded Standard or ThinLinux image.....	114

Pulling log file.....	116
Renaming thin client.....	117
Chapter 6: Apps and data.....	118
Configuring app inventory.....	119
Mobile app inventory.....	119
Configuring thin client and Wyse Software thin client app inventory.....	119
Deploying applications to thin clients.....	120
Creating and deploying advanced application policy to thin clients.....	120
Adding Windows Embedded Standard operating system and ThinLinux images to inventory.....	121
Managing ThinOS firmware inventory.....	122
Managing Windows Embedded Standard and ThinLinux image policies.....	122
Managing file repository	123
Changing wallpaper for all devices belonging to marketing group.....	123
Chapter 7: Managing rules.....	125
Registering unmanaged devices.....	125
Creating unmanaged device auto assignment rules	126
Alert Notification.....	127
Chapter 8: Managing Jobs.....	129
Sync BIOS admin password.....	130
Scheduling the image policy.....	130
Scheduling the application policy.....	130
Scheduling the device command job.....	131
Chapter 9: Events.....	132
Viewing a summary of events.....	132
Viewing audit log.....	133
Chapter 10: Managing users.....	134
Adding new admin user.....	135
Editing admin user.....	135
Deactivating admin account.....	136
Deleting admin.....	136
Chapter 11: Portal administration.....	137
Configuring console settings.....	137
Active Directory.....	137
Alert classifications.....	139
External application services.....	139
File repository.....	139
Other settings.....	140
Thin clients.....	140
Two-Factor authentication.....	140
Generating reports.....	141
Multi Tenant.....	142
Configuring account settings.....	143
Custom branding.....	143

License subscription.....	143
System setup.....	143
Appendix A: Installing or upgrading Wyse Device Agent.....	145
Upgrading Wyse Device Agent using Wyse Management Suite application policy.....	145
Installing Wyse Device Agent manually.....	145
Installing or upgrading Wyse Device Agents on ThinLinux and Linux clients.....	146
Appendix B: Wyse Management Suite feature matrix.....	147
Appendix C: Supported thin clients on Wyse management Suite.....	149
Appendix D: Wireless profiles password editor.....	151
Configuring the Wireless Profiles Password Editor.....	151
Limitations of Wireless Profiles Password Editor.....	152
Appendix E: Creating and configuring DHCP option tags.....	153
Appendix F: Creating and configuring DNS SRV records.....	159

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

Getting started with Wyse Management Suite

Topics:

- [Logging in to Wyse Management Suite on public cloud](#)
- [Getting started with Wyse Management Suite on private 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**.

Getting started with Wyse Management Suite on private cloud

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	<p>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.</p> <ul style="list-style-type: none">• 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)		<p>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.</p>
Supported browsers	<ul style="list-style-type: none">• 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.
- 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:

About this task

- The **Dashboard** page provides information about each functional area of the system.
- The **Groups** 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 functions, 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 Admin** page enables administrators 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 heirarchy, for example marketing, sales, and engineering, or based on the location hierarchy, for example, country, state, and city.

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.
- 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.

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. 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.

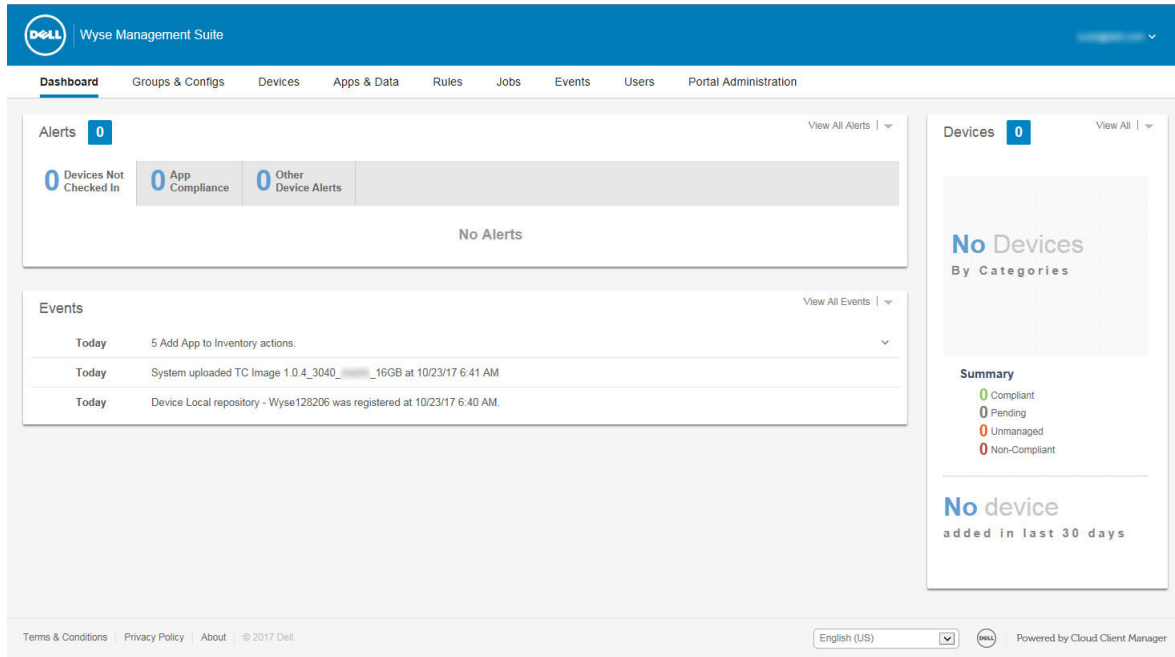


Figure 1. Dashboard

Dashboard page includes the following links:

- **Alerts**—Displays the summary of all the alerts. You can navigate to the functional areas of the system that requires your attention. The **Alerts** section displays the following attributes:
 - **Devices Not Checked In**
 - **App Compliance**
 - **Other Device Alerts**
 To view the detailed list of all the alerts, click **View All Alerts**.
- **Events**—Displays the summary of events that have occurred in the last few days. To view the detailed list of all the events, click **View All Events**.
- **Devices**—Displays 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, click **View All** which redirects to the Device page.
- **User Preferences**— On the upper-right corner, click the login drop-down menu to perform the following actions:
 - **Alerts**—Select the alert classification and the notification type.
 - **Policies**—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 ThinOS policy settings.
 - **Page Size**—Enter the number of options to be displayed on the screen. The range is 10–100.

Managing groups and configurations

Prerequisites

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 policy and categorize devices based on your requirements. For example, devices may be grouped based on job functions, device type, and so on.

About this task

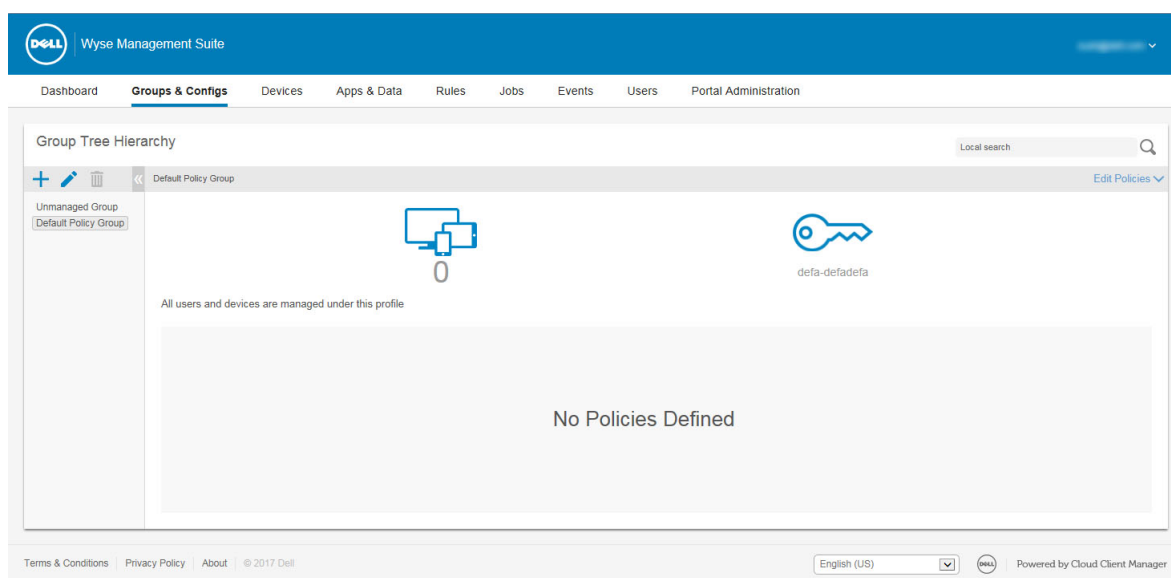


Figure 2. Groups and configuration

For each group, you can define policies for the following device types:

- **ThinOS**
- **WES**
- **Linux**
- **ThinLinux**
- **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.

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.

i 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 ThinLinux and ThinOS, you must restart the device for changes to take effect.

The policies are enforced in the following precedence:

- Global
- Group
- Device

Topics:

- [Configuring global level policy](#)
- [Configuring group level policy](#)
- [Configuring device level policy](#)
- [Group tree hierarchy](#)
- [Unmanaged group](#)
- [Configuring ThinOS policy settings](#)
- [Configuring Windows Embedded Standard policy settings](#)
- [Configuring Linux policy settings](#)
- [Configuring ThinLinux policy settings](#)
- [Configuring Wyse Software thin client policy settings](#)

Configuring global level policy

About this task

To configure a global level policy, do the following:

Steps

1. In the **Groups** page, from the **Edit Policies** drop-down menu, select a device type you want to configure.
In the left pane, the policy settings of the respective device type are displayed.
2. Click the policy setting you want to configure, and then click **Configure this item**.
3. Click **Save and Publish**.

Configuring group level policy

About this task

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

Steps

1. In the **Groups** 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.
In the left pane, the policy settings of the device type are displayed.
3. Click a policy setting and then click **Configure this item**.
4. Click **Save and Publish**.

Configuring device level policy

About this task

To configure a device level policy, do the following:

Steps

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

Group tree hierarchy

Group tree hierarchy consists of the following options:



- Add Group
- Edit Group
- Remove Group

Adding a group

About this task

To add a group, do the following:

Steps

1. On the **Groups & Configs** page, in **Group Tree Hierarchy**, click the **+** icon.
2. In the **Add New Groups** 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, in **Group Token**, select the **Enabled** check box.
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. Click **Save**.
The group is added to the list of available groups on the **Groups & Configs** page.

Editing a group

About this task

To edit a group, do the following:

Steps

1. On the **Groups & Configs** page, in **Group Tree Hierarchy**, click the **Edit Group** 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.
4. Enter the group token.
The devices can be registered to a group by entering the group token which is available on the device registration screen.
5. Click **Save**.

Removing a group

About this task

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

Steps

1. In the **Groups** page, under **Group Tree Hierarchy**, click the **Remove Group** icon.

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

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 target group.

2. Click **Remove Group**.

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 configure an unmanaged group, do the following:

1. Click **Edit group**.

The **Editing Unmanaged Group** page is displayed.

The following options are displayed on the page:

- **Group Name**—Displays the name of the group.
- **Description**—Displays a brief description of the group.
- **Group Token**—Select this option to enable group token.

2. Click **Save**.

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

Configuring ThinOS policy settings

NOTE: In the document, the term **8.5+** indicates that the specific policy setting is applicable for ThinOS 8.5 and later versions.

1. Select a group and click **Edit Policies**.
2. Click **ThinOS**.

The **Select ThinOS Configuration Mode** window is displayed.

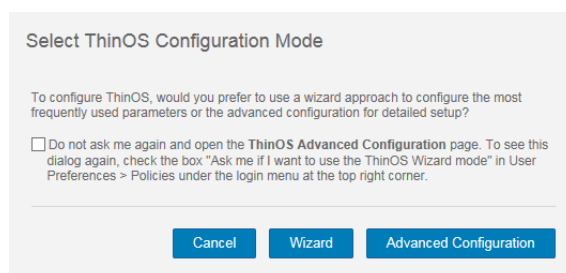


Figure 3. Select ThinOS configuration mode

3. 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.

4. After configuring the options, 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.

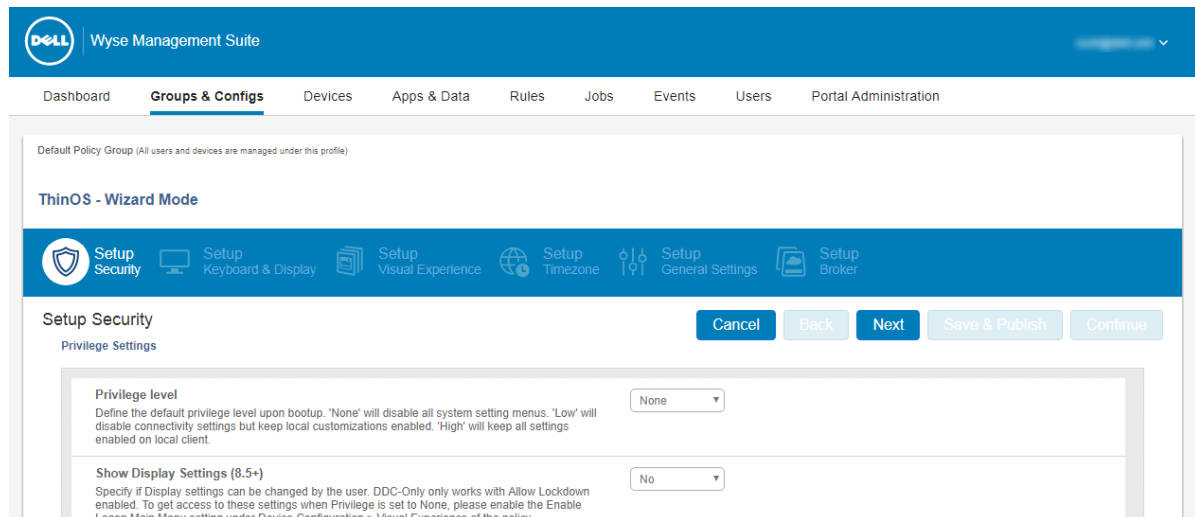


Figure 4. ThinOS—Wizard mode

- 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.

Setup security

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

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: <ul style="list-style-type: none">• None—Disables all the system setting option.• High—Disables the connectivity settings except local customization.

Table 2. Configuring Privilege Settings (continued)

Option	Description
	<ul style="list-style-type: none"> 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.
Enable Admin mode	Select this option to access the admin mode by entering the user name and 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.
Auto-install certificates	Select this option to automatically install the certificates.
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 .
Auto detect monitors—ThinOS 8.5+	<p>Select the check box to detect the total number of monitors connected to the system.</p> <p>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.</p>

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. Visual experience

Parameter	Description
Classic Desktop vs Zero Launchpad	Allows you 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.
Action after all session exit	Allows you to define the action after you close the last active session. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none">• None• Sign-off automatically• Shut down the system automatically• Restart the system automatically
Enable Zero toolbar activation in left margin	Allows you to select any one of the following options to activate the Zero toolbar: <ul style="list-style-type: none">• No• On mouse over after specified seconds• Only after clicking
Number of seconds before toolbar is activated	Allows you to set the time (in seconds) before the toolbar is activated. Select one of the following timings based on your preference: <ul style="list-style-type: none">• 0.5 seconds• 1 second• 1.5 seconds• 2 seconds
Disable Hotkey (CTRL+ALT+UP) to show toolbar	Allows you to disable the hotkey from showing the toolbar when the key is pressed.
Always disable toolbar when only one session available	Allows you to disable the toolbar when a single session is available.
Disable Home Icon	Allows you to disable the home icon.
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.
Auto-hide toolbar after specified seconds	Allows you to automatically hide the toolbar after a specified time. From the drop-down menu, select the timings (0.5–10.0 seconds).
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 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 using this option.

Configuring timezone

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

Table 6. 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.

-  **NOTE:**
- Remote firmware imaging from the cloud is supported with the ThinOS firmware version 8.0_037 or later.

Table 7. 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 8. 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	<p>This option maps the specific firmware versions to different platform types.</p> <p>To map a platform type to a specific firmware version, do the following:</p> <ol style="list-style-type: none">From the Platform Type drop-down menu, select a platform.From the Firmware to auto-deploy drop-down menu, select a firmware version. <p>The list of platform types and the number of firmware versions currently uploaded to the File Repository Inventory page are displayed.</p>


Table 9. 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.

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 10. 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: <ul style="list-style-type: none">• 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.

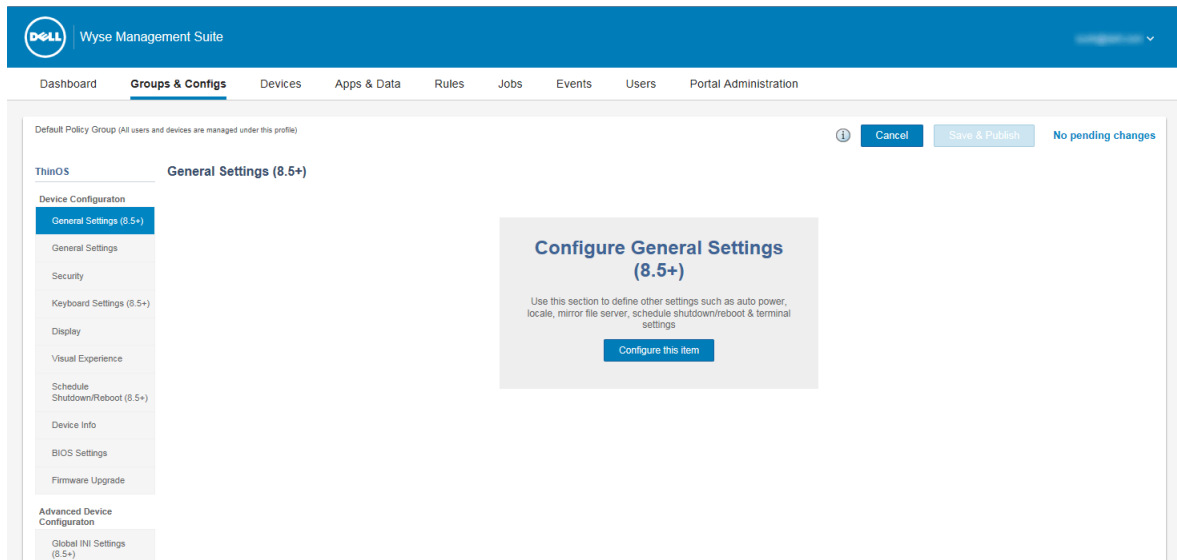


Figure 5. ThinOS—Advanced mode

- **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—ThinOS 8.5+

Use this page to configure the thin client general settings, such as auto power settings, local settings, mirror file server settings, and terminal settings for ThinOS devices.

Table 11. 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 12. 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 menu, 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 menu, select the font files added in the file repository.

Table 13. 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 14. 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. You must 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 menu 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 menu 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.

Configuring general settings—ThinOS

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

Table 15. 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 16. 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—ThinOS

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

Table 17. 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 18. 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: <ul style="list-style-type: none"> 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 19. 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.

Table 19. Configuring administrator mode (continued)

Option	Description
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 20. 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 21. 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 22. 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.

Table 22. Configuring VNC settings (continued)

Option	Description
Prompt user on start	Select this option to perform the shadowing process on the terminal.
Query user timeout	Enter the total amount of time in seconds to accept or reject the shadowing session. The range is 10–600 seconds.
Prompt 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 23. 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—ThinOS 8.5+

Use this page to configure the keyboard layouts, and the behavior of keyboard shortcuts.

Table 24. Configuring keyboard settings

Option	Description
Character Set	Select this option to set an appropriate character set. From the drop-down menu, select your preferred character set.
Keyboard Layout	Select this option to set an appropriate keyboard layout. From the drop-down menu, 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 menu, 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 menu, select one of the following options based on your preference: <ul style="list-style-type: none"> • 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.
Win + L	Press the Win+L keys to lock the system.

Table 24. Configuring keyboard settings (continued)

Option	Description
Alt-Tab	Press the Alt-Tab keys to lock the system.

Display

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

Table 25. Display

Parameter	Description
Monitor Resolution	Allows you 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.
Monitor Rotation	Allows you to define the direction—Left, Right, or None—to enable the rotation. From the drop-down menu, select the appropriate rotation direction. NOTE: If you select an unsupported resolution, the device ignores the setting.
Desktop Color Depth	Allows you to set the color depth for your desktop. From the drop-down menu, select the color depth—16-bit or 32-bit.
Enable Dual Monitor	Allows you to enable the dual monitor functionality. From the Display Mode drop-down menu, select either Mirror Mode or Span Mode .

Configuring visual experience settings—ThinOS

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

Table 26. 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.
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 27. 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.

Table 27. Configuring visual experience (continued)

Option	Description
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • None • Sign-off automatically • Shut down the system automatically • Restart the system automatically.

Schedule shutdown or reboot settings—ThinOS 8.5+

Use this page to configure a scheduled restart or shutdown.

Table 28. 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 shut down.
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 device details.

Table 29. 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—ThinOS

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

Table 30. System configuration

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

Table 31. 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 32. 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 33. 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 34. 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.

Table 34. Configuring USB (continued)


Option	Description
	 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 35. 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 enable USB devices to wake the system from OFF state or from the hibernate state.

Table 36. Reboot schedule

Option	Description
Reboot Option	Some BIOS settings require system reboot. When the reboot later option is selected, devices restart when the current time matches the set time. From the drop-down list, you can select any of the following options: <ul style="list-style-type: none"> • Reboot immediately • Reboot later • Do not reboot


Configuring firmware upgrade

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

Table 37. 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: <ul style="list-style-type: none"> • 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.

Table 37. Configuring firmware upgrade (continued)

Option	Description
	<p> 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.</p>
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	<p>This option maps the specific firmware versions to different platform type.</p> <p>To map a platform type to a specific firmware version, do the following:</p> <ol style="list-style-type: none"> 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. <p>The list of platform types and the number of firmware versions currently uploaded to the File Repository Inventory page are displayed.</p>

Configuring global INI settings—ThinOS 8.5+

Use this page to configure global INI settings.

Table 38. Configuring global INI settings

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

Configuring central configuration settings—ThinOS

Use this section to specify a file server where the thin client checks for configuration and image updates.

Table 39. 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—ThinOS

Use this page to configure additional settings which are 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 40. 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—ThinOS

Use this page to configure the thin client remote connection settings, such as addresses and credentials for broker and direct connections.

Table 41. 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: <ul style="list-style-type: none">• 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.

Table 41. Configuring connection broker settings (continued)

Option	Description
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 42. 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.
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. i 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: <ul style="list-style-type: none"> • Play locally • Play on remote computer • Do not Play

Table 43. 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. i 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.

Table 43. Session behavior defaults (continued)

Option	Description
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 44. 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. <ul style="list-style-type: none"> • Multimedia redirection • Enable Session Reliability • Enable progressive Display • Enable ICA Ping • Offscreen support

Table 45. Configuring peripheral behavior

Option	Description
Auto-connect selected local	Select this option to automatically connect the following peripherals: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • No • Yes, redirect all USB devices • Yes, but exclude some devices

Table 45. Configuring peripheral behavior (continued)


Option	Description
	 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 46. 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+

Use this page to configure VDI global settings for a session.


Table 47. 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.

Table 47. Configuring local resources settings (continued)

Option	Description
Disks Read Only	Select this option to enable read only disks.
Enable USB Redirection	<p>Select this option to redirect the USB drives to the remote session. From the drop-down menu, select your preferred option. If Exclude some devices option is selected, you can exclude the following devices from the session:</p> <ul style="list-style-type: none"> • Exclude disk devices • Exclude audio devices • Exclude printer devices • Exclude video devices


Table 48. 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	<p>Select this option to use the fast disconnect key.</p> <p> NOTE: To disconnect from the sessions, press the F12 key.</p>

Configuring USB redirection settings—ThinOS 8.5+

USB redirection (Universal Serial Bus redirection) is a technology that allows 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 this page to force redirect the USB connected devices to the remote session.

Table 49. USB redirection settings

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

Configuring third party authentication settings—ThinOS 8.5+

Use this page to configure Single Sign-On (SSO) authentication settings.

Table 50. 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: <ul style="list-style-type: none">• Imprivata• Caradiam• SecureMatrix• HealthCast

Table 51. 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 52. 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.

Table 52. Configuring imprivata settings (continued)

Option	Description
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 53. 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 54. 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 55. 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.

Table 55. Configuring HealthCast settings (continued)

Option	Description
Client Certificate	From the drop-down menu, select your preferred option. The certificates are uploaded to the file repository.

Configuring citrix broker connection settings—ThinOS 8.5+

Use this page to configure the citrix broker connection settings.

Table 56. 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.
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 57. 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 58. 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.

Table 58. Configuring multi logon settings (continued)

Option	Description
Sequential Domain	Select this option to choose the domains in sequential order which are listed in the DomainList option.

Configuring citrix HDX connection settings—ThinOS 8.5+

Use this page to define VDI global settings for citrix connections.

Table 59. 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.
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 60. 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—ThinOS 8.5+

Use this page to configure the VMware broker connection settings.

Table 61. Configuring basic settings

Option	Description
Broker Server	Enter the broker server host name or IP address.


Table 61. Configuring basic settings (continued)

Option	Description
	 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 PCoIP connections—ThinOS 8.5+

Use this page to configure the VDI global settings for PCoIP connections.



Table 62. 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—ThinOS 8.5+

Use this page to configure the Microsoft broker connections.

Table 63. 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—ThinOS 8.5+

Use this page to configure the Microsoft RDP connection settings.


Table 64. 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 65. 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 66. 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.
Enable RDP H.264	Select this option to enable the H.264 encoding process for the RDP connections.

Configuring vWorkspace broker connection settings—ThinOS 8.5+

Use this page to configure the vWorkspace broker connection settings.



Table 67. 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—ThinOS 8.5+

Use this page to configure the AWS broker connection settings.

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 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—ThinOS 8.5 and later versions

Use the direct RDP connection settings page to configure the RDP connections which can be accessed on the thin client.

Table 69. 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.

Table 69. Configuring basic settings (continued)

Option	Description
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 70. 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 71. 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: <ul style="list-style-type: none"> • Do not Play • 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 72. 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. <div> <i>i</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. </div>

Table 73. Configuring terminal gateway settings

Option	Description
Use Terminal Server Gateway	<p>Select this option to specify the Windows terminal server login details. If enabled, enter the following details:</p> <ul style="list-style-type: none"> • RD host name or IP address • RD user name • RD password • RD domain name

Configuring direct ICA connection settings—ThinOS 8.5+

Use this page to configure the ICA connections which can be accessed on the thin client.

Table 74. 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	<p>Enter the password for the application login.</p> <p> 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.</p>
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 75. 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	<p>Select this option to set the resolution for your monitor. From the drop-down menu, select the appropriate resolution for your monitor.</p> <p> NOTE: If you select an unsupported resolution, the device ignores the setting.</p>

Table 76. 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.


Table 76. Configuring local resources (continued)

Option	Description
Map SmartCards	Select this option to redirect the smartcards to the remote session.

Table 77. 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 78. 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.  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—ThinOS 8.5+

Use this page to configure global printer settings.

Table 79. 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—ThinOS 8.5+

Use this page to configure a new printers.

Table 80. Configuring printer select

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

Table 80. Configuring printer select (continued)

Option	Description
	<ul style="list-style-type: none"> Local printer LPD printer SMB printer
Local Printer	From the drop-down menu select the local printer connection.

Table 81. 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: <ul style="list-style-type: none"> 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—ThinOS 8.5+

Use this page to configure WLAN global settings.

Table 82. 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.

Table 82. Configuring WLAN global settings (continued)

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—ThinOS 8.5+

Use this page to configure the thin client WLAN connections.

Table 83. 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: <ul style="list-style-type: none"> • 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 84. 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 85. 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.

Table 85. Configuring IEEE 802.1X settings for WPA-Enterprise and WPA2-Enterprise (continued)

Option	Description
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 Windows Embedded Standard policy settings

To configure the policy settings for Windows Embedded Standard (WES) devices, do the following:

1. Select a group and click **Edit Policies**.
2. Click **WES**.
3. After configuring the options, click **Save and Publish**.

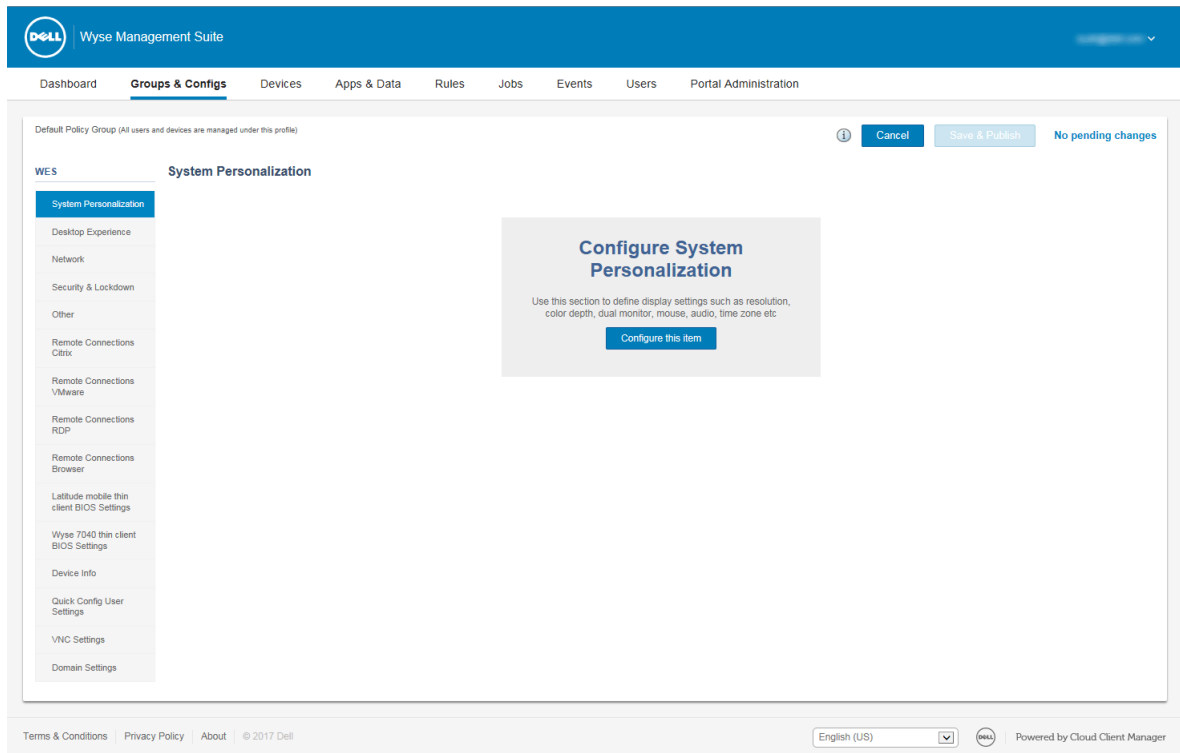


Figure 6. Windows Embedded Standard

The Windows Embedded Standard thin client policy settings include the following options:

- System Personalization
- Desktop Experience
- Network
- Security and Lockdown
- Other
- 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

Configuring system personalization

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

Table 86. Configuring display options

Option	Description
Enable Dual Monitor	Select this option to enable the dual monitor functionality.

Table 86. Configuring display options (continued)

Option	Description
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 for your monitor. From the drop-down menu, select one of the following options based on your preference: <ul style="list-style-type: none"> • Landscape • Portrait • Landscape—flipped • Portrait—flipped

Table 87. 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.
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 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: <ul style="list-style-type: none"> • 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.

Table 88. Configuring mouse and mouse pointer 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.

Table 88. Configuring mouse and mouse pointer options (continued)

Option	Description
Click Lock	Select this option to highlight or drag function without holding down the mouse button. 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. i 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. i 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 89. 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 90. 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 91. Configuring desktop experience

Option	Description
Desktop Wallpaper	<p>Select this option to set a wallpaper for your desktop.</p> <p>After you enable the desktop wallpaper option, do the following:</p> <ul style="list-style-type: none">From the Wallpaper File drop-down list, select a wallpaper for your desktop. <p>NOTE: Select a wallpaper only from the list of images uploaded to the file repository.</p> <ul style="list-style-type: none">From the Wallpaper Layout drop-down list, select any of the following layouts for your desktop wallpaper:<ul style="list-style-type: none">CenterTileStretchFill
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 92. Configuring network settings

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

Configuring security and lockdown settings

Use this page to configure the security and lockdown settings.

Table 93. Configuring security and lockdown settings

Option	Description
Install Certificates	Select this option to view the certificates that are uploaded to the file repository.

Table 93. Configuring security and lockdown settings (continued)

Option	Description
Disable USB Storage Device Access	Select this option to enable or disable the USB mass storage device access for non-admin users.
Disable Print Screen	Select this option to enable or disable the print screen functionality for non-admin users.
Disable Task Manager	Select this option to enable or disable the task manager access for non-admin users.

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 94. Configuring appliance mode

Option	Description
Appliance Mode	<p>Select this option to set an appropriate mode for the appliance. From the drop-down menu, select any of the following options:</p> <ul style="list-style-type: none"> • Off • Generic • VMware View • Citrix • Internet Explorer • RDP

Table 95. Configuring power settings

Option	Description
Device Power Plan	<p>Select this option to choose a power plan for your device. From the drop-down menu, select either of the following options:</p> <ul style="list-style-type: none"> • Balanced • Power Saver

Table 96. 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 97. 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.

Table 97. Configuring power settings when plugged-in (continued)

Option	Description
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 98. Configuring shared drives


Option	Description
Shared Drive	<p>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.</p> <p> NOTE: To delete a shared drive from the list, select the shared drive that you want to remove and click Remove.</p>

Table 99. Configuring clock settings

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

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 100. 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	<p>Select this option to set a connection type. From the drop-down menu, select any of the following options:</p> <ul style="list-style-type: none"> • 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.

Table 100. Basic options (continued)

Option	Description
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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Default User Key Combos Passthrough • On the local desktop • On the remote desktop • In full screen desktops only

Table 101. 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. 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 102. Server options

Option	Description
Logon Method	Select this option to choose a logon method for your Citrix connection. <ul style="list-style-type: none"> • Default Logon Method • Prompt Logon Method

Table 103. 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 104. 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 105. 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: <ul style="list-style-type: none"> • PCOIP • RDP

Table 105. Configuring remote connections—VMware (continued)

Option	Description
	<ul style="list-style-type: none"> 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	<p>Select this option to set the VMware connection window in full screen mode.</p> <p>If you do not select the fullscreen mode, from the drop-down menu, select the Window Size.</p>
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 106. 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.

Table 106. Configuring basic settings (continued)

Option	Description
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 107. Configuring RD gateway

Option	Description
Use RD Gateway settings	<p>Select this option to configure the settings for RD Gateway. After you enable the option, enter the RD Server name for the gateway.</p> <p>From the RD Gateway Logon Method drop-down menu, specify the credentials to validate the connection with the RD Gateway:</p> <ul style="list-style-type: none"> • Ask for password NTLM • Smartcard • Allow me to select later • <p>From the RD Gateway Usage Method drop-down menu, select any of the following ways to use a remote desktop server:</p> <ul style="list-style-type: none"> • 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 108. Configuring display settings

Option	Description
Fullscreen	<p>Select this option to set the connection window in the full screen mode.</p> <p>After the full screen mode is enabled, from the drop-down menu, select the window size.</p>
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)	<p>Select this option to define the screen color depth of the connection.</p> <ul style="list-style-type: none"> • RDP 15-Bit High Color • RDP 16-Bit High Color • RDP 24-Bit True Color • RDP 32-Bit Highest Quality

Table 109. 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. <ul style="list-style-type: none"> • Connect and don't warn me • Do not connect • Warn me

Table 110. 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.

Table 110. Configuring local resources (continued)

Option	Description
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 111. 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 112. Internet Explorer (IE) favorites and trusted site settings


Option	Description
IE Favorite	<p>Select this option to add your favorite and trusted sites. Perform the following steps to add your favorite and trusted sites:</p> <ol style="list-style-type: none"> 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. <p> NOTE: URL must begin with Https:// when the Trusted Sites check box is selected.</p>
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 113. Internet Explorer—IE proxy settings

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

Table 114. Firewall

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

Table 114. Firewall (continued)

Option	Description
Public Firewall	Select this option to enable the public firewall.

Table 115. Aero—valid for Windows Embedded Standard 7

Option	Description
Aero	<p>Select this option to enable the Aero feature for the browser.</p> <p>NOTE: This feature is available only for Windows Embedded Standard 7</p>

Latitude mobile thin client BIOS settings

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

Table 116. System configuration

Parameter	Description
Serial Port 1	<p>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.</p> <ul style="list-style-type: none"> 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 117. USB configuration

Parameter	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 118. Wireless settings

Parameter	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 119. Security settings

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

Table 120. Admin password settings

Parameter	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 121. Power management settings

Parameter	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 122. Auto-On settings

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

Table 123. Reboot schedule

Parameter	Description
Reboot Option	Some BIOS settings require system reboot. When Reboot later option is selected, the devices restart if the current time matches the set time. From the drop-down list, select any one of the following options: <ul style="list-style-type: none"> Reboot immediately Reboot later Do not reboot

Wyse 7040 thin client BIOS settings

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

Table 124. System configuration

Parameter	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 125. Security settings

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

Table 126. Admin password settings

Parameter	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 127. Auto-On settings

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

Table 128. Reboot schedule

Parameter	Description
Reboot Option	Some BIOS settings require system reboot. When Reboot later option is selected, devices restart when the current time matches the set time. From the drop-down list, you can select any of the following options: <ul style="list-style-type: none"> • Reboot immediately • Reboot later • Do not reboot

Table 129. USB configuration

Parameter	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 130. Power management settings

Parameter	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: <ul style="list-style-type: none"> • 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 131. 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 this page to configure the Wyse Easy Setup settings for the control panel and the user interface.

Table 132. Configuring system

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

Table 133. Configuring peripherals

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

Table 134. Configuring Kiosk mode

Option	Description
Kiosk Mode	Select this option to replace the default Windows desktop with the Wyse easy setup desktop.
Applications	Enter the details to register a new application.
Application Exit Action	From the application exit action drop-down menu, select the preferred option.

Table 135. 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	The logo files are presented and you can upload the files from Apps & Data > File Repository > Inventory .

Table 136. Configuring taskbar

Option	Description
Date & Time	Select this option to display the date and time option in the taskbar.
Sound	Select this option to display the sound option in the taskbar.
Network	Select this option to display the network option in the taskbar.
Touch Keyboard	Select this option to display the touch keyboard option in the taskbar.

Table 137. Configuring Start menu

Option	Description
Allow Shutdown	Select this option to shut down the system.
Allow Restart	Select this option to restart the system.
Allow Log off	Select this option to log off the system.

Configuring VNC settings

Use this page to configure the VNC settings.

Table 138. 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
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 139. 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 Linux policy settings

To configure the policy settings for Linux devices, do the following:

1. Select a group and click **Edit Policies**.
2. From the menu, select **Linux**.
3. After configuring the options, click **Save and Publish**.

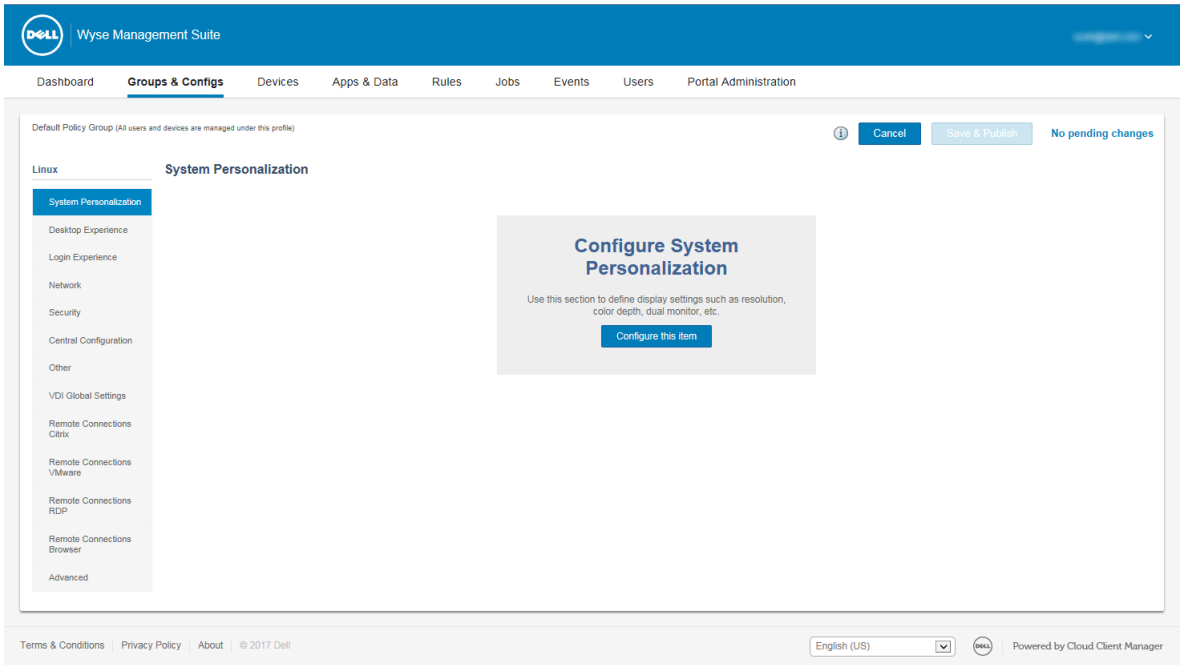


Figure 7. Linux

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

System personalization

Use this page to configure system personalization.

Table 140. System personalization

Setting	Description
Monitor Resolution (Primary)	Allows you to set the monitor resolution. From the drop-down menu, select your preferred monitor resolution.

Table 140. System personalization (continued)

Setting	Description
Monitor Rotation	Allows you to define the orientation of the monitor. From the drop-down list, select either Vertical or Horizontal based on your preference.
Enable Dual Monitor	Allows you to enable the dual monitor functionality. When you select this check box, the following options are displayed: <ul style="list-style-type: none"> • Mirror Mode—Display is mirrored. • Span Mode—Display is spanned. From the drop-down, select one of the options: <ul style="list-style-type: none"> ○ On Left ○ On Right ○ Bottom ○ Top
Layout	Allows you to set the keyboard layout of the thin client. From the drop-down menu, select your preferred option.
System Language	Allows you to set the language for the system. From the drop-down list, select your preferred option.
Mouse Speed	Allows you to specify the speed of the mouse pointer when moving the mouse. The range of mouse speed is 0–6.
Left-handed Mouse	Allows you 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	Allows you to set the time zone based on your location. From the drop-down menu, select your preferred time zone.
Time Format	Allows you to select the time format. From the drop-down menu, select either 12-hour or 24-hour format.
Time Servers (NTP Servers)	Allows you to list the time servers. Time servers allow the NTP server to synchronize the time.
Audio Volume	Allows you to set the audio volume of the thin client. The range of the audio volume is 0–100.
Audio Mute	Allows you to set the thin client to mute mode.
Microphone Volume	Allows you to set the microphone volume of the thin client. The range of the microphone volume is 0–100.
Microphone Mute	Allows you to set the microphone to mute mode.

Desktop experience

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

Table 141. Desktop experience

Parameter	Description
Desktop Wallpaper	Allows you to change the default wallpaper.

Table 141. Desktop experience (continued)

Parameter	Description
Wallpaper File	Allows you to select your preferred wallpaper. Images uploaded to the file repository are displayed.
Wallpaper Layout	Allows you to set the wallpaper Layout. From the drop-down menu, select your preferred wallpaper layout. The default wallpaper layout is center .
Hot Keys	<p>Allows you to disable the hot keys for the following actions:</p> <ul style="list-style-type: none"> • 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

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 142. Login experience

Setting	Description
Auto Login	Allows you 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	<p>Select the Auto Login check box to define the default user for auto login. From the drop-down menu, select your preferred option.</p> <ul style="list-style-type: none"> • admin • thinuser • guest
Enable Banner on Login window	<p>Allows you 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.</p> <p>Enter a customized text in the box displayed on the login screen.</p>
Root Password	Enter the password if you want to change the root password.

Table 142. Login experience (continued)

Setting	Description
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.

Network

Use this page to configure the network settings.

Table 143. Network settings

Parameter	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.

Security

Use this page to configure the security options.

Table 144. Security

Setting	Description
Password Encryption Algorithm	Allows you to select the password encryption algorithm. From the drop-down menu, select any of the following options: <ul style="list-style-type: none"> • 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	Allows you to select 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	Allows you to enable Secure Shell (SSH) on the device.
Allow “root” SSH login	Allows you to enable the root SSH login.
Enable VNC Server	Allows you to enable the VNC Server.

Table 144. Security (continued)

Setting	Description
Require User to enter password	Allows you to set the VNC password.
VNC Password	Allows you to enter the VNC password.
Prompt user on VNC session start	Allows you 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 145. Configuring central configuration settings

Option	Description
File Server Path	Enter the full path of the folder that contains the <code>w1x</code> 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 <code>/w1x</code> is appended to the root path entry before use. If root path is not provided, <code>/wyse</code> is considered.
Firmware Server/ Path	Enter the full path of folder that contains the firmware images. Supported protocols include ftp, http, and https. 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 <code>/wtx</code> is appended to the root path entry before use. If the root path is not provided, <code>/wyse</code> is considered.

Other settings

Use this page to configure the other options.

Table 146. Other settings

Parameter	Description
Auto Power-On	Allows you 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.

Table 146. Other settings (continued)

Parameter	Description
	<ul style="list-style-type: none"> • Interactive • Restart • Shutdown • None
DHCP Vendor ID	Allows you to change the DHCP Vendor ID. The default Vendor ID is wyse-5000 .
Browser Homepage	Allows you to change the browser homepage. Enter the URL address of your choice to set the browser homepage.

VDI global settings

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

Table 147. Citrix general

Parameter	Description
ICA Browsing Protocol	Allows you to set the default browsing protocol.
Browser IP	Enter the browser IP address.
Store Name	Allows you to specify the store name.
Domain Name	Enter the domain name.
PN Desktop Setup (Show All Application)	Allows you to enable the PN desktop setup. When this option is enabled, all the published applications are displayed on the desktop.
Enable Multimedia Redirection (MMR)	Allows you to enable the Multimedia Redirection.
Enable H.264 Decoding Support	Allows you to enable the H.264 decoding support for the ICA connections.
HDX Webcam Frame Rate	Allows you to set the preferred frame rate for the HDX Webcam.
HDX Webcam Image Width	Allows you to set the width of image request from the HDX Webcam.
HDX Webcam Image Height	Allows you to set the height of image request from the HDX Webcam.
Audio Bandwidth Limit	<p>Allows you to set the bandwidth used for audio input. From the drop-down menu, select any one of the following options:</p> <ul style="list-style-type: none"> • Low • Medium • High
Enable UDP Audio	Allows you to enable the transport of audio data through UDP.
Flash Redirection Policy	Allows you to set the Flash Redirection policy. From the drop-down menu, select either allow or deny the Flash Redirection policy.

Table 147. Citrix general (continued)

Parameter	Description
Transparent Key Passthrough	Allows you 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: <ul style="list-style-type: none"> • Local • Remote • Full Screen Only
Use Alternate Address	Allows you to use an alternate IP address from the ICA master browser to pass firewalls.
ICA Proxy Type	Allows you to select the proxy type for the ICA connection. The default value is None .

Table 148. Citrix USB redirection

Parameter	Description
Allow USB Redirection of devices plugged in before ICA Session start	Allows you 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	Allows you to enable the Citrix 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 Citrix sessions.

Table 149. Citrix drive mapping

Parameter	Description
Enable ICA Dynamic Drive Mapping	Allows you 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 150. VMware USB redirection

Parameter	Description
Enable USB Redirection	Allows you 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.

Remote connection—Citrix

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

Table 151. Remote connection Citrix

Parameter	Description
Connection Name	Allows you to enter a name to identify the connection.
Auto Launch Connection on Logon	Allows you to automatically launch the connection after you log in.
Connection Type	Allows you to set a connection type. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Server Connection • Published Application • Store Front
Citrix Server FQDN or IP Address	Allows you 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	Allows you to specify a published application to start. This option is displayed when you select the connection type as Published Application or Storefront .
Connection Server	Allows you to enter the IP address or FQDN of the Citrix connection server.
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	Allows you to set a browsing protocol for the secure and non-secure connections. From the drop-down list, select either of the following options: <ul style="list-style-type: none"> • http • https
Low Bandwidth	Allows you to set the slow bandwidth optimization.
Enable Sound	Allows you to enable sound.
SmartCard Login	Allows you to enable the smart card login feature for ICA connection.
Encryption Level	Allows you to set an encryption level. From the drop-down menu, select any one of the following encryption levels: <ul style="list-style-type: none"> • Basic • RC5 (128-bit – Log in Only) • RC5 (40-bit) • RC5 (56-bit) • RC5 (128- bit)
Windows Size	Allows you to set a window size. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Default

Table 151. Remote connection Citrix (continued)

Parameter	Description
	<ul style="list-style-type: none"> Seamless 640 x 480 1024 x 768 800 x 600 1280 x 1024 1600 x 1200 Full Screen
Screen Color Depth	<p>Allows you to set a screen color depth. From the drop-down menu, select any one of the following options:</p> <ul style="list-style-type: none"> 64K 256 16M
Auto Reconnect	Allows you to enable the thin client to reconnect to the Citrix session automatically.
Delay before trying to reconnect	Allows you to set the time in seconds to delay the reconnection attempt. When you select the Auto Reconnect check box, this option is displayed.

Remote connection—VMware

Use this page to create a VMware View broker connection.

Table 152. Remote connection VMware

Parameter	Description
Connection Name	Allows you to enter a name to identify the connection.
Auto Launch Connection On Logon	Allows you 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)	Allows you to use the SSL connection.
Protocol	Allows you to set PCOIP or RDP as protocol.
Enable NLA	Allows you 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	Allows you to enable the User Interactive mode.
Lock the Server URL / Host field	Allows you to lock the server URL.

Table 152. Remote connection VMware (continued)

Parameter	Description
Security Mode	Allows you to set the security mode. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Never connect to untrusted servers • Warn before connecting to untrusted servers • Do not verify server identity certificates.
Fullscreen Mode	Allows you to view the remote session in the fullscreen mode.
Window Size	Allows you to set a window size. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Use all monitors • Full Screen • Large Screen • Small Screen • 1024 x 768 • 800 x 600 • 640 x 480
Disable Fullscreen drop down menu bar	Allows you to disable the drop-down menu in the fullscreen mode.
Automatically launch this Desktop	Allows you to specify the name of the published desktop to automatically launch upon successful connection.
Auto Reconnect	Allows you 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.

Remote connection—RDP

Use this page to create an RDP broker connection.

Table 153. Remote connection RDP

Setting	Description
Connection Name	Allows you to enter the name to identify the connection.
Auto Launch Connection on Logon	Allows you to automatically launch the connection after you log in.
Server Address	Enter the server name or the IP address.
SmartCard Login	Allows you to enable the smart card authentication.
Use Network Level Authentication (NLA)	Allows you to enable the Network Level authentication.
Username	Enter the user name.
Password	Enter the password.
Domain Name	Enter the domain name.

Table 153. Remote connection RDP (continued)

Setting	Description
Window Size	Allows you to set a window size. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Default • 640 x 480 • 1024 x 768 • 800 x 600 • 1280 x 1024 • 1600 x 1200 • Full Screen
Forward All Printers	Allows you to forward all the printers to the remote connection.
Auto Reconnect	Allows you 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	Allows you to map drives on the RDP session. Click the Add Drive Mapping button, and enter the following details: <ul style="list-style-type: none"> • Drive Letter—From the drop-down menu, select the drive letter. • Drive Type—Select any one of the following drive types: <ul style="list-style-type: none"> ○ USB Disk or Memory Stick ○ USB CD ROM ○ USB Floppy
Use RD Gateway settings	Allows you to use the RD gateway settings. The RD Server , and the Use Remote Desktop credentials for RD Gateway options are displayed.
RD Server	Allows you to specify the RD gateway host address.
Use Remote Desktop Credentials for RD Gateway	Allows you 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.

Remote connection—Browser

Use this page to configure the remote connections browser.

Table 154. Remote connection browser

Setting	Description
Connection Name	Enter the name to identify the connection.

Table 154. Remote connection browser (continued)

Setting	Description
Auto launch Connection on Logon	Allows you to automatically launch the connection during login.
URL	Enter the starting URL.
Kiosk Mode	Allows you to enable the kiosk mode.
Window Size	Allows you to set a window size. From the drop-down menu, select the size of the window of your choice.
Auto Reconnect	Allows you 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 155. 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 ThinLinux policy settings

To configure the policy settings in ThinLinux devices, do the following:

1. Select a group and click **Edit Policies**.
2. From the menu, select **ThinLinux**.
3. After configuring the options, click **Save and Publish**.

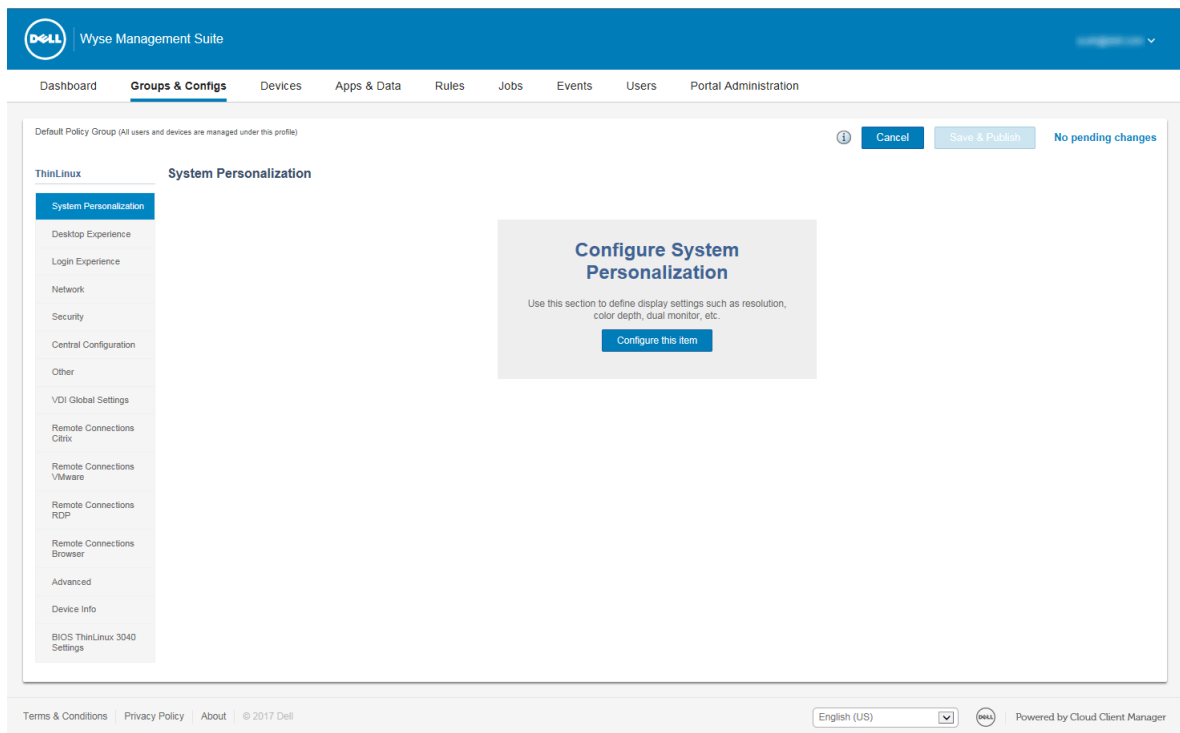


Figure 8. ThinLinux

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

System personalization

Use this page to configure the system personalization.

Table 156. Display

Parameter	Description
Monitor Resolution—Primary	Allows you to set the monitor resolution. From the drop-down menu, select your preferred monitor resolution.
Monitor Rotation	Allows you to define the orientation of the monitor. From the drop-down list, select either vertical or horizontal based on your preference.

Table 156. Display (continued)

Parameter	Description
Enable Dual Monitor	Allows you to enable the dual monitor functionality. If you select this check box, the following options are displayed: <ul style="list-style-type: none"> • 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—From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> ○ On Left ○ On Right ○ Bottom ○ Top

Table 157. Keyboard

Parameter	Description
Layout	Allows you to set the keyboard layout of the thin client. From the drop-down menu, select your preferred option.

Table 158. Language

Parameter	Description
System Language	Allows you to set the language of the system. From the drop-down list, select your preferred option.

Table 159. Mouse

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

Table 160. Time zone

Parameter	Description
Time Zone	Allows you to set the time zone based on your location. From the drop-down menu, select your preferred time zone.
Time Format	Allows you 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)	Allows you to list the time servers. Time servers allow the NTP server to synchronize the time. Multiple servers are allowed, and the server names must be separated by commas.

Table 161. Audio

Parameter	Description
Audio Volume	Allows you to set the audio volume of the thin client. The range of the audio volume is 0–100.

Table 161. Audio (continued)

Parameter	Description
Audio Mute	Allows you to set the thin client to mute mode.
Microphone Volume	Allows you to set the microphone volume of the thin client. The range of the microphone volume is 0–100.
Microphone Mute	Allows you to set the microphone to mute mode.

Desktop experience

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

Table 162. Desktop experience

Parameters	Description
Desktop Wallpaper	Allows you to change the default wallpaper.
Wallpaper File	Allows you to select your preferred wallpaper. Images uploaded to the file repository are displayed.
Wallpaper Layout	Allows you 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.

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 163. Login experience

Parameter	Description
Auto Login	Allows you to enable the thin client to automatically log in without any user intervention.
Enable Banner on Login window	Allows you 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.

Table 163. Login experience (continued)

Parameter	Description
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

Network

Use this page to configure the network settings.

Table 164. Network

Parameter	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 165. 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 166. 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 167. 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.

Table 167. Configuring VNC settings (continued)

Option	Description
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.

Central configuration

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

Table 168. Central configuration

Parameter	Description
File Server/ Path	Enter the full path of the folder that contains the w1x2 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 /w1x2 is appended to the root path entry before use. If root path is not provided, /wyse is considered.
Enable Delayed Update	Allows you 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	Allows you to set the update mode for delayed update process.
Reset to factory defaults	Allows you to set the device to the factory default condition after the imaging process.
Allow base image downgrade	Allows you to enable the base image downgrade.

Other settings

Use this page to configure the other options.

Table 169. Other settings

Parameter	Description
Auto Power-On	Allows you to enable the system to boot when power is restored without waiting for the user to press the power button.

Table 169. Other settings (continued)

Parameter	Description
Power Button Action	<p>From the drop-down menu, select any one of the options:</p> <ul style="list-style-type: none"> • Interactive • Restart • Shutdown • None <p>The options define the action to be taken when you press the power button.</p>
DHCP Vendor ID	Allows you to change the DHCP Vendor ID. The default Vendor ID is wyse-5000 .
Browser Homepage	Allows you to change the browser homepage. Enter the URL address of your choice to set the browser homepage.

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 170. Citrix General

Parameter	Description
ICA Browsing Protocol	Allows you to set the default browsing protocol.
ICA PAM Login	Allows you 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)	Allows you to enable the PN desktop setup. When this option is enabled, all the published applications are displayed on the desktop.
Enable Multimedia Redirection (MMR)	Allows you to enable the Multimedia Redirection.
Enable H.264 Decoding Support	Allows you to enable the H.264 decoding support for the ICA connections.
HDX Webcam Frame Rate	Allows you to set the preferred frame rate for the HDX Webcam.
HDX Webcam Image Width	Allows you to set the width of image request from the HDX Webcam.
HDX Webcam Image Height	Allows you to set the height of image request from the HDX Webcam.
Audio Bandwidth Limit	<p>Allows you to set the bandwidth used for audio input. From the drop-down menu, select any one of the following options:</p> <ul style="list-style-type: none"> • Low • Medium • High

Table 170. Citrix General (continued)

Parameter	Description
Enable UDP Audio	Allows you to enable the transport of audio data through UDP.
Flash Redirection Policy	Allows you to either allow or deny Flash Redirection Policy.
Transparent Key Passthrough	Allows you 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: <ul style="list-style-type: none"> • Local • Remote • Full Screen Only
Use Alternate Address	Allows you to use an alternate IP address from the ICA master browser to pass firewalls.
ICA Proxy Type	Allows you to select the proxy type for the ICA connection. The default value is None .

Table 171. Citrix USB redirection

Parameter	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	Allows you 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 172. Citrix Drive mapping

Parameter	Description
Enable ICA Dynamic Drive Mapping	Allows you 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)	Allows you to redirect all the USB device contents in the ICA session under a single directory—Wyse USB.

Table 173. VMware USB redirection

Parameter	Description
Enable USB Redirection	Allows you to either allow or deny USB redirection policy in to the VMware sessions.

Remote connection—Citrix

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

Table 174. Remote connection Citrix

Parameter	Description
Connection Name	Allows you to enter a name to identify the connection.
Auto Launch Connection on Logon	Allows you to automatically launch the connection after you log in.
Connection Type	Allows you to set a connection type. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Server Connection • Published Application • Store Front
Connection Server	Allows you to enter the IP address or FQDN of the Citrix server.
Citrix Server FQDN or IP address	Allows you to enter the Citrix server FQDN or IP address. This is applicable for Published Application and StoreFront connection type.
Published Application	Allows you 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	Allows you to set a browsing protocol for the secure and non-secure connections. From the drop-down list, select either of the following options: <ul style="list-style-type: none"> • 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	Allows you to set an encryption level. From the drop-down menu, select any one of the following encryption levels: <ul style="list-style-type: none"> • Basic • RC5 (128-bit – Log in Only) • RC5 (40-bit) • RC5 (56-bit) • RC5 (128-bit)
Windows Size	Allows you to set a window size. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Default • Seamless • 640 x 480

Table 174. Remote connection Citrix (continued)

Parameter	Description
	<ul style="list-style-type: none"> • 1024 x 768 • 800 x 600 • 1280 x 1024 • 1600 x 1200 • Full Screen
Screen Color Depth	<p>Allows you to set a screen color depth. From the drop-down menu, select any one of the following options:</p> <ul style="list-style-type: none"> • 64K • 256 • 16M
Auto Reconnect	Allows you to enable the thin client to reconnect to the Citrix session automatically.
Delay before trying to reconnect	Allows you to set the time in seconds to delay the reconnection attempt. When you select the Auto Reconnect check box, this option is displayed.

Remote connection—VMware

Use this page to create a VMware View broker connection.

Table 175. Remote connection VMware

Parameter	Description
Connection Name	Allows you to enter a name to identify the connection.
Auto Launch Connection On Logon	Allows you 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)	Allows you to use the SSL connection.
Protocol	Allows you 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	Allows you 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.
Password	Enter the password when the PCoIP protocol is selected.
Domain Name	Enter the domain name.
Interactive Mode	Allows you to enable the User Interactive mode.

Table 175. Remote connection VMware (continued)

Parameter	Description
Lock the Server URL / Host field	Select the check box to lock the server URL.
Security Mode	Allows you to set the security mode. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Never connect to untrusted servers • Warn before connecting to untrusted servers • Do not verify server identity certificates.
Fullscreen Mode	Allows you to view the remote session in the fullscreen mode.
Window Size	Allows you to set a window size. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Use all monitors • Full Screen • Large Screen • Small Screen • 1024 x 768 • 800 x 600 • 640 x 480
Disable Fullscreen Drop Down Menu Bar	Allows you to disable the drop-down menu in the fullscreen mode.
Automatically Launch This Desktop	Allows you to specify the name of the published desktop to automatically launch upon successful connection.
Auto Reconnect	Allows you 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.

Remote connection—RDP

Use this page to create an RDP broker connection.

Table 176. Remote connection RDP

Parameter	Description
Connection Name	Allows you to enter the name to identify the connection.
Auto Launch Connection on Logon	Allows you to automatically launch the connection after you log in.
Server Address	Enter the server name or the IP address.
SmartCard Login	Allows you to enable the smart card authentication.
Use Network Level Authentication (NLA)	Allows you to enable the Network Level authentication.
Username	Enter the user name.
Password	Enter the password.

Table 176. Remote connection RDP (continued)

Parameter	Description
Domain Name	Enter the domain name.
Window Size	Allows you to set a window size. From the drop-down menu, select any one of the following options: <ul style="list-style-type: none"> • Default • 640 x 480 • 1024 x 768 • 800 x 600 • 1280 x 1024 • 1600 x 1200 • Full Screen
Forward All Printers	Allows you to forward all the printers to the remote connection.
Auto Reconnect	Allows you 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	Allows you to map all the devices to a single shared name—WyseUSB.

Table 177. RD gateway

Setting	Description
Use RD Gateway settings	Allows you to use the RD gateway settings. The RD Server and the Use Remote Desktop credentials for RD Gateway options are displayed.
RD Server	Allows you to specify the RD gateway host address.
Use Remote Desktop credentials for RD Gateway	Allows you to use the remote desktop credentials for the RD gateway.

Remote connection—Browser

Use this page to configure the Remote connections browser.

Table 178. Remote connection browser

Parameter	Description
Connection Name	Enter the name to identify the connection.
Auto launch Connection on Logon	Allows you to automatically launch the connection during login.
URL	Enter the starting URL.
Kiosk Mode	Allows you to enable the kiosk mode.
RC Disable Panel in kiosk mode	Allows you to disable the RC panel in the kiosk mode.

Table 178. Remote connection browser (continued)

Parameter	Description
Window Size	Allows you to set a window size. From the drop-down menu, select the size of the window of your choice.
Auto Reconnect	Allows you 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.

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 179. Advanced

Parameter	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 180. 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 181. Configuring general settings

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

Table 182. Configuring system configuration

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.

Table 182. Configuring system configuration (continued)

Option	Description
Integrated NIC	From the drop-down list, select the preferred option.
Audio	Select this option to enable the audio device.

Table 183. Configuring USB configuration



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 184. Configuring wireless settings

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

Table 185. Configuring security settings

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

Table 186. Configuring 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 admin password. This option is available only if you select the Enable Admin Password check box.

Table 187. Configuring 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 188. 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 189. Configuring 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 190. Configuring reboot schedule

Option	Description
Reboot Option	<p>Some BIOS settings require system reboot. When Reboot later option is selected, devices restart when the current time matches the set time. From the drop-down list, you can select any of the following options:</p> <ul style="list-style-type: none"> • Reboot immediately • Reboot later • Do not reboot

Configuring Wyse Software thin client policy settings

To configure the policy settings for Wyse Software thin client devices, do the following:

1. Select a group, and click **Edit Policies**.
2. Click **Wyse Software Thin Client**.
3. After configuring the options, click **Save and Publish**.

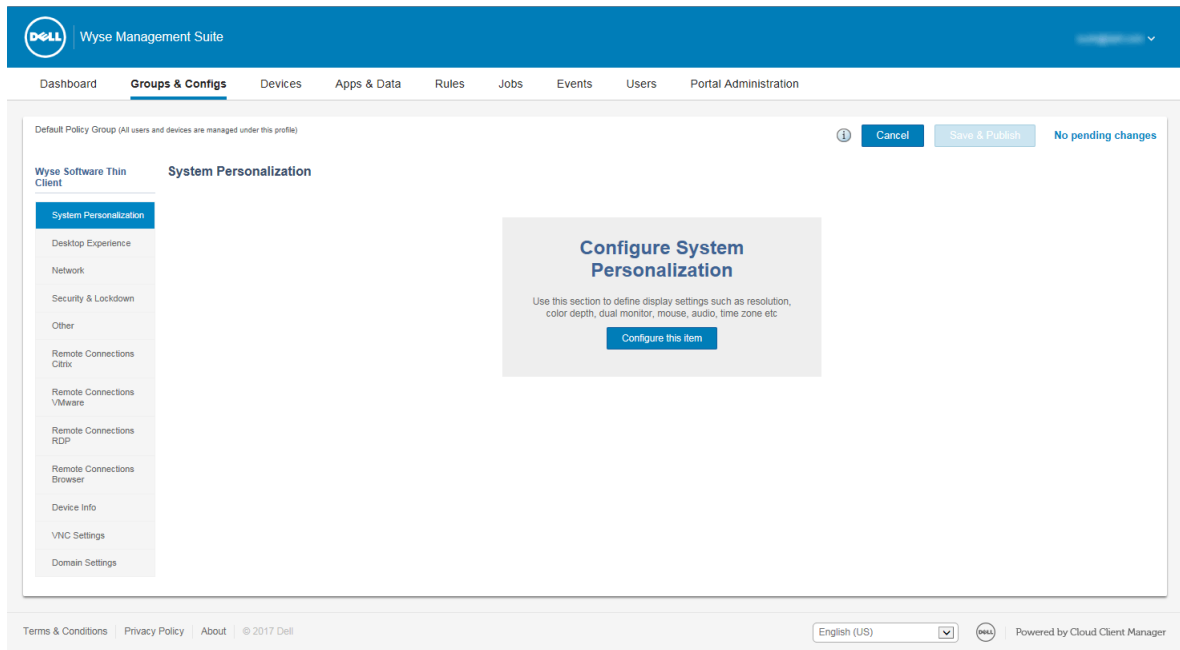


Figure 9. Wyse Software Thin Client

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
- VNC Settings
- Domain Settings

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 191. 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.

Table 191. Configuring display options (continued)

Option	Description
Monitor Rotation (Primary)	<p>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:</p> <ul style="list-style-type: none"> • Landscape • Portrait • Landscape—flipped • Portrait—flipped

Table 192. 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—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	<p>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:</p> <ul style="list-style-type: none"> • 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 enable the MS Gina layout on your keyboard.

Table 193. 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 194. 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 195. 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 196. 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 197. 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 198. 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 199. Configuring audio settings

Option	Description
Audio Mute	Select this option to mute the audio of your device.

Table 199. Configuring audio settings (continued)

Option	Description
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 200. Configuring desktop experience

Option	Description
Desktop Wallpaper	<p>Select this option to set a wallpaper for your desktop. After you enable the desktop wallpaper option, do the following:</p> <ul style="list-style-type: none"> From the Wallpaper File drop-down list, select a wallpaper for your desktop. <p>NOTE: Select a wallpaper only from the list of images uploaded to the file repository.</p> <ul style="list-style-type: none"> From the Wallpaper Layout drop-down list, select any of the following layouts for your desktop wallpaper: <ul style="list-style-type: none"> 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 201. Configuring network settings

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

Configuring security and lockdown settings

Use this page to configure the security and lockdown settings.

Table 202. 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 203. Configuring appliance mode

Option	Description
Application Mode	Select this option to set an appropriate mode for the appliance. From the drop-down menu, select any of the following options and perform the required action: <ul style="list-style-type: none">• 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 204. 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: <ul style="list-style-type: none">• Balanced• Power Saver

Table 205. 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.

Table 205. Power settings on battery (continued)

Option	Description
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 206. 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 207. 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 208. 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 209. 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: <ul style="list-style-type: none"> • Citrix XenApp • Citrix XenDesktop • Citrix Gateway • Citrix StoreFront

Table 209. Configuring basic options (continued)

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. From the drop-down menu, select any of the following options: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Default User Key Combos Passthrough • On the local desktop • On the remote desktop • In full screen desktops only

Table 210. 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.

Table 210. Configuring application display settings (continued)

Option	Description
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 211. Configuring server options

Option	Description
Logon Method	Select this option to choose a logon method for your Citrix connection. <ul style="list-style-type: none"> • Default Logon Method • Prompt Logon Method

Table 212. 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 213. 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 214. Configuring remote connection settings—VMware

Option	Description
Connection Name	Select this option to define the name to identify the connection.

Table 214. Configuring remote connection settings—VMware (continued)

Option	Description
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: <ul style="list-style-type: none"> • 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 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 215. 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.

Table 215. Configuring basic settings (continued)

Option	Description
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 216. Configuring RD gateway settings

Option	Description
Use RD Gateway settings	<p>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.</p> <p>From the RD Gateway Logon Method drop-down menu, select any one of the following:</p> <ul style="list-style-type: none"> • Ask for password NTLM • Smartcard • Allow me to choose later <p>From the RD Gateway Usage Method drop-down menu, select any of the following ways to use a remote desktop server:</p> <ul style="list-style-type: none"> • 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 217. Configuring display settings

Option	Description
Fullscreen	<p>Select this option to set the connection window in the full screen mode.</p> <p>After the full screen mode is enabled, from the drop-down menu, select the window size.</p>
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.

Table 217. Configuring display settings (continued)

Option	Description
Screen Color Depth (in bits)	<p>Select this option to define the screen color depth of the connection.</p> <ul style="list-style-type: none"> • RDP 15–Bit High Color • RDP 16–Bit High Color • RDP 24–Bit True Color • RDP 32–Bit Highest Quality

Table 218. 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.
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 219. 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 220. 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. <ul style="list-style-type: none"> • 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 221. 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 222. Configuring Internet Explorer (IE) favorites and trusted site settings

Option	Description
IE Favorite	<p>Select this option to add your favorite and trusted sites. Perform the following steps to add your favorite and trusted sites:</p> <ul style="list-style-type: none"> 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. <p>NOTE: The URL must begin with https:// when the Trusted Sites check box is selected.</p>
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 223. Configuring Internet Explorer (IE) proxy settings

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

Table 224. 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 225. Configuring Aero (Valid for Windows Embedded Standard 7) settings

Option	Description
Aero	<p>Select this option to enable the Aero feature for the browser.</p> <p>NOTE: This feature is available only for Windows Embedded Standard 7</p>

Configuring device information

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

Table 226. Configuring device information

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

Configuring VNC settings

Use this page to configure the VNC settings.

Table 227. 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 228. 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.

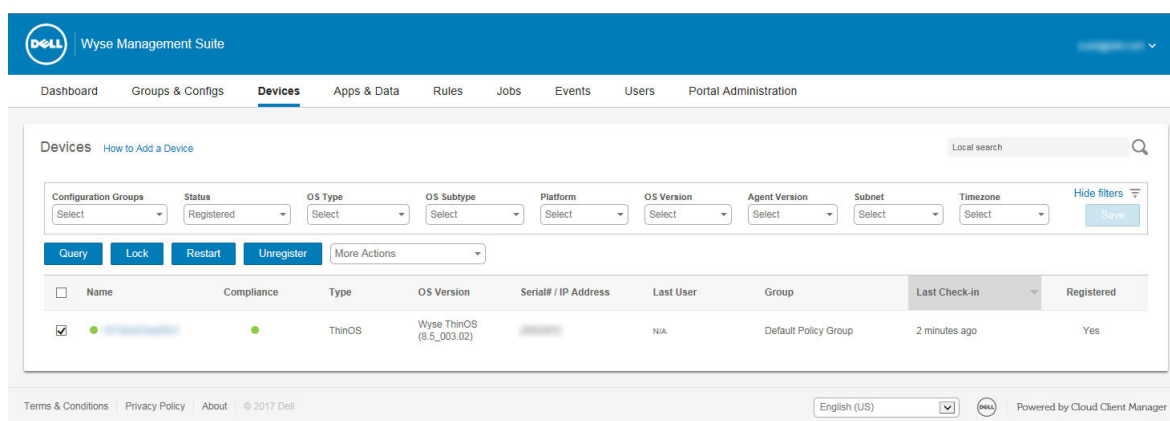


Figure 10. Devices

Topics:

- [Using filters](#)
- [Registering devices into Wyse Management Suite](#)
- [Viewing and managing device details](#)
- [Pulling Windows Embedded Standard or ThinLinux image](#)
- [Pulling log file](#)
- [Renaming thin client](#)

Using filters

About this task

You can filter the devices details based on your requirements by using the following filtering options:

- **Configuration Groups**
- **Status**
- **OS Type**
- **OS Subtype**
- **Platform**
- **OS Version**
- **Agent Version**
- **Subnet**
- **Timezone**

Steps

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
 - Not Registered
 - Compliant
 - Pending
 - Non-Compliant
 - **Online Status**
 - Online
 - Offline
 - Unknown
 - **Others**
 - Recently Added
3. From the **OS Types** drop-down list, select any one of the following operating systems:
 - Linux
 - ThinLinux
 - ThinOS
 - WES
 - 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.

Save current filter

About this task

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

Steps

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**.

Registering devices into Wyse Management Suite

Register a 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.

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 thin clients through WDA User Interface

Prerequisites

Creating a group is a pre-requisite for registering the thin client to the Wyse Management Suite.

Steps

1. On your supported thin client, open the **Central Configuration** dialog box.
For example, click the **System Settings** icon on the Zero Toolbar, and then click **Central Configuration**. For more information about ThinOS, refer to the ThinOS documentation.
 2. Enter a valid group token and the server URLs.
 3. Click **OK**, and follow the instructions displayed on the screen.
 4. Enter the corporate credentials when prompted.
-  **NOTE:** To verify whether your entry is correct, use the validate key. If a success message is displayed, click **OK** to restart the device, and complete the registration process. If a failure message is displayed, double-check the group registration key which you have entered, and verify whether you have a proper network connectivity.
5. To verify the network connectivity for the real-time commands, go to the **Devices** page. Click the **Name** link to open the **Device Details page** for your thin client, and then click **Restart**.
The thin client basic connectivity is complete, and the thin client is successfully registered. You can send a real-time command to the thin client, and configure the policies at the group level.

Registering Windows Embedded Standard thin clients through Wyse Device Agent User Interface

About this task


 **NOTE:** Creating a group is a pre-requisite for registering the thin client device to the Wyse Management Suite.

Steps

1. Open the **Wyse Device Agent** (WDA) 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 through Wyse Device Agent User Interface

About this task

 **NOTE:** Creating a group is a pre-requisite for registering the thin client to Wyse Management Suite.

Steps

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 devices by using DHCP option tags


About this task

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

NOTE:

For detailed instructions on how to add DHCP option tags on the Windows server, see [Creating and configuring DHCP option tags](#).

Table 229. 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, <code>wmsserver.acme.com:443</code> , where <code>wmsserver.acme.com</code> 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 .  NOTE: Do not use <code>https://</code> 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, <code>wmsservername.domain.com:1883</code> . 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	This tag is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this option tag if you are registering your devices with Wyse Management Suite on public cloud. 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.
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.

 **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 230. Configuring device by using DNS SRV record





URL/Tag	Description
Record Name —_WMS_MGMT Record FQDN —_WMS_MGMT._tcp.<Domainname> Record Type — SRV	<p>This record points to the Wyse Management Suite server URL. For example, <code>wmserver.acme.com:443</code>, where <code>wmserver.acme.com</code> 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.</p> <p> NOTE: Do not use <code>https://</code> in the server URL, or the thin client will not register under Wyse Management Suite.</p>
Record Name —_WMS_MQTT Record FQDN —_WMS_MQTT._tcp.<Domainname> Record Type —SRV	<p>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, <code>wmservername.domain.com:1883</code>.</p> <p> NOTE: MQTT is optional for the latest version of Wyse Management Suite.</p> <p>To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example,</p> <p>US1—us1-pns.wysemanagementsuite.com EU1—eu1-pns.wysemanagementsuite.com</p>
Record Name —_WMS_GROUPTOKEN Record FQDN —_WMS_GROUPTOKEN._tcp.<Domainname> Record Type — TEXT	<p>This record is required to register the ThinOS devices with Wyse Management Suite on public or private cloud.</p> <p>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.</p> <p> NOTE: Group Token is optional for the latest version of Wyse Management Suite on private cloud.</p>
Record Name —_WMS_CAVALIDATION Record FQDN — _WMS_CAVALIDATION._tcp.<Domainname> Record Type —TEXT	<p>This record is required if Wyse Management Suite is installed on your system in your private cloud. Do not add this optional record if you are registering your devices with Wyse Management Suite on public cloud.</p> <p>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.</p>

Table 230. Configuring device by using DNS SRV record (continued)


URL/Tag	Description
	<p>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.</p> <p> NOTE: CA Validation is optional for the latest version of Wyse Management Suite.</p>

Viewing and managing device details

About this task

On the **Devices** page, the following attributes are displayed:

- **Device Name**
- **Compliance**
- **Device Type**
- **OS Version**
- **Serial# / IP Address**
- **Last User**
- **Group**
- **Last Checked-in**
- **Health**
- **Registered**

 **NOTE:** Devices in the unmanaged group are displayed with a red icon.

To manage the device details, click a device, and then click the relevant tabs on the **Device details** page.

Table 231. Device details


Parameter	Description
Query	Allows you to send a command to update the device information in the system.
Restart	Allows you to restart the thin client.
Unregister	Allows you to remove the device from system policies and management.
Delete Device	Allows you to delete a device from the system. Only a device that is not currently registered can be deleted from the system.
Wipe	Allows you to remove all the data and applications from a device.
Send Message	Allows you to send a message (128 characters or less) to a device.
Change Group	Allows you to select a new group for a particular device.
Wake on LAN	<p>If a device is turned off or in the sleep mode, and you want to activate the device, then select the device, and click the Wake on LAN option.</p> <p> NOTE: The Wake on LAN option must be enabled to wake up the device from the sleep mode.</p> <p>To enable the Wake on LAN option, do the following:</p> <ol style="list-style-type: none"> 1. Go to Portal Admin > File Repository. 2. Select the device, and click Edit.

Table 231. Device details (continued)

Parameter	Description
	<p>A window is displayed with the repository and server details.</p> <p>3. Select the check box.</p>
Export Devices to CSV	Allows you to generate a CSV with a list of the asset information for all the devices filtered on the screen.
Summary tab	Allows you to view and manage information on the Notes, Group Assignment, Alerts, and Device Configuration.
Update Image	Displays a schedule in the WES Firmware Update Job window.
Change Group Assignment	Allows you to change the group to which the thin client belongs. This option is available in the Group Assignment section.
Device level exceptions (Applicable to all device types)	<p>The device configuration details, such as the default policy group name, and the summary of current policy are displayed.</p> <p>To create or edit a device level exception, click Create/Edit exceptions, and configure a particular device policy on the Devices page.</p>
System Info	<p>The following details are displayed in the System Info tab:</p> <ul style="list-style-type: none"> • Hardware Details • OS Details • Network Details Current Connection. • Network adapters • Wi-Fi Profiles • Security Settings • Anti-virus Settings • Firewall Settings • BIOS Cards
Events tab	Allows you to view and manage information on the system events pertaining to a device—Creation, device registration, and various tasks performed by the system and the device.
Troubleshooting	<p>Allows you to view and manage the troubleshooting information.</p> <ul style="list-style-type: none"> • Screen Capture on Demand—Administrator can capture the screenshot of the thin client with or without the client's permission. If the Require User Acceptance check box is selected, a message to indicate that administrator wants to take a screenshot is displayed on the client. This option is applicable only for Windows Embedded Standard and Linux devices. • Task Troubleshooting <ol style="list-style-type: none"> 1. Click Request Processes List, to view the list of the processes running on the thin client. 2. Click End Process, to end a process. 3. Click Request Services List, to view the list of the services running on the thin client. • Performance Monitoring <ol style="list-style-type: none"> 1. Click Start Monitoring, to access the Performance metric console.

Table 231. Device details (continued)

Parameter	Description
	<p>On the Performance metric console, the following details are displayed:</p> <ul style="list-style-type: none"> ○ Average CPU last minute. ○ Average memory usage last minute. <p>2. Click Clear.</p>
Installed Apps	<p>This option is available for Windows Embedded Standard, Linux, and ThinLinux devices. The current number of installed applications is displayed next to the Installed Apps title. The following are the attributes displayed on the page:</p> <ul style="list-style-type: none"> ● Name ● Publisher ● Version ● Installed On <p>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.</p>

NOTE: Only the unregister command and the change group assignment commands are available for devices which are in unmanaged group.

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, go to the **WES** or **ThinLinux** device page, and from the **More Actions** drop-down list, select **Pull OS Image**.

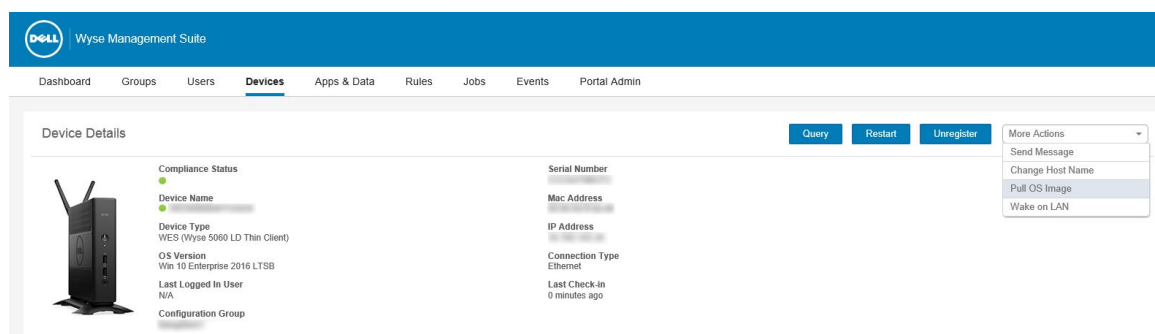


Figure 11. Pull OS image

A **Pull OS image screen** screen with the following parameters is displayed:

Figure 12. Pull OS image screen

Table 232. Pull OS image screen details

Option	Description
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 menu, select the file repository to where the image is uploaded. There are two types of file repository: <ul style="list-style-type: none"> Local repository Remote Wyse Management Suite repository
Pull Type	Select either Default or Advanced based on your pull type requirement. <ul style="list-style-type: none"> When the Default pull type is selected, the following options are displayed: <ul style="list-style-type: none"> Compress OS BIOS When the Advanced pull type is selected, a drop-down menu for selecting the templates is displayed. Select any template which is available by default. <p>NOTE: You can use the custom templates created manually by editing the existing or default templates.</p>

Performing the image pull process on the client side

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

NOTE:

- Wyse Device Agent and Merlin must be upgraded on your devices.
- 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.

Pulling log file

About this task

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

Steps

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.

The screenshot shows the 'Device Details' page for a device named 'WIE10Device1'. The page has a top navigation bar with buttons for 'Query', 'Restart', 'Unregister', and a 'More Actions' dropdown. Below the navigation bar, there's a section for device details including Compliance Status (green dot), Device Name (WIE10Device1), Device Type (Thin Client (Wyse 5020 thin client)), OS Version (Win 10 Enterprise 2015 LTSB), Last Logged In User (WIE10Device1\Admin), Configuration Group (test11), and Agent Version (12.1.1.25). To the right of these details, there's a section for network information including Serial Number, Mac Address, IP Address, Connection Type (Ethernet), and Last Check-in (1 minute ago). Below the details section, there's a tabbed interface with tabs for 'Summary', 'System Info', 'Events', 'Installed Apps' (with a badge showing 23), 'Device Log' (which is selected and has a circled '1' above it), and 'Troubleshooting'. Below the 'Device Log' tab, there's a 'Request Log File' button (with a circled '2' above it) and a message stating 'Current log updated at: 6 days ago' and 'To download log file, [click here](#).' (with a circled '3' above the link).

Figure 13. Log file pull

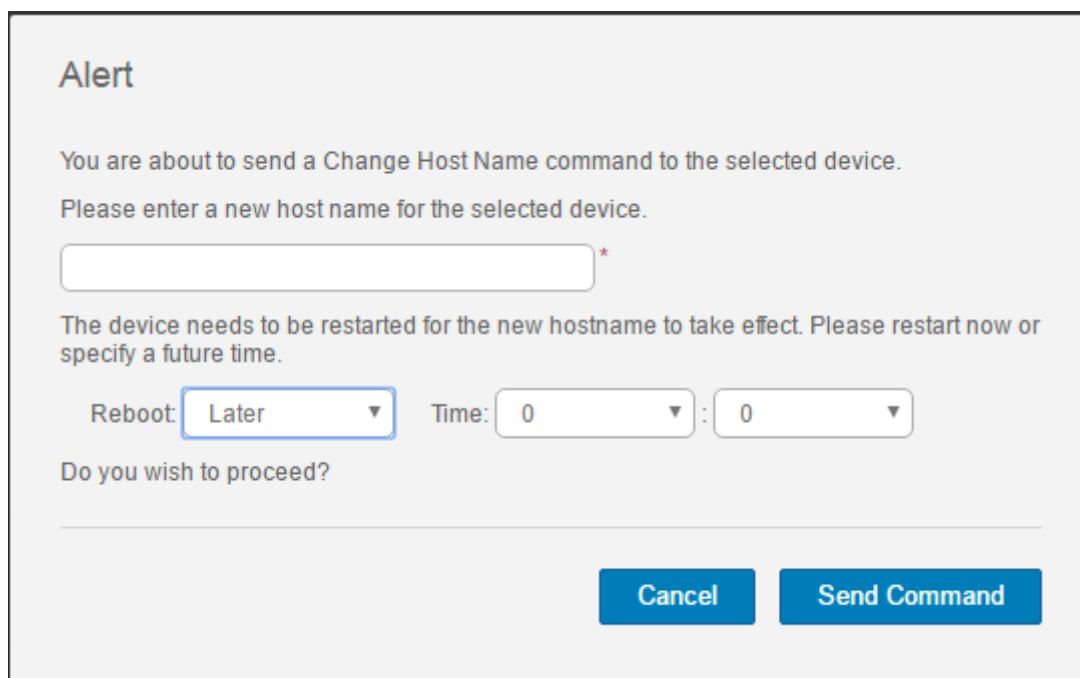
NOTE:

- The device must be enabled to pull the log file.
- The ThinOS device uploads the system logs.
- The Windows Embedded Standard or Linux device uploads the Wyse Device Agent logs, and the system logs.
- To extract a ThinLinux log, use `7zip.exe` or any equivalent software.

Renaming thin client

Use this page to change the host name of Windows Embedded Standard, ThinLinux, and ThinOS thin clients. 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.



The image shows an 'Alert' dialog box with a light gray background. At the top, the title 'Alert' is in bold. Below it, the text reads: 'You are about to send a Change Host Name command to the selected device. Please enter a new host name for the selected device.' This is followed by a text input field with a red asterisk to its right. Below the input field, the text says: 'The device needs to be restarted for the new hostname to take effect. Please restart now or specify a future time.' Underneath this, there are two labels: 'Reboot:' and 'Time:'. The 'Reboot:' label is followed by a dropdown menu currently showing 'Later'. The 'Time:' label is followed by two dropdown menus, both showing '0', separated by a colon. Below these fields, the text asks 'Do you wish to proceed?'. At the bottom right, there are two buttons: 'Cancel' and 'Send Command'.

Figure 14. 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.

Apps and data

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

The screenshot shows the 'Apps & Data' tab in the Wyse Management Suite. The left sidebar contains navigation links: Dashboard, Groups & Configs, Devices, **Apps & Data**, Rules, Jobs, Events, Users, and Portal Administration. The main content area is titled 'Apps & Data – Thin Client App Inventory' and includes a local search bar. On the left, there are sections for 'App Inventory' (Thin Client, Wyse Software Thin Client), 'App Policies' (Thin Client, Wyse Software Thin Client), 'OS Image Repository' (WES / ThinLinux, ThinOS), 'OS Image Policies' (WES / ThinLinux), and 'File Repository' (Inventory). The main table displays the following data:

Name	Version	Repository Name	Size	Date Added	Status
7z920-x64.msi		Local repository - Wyse128206	1.3 MB	10/23/17 6:41 AM	✓
MerlinPackage_Common.exe		Local repository - Wyse128206	50.8 MB	10/23/17 6:41 AM	✓
WDA_13.0.0.167_x64.exe		Local repository - Wyse128206	35.6 MB	10/23/17 6:41 AM	✓
WDA_13.0.0.167_x64_WIE10.exe		Local repository - Wyse128206	35.6 MB	10/23/17 6:41 AM	✓
WDA_13.0.0.167_x86.exe		Local repository - Wyse128206	32.5 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3139398-v2-x86.msu		Local repository - Wyse128206	500.1 KB	10/23/17 6:41 AM	✓
Windows6.1-KB3139923-v2-x86.msu		Local repository - Wyse128206	1.8 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3146963-x86.msu		Local repository - Wyse128206	671.7 KB	10/23/17 6:41 AM	✓
Windows6.1-KB3147071-x86.msu		Local repository - Wyse128206	13.8 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3148851-x86.msu		Local repository - Wyse128206	474.7 KB	10/23/17 6:41 AM	✓
Windows6.1-KB3149090-x86.msu		Local repository - Wyse128206	4.3 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3156417-x86.msu		Local repository - Wyse128206	3.5 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3159398-x86.msu		Local repository - Wyse128206	1.2 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3161561-x86.msu		Local repository - Wyse128206	3.8 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3161664-x86.msu		Local repository - Wyse128206	1.3 MB	10/23/17 6:41 AM	✓
Windows6.1-KB3161949-x86.msu		Local repository - Wyse128206	664.5 KB	10/23/17 6:41 AM	✓
platform_util-1.0.12-0.3.x86_64.rpm		Local repository - Wyse128206	128.2 KB	10/23/17 6:41 AM	✓
platform_util-1.0.3-0.1.sle11sp3.rpm		Local repository - Wyse128206	146.9 KB	10/23/17 6:41 AM	✓
wda-2.0.11-00.1.sle11sp3.rpm		Local repository - Wyse128206	627.3 KB	10/23/17 6:41 AM	✓
wda-2.0.24-00.01.x86_64.rpm		Local repository - Wyse128206	403.7 KB	10/23/17 6:41 AM	✓

The footer of the page includes links for Terms & Conditions, Privacy Policy, and About, along with the copyright notice © 2017 Dell, a language selector set to English (US), and the text 'Powered by Cloud Client Manager'.

Figure 15. Apps and data

Windows Embedded Standard operating system image updates are performed in the **Apps and Data** tab.

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

- **Standard application**—This policy allows you to install a single application package.
- **Advanced application**—This policy allows you to deploy an application to current and all subgroups. You can deploy an operating system image to the current group only.

NOTE: Restart the system at the start and end of each policy deployment for Windows Embedded Standard devices. Since multiple applications can be packaged within a single advanced policy, restart the system twice to deploy the multiple applications.

You can configure the 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 the thin clients can be scheduled immediately or later, based on a specific time zone, or time zone that is configured on your device.

Topics:

- [Configuring app inventory](#)
- [Deploying applications to thin clients](#)
- [Adding Windows Embedded Standard operating system and ThinLinux images to inventory](#)
- [Managing ThinOS firmware inventory](#)
- [Managing Windows Embedded Standard and ThinLinux image policies](#)
- [Managing file repository](#)
- [Changing wallpaper for all devices belonging to marketing group](#)

Configuring app inventory

Prerequisites

This section allows you to view and add an application to the inventory. You have the following options:

- Mobile
- Thin Client
- Wyse Software Thin Client

Mobile app inventory

About this task

To add a mobile application, do the following:

Steps

1. Go to **Apps and Data > App Inventory > Mobile** tab.
2. You can select any one of the following options:
 - a. Click **Add Apps** to add an application, and do the following:
 - i. From the **Search Type** drop-down menu, select your preferred option.
 - ii. Enter the application name.
 - iii. From the **Country** drop-down menu, select your preferred option.
 - iv. Click **Search**.
 - b. Click **Add Enterprise App** to add an enterprise application, and select any one of the following options:
 - **Upload application to repository**—Click **Browse** and select an enterprise iOS application or android application to upload to the application Inventory.
 - **Link to Enterprise Application**—Enter the link to secure the webserver hosting enterprise iOS application or android application.

Configuring thin client and Wyse Software thin client app inventory

About this task

To configure an application to the thin client and Wyse Software thin client inventory, do the following:

Steps

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, do the following:
 - a. 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.

- b. Place the Windows Embedded Standard imaging files in the <repo-dir>\repository\osImages\Zippedfolder. The image is automatically extracted and placed in a valid folder. The image is listed in the Windows Embedded Standard image inventory.

Deploying applications to thin clients

The standard application policy allows you to install a single application package and requires reboot before and after installing each application. Using the advanced application policy, you can install multiple application packages with only two reboots. The advanced application policy also supports execution of pre and post installation scripts that may be needed to install a particular application. For more information, see [Appendix B](#).

Creating and deploying advanced application policy to thin clients

About this task

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

1. Copy the application and the pre or post install scripts to deploy to the thin clients in the `thinClientApps` folder in the local repository or the Wyse Management Suite repository.
2. Go to **Apps & Data > App Inventory** and select **Thin Client** to verify if the application is registered.
3. Click **Thin Client** under **App Policies**.
4. Click **Add Advanced Policy**.

Figure 16. Add Advanced App Policy

Table 233. Add advanced app policy

Parameter	Description
Policy Name	Enter the name of the policy.
Group	Allows you to select the group to assign the policy.
Sub Groups	Select the check box to include all the sub groups.

Table 233. Add advanced app policy (continued)

Parameter	Description
Task	Allows you to specify the task for the policy. From the drop-down menu, select the task.
OS Type	Allows you to select the OS type for the policy.
Application	Allows you to add or remove the application from the policy. Click the Add app option and select the preferred application. NOTE: The preferred order of the package update is RTME, FR, TCX, and Blast.
OS Subtype Filter	Allows you to select the filter for the OS subtype.
Platform Filter	Allows you to select the platform filter.
Apply Policy Automatically	From the Apply Policy Automatically drop-down menu, select one of the following option: <ul style="list-style-type: none"> Do not apply automatically—The image policy is not applied automatically to a device registered with Wyse Management 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.
Max retries	Allows you to select the number of retries to execute the policy. From the drop-down menu, select the number.

Adding Windows Embedded Standard operating system and ThinLinux images to inventory

Prerequisites

Prerequisites

- If you are using Wyse Management Suite with cloud deployment, go to **Portal Administration > Console Settings > File Repository**. Click **Download version 1.1** to download the WMS_Repo.exe file and install the Wyse Management Suite repository installer. For more information, see [File repository](#).
- If you are using Wyse Management Suite with on-premise deployment, the local repository is installed during Wyse Management Suite installation process.

About this task

To add an image to the inventory folder on your system, do the following:

Steps

- 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 compressed 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.

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.

Managing ThinOS firmware inventory

To add a file to the ThinOS image inventory, do the following:

Steps

1. In the **Apps & Data** tab, under **OS Image Repository**, click **WTOS**.
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.
 **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**.

Managing Windows Embedded Standard and ThinLinux image policies

About this task

To add a file to the Windows Embedded Standard image or ThinLinux policy, do the following:

Steps

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 thin client 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**.

Changing 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.

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:

- [Registering unmanaged devices](#)
- [Creating unmanaged device auto assignment rules](#)
- [Alert Notification](#)

Registering unmanaged devices

Configure the rules for unmanaged devices by using the **Registration** option.

You can select the **Notification Target** or disable the alert notification for the following:

- Group Admin
- Global Admin
- Global and Group Admin

NOTE: The notification frequency can be configured for every 4 hours, every 12 hours, daily, or weekly basis to the target device.

By default, registration of unmanaged devices are unregistered after 30 days and can be configured by using the **Apply rule after** option.

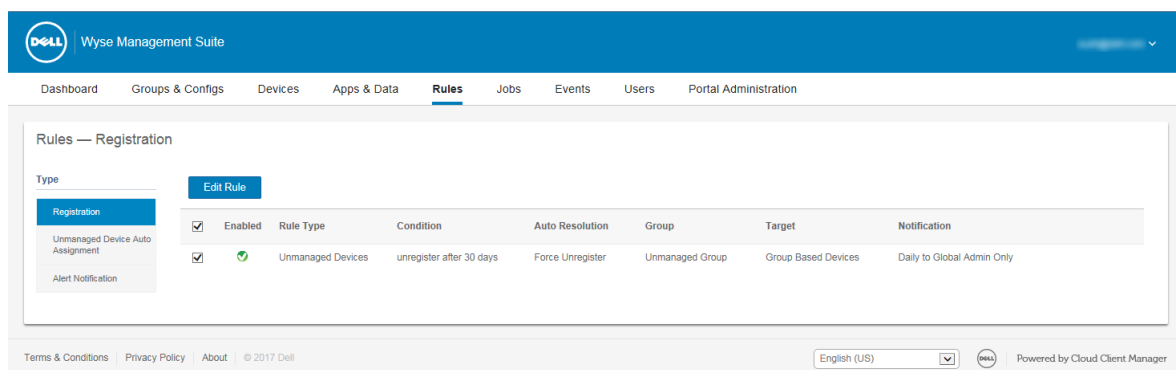
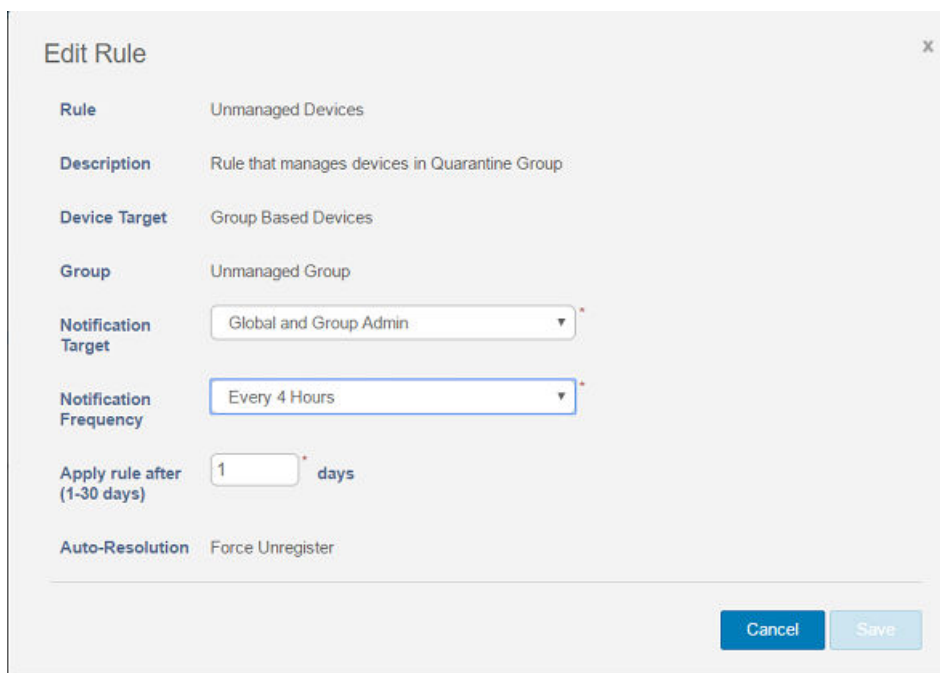


Figure 17. Registration of unmanaged devices

To edit a rule, do the following:

1. Click the **Edit Rule** option.
2. From the drop-down list, select a target client to apply the **Notification Target** option and the time duration to apply the **Notification Frequency** option.
3. Enter the number of day until you want to apply the rule.



Edit Rule

Rule Unmanaged Devices

Description Rule that manages devices in Quarantine Group

Device Target Group Based Devices

Group Unmanaged Group

Notification Target Global and Group Admin

Notification Frequency Every 4 Hours

Apply rule after (1-30 days) 1 days

Auto-Resolution Force Unregister

Cancel Save

Figure 18. Edit Rule

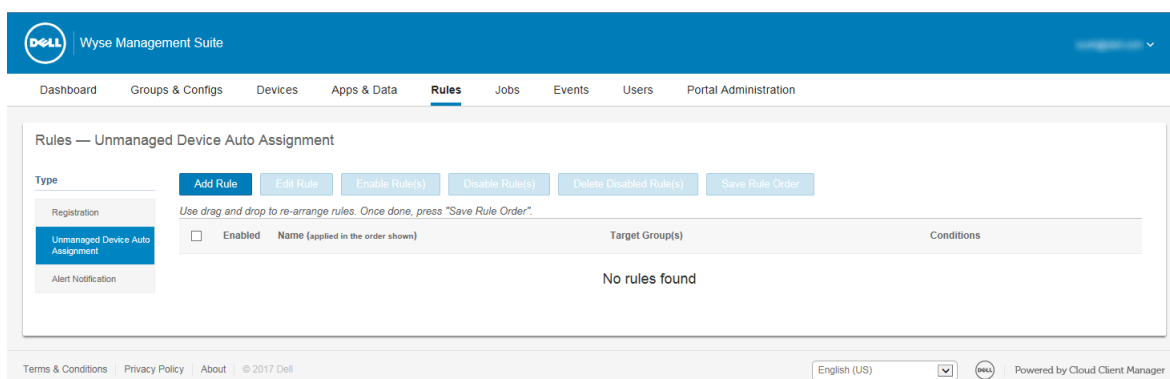
4. Click **Save**.

Creating unmanaged device auto assignment rules

To create rules for the unmanaged device auto assignment, do the following:

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.



Wyse Management Suite

Dashboard Groups & Configs Devices Apps & Data **Rules** Jobs Events Users Portal Administration

Rules — Unmanaged Device Auto Assignment

Type

Registration

Unmanaged Device Auto Assignment

Alert Notification

Add Rule **Edit Rule** **Enable Rule(s)** **Disable Rule(s)** **Delete Disabled Rule(s)** **Save Rule Order**

Use drag and drop to re-arrange rules. Once done, press "Save Rule Order".

Enabled	Name (applied in the order shown)	Target Group(s)	Conditions
No rules found			

Terms & Conditions Privacy Policy About © 2017 Dell English (US) Powered by Cloud Client Manager

Figure 19. Unmanaged Device Auto Assignment Rules

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

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Select the rule and click the **Edit** option.
4. Click **Save**.

Disabling and deleting rule

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Select a rule and click the **Disable Rule** option.
4. Click the **Delete Disabled Rule(s)** option.

Saving rule order

If multiple rules are present, then you can change the order of a rule to be applied on the devices.

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**.

Alert Notification

You can select **Notification Target** or disable the alert notification for the following:

- Group Admin
- Global Admin
- Global and Group Admin

NOTE: The notification frequency can be configured for every 4 hours, every 12 hours, daily or weekly basis to the target client.

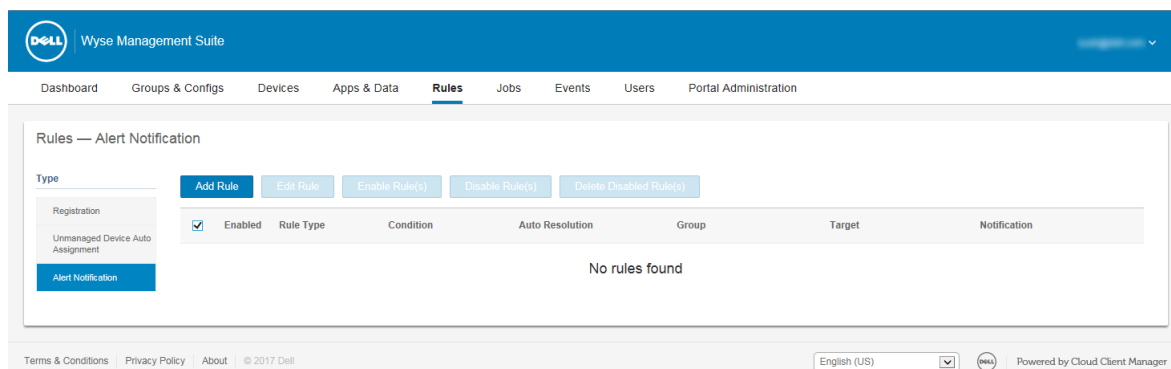


Figure 20. Alert Notification

1. To add a rule, click the **Add Rule** option and enter the following details:
 - a. From the drop-down list, select **Rule**.

- b. Enter the **Description**.
- c. From the drop-sown list, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.

Add Rule

Rule

Device Health Notification

Description

Device Target

Edge Gateway, Embedded PC and Thin Client

Group

All Groups

Notification Target

<select one>

Notification Frequency

<select one>

Cancel

Save

Figure 21. Add Rule

- 2. Click **Save**.

Managing Jobs

This section describes how to schedule and manage jobs in the management console.

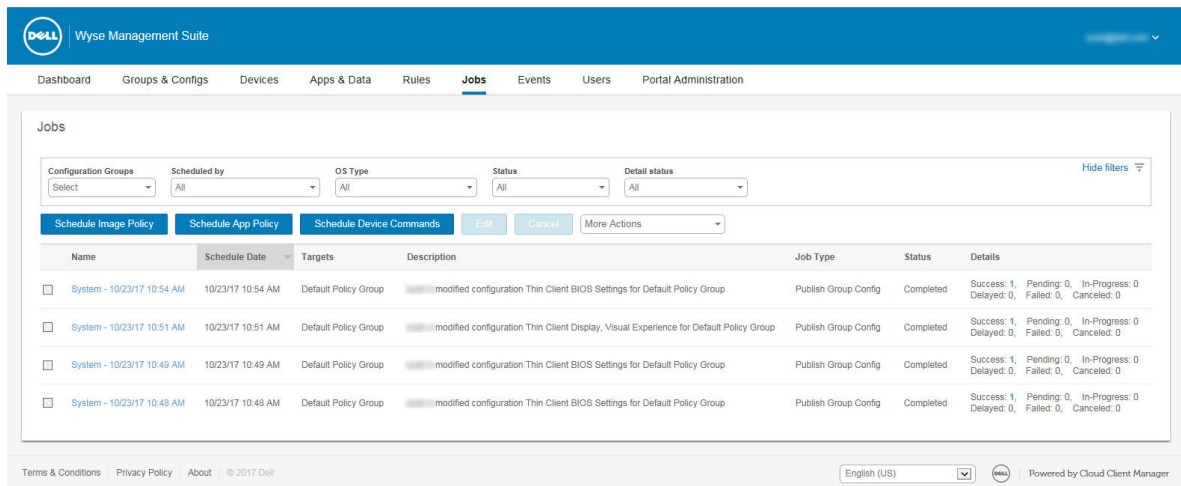


Figure 22. Jobs

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](#)
- [Scheduling the image policy](#)
- [Scheduling the application policy](#)
- [Scheduling the device command job](#)

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**.

Scheduling the image policy

About this task

Image policy is not a recurring job. Each command is specific to a device. To schedule an image policy, do the following:

Steps

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 the application policy

About this task

Application policy is not a recurring job. Each command is specific to a device. To schedule an application policy, do the following:

Steps

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

About this task

To schedule a device command job, do the following:

Steps

1. On the **Jobs** page, click the **Schedule device command job** option.
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.

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.

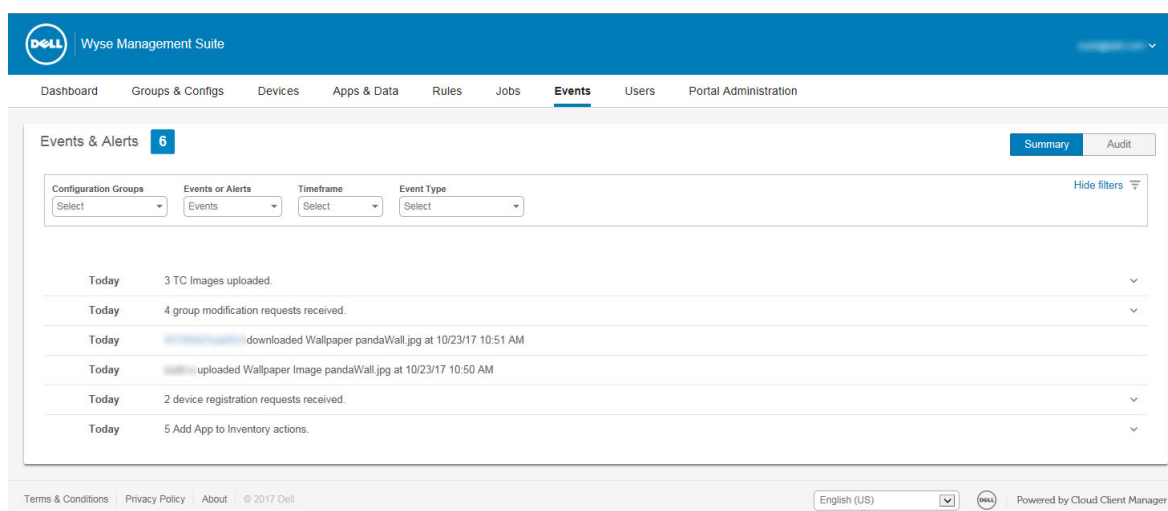


Figure 23. Events

Topics:

- [Viewing a summary of events](#)
- [Viewing audit log](#)

Viewing a summary of events

Prerequisites

The **Events and Alerts** window displays all the events and alerts that have taken place in the system. To log in to **Events and Alerts**, go to **Events > Summary**.

About this task

The following are the options that are available for which all the events can be easily distinguished:

- **Configuration Groups**—To select the Configuration Group, click the drop-down menu. The following options are displayed:
 - Default Policy Group
 - Unmanaged Group
- **Event**—To select the Event type, click the drop-down menu. The following options are displayed:
 - Events
 - Current Alerts
 - Alert History
- **Timeframe**—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
- **Event Groups**—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 audit log

Prerequisites

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.

Steps

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)

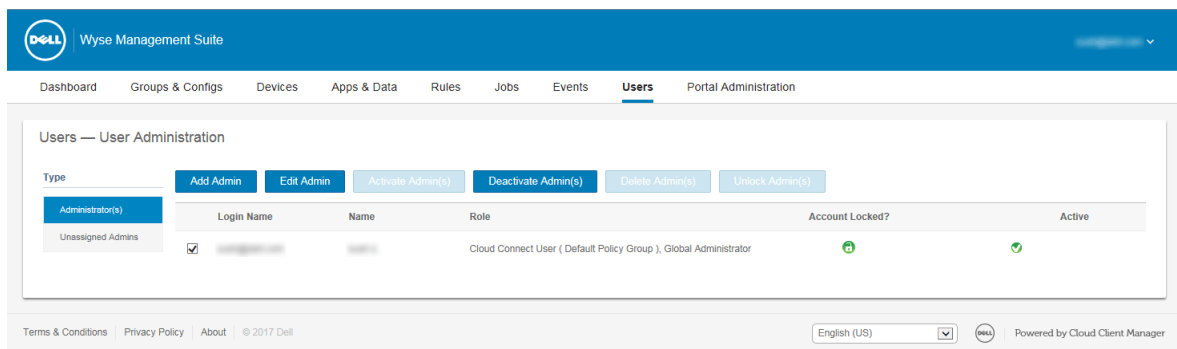


Figure 24. Administrator

- **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)

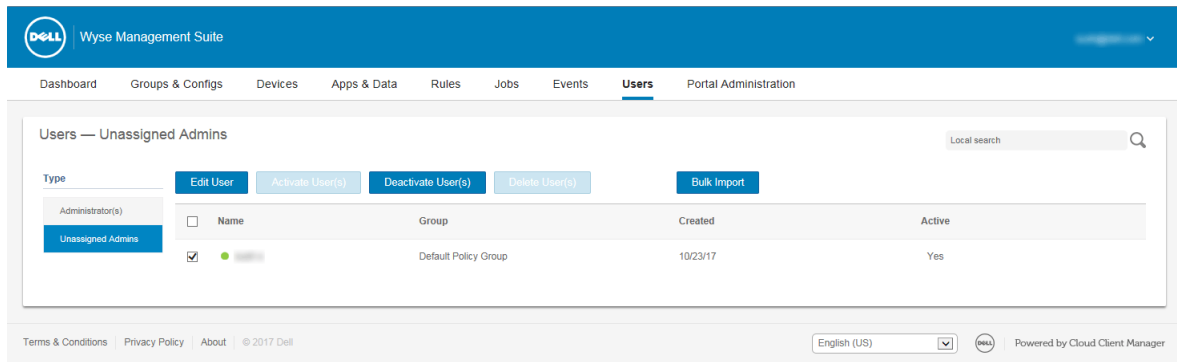


Figure 25. Unassigned admins

NOTE: To import users from the CSV file, click **Bulk Import**.

Topics:

- [Adding new admin user](#)
- [Editing admin user](#)
- [Deactivating admin account](#)
- [Deleting admin](#)

Adding new admin user

Prerequisites

To add an admin user, do the following:

Steps

1. Enter your email ID and user name in the respective fields.
2. Select the check box to use the same user name as mentioned in the email.
3. 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:
 - a. In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
 - b. In the **Password** section, do the following:
 - i. Enter the custom password.
 - ii. To generate any random password, select the **Generate random password** radio button.
4. Click **Save**.

Editing admin user

Prerequisites

To edit an admin user, do the following:

Steps

1. 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.

2. 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:
 - a. In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
 - b. In the **Password** section, do the following:
 - i. Enter the custom password.
 - ii. To generate any random password, select the **Generate random password** radio button.
3. Click **Save**.

Deactivating admin account

About this task

Deactivating the user account 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:

Steps

1. From the list, select a user and click **Deactivate Admin(s)**.
An alert window is displayed.
2. Click **OK**.

Deleting admin

Prerequisites

Users must be deactivated before you delete them. To delete a user, do the following:

Steps

1. Select the check box of a particular user or users which you want to delete.
2. From the **More Actions** drop-down menu, select **Delete User(s)**.
3. Click **Yes**.

Portal administration

This section contains a brief overview of your system administration tasks that are required to set up and maintain your system.

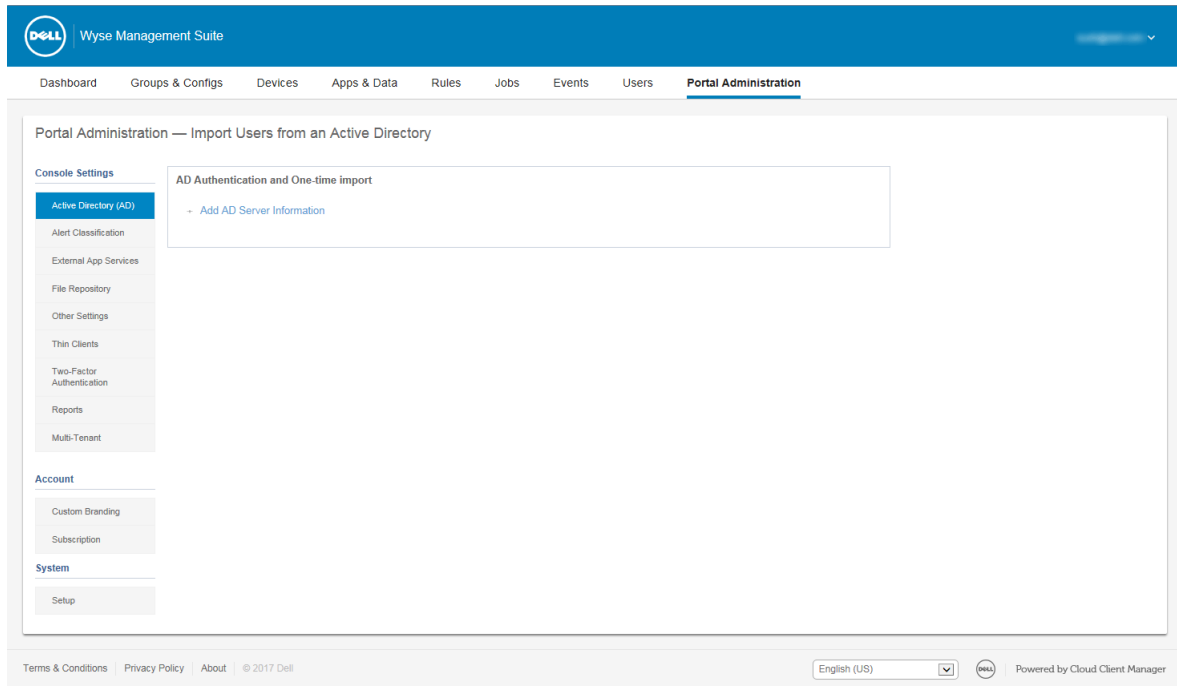


Figure 26. Portal admin

Topics:

- [Configuring console settings](#)
- [Configuring account settings](#)
- [System setup](#)

Configuring console settings

This section helps you to configure settings for the Wyse Management Suite console.

Active Directory


About this task

To import Active Directory users on the Wyse Management Suite private cloud, do the following:

Steps

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.
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.

Next steps

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.


Active Directory Federation Services feature on public cloud

About this task


To configure Active Directory Federation Services (ADFS) on a public cloud, do the following:

Steps

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](https://technet.microsoft.com/en-us/windowsserver/dd448613).

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

External application services

Prerequisites

This section allows you to create secured Application Programming Interface (API) accounts. This service provides the ability to create special accounts.

About this task

To configure the external application service, do the following:

Steps

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**.

File repository

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 validate the file repository certificate to download the files.
 - e. Add a note in the provided box.
 - f. Click **Save Settings**.

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.

Two-Factor authentication

You must have at least two active global administrator users in the system.

Prerequisites

Create two or more global administrators before proceeding to the task.

About this task

To enable two factor authentication, do the following:

1. You must select the check box to enable the two factor authentication.

NOTE: Administrators must verify the second authentication factor using one time passcodes to log in to the management portal.

2. 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

About this task

To generate the reports, do the following:

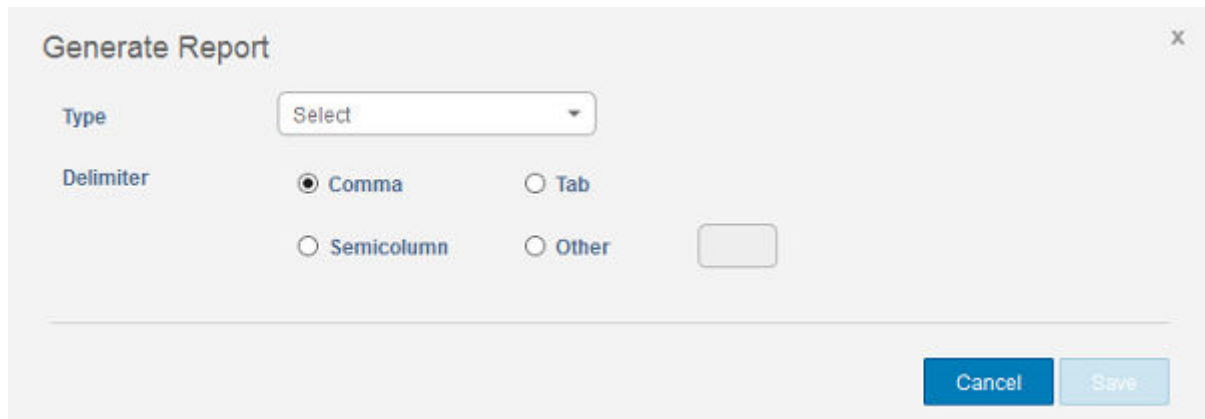


Figure 27. Generate report

Steps

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.

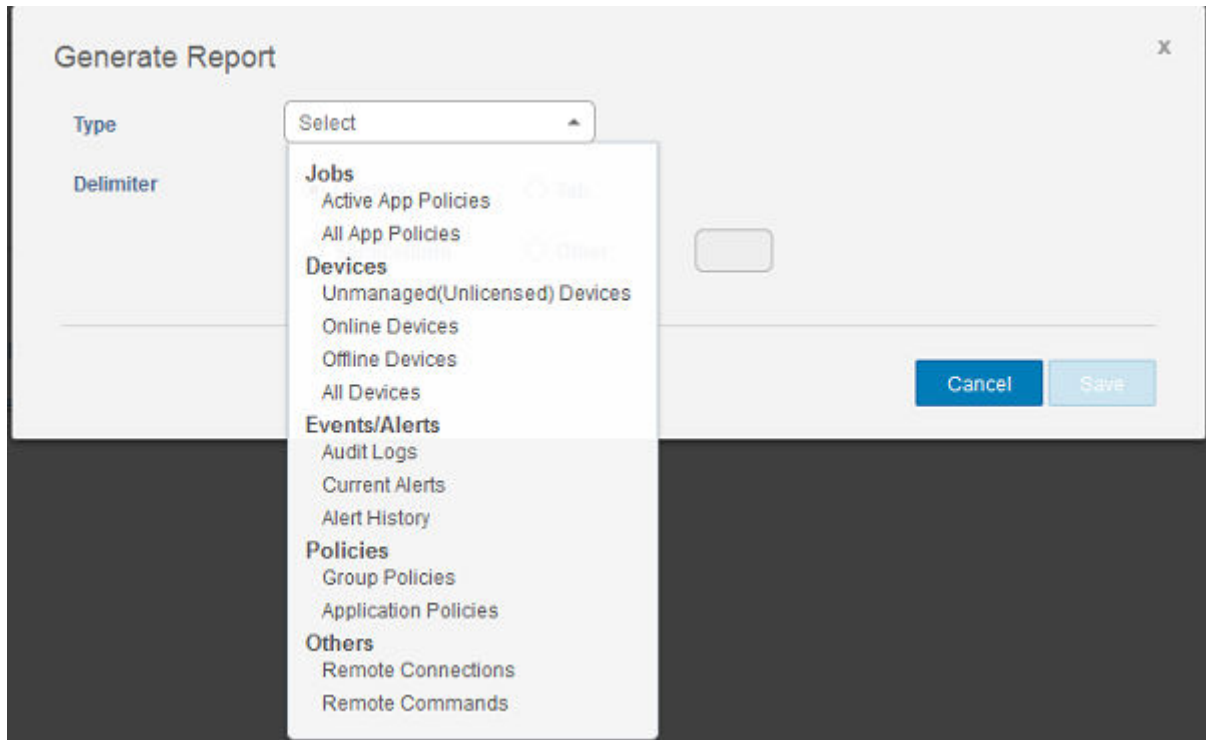


Figure 28. Types of report

4. Select the delimiter.
5. Click **Save**.

Multi Tenant

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.

1. Select the check box to enable multi-tenant option.
2. Enter the following details:
 - User name
 - Password
 - Confirm password
 - Email
3. Click **Save Settings**.

Configuring account settings

This section helps you to configure account settings for Wyse Management Suite console.

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.


About this task

To access and specify custom branding:

Steps

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**.

License subscription

About this task

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)**

System setup

This section provides the information about the following:

1. **Certificate validation**—Select the check box to perform server certificate validation for all device-to-server communication.
2. **Update SMTP for Email Alerts**

Enter the following details:

- SMTP server
- Send from address
- Username
- Password
- Test address

Current Certificate: It provides the information about the current certificate.

3. 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.

4. Click **Save**.

Installing or upgrading Wyse Device Agent

Prerequisites

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 <https://www.dell.com/support/home> 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

Prerequisites

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:

Steps

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

About this task

To install Wyse Device Agent manually, do the following:


Steps

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

About this task



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:
 - Wyse Device Manager
 - Using INI parameters
 - Add-ons Manager
 - RPM commands

Steps

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.
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 234. 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
Delegated administration	Not supported	Supported	Supported
Dynamic group creation and assignment based on device attributes	Not supported	Supported	Supported

Table 234. Feature matrix for each subscription type (continued)

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
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

 **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

The following table lists the supported thin clients on Wyse Management Suite:

Table 235. 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	1.0.3 WDA version 2.0.24-00.01 and later Platform Utility version 1.0.12-03 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	895 WDA versions 14.x and later. merlin version 3.4.6 and later
Windows Embedded Standard 7P (WES7P)	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client Wyse 7010 Extended thin client	896 WDA versions 14.x and later. merlin version 3.4.6 and later
	Wyse 7040 thin client	7020 WDA versions 14.x and later. merlin version 3.4.6 and later
	Latitude 3460 mobile thin client	7041 WDA versions 14.x and later. merlin version 3.4.6 and later
	Latitude E7270 mobile thin client	7010 WDA versions 14.x and later. merlin version 3.4.6 and later

Table 235. Supported thin clients (continued)

Operating System	Device Type	Build number
	Wyse 5060 thin client	7038 WDA versions 14.x and later. merlin version 3.4.6 and later
Windows 10 IoT Enterprise (WIE10)	Wyse 5020 thin client Wyse 7020 thin client Latitude 3480 mobile thin client Latitude 5280 mobile thin client	0A0F WDA versions 14.x and later. merlin version 3.4.6 and later
Windows Embedded 8 Standard (WE8S)	Wyse 5010 thin client Wyse 7010 thin client Wyse 5020 thin client Wyse 7020 thin client	924 WDA versions 14.x and later. merlin version 3.4.6 and later
ThinOS	Wyse 5040 AIO Wyse 3010 thin client 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	8.3 HF, 8.4 Firmware version 8.4_009

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 the Wireless Profiles Password Editor](#)
- [Limitations of Wireless Profiles Password Editor](#)

Configuring the Wireless Profiles Password Editor

To configure the wireless profiles password editor, do the following:

Steps

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.

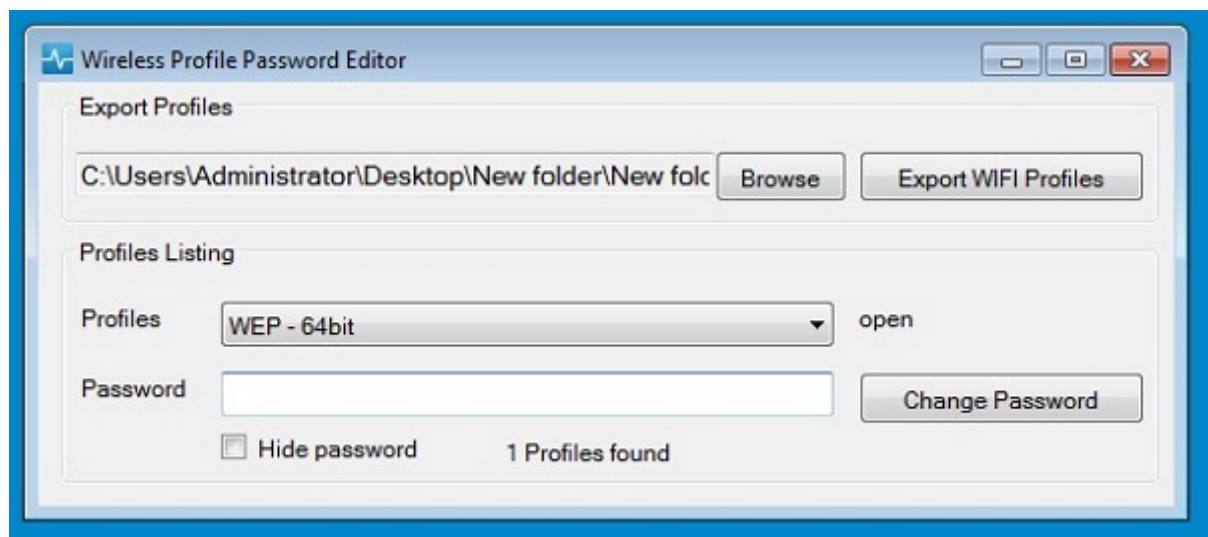


Figure 29. Wireless Profiles Password Editor

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 inventory](#)

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

Creating and configuring DHCP option tags

About this task

To create a DHCP option tag, do the following:

Steps

1. Open the Server Manager.
2. Go to **Tools** and click **DHCP option**.
3. Go to **FQDN > IPv4** and right-click **IPv4**.

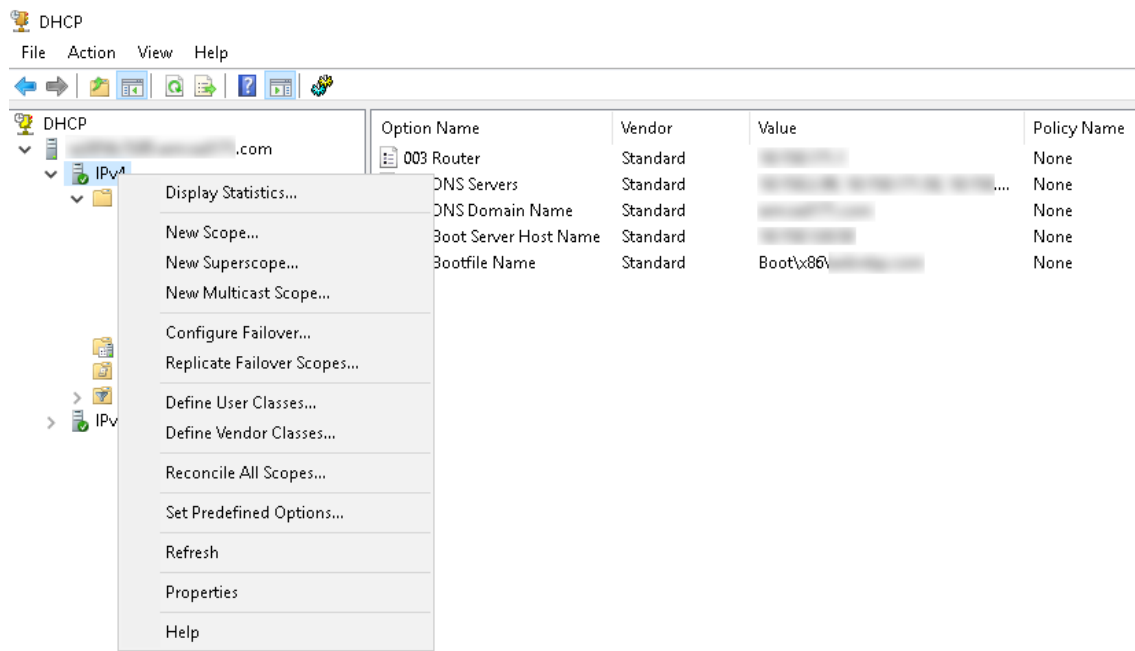


Figure 30. DHCP

4. Click **Set Predefined Options**.
The **Predefined Options and Values** window is displayed.
5. From the **Option class** drop-down menu, select the **DHCP Standard Option** value.

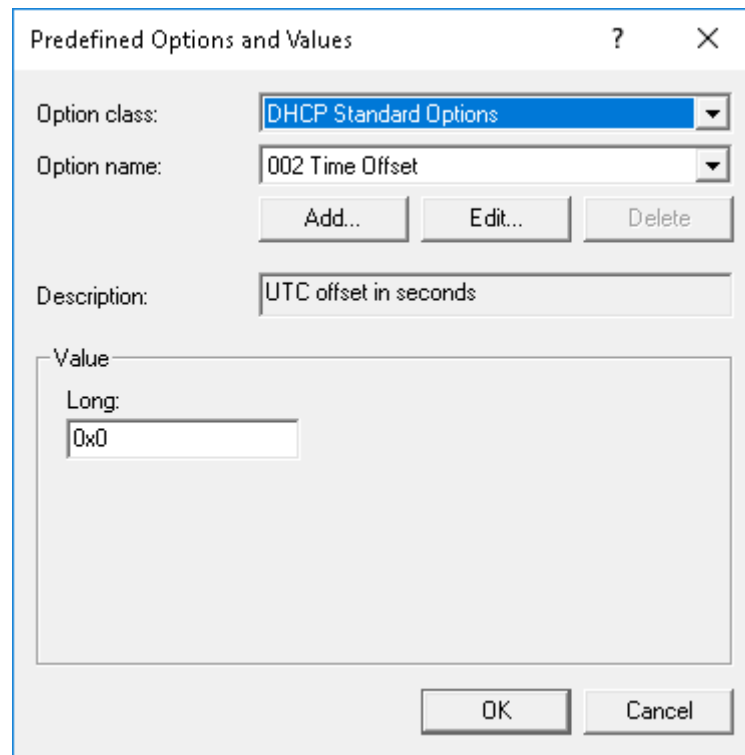


Figure 31. Predefined Options and Values

6. Click **Add**.
The **Option Type** window is displayed.

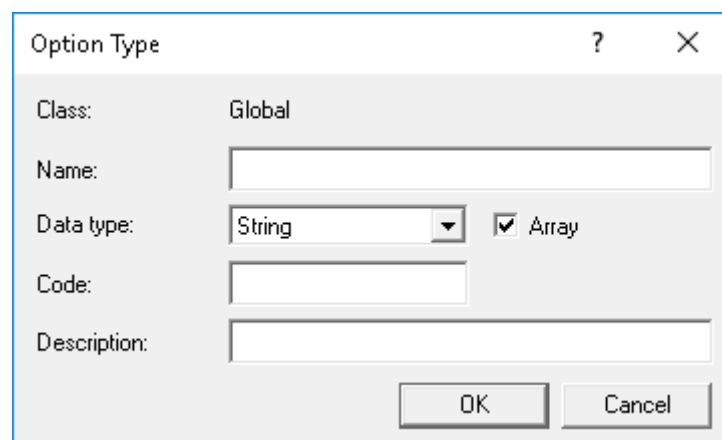


Figure 32. Option Type

Example

The options need to 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:
 1. Enter the following values and click **OK**.
 - Name—WMS
 - Data type—String
 - Code—165
 - Description—WMS_Server
 2. Enter the following value and then click **OK**.

String—WMS FQDN

For example, WMSServerName.YourDomain.Com:443.

The screenshot shows a Windows-style dialog box titled "Predefined Options and Values". It has a standard title bar with a question mark and a close button. Inside the dialog, there are several input fields and buttons. The "Option class:" field is a dropdown menu currently showing "DHCP Standard Options". The "Option name:" field is another dropdown menu showing "165 WMS". Below these are three buttons: "Add...", "Edit...", and "Delete". The "Description:" field is a text box containing "WMS_Server". Below the description is a section titled "Value" which contains a "String:" label and a text box with the value "WMSServerName.YourDomain.Com:443". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Figure 33. 165 Wyse Management Suite server URL option tag

- To create the 166 MQTT server URL option tag, do the following:

1. Enter the following values and click **OK**.
 - Name—MQTT
 - Data type—String
 - Code—166
 - Description—MQTT Server

2. Enter the following value and click **OK**.

String—MQTT FQDN

For example, WMSServerName.YourDomain.Com:1883

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 166 MQTT Server

Add... Edit... Delete

Description: MQTT Server

Value

String: WMSServerName.YourDomain.Com:1883

OK Cancel

Figure 34. 166 Wyse Management Suite server URL option tag

- To create the 167 Wyse Management Suite CA Validation server URL option tag, do the following:
 1. Enter the following values and click **OK**.
 - Name—CA Validation
 - Data type—String
 - Code—167
 - Description—CA Validation
 2. Enter the following values, and click **OK**.
 - String—TRUE/FALSE

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 167 CA Validation

Add... Edit... Delete

Description: CA Validation

Value

String: FALSE

OK Cancel

Figure 35. 167 Wyse Management Suite server URL option tag

- To create the 199 Wyse Management Suite Group Token server URL option tag, do the following:
 1. Enter the following values and click **OK**.
 - Name—Group Token
 - Data type—String
 - Code—199
 - Description—Group Token
 2. Enter the following values and click **OK**.
 - String—defa-quarantine

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 199 Group token key

Add... Edit... Delete

Description: Group token key

Value

String: defa-quarantine

OK Cancel

Figure 36. 199 Wyse Management Suite server URL option tag

Creating and configuring DNS SRV records

About this task

To create a DNS SRV record, do the following:

Steps

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.

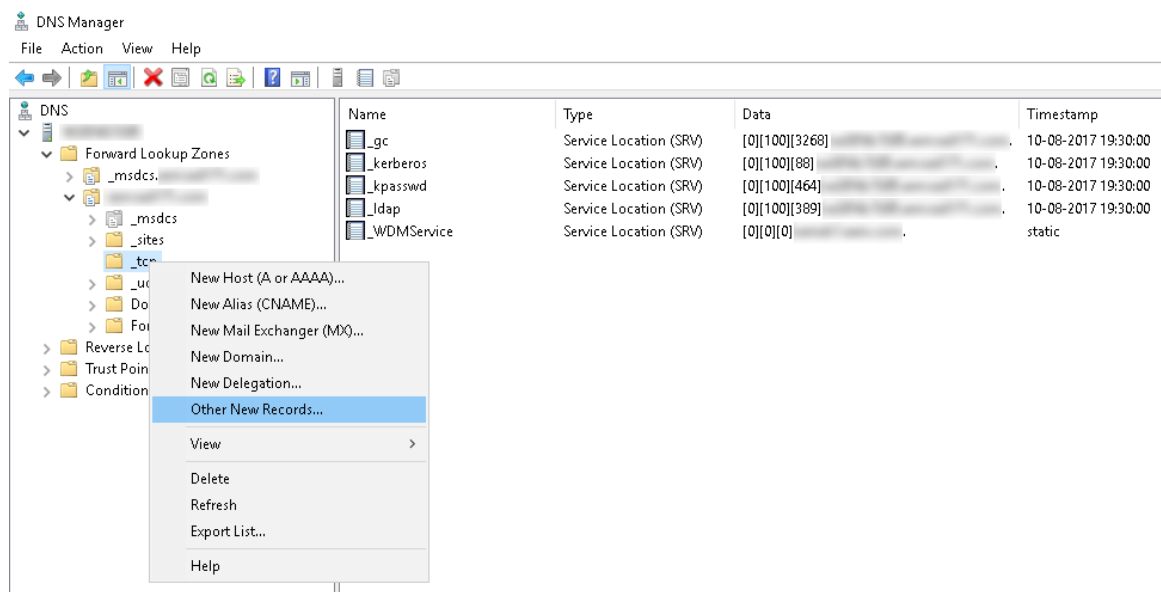


Figure 37. DNS Manager

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:

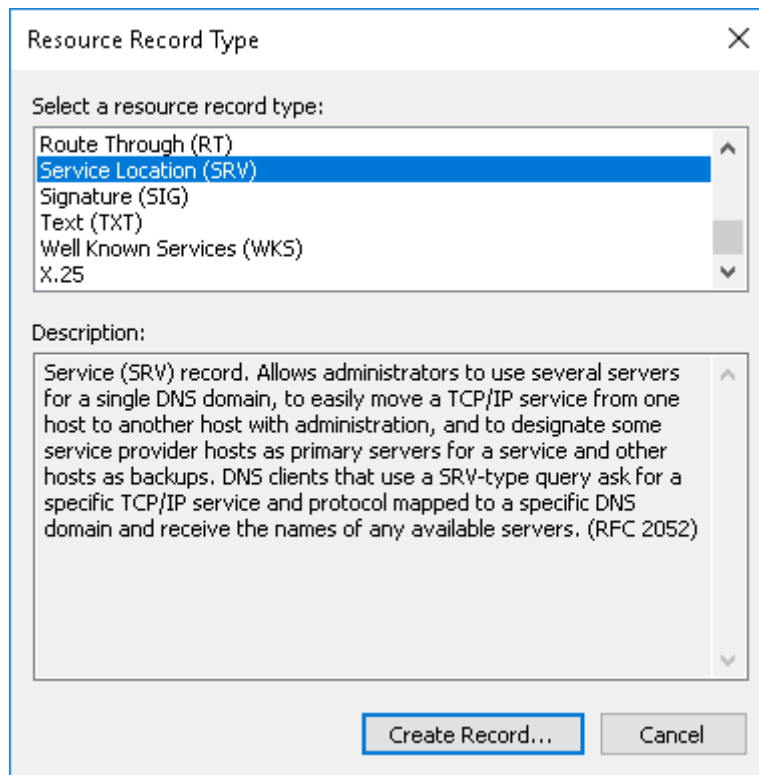


Figure 38. Resource Record Type

- 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

New Resource Record

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

Figure 39. _WMS_MGMT service

- b. To create MQTT server record, enter the following values, and then click **OK**.
- Service—_WMS_MQTT
 - Protocol—_tcp
 - Port number—1883
 - Host offering this service—FQDN of MQTT server

New Resource Record

Service Location (SRV)

Domain: .

Service: _WMS_MQTT

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 1883

Host offering this service:
FQDN of MQTT server

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

Figure 40. _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:

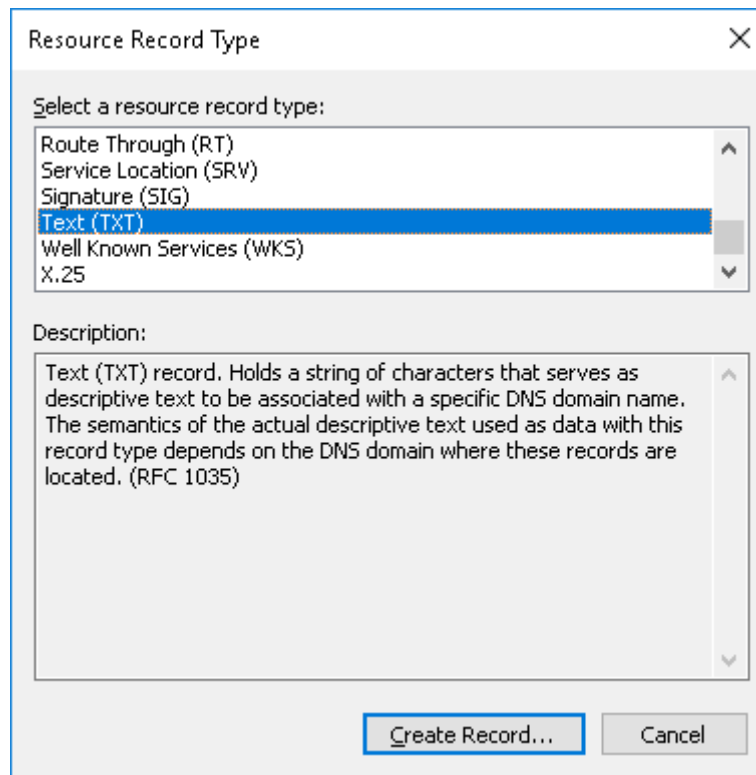


Figure 41. Resource Record Type

- a. To create Wyse Management Suite Group Token record, enter the following values, and click **OK**.
- Record name— `_WMS_GROUPTOKEN`
 - Text—WMS Group token

The image shows a 'New Resource Record' dialog box with a 'Text (TXT)' tab. It contains three input fields: 'Record name (uses parent domain if left blank):' with the value '_WMS_GROUPTOKEN', 'Fully qualified domain name (FQDN):' with the value '_WMS_GROUPTOKEN.', and a 'Text:' text area with the value 'WMS Group token'. At the bottom are 'OK' and 'Cancel' buttons, with 'OK' being the active button.

Figure 42. _WMS_GROUPTOKEN record name

- b. To create Wyse Management Suite CA validation record, enter the following values, and then click **OK**.
- Record name—_WMS_CAVVALIDATION
 - Text—TRUE/FALSE

New Resource Record

Text (TXT)

Record name (uses parent domain if left blank):

_WMS_CAVALIDATION

Fully qualified domain name (FQDN):

_WMS_CAVALIDATION._

Text:

False

OK Cancel

Figure 43. _WMS_CAVALIDATION record name