Dell Wyse Management Suite

Version 3.3 Administrator's Guide

July 2021
Rev. A00

Notes, cautions, and warnings

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

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

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

Contents

1

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 Hybrid Client powered endpoints and Dell thin clients. It also offers advanced feature options such as cloud and 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.

Topics:

Editions of Wyse Management Suite

Wyse Management Suite is available in the following editions:

- **Standard (Free)**—The Standard edition of the Wyse Management Suite offers basic functionalities and is available only for a private cloud deployment. You do not require a license key to use the Standard edition. This version can only manage Dell Thin Clients. The Standard edition is suitable for small and medium businesses.
- **Pro (Paid)**—The Pro edition of the Wyse Management Suite is a more robust solution. It is available for both public and private cloud deployment. A license key is required to use the Pro edition (subscription-based licensing). With the Pro solution, organizations can adopt a hybrid model and float licenses between private and public clouds if required. This version is required to manage any Teradici-based devices, Wyse Covert for PCs-based thin clients, Dell Hybrid Client devices, Embedded PC, and Edge Gateway devices. It also offers more advanced features to manage Dell thin clients. For a public cloud deployment, the Pro edition can be managed on non-corporate networks such as home office, third party, partners, mobile thin clients, and so on.

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

  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 U.S. and Germany. Customers in countries with data residency restrictions may not be able to take advantage of the cloud-based service.

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

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

Wyse Management Suite Feature Matrix

The following table provides information about the features that are supported for each subscription type.

Table 1. 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 thousand devices	Up to 120 thousand devices	Up to 1 million devices
License term	Free download	Per seat subscription	Per seat subscription
License key	Not required	Required	Required
Architecture	Private cloud	Private cloud	Public cloud
Flexible deployment or hybrid cloud	X	√	√
Advanced installer	X	√	√
Multi-tenancy	X	√	√
Delegated Administration for permissions granularity	X	√	√
Multiple repositories to support your distributed architecture	X	√	√
Option to configure Wyse Management Suite server alias	X	√	√
High Availability reference architecture	X	√	X
Proxy support—SOCKS5 and HTTPS	√	√	√
API support	X	√	X
Dell ProSupport for Software included	X	√	√
Dell Endpoints			
OptiPlex 7070 Ultra with Dell Hybrid Client	X	√	√
OptiPlex 3090 Ultra and 7090 Ultra with Dell Hybrid Client	X	√	√
Latitude 3320 with Dell Hybrid Client	X	√	√
Wyse 5070 with Dell Hybrid Client	X	√	√
Wyse thin clients with ThinOS	√	√	√
Wyse thin clients with ThinLinux	√	√	√
Wyse thin clients with Windows 10 IoT Enterprise	√	√	√
Wyse PCoIP zero clients (Teradici firmware)	X	√	√
Software thin clients with Wyse Converter for PCs	X	√	√
Reporting and Monitoring			
Localized management console	X	√	√
Alerts, Events, and Audit log using email and mobile application	X	√	√
Enterprise-Grade Reporting	X	√	√

The following table provides information about the Dell Hybrid Client management features supported for each subscription type.

Table 2. Dell Hybrid Client management feature matrix

Dell Hybrid Client management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Complete Asset Visibility			
Automatic device discovery	X	√	√
Asset, Inventory, and systems management	X	√	√
View effective configuration at device Wyse Management Suite level after inheritance	X	√	√
Security			
Secure communication (HTTPS)	X	√	√
Secure MQTT	X	√	√
Multi-factor authentication	X	√	√
Active Directory authentication for role-based administration	X	√	√
AD mapping using LDAPs	X	√	√
Single-sign-on	X	√	√
Lockdown settings (enable/ disable ports of supported endpoints)	X	√	√
Comprehensive Management			
Operating system Patch and Image management	X	√	√
Smart Scheduling	X	√	√
Silent Deployment	X	√	√
Bundle applications to simplify deployment and minimize reboots	X	√	√
Dynamic group creation and assignment based on device attributes	X	√	√
Repository assignment to application policy and subnet mapping	X	√	√
Advanced App Management and app policy	X	√	√
User Group inheritance	X	√	√
End-User Exception	X	√	√

Table 2. Dell Hybrid Client management feature matrix (continued)

Dell Hybrid Client management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Automatic unregistering of devices	X	√	√
Configuration			
Dell Hybrid Client wizard configuration	X	√	√
Multi-Monitor Support	X	√	√
Follow-me Profile	X	√	√
File affiliation to prioritize application delivery mode	X	√	√
BIOS settings and configuration support	X	√	√
Export or import policy configurations	X	√	√
Default user group policy	X	√	√
Browser configuration	X	√	√
Configure cloud provider	X	√	√
Dell signed applications automated update	X	√	√
User personalization data roaming	X	√	√
Configure VNC	X	√	√
Configure SSH	X	√	√

NOTE: Upgrade the system to 12 GB RAM as there is more memory requirement to enable secure communication.

NOTE: For a standard license, you can use secure MQTT connection (8443) by blocking the port 1883 from Wyse Management Suite server installed system using Windows Firewall.

The following table provides information about the Wyse thin clients and zero clients management features supported for each subscription.

Table 3. Wyse thin clients and zero clients management feature matrix

Wyse thin clients and zero clients management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Complete Asset Visibility			
Automatic device discovery	√	√	√
Asset, Inventory, and systems management	√	√	√
View effective configuration at device level after inheritance	√	√	√
Reporting and Monitoring			
Remote shadow using VNC	√	√	

Table 3. Wyse thin clients and zero clients management feature matrix (continued)

Wyse thin clients and zero clients management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Configurable heartbeat and check-in interval	√	√	√
Security			
Secure communication (HTTPS)	√	√	√
802.1x certificate deployment	√	√	√
Secure MQTT	√	√	√
Two-factor authentication	X	√	√
Active Directory authentication for role-based administration	X	√	√
Domain join feature (Windows 10 IoT Enterprise)	X	√	√
AD mapping using LDAPs	X	√	√
Lockdown settings (enable or disable ports of supported endpoints)	X	√	√
Comprehensive Management			
Operating system Patch and Image management	√	√	√ **
Smart Scheduling	√	√	√
Silent Deployment	√	√	√
Bundle applications to simplify deployment and minimize reboots	X	√	√
Dynamic group creation and assignment based on device attributes	X	√	√
Repository assignment to application policy and subnet mapping	X	√	√
Automatic unregister of devices	√	√	√
Advanced app policy	X	√	√
Configuration			
Wyse ThinOS 8.x and 9.x wizard configuration	√	√	√
Multi-Monitor Support	√	√	√
Wyse Easy Setup and Wyse Overlay Optimizer	√	√	√
Scripting Support for customizing application installation	X	√	√

Table 3. Wyse thin clients and zero clients management feature matrix (continued)

Wyse thin clients and zero clients management features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
BIOS settings and configuration support	X	√	√
Export/import policy configurations	X	√	√
RSP package support	X	√	√
WDM import tool	X	√	X
Bulk device exception	X	√	√

NOTE: **Double asterisk indicates that for ThinLinux and Windows 10 IoT Enterprise operating systems, an on-premise repository is required when you use the Wyse Management Suite public cloud environment.

NOTE: Upgrade the system to 12 GB RAM as there is more memory requirement to enable secure communication.

NOTE: For a standard license, you can use secure MQTT connection (8443) by blocking the port 1883 from Wyse Management Suite server installed system using Windows Firewall.

What is new in Wyse Management Suite version 3.3

- Supports Wyse Management Suite public cloud repository for Dell Hybrid Client packages.
- Supports configuring Edge browser, based on Chromium, settings for Windows 10 IoT Enterprise devices.
- Supports configuring email notification to tenants before the license is expires.

2

Getting started with Wyse Management Suite

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

Topics:

Log in to Wyse Management Suite on public cloud

To log in to the Wyse Management Suite console, you must have a supported web browser that is installed on your system. 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 data center**—us1.wysemanagementsuite.com/ccm-web
   - **EU data center**—eu1.wysemanagementsuite.com/ccm-web
2. Enter your username and password.
3. Click **Sign In**.

   If you log in to the Wyse Management Suite console for the first time, 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**.

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.

NOTE: 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, do the following:

1. Click the account link in the upper-right corner of the management console.
2. Click **Change Password**.

NOTE: It is recommended to change your password after logging in for the first time. The default username and password for additional administrators are created by the Wyse Management Suite account owner.

Logging out

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

1. Click the account link at the upper-right corner of the management console.
2. Click **Sign out**.

Prerequisites to deploy Wyse Management Suite on the private cloud

Table 4. Prerequisites

Description	10,000 devices or less	50,000 devices or less	120,000 devices or less	Wyse Management Suite – Software repository
Operating system	Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 Standard. The Wyse Management Suite web server has an inbuilt Apache Tomcat web server. Ensure that you do not install Microsoft IIS, Apache Tomcat web servers separately. Supported language pack—English, French, Italian, German, Spanish, Japanese, and Traditional Chinese			
Minimum disk space	40 GB	120 GB	200 GB	120 GB
Minimum memory (RAM)	8 GB	16 GB	32 GB	16 GB
Minimum CPU requirements	4	4	16	4
Network communication ports	The Wyse Management Suite installer adds Transmission Control Protocol (TCP) ports 443, 8080, and 1883 to the firewall exception list. The ports are added to access the Wyse Management Suite console and to send push notifications to the thin clients. • TCP 443—HTTPS communication • TCP 1883—MQTT communication • TCP 3306—MariaDB (optional if remote) • TCP 27017—MongoDB (optional if remote) • TCP 11211—Memcached • TCP 5172, 49159—End-User Management Software Development Kit (EMSDK)—optional and required only to manage Teradici devices • TLS 443—Secure MQTT communication The default ports that are used by the installer may be changed to an alternative port during installation.			The Wyse Management Suite repository installer adds TCP ports 443 and 8080 to the firewall exception list. The ports are added to access the operating system images and application images that are managed by Wyse Management Suite.
Supported browsers	Internet Explorer version 11 Google Chrome version 58.0 and later Mozilla Firefox version 52.0 and later Edge browser on Windows—English only			

- The Overlay Optimizer version 1.0 and installation scripts are provided with the Wyse Management Suite Installer. Administrator must run the scripts to enable the Overlay Optimizer to be made available in Wyse Management Suite.
- The Dell Secure Client version 1.0 installation scripts are provided with the Wyse Management Suite Installer. Administrator must run the scripts to enable the Dell Secure Client to be made available in Wyse Management Suite.

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. Also, it is not necessary that the software repository and the Wyse Management Suite server have the same operating system.

NOTE: For 10,000 devices setup, the minimum memory (RAM) should be 12 GB for secure MQTT communications.

NOTE: From Wyse Management Suite 3.3, you must use MongoDB version 4.2.12 for distributed setups. You can not install or upgrade Wyse Management Suite 3.3 using any other version of external MongoDB server.

NOTE: Wyse Management Suite server and repository installation is not supported on cloud hosted servers such as Azure, Amazon Web Services, and Google Cloud Platform.

Functional areas of management console

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

- The **Dashboard** page provides information about the current status on each functional area of the system.
- The **Groups & Configs** page employs a hierarchical group policy management for device configuration. Optionally, subgroups of the global group policy can be created to categorize devices according to corporate standards. For example, devices may be grouped based on job function, device type, and so on.
- The **Users** page enables local users and users imported from the Active Directory to be assigned as 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 that are assigned to them. Also, the **End User** tab is added for end user management.
- The **Devices** page enables you to view and manage devices, device types, and device-specific configurations.
- The **Apps & Data** page enables management of device applications, application inventory, and file repository.
- 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, Wakeup On LAN, and application or image policy that must be deployed on registered devices.
- The **Events** page enables you to view and audit system events and alerts.
- The **Portal Administration** page enables you to configure various system settings such as local repository configuration, Dell Hybrid Client 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 the rules that are defined by the system administrator. You can organize the groups based on the functional hierarchy, for example marketing, sales, and engineering, or based on the location hierarchy, for example, country/region, 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.

    For example,

    - Configure the policies for default policy group (parent group). After configuring the policies, check the custom group (child group) policies. Same sets of policies are applied to child group as well. Configurations in Default Policy Group settings are the global set of parameters that all groups and subgroups inherit from parent group.
    - Configure different settings for the custom group. The custom group receives both the payloads, but devices in the Default Policy Group do not receive the payload that is configured for Custom Policy Group.

- Configure different settings for the custom group. The settings that are configured at lower-level groups take precedence over the settings that were configured at the parent or higher-level groups.

- Settings that are specific to a particular device which can be configured from the **Device Details** page. These settings, like lower-level groups, take precedence over the settings that are 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 a 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 that are inherited from the global group and intermediate level groups.

Configuration policies are published immediately, and cannot be scheduled for a later time. A 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. The device restarts during installing an application. 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 running of pre-and-post installation scripts that may be required 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 go to the **Device Details** page for that device, click the device entry that is 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 that are configured in this section override any parameters that were configured at the groups and/or global level.

- **Reports**—You can generate and view reports based on the predefined filters. To generate reports, click the **Reports** tab on the **Portal Administration** 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 Device Agent

The Wyse Device Agent (WDA) is a unified agent for all thin client management solutions. If you install WDA, you can manage thin clients using Wyse Management Suite.

The following three types of customer security environments are supported by the Wyse Device Agent:

- **Highly secured environments**—To mitigate the risk against rouge DHCP or DNS server for new device discovery, administrators must log in to each device individually and configure the Wyse Management Suite server URL. You can use either CA-signed or self-signed certificates. However, Dell recommends that you use a CA-signed certificate. In Wyse Management Suite private cloud solution with self-signed certificate, the certificate should be manually configured in every device. Also, the certificate must be copied to the `Agent Configuration` folder to preserve the certificate and mitigate the risk against rouge DHCP or DNS server even after you reimage the device.

The `Agent Configuration` folder is available at the following location:

- Windows Embedded Standard devices—`%SYSTEMDRIVE%\\Wyse\\WCM\\ConfigMgmt\\Certificates`
- ThinLinux devices—`/etc/addons.d/WDA/certs`
- ThinOS devices—`wnos/cacerts/`

NOTE: You must import the certificate to a thin client running ThinOS operating system using a USB drive or FTP paths.

- **Secured environments**—To mitigate the risk against rouge DHCP or DNS server for new device discovery, administratos must configure Wyse Management Suite server using CA-signed certificates. The device can fetch the Wyse Management Suite server URL from the DHCP/DNS records and perform the CA validation. Wyse Management Suite private cloud solution with self-signed certificate requires the certificate to be pushed to the device after first registration if the device does not have the certificate before registration. This certificate is preserved even after you reimage or restart the device to mitigate the risk against rouge DHCP or DNS server.
- **Normal environments**—The device obtains the Wyse Management Suite server URL from the DHCP/DNS records for Wyse Management Suite private cloud that is configured with CA-signed or self-signed certificate. If CA validation option is disabled on the device, Wyse Management Suite administrator is notified after you register the device for the first time. In this scenario, Dell recommends that the administrators perform a certificate push to the device where the server is configured with self-signed certificate. This environment is not available for public cloud.

Dell Client Agent

Dell Client Agent (DCA) is a unified agent for Dell Hybrid Client management solutions. If you install DCA, you can manage Dell Hybrid Clients using Wyse Management Suite.

To install Dell Hybrid Client on the OptiPlex 7070 Ultra device:

1. Register the device to Wyse Management Suite using discovery method (DNS or DHCP) or the **reg.json** manual method—see Methods to register devices to Wyse Management Suite.
2. Reimage your OptiPlex 7070 Ultra device—see Reimage your Dell Hybrid Client.

Dell Client Agent-Enabler

Dell Client Agent-Enabler (DCA-Enabler) is a client agent for managing Ubuntu versions 18.04 and 20.04 LTS 64-bit on Dell Ubuntu devices. The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCA-Enabler). DCA-Enabler supports and allows you to do the following actions that are managed by Wyse Management Suite:

- Registration of Ubuntu devices
- Deploy Real-Time commands such as Query, Restart, Shutdown, and Wake-on-LAN.
- Device Pull Log command.
- Unregistration from the server
- Convert to Hybrid Client command using Jobs, Devices, or Device Details page.
- Deploy Standard Application Policy.
- Deploy Advanced Application Policy.
- Deploy Generic Client to Dell Hybrid Client conversion policy.
- Deploy certificate policy .

DCA-Enabler is preloaded in most of the Dell Ubuntu platforms. DCA-Enabler folders and the relevant files are found at the following locations:

- `/etc/dcae/config/`
- `/etc/dcae/certificates/`
- `/var/log/dcae/dcae.log`
- `/usr/sbin/dcae`

You can verify the DCA-Enabler service and package in the Dell Ubuntu platform using the following commands:

- `systemctl status dcae.service`—The active running version is displayed.
- `dpkg -l | grep dca-enabler`—The DCA-ENabler version is displayed in the **dca-enabler 1.x.0-xx** format.

3

Installing or upgrading Wyse Device Agent

This section provides information about how to install or upgrade Wyse Device Agent on your thin clients, such as Windows Embedded Standard, Linux, and ThinLinux devices by using Wyse Management Suite.

- **Windows Embedded Standard devices**—Wyse Device Agent version 1.4.x can be downloaded from support.dell.com. You can install or upgrade Wyse Device Agent on Windows Embedded Standard devices using any of the following methods:
  - Installing Wyse Device Agent manually
  - Upgrading Wyse Device Agent using Wyse Management Suite application policy

  NOTE: You can also upgrade the Wyse Device Agent manually by double-clicking the latest version of Wyse Device Agent .exe file.

  NOTE: Wyse Device Agent can be installed on Windows Embedded Standard 7 operating system only if KB3033929 is available.
- **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:

Installing Wyse Device Agent manually on a Windows Embedded device

Steps

1. Copy the `WDA.exe` file to the thin client.
2. Double-click the `WDA.exe` file.
3. Click **Yes**.

   NOTE: A warning message is displayed when an older version of Wyse Device Agent or HAgent is installed on the device.

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.

Upgrading Wyse Device Agent using Wyse Management Suite application policy

Prerequisites

It is recommended that you use the Wyse Management Suite application to upgrade Wyse Device Agent. 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.

Steps

1. After the `WDA.exe` file is copied to the repository, go to **Apps and Data**, and create a standard application policy with this package—see Create and deploy standard application policy to thin clients.

   NOTE: Advanced application policy is supported only from Wyse Device Agent 14.x onwards. It is recommended that you use the standard application policy when you upgrade 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, it is recommended that you use HTTP as the repository protocol.

   After a successful installation, the status is sent to the server.

Installing or upgrading Wyse Device Agents on ThinLinux and Linux clients

Prerequisites

- To install Wyse Device Agents on Dell Wyse 3040 Thin Clients with ThinLinux version 2.0, image version 2.0.14, and Wyse Device Agent version 3.0.7, you must install the `wda3040_3.0.10-01_amd64.deb` file, and then install the `wda_3.2.12-01_amd64.tar` file.
- You must install the platform utility add-on and Wyse Device Agent add-on for Linux thin clients. You can install `wda_x.x.x.tar` file for ThinLinux thin clients.

About this task

You can install or upgrade add-ons by using any of the following options:

- 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 the local repository.
2. 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.

3. On the **Jobs** page, schedule a job to upgrade Wyse Device Agent on the client.

   NOTE: The Linux client restarts after installing the Wyse Device Agent add-on version 2.0.11.

4

Installing or upgrading DCA-Enabler on Ubuntu devices

This section provides information about how to install or upgrade DCA-Enabler on Ubuntu devices.

Topics:

Install DCA-Enabler on Ubuntu devices

DCA-Enabler is preloaded in most of the Dell Ubuntu platforms. If DCA-Enabler is not preloaded, you can install DCA-Enabler.

Steps

1. Download the DCA-Enabler packages from www.dell.com/support.
2. Extract the downloaded file.
   The extracted file contains .deb files.
3. Install the DCA-Enabler-package and DCA-Enabler package using the following commands:
   - `"dpkg -i < dca-enabler-packages_1.x-x_amd64.deb >"`
   - `"dpkg -i < dca-enabler_1.x.x-x_amd64.deb >"`

Upgrade DCA-Enabler on Ubuntu devices

You can upgrade DCA-Enabler on Ubuntu devices using any of the following methods:

- Register the device to Wyse management Suite and deploy the latest DCA-Enabler package using the application policy.
- Manually download and extract the package, and then run the following commands on the device:
  - `"dpkg -i < dca-enabler-packages_1.x-x_amd64.deb"`
  - `"dpkg -i < dca-enabler_1.x.x-x_amd64.deb"`

5

Registering and configuring a new device using Wyse Management Suite

Topics:

Register and configure a new Windows Embedded Standard device using Wyse Management Suite

Steps

1. Install Wyse Device Agent on your thin client—see Installing or upgrading Wyse Device Agent.
2. Register your thin client to Wyse Management Suite—see Registering Windows Embedded Standard thin clients to Wyse Management Suite by using Wyse Device Agent.

   NOTE: You can also register the devices using any of the following methods:
   - Using DHCP option tags—see Register devices by using DHCP option tags.
   - Using DNS SRV record—see Registering devices by using DNS SRV record.

   NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

3. Add the device to your desired group (optional)—see Managing groups and configs.
4. Configure the thin client using any of the following options:
   - Using the **Groups and Configs** page—see Edit the Windows Embedded Standard policy settings.
   - Using the **Devices page**—see Managing Devices.

Register and configure a new ThinOS 8.x device using Wyse Management Suite

Steps

1. From the desktop menu of the thin client, go to **System Setup** > **Central Configuration**.
   The **Central Configuration** window is displayed.
2. Enter the **Group Registration Key** as configured by your administrator for the wanted group.
3. Select the **Enable WMS Advanced Settings** check box.
4. In the **WMS server** field, enter the Wyse Management Server URL.

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

   To enable the CA validation option in the private cloud, you must install the same self-signed certificate on the ThinOS device as well. If you have not installed the self-signed certificate in the ThinOS device, do not select the **Enable CA Validation** check box. You can install the certificate to the device by using Wyse Management Suite after registration, and then enable the CA validation option.
6. To verify the setup, click **Validate Key**.

   NOTE: If the key is not validated, verify the group key and WMS server URL which you have provided. Ensure that ports mentioned are not blocked by the network. The default ports are 443 and 1883.
7. Click **OK**.

   NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

   The device is registered to Wyse Management Suite.
8. Log in to Wyse Management Suite.
9. Add the device to your desired group (optional)—see Managing groups and configs.
10. Configure the thin client using any of the following options:
    - Using the **Groups and Configs** page—see Edit the ThinOS policy settings.
    - Using the **Devices page**—see Managing Devices.

Register and configure a new ThinOS 9.x device using Wyse Management Suite

Steps

1. From the desktop menu of the thin client, go to **System Setup** > **Central Configuration**.
   The **Central Configuration** window is displayed.
2. Enter the **Group Registration Key** as configured by your administrator for the wanted group.
3. Select the **Enable WMS Advanced Settings** check box.
4. In the **WMS server** field, enter the Wyse Management Server URL.
5. Enable or disable CA validation based on your license type. For public cloud, select the **Enable CA Validation** check box, and for private cloud, select the **Enable CA Validation** check box if you have imported certificates from a well-known certificate authority into your Wyse Management Suite server.

   To enable the CA validation option in the private cloud, you must install the same self-signed certificate on the ThinOS device as well. If you have not installed the self-signed certificate in the ThinOS device, do not select the **Enable CA Validation** check box. You can install the certificate to the device by using Wyse Management Suite after registration, and then enable the CA validation option.
6. To verify the setup, click **Validate Key**.

   NOTE: If the key is not validated, verify the group key and WMS server URL which you have provided. Ensure that ports mentioned are not blocked by the network. The default ports are 443 and 1883.

   An alert window is displayed.
7. Click **OK**.
8. Click **OK** in the **Central Configuration** window.

   NOTE: You can also register the devices using any of the following methods:
   - Using DHCP option tags—see Register devices by using DHCP option tags.
   - Using DNS SRV record—see Registering devices by using DNS SRV record.

   NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices**

page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

The device is registered to Wyse Management Suite.

9. Log in to Wyse Management Suite.
10. Add the device to your desired group (optional)—see Managing groups and configs.
11. Configure the thin client using any of the following options:
    - Using the **Groups and Configs** page—see Edit the ThinOS 9.x policy settings.
    - Using the **Devices page**—see Managing Devices.

Register and configure a new Linux or ThinLinux device using Wyse Management Suite

Steps

1. Install Wyse Device Agent on your thin client—see Installing or upgrading Wyse Device Agent.
2. Register your thin client to Wyse Management Suite—see Register Linux/ThinLinux thin clients to Wyse Management Suite by using Wyse Device Agent.

   NOTE: You can also register the devices using any of the following methods:
   - Using DHCP option tags—see Register devices by using DHCP option tags.
   - Using DNS SRV record—see Registering devices by using DNS SRV record.

   NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

3. Add the device to your desired group (optional)—see Managing groups and configs.
4. Configure the thin client using any of the following options:
   - Using the **Groups and Configs** page—see Edit the ThinLinux policy settings or Edit the Linux policy settings.
   - Using the **Devices page**—see Managing Devices.

Register and configure a new Wyse Software Thin Client using Wyse Management Suite

Steps

1. Install Wyse Device Agent on your thin client—see Installing or upgrading Wyse Device Agent.
2. Register your thin client to Wyse Management Suite—see Register Wyse Software Thin Client to Wyse Management Suite by using Wyse Device Agent.

   NOTE: You can also register the devices using any of the following methods:
   - Using DHCP option tags—see Register devices by using DHCP option tags.
   - Using DNS SRV record—see Registering devices by using DNS SRV record.

   NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

3. Add the device to your desired group (optional)—see Managing groups and configs.
4. Configure the thin client using any of the following options:
   - Using the **Groups and Configs** page—see Edit the Wyse Software Thin Client policy settings.

- Using the **Devices page**—see Managing Devices.

Register and configure Dell Hybrid Client using Wyse Management Suite

Prerequisites

Before registering the device, ensure that your device has network connectivity to contact the Wyse Management Suite server.

NOTE: You can register or unregister the device only from the guest user account.

Steps

1. Log in to the Dell Hybrid Client as a guest user.
2. On the top bar, click .

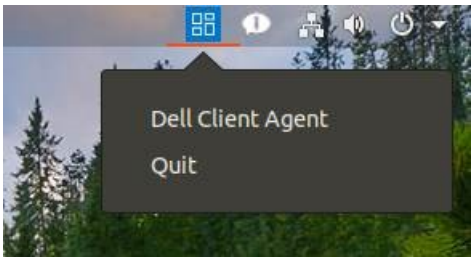


Figure 1. DCA icon

3. Click **Dell Client Agent**.
   The **Dell Client Agent** dialog box is displayed.
4. Click **Registration**.
   The default status is displayed as **Discovery In Progress**.
5. To register manually, click the **Cancel** button.
6. In the **WMS Server** field, enter the URL of the Wyse Management Suite server.
7. In the **Group Token** field, enter your group registration key. The group token is a unique key for registering your devices to groups directly.

   NOTE: If the tenant and group fields are empty, the device is registered to the unmanaged group. However, the group token is mandatory for registering the device to a public cloud.

8. Click the **ON/OFF** button to enable or disable the **Validate Server Certificate CA** option. Enable this option to perform the server certificate validation for all device-to-server communication.

   The CA Validation option is enabled automatically and cannot be disabled if a public cloud URL is entered.
9. Click **Register** to register your hybrid client on the Wyse Management Suite server.

   You can also register the devices using any of the following methods:
   - Using DHCP option tags—see Register devices by using DHCP option tags.
   - Using DNS SRV record—see Registering devices by using DNS SRV record.

   NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

   When your hybrid client is successfully registered, the status is displayed as **Registered** with the green color tick next to the **Registration Status** label. The caption of the **Register** button changes to **Unregister**.

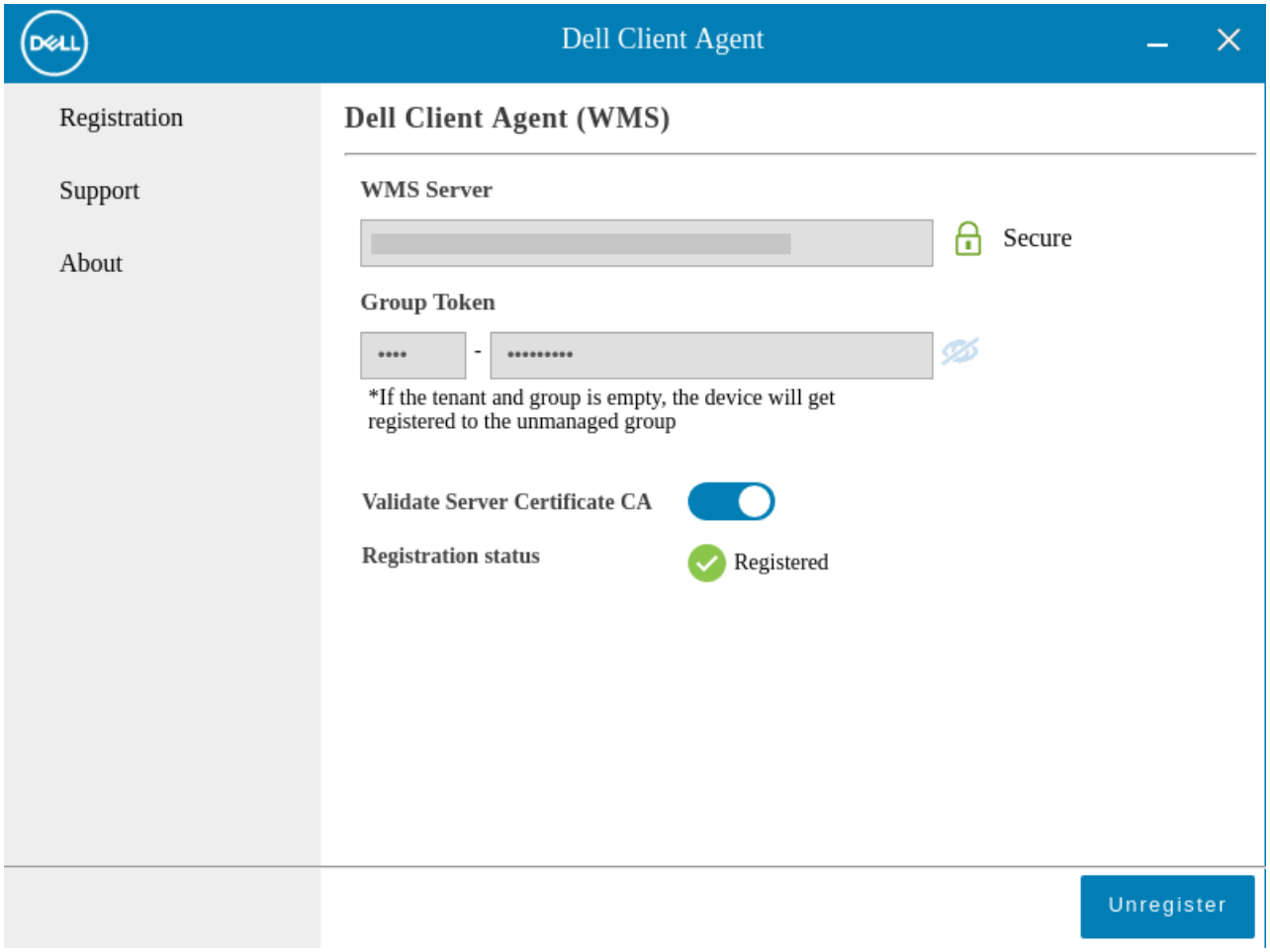


Figure 2. Dell Client Agent

10. Log in to Wyse Management Suite.
11. Add the device to your wanted group (optional)—see Managing Groups and Configs.
12. Configure the thin client using any of the following options:
    - Using the **Groups and Configs** page—see Edit the Dell Hybrid Client policy settings.
    - Using the **Devices page**—see Managing Devices.

Register and configure Dell Generic Client using Wyse Management Suite

Prerequisites

- Before registering the device, ensure that your device has network connectivity to contact the Wyse Management Suite server.
- DCA-Enabler is installed on the device.

NOTE: You can register or unregister the device only from the Ubuntu user account.

Steps

1. Log in to the Dell Generic Client running Ubuntu operating system.
2. Open Terminal.
3. Restart the dcae_service using the command `systemctl restart dcae.service`.

   The DCA-Enabler service tries to manually register the device using the reg.json file that is present in the `/etc/dcae/config` folder.

You can also register the devices using any of the following methods:

- Using DHCP option tags—see Register devices by using DHCP option tags.
- Using DNS SRV record—see Registering devices by using DNS SRV record.

NOTE: When the **Enrollment Validation** option is enabled, the manual or auto-discovered devices are in **Enrollment Validation Pending** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

4. Log in to Wyse Management Suite.
5. Add or move the device to your wanted group (optional)—see Managing Groups and Configs.
6. Configure the Generic client using any of the following options:
   - Using the **Groups and Configs** page—see Edit the Dell Generic Client settings.
   - Using the **Devices page**—see Managing Devices.

6

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 enables you to view the device summary.

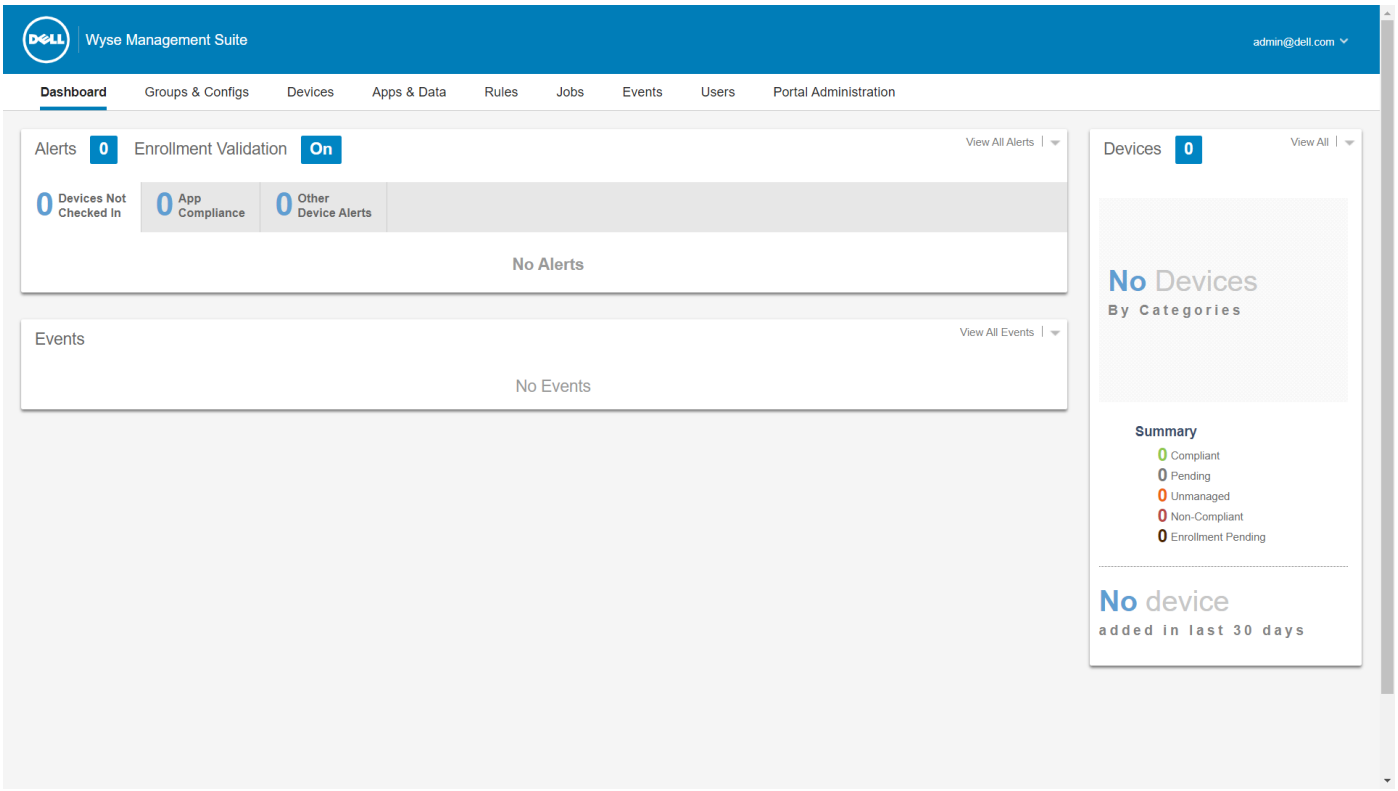


Figure 3. Dashboard

Topics:

- View alerts
- View the list of events
- View the device status
- Enable Enrollment Validation
- Change user preferences
- Access online help
- Change your password
- Log out from the management console

View alerts

The **Alerts** section displays the summary of all the alerts.

Steps

1. Click **Dashboard**.
   The alerts summary is displayed.

2. Click **View All Alerts**.
   The following attributes are displayed in the **Events** page:
   - **Devices Not Checked In**
   - **App Compliance**
   - **Other Device Alerts**

View the list of events

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

Steps

1. Click **Dashboard**.
   The events summary is displayed.
2. Click **View All Events**.
   The **Events** page is displayed with list of all the events.

View the device status

The **Display** section provides the summary of device status.

Steps

1. Click **Dashboard**.
   The devices summary is displayed.
2. Click **View All**.
   The **Devices** page is displayed with list of all the registered devices. The **Summary** section displays the device count based on the following device status category:
   - **Compliant**
   - **Pending**
   - **Unmanaged**
   - **Non-Compliant**
   - **Enrollment Pending**

Enable Enrollment Validation

You can enable **Enrollment Validation** to enable administrators to control the manual and auto registration of thin clients to a group.

Steps

1. Click **Dashboard**.
2. Click the **ON/OFF** button next to the **Enrollment Validation** option.
   You are redirected to the **Other Settings** option in the **Portal Administration** page.
3. Enable or disable the **Enrollment Validation** option.

Change user preferences

You can change the user preferences, such as alert notification, policy settings, and page size.

Steps

1. On the upper-right corner of the **Dashboard** page, click the login drop-down menu.
2. Click **User Preferences**.
   The **User Preferences** window is displayed.

3. Click **Alerts**, and select the appropriate check boxes to assign an alert type—Critical, Warning or Info—for notifications from your emails and mobile applications.
4. Click **Policies**, and select the **Ask me if I want to use the ThinOS Wizard mode** check box to display the **Select ThinOS Configuration Mode** window every time you configure the ThinOS policy settings.
5. Click **Page size**, and enter a number from 10 to 100 in the **Number Of Items Per Page** text box. This option enables you to set the number of items displayed on each page.

Access online help

Steps

1. On the upper-right corner of the **Dashboard** page, click the login drop-down menu.
2. Click **WMS Help**.
   The **Support for Wyse Management Suite** page is displayed.

Change your password

Steps

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

Log out from the management console

Steps

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

7

Managing groups and configurations

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

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

- **ThinOS**
  - **ThinOS**
  - **ThinOS 9.x**
- **WES**
- **Linux**
- **ThinLinux**
- **Teradici**
- **Wyse Software Thin Client**
- **Hybrid Client**
- **Generic Client**

Devices inherit policies in the order that they are created. The settings that are 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 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.

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

The policies are enforced in the following precedence:

- Global level policy
- Device Group level policy
- Device exceptions
- User Group level policy
- User exceptions
- User personalization

The configurations such as wallpaper or firmware policy applied to the Default Device group are applied by default to the child groups. From Wyse Management Suite 3.2, you can override these configurations for the child groups.

NOTE: From Wyse Management Suite 3.3, 5000 concurrent downloads of the configurations to the client are supported. Any further concurrent download is moved to a queued state until a slot is free. The request is timed out after 60 s.

Topics:

- Create a user policy group
- Configure a global level policy
- Import a user policy group
- Remove a group
- Configure a device level policy
- Export group policies
- Importing group policies
- Edit the ThinOS policy settings
- Edit the ThinOS 9.x policy settings
- Edit the Windows Embedded Standard policy settings
- Edit the Linux policy settings
- Edit the ThinLinux policy settings
- Edit the Wyse Software Thin Client policy settings
- Edit the Cloud Connect policy settings
- Edit the Dell Hybrid Client policy settings
- Edit the Dell Generic Client policy settings
- Create and import bulk device exception file

Edit an unmanaged group

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

Steps

1. On the **Groups & Configs** page, select **Unmanaged Group**.
2. Click .
   The **Editing Unmanaged Group** page is displayed. The **Group Name** displays the name of the group.
3. Edit the following details:
   - **Description**—Displays a brief description of the group.
   - **Group Token**—Select this option to enable the group token.
4. Click **Save**.

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

Create a default device policy group

You can create groups for the global device group policies and categorize devices based on your requirements.

Steps

1. On the **Groups & Configs** page, click the **Default Device Policy Group** option.
2. Click .
3. In the **Add New Group** dialog box, enter the **Group Name** and **Description**.
4. Select the **This is a ThinOS Select group parent** option to create a parent select group for ThinOS devices. This step is optional.

   For more information, see Create a ThinOS Select group.
5. In the **Registration** tab, select the **Enabled** check box under Group Token.
6. Enter the group token.
7. In the **Administration** tab, you can select the name of group administrators who are tasked with managing this group. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group**

Admins box. To move one group from the **Assigned Group Admins** to **Available Group Admins**, do the reverse. This step is optional.

8. Click **Save**.

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

   NOTE: The devices can be registered to a group by entering the group token which is available in the **Groups and Configs** page for the respective group.

   NOTE: The parent device policy group can have only 10 child device groups.

Create a ThinOS Select group

Steps

1. On the **Groups & Configs** page, click the **Default Device Policy Group** option.
2. Click +.
3. In the **Add New Group** dialog box, enter the **Group Name** and **Description**.
4. Select the **This is a ThinOS Select group parent** option.
5. Select the name of the group administrators who are tasked with managing this group. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box. To move one group from the **Assigned Group Admins** to **Available Group Admins**, do the reverse. This step is optional.
6. Click **Save**.

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

   To add sub groups to the created parent group, click the parent group on the **Groups & Configs** page, and follow the steps that are mentioned in Create device policy group.

   NOTE: The parent select group can have 10 child select group and you can register the devices to child select group. Profiles can be configured for other operating systems. The created profiles are the same as other custom groups.

   NOTE: Some policies that are changed in sub groups require a client reboot for changes to take effect.

Edit a default device policy group

Steps

1. Go to the **Groups & Configs** page and select the **Default Device Policy Group**.
2. In the **Editing Default Device Policy Group** dialog box, edit the required group information.
3. Click **Save**.

Edit a ThinOS select group

Steps

1. Go to the **Groups & Configs** page and click the ThinOS select group that you want to edit.
2. Click .
3. In the **Editing Default Policy group** dialog box, edit the group information such as **Group Name** and **Description**.
4. In the **Administration** tab, select the name of group administrators who are tasked with managing this group. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box. To move one group from the **Assigned Group Admins** to **Available Group Admins**, click the left arrow. This step is optional.
5. Click **Save**.

Remove a ThinOS select group

As an administrator, you can remove a group from the group hierarchy.

Steps

1. In the **Groups & Configs** page, select the ThinOS select group that you want to delete.
2. Click  .
   A warning message indicating that this action removes one or more groups from the group tree hierarchy is displayed.
3. From the groups drop-down list, select a new target group for users and devices in the current group.
4. Click **Remove Group**.

   NOTE: When you remove a group from the group hierarchy, all users and devices that belong to the deleted group are moved to the custom, default, or unmanaged group.

   NOTE: When you delete the select group, the devices of removed group cannot be moved to another select group.

Create a user policy group

You can create groups for the global user group policies and categorize users and devices based on their user groups.

Steps

1. On the **Groups & Configs** page, click the **Default User Policy Group** option.
2. Click  .
3. In the **Add New Group** dialog box, enter the **Group Name**, **Description**, **Domain**, **AD Attribute** (AD group or OU group) and **AD Attribute Name** which is the name present in the AD domain. You must use the **Group Name** as the **AD Attribute name**.

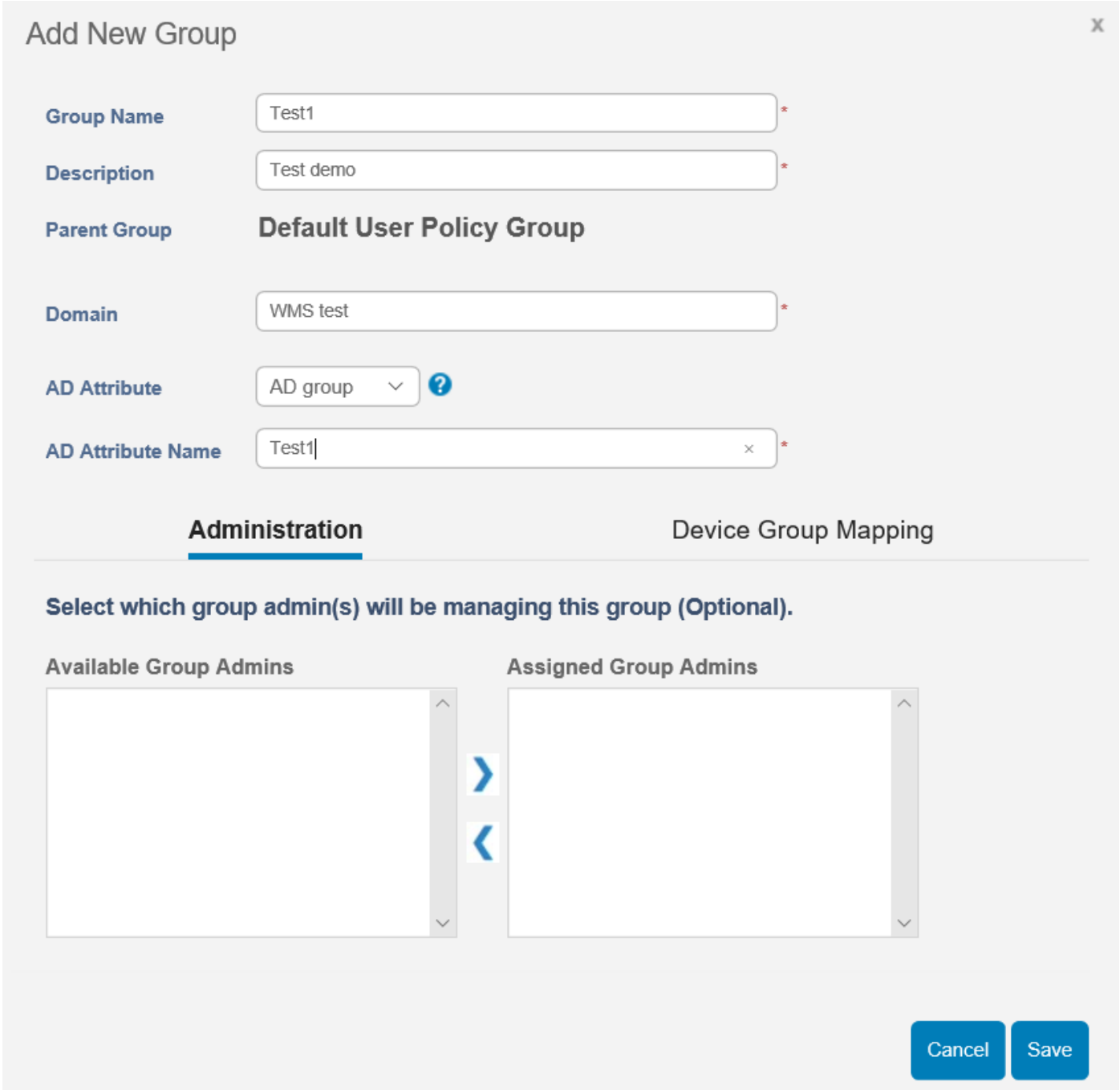


Figure 4. Add a new group

NOTE: If the AD group is inside an OU group in the domain, then you must select the OU group as the AD Attribute.

4. Select the name of the group administrators who are tasked with managing this group.
5. From the **Available Group Admins** box, select the particular group and click the right arrow to move it to the **Assigned Group Admins** box.
   To move one group from the **Assigned Group Admins** to **Available Group Admins**, do the reverse.
6. Click **Save**.
   The group is added to the list of available groups on the **Groups & Configs** page.
   NOTE: A user policy group must be mapped to an AD group or an organizational unit, but not both.

7. Select the **Device Group Mapping** option to import user groups with device mapping to control the configurations that are applied to all device groups by default.

   AD User groups which are imported into Wyse Management Suite can be mapped to the respective device group. By mapping the devices, they do not receive unwanted user group policies.

   NOTE: By default, user groups are not mapped to a device group. If you select the **Default device group** policy, all sub-device groups are selected. This feature is available only on Wyse Management Suite Pro license. You can import 100 user groups to Wyse Management Suite.

   NOTE: User group and device group mapping supports up to 25 thousand devices.

Edit a user policy group

Steps

1. Go to the **Groups & Configs** page and select the default user policy group.
2. Click .
3. In the **Editing Default User Policy group** dialog box, edit the required group information.
4. Click **Save**.

Configure a global level policy

Steps

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

   The policy settings of the respective device type are displayed.
2. Select the policy setting you want to configure and click **Configure this item**.
3. After configuring the options, click **Save and Publish**.

Import a user policy group

Steps

1. On the **Groups & Configs** page, click the **Default User Policy Group** option.
2. Click .
3. In the **Bulk Import** dialog box, click **Browse** and select the .csv file.

   The .csv file must contain the details in the following order:
   - Group name—Display name
   - Description
   - Domain—Domain name
   - AD attribute—AD group or OU group
   - AD attribute name—Group name present in AD Domain

   NOTE: You must use the Group Name as the AD Attribute name. Also, if the AD group is inside an OU group in the domain, then you must select **OU group** as the **AD Attribute**.
4. Select the **CSV file has header line** check box if the .csv file contains a header line.
5. Click **Import**.

Remove a group

As an administrator, you can remove a group from the group hierarchy.

Steps

1. In the **Groups & Configs** page, select the group that you want to delete.
2. Click  .
   A warning message indicating that this action removes one or more groups from the group tree hierarchy is displayed.
3. From the drop-down list, select a new group to move the users and devices in the current group.
4. Click **Remove Group**.

   NOTE: When a device group is deleted, all the devices of the group are moved to a selected device group. When a user group is deleted, there are no devices or users who are associated with it.

Configure a device level policy

Steps

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

Export group policies

The **Export Policies** option enables you to export the policies from the current group. This option is available for Wyse Management Suite Pro license users.

Steps

1. From the **Groups & Configs** page, select the group that you would like to export policies from. The group must have configured policies.
2. Click **Export Policies**.
   The **Export Policies** screen is displayed.
3. Select the device type policies to export.
   The following options are available:
   - All device type policies—All device type policies are exported.
   - Specific device type policies—Select one or more device types from the drop-down list. Only the selected device type policies are exported.
4. Click the **Yes** button to export the selected device type policies.
   Parent group policies are not exported. Only policies that are configured at the selected or targeted group level are exported.
5. Click the download link or right-click the file, and then click **Save as** to save the `JSON` file.

   NOTE: The passwords are encrypted in the exported file. The file name is in `[Group Name]-[ALL]-[Exported Date & Time]UTC.json` format.

   NOTE: To avoid the failure of importing policies, ensure that you remove passwords and any reference to files such as certificate, wallpaper, firmware, logo, and so on, before you export to a file.

Importing group policies

The **Import Policies** option enables you to import the policies. This option is available for Wyse Management Suite PRO license users. You can import the group policies from the **Groups & Configs** page or from the **Edit Policies** page.

Import group policies from Groups and Configs page

Steps

1. On the **Groups & Configs** page, select your preferred group.

   If the destination group contains policies of the same device type as the imported ones, they are removed and new ones are added.
2. Click **Import Policies**.
   The **Import Policies Wizard** screen is displayed.
3. Select the mode of importing the group policies from the selected group.
   The following options are available:
   - From an existing group—Select a group from the drop-down list. Policies from that group are copied to the current group.
   - From an exported file—Browse the `.json` file. Policies from that file are copied to the current group.
4. Click **Next**.
5. Select the device type configurations to import.
   The following options are available:
   - All device type policies—All configured device type policies are imported to the current group.
   - Specific device type policies—Select one or more device types from the dropdown list. Only the selected device type policies are imported to the current group.
6. Click **Next**.
   A preview of the policies in the selected group is displayed.
7. Click **Next**.

   The summary of the import process is displayed. The following types of warnings can be displayed:
   - **Imported <operating system type> policies are applied to group <group name>**—This warning is displayed when you import the operating system configurations to a group that does not contain any of the configurations.
   - **<Operating system type> policies already exists for the <group name> group. Existing <operating system type> policies are removed policies are applied**—This warning is displayed when you import new operating system type configurations to a group that contains the operating system type configurations.
   - **Importing policies from a file that contains dependencies to inventory files will fail. To allow this import, use the import option from the "Edit Policies" window**—This warning is displayed when you import the device type configurations from a file that contains references to inventory files.
8. Click **Import**.

   NOTE: Only the device type configurations that are selected can be imported. The policies that are defined in the target group for the selected device type are removed before applying the new policies of the same device type.

   NOTE: While importing the group policies, the passwords and reference files are not imported. The administrator must select them before publishing the policy.

Import group policies from Edit Policies page

Steps

1. On the **Groups & Configs** page, select your preferred group.
2. Click **Edit Policies** and select your preferred option.
3. Click **Import**.
   The **Import Policies Wizard** screen is displayed.
4. Select the mode of importing the group policies from the selected group. The following options are available:

- From an existing group—Select a group from the drop-down list. Policies from that group are copied to the current group.
- From an exported file—Click **Browse** and select the `.JSON` file. Policies from that file are copied to the current group.

5. Click **Next**.
   A preview of the policies in the selected group is displayed.
6. Click **Next**.The summary of the import process is displayed. The following types of warnings can be displayed:
   - **Imported <device type> policies will be applied to group <group name>**—This warning is displayed when you import the device type configurations to a group that does not contain any of these device type configurations.
   - **<Device type> policies already exists for the <group name> group. Existing <device type> policies will be removed and imported policies will be applied**—This warning is displayed when you import the device type configurations to a group that contains the device type configurations.
   - **Importing policies from a file that contains dependencies to inventory files will fail. To allow this import, use the import option from the Edit Policies window**—This warning is displayed when you import the device type configurations from a file that contains references to inventory files.
7. Click **Import**.

   NOTE: When you import a policy from a file, and if there are references or invalid dependencies, the import fails and an error message is displayed. Also, if the file to be imported has a reference or dependency file, go to **Edit policy** page of the respective device type and then import the group policies.

   NOTE: You can import or export group policies from a device to a user group and vice versa using a file or from one group to another. The unsupported configurations such as BIOS, Domain Join and so on are ignored when you import configurations to a user group.

Results

If the destination group contains policies of the same device type as the imported ones, they are removed and new ones are added.

NOTE: While importing the group policies, the passwords are not imported. The administrator must reenter the password in all password fields.

Edit the ThinOS policy settings

Steps

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

   NOTE: To set the ThinOS Advanced Configuration as the default mode, select the check box.

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

   NOTE: The thin client reboots if you make any changes to the following settings:
   - BIOS setting
   - DP audio
   - Jack popup
   - Terminal name
   - Ethernet speed
   - Display change—resolution, rotate, refresh, dual display, and multiple display
   - System mode—VDI, Storefront, and Classic

- LPT port bind

ThinOS—Wizard mode

Use this page to configure the most frequently used parameters for the ThinOS devices.

Steps

1. Select **Wizard** as the mode of configuration.
2. Configure the options are required.
3. Click **Next** to go to the next policy setting.
4. Click **Save & Publish** after you configure the options.

   NOTE: To go to ThinOS advanced configuration mode, click **Continue**.

ThinOS—Advanced mode

Use this page to configure the advanced policy settings for the ThinOS devices.

Steps

1. Select **Advanced Configuration** as the mode of configuration.
2. Configure the options as required.
3. Click **Save & Publish** to save and publish your configuration.

   NOTE: To go back to the **ThinOS** page, click **Remove Policy**.

Edit the ThinOS 9.x policy settings

Prerequisites

- Create a group, with a group token, for the devices you want to push the application package.
- Register the thin client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.

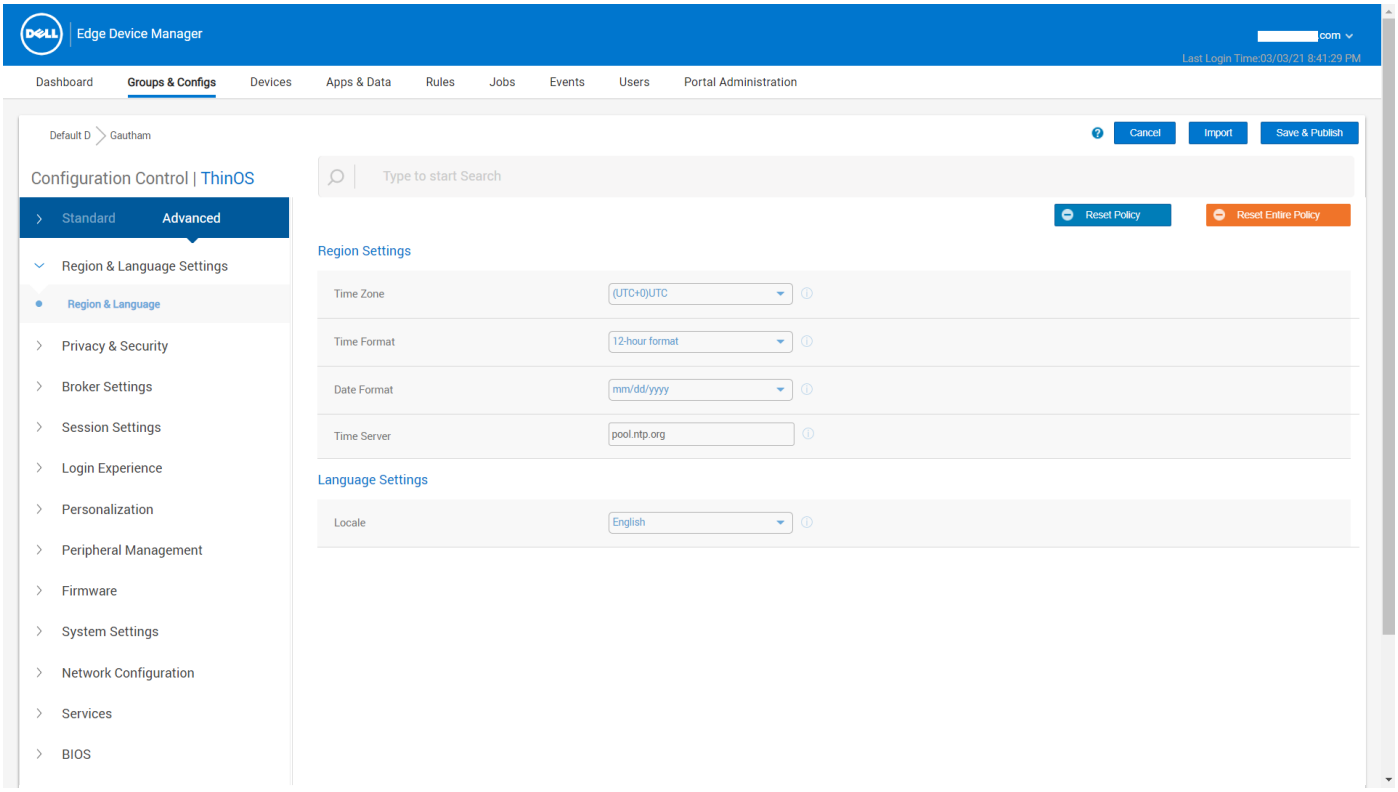


Figure 5. Configuration Control | ThinOS

3. Click the **Advanced** or **Standard** option.
4. Select the options that you want to configure.
5. In the respective fields, click the option that you want to configure.

   You can use the Global search option to find the relevant settings or parameters that are available in the Policy Settings. The search result displays the settings in the following order:

   - Setting
   - Parameter Group
   - Parameter sub group
   - Parameter
6. Configure the options as required.

   NOTE: From Wyse Management Suite 3.2, you can click the **Reset Policy** option if you want to reset the policy to default configurations. You can also click **Reset Entire Policy** option if you want to clear all configurations.
7. Click **Save & Publish**.

   NOTE: For information about the changes or updates to the ThinOS configurations, see *ThinOS 9.x Administrator's Guide and Release notes* at www.dell.com/support.

   NOTE: After you click **Save & Publish**, the configured settings are also displayed in the **Standard** tab.

   NOTE: The policy configurations with reference file such as firmware, package, wallpaper and so on applied to the parent group, for example Default Device group, are applied by default to the child groups. From Wyse Management Suite 3.2, you can override these configurations and remove them from the child groups.

   NOTE: You can only upload and deploy 10 certificates, wallpapers, and reference files from the **Configuration Control | ThinOS** window.

BIOS configurations for ThinOS 9.x

About this task

BIOS configuration settings can be configured to ThinOS 9.x devices using Wyse Management Suite 2.1. You can deploy the BIOS packages using the **Groups & Configs** page, or using the subnet mapping option.

NOTE: This feature is available only with Wyse Management Suite Pro license.

Steps

1. Go to the **Groups & Configs** page, and select a group.
   The Configuration Control | ThinOS window is displayed.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
3. Click **Advanced**.
4. In the **BIOS** field, click **select your platform** to choose the platform where you want to configure the BIOS settings.

Upgrade ThinOS 9.x to later versions using Wyse Management Suite

Prerequisites

- Ensure that you have created a group with a group token. Use this group token to register the ThinOS 9.x devices.
- Ensure that the thin client is registered to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. Click **Advanced**.
4. In the **Firmware** field, click **OS Firmware Updates**.
5. Click **Browse** to browse and upload the firmware.
   The EULA details of the package and the name of the vendors are displayed.
6. To select a file, click **Browse** and go to the location where your firmware is located.
   - If the EULA is embedded in the package, the EULA details of the package and the name of the vendors are displayed. You can click the vendor names to read the license agreement of each vendor. Click **Accept** to upload the package. If you upload multiple packages, the EULA details of each package are displayed. You must accept the license agreement of the packages individually.
   - If you do not accept the EULA, the firmware is not installed.

   NOTE: You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository or operator cloud repository.
7. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.

   NOTE: You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository, or operator cloud repository.
8. Click **Save & Publish**.
   The thin client downloads the firmware and restarts. The firmware version is upgraded.

Upload and push BIOS packages

Prerequisites

- Create a group in Wyse Management Suite with a group token. Use this group token to register the ThinOS 9.x devices.
- Register the thin client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The Configuration Control | ThinOS window is displayed.
3. Click **Advanced**.
4. In the **Firmware** field, click **BIOS Firmware Updates**.
5. From the **Select the ThinOS BIOS to deploy** drop-down menu, select the package.

   NOTE: You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository or operator cloud repository. You can upload 10 packages from tenant cloud repository.

6. Click **Save & Publish**.
   The thin client restarts and the application package is installed.

   You can also upload BIOS firmware from **Apps & Data** on Wyse Management Suite 2.1 as mentioned in the following steps:
   a. Go to the **Apps & Data** page.
   b. Click on **OS Image Repository** and select **ThinOS 9.x**.
   c. Click **Add BIOS file** to browse and add the file you want to add to the repository.

      NOTE: This feature is available only on Wyse Management Suite Pro license.

Upload and push ThinOS 9.x application packages using Groups and Configs

Prerequisites

- Ensure that you have created a group with a group token. Use this group token to register the ThinOS 9.x devices.
- Register the thin client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. Click **Advanced**.
4. In the **Firmware** field, click **Application Package Updates**.
5. To select a file, click **Browse** and go to the location where your file is located.
   - If the EULA is embedded in the package, the EULA details of the package and the name of the vendors are displayed. You can click the vendor names to read the license agreement of each vendor. Click **Accept** to upload the package. If you upload multiple packages, the EULA details of each package are displayed. You must accept the license agreement of the packages individually.
   - If the EULA is not embedded in the package, go to step 6.

   NOTE: You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository or operator cloud repository.

6. From the **Select the ThinOS Package(s) to deploy** drop-down menu, select the package.
7. Click **Save & Publish**.
   The thin client restarts and the application package is installed.

Edit the Windows Embedded Standard policy settings

Steps

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

The **WES** page is displayed.

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

Configure deployment settings for Windows Embedded devices

From Wyse Management Suite 3.1, you can configure the deployment settings for Windows Embedded devices. You can configure the settings to silently deploy configurations to devices.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **WES** or **ThinLinux.**.
3. Click **Deployment Setting**.
4. Click **Configure this item**.
5. Configure the following options:
   - **Enable/Disable All Notifications**—If you disable this option, all the options and notifications are disabled.
   - **Configure Update Notification**—If you disable this option, the configuration update dialog box is not displayed on the device.
   - **Application Update Notification**—If you disable this option, the user notification is not displayed when you deploy an application policy.
   - **Image Update Notification**—If you disable this option, the user notification is not displayed when you deploy an image policy.
   - **Logoff Notification**—If you disable this option, the user notification is not displayed for a user to log off from the device.
   - **Reboot Notification**—If you disable this option, the user notification is not displayed when the device reboot configuration is deployed.
   - **Display Lock-screen**—If you disable this option, the lock screen is not displayed during application and image updates.

   NOTE: All the options are enabled by default.

6. Click **Save & Publish**.

Configure Edge browser settings for Windows 10 IoT Enterprise

From Wyse Management Suite 3.3, you can configure Edge browser settings for thin clients running Windows 10 IoT Enterprise.

Prerequisites

Edge browser must be installed on the clients to configure the Edge browser settings from Wyse Management Suite settings.

Steps

1. Go to the **Groups & Configs** page, and select a group
2. From the **Edit Policies** drop-down menu, click **WES**.
3. Click **Remote Connections Chromium Browser**.
4. In the respective fields, configure the options as required.
5. Click **Save & Publish**.

   The following table lists the feature set that you can configure in the **Remote Connections Chromium Browser** window.

Table 5. Remote Connections Chromium Browser

Field name	Option
Remote Connections Chromium Browser	Connection name
	Auto Launch on Logon
	URL
	ON Startup

Table 5. Remote Connections Chromium Browser (continued)

Field name	Option
Favorites	Add favorites, trusted sites and shortcuts
	Require Server Verification (https:) for all sites in this zone
Privacy	Do Not Track requests
	Track prevention
Appearance	Home Button
	Favorites Bar
	Collections Button
	User Feedback Button
	Share Button
System	Hardware Acceleration

Edit the Linux policy settings

Steps

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **Linux**.
4. After configuring the policy settings, click **Save and Publish**.

Edit the ThinLinux policy settings

Steps

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **ThinLinux**.
4. After configuring the policy settings, click **Save and Publish**.

Configure deployment settings for ThinLinux devices

From Wyse Management Suite 3.1, you can configure the deployment settings for ThinLinux devices. You can configure the settings to silently deploy configurations to devices.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinLinux**.
3. Click **Deployment Setting**.
4. Click **Configure this item**.
5. Configure any of the following options:
   - **Enable/Disable All Notifications**—If you disable this option, all the options and notifications are disabled.
   - **Configure Update Notification**—If you disable this option, the configuration update dialog box is not displayed on the device.

- **Application Update Notification**—If you disable this option, the user notification is not displayed when you deploy an application policy.
- **Image Update Notification**—If you disable this option, the user notification is not displayed when you deploy an image policy.
- **Logoff Notification**—If you disable this option, the user notification is not displayed for a user to log off from the device.
- **Reboot Notification**—If you disable this option, the user notification is not displayed when the device reboot configuration is deployed.
- **Display Lock-screen**—If you disable this option, the lock screen is not displayed during application and image updates.

NOTE: All the options are enabled by default.

6. Click **Save & Publish**.

Edit the Wyse Software Thin Client policy settings

Steps

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **Wyse Software Thin Client**.
   The **Wyse Software Thin Client** page is displayed.
4. After configuring the policy settings, click **Save and Publish**.

Edit the Cloud Connect policy settings

Steps

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **Cloud Connect**.
4. After configuring the policy settings, click **Save and Publish**.

Edit the Dell Hybrid Client policy settings

Prerequisites

- Create a group with a group token for the devices you want to push the application package.
- Register Dell Hybrid Client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **Hybrid Client**.
   The **Configuration Control | Hybrid Client** window is displayed.
3. Click the **Advanced** option.
4. Select the options that you want to configure.
5. In the respective fields, click the setting and configure the options as required.

   NOTE: From Wyse Management Suite 3.2, you can click the **Reset Policy** option if you want to reset the policy to default configurations. You can also click **Reset Entire Policy** option if you want to clear all configurations.

6. Click **Save & Publish**.

   NOTE: After you click **Save & Publish**, the configured settings are also displayed in the **Standard** tab.

The following table lists the feature set that you can configure in the **Configuration Control | Hybrid Client** window.

Table 6. Hybrid Client policy settings

Feature	Sub feature—User policy group	Sub feature—Device policy group
Peripheral Management	Display settings	Display settings
	Printers	Printers
	Audio	Audio
	Mouse	Mouse
	Keyboard	Keyboard
Network Configuration	Wireless	Wireless
		Proxy
		Bluetooth
Browser settings	Google Chrome settings	Browser shortcuts
	Firefox settings	
	Browser shortcuts	
	Default Browser	
Region & Language settings	Region	Region
		Time server
		Language
Personalization	Desktop	Desktop
		Device info
SignOn	Not applicable	Domain join
		Previously Logged-in User List
Privacy & Security	Not applicable	Certificate
		Guest user account properties
		USB Lockdown
		GRUB password
		Bremen Password
		VNC Server
		SSH Server
Power Settings	Power saving	Power saving
	Suspend and Power button	Suspend and Power button
Citrix Workspace	Citrix Broker Session	Citrix Broker Session
	Citrix Global Settings	Citrix Global Settings
VMware ViewClient	VMware ViewClient Broker Session	VMware ViewClient Broker Session
	VMware Global Settings	VMware Global Settings
RDP	RDP Broker Session	RDP Broker Session
Dell Hybrid Client Mode	Dell Hybrid Client Mode	Dell Hybrid Client Mode
WMS settings	Not applicable	WMS client settings

Table 6. Hybrid Client policy settings (continued)

Feature	Sub feature—User policy group	Sub feature—Device policy group
		Deployment Settings
Application Security	VLC Media Player	VLC Media Player
	Image Viewer	Image Viewer
	Libre Office	Libre Office
Network Drives	Network Drives list	Network Drives list
BIOS	Not applicable	Select your platform: • DHC 3090 • DHC 3320 • DHC 5070 • DHC 7070 • DHC 7090

NOTE: For information about the changes or updates to the Dell Hybrid Client configurations, see *Dell Hybrid Client Administrator's Guide and Release notes* at www.dell.com/support.

NOTE: Do not use special characters or add spaces in the resource file name such as wallpaper, certificate, ad logo files.

For more information about how to configure your Dell Hybrid Client, see *Dell Hybrid Client Administrator's Guide* at www.dell.com/support.

Configure Wyse Management Suite client settings for Dell Hybrid Client

As an administrator, you can configure the Wyse Management Suite agent behavior with respect to Dell Hybrid Client configurations. Administrators can also configure devices to apply configurations outside of business hours.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **Hybrid Client**.
   The **Configuration Control | Hybrid Client** window is displayed.
3. Click the **Standard** option.
4. Go to **WMS Settings** > **WMS Client Settings**.
5. To configure the business hours and business days for the device group, click **Add Row** in the **Business Hour** field and the days from the **Business days** drop-down menu.
6. To enable the agent to report user sessions, enable the **Enable Session Reporting** option and select the timing from the **Report Session** drop-down menu. The available options are:
   - **Send user session at run time**—The Dell Client Agent sends the user session report every time a user logs off from the device.
   - **Send user session at check-in time**—The Dell Client Agent sends the user session report every 8 hours.
   - **Send user session outside of business hours**—The Dell Client Agent sends the user session report outside of business hours which is configured in step 5.
7. To deploy the configurations to any device based on the user level configurations, enable the **Enable User Personalization Roaming** option. If this option is enabled, the settings that are configured by a user on a device such as Google Chrome browser data, Firefox browser data, desktop customization, custom wallpaper, browser application state, cloud data, and VDI session details are saved in the Wyse Management Suite server. These configurations are applied automatically when a user logs in to a different device. The configured settings take precedence over all other configurations. Also, the setting can be configured from user policy group.
8. To enable notifications on the device, enable the **Enabling Push Notification** option. If this option is enabled, the settings that are configured are applied immediately after you click **Save & Publish**. If you disable this option, the configurations are applied when the device sends a heartbeat signal.

NOTE: If you disable the option, the application deployment may enter an error state since Wyse Management Suite does not send the push notification to Dell Hybrid Clients.

9. To apply the configuration outside of the specified business hours, select the option from the drop-down menu. The available options are:
   - **Immediately**—If you select this option, the configurations are applied immediately after you click **Save & Publish**.
   - **Outside of specified business hour**—If you select this option, the configurations are applied outside of business hours which are configured in step 5.
   - **When no user has logged on to the device for a period of time**—If you select this option, the configuration are applied when no user has logged in to the device for defined time. You can specify the idle time after which the configurations are applied to the device.

   NOTE: You can also configure these settings for a particular device from the **Devices** page. For more information, see Configure a device level policy.

10. To save user configurations deploy them across devices, enable the **User Data Roaming** option. You can configure to save the settings after a specified function, to a repository of your choice, or the configurations that needs to be saved to the repository. This configuration is supported from Dell Hybrid Client version 1.5 and later.
11. To enable auto update of Dell-signed applications after the Dell Hybrid Client device checks-in to Wyse Management Suite, enable the **Auto Update** option. The application is automatically updated if the application package version in the Wyse Management Suite repository is greater than the version installed on the Dell Hybrid Client powered device. You can also select the application and configure the frequency at which the auto update must be performed.

    NOTE: The dell Hybrid Client powered device must be turned on for the configuration to be applied to the device.

12. To enable the debug mode for the Dell Client Agent log, enable the **Support Mode** option.

Configure deployment settings for Dell Hybrid Client devices

From Wyse Management Suite 3.1, you can configure the deployment settings for Dell Hybrid Client devices. You can configure the settings to silently deploy configurations to devices.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **Hybrid Client**.
3. Go to **WMS Settings** > **Deployment Setting**.
4. Configure any the following options:
   - **Configure Update Notification**—If you disable this option, the configuration update dialog box is not displayed on the device.
   - **Application Update Notification**—If you disable this option, the user notification is not displayed when you deploy an application policy.
   - **Image Update Notification**—If you disable this option, the user notification is not displayed when you deploy an image policy.
   - **Logoff Notification**—If you disable this option, the user notification is not displayed for a user to log off from the device.
   - **Reboot Notification**—If you disable this option, the user notification is not displayed when the device reboot configuration is deployed.
   - **Display Lock-screen**—If you disable this option, the lock screen is not displayed during application and image updates.

   NOTE: You can enable the **Enable/Disable All Notifications** option if you want to enable all the options and notifications.

   NOTE: **Configure Update Notification** and **Display Lock-screen** are disabled by default.

5. Click **Save & Publish**.

Edit the Dell Generic Client policy settings

Prerequisites

- Create a group with a group token for the devices.
- Register the Dell Generic Client to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **Generic Client**.
   The **Configuration Control | Generic Client** window is displayed.
3. Click the **Advanced** option.
4. Select the options that you want to configure.
5. In the respective fields, click the setting and configure the options as required.

   NOTE: From Wyse Management Suite 3.2, you can click the **Reset Policy** option if you want to reset the policy to default configurations.

6. Click **Save & Publish**.

   NOTE: After you click **Save & Publish**, the configured settings are also displayed in the **Standard** tab.

   The following table lists the feature set that you can configure in the **Configuration Control | Generic Client** window.

Table 7. Generic Client policy settings

Feature	Sub feature—User policy group	Sub feature—Device policy group
Privacy & Security	Certificate	Certificate
Agent Logging Level	Logging level	Logging level

Create and import bulk device exception file

From Wyse Management Suite 3.1, you can deploy device exception configurations to multiple ThinOS 9.x devices.

Steps

1. Create a bulk device exception file. To create a file, do any of the following:
   - Create a group policy for a test group and then export that policy to a file. If the configuration contains passwords, they are replaced with * in the exported file. For example:

```
{
    "WMSVersion": "4.6.8",
    "exportedDate": "1581466633677",
    "deviceTypes": [
        {
            "type": 6,
            "configurations": {
                "version": "0.0.1",
                "sequence": 1581466506281,
                "parameters": {
                    "AdminModeUsername": {
                        "value": "admin",
                        "updatedAt": "1581466506234"
                    },
                    "AdminModePassword": {
                        "value": "********",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalName": {
                        "value": "outpatient",
```

```
                        "updatedAt": "1581466506234"
                    },
                    "TimeServer": {
                        "value": "10.10.10.10",
                        "updatedAt": "1581466506234"
                    },
                    "timeZone": {
                        "value": "America/Phoenix",
                        "updatedAt": "1581466506234"
                    },
                    "TerminalNameCapital": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    },
                    "DeviceNICDefault": {
                        "value": "Wlan",
                        "updatedAt": "1581466506234"
                    },
                    "AdminMode": {
                        "value": "yes",
                        "updatedAt": "1581466506234"
                    }
                }
            }
        }
    ]
}
```

- Create a .json file using the following format:

```
{

"devices": {

<serialnumber>: {

"parameters": {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}

},

configurations: [<configuration name>]

}

}

"configurations": {

<configurationName>: {

"<parametername>": {

       "value": <value>

},

"<parametername>": {

       "value": <value>

}
```

```
  }

}

}
```

For example,

```
{
    "devices": {
        "9EPDL900051": {
            "parameters": {
                "TerminalName": {
                    "value" : "Cubical 5 - Floor 3"
                },
                "TerminalNameCapital": {
                    "value": "no"
                }
            },
            configurations: ["westWingExceptions"]
        },
        "5LGDO600108": {
            "parameters": {
                "TerminalName": {
                    "value" : "Cubical 15 - Floor 2"
                },
                "TerminalNameCapital": {
                    "value": "no"
                }
            },
            configurations: ["westWingExceptions"]
        }
    },
    "configurations": {
        "westWingExceptions": {
            "DeviceNICDefault": {
                "value": "Wlan"
            },
            "timeZone": {
                "value": "America/Phoenix"
            },
            "TimeServer": {
                "value": "10.10.10.10"
            },
            "TerminalNameCapital": {
                "value": "yes"
            },
            "AdminMode": {
                "value": "yes"
            },
            "AdminModeUsername": {
                "value": "admin"
            },
            "AdminModePassword": {
                "value": "password"
            }
        }
    }
}
```

2. Compress and encrypt the file.

   NOTE: You can use 7-zip software to compress and encrypt the file.

   NOTE: File size should not be more than 1 MB.

3. Go to **Groups & Configs** and click **Import Policies**.
   The **Import Policies Wizard** screen is displayed.
4. Select **Bulk Device Exceptions**.
5. Click **Browse** and select the password encrypted .zip file.

6. Click **Next**.

   Select the device type configurations to import page is displayed.
7. Click **Next**.

   NOTE: Since you can bulk import a device exception file for ThinOS 9.x devices, you cannot configure the options in the page.
8. Enter the .zip file password that was used to zip the .json file.
9. Click **Next**.

   A summary of the bulk device exceptions import is displayed.
10. Click **Import**.

    After the configurations are imported, a report generation link is generated in the **Group & Configs** page which can be downloaded. A success message is displayed in the **Group & Configs** page.

    NOTE: If a device is not registered and the configurations are imported, exceptions are applied to this device only if the device registers with one of the preloaded serial numbers device in the next 30 days.

    NOTE: If a device is already registered and the configurations are imported with device serial number, then the device exceptions are applied to the device.

    NOTE: Imported file is a password protected. AES-256 and ZipCrypto encryption is supported.

    NOTE: Configurations such as certificates, wallpaper, logo, and so on, with resources associated with them are not imported.

8

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.

You can sort the device list based on the following:

- Type
- Platform
- Operating system version
- Serial number
- IP address
- Last user details
- Group details
- Last check-in time
- Registration status
- Write filter status

To view the **Device Details** page of a particular device, click the device entry that is 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 that are configured in this section override any parameters that were configured at the groups and/or at the global level.

NOTE: From Wyse Management Suite 3.2, you cannot export device details to a CSV file from the **Devices** page. You must go to **Portal Administration** > **Reports** > **Generate Report** and select an option under **Devices** category in the **Type** drop-down list to export the details.

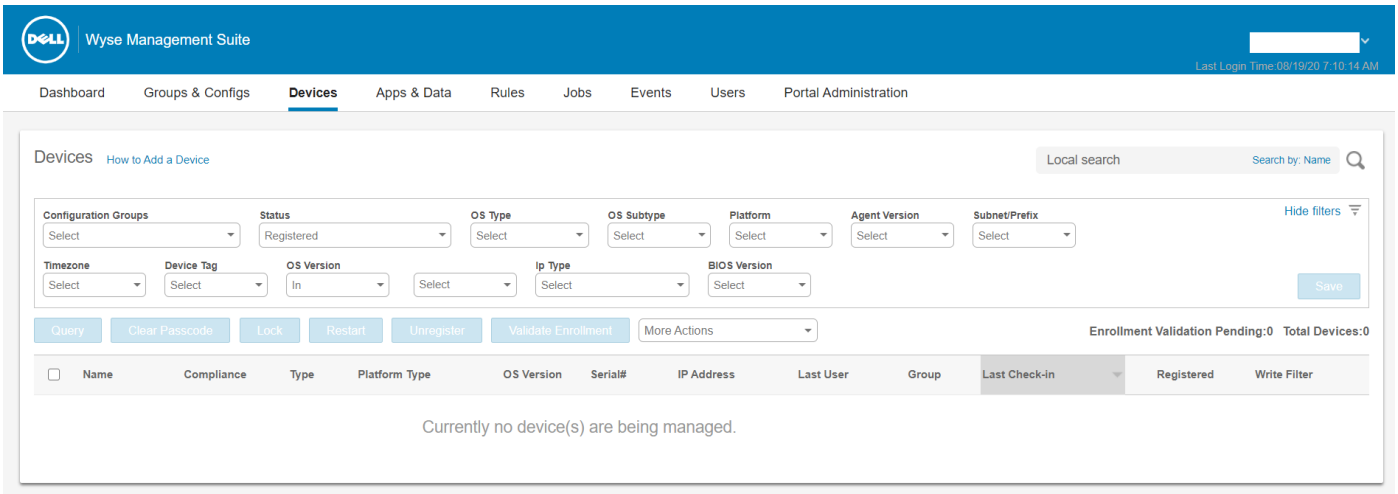


Figure 6. Devices page

Topics:

- Methods to register devices to Wyse Management Suite
- Search a device by using filters
- Save the filter in Devices page
- Query the device status
- Lock the devices
- Restart the devices
- Unregister the device

- Enrollment Validation
- Reset the device to factory default settings
- Change a group assignment on the Devices page
- Send messages to a device
- Wake On LAN command
- View the device details
- View the display parameters
- View the virtual NIC details
- View the BIOS details
- Manage the device summary
- View the system information
- View device events
- View the installed applications
- Rename the thin client
- Enable remote shadow connection
- Configure remote shadow connection for Dell Hybrid Client devices
- Shutting down devices
- Tag a device
- Device compliance status
- Pulling Windows Embedded Standard or ThinLinux image
- Request a log file
- Troubleshooting your device
- Reimage your Dell Hybrid Client
- Convert your Dell Generic Client to Hybrid Client
- Pull configuration user interface package for Dell Hybrid Client
- Reset your Dell Hybrid Client to factory settings
- Bulk group change of devices

Methods to register devices to Wyse Management Suite

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

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

NOTE:

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

Register Dell Hybrid Client manually

Prerequisites

Before registering the device, ensure that your device has network connectivity to contact the Wyse Management Suite server.

NOTE: You can register the device only from the guest user account. As a guest user, you can unregister the device from Wyse Management Suite only in dev mode. Domain users cannot unregister the device from Wyse Management Suite.

Steps

1. Log in to Dell Hybrid Client as a guest user. By default, the username is **guest**.

2. On the top bar, click .
3. Click **Dell Client Agent**.
   The **Dell Client Agent** window is displayed.
4. Click **Registration**.
   The default status is displayed as **Discovery In Progress**.
5. To register manually, click the **Cancel** button.
6. In the **WMS Server** field, enter the URL of the Wyse Management Suite server.
7. In the **Group Token** field, enter your group registration key. The group token is a unique key for registering your devices to groups directly.

   NOTE: If the tenant and group fields are empty, the device is registered to the unmanaged group. However, the group token is mandatory for registering the device to a public cloud.

8. Click the **ON/OFF** button to enable or disable the **Validate Server Certificate CA** option. Enable this option to perform the server certificate validation for all device-to-server communication.

   The CA Validation option is enabled automatically and cannot be disabled if a public cloud URL is entered.
9. Click **Register** to register your device on the Wyse Management Suite server.

   When your device is successfully registered, the status is displayed as **Registered** with the green color tick next to the **Registration Status** label. The caption of the **Register** button changes to **Unregister**.

   NOTE: Administrators or guest users cannot unregister the device directly from the **Dell Client Agent** window. To unregister the device, you must either enter the dev mode or use the Wyse Management Suite console.

Register Dell Generic Client by using manual discovery method

You can use the manual discovery method to register Dell Ubuntu devices such as OptiPlex 3090 Ultra, OptiPlex 7090 Ultra, OptiPlex 7070 Ultra, and Latitude 3320 running Ubuntu version 18.04 or 20.04 LTS 64-bit to Wyse Management Suite using the Dell Client Agent-Enabler agent.

Steps

1. Create a reg.json file using the following template:

```
{"ccm":
{"ccmserver":"WMSServerURL.Domain.com","ccmport":"443","usessl":"true","mqttserver":"
WMSServerURL.Domain.com
","mqttport":"1883","grouptoken":"GroupToken","isCaValidationOn":"false"}}
```

2. Copy the reg.json file to `/etc/dcae/config`.
3. Restart the device.

   NOTE: Dell Ubuntu devices are registered to Wyse Management Suite as Dell Hybrid Client if the DCA-Enabler version is 1.1.0-17 or lower. If the DCA-Enabler version is 1.2.0-xx or greater, the devices are registered as Dell Generic Client.

Register Dell Hybrid Client by using manual discovery method

You can use the manual discovery method to register OptiPlex 7070 Ultra devices running Ubuntu version 18.04 LTS 64-bit to Wyse Management Suite using the Dell Client Agent Enabler agent.

Steps

1. Create a reg.json file using the following template:

```
{"ccm":
{"ccmserver":"WMSServerURL.Domain.com","ccmport":"443","usessl":"true","mqttserver":"
WMSServerURL.Domain.com
","mqttport":"1883","grouptoken":"GroupToken","isCaValidationOn":"false"}}
```

2. Copy the reg.json file to `/etc/dcae/config`.

3. Restart the device.

Register ThinOS devices by using Wyse Device Agent

To register the ThinOS devices manually, do the following:

Steps

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

   WMS is selected by default.
3. Select the **Enable Wyse Management Suite** check box to enable Wyse Management Suite.
4. Enter the **Group Registration Key** as configured by your administrator for the wanted group.
5. Select the **Enable WMS Advanced Settings** option, and enter the WMS server or MQTT server details.
6. Enable or disable CA validation based on your license type. For public cloud, select the **Enable CA Validation** check box, and for private cloud, select the **Enable CA Validation** check box if you have imported certificates from a well-known certificate authority into your Wyse Management Suite server.

   To enable the CA validation option in the private cloud, you must install the same self-signed certificate on the ThinOS device as well. If you have not installed the self-signed certificate in the ThinOS device, then, do not select the **Enable CA Validation** check box. You can install the certificate to the device by using Wyse Management Suite after registration, and then enable the CA validation option.

   NOTE:
   - A warning message is displayed if you disable CA validation. You must click Ok to confirm.
   - For the public cloud version of Wyse Management Suite in USA data-center, do not change the default WMS server and MQTT server details. For the public cloud version of Wyse Management Suite in Europe data-center, use the following:
     - CCM Server—eu1.wysemanagementsuite.com
     - MQTT Server—eu1-pns.wysemanagementsuite.com:1883
   - A warning message is displayed if the server address contains http. You must click Ok to confirm.
7. To verify the setup, click **Validate Key**. The device automatically restarts after the key is validated.

   NOTE: If the key is not validated, verify the group key and WMS server URL which you have provided. Ensure that ports 443 and 1883 are not blocked by the network.
8. Click **OK**.
   The device is registered to Wyse Management Suite.

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

Prerequisites

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

Steps

1. Open the Wyse Device Agent application.
   The Wyse Device Agent screen is displayed.
2. From the **Management Server** drop-down list, select **Wyse Management Suite**.
3. Enter the server address and the port number in the respective fields.

   NOTE: If the server address contains **http**, a warning message is displayed. Click **Ok** to confirm.
4. Enter the group token. For a single tenant, the group token is an optional step.

NOTE: The group token that is entered in the **Group Token** field is not displayed in clear text.

5. Enable or disable CA validation that is based on your license type.

   NOTE: If you disable CA validation, a warning message is displayed. Click **Ok** to confirm.

6. Click **Register**.

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

Prerequisites

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

Steps

1. Open the **Wyse Device Agent** application.
   The **Wyse Device Agent** window is displayed.
2. Enter the device registration details.
3. From the **Management Server** drop-down list, select **Wyse Management Suite**.
4. Enter the server address and the port number in the respective fields.

   NOTE: If the server address contains **http**, a warning message is displayed. Click **Ok** to confirm.

5. Enter the group token. For a single tenant, the group token is an optional step.
6. Enable or disable CA validation that is based on your license type.

   NOTE: If you disable CA validation, a warning message is displayed. Click **Ok** to confirm.

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

Register ThinLinux thin clients by using Wyse Device Agent

Prerequisites

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

Steps

1. Open the Wyse Device Agent application.
   The Wyse Device Agent screen is displayed.
2. Enter the device registration details.
3. In Wyse Management Suite, enter the Wyse Management Suite server details.
4. Enter the group token.
   For a single tenant, the group token is an optional step.
5. Click **Register**.
   After the registration is complete, the confirmation message is displayed.

Register ThinOS devices by using the FTP INI method

Prerequisites

Create a group to register in Wyse Management Suite.

Steps

1. Create a `wnos.ini` file. Enter the following parameter:

   CCMEnable=`yes/no` **CCMServer**=`FQDN of WMS Server` **GroupPrefix**=`The prefix of the Group Token` **GroupKey**=`The Group Key` **CAValidation**=`yes/no` **Discover**=`yes/no`

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

   CCMEnable=`yes` **CCMServer**= `is ServerFQDN.domain.com` **GroupPrefix**=`defa` **GroupKey**=`defadefa` **CAValidation**=`yes` **Discover**=`yes`

2. Place the `wnos.ini` file inside wnos folder of any FTP path.
3. Go to **Central Configuration** on the ThinOS device.
4. In the **General** tab, provide the FTP path in file servers or path until the parent folder.
5. Enter the FTP credentials if required. If FTP does not need credentials, username and password can be anonymous.
6. Click **OK**, and then restart the thin client.
7. Go to **Central Configuration** on the ThinOS device.
   In the **Wyse Device Agent** tab, observe that the Wyse Management Server details are available in the respective field and the client entry can be seen in Wyse Management Server>Devices page.

Register ThinLinux version 2.0 devices by using FTP INI method

Prerequisites

Create a group to register in Wyse Management Suite.

Steps

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

   WMSEnable=`yes\no`

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

   GroupRegistrationKey=`GroupToken present in WMS Server`

   CAValidation=`True/False`

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

   WMSEnable=`yes`

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

   GroupRegistrationKey=`defa-defadefa`

   CAValidation=`True`

2. Place the wlx ini file in the wyse\wlx2 folder.
3. Go to **Settings** and switch to admin on the ThinLinux thin client.
4. Go to **Management** > **INI**.
5. Enter the FTP server URL.
6. Click **Save**, and then restart the thin client.
7. Go to **Management** > **Wyse Device Agent**.
   In the Wyse Device Agent tab, observe that the Wyse Management Server details are available in the respective field and the client entry can be seen in Wyse Management Server>Devices page.

Register ThinLinux version 1.0 devices by using FTP INI method

Prerequisites

Create a group to register in Wyse Management Suite.

Steps

1. Create a `wlx.ini` file and enter the following parameter:

   WMSEnable=`yes\no`

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

   GroupRegistrationKey=`GroupToken present in WMS Server`

   CAValidation=`True/False`

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

   WMSEnable=`yes`

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

   GroupRegistrationKey=`defa-defadefa`

   CAValidation=`True`

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

Registering devices by using DHCP option tags

You can register the devices by using the DHCP option tags.

Table 8. Registering device by using DHCP option tags

Option Tag	Description
Name—WMS **Data Type**—String **Code**—165 **Description**—WMS Server FQDN	This tag points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com`, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. **NOTE:** Do not use https://FQDN or FQDN:443 in the server URL, or the thin client will not register to Wyse Management Suite.
Name—MQTT **Data Type**—String **Code**—166 **Description**—MQTT Server	This tag directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, `wmsservername.domain.com:1883`. To register your devices in Wyse Management Suite public cloud, the device should point to the PNS (MQTT) servers in public cloud. For example, US1: us1-pns.wysemanagementsuite.com EU1: eu1-pns.wysemanagementsuite.com You must enter the MQTT server details when you configure Wyse Device Agent details in the older version of ThinOS and Windows Embedded devices. MQTT is a component of WMS which is required to notify the thin clients. The URLs—with and without MQTT details—must be added to the allowlist in the Wyse Management Suite public cloud environment. **NOTE:** You cannot use the MQTT URLs to log in to Wyse Management Suite.

Table 8. Registering device by using DHCP option tags (continued)

Option Tag	Description
Name—CA Validation **Data Type**—String **Code**—167 **Description**—Certificate Authority Validation	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. By default, the CA validation is enabled in the public cloud. You can disable the CA validation in the public cloud as well. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server.
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.

NOTE: For detailed instructions on how to add DHCP option tags on the Windows server, see How do I create and configure DHCP option tags.

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 How do I create and configure DNS SRV record.

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

Table 9. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name—_WMS_MGMT **Record FQDN**—_WMS_MGMT._tcp.<Domainname> **Record Type**— SRV	This record points to the Wyse Management Suite server URL. For example, `wmsserver.acme.com`, where wmsserver.acme.com is fully qualified domain name of the server where Wyse Management Suite is installed. **NOTE:** Do not use https://FQDN or FQDN:443 in the server URL, or the thin client will not register to Wyse Management Suite.
Record Name—_WMS_MQTT **Record FQDN**—_WMS_MQTT._tcp.<Domainname> **Record Type**—SRV	This record directs the device to the Wyse Management Suite Push Notification server (PNS). For a private cloud installation, the device gets directed to the MQTT service on the Wyse Management Suite server. For example, `wmsservername.domain.com:1883`. **NOTE:** MQTT is optional for the latest version of Wyse Management Suite.

Table 9. Configuring device by using DNS SRV record (continued)

URL/Tag	Description
	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 You must enter the MQTT server details when you configure Wyse Device Agent details in the older version of ThinOS and Windows Embedded devices. MQTT is a component of WMS which is required to notify the thin clients. The URLs—with and without MQTT details—must be added to the allowlist in the Wyse Management Suite public cloud environment. **NOTE:** You cannot use the MQTT URLs to log in to Wyse Management Suite.
Record Name—_WMS_GROUPTOKEN **Record FQDN**—_WMS_GROUPTOKEN._tcp.<Domainname> **Record Type**— TEXT	This record is required to register the ThinOS devices with Wyse Management Suite on public or private cloud. This record is optional to register the Windows Embedded Standard or ThinLinux devices with Wyse Management Suite on private cloud. If the record is not available, then the devices are automatically registered to the unmanaged group during on-premise installation. **NOTE:** Group Token is optional for the latest version of Wyse Management Suite on private cloud.
Record Name—_WMS_CAVALIDATION **Record FQDN**—_WMS_CAVALIDATION._tcp.<Domainname> **Record Type**—TEXT	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. By default, the CA validation is enabled in the public cloud. You can disable the CA validation in the public cloud as well. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False** , if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. **NOTE:** CA Validation is optional for the latest version of Wyse Management Suite.

Search a device by using filters

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 of the following options:
   - **Registration**
     - Registered
     - Pre-registered
     - Not Registered
     - Compliant
     - Enrollment Validation Pending

    - Pending
    - Non-Compliant
- **Online Status**
    - Online
    - Offline
    - Unknown
- **Others**
    - Recently Added

3. From the **OS Type** drop-down list, select any of the following operating systems:
    - **Thin Client**
        - Linux
        - ThinLinux
        - ThinOS
        - WES
        - Teradici (Private cloud)
        - Wyse Software Thin Client
    - **Hybrid Client**
        - Hybrid 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 operating system version.
7. From the **Agent Version** drop-down list, select an agent version.
8. From the **Subnet/prefix** drop-down list, select a subnet.
9. From the **Timezone** drop-down list, select the time zone.
10. From the **Device Tag** drop-down list, select the device tag.
11. From the **IP Type** drop-down list, select the IP type.
12. From the **BIOS version** drop-down list, select the BIOS version.

Save the filter in Devices page

You can save the current filter as a group by configuring the required filter options.

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**.

Query the device status

You can send a command to update the device information and status in the system.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. Click **Query**.
   An **Alert** window is displayed.
5. Click **Send Command** to send the query command.

Lock the devices

You can send a command to lock the registered device for a group of devices that are connected to a VDI session. This option is applicable for thin clients running ThinOS operating system.

Prerequisites

The device should be connected to a VDI connection, and a user must be logged in to the device.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. Click **Lock**.
   An **Alert** window is displayed.
5. Click **Send Command** to send the lock command.

   From Wyse Management Suite 3.2, you can also send a command to lock the device from the **Jobs** page. For more information, see Schedule a device command job.

Restart the devices

You can send a command to restart a registered device.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. Click **Restart**.
   An **Alert** window is displayed.
5. Click **Send Command** to send the restart command.

Unregister the device

You can send a command to unregister a device from Wyse Management Suite.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. Click **Unregister**.
   An **Alert** window is displayed.
5. Select the **Force Unregistration** check box.
6. Click **Send Command** to send the unregister command.

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

Enrollment Validation

When you register a device manually or using DHCP/DNS auto discovery method, the device gets registered to a particular group if the group token is defined. If the group token is not defined, the device gets registered to the unmanaged group.

In Wyse Management Suite, the **Enrollment Validation** option is introduced where the tenant must manually approve before the device is registered to a group.

When the **Enrollment Validation** option is enabled, the auto-discovered devices are in **Pending Validation** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated. For more information about how to validate the devices, see Enrollment validation.

NOTE: The **Enrollment Validation** option is disabled for existing tenants in the public cloud or when you upgrade on-premise tenants.

The validation status of the devices is also displayed in the **Devices** section on the **Dashboard** page.

Validate the enrollment of a device

You can enable **Enrollment Validation** to enable administrators to control the manual and auto registration of thin clients to a group. You can filter the devices in **Pending Validation** state by clicking the **Pending** count in the **Dashboard** page or by selecting the **Enrollment Validation Pending** in the **Status** drop-down list in the **Devices** page.

Prerequisites

- You must enable the **Enrollment Validation** option when you install Wyse Management Suite or in the **Portal Administration** page.
- The device must be in Enrollment Pending state.

Steps

1. Select the check box of the device that you want to validate.
2. Click the **Validate Enrollment** option.
   An **Alert** window is displayed.
3. Click **Send Command**.
   The device moves to the wanted group, and the device is registered.

Reset the device to factory default settings

You can send a command to reset your device to factory default settings.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Factory Reset**.
   An **Alert** window is displayed.
5. Enter the reason for the client reset.
6. Click **Send Command**.

   From Wyse Management Suite 3.2, you can also send a command to lock the device from the **Jobs** page. For more information, see Schedule a device command job.

Change a group assignment on the Devices page

You can change the group assignment of a device using the **Devices** page.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Change Group**.
   The **Change Group Assignment** window is displayed.
5. From the drop-down menu, select a new group for the device.
6. Click **Save**.

Send messages to a device

You can send a message to a registered device using the **Devices** page.

Steps

1. Click **Devices**.
   The **Devices** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Send Message**.
   The **Send Message** window is displayed.
5. Enter the message.
6. Click **Send**.

   From Wyse Management Suite 3.2, you can also send a message to the device from the **Jobs** page. For more information, see Schedule a device command job.

Wake On LAN command

You can send a command to activate a device if it is turned off or in the Sleep mode.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Wake On LAN**.
   An **Alert** window is displayed.
5. Click **Send Command**.

View the device details

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.

3. Click any of the displayed devices.
   The **Device Details** page is displayed.

View the display parameters

From Wyse Management Suite 3.1, you can view the display setup of the devices running a Windows Embedded and ThinLinux operating system. You can view the vendor name, model number, serial number, resolution, aspect ratio, mode, alignment, and rotation details of the display setup.

Steps

1. Go to the **Devices** page.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.

   The **Device Details** page is displayed.

4. Go to **System Info** > **Peripherals**.
   You can view the display setup details.

Peripherals

Monitor

Vendor	Model	Serial Number	Resolution	Aspect Ratio	Rotation	Mode	Alignment
DELL	UP3017	216L	2560x1600	16:10	normal	Span	3840,0
DELL	P2415Q	J0V0B(Primary)	3840x2160	16:9	normal	Span	0,0
DELL	P2415Q	V0D4L	3840x2160	16:9	normal	Span	6400,0
DELL	UP3017	211L	2560x1600	16:10	normal	Span	10240,0
DELL	P2415Q	YRB	0x0	0:0	normal	Span	12800,0
DELL	P2415Q	D5L	0x0	0:0	normal	Span	12800,0

Figure 7. Display parameters

View the virtual NIC details

From Wyse Management Suite 3.1, you can view the network adapter details of the devices running a Windows Embedded and ThinLinux operating system. You can view the adapter name, MAC address, IP address, Gateway IP address, and DNS server details of the Network Adaptor.

Steps

1. Go to the **Devices** page.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.

   The **Device Details** page is displayed.

4. Go to **System Info** > **Network Details - Network Adapters**.
   You can view the virtual NIC details in the **Network Details - Network Adapters** section.

Figure 8. Network Details - Network Adapters

View the BIOS details

From Wyse Management Suite 3.1, you can view the BIOS parameter value on the **Device Details** page.

Steps

1. Go to the **Devices** page.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.

   The **Device Details** page is displayed. You can view the BIOS details in the **BIOS settings** section of the **SystemInfo** tab.

Manage the device summary

You can view and manage information about the Notes, Group Assignment, Alerts, and Device Configuration using the **Devices** page.

Steps

1. Click **Devices**.
2. On the **Device Details** page, click **Summary** tab.
   The device summary is displayed.
3. In the right pane, click **Add note**.
   An **Add Note** window is displayed.
4. Type the message in the provided field and click **Save**.
5. In the right pane, click **Change Group Assignment**.
   The **Change Group Assignment** window is displayed.
6. From the drop-down menu, select a new group for the device.
7. Click **Save**.
8. Click **Create/Edit exceptions** to create or edit a device level exception, and configure a particular device policy on the **Devices** page.

View the system information

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.
   The **Device Details** page is displayed.
4. Click **System Info**.
   The system information is displayed.

View device events

You can view and manage information about the system events pertaining to a device.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.
   The **Device Details** page is displayed.
4. On the **Device Details** page, click **Events** tab.
   The events on the device are displayed.

View the installed applications

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
   The preferred device list is displayed.
3. Click any of the displayed devices.
   The **Device Details** page is displayed.
4. Click **Installed Apps** tab.
   The list of installed applications on the device is displayed.

   This option is available for Windows Embedded Standard, Linux, and ThinLinux devices. The following are the attributes that are displayed on the page:
   - Name
   - Publisher
   - Version
   - Installed On

   NOTE:

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

Rename the thin client

You can use this page to change the hostname of thin clients that run on Windows Embedded Standard, ThinLinux, and ThinOS operating systems.

Steps

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 hostname 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 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 hostname is updated.

   NOTE: A ThinLinux device need not be restarted to update the hostname.

5. Click **Send Command**.
   A confirmation message is displayed.

Enable remote shadow connection

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

Steps

1. On the **Devices** page, click the device.
2. From the **More options** drop-down list, select the **Remote Shadow (VNC)** option.
   The IP address and the port number of the target thin client is displayed in the **Remote Shadow (VNC)** dialog box.
   NOTE: The default port number is 5900.
3. Change the port number of the target thin client—optional.
4. Click **Connect** to initiate a remote session to the target thin client.
   NOTE: Wyse Management Suite portal supports a maximum of five remote shadow sessions per tenant.

Configure remote shadow connection for Dell Hybrid Client devices

Use this page to enable global and group administrators to access the Dell Hybrid Client devices sessions remotely. This feature is applicable to only to private cloud and is available for both Standard and Pro licenses.

Steps

1. Deploy the VNC add-on package from Wyse Management Suite using Standard or advanced application policy—see Application Policy.
   The add-on is installed and the device reboots.
2. Configure and deploy the VNC server options from Wyse Management Suite. To configure the VNC Server options, do the following:
   a. Go to the **Groups & Configs** page, and select a group.
   b. From the **Edit Policies** drop-down menu, click **Hybrid Client**.
      The **Configuration Control | Hybrid Client** window is displayed.
   c. Click the **Standard** or **Advanced** option.
   d. Go to **Privacy & Security** > **VNC Server** and configure the options.
   e. Click **Save & Publish**.

Shutting down devices

Wyse Management Suite enables you to shut down the devices such as Windows Embedded Standard, ThinLinux, and ThinOS thin clients.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to locate the preferred device.
   The preferred device list is displayed.
3. From the **More Options** drop-down list, click **Shutdown Now**.
   The remote command to shut down the device is sent to the selected device. The device responds to the server, and the command is applied successfully.

NOTE: The **Shutdown Now** option is not enabled for thin clients running on Linux operating system.

Tag a device

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

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to locate the preferred device.
   The preferred device list is displayed.
3. Select one or more devices. From the **More Options** drop-down list, click **Tag Device**.
   The **Set Device Tag** window is displayed.
4. Enter the preferred tag name.
5. Click **Set Tag**.

Device compliance status

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

- Red—when the registered device has not been checked in for more than seven days.
- Gray—When you apply any configuration policy to the device.
- Green—When you apply all the configuration policies to the device.

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

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

- Red—When the device has not sent its heartbeat for more than three attempts .
- Gray—When the device has not sent its heartbeat for more than two attempts but fewer than three attempts.
- Green—When the device sends its heartbeat regularly.

Pulling Windows Embedded Standard or ThinLinux image

Prerequisites

- If you are using Wyse Management Suite 1.3 remote repository, then Recovery/ Recovery + OS pull template are not available in the repository. You must upgrade Wyse Management Suite to 1.4 or later versions to access the templates.
- To perform ThinLinux image pull operation, you must close the **Settings** window in the ThinLinux device. You must perform this operation before pulling an OS/OS+Recovery image from the ThinLinux device.
- To upgrade from ThinLinux 1.x to 2.x, the administrator must update the device with the latest WDA and merlin and then pull the image. This pulled image must be used to upgrade from ThinLinux 1.x to 2.x.
- Ensure that the virtual machine where the server is running has sufficient memory to perform the pull and run the required services for Wyse management Suite if you are using a local repository.

Steps

1. Go to the **Windows Embedded Standard** or **ThinLinux** device page.
2. Select **Pull OS Image** option, from the **More Actions** drop-down list.
3. Enter or select the following details:
   - **Name of Image**—Provide a name for the image. To replace the image with a similar name and the image files which are not completed successfully, click **Override name**.
   - **File repository**—From the drop-down list, select the file repository to where the image is uploaded. There are two types of file repositories:
     - Local repository

- Remote Wyse Management Suite repository
- **Pull Type**—Select either **Default** or **Advanced** based on your pull type requirement.
  - When the **Default** pull type is selected, the following options are displayed:
    - Compress
    - OS
    - BIOS
    - Recovery––For ThinLinux 2.x
  - When the **Advanced** pull type is selected, a drop-down list for selecting the templates is displayed. Select any template which is available by default.

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

4. Click **Prepare for Image Pull**.

Results

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

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

  NOTE: This option is applicable for Windows Embedded Standard devices.
- **Pull now**—The device boots to the Merlin operating system and the image pull operation is performed.

Request a log file

You can request a device log from Windows Embedded Standard, ThinOS, and ThinLinux devices. The ThinOS device uploads the system logs. The Windows Embedded Standard uploads Wyse Device Agent logs and Windows Event viewer logs. Linux or ThinLinux uploads Wyse Device Agent logs and system logs.

Prerequisites

The device must be enabled to pull the log file.

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.

   NOTE: The device logs are in `Hostname-timestamp` format. Dell Hybrid Client, Linux, or ThinLinux uploads the log file in `.tar` format and Windows or ThinOS 9.x system uploads the log file in `.zip` format.

Troubleshooting your device

You can view and manage the troubleshooting information using the **Devices** page.

Steps

1. On the **Device Details** page, click **Troubleshooting** tab.
2. Click **Request Screen Shot**.

   You can capture the screenshot of the thin client with or without the client permission. If you select the **Require User Acceptance** check box, then a message is displayed on the client. This option is applicable only for Windows Embedded Standard, Linux, and ThinLinux devices.
3. Click **Request Processes List**, to view the list of the processes running on the thin client.

4. Click **Request Services List**, to view the list of the services running on the thin client.
5. Click **Start Monitoring**, to access the performance metric console.
   On the **Performance metric** console, the following details are displayed:
   - Average CPU last minute
   - Average memory usage last minute

Reimage your Dell Hybrid Client

You can send a command to reimage your Dell Hybrid Client.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **ReImage**.
   An **Alert** window is displayed.
5. Click **Send Command**.
   This action performs recovery image function for the device.

Convert your Dell Generic Client to Hybrid Client

You can send a command to convert your Dell Generic Client to Dell Hybrid Client.

Prerequisites

Dell Ubuntu device (Generic Client) should be preloaded with Dell Hybrid Bundle in the recovery partition.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred Generic Client device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Convert to Hybrid**.
   An **Alert** window is displayed.
5. Click **Send Command**.

   NOTE: The **Convert to Hybrid** command is also available in the **Jobs**, **Devices**, and **Device Details** page.

Pull configuration user interface package for Dell Hybrid Client

When a Dell Hybrid Client has a higher version of the configuration schema than the version present in the Wyse Management Suite server, you can pull the latest configuration user interface package.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. click the device you want to configure.
   The **Device Details** page is displayed.

4. From the **More Actions** drop-down menu, click **Pull Configuration UI Package**.
   An **Alert** window is displayed.
5. Click **Send Command**.

Reset your Dell Hybrid Client to factory settings

You can send a command to reset your Dell Hybrid Client to factory settings.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. From the **More Actions** drop-down menu, click **Factory Reset**.
   An **Alert** window is displayed.
5. Enter the reason for the Dell Hybrid Client reset.
6. Click **Send Command**.

Bulk group change of devices

From Wyse Management Suite 3.2, you can change the group of several devices using the serial number, MAC address, or Hostname. This option is applicable only for Wyse Management Suite with a pro license.

Prerequisites

Create a CSV file with the serial number, MAC address, or Hostname of the devices.

Steps

1. Click **Devices**.
   The **Devices** page is displayed.
2. From the **More Actions** drop-down list, select **Bulk Change Group**.
   The **Bulk Change Group Assignment** window is displayed.
3. From the **Select the property to filter Device** drop-down list, select a property to filter the devices to change to a new group based on the selected property.
4. To select the CSV file, click **Browse** and go to the location where the CSV file is located.
5. From the **Select a new group for these devices** drop-down list, select the new group for the devices.
6. Click **Save**.

   NOTE: You can change the group of a maximum of 100 devices at a time.

9

Apps and data

This section describes how to perform routine device application tasks, operating system imaging, inventory management, and set policies by using the Wyse management console. The repository names are color coded to indicate the status.

You can configure the following type of policies using the **Apps and Data** page:

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

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

NOTE: From Wyse Management Suite 3.3, 5000 concurrent downloads of the configurations to the client are supported. Any further concurrent download is moved to a queued state until a slot is free. The request is timed out after 60 s.

Topics:

Application policy

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

- Configure thin client application inventory
- Configure Wyse Software thin client application inventory
- Create and deploy standard application policy to thin clients
- Create and deploy advanced application policy to thin clients
- Create and deploy standard application policy to Wyse Software Thin Clients
- Create and deploy advanced application policy to Wyse Software Thin Clients

Important notes for Windows-based devices:

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

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

- For deploying .exe applications by using Wyse Management Suite, follow the silent installation method. You must enter the appropriate silent parameters if required. For example, **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**.

- Supports script deployments with file extensions .bat, .cmd, .ps1, .vbs.

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

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

Important notes for Linux devices:

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

Configure thin client application inventory

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, place the thin client application files in the `<repo-dir>\repository\thinClientApps` folder.
   Wyse Management Suite Repository sends metadata for all the files to the Wyse Management Suite server periodically.
4. To edit the application, do the following:
   a. Select the uploaded application from the list.
   b. Click **Edit App**.
      The **Edit Application** window is displayed.
   c. Enter the note.
   d. Click **Save**.

      NOTE: Global suffix is added to the applications uploaded by the operator.

   The applications that are present in different repositories are listed once. The **Repository Name** column displays the number of repositories in which the application is present. You can hover over the column to view the name of the repositories. Also, the name of the repository is color coded to specify the availability.

Configure Wyse Software thin client application inventory

Steps

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

Create and deploy standard application policy to thin clients

Steps

1. In the local repository, go to **thinClientApps**, and copy the application to the folder.
2. Go to **Apps & Data** > **App Inventory** > **Thin Client** and verify that the application is registered to Wyse Management Suite.

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

3. Go to **Apps & Data** > **App Policies** > **Thin Client**.
4. Click **Add Policy**.
   Add Standard App Policy window is displayed.
5. Enter the **Policy Name**.
6. From the **Group** drop-down list, select the group.
7. From the **Task** drop-down list, select the task.
8. From the **OS Type** drop-down list, select the operating system.
9. Select the **Filter files based on extensions** checkbox to filter the applications.
10. From the **Application** drop-down list, select the application.
    If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.

    NOTE: From Wyse Management Suite 3.1, you can add a script to install application on ThinLinux devices. You must verify if a valid shebang is present in the script for ThinLinux.

11. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.

12. From the **Apply Policy Automatically** drop-down list, select any of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.

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

13. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.

    NOTE: The **Application Installation Timeout** option is applicable only for Windows Embedded Standard, Wyse Software thin clients, Linux, and Thin Linux devices.

14. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
15. Select **Yes** to schedule a job on the same page.
16. Select any of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
17. To create the job, click **Preview** and schedules are displayed on the next page.
18. You can check the status of the job by going to the **Jobs** page.

    NOTE: You can update BIOS using the standard application policy. You must use `/s/r/f/p=fireport` as install parameters to update BIOS.

Create and deploy standard application policy to Wyse Software thin clients

Steps

1. In the local repository, go to **softwareTcApps**, and copy the application to the folder.
2. Go to **Apps & Data** > **App Inventory** > **Wyse Software thin client** and verify that the application is registered to Wyse Management Suite.

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

3. Click **Add Policy**.
   Add Standard App Policy window is displayed.
4. Enter the **Policy Name**.
5. From the **Group** drop-down list, select the group.
6. From the **Task** drop-down list, select the task.
7. From the **OS Type** drop-down list, select the operating system.
8. Select the **Filter files based on extensions** checkbox to filter the applications.
9. From the **Application** drop-down list, select the application.
   If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
10. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.

11. From the **Apply Policy Automatically** drop-down list, select any of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that are registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.

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

12. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.

    NOTE: The **Application Installation Timeout** option is applicable only for Windows Embedded Standard devices and Wyse Software thin clients.

13. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
14. Select **Yes** to schedule a job on the same page.
15. Select any of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
16. To create the job, click **Preview** and schedules are displayed on the next page.
17. You can check the status of the job by going to the **Jobs** page.

Enable single sign-on for Citrix StoreFront using standard application policy

To enable single sign-on for Citrix StoreFront, do the following:

- **Scenario 1**—If you want to enable single sign-on for StoreFront on the current version of Citrix Receiver, do the following:
  1. Create and deploy a standard application policy to uninstall the Citrix Receiver using the parameter **`/silent`**.
  2. Create and deploy a standard application policy to install the Citrix Receiver again using the parameter **`/silent /includeSSON /AutoUpdateCheck = Disabled`**.
- **Scenario 2**—If you want to upgrade Citrix Receiver and enable single sign-on for StoreFront, do the following:
  1. Create and deploy a standard application policy to upgrade the Citrix Receiver using the parameter **`/silent /includeSSON /AutoUpdateCheck = Disabled`**.
- **Scenario 3**—If you want to downgrade Citrix Receiver and enable single sign-on for StoreFront, do the following:
  1. Create and deploy a standard application policy to downgrade the Citrix Receiver using the parameter **`/silent /includeSSON /AutoUpdateCheck = Disabled`**.

Create and deploy advanced application policy to thin clients

Steps

1. Copy the application and the pre or post install scripts (if necessary) to deploy to the thin clients.
2. Save the application and the pre/post install scripts in the `thinClientApps` folder of the local repository or the Wyse Management Suite repository.
3. Go to **Apps & Data** > **App Inventory** > **Thin Client** and verify that the application is registered.

4. Go to **Apps & Data** > **App Policies** > **Thin Client**.
5. Click **Add Advanced Policy**.
   Add Advanced App Policy page is displayed.
6. Enter the **Policy Name**.
7. From the **Group** drop-down list, select the group.
8. Select the **Sub Groups** check box to apply the policy to sub groups.
9. From the **Task** drop-down list, select the task.
10. From the **OS Type** drop-down list, select the operating system.
11. Select the **Filter files based on extensions** checkbox to filter the applications.
12. Click **Add app**, and select one or more applications under **Apps**. For each application, you can select a pre and post-install script under **PreInstall**, **PostInstall**, and **Install Parameters**.

    NOTE: From Wyse Management Suite 3.1, you can add a script to install application on ThinLinux devices. You must verify if a valid shebang is present in the script for ThinLinux.

13. If you want the system to reboot after the application is successfully installed, select **Reboot**.
14. Click **Add app** and repeat the step to add multiple applications.

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

    If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
15. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
16. Specify the number of minutes the message dialog box should be displayed on the client.
    A message on the client which gives you time to save your work before the installation begins.
17. To enable delay in implementation of the policy, select the **Allow delay of policy execution** checkbox. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay running the policy.
    - From the **Max delays** drop-down list, select the number of times (1–3) you can delay running the policy.
18. From the **Apply Policy Automatically** drop-down list, select any of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.

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

19. Select the **Skip write filter check** check box to skip the write filter cycles. This option is applicable for Windows Embedded Standard operating system devices and Wyse Software thin client devices.
20. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.

    NOTE: The **Application Installation Timeout** option is applicable only for Windows Embedded Standard devices and Wyse Software thin clients.

21. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
22. Select **Yes** to schedule a job on the same page.
23. Select any of the following options:
    - **Immediately**—Server runs the job immediately.

- **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
- **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.

24. To create the job, click **Preview** and schedules are displayed on the next page.
25. You can check the status of the job by going to the **Jobs** page.

Create and deploy advanced application policy to Wyse Software Thin Clients

Steps

1. Copy the application and the pre/post install scripts (if necessary) to deploy to the thin clients.
2. Save the application and the pre/post install scripts in the `softwareTcApps` folder of the local repository or the Wyse Management Suite repository.
3. Go to **Apps & Data** > **App Inventory** > **Wyse Software thin client** and verify that the application is registered.
4. Go to **Apps & Data** > **App Policies** > **Wyse Software thin client**.
5. Click **Add Advanced Policy**.
   Add Advanced App Policy page is displayed.
6. Enter the **Policy Name**.
7. From the **Group** drop-down list, select the group.
8. Select the **Sub Groups** check box to apply the policy to sub groups.
9. From the **Task** drop-down list, select the task.
10. From the **OS Type** drop-down list, select the operating system.
11. Select the **Filter files based on extensions** checkbox to filter the applications.
12. Click **Add app**, and select one or more applications under **Apps**. For each application, you can select a pre and post-install script under **PreInstall**, **PostInstall**, and **Install Parameters**.
13. If you want the system to reboot after the application is successfully installed, select **Reboot**.
14. Click **Add app** and repeat the step to add multiple applications.

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

    If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
15. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
16. Specify the number of minutes the message dialog box should be displayed on the client.
    A message on the client which gives you time to save your work before the installation begins.
17. To enable delay in implementation of the policy, select the **Allow delay of policy execution** checkbox. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay running the policy.
    - From the **Max delays** drop-down list, select the number of times (1–3) you can delay running the policy.
18. From the **Apply Policy Automatically** drop-down list, select any of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.

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

19. Select the **Skip write filter check** check box to skip the write filter cycles. This option is applicable for Windows Embedded Standard operating system devices and Wyse Software thin client devices.
20. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.

    NOTE: The **Application Installation Timeout** option is applicable only for Windows Embedded Standard devices and Wyse Software thin clients.

21. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
22. Select **Yes** to schedule a job on the same page.
23. Select any of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
24. To create the job, click **Preview** and schedules are displayed on the next page.
25. You can check the status of the job by going to the **Jobs** page.

Create and deploy standard application policy to Dell Hybrid Clients

Steps

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

   NOTE: You can deploy and install only Dell-signed applications on Dell Hybrid Clients.

   NOTE: The operator can upload the Dell Hybrid Client bundles and packages from the operator account. After the operator uploads the packages and files, they are visible to all the tenants. Tenants cannot delete or modify the files. The operator cannot upload ISO files.

2. Go to **Apps & Data** > **App Inventory** > **Hybrid Client** and verify that the application is registered to Wyse Management Suite.

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

3. Go to **Apps & Data** > **App Policies** > **Hybrid Client**.
4. Click **Add Policy**.
   Add Standard App Policy window is displayed.
5. Enter the **Policy Name**.
6. From the **Group** drop-down list, select the group.
7. From the **Task** drop-down list, select the task.
8. From the **OS Type** drop-down list, select the operating system.
9. From the **Application** drop-down list, select the application.
   If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
10. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
11. In the **Install Parameters** field, enter the install parameters for the selected application.
12. From the **Apply Policy Automatically** drop-down list, select one of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present

in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.

13. Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1-999 min)** box. Timeout displays a message on the client which gives you time to save your work before the installation begins.
14. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.
15. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
16. Select **Yes** to schedule a job on the same page.
17. Select any of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
18. To create the job, click **Preview** and schedules are displayed on the next page.
19. You can check the status of the job by going to the **Jobs** page.

NOTE: You must push the **DHCImageupgardeAddon** package before upgrading Dell Hybrid Client version 1.1 to 1.5.

Create and deploy advanced application policy to Dell Hybrid Clients

Steps

1. Copy the application and the install scripts (if necessary) to deploy to the thin clients.

   NOTE: You can deploy and install only Dell-signed applications and scripts on Dell Hybrid Clients.

   NOTE: The operator can upload the Dell Hybrid Client bundles and packages from the operator account. After the operator uploads the packages and files, they are visible to all the tenants. Tenants cannot delete or modify the files. The operator cannot upload ISO files.

2. Save the application and the install scripts in the `hybridClientApps` folder of the local repository or the Wyse Management Suite repository.
3. Go to **Apps & Data** > **App Inventory** > **Hybrid Client** and verify that the application is registered.
4. Go to **Apps & Data** > **App Policies** > **Hybrid Client**.
5. Click **Add Advanced Policy**.
   Add Advanced App Policy page is displayed.
6. Enter the **Policy Name**.
7. From the **Group** drop-down list, select the group.
8. Select the **Sub Groups** check box to apply the policy to sub groups.
9. From the **Task** drop-down list, select the task.
10. From the **OS Type** drop-down list, select the operating system.
11. Select the **Filter files based on extensions** checkbox to filter the applications.
12. Click **Add app**, and select one or more applications under **Apps**. For each application, you can select a pre and post-install script under **PreInstall**, **PostInstall**, and **Install Parameters**.
13. If you want the system to reboot after the application is successfully installed, select **Reboot**.
14. Click **Add app** and repeat the step to add multiple applications.

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

    If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
15. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.

16. Specify the number of minutes the message dialog box should be displayed on the client.
A message on the client which gives you time to save your work before the installation begins.
17. To enable delay in implementation of the policy, select the **Allow delay of policy execution** checkbox. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay running the policy.
    - From the **Max delays** drop-down list, select the number of times (1–3) you can delay running the policy.
18. From the **Apply Policy Automatically** drop-down list, select one of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.
19. Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1-999 min)** box. Timeout displays a message on the client which gives you time to save your work before the installation begins.
20. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.
21. Click **Save** to create a policy.
A message is displayed to enable the administrator to schedule this policy on devices based on group.
22. Select **Yes** to schedule a job on the same page.
23. Select one of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
24. To create the job, click **Preview** and schedules are displayed on the next page.
25. You can check the status of the job by going to the **Jobs** page.

NOTE: You must push the **DHCImageupgardeAddon** package before upgrading Dell Hybrid Client version 1.1 to 1.5.

Create and deploy standard application policy to Dell Generic Clients

Steps

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

   NOTE: You can deploy and install only Dell-signed (DHC Fish scripts, DCA-Enabler packages, DHC Bundles, or DHC ISO Image files) applications on Dell Generic Clients.
2. Go to **Apps & Data** > **App Inventory** > **Generic Client** and verify that the application is registered to Wyse Management Suite.

   NOTE: The App Inventory interface takes approximately two minutes to populate the recently added programs.
3. Go to **Apps & Data** > **App Policies** > **Generic Client**.
4. Click **Add Policy**.
Add Standard App Policy window is displayed.
5. Enter the **Policy Name**.
6. From the **Group** drop-down list, select the group.

7. From the **Task** drop-down list, select the task.
8. From the **OS Type** drop-down list, select the operating system.
9. From the **Application** drop-down list, select the application.
   If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
10. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
11. From the **Apply Policy Automatically** drop-down list, select one of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.
12. Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1-999 min)** box. Timeout displays a message on the client that gives you time to save your work before the installation begins.
13. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.
14. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
15. Select **Yes** to schedule a job on the same page.
16. Select any of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
17. To create the job, click **Preview** and schedules are displayed on the next page.
18. You can check the status of the job by going to the **Jobs** page.

Create and deploy advanced application policy to Dell Generic Clients

Steps

1. Copy the application and the install scripts (if necessary) in the `genericClientApps` folder of the local repository or the Wyse Management Suite remote repository.

   NOTE: You can deploy and install only Dell-signed applications and scripts (DHC Fish scripts, DCA-Enabler packages, DHC Bundles, or DHC ISO Image files) on Dell Generic Clients.
2. Go to **Apps & Data** > **App Inventory** > **Generic Client** and verify that the application is registered.
3. Go to **Apps & Data** > **App Policies** > **Generic Client**.
4. Click **Add Advanced Policy**.
   Add Advanced App Policy page is displayed.
5. Enter the **Policy Name**.
6. From the **Group** drop-down list, select the group.
7. Select the **Sub Groups** check box to apply the policy to sub groups.
8. From the **Task** drop-down list, select the task.
9. From the **OS Type** drop-down list, select the operating system.
10. Select the **Filter files based on extensions** check box to filter the applications.
11. Click **Add app**, and select one or more applications under **Apps**.
12. If you want the system to reboot after the application is successfully installed, select **Reboot**.

13. Click **Add app** and repeat the step to add multiple applications.

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

    If the application files are available on multiple repositories, then the number of repositories is displayed next to the file name.
14. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
15. Specify the number of minutes the message dialog box should be displayed on the client.
    A message on the client that gives you time to save your work before the installation begins.
16. To enable delay in implementation of the policy, select the **Allow delay of policy execution** check box. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down list, select the maximum hours (1–24 hours) you can delay running the policy.
    - From the **Max delays** drop-down list, select the number of times (1–3) you can delay running the policy.
17. From the **Apply Policy Automatically** drop-down list, select one of the following options:
    - **Do not apply automatically**—This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices**—This option automatically applies the policy to a registered device that belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.
    - **Apply the policy to devices on check in**—This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

    NOTE: The job status of the newly added device count that is checked in to Wyse Management Suite is not displayed.
18. Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1-999 min)** box.
    Timeout displays a message on the client that gives you time to save your work before the installation begins.
19. To stop the installation process after a defined value, specify the number of minutes in the **Application Installation Timeout** field. The default value is 60 minutes.
20. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
21. Select **Yes** to schedule a job on the same page.
22. Select one of the following options:
    - **Immediately**—Server runs the job immediately.
    - **On device time zone**—Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone**—Server creates one job to run at the date or time of the designated time zone.
23. To create the job, click **Preview** and schedules are displayed on the next page.
24. You can check the status of the job by going to the **Jobs** page.

Image policy

Wyse Management Suite supports the following types of operating system image deployment policies:

- Add Windows Embedded Standard operating system and ThinLinux images to the repository
- Add ThinOS firmware to the repository
- Add ThinOS package file to the repository
- Add ThinOS BIOS file to the repository
- Add Teradici firmware to the repository
- Create Windows Embedded Standard and ThinLinux image policies
- Create Dell Hybrid Client image policies

Add Windows Embedded Standard operating system and ThinLinux images to repository

Prerequisites

- If you are using Wyse Management Suite with cloud deployment, go to **Portal Administration** > **Console Settings** > **File Repository**. Click **Download version 3.2.0** to download the `WMS_Repo.exe` file and install the Wyse Management Suite repository installer.
- If you are using Wyse Management Suite with on-premise deployment, the local repository is installed during Wyse Management Suite installation process.

Steps

1. Copy the Windows Embedded Standard operating system images or ThinLinux images to the `<Repository Location>\repository\osImages\zipped` folder.

   Wyse Management Suite extracts the files from the zipped folder and uploads the files in the `<Repository Location>\repository\osImages\valid` location. The image extraction may take several minutes depending upon the image size.

   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.

Add ThinOS firmware to repository

Steps

1. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS**.
2. Click **Add Firmware file**.
   The **Add File** screen is displayed.
3. To select a file, click **Browse** and go to the location where your file is located.
4. Enter the description for your file.
5. Select the check box if you want to override an existing file.
6. Click **Upload**.

   NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy firmware to a device or a group of devices, go to the respective device or group configuration page.

Add ThinOS BIOS file to repository

Steps

1. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS**.
2. Click **Add BIOS file**.
   The **Add File** screen is displayed.
3. To select a file, click **Browse** and go to the location where your file is located.
4. Enter the description for your file.
5. Select the check box if you want to override an existing file.
6. Select the platform from the BIOS platform type drop-down list.
7. Click **Upload**.

   NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy the BIOS file to a device or a group of devices, go to the respective device or group configuration page.

Add ThinOS package file to repository

Steps

1. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS**.
2. Click **Add Package file**.
   The **Add File** screen is displayed.
3. To select a file, click **Browse** and go to the location where your file is located.
4. Enter the description for your file.
5. Click **Upload**.

   NOTE: If the application exists in the public repository, the application reference is added to the inventory. Else, the application is uploaded to the public repository and the reference is added to the inventory. Also, ThinOS firmware and BIOS packages that are uploaded by the operator cannot be deleted by tenant administrators.

Create Windows Embedded Standard and ThinLinux image policies

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 options:
      - 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**.

Add ThinOS 9.x firmware to the repository

Steps

1. Log in to Wyse Management Suite.
2. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS 9.x**.
3. Click **Add Firmware file**.
   The **Add File** screen is displayed.
4. To select a file, click **Browse** and go to the location where your file is located.
5. Enter the description for your file.
6. Select the check box if you want to override an existing file.
7. Click **Upload**.

NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy firmware to a device or a group of devices, go to the respective device or the group configuration page.

NOTE: The operator can upload the firmware from operator account and is visible to all the tenants. Tenants cannot delete or modify the files.

Add ThinOS 9.x BIOS file to repository

Steps

1. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS 9.x**.
2. Click **Add BIOS file**.
   The **Add File** screen is displayed.
3. To select a file, click **Browse** and go to the location where your file is located.
4. Enter the description for your file.
5. Select the check box if you want to override an existing file.
6. Select the platform from the BIOS platform type drop-down list.
7. Click **Upload**.

   NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy the BIOS file to a device or a group of devices, go to the respective device or group configuration page.

   NOTE: The operator can upload the firmware from operator account and is visible to all the tenants. Tenants cannot delete or modify the files.

Add ThinOS application packages to the repository

Steps

1. Log in to Wyse Management Suite using your tenant credentials.
2. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS 9.x**.
3. Click **Add Package file**.
   The **Add Package** screen is displayed.
4. To select a file, click **Browse** and go to the location where your file is located.
   - If the EULA is embedded in the package, the EULA details of the package and the name of the vendors are displayed. You can click the vendor names to read the license agreement of each vendor. Click **Accept** to upload the package. You can select the **Do not show this again** if you do not want to see the EULA details of the same vendor again. You must accept the license agreement of the packages individually. The package is not uploaded if you click **Decline**.
   - If the EULA is not embedded in the package, go to step 5.
5. Click **Upload**.

   NOTE: The operator can upload the package from operator account and is visible to all the tenants. Tenants cannot delete or modify these files.

Create Dell Hybrid Client image policies

You can create a Dell Hybrid Client image policy to convert Wyse 5070 Thin Clients running Windows 10 IoT Enterprise, ThinLinux 2.x and ThinOS 8.x operating system to Dell Hybrid Client devices.

Steps

1. In the **Apps & Data** tab, under **OS Image policies**, click **Hybrid Client**.
2. Click **Add Policy**.

3. In the **Add Hybrid Client 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 **Force this version**.
   h. From the **Apply Policy Automatically** drop-down menu, select one of the following options:
      - 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.
4. Click **Save**.

NOTE: The number of DHC licenses must be greater than or equal to the number of Wyse 5070 Thin Clients that are converted to Dell Hybrid Client.

NOTE: The DHC Conversion OS image provided in the zipped or exe format must be copied to the `\repository\osImages\zipped` folder. The DHC OS Image is displayed under **Apps & Data** > **OS Image Repository** > **Hybrid Client** after the repository synchronization.

NOTE: You must create an OS Image Policy to deploy DHC Conversion Image to Wyse 5070 Thin Clients running Windows Embedded, ThinLinux, ThinOS and ThinOS with PCoIP operating system.

NOTE: Ensure that the merlin package is updated to 408 or higher for thin clients running Windows 10 IoT Enterprise and ThinLinux 2.x operating system.

Manage file repository

This section enables you to view and manage the file repository inventories, such as wallpaper, logo, EULA text file, Windows wireless profile, and certificate files.

Steps

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 go 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
   - Hosts
   - Rules

   NOTE: To view the maximum size and the supported format of the files that you can upload, click the **information (i)** icon.
5. Select the check box if you want to override an existing file.

NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To assign the file, go to the respective device configuration page.

6. Click **Upload**.

How to change wallpaper for all devices belonging to marketing group

Steps

1. Go 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 select 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. Go to the **Groups & Configs** page.
2. Select a policy group.
3. Click **Edit Policies**, and select **WES**.
4. Select **Desktop Experience** and click **Configure this item**.
5. Select **Desktop Wallpaper**.
6. From the drop-down list, select the wallpaper file.
7. 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.

10

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**

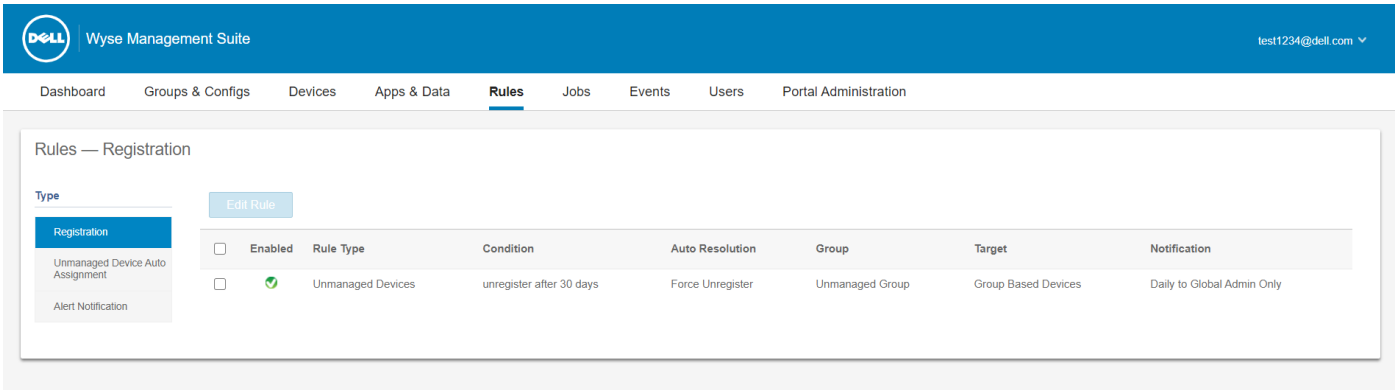


Figure 9. Rules page

Topics:

Edit a registration rule

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

Steps

1. Click **Rules**.
   The **Rules** page is displayed.
2. Click **Registration**, and select the unmanaged devices option.
3. Click **Edit Rule**.
   The **Edit Rule** window is displayed.

   You can view the following details:
   - Rule
   - Description
   - Device Target
   - Group
4. From the drop-down menu, select a target client to apply the **Notification Target** option and the time duration to apply the **Notification Frequency** option.

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

5. Enter the number of days until you want to apply the rule in the **Apply rule after (1–30 days)** box.

   NOTE: By default, registration of an unmanaged device are unregistered after 30 days.

6. Click **Save**.

Create auto assignment rules for unmanaged devices

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Click the **Add Rules** tab.
4. Enter the **Name**, and select the **Destination group**.
5. Click the **Add Condition** option, and select the conditions for assigned rules.
6. Click **Save**.

   The rule is displayed in the unmanaged group list. This rule is applied automatically, and the device is listed in the destination group.

   NOTE: The rules are not applied to devices in **Enrollment Pending** state.

Edit an unmanaged device auto assignment rule

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Select the rule, and click the **Edit** option.
4. Enter the **Name**, and select the **Destination group**.
5. Click the **Add Condition** option, and select the conditions for assigned rules.
6. Click **Save**.

Disable and delete rule for the unmanaged device auto assignment

Steps

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

Save the rule order

Prerequisites

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

Steps

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**.

   NOTE: You cannot change the IPV6 Prefix rule order.

Add a rule for alert notification

Steps

1. Click the **Rules** tab.
2. Select the **Alert Notification** option.
3. Click **Add Rule**.
   An **Add Rule** window is displayed.
4. From the **Rule** drop-down list, select a rule.
5. Enter the **Description**.
6. From the **Group** drop-down list, select the preferred option.
7. From the drop-down menu, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.
8. Click **Save**.

Edit an alert notification rule

Steps

1. Click the **Rules** tab.
2. Select the **Alert Notification** option.
3. Click **Edit Rule**.
   An **Edit Rule** window is displayed.
4. From the **Rule** drop-down list, select a rule.
5. Enter the **Description**.
6. From the **Groups** drop-down list, select a group.
7. From the drop-down list, select a target device to apply **Notification Target** and the time duration to apply **Notification Frequency**.
8. Click **Save**.

Create rule to auto-unregister a device

From Wyse Management Suite 3.2, you can create a rule to auto-unregister a device if it does not check-in with Wyse Management Suite for a period of time.

Steps

1. Click the **Rules** tab.
2. Click the **Failed Check-In** option.

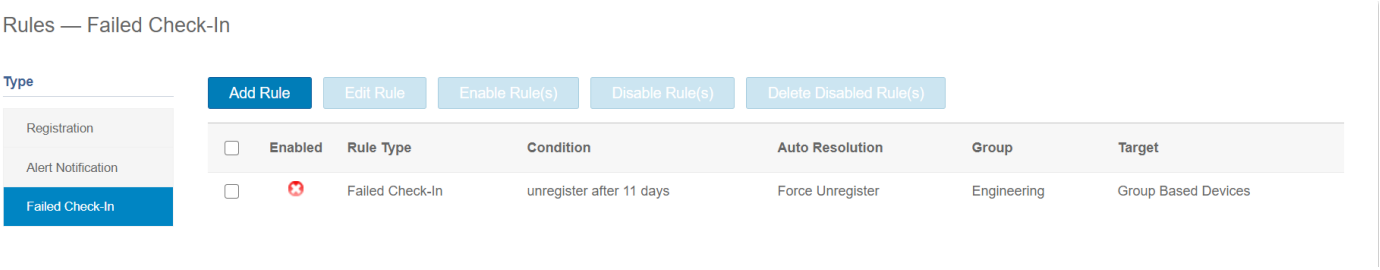


Figure 10. Failed Check-In tab

3. Click **Add Rule**.
   The **Add Rule** window is displayed.

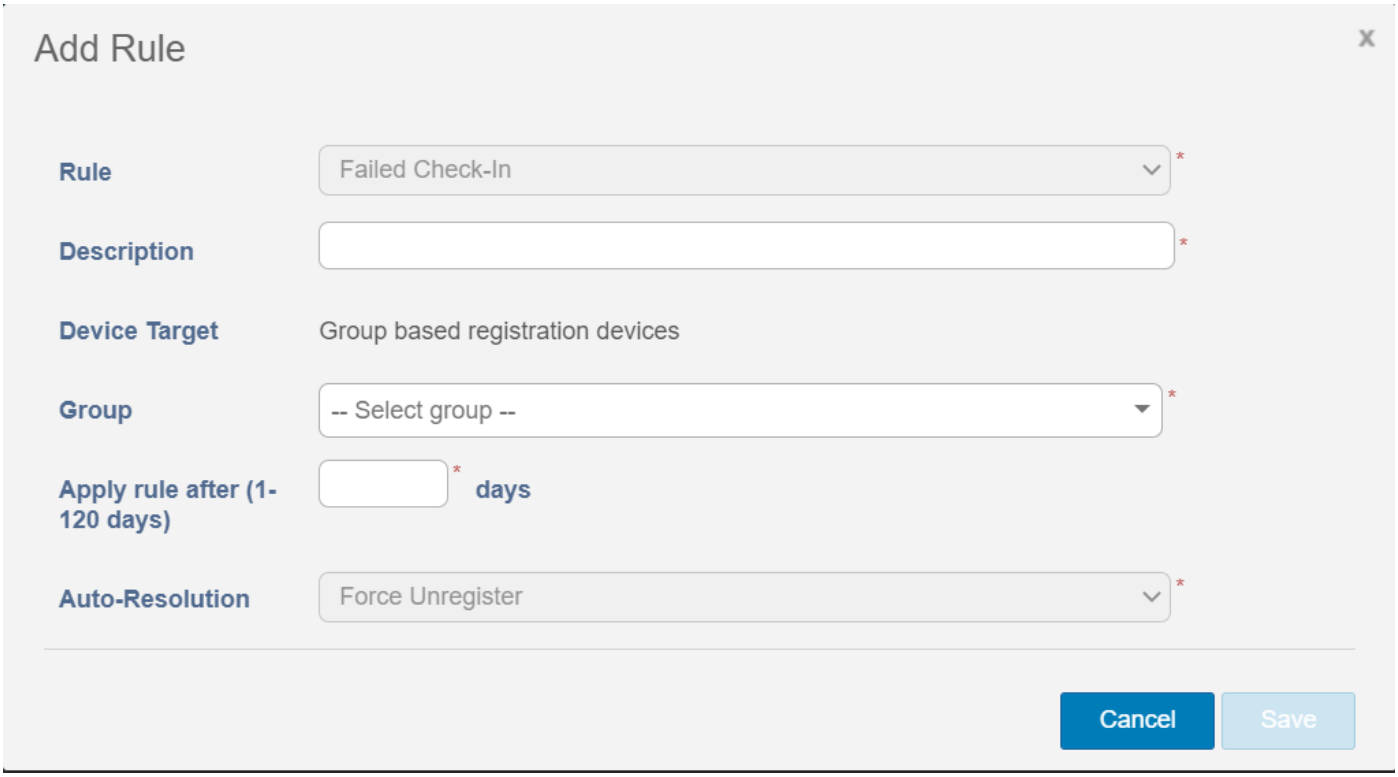


Figure 11. Add rule

4. Enter the description for the rule.
5. Select the group from which the devices must be unregistered.
6. In the **Apply rule after (1-120 days)** field, enter the duration in days after which the device is unregistered from Wyse Management Suite.

   NOTE: The device is unregistered from Wyse Management Suite only if the device does not check-in for the specified number of days.
7. Click **Save**.
   You can also edit, enable, disable, or delete the rule.

11

Managing Jobs

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

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
  - Hybrid Client
  - Generic Client
- **Status**—From the drop-down menu, select the status of the job. The available options are:
  - Scheduled
  - Running/In Progress
  - Completed
  - Canceled
  - 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 canceled
  - 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.

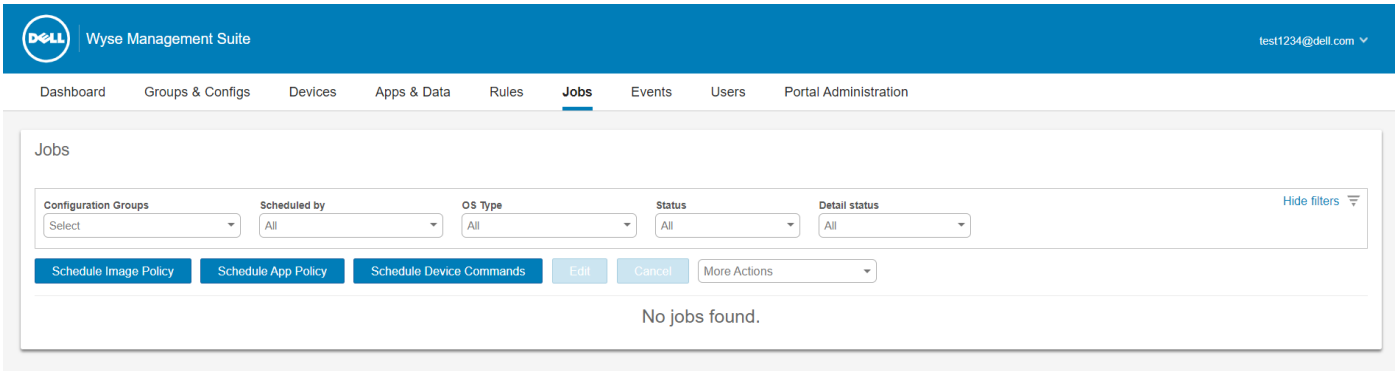


Figure 12. Jobs page

Topics:

Sync BIOS admin password

Steps

1. Click **Jobs**.
   The **Jobs** page is displayed.
2. From the **More Actions** drop-down menu, select the **Sync BIOS Admin Password** option.
   The **Sync BIOS Admin Password Job** window is displayed.
3. Enter the password. The password must be a minimum of 4 and a maximum of 32 characters.
4. Select the **Show Password** check box to view the password.
5. From the **OS Type** drop-down menu, select your preferred option.
6. From the **Platform** drop-down menu, select your preferred option.
7. Enter the name of the job.
8. From the **Group** drop-down menu, select your preferred option.
9. Select the **Include All Subgroup** check box to include the subgroups.
10. Enter the description in the **Description** box.
11. Click **Preview**.

Search a scheduled job by using filters

This section describes how to search a scheduled job and manage the jobs in the management console.

Steps

1. Click **Jobs**.
   The **Jobs** page is displayed.
2. From the **Configuration Groups** drop-down menu, select either the default policy group or the groups which are added by an administrator.
3. From the **Scheduled by** drop-down menu, select a scheduler who performs the scheduling activity.
   The available options are:
   - Admin
     - App Policy
     - Image Policy
     - Device Commands
   - System
     - Publish Group Configuration
     - Others
4. From the **OS Type** drop-down menu, select the operating system.
   The available options are:
   - ThinOS
   - WES
   - Linux
   - Thin Linux
   - Wyse Software Thin Client
   - Teradici-Private cloud

- Dell Hybrid Client

5. From the **Status** drop-down menu, select the status of the job.
   The available options are:
   - Scheduled
   - Running/In Progress
   - Completed
   - Canceled
   - Failed
6. From the **Detail Status** drop-down menu, select the status in detail.
   The available options are:
   - 1 or more failed
   - 1 or more pending
   - 1 or more In progress
   - 1 or more canceled
   - 1 or more completed
7. From the **More Actions** drop-down menu, select the **Sync BIOS Admin Password** option.
   The **Sync BIOS Admin Password Job** window is displayed. For more information, see Sync BIOS admin password.

Schedule a device command job

Steps

1. On the **Jobs** page, click **Schedule device command job**.
   The **Device Command Job** screen is displayed.
2. Configure the following options:
   a. From the **Command** drop-down list, select a command. The available options are:
      - Restart
      - Wake on LAN
      - Shutdown
      - Query
      - Reimage
      - Lock—Applicable for ThinOS 8.x and ThinOS 9.x devices
      - Send message—Applicable for Windows Embedded, ThinLinux, ThinOS 8.x, ThinOS 9.x, and Dell Hybrid Client powered devices
      - Factory Reset—Applicable for ThinOS 8.x, ThinOS 9.x, and Dell Hybrid Client powered devices

      The 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.
   b. From the **OS Type** drop-down list, select the type of operating system.
   c. In the **Name** field, Enter the name of the job.
   d. From the **Group** drop-down list, select a group name.
   e. Enter the job description.
   f. From the **Run** drop-down list, select the date or time.
   g. Enter or 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.
3. Click the **Preview** option to view the details of the scheduled job.
4. On the next page, click the **Schedule** option to initiate the job.

Schedule the image policy

Image policy is not a recurring job. Each command is specific to a device.

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.

Schedule an application policy

Application policy is not a recurring job. Each command is specific to a device.

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.

Restart a failed job

From Wyse Management Suite 3.2, you can restart a failed job of device commands, application policy, and image policy. You can also create a schedule for the failed job. This option is applicable only for Wyse Management Suite with a pro license.

Prerequisites

- Job should be scheduled and should have failed.
- The scheduled job should be device command, application policy, or an image policy.

Steps

1. Click the **Jobs** tab.
2. Select the failed job and click **Restart Failed Job**.
   The status of the job is changed to **Restarted**.
3. From the **Run** drop-down list, schedule the job.
4. Click the **Preview** option to view the details of the scheduled job.
5. On the next page, click the **Schedule** option to initiate the job.

NOTE: The global administrator, user with a custom role (if job permissions are assigned), or a group administrator for specific group can restart a failed job.

NOTE: You can only restart a failed job once, since a new child job is created for the failed one.

12

Managing Events

In the **Events** page, you can view all events and alerts in the management system using the management console. It also provides instructions on viewing an audit of events and alerts for system auditing purposes.

A summary of events and alerts is used to obtain an easy-to-read daily summary of what has happened in the system. The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

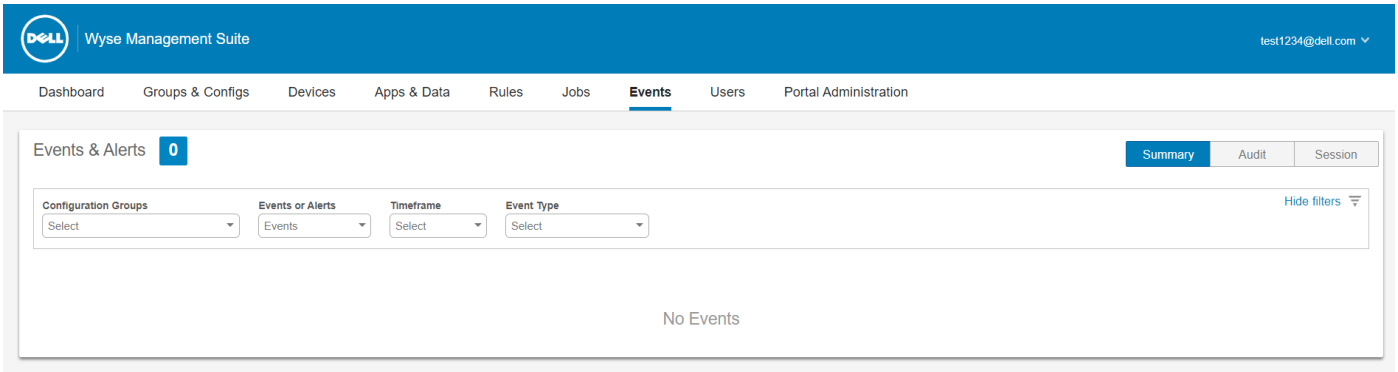


Figure 13. Events page

Topics:

- Search an event or alert using filters
- View the summary of events
- View the audit log
- End user session reporting

Search an event or alert using filters

Steps

1. Click **Events**.
   The **Events** page is displayed.
2. From the **Configuration Groups** drop-down menu, select either the default policy group or the groups which are added by an administrator.
3. From the **Events or Alerts** drop-down menu, select any one of the following options:
   - Events
   - Current Alerts
   - Alert History
4. From the **Timeframe** drop-down menu, select any one of the following operating systems:
   This option enables you to view the events which occurred in a particular timeframe. The available options in the drop-down menu are:
   - Today
   - Yesterday
   - This Week
   - Custom
5. From the **Event Type** drop-down menu, select the operating system.
   All the events are classified under particular groups. The available options in the drop-down menu are:
   - Access

- Registration
- Configuration
- Remote Commands
- Management
- Compliance

View the summary of events

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

View the audit log

The **Audit** window arranges the information into a typical audit log-view. You can view the timestamp, event type, source, and description of each event in the order of time.

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.

   NOTE: The audit files are not translated and are available only in English.

End user session reporting

You can use the end user session reporting option to report the user session during different time intervals.

Prerequisites

The **Enable Session Reporting** option must be enabled. For more information, see Configure Wyse Management Suite client settings for Dell Hybrid Client.

Steps

1. Click **Events**.
   The **Events** page is displayed.
2. Click **Session**.
   The **End Users Session** page is displayed.
3. From the **Timeframe** drop-down menu, select an option to view the events. The available options in the drop-down menu are:
   - Today
   - Yesterday
   - This Week
   - Custom

13

Managing users

This section describes how to perform a routine user management task in the management console. The following are the three 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)

- **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:
  - Add user
  - Edit User
  - Activate User(s)
  - Deactivate User(s)
  - Delete User(s)

- **End Users**—You can add individual users to Wyse Management Suite using the **End Users** tab. You can configure and deploy settings to an individual user. The settings are applied to the user account and are applied to the thin client when the user logs in. This option is applicable only to thin clients running the ThinOS 9.x operating system and Dell Hybrid Clients.

NOTE: You can bulk import users only from the .CSV file. You cannot bulk import end users from an Active Directory.

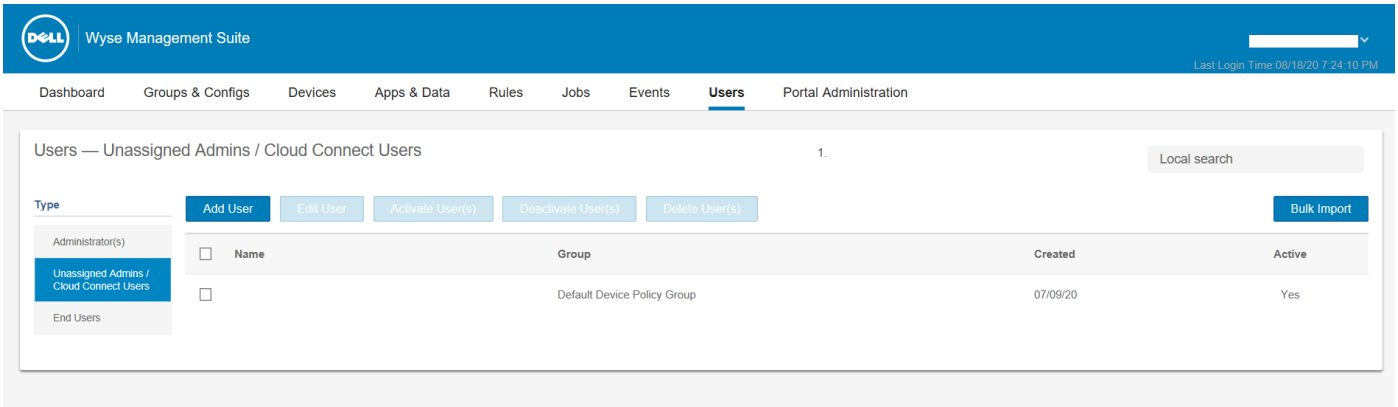


Figure 14. Users page

Topics:

- Add a new admin profile
- Create a WMS custom role in Wyse Management Suite

- Assign WMS custom roles to imported AD groups
- Bulk import unassigned administrators or cloud connect users
- Edit an administrator profile
- Activate an administrator profile
- Deactivate an administrator profile
- Delete an administrator profile
- Unlock an administrator profile
- Deactivate an administrator profile
- Create auto assignment rules for unmanaged devices
- Add end user
- Edit an end user
- Configure end user policy
- Bulk import end users
- Deleting end user
- Edit a user profile

Add a new admin profile

Steps

1. Click **Users**.
2. Click **Administrator(s)**.
3. Click **Add Admin**.
   The **New Admin User** window is displayed.
4. Enter your email ID and user name in the respective fields.
5. Select the check box to use the same user name as mentioned in the email.
6. Do one of the following:
   - If you click the **Personal Information** tab, enter the following details:
     - First name
     - Last name
     - Title
     - Mobile phone number
   - If you click the **Roles** tab, enter the following details:
     a. In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
        - Global Administrator
        - Group Administrator
        - Viewer

          NOTE: If you select the **Administrator role** as **Viewer**, the following administrative tasks are displayed:
          - Query Device
          - Unregister Device
          - Restart/Shutdown Device
          - Change Group Assignment
          - Remote Shadow
          - Lock Device
          - Wipe Device
          - Send Message
          - WOL Device

     b. In the **Password** section, enter the custom password. To generate a random password, select the **Generate random password** radio button.
7. Click **Save**.

Create a WMS custom role in Wyse Management Suite

Using Wyse Management Suite 3.1 or later versions, a global administrator can create a new administrator role and provide granular permissions for different functionalities of Wyse Management Suite. You can create multiple users using the Custom Global Administrator role.

Steps

1. Go to the **Users** tab.
2. Click **Administrator(s)**.
3. Click **Add Admin**.
   The **New Admin User** window is displayed.
4. Enter the email ID and username in the respective fields.
5. Click **Roles**.
6. From the **Role** drop-down list, select **Custom WMS Role**.
7. Under each category, select the appropriate function that the user is allowed to perform.
8. Click **Save**.
   The following table provides details about the supported and unsupported permissions that can be assigned to a custom role:

Table 10. Permissions for a custom role

Supported	Not supported
Edit or Remove Configuration	Bulk Device Exception
Add, Edit, Delete Groups	Create of Group Admin
Upload Reference files	Creation of Global Admin
Create device detail exception	Creation of Viewer Admin
Rules	Assigning Role to un-assigned Administrators
Apps and data	Subscription (Export and Import license)
Bulk import End users	Changing WMS server URL
Manage Remote Repository	Changing MQTT URL
Reports	Uploading Config UI
Others	Custom Branding
Active Directory on Portal Admin Page	

Assign WMS custom roles to imported AD groups

From Wyse Management Suite 3.2, you can assign roles to groups imported from the active directory. The permission assigned to the group is applied to all users of the group.

Steps

1. Log in as a global administrator.
2. Go to **Portal Administration** > **Active Directory** > **One Time Import** and enter the credentials.
   All the groups of the domain are listed in the left pane.
3. Select the groups that you want to import.
   The selected groups are moved to the right pane of the page.
4. Select the **Assign Roles** check box to import the groups for group role assignment.

NOTE: If the **Assign Roles** option is not selected, then the group is added to the Default User Policy group and can be viewed from the **Groups** page.

5. Click **Import Groups**.
   The groups are imported and assigned default roles.
6. Go to the **Users** tab and click **Group Assignment**.

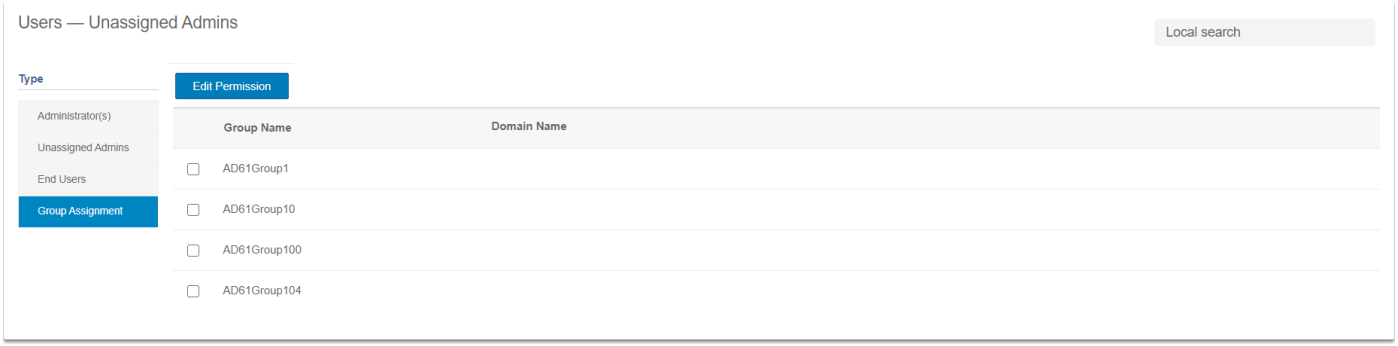


Figure 15. Group Assignment

The imported groups are listed in the **Group Assignment** tab.

7. Select the group that you want to assign roles and click **Edit Permissions**.
   The **Roles** window is displayed.
8. Select the role that you want to assign from the drop-down list and click **Save**.

NOTE: If a user is already assigned roles using the group role assignment, go to **Users** > **Administrator(s)** and edit the permissions of individual users or subgroups. These permissions take precedence over the group role assignment.

NOTE: For public cloud, you can assign WMS custom roles using Wyse Management Suite repository version 3.2.

NOTE: To log in with a domain user, you must first import groups and then the users. You can then assign roles to the groups using the Group Assignment tab.

NOTE: If you want to import users, the user details must have a first name, last name and an email configured in the Active Directory. These users are listed in the **Unassigned Admins** tab.

NOTE: You can add only one domain controller. When you import multiple domain, the users cannot log in to the server.

Bulk import unassigned administrators or cloud connect users

Steps

1. Click **Users**.
   The **Users** page is displayed.
2. Select the **Unassigned Admins** option.
3. Click **Bulk Import**.
   The **Bulk Import** window is displayed.
4. Click **Browse** and select the CSV file.
5. Select the user group to which the imported users must be assigned.
6. Click **Import**.

Edit an administrator profile

Steps

1. Click **Users**.
2. Click **Administrator(s)**.
3. Click **Edit Admin**.
   The **Edit Admin User** window is displayed.
4. Enter your email ID and user name in the respective fields.

   NOTE: When you update the login name, you are forced to log out from the console. Log in to the console using the updated account login name.

5. Do one of the following:
   - If you click the **Personal Information** tab, enter the following details:
     - First name
     - Last name
     - Title
     - Mobile phone number
   - If you click the **Roles** tab, enter the following details:
     a. In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
     b. In the **Password** section, enter the custom password. To generate a random password, select the **Generate random password** radio button.
6. Click **Save**.

Activate an administrator profile

Steps

1. Click **Users**.
2. Click **Administrator(s)**.
3. Select the administrators that you want to activate.
4. Click **Activate Admin**.

Deactivate an administrator profile

Deactivating the admin profile prevents you from logging in to the console, and removes your account from the registered devices list.

Steps

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

Delete an administrator profile

About this task

Administrator must be deactivated before you delete them. To delete an administrator profile, do the following:

Steps

1. Click **Users**.
2. Click **Administrator(s)**.
3. Select the check box of a particular admin or admins which you want to delete.
4. Click **Delete Admin(s)**.
   An **Alert** window is displayed.
5. Enter a reason for the deletion to enable the **Delete** link.
6. Click **Delete**.

Unlock an administrator profile

Steps

1. Click **Users**.
2. Click **Administrator(s)**.
3. Select the administrators that you want to unlock.
4. Click **Unlock Admin(s)**.

Deactivate an administrator profile

Steps

1. Click **Users**.
2. Click **Administrator(s)**.
3. Select the administrators that you want to deactivate.
4. Click **Dectivate Admin(s)**.

Create auto assignment rules for unmanaged devices

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Click the **Add Rules** tab.
4. Enter the **Name** and select the **Destination group**.
5. Click the **Add Condition** option and select the conditions for assigned rules.
6. Click **Save**.
   The rule is displayed in the unmanaged group list. This rule is applied automatically and the device is listed in the destination group.

Add end user

Steps

1. Click the **Users** tab.
2. Click **End Users**.
3. Click **Add User**.
4. Enter the username, domain, first name, last name, email address, title, and phone number
5. Click **Save**.

Edit an end user

Steps

1. Click the **Users** tab.
2. Click **End Users**.
3. Click **Edit End Users**.
4. Enter your email ID and user name in the respective fields.
5. Click **Save**.

Configure end user policy

You can configure and deploy settings to an individual user. The settings are applied to the user account and are applied to the thin client when the user logs in. This option is applicable only to thin clients running the ThinOS 9.x operating system and Dell Hybrid Clients.

Steps

1. Click the **Users** tab.
2. Click **End Users**.
3. Select a user.
   The **End User Details** page is displayed.
4. Click the **Edit Policies** drop-down menu and select the operating system.
5. Configure the required policies and click **Save and Publish**.

   NOTE: There is no limit on the number of users in an on-premise environment. You can add 10,000 users in a public cloud environment.

Bulk import end users

Steps

1. Click the **Users** tab.
2. Click **End Users**.
3. Click **Bulk Import**.
4. Click **Browse**, and select the .csv file.
5. Select the **CSV file has header line** option if the .csv file contains a header.
6. From the **Choose a user group** drop-down list, select the user group to which you want to add the users.
7. Click **Import**.

   NOTE: You can add up to 100 users per file to Wyse Management Suite and the file size of the .csv file should not exceed 150 KB.

   NOTE: You can add a maximum of 10,000 users in public cloud. There is no limit on the number of users that can be added in a private cloud.

Deleting end user

Steps

1. Click **End Users** tab.
2. Click **Delete End User**.
   An Alert window is displayed. Enter a reason for the deletion to enable the Delete link.

3. Click **Delete**.

Edit a user profile

Steps

1. Click **Users**.
2. Click **Unassigned Admins**.
3. Click **Edit User**.
   The **Edit Admin User** window is displayed.
4. Enter your email ID and user name in the respective fields.

   NOTE: When you update the login name, you are forced to log out from the console. Log in to the console using the updated account login name.

5. Do one of the following:
   - Click the **Personal Information** tab and enter the following details:
     - First name
     - Last name
     - Title
     - Mobile phone number
   - Click the **Roles** tab and enter the following details:
     a. In the **Roles** section, from the **Role** drop down list, select the **Administrator role**.
     b. In the **Password** section, enter the custom password. To generate a random password, select the **Generate random password** radio button.
6. Click **Save**.

14

Portal administration

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

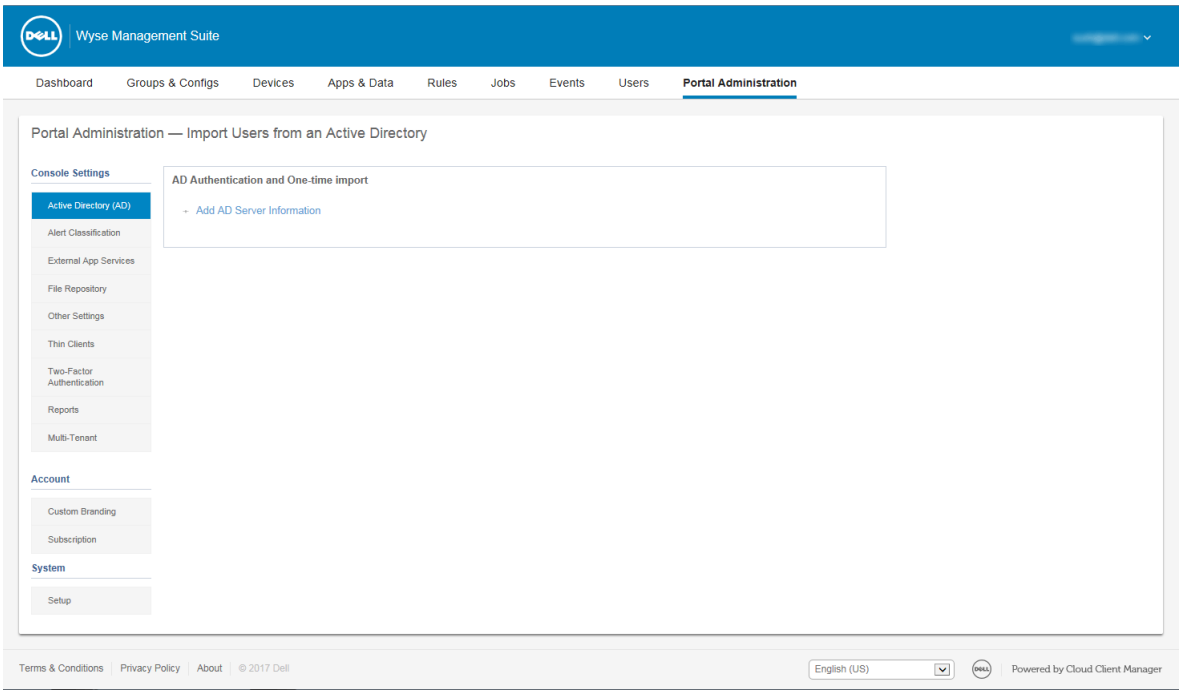


Figure 16. Portal admin

Topics:

- Import unassigned users or user groups to public cloud through active directory
- Adding the Active Directory server information
- Alert classifications
- Create an Application Programming Interface-API accounts
- Access Wyse Management Suite file repository
- Configuring other settings
- Managing Teradici configurations
- Enable Two-Factor authentication
- Enabling multi-tenant accounts
- Generate reports
- Enabling custom branding
- Manage system setup
- Configure secure MQTT
- Enable secure LDAP over SSL

Import unassigned users or user groups to public cloud through active directory

Steps

1. Download and install the file repository, see Accessing file repository. The repository must be installed by using the company network and must have the access to the AD server to pull the users.
2. Register the repository to public cloud. Once registered, follow the steps mentioned on the UI to import the users to Wyse Management Suite public cloud. You can edit the roles of the AD user after importing to Wyse Management Suite public cloud.
3. Set up ADFS on public cloud.

Adding the Active Directory server information

You can import Active Directory users and user groups to the Wyse Management Suite private cloud.

Steps

1. Log in to the Wyse Management Suite private cloud.
2. Go 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**.
   If you connect using LDAP port 389, a warning message is displayed to enable secure LDAP. To configure and enable secure LDAP over SSL, see Enable secure LDAP over SSL.
5. Click **Save**.
6. Click **Import**.
7. Enter the username and password.

   NOTE: To search groups and users, you can filter them based on **Search Base**, and **Group name contains** options. You can enter the values as following:

   - `OU=<OU Name>`.

     For example, `OU=TestOU`.

   - `DC=<Child Domain>, DC=<Parent Domain>, DC=com,`.

     For example, `DC=Skynet, DC=Alpha, DC=Com`.

   You can enter a space after a comma, but you cannot use single or double quotes.

8. Click **Login**.
9. On the **User Group** page, click **Group name** and enter the group name.
10. In the **Search** field, type the group name that you want to select.
11. Select a group.
    The selected group is moved to the right pane.
12. In the **User Name Contents field**, enter the user name .
13. Click **Import Users** or **Import Groups**.

    The entries are skipped and cannot be imported into Wyse Management Suite during the user import process in the following scenarios:

    - If you provide an invalid name
    - If you do not provide a last name
    - If you provide an email address as name

    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**. The confirmation messages also displays where the groups are imported.
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.

NOTE: To close the **AD Authentication and One-time Import** page during the configuration, click **AD LogOut** option.

NOTE: To log in as a domain user after you import groups, the administrator must import group users using the Unassigned Users tab under Users tab. You cannot sign in with domain users without importing group users if the administrator imports only groups and assign role to groups only.

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**.

To log in to the Wyse Management Suite portal using child domain credentials, 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. Click **Change user domain**.
4. Enter the user credentials and the complete domain name.
5. Click **Sign In**.

The imported Active Directory users can be activated or deactivated on the **Users** page by using the global administrator login. If your account is deactivated, you cannot log in to the Wyse Management Suite Management portal.

NOTE: To configure and enable secure LDAP over SSL, see Enable secure LDAP over SSL.

Configuring Active Directory Federation Services feature on public cloud

You can configure Active Directory Federation Services (ADFS) on a public cloud.

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 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 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 that is 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 that are 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. To import a user to the public cloud , remote repository must be installed. For more information about the ADFS documentation, go to Technet.microsoft.com.

Results

After the ADFS test connection is successful, import the users using AD connector present in the remote repository.

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

Create an Application Programming Interface-API accounts

About this task

This section allows you to create secured Application Programming Interface (API) accounts. This service provides the ability to create special accounts. To configure the external application service, do the following:

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**.

Access Wyse Management Suite file repository

File repositories are places where **files** are stored and organized. Wyse Management Suite has two types of repositories:

- **Local Repository**—During the Wyse Management Suite private cloud installation, provide the local repository path in the Wyse Management Suite installer. After the installation, go to **Portal Admin** > **File Repository** and select the local repository. Click the **Edit** option to view and edit the repository settings.

- **Wyse Management Suite Repository**—Log in to Wyse Management Suite public cloud, go to ,**Portal Admin** > **File Repository** and download the Wyse Management Suite repository installer. After the installation, register the Wyse Management Suite repository to Wyse Management Suite Management server by providing the required information.

You can enable the **Automatic Replication** option to replicate files that are added to any of the file repositories to other repositories. When you enable this option, an alert message is displayed. You can select the **Replicate existing files** check box to replicate the existing files to your file repositories.

Replicate existing file option is applicable if the repository is already registered. When a new repository is registered, then all the files are copied to the new repository. You can view the file replication status in the **Events** page.

The `Image Pull` templates are not replicated automatically to other repositories. You must copy these files manually.

File Replication feature is supported only on repositories from Wyse Management Suite 2.0 and later versions.

You cannot import self-signed certificate of the remote repository to the Wyse Management Suite server. If the CA Validation is enabled for remote repository, then the replication of files from the remote repository to the local repository fails.

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.
9. From the drop-down list of **Concurrent File Downloads** option, select the number of files.
10. Enable or disable **Wake on LAN** option.
11. 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.
12. Select the **Certificate Validation** check box to enable the CA validation for public cloud.

    NOTE: When CA Validation from Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations such as, Apps and Data, Image Pull/Push is successful. If certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate Certificate Authority** under **Events** page. All the operations such as, Apps and Data, Image Pull/Push is not successful. Also, when CA Validation from Wyse Management Suite server is disabled, the communication from server and client happens in secure channel without Certificate Signature validation.
13. Add a note in the provided box.
14. Click **Save Settings** .

Subnet mapping

From Wyse Management Suite 2.0, you can assign a subnet to a file repository. You can associate a file repository up to 25 subnets or ranges. You can also prioritize the subnets that are associated with the repository.

You can deploy the BIOS packages using subnet mapping from Wyse Management Suite 2.1 .You can upload and deploy multiple firmware packages from the remote repository, tenant cloud repository, or operator cloud repository. This feature is applicable only on Wyse Management Suite Pro license.

Configure subnet mapping

Steps

1. Go to **Portal Administration** > **File Repositories**.

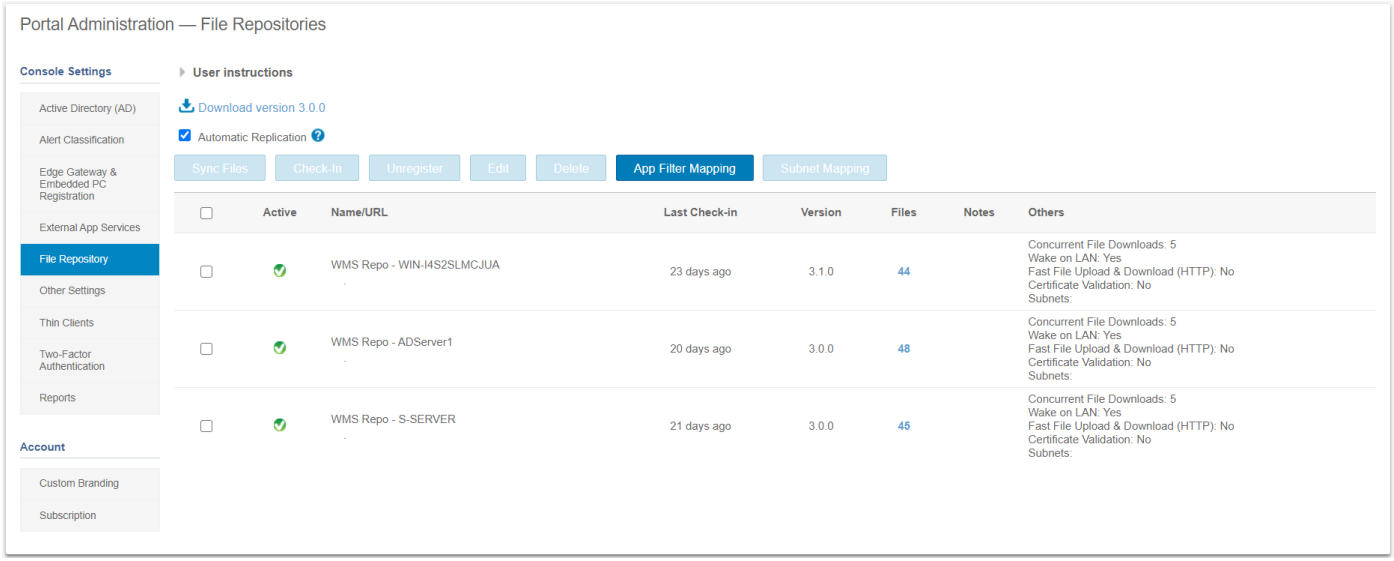


Figure 17. File repository

2. Select a file repository.
3. Click the **Subnet Mapping** option.
4. Enter subnets or ranges, one value per line. You must use hyphen for range separation.
5. Optionally, clear the **Allow devices from subnets not mapped to this file repository to download files from this repository as a fallback method using subnet proximity** check box if you want the file repository to be accessed only through the configured subnets or ranges.

   NOTE: The **Allow devices from subnets not mapped to this file repository to download files from this repository as a fallback method using subnet proximity** option is selected by default.

Configuring other settings

You can use the following settings to enforce the **APNS Warnings**, **License Expiration Warnings**, and other **Self Service Legal Agreements**.

- **Dismiss License Expiration Warning on Dashboard page**—Select this check box to disable the warning for a license expiration from displaying on the **Dashboard** page.
- **Enable License Expiration Notifications on Email**—Select this check box to enable license expiration email notifications. An email notification is sent to tenants before the license expires. This option is enabled by default. The email notification is sent when the license is expiring in:
  - 60 days
  - 30 days
  - 14 days
- **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 a heartbeat signal every 60 minutes to 360 minutes. The minimum interval is 5 minutes for private cloud.
- **Checkin interval**—Enter the time. The device sends full checking signal every 8 hours 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.
- **WMS Console timeout**—Enter the idle time in minutes after which the user is logged out of the console. This setting can be configured by any global administrator. The default value is 30 minutes.
- **Enrollment Validation**—When the **Enrollment Validation option** is enabled, the auto-discovered devices are in **Pending Validation** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page and validate the enrollment. The devices are moved to the intended group after they are validated.
- **Reset EULA Acceptance**—Select this check box if you want to reset **EULA Acceptance** page to show the wizard again during upload EULA Embedded firmware/packages upload for ThinOS 9.x.

- **WMS API**—Select this check-box to enable Wyse Management Suite API.

Enable Wyse Management Suite API

Wyse Management Suite server uses a proprietary API to serve request generated from the user interface components. User Interface created with java scripts which uses a rest like API call to get required data in JSON format. The JSON format is request-specific. You can retrieve the device details or perform actions from Wyse Management Suite server and integrate the server with your custom client such as service now.

Prerequisites

Pro license type is required to use the Wyse Management Suite APIs.

Steps

1. Log in as an administrator.
2. Go to **Portal Administration** > **Other Settings**.
3. Select the **Enable WMS API** check box.
4. Click **Save Settings**.

   For information about the supported APIs and the relevant documentation, see Wyse Management Suite APIs at https://api-marketplace.dell.com.

Managing Teradici configurations

To add a Teradici server, do the following:

Steps

1. In the **Portal Administration** tab, under **Console Settings**, click **Teradici**.
2. Click **Add Server**.
   The **Add Server** screen is displayed.
3. Enter the **Server Name**. The port number is automatically populated.
4. Select the **CA Validation** check box to enable CA validation.
5. Click **Test**.

Enable 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

1. Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.
2. Click **Two Factor Authentication** under **Console Settings**.
3. You must select the check box to enable the two factor authentication.

   NOTE: Administrators must verify the second authentication factor using one time passcodes to log in to the management portal.
4. You will receive a onetime passcode to your e-mail address. Enter the one time passcode.

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.

Enabling multi-tenant accounts

This section allows you to create tenant accounts which can be managed independently of one another. You can manage the organizations independently. Each account must have its own license key and can set up its own set of admin accounts, policies, operating system images, application, rules, alerts, and so on. The high level operator creates these organizations.

To enable multi tenant accounts, do the following:

1. Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.
2. Select **Multi-Tenant** under **Console Settings**.
3. Select the check box to enable multi-tenant option.
4. Enter the following details:
   - User name
   - Password
   - Confirm password
   - Email
5. Click **Save Settings**.

Generate reports

You can download reports of the jobs, devices, groups, events, alerts, and policies. The reports can be shared with the administrator if you want to troubleshoot the end points.

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.
4. From the **Groups** drop-down list, select the group.
5. Select the delimiter.
6. Click **Save**.

Enabling custom branding

About this task

This option allows you to add the name of your company and its logo or brand. You can upload your own header logo, favicon, add a header title, and change header colors to customize the Wyse Management Suite portal. To access and specify custom branding:

Steps

1. Go to **Portal Administrator** > **Account** > **Custom Branding**.
2. Click **Enable Custom Branding**.
3. In **Header Logo**, click **Browse** 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**.

Manage system setup

You can change the SMTP details, certificates, MQTT details, and external Wyse Management Suite URL details configured during the installation.

From Wyse Management Suite 2.1, the **Dynamic Schema Configuration** is supported for ThinOS 9.x devices that enables you to update the latest configuration settings without any changes on the server side. In public cloud, the Wyse Management Suite operator can upgrade the 9.x configuration user interface. For private cloud—pro feature only—the Global user can upgrade the 9.x configuration user interface. If the **Multi-Tenant** feature is enabled, the Wyse Management Suite operator can upload the latest schema from the **Administration** section,

Steps

1. Log in to the Wyse Management Suite portal and click the **Portal Admin** tab.
2. Click **Setup** under **Systems**.
3. Select the check box to perform server certificate validation for all device-to-server communication.
4. Enter the following details in the **Update SMTP for Email Alerts** area:
   - SMTP server
   - Send from address
   - Username
   - Password
   - Test address

   Current Certificate—Select the **Certificate Validation** check box to enable the CA validation for private cloud. All the communication from the server and the client including file download, operating system image download from Local Repo uses the certificate.

   NOTE: When CA Validation from Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations such as, Apps and Data, Image Pull/Push is successful. If certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate Certificate Authority** under **Events** page. All the operations such as, Apps and Data, Image Pull/Push is not successful. Also, when CA Validation from Wyse Management Suite server is disabled, then the communication from server and client happens in secure channel without Certificate Signature validation.
5. Select the following options and enter the details:
   - **Key/Certificate**—Upload HTTPS key/certificate file pair (only PEM format is supported).
   - **PKCS-12**—Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is required for IIS pfx.
6. To update the external MQTT details, click the **Change External MQTT** option and configure the details.
7. To update the external Wyse Management Suite URL, click the **Change External WMS URL** option and configure the details.

   NOTE: To revert to the previous configurations click the **Revert Last URLs** option, and the click **Save**.
8. If you want to upgrade the 9.x configuration user interface, click **Choose Files** in the **Configuration UI Package** field, and browse to the .zip file.

   NOTE: This option is not available, if the **Multi-Tenant** feature is enabled.
9. Click **Save**.

Configure secure MQTT

From Wyse Management Suite 3.2, you can configure secure MQTT connections for Windows 10 IoT Enterprise, Dell Hybrid clients, ThinOS 9.1 MR1 and remote repository.

Steps

1. Go to **Portal Administration** > **Systems** > **Setup**.
2. To configure secure MQTT, select **External Secure MQTT** from the **Preferred MQTT** drop-down list in the **WMS URLs** field.

   NOTE: Upgrade the system to 12 GB RAM as there is more memory requirement to enable secure communication.

NOTE: For a standard license, you can use secure MQTT connection (8443) by blocking the port 1883 from Wyse Management Suite server installed system using Windows Firewall.

Important information

Devices with older agents continue to communicate with non-secure port and the devices with new agents such as Windows Embedded device and Dell Hybrid Client powered device can communicate with the secure port.

Default selection for preferred MQTT is External MQTT—`tcp://<WMS URL>:1883`.

For public cloud, the default selection for preferred MQTT is External MQTT—`tcp://<WMS URL>:443`.

Any device registered to Wyse Management Suite public server connects to External MQTT. In case the remote port 1883 is blocked, then the agent connects back to the Secure MQTT server.

Preferred MQTT selection between External MQTT and External Secure MQTT is available only in Wyse Management Suite on-premise server. Based on the requirement, preferred MQTT can be updated to External Secure MQTT—`tls://<WMS URL>:8443`.

Any device with latest agent that supports secure MQTT connects to External Secure MQTT. The older agent that does not support secure MQTT continues to use External MQTT—`tcp://<WMS URL>:1883`.

Enable secure LDAP over SSL

Steps

1. Download, export, or create the SSL certificate as per the requirement

   NOTE: For information on how to create an SSL certificate, see *Enable LDAP over SSL with a third-party certification authority* at https://docs.microsoft.com/.

2. Log in to Wyse Management Suite.
3. Go to **Portal Administration** > **Setup** > **Trust Store certificates** and import the certificate.

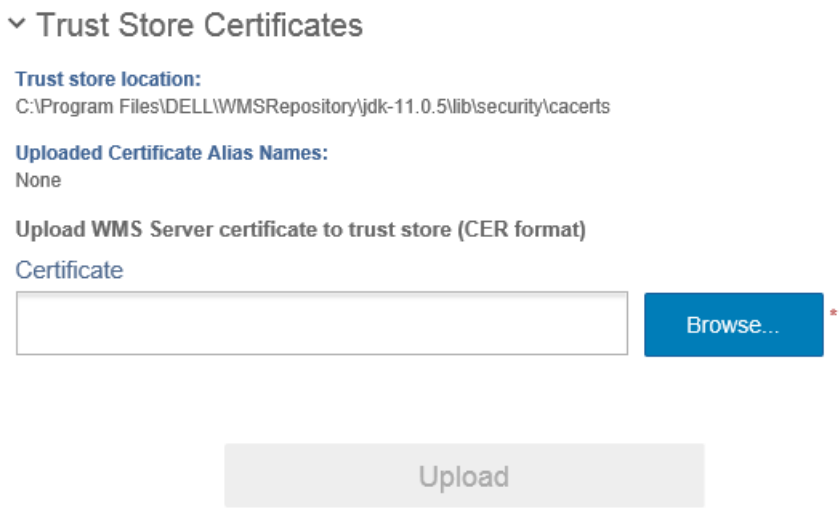


Figure 18. Trust Store Certificate

4. After the LDAP certificate is uploaded, you can click **Save** or **Save & Restart**.

   NOTE: You can also click **Cancel** to stop the upload process.

5. On your thin client, go to **Start** > **Services**, and restart **Dell WMS: Tomcat Service**.
6. Log in to Wyse Management Suite again.

7. Go to **Portal Administration** > **Actve Directory** > **AD Authentication & one time import**.
8. In the **Server URL** field, enter the LDAPS address.
9. In the **Port** field, enter the configured secure port. For example, 636 or 3269.
10. Click **Save**.
11. Enter the AD credentials and connect to the active directory.

    NOTE: After the on-premise installation, you can import the server certificate and configure secure LDAP by updating the certificate in the OOBE screen.

Next steps

- After the on-premise installation with a single tenant, go to **Portal Administration** > **Setup** to import the public key of the certificate to the trust store. For multi-tenant setup, go to **WMS Operator Administration** > **System Settings** > **LDAPS**. After the public key is imported, click **Save and Restart** and the Tomcat service is restarted.
- After you import the certificate using the OOBE screen, click **Restart Now** and Tomcat restarts automatically.

15

Convert Dell Wyse 5070 devices and Dell Ubuntu Generic Clients to Dell Hybrid Client

You can convert the Dell Wyse 5070 devices running Windows 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x, and ThinOS 8.6 to Dell Hybrid Client using Wyse Management Suite Pro 3.1 or later versions. You can also convert the Dell OptiPlex 7070 Ultra systems running Ubuntu 18.04 and Windows 10 to Dell Hybrid Client using Wyse Management Suite Pro 3.1 or later versions.

Topics:

Dell Wyse 5070 Conversion

Prerequisites

- If the Wyse 5070 device running either Windows 10 or ThinLinux 2.x does not have the latest boot agent which is equal or later than 4.0.8, download it from the Dell support site.
- If the Wyse 5070 device running ThinOS 8.6_511 does not have the latest boot agent which is equal or later than 4.0.8, download it from the Dell support site.
- If you are converting Windows 10 IoT Enterprise devices, download the Dell Hybrid Client image, DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_32GB.exe from the Dell support site.
- If you are converting ThinLinux 2.x or ThinOS 8.6 devices, download the Dell Hybrid Client image, DHC_Wyse_5070_Conversion_Merlin_Image_xxxx_16GB.exe from the Dell support site.
- Ensure that you use Wyse Management Suite Pro 3.1 or later version.
- Ensure that the number of Hybrid Client licenses is equal or more than the number of devices that need to be converted to Dell Hybrid Client. The Dell Hybrid Client licenses can be imported into Wyse Management Suite.
- If Wyse Management Suite is set up on a public cloud and you want to register the conversion image to a public cloud, the on-premise repository should be set up and configured locally. For more information, see Remote Repository.

About this task

The process of converting Windows 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x and ThinOS 8.6 to Dell Hybrid Client removes the contents and partition structure of the existing drive. The conversion process preserves only the certificates and settings relevant to register the device to Wyse Management Suite. All other data, certificates and configuration settings are not preserved. After the conversion to Dell Hybrid Client, it is not possible to convert the device back to the original state. However, you can restore the original operating system using the Dell Wyse USB Imaging Tool from the Dell support site. The existing data and settings are not restored.

Steps

1. Register the Dell Hybrid client image to Wyse Management Suite. For details about how to register, see Adding Hybrid Client images to repository.
   - If the storage size of the device is more than 16 GB, use DHC_CONVERSION_5070.exe.
   - If the storage size of the device is 16 GB, use DHC_CONVERSION_5070_16GB.exe.
2. Create the Dell Hybrid Client image policy. For details on how to create Hybrid Client image policy, see Creating Hybrid Client image policies.
3. Convert the device to Dell Hybrid Client. For details on how to schedule an image, see Scheduling the image policy.
   - The device receives an image update notification. The boot agent downloads the image from the Wyse Management Suite repository and installs the Dell Hybrid Client image by internally triggering the Dell Recovery Tool. After the imaging is completed, the device boots to Dell Hybrid Client.
   - Dell Client Agent registers the device, as Dell Hybrid Client to Wyse Management Suite.

- Wyse Management Suite manages the device as a Dell Hybrid Client device.

Adding Dell Hybrid Client images to repository

Steps

1. Copy the Dell Hybrid Client conversion image to the repository location or the operating system images folder using Wyse Management Suite.

   NOTE: Dell Technologies recommends to copy the image file to the local system and then copy the file to Wyse Management Suite repository location. Wyse Management Suite extracts the files from the zipped folder and uploads the files to the repository location or operating system images folder.

   The image is added to the repository.
2. Go to **Apps & Data** > **OS Image Repository** > **Hybrid Client** to view the saved image.

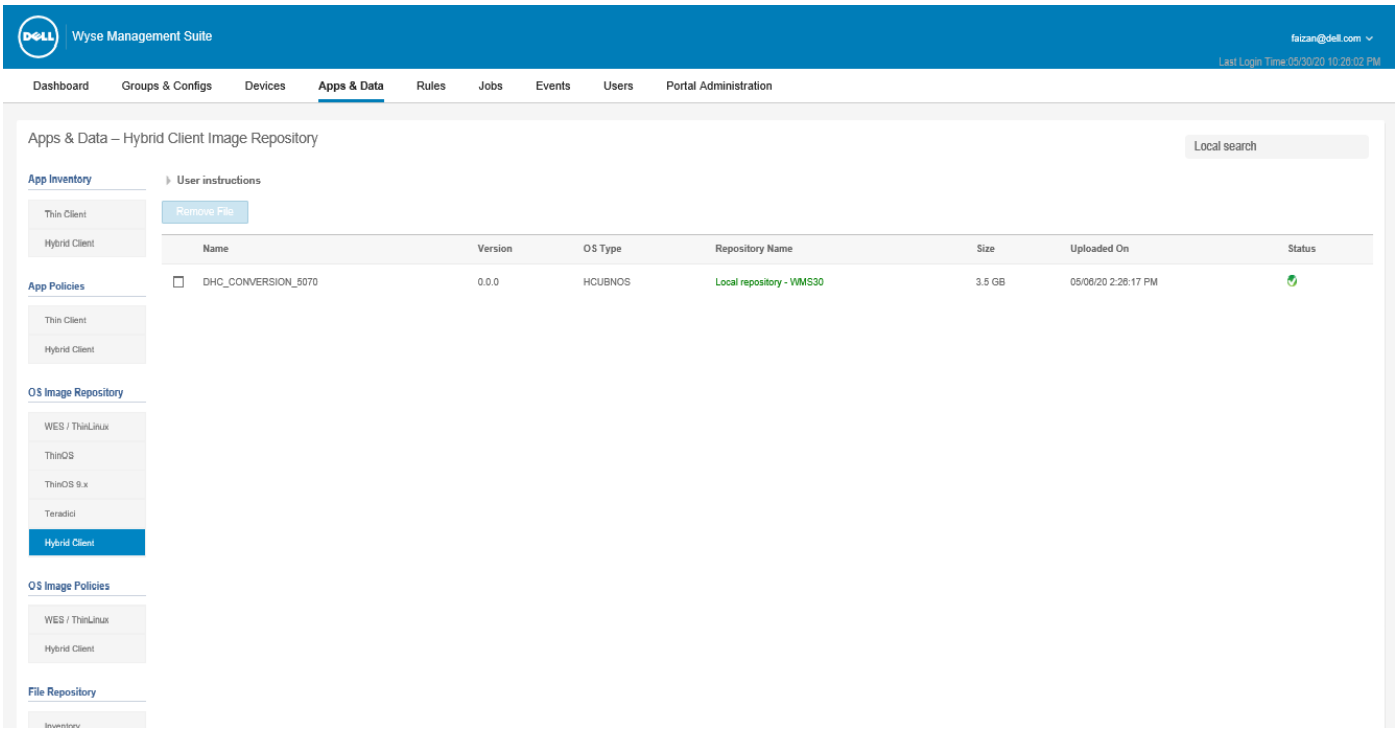


Figure 19. Adding Dell Hybrid Client images to repository

Creating Hybrid Client image policies

Steps

1. Go to **Apps & Data**, click **Hybrid Client** under **OS Image Policies**.
2. Click **Add Policy** and go to **Edit Hybrid Client Policy** tab.
3. Enter the **Policy name** and select a group from the drop-down menu of the **Group** tab.
4. Select the operating system type from the drop-down menu of the **OS Type** tab.
5. Select an operating system subtype filter from the drop-down menu of the **OS Subtype Filter** tab.

   NOTE: If you want to deploy an image to a specific operating system or platform, select either **OS Subtype Filter** or **Platform Filter**.
6. Select an image file from the drop-down menu of the **OS image** tab.
7. Select **Force this version** from the drop-down menu of the **Rule** tab.
8. Select one of the following option from the drop-down menu of the **Apply Policy Automatically** tab:

- **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.

9. Click **Save**.

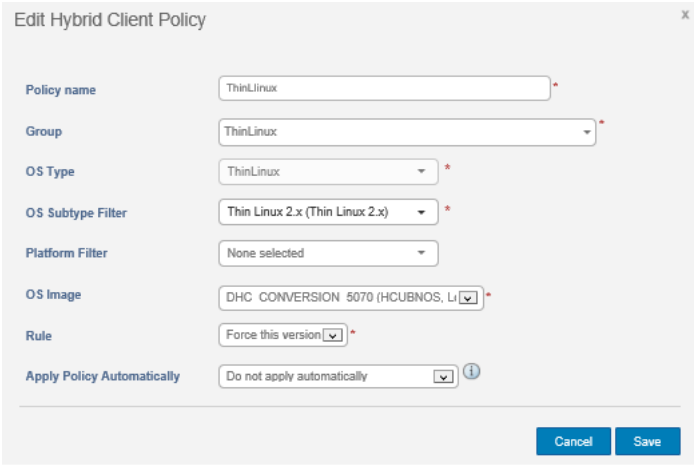


Figure 20. Creating Hybrid Client image policies

Scheduling the image policy

Steps

1. Go to **Jobs** and click the **Schedule Image Policy** tab.
   The **Image Update Job** tab is displayed.
2. Select a policy from the drop down menu of the **Policy** tab.
3. Enter the job description on the **Description** tab.
4. Select the date or time from the drop down list of the **Run** tab as following:
   - **Effective**— Enter the start and end date
   - **Start between**— Enter the start and end time
   - **On day(s)**— Select the days of the week
5. Click **Preview** to view details of the scheduled job.
6. Click **Schedule** to initiate the job.

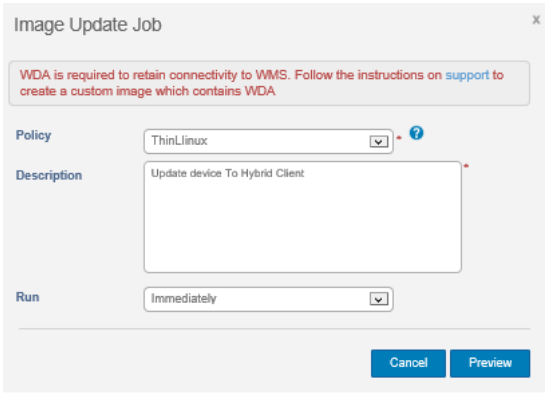


Figure 21. Schedule a job

Convert Dell Generic Client to Dell Hybrid Client

Prerequisites

- DCA-Enabler version 1.2 is required to convert Ubuntu 18.04 or 20.04 on Dell Ubuntu Generic device to Dell Hybrid Client. You can download the package from the **Drivers and Downloads** page atwww.dell.com/support.
- If DCA-Enabler version 1.0 or 1.1 is installed on your device, you must upgrade it to 1.2. To upgrade DCA-Enabler, you must register the device to Wyse Management Suite 3.2 and push the `DCA_Enabler_ Package 1.2.0-xx` to the device using Wyse Management Suite and then deploy `DCA-Enabler 1.2.0-xx`.
- If the device is not preloaded with the Dell Hybrid client bundle in the recovery partition, you must first deploy and install the DHC-Fish-Scripts package.

NOTE: If the DCA-Enabler version is 1.1.0-17 or lower, Dell Ubuntu devices are registered to Wyse Management Suite as Dell Hybrid Client. If the DCA-Enabler version is 1.2.0-xx or greater, the devices are registered as Dell Generic Client.

Steps

1. Register the device to Wyse Management Suite using DCA-Enabler version 1.2.
2. Convert the generic client to Hybrid Client using any of the following methods:
   - Using the command Convert to Hybrid Client—see Convert your Dell Generic Client to Hybrid Client.
   - Deploying the Dell Hybrid Client 1.1/1.5 Bundles or ISO Image files using the application policy—see Create and deploy standard application policy to Dell Generic Clients and Create and deploy advanced application policy to Dell Generic Clients.

   NOTE: Before the device conversion is initiated, DCA-Enabler backs-up Wyse Management Suite connection data and then triggers the Dell Hybrid Client ISO or installer bundle.

   The installer completes the conversion and device restarts automatically. After the conversion, the device boots into the converted Dell Hybrid Client operating system. Dell Client Agent reads the backed-up Wyse Management Suite connection data and registers to Wyse Management Suite server as a Dell Hybrid Client device.

Example

To convert Dell Generic Clients running Ubuntu 18.04 LTS:

- To Dell Hybrid Client 1.0 or 1.1, you must push the Dell Hybrid Client 1.0 or 1.1 bundle package files using the application policy.
- To Dell Hybrid Client 1.5, you must push the Dell Hybrid Client ISO package using the application policy. You must push the OS-image upgrade tool `os-upgrade_1.1-10_amd64.deb` package, and then push the Dell Hybrid Client 1.5 ISO package file.

To convert Dell Generic Clients running Ubuntu 20.04 LTS to Dell Hybrid Client 1.5, you must push the Dell Hybrid Client 1.5 bundle package files using the application policy.

16

Security configurations

This section describes the key security features of Wyse Management Suite and provides the procedures that are required to ensure data protection and appropriate access control.

Topics:

Support for configuring TLS versions in Wyse Management Suite installer

From Wyse Management Suite 3.0, the on-premise installer is improved to select the Transport Layer Security (TLS) version during the installation or upgrade of the Wyse Management Suite. The recommended version of Transport Layer Security is 1.2. Ensure that you select all the appropriate versions of TLS based on the device agent and the merlin image. Older versions of Windows Embedded System, Wyse Device Agent (versions below WDA_14.4.0.135_Unified), and 32-bit merlin image versions are only compatible with TLSv1.0. Also, the import tool is only compatible with TLSv1.0.

NOTE: You must select TLS 1.2 to configure Dell Hybrid Client 1.5.

Configure Active Directory Federation Services feature on public cloud

Prerequisites

- Notepad++ or any equivalent application must be installed on the server.
- ADFS must be installed on the server.

Steps

1. On the **Portal Admin** page, under **Console Settings**, click **Active Directory (AD)**.
2. Click **Download WMS xml file** in the **Provide WMS details to ADFS** section.
   `CCM_SP_Metadata.xml` file is downloaded.
3. Right-click the downloaded file and select **Edit with Notepad++**.
4. Copy the ID value from the file. For example, ccm-sq3.
5. Go to the ADFS setup console.
6. Right-click **Relay Party Trusts** and select **Add Relaying Party Trust**.
   Add Relaying Party Trust window is displayed.
7. Click **Start**.
   Select Data Source window is displayed.
8. Select the **Import data about the relaying party from the file** option and browse the downloaded `CCM_SP_Metadata.xml` file.
9. Click **Next**.
10. Enter the ID value (ccm-sq3) in the **Display name** field and click **Next**.
11. On the **Choose Access Control Policy** page, click **Next**.
12. On the **Ready to Add Trust** page, click **Next**.

13. Click **Close**.
    The created relay trust is listed in the **Relay Party Trust** console.
14. Log in to the Wyse Management Suite public cloud server.
15. Go to **Portal Administration** > **Active Directory** and click **Show WMS rules**.
16. Copy the content displayed in the **WMS Rules** window.
17. Go to the ADFS console, right-click the relay trust, and select **Edit Clam Issuance Policy**.
18. Click **Add Rule** in the **Issuance Transform Rules** tab.
19. Click **Ok**.
    The **Select Rule Template** window is displayed.
20. From the **Claim rule template** drop-down list, select the **Send Claims using a Custom Rule** option and click **Next**.
21. Click **Add Rule**.
22. Enter the **Claim Rule name** and paste the content that is copied in step 16 in the **Custom rule** field.
23. Click **Finish**.
24. Click **Apply** and then click **Ok**.
25. Go to **Portal Administration** > **Active Directory** and click **Add Configuration**.
26. 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`.
27. Click **Update Configuration**.
28. 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.
29. To validate the configuration information, click **Test ADFS Login**. This enables tenants to test their setup before saving.
30. Enter the ADFS credentials and click **Sign in**.
    After ADFS is configured, **Test Successful** message is displayed.
31. Import the AD Domain users from the remote repository to the Wyse Management Suite public cloud.
32. Go to the **Users** page and assign roles to the imported AD Domain users.
33. Go to the Wyse Management Suite public cloud portal and click the **Sign in with your domain credentials** link.
34. Enter the email address of the imported AD Domain user and click **Sign In**.
    You are redirected to Wyse Management Suite server after you log in to ADFS.

Configure secure LDAP or LDAPS setup

To request the Root certificate from the Active Directory Certificate Services and configure a secure LDAP or LDAPS setup, do the following:

Steps

1. Go to the Active Directory domain server.
2. Go to **Start** > **Run**.
3. Enter **mmc** and click **Ok**.
   The **Console1** window is displayed.
4. Go to **File** > **Add or Remove Snap-ins**.
5. Add the certificates to the local system and click **Ok**.
6. Expand the `Personal` folder in the left pane.
7. Right-click certificates and go to **All Tasks** > **Request New Certificate**.
   Certificate Enrollment window is displayed.
8. Click **Next**.
9. In the **Select Certificate Enrollment Policy** tab, click **Next**.
10. Select **Domain Controller** and click **Enroll**.
    The domain certificate is installed on your domain controller.
11. Click **Finish**.
    The certificate issued to your domain controller is displayed on your certificate page.
12. Right-click the certificate and export the certificate to your desktop.

13. Import the AD domain server certificate into Wyse Management Suite java key store manually to the Wyse Management Suite server setup. To import the certificate, do the following:
    a. Go to the server where Wyse Management Suite is installed.
    b. Open **Command Prompt** and run the command `<C:\Program Files\DELL\WMS\jdk-11.0.7\bin>keytool.exe> -importcert -alias <certificate name> -keystore "<C:\Program Files\Dell\WMS\jdk-11.0.7\lib\security\cacerts>" -storepass changeit -file "C:\<certificate name>`.
14. After the certificate is installed, restart the Wyse Management Suite Tomcat Service.
15. Log in to the Wyse Management Suite server.
16. Go to **Portal Administration** > **Active Directory (AD)**.
17. Click the **Add AD Server Information** link.
18. Enter the AD domain name.
19. Enter the server URL as **`ldaps://hostname.domain.com`**. For example, **`ldaps://WMS-DC97.WMSAD97.com`**.
20. Enter the port name as **`636`**.
21. Click **Save**.
22. Click **Import**.
23. Enter the username and password.
24. Click **Login**.
25. On the **User Group** page, click **Group name** and enter the group name.
26. In the **Search** field, type the group name that you want to select.
27. Select a group.
    The selected group is moved to the right pane of the page.
28. In the **User Name Contents field**, enter the username .
29. Click **Import Users** or **Import Groups**.
    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**.

Deprecated protocol

Server Message Block (SMB) protocol version 2.0 is deprecated.

17

Teradici device management

The Teradici device management section provides the information about managing and discovering the teradici divices. The teradici management console uses SDK's to support management, configuration for tera devices. This is applicable only for Wyse Management Suite private cloud with pro license type.

Topics:

Discovering Teradici devices

Prerequisites

- Install the latest version of Wyse Management Suite on Microsoft Windows 2012 Server or later versions. Threadx 5.x and 6.x devices works with the latest version of the operating system.
- Install and enable the **EMSDK** component.
- The FQDN of the Wyse Management Suite server must be available for **DHCP** or **DNS** configurations.
- `Cert.pem` must be placed in the default path `C:\Program Files\Dell\WMS\Teradici\EMSDK`. It is used to discover Threadx devices.

Security Level

Depending on an endpoint's configured security level, you may also need to provision endpoints with an EBM/EM certificate.

Endpoints configured for medium or high security must have a trusted certificate in their certificate store before they can connect to an EBM or EM. For some endpoints, certificates may be pre-loaded by the vendor as a factory default. Otherwise, you can manually upload certificates using an endpoint's AWI.

Endpoints that are configured for low security do not need an MC certificate in their trusted certificate stores if either of the following is true:

- They are using DHCP discovery or DNS discovery and the DHCP or DNS server has provisioned them with the EBM certificate's fingerprint.
- They are discovered using the manual discovery method.

Table 11. Certificate Requirements for Endpoints

Discovery Method	Low Security	Medium Security	High Security
DHCP/DNS discovery without EBM fingerprint provisioned	Certificate required	Certificate required	Not applicable
DHCP/DNS discovery with EBM fingerprint provisioned	Certificate not required	Certificate required	Not applicable
Discovery initiated by an endpoint configured for a high security environment	Not applicable	Not applicable	Certificate required
Manual discovery initiated by the MC	Certificate not required	Not applicable	Not applicable

Manual discovery from the client

1. Go to, `https://<clientIP>`.

2. Accept the certificate warning message.
3. Enter the administrator password (default password is Administrator) and login.
4. Go to, **upload** > **certificate**. Select the `Cert.pem`file from the default path and click **Upload**.
5. Go to **Configuration** > **Management**. Click the **clear management state** button to register the device to the new Management Server.
6. Set the **manager discovery mode** to manual
7. Enter the **Endpoint Bootstrap Manager URL** in the following format **wss://<IP Address of the WMS server>**

   NOTE: If EMSDK is installed with custom port then provide **Endpoint Bootstrap Manager URL** in the following format **wss://<IP Address:Custom port.**
8. Click **Apply**, and then click **Continue.**
9. The **management status** is displayed as Connected to the Endpoint server.

Adding the PCoIP endpoint vendor class to DHCP server

1. Log in to your DHCP server.
2. Right-click the DHCP server in the **SERVERS** pane, and select **DHCP Manager**.
3. Right-click the **IPv4** option, and then select **Define Vendor Classes**.
4. Click **Add** to add a new DHCP vendor class.
5. Enter the **PCoIP Endpoint** in the **Display name** field.
6. Enter the **PCoIP Endpoint** in the **ASCII** column as the Vendor ID.
7. Click **OK** to save the settings.

Configuring DHCP options

1. Right-click the **IPv4** option, and the select **Set Predefined Options**.
2. Select **PCoIP Endpoint** as the **Option** class, and then click **Add**.
3. In the **Option Type** dialog box, enter the name as **EBM URI**, data type as **String**, code as **10**, and description as **Endpoint Bootstrap Manager URI**, and then click **OK**.
4. Click **OK** to save the settings.
5. Expand the DHCP scope to which you want to apply the options.
6. Right-click the **Scope Options**, and then select **Configure Options**.
7. Click the **Advanced** tab, and then select the **PCoIP Endpoint** vendor class.
8. Select the **010 EBM URI** check box, and then enter a valid Management Console URI in the **String** field. Click **Apply**. This URI requires a secured WebSocket prefix, for example, `wss://<MC IP address>:[port number]`. 5172 is the MC's listening port . Entering this port number is an optional step.
9. Click **OK** to save the settings.
10. Select **PCoIP Endpoint** as the **Option** class, and then click **Add**.
11. In the **Option Type** dialog, enter the name as **EBM X.509 SHA-256 fingerprint**, data type as **String**, code as **11**, and the description as **EBM X.509 SHA-256 fingerprint**, and then click **OK**.
12. Expand the DHCP scope to which you want to apply the options.
13. Right-click the **Scope Options**, and then select **Configure Options**.
14. Click the **Advanced** tab, and then select the **PCoIP Endpoint** vendor class.
15. Select the **011 EBM X.509 SHA-256 fingerprint** check box, and paste the SHA-256 fingerprint.

16. Click **OK** to save the settings.
17. Go to the client web browser.
18. Go to **Configuration** > **Management**, and set the **manager discovery mode** to **Automatic**
19. The client is connected to the server which is mentioned in the DHCP server.

Creating the DNS SRV record

1. Log in to the **DNS server**.
2. Right-click the DNS server in the **SERVERS** pane, and the select **DNS Manager** from the context menu.
3. In **Forward Lookup Zones**, right-click the domain, and then select **Other New Records** from the context menu.
4. In the **Resource Record Type** dialog box, select **Service Location (SRV)** from the list, and click **Create Record**.
5. Set **Service** to **_pcoip-bootstrap**, protocol to **_tcp**, and **Port number** to **5172**, which is MC's default listening port. For **Host offering this service**, enter the MC's FQDN.

   NOTE: The MC's FQDN must be entered because the DNS specification does not allow an IP address in the SRV records.
6. Click **OK**.

Adding a DNS TXT record

1. In **Forward Lookup Zones**, right-click the domain, and then select **Other New Records** from the context menu.
2. In the **Resource Record Type** dialog box, select the **Text (TXT)** from the list, and then click **Create Record**.
3. Enter the following details:
   a. In the **Record name** field, enter the host name of the Wyse Management Suite server offering the service. The FQDN field is populated automatically. This should match the FQDN of the Wyse Management Suite server.
   b. In the **Text** field, enter **pcoip-bootstrap-cert=** and then paste the Wyse Management Suite server certificate SHA-256 fingerprint.
4. Click **OK**.
5. Go to the client web browser.
6. The client is connected to the Wyse Management Suite server which is mentioned in the DNS server.

Creating SHA-256 fingerprint

1. Start the Mozilla Firefox.
2. Navigate to **Options Advanced** Tab
3. Click **Certificates** to view the certificates.
4. Under **Certificate Manager** , click **Authorities**, and the click **Import**.
5. Browse the certificate, and the click **View**.
6. Copy the **SHA-256** fingerprint.

CIFS use case scenarios

The following use cases are supported in Wyse Management Suite:

- When you select **Wyse Management Suite** as **Setup Type** while installing Wyse Management Suite private cloud.

- CIFS configuration page is displayed. This page is required as we need to configure the shared folder.

  NOTE: The **Configure CIFS User Credentials** option is disabled by default.

- When you select **Teradici EMSDK** as **Setup Type** while installing Wyse Management Suite private cloud.
  - For CIFS credentials, you can use an existing account or create a new one.
- When you select both **Wyse Management Suite** and **Teradici EMSDK** as **Setup Type** while installing Wyse Management Suite private cloud.
  - CIFS configuration page is displayed. This page is required as we need to configure the shared folder.

    NOTE: The **Configure CIFS User Credentials** option is disabled by default.

  - For CIFS credentials, you can use an existing account or create a new one.
- When you install only EMSDK on a system which already has the EMSDK service installed.
  - If Teradici EMSDK is selected then a warning message is displayed when you click **Next** from the **Setup Type** page. The message is **The installer has detected that the Teradici EMSDK is already installed. The EMSDK will be updated if required**. No port number is required.
    - If **Configure CIFS User Credentials** option is selected (By default)
      1. Stop the service.
      2. Update the EMSDK service.
      3. Restart the service. It operates under the same pre-configured user.
    - If **Configure CIFS User Credentials** option is selected with **Use an existing user**option.
      1. Stop the service.
      2. Update the EMSDK service.
      3. Update the service log on user to the one selected.
      4. Restart the service. It operates under the same pre-configured user.
    - If **Configure CIFS User Credentials** option is selected with **Create a New User** option.
      1. Stop the service.
      2. Update the EMSDK service.
      3. Update the service log on user to the newly created user.
      4. Restart the service. It operates under the same pre-configured user.
- When you install both **Wyse Management Suite** and **Teradici EMSDK** on a system that has already the EMSDK service installed.
  - Same as **When you install only EMSDK on a system which already has the EMSDK service installed** except that the **Configure CIFS User Credentials** option is selected by default and greyed out. You must enter CIFS credentials.

18

Managing license subscription

This section enables 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 provides the following information:

- License Subscription
- License Orders
- License Usage—Registered Thin Client Devices
- Server Information
- Import License—Private cloud
- Export License for Private Cloud—Public cloud

Topics:

Import licenses from Wyse Management Suite public cloud

You can import licenses from Wyse Management Suite public cloud to Wyse Management Suite private cloud.

Steps

1. Log in to Wyse Management Suite Private Cloud console.
2. Go to **Portal Administration** > **Accounts** > **Subscription**.
3. Enter the Wyse Management Suite public cloud details:
   - Username
   - Password
   - Data center
   - Number of TC seats
   - Number of Edge Gateway and Embedded PC seats
   - Number of Wyse Software Thin Client seats
   - Number of Hybrid Client seats
   - Number of Generic Client seats/devices
4. Click **Import**.

   NOTE: Wyse Management Suite private cloud must be connected to Wyse Management Suite public cloud.

   NOTE: Total number of manageable Generic devices depends on the total number available seat(s) for Hybrid Client and Thin Client license.

Export licenses to Wyse Management Suite Private Cloud

You can export licenses to Wyse Management Suite Private Cloud from Wyse Management Suite public cloud.

Steps

1. Log in to Wyse Management Suite public cloud console.
2. Go to **Portal Administration** > **Accounts** > **Subscription**.
3. Enter the number of thin client seats that must be exported to Wyse Management Suite Private Cloud.
4. Click **Export**.
5. Copy the generated license key.
6. Log in to Wyse Management Suite Private Cloud console.
7. Go to **Portal Administration** > **Accounts** > **Subscription**.
8. Enter the generated license key in the box.
9. Click **Import**.

Thin client licenses allocation

You can allocate the thin client licenses between Wyse Management Suite Private Cloud and Wyse Management Suite Public Cloud account.

Steps

1. Log in to the Wyse Management Suite Public Cloud console.
2. Go to **Portal Administration** > **Accounts** > **Subscription**.
3. Enter the number of thin client seats.

   NOTE: The thin client seats should be manageable in the Public Cloud. The entered number of thin client seats must not exceed the number displayed in **Manageable** option.

4. Click **Export**.

   NOTE: The number of Public Cloud licenses is adjusted based on the number of thin client seats exported to the Private Cloud.

5. Copy the generated license key.
6. Log in to Wyse Management Suite Private Cloud console.
7. Go to **Portal Administration** > **Accounts** > **Subscription**.
8. Import the exported license key to the Private Cloud.

   NOTE: The license cannot be imported if it has insufficient thin client seats to manage the number of devices currently being managed in the Private Cloud. In this case repeat steps 3–8 to allocate the thin client seats.

   NOTE: From Wyse Management Suite 3.2, older Wyse Management Suite server cannot be activated online from public cloud.

License orders

In public cloud, the **License Orders** section displays the list of placed orders including the expired licenses. By default, expired orders are not displayed. Select the **Include expired orders** check box to view the expired orders. The expired orders are displayed in red color, and the orders which expire in 30 days or less are displayed in orange.

NOTE: This feature is not applicable for on-premises deployment as it does not display the order history. However, the on-premises license order history is available when you log in to the public cloud portal as tenant admin.

Configure license expiry email notifications

You can enable license expiration email notifications. An email notification is sent to tenants before the license expires.

Steps

1. Log in to Wyse Management Suite private cloud.
2. Go to **Portal Administration** > **Other Settings**.
3. Select the **Enable License Expiration Notifications on Email** check box.
   The email notification is sent before the license expires in:
   - 60 days
   - 30 days
   - 14 days

   NOTE: The **Enable License Expiration Notifications on Email** option is enabled by default.

   A notification is also sent 24 hours after the license has expired.

19

Firmware upgrade

You can use Wyse Management Suite to upgrade your firmware.

Topics:

Upgrading ThinLinux 1.x to 2.1 and later versions

If you want to pull a customized image from TL 2.x before you upgrade, you must prepare the ThinLinux 2,x and then upgrade the ThinLinux 1.x image.

Prepare the ThinLinux 2.x image

Prerequisites

Use Wyse Management Suite version 1.4 or later versions to upgrade the ThinLinux build version 2.0.19 or 2.1 to 2.2.

Steps

1. Go to www.dell.com/support.
2. Click **Product Support**, enter the **Service Tag** of your thin client, and then press **Enter**.

   NOTE: If you do not have **Service Tag**, manually browse for your thin client model.

3. Click **Drivers and downloads**.
4. From the **Operating system** drop-down list, select **ThinLinux**.
5. Download the `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` and `wda_3.4.6-05_amd64.tar` add-on.
6. Copy the downloaded add-on to `<drive C>/wms/localrepo/repository/thinClientsApps/`.
7. On the thin client running ThinLinux 2.x, go to **Settings** > **Management** > **Wyse Device Agent**.
8. Register the device to the Wyse Management Suite server.
9. Close the **Settings** window.

   NOTE: If the Settings window is not closed, the **Profile Locked** error is displayed after you deploy the image.

10. Log in to the Wyse Management Suite console.
11. Create and deploy app policy for `merlin_nonpxe-4.0.1-0 0.04.amd64.deb` and `wda_3.4.6-05_amd64.tar` add-ons.
12. Reboot the thin client.
13. Log in to the Wyse Management Suite server.
14. Go to the Device page and ensure that the Merlin and WDA versions are updated.
15. Click the registered device, and go to **More Actions** > **Pull OS Image**.
    The **Pull OS Image** window is displayed.
16. Enter the name of the image.
17. From the File repository drop-down list, select the file repository.
18. Select the type of pull operation that you want to perform.
    - **Default**—Select the **OS+Recovery** check box and pull the image (Compressed/UnCompressed).
    - **Advanced**—Select the template `Compress_OS_Recovery_Commandsxml/uncompress_OS_Recovery_CommandsXml` and pull the image.

Results

NOTE:

- If you are using Wyse Management Suite 1.3 remote repository, then the xml file is not available in the repository. You must upgrade Wyse Management Suite to 1.4 or later versions to access the file.
- Recovery Pull operation does not preserve the user settings.

Upgrade ThinLinux 1.x to 2.x

Steps

1. Go to www.dell.com/support.
2. Click **Product Support**, enter the **Service Tag** of your thin client, and then press **Enter**.

   NOTE: If you do not have **Service Tag**, manually browse for your thin client model.

3. Click **Drivers and downloads**.
4. From the **Operating system** drop-down list, select **ThinLinux**.
5. Scroll down the page, and do the following:
   - Download the `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm`, and `merlin-nonpxe_3.7.7-00.05_amd64.deb` add-ons.
   - Download the latest ThinLinux version 2.x image file (`2.1.0.01_3040_16GB_merlin.exe` or `2.2.0.00_3040_merlin_16GB.exe`).
6. On the thin client, go to **Settings** > **Management** > **Wyse Device Agent**.
7. Register the device to the Wyse Management Suite server.
8. Log in to the Wyse Management Suite console.
9. Create and deploy app policy for `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm`, and `merlin-nonpxe_3.7.7-00.05_amd64.deb` add-ons.
10. Reboot the thin client.
11. Log in to the Wyse Management Suite server.
12. Copy the downloaded image (`2.2.0.00_3040_merlin_16GB.exe` file) to `<drive C>/wms/localrepo/repository/osimages/zipped/`.

    NOTE: The image in the zipped folder gets extracted to a valid folder. The extraction process may take 10-15 minutes.

13. Log in to the Wyse Management Suite console.
14. Go to **Apps & Data** > **OS Image repository** > **WES/ThinLinux**, and verify that the ThinLinux image is available.
15. Go to **Apps & Data** > **OS Image policies (WES/ThinLinux)**, and click **Add Policy**.
16. In the Add Policy window, configure the following options:
    - **OS Type**—ThinLinux
    - **OS Sub filter**—ThinLinux(ThinLinux)
    - **Rule**—Upgrade Only/Force this version

    NOTE: Select the pulled image/fresh image that is copied to the repository while creating the policy.

17. Update the other required fields as required, and click **Save**.
18. Schedule the job.
19. Click **Update now** on the client to update the image.

Upgrading ThinOS 8.x to 9.0

You must use Wyse Management Suite version 2.0 and later versions to upgrade your ThinOS firmware to 9.0.

The following table lists the ThinOS firmware images:

Table 12. Firmware images

Platform	ThinOS firmware image
Wyse 3040 Thin Client	A10Q_wnos
Wyse 5070 Thin Client—Celeron processor	X10_wnos
Wyse 5070 Thin Client—Pentium processor	X10_wnos
Wyse 5070 Extended Thin Client—Pentium processor	X10_wnos
Wyse 5470 Thin Client	X10_wnos
Wyse 5470 All-in-One Thin Client	X10_wnos

Add ThinOS 9.x firmware to the repository

Steps

1. Log in to Wyse Management Suite.
2. In the **Apps & Data** tab, under **OS Image Repository**, click **ThinOS 9.x**.
3. Click **Add Firmware file**.
   The **Add File** screen is displayed.
4. To select a file, click **Browse** and go to the location where your file is located.
5. Enter the description for your file.
6. Select the check box if you want to override an existing file.
7. Click **Upload**.

   NOTE: The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To deploy firmware to a device or a group of devices, go to the respective device or the group configuration page.

   NOTE: The operator can upload the firmware from operator account and is visible to all the tenants. Tenants cannot delete or modify the files.

Upgrade ThinOS 8.6 to ThinOS 9.x

Prerequisites

- Ensure to upgrade to ThinOS 8.6_807 with the latest available BIOS installed. For more information about how to upgrade BIOS, see *Dell Wyse ThinOS 8.6* documentation at www.dell.com/support..
- The ThinOS conversion image must be added to the ThinOS firmware repository. For more information, see Add ThinOS firmware to repository.
- Create a group in Wyse Management Suite with a group token. Use this group token to register the ThinOS 8.6 devices.
- The thin client must be registered to Wyse Management Suite.
- Do not configure any wallpaper settings on Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS**.
   The **Select ThinOS Configuration Mode** window is displayed.
3. Select **Advanced Configuration Mode**.
4. Go to **Firmware Upgrade**, and click **Configure this item**.
5. Clear **Disable Live Upgrade** if you want to upgrade immediately, and clear the **Verify Signature** check boxes.
6. From the **Platform Type** drop-down list, select the platform.
7. From the **Firmware to auto-deploy** drop-down list, select the firmware added to the repository.
8. Click **Save & Publish**.

The firmware is deployed to the thin client. The conversion process takes 15 s to 20 s, and the thin client restarts automatically.

Upgrade ThinOS 9.x to later versions using Wyse Management Suite

Prerequisites

- Ensure that you are running ThinOS 9.0.4024 or later versions on your thin client.
- Ensure that you have created a group in Wyse Management Suite with a group token. Use this group token to register the ThinOS 9.x devices.
- Ensure that the thin client is registered to Wyse Management Suite.

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. Click **Advanced**.
4. In the **Firmware** field, select **OS Firmware Updates**.
5. Click **Browse** to browse and upload the firmware.
   The EULA details of the package and the name of the vendors are displayed.
   NOTE: The ThinOS 9.1.3112 has two images. One image is for upgrading from ThinOS 9.0.4024, and the other image is for upgrading from previous version of ThinOS 9.1. Ensure that you select your preferred image.
6. Click the vendor names to read the license agreement of each vendor and then click **Accept** to upload the package.
   You can select the **Do not show this again** if you do not want to see the EULA details of the same vendor again.
   NOTE: If you upload multiple packages, the EULA details of each package are displayed. You must accept the license agreement of the packages individually. The firmware is not uploaded if you click **Decline**.
7. From the **Select the ThinOS Firmware to deploy** drop-down menu, select the uploaded firmware.
8. Click **Save & Publish**.
   The thin client downloads the firmware and restarts. The firmware version is upgraded.

20

Remote repository

Wyse Management Suite allows you to have local and remote repositories for applications, operating system images and so on. If the user accounts are distributed across geographies, it would be efficient to have a separate local repository for each of the distributed user account so the devices can download images from its local repository. This flexibility is provided with `WMS_Repo.exe` software. The `WMS_Repo.exe` is a Wyse Management Suite file repository software that helps to create distributed remote repositories which can be registered with Wyse Management Suite. The `WMS_Repo.exe` is available only for **Pro** license subscribers only.

Prerequisites

- If you are using Wyse Management Suite with cloud deployment, go to **Portal Administration** > **Console Settings** > **File Repository**. Click **Download version x.x** and download the `WMS_Repo.exe` file
- The server requirements to install Wyse Management Suite repository software are:
  - Windows 2012 R2 or Windows 2016 Server Standard
  - 4 CPU
  - 8 GB RAM
  - 40 GB storage space

NOTE: Wyse Management Suite server and repository installation is not supported on cloud hosted servers such as Azure, Amazon Web Services, and Google Cloud Platform.

About this task

Do the following to install **WMS-Repo** software:

Steps

1. Log in as **Administrator**, and install `WMS_Repo.exe` on the repository server.
2. Click **Next** and follow the instructions on the screen to complete the installation.
3. Click **Launch** to launch the **WMS Repository registration** screen on the web browser.
4. Select the **Register to public WMS Management Portal** if you are registering on the public cloud.

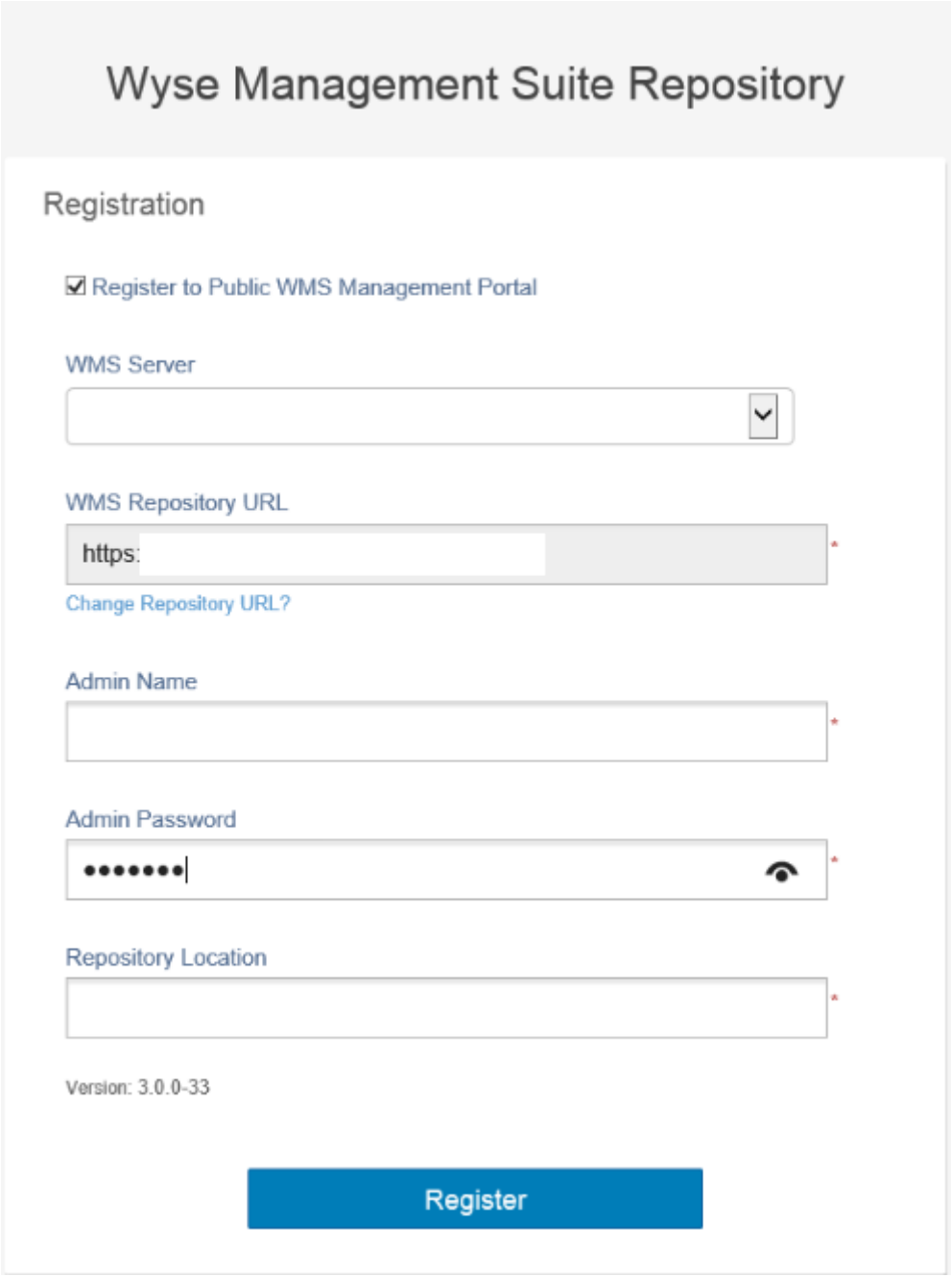


Figure 22. Register on a public cloud

5. Enter the following details:
   a. Wyse Management Suite server URL

      NOTE: Unless you register with Wyse Management Suite version 1.0, you cannot use MQTT Server URL.

   b. WMS Repository URL (update the URL with the domain name)
   c. Wyse Management Suite administrator login username information
   d. Wyse Management Suite administrator login password information
   e. Repository path information
6. Click **Register**.
7. If the registration is successful, the **Registration** window is displayed:

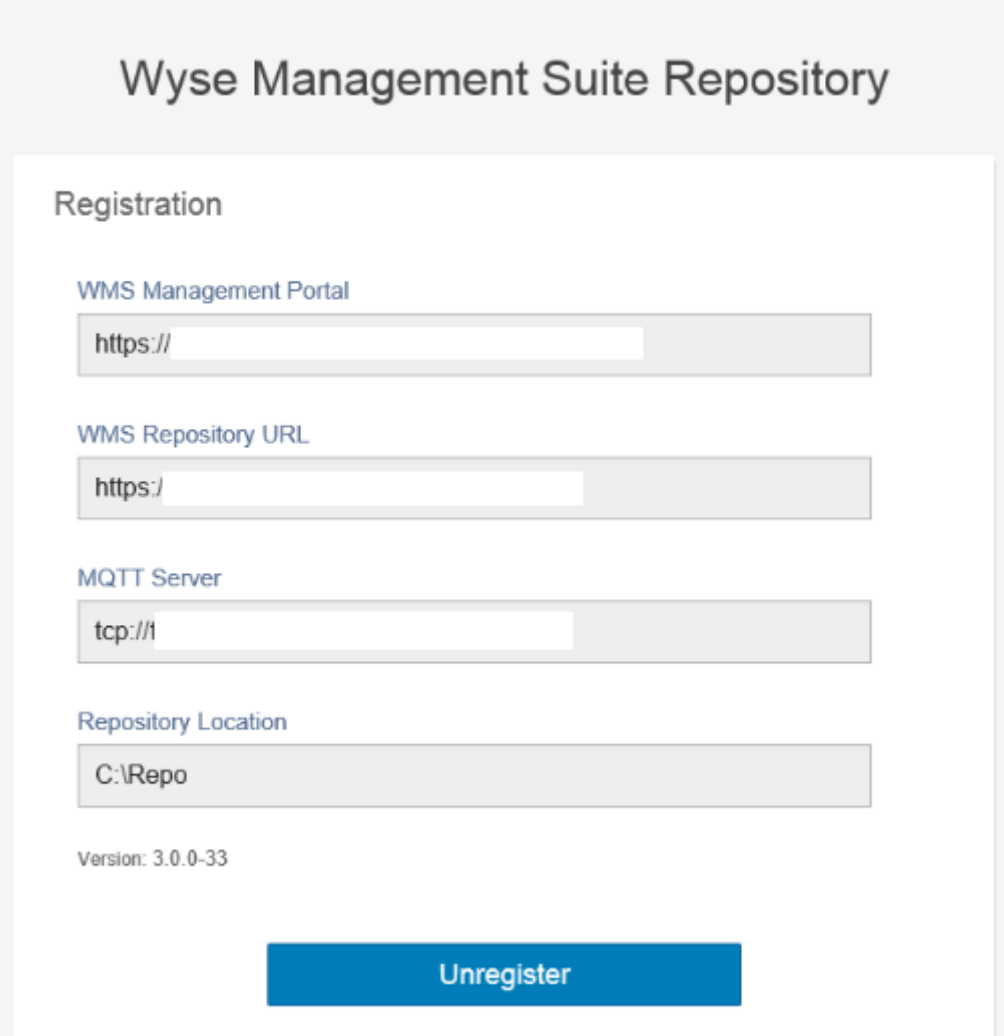


Figure 23. Registration successful

8. The following screen on the Wyse Management Suite portal confirms the successful registration of the remote repository:

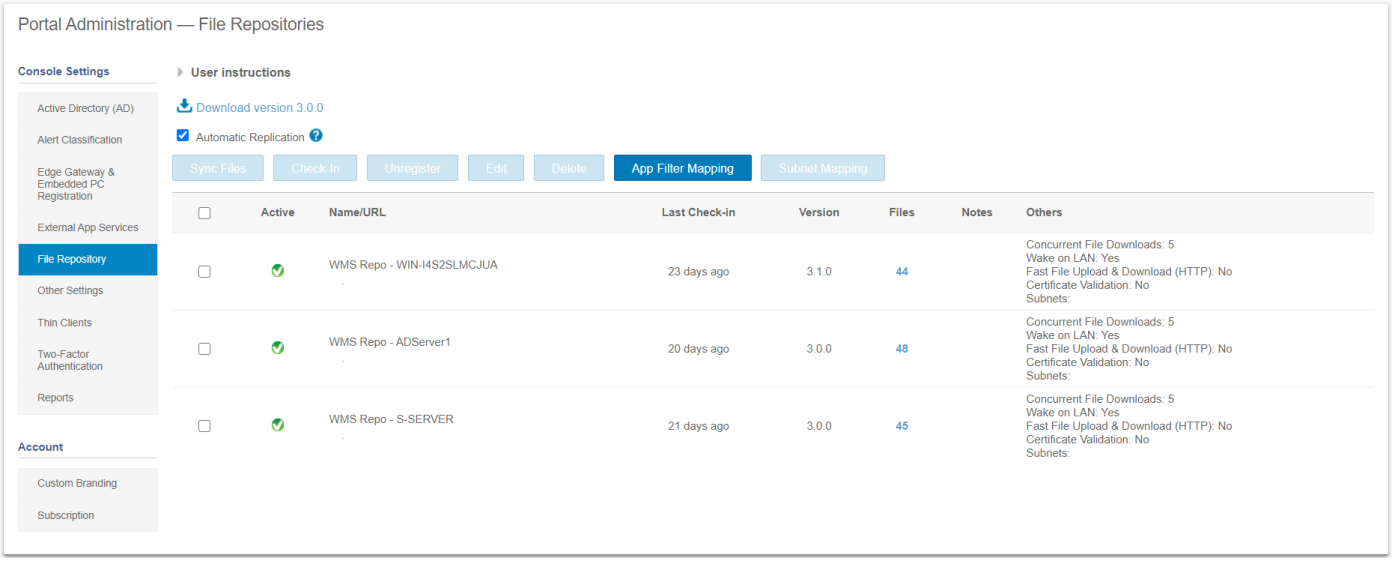


Figure 24. Registration successful on the portal

9. HTTPS is by default enabled with `WMS_Repo.exe`, and is installed with the self-signed certificate. To install your own domain-specific certificate, scroll down the registration page to upload the SSL certificates.

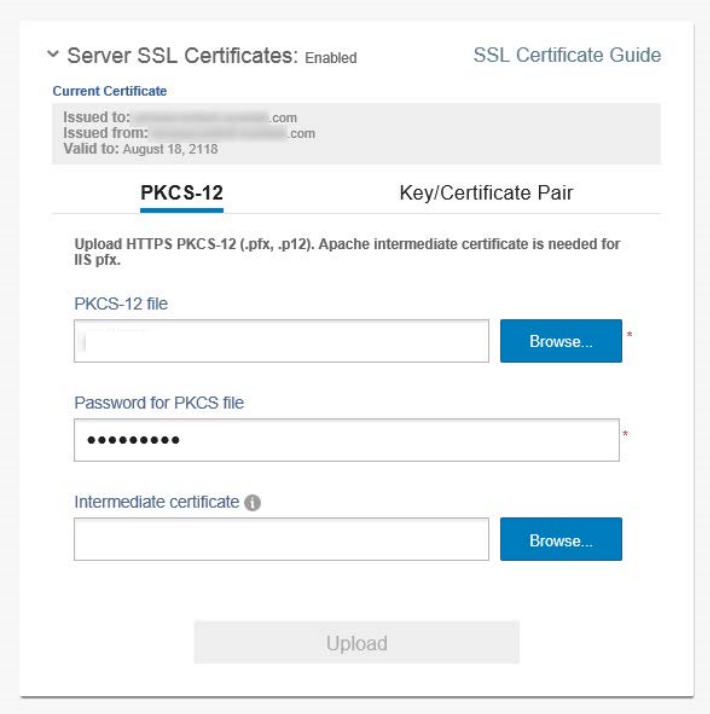


Figure 25. Certificate upload

10. The server restarts, and the uploaded certificate is displayed.

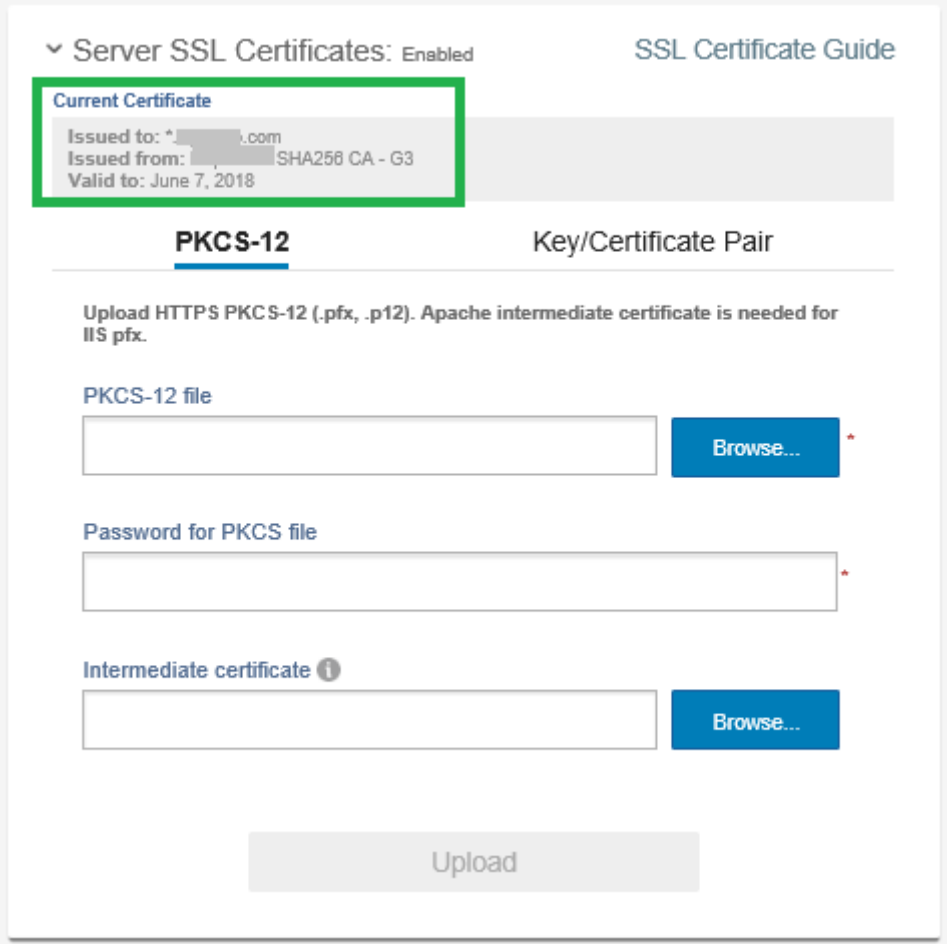


Figure 26. SSL certificate enabled

11. If the Wyse Management Suite is enabled with self-signed or a private domain certificate, you can upload the certificate on the Wyse Management Suite repository server to validate the Wyse Management Suite CA credentials.

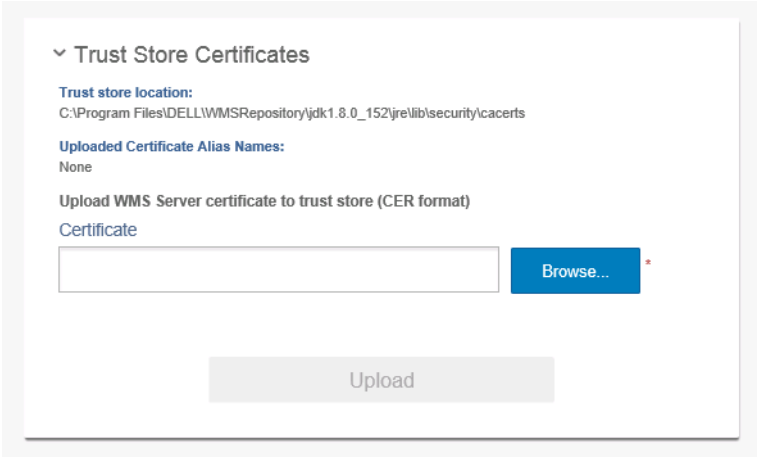


Figure 27. Trust store certificates

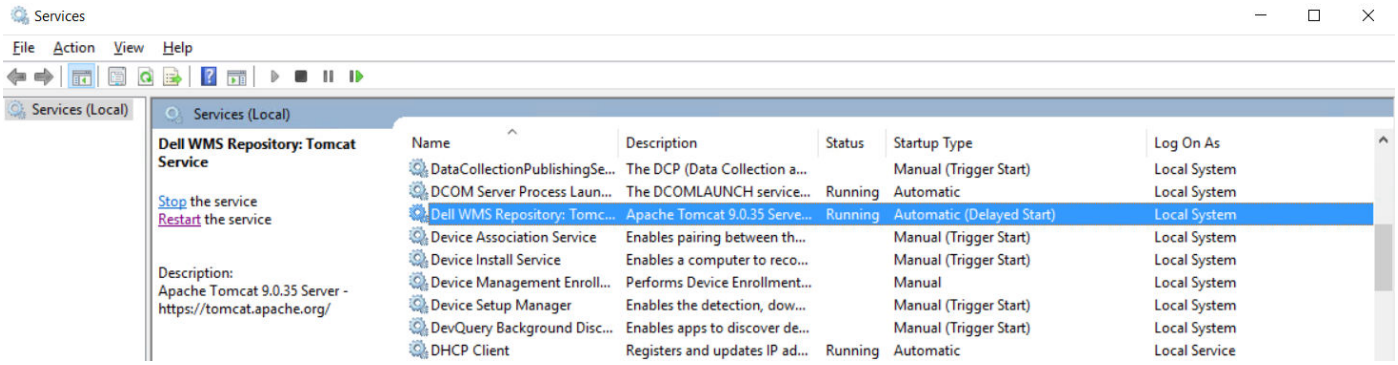
12. Navigate to the `C:\wmsrepo` location that you entered during registration, and you can view the folders where all the repository files are saved and managed.

Topics:

- Manage Wyse Management Suite repository service
- Proxy support for Wyse Management Suite remote repositories

Manage Wyse Management Suite repository service

Wyse Management Suite repository is displayed as **Dell WMS Repository: Tomcat Service** in the Windows Local Services window and is configured to start automatically when the server restarts.



Proxy support for Wyse Management Suite remote repositories

From Wyse Management Suite 3.2, remote repositories support HTTPS and SOCKS5 proxy for all HTTPS and MQTT communications to Wyse Management Suite.

Only system-wide proxies are supported since the remote repository runs as a Windows service. Also, only proxies with AD authentication or no authentication are supported. You can configure the proxy servers using any method. Following are a few examples on how to configure proxy server information:

- Using the netsh command—You can use the following command to configure the proxy server information
  - SOCKS5 proxy

```
netsh winhttp set proxy proxy-server="socks=localhost:9090" bypass-list="localhost"

C:\Users\administrator.WMSAD61>netsh winhttp set proxy proxy-server="socks=<proxy
server IP>" bypass-list="localhost"

Current WinHTTP proxy settings:

    Proxy Server(s) :  socks=<proxy server IP>
    Bypass List     :  localhost
```

  - HTTPs proxy

```
netsh winhttp set proxy proxy-server="https=<ProxyServerIP>:<Port number>" bypass-
list="localhost"

C:\Users\administrator.WMSAD61>netsh winhttp set proxy proxy-server="https=<proxy
server IP>" bypass-list="localhost"

Current WinHTTP proxy settings:

    Proxy Server(s) :  https=<proxy server IP>
    Bypass List     :  localhost
```

- Using the WPAD file configured in DHCP—Wyse Management Suite repository server must be configured with DHCP IP address and Internet Explorer must be configured with Automatically Detect settings. You must configure the DHCP option tag 252 with the WPAD.pac file. Following is a sample PAC file content:

```
function FindProxyForURL(url, host)
{
    if (shExpMatch(host, "*wysemanagementsuite.com*")) {
    return "SOCKS <proxy server IP>";
}
```

```
    return "DIRECT";
}
```

You can also configure the proxy settings using group policies.

NOTE: Proxy settings are read when the repository service starts. If you make any changes to the proxy settings later, you must restart the repository service.

NOTE: Host name resolution is not set if SOCKS4 proxy is used. You must update the hosts file present in `C:\Windows\System32\drivers\etc` to resolve the public cloud URL/hostname on the server where Wyse Management Suite repository is installed. If SOCKS5 proxy is used, the hostname resolution using the DNS configured in network settings of the server is resolved.

21

Proxy support for Windows Embedded Standard WDA and Dell Hybrid Client DCA

Windows Embedded Standard WDA supports HTTPS proxy, and Dell Hybrid Client DCA supports HTTPs and SOCKS5 proxy for all HTTP and secure MQTT communications with Wyse Management Suite public server. Only system-wide proxies are supported as WDA and DCA run as a service.

Proxies with AD authentication or no authentication are supported. PAC script that is configured using DHCP option tag 252 is supported. Proxy settings are read when WDA and DCA services start. If there are changes in the proxy settings, the WDA and DCA services must be restarted.

The following are the limitations of the proxy support:

- Proxies that are configured at the user level are not supported.
- There is no provision for user to enter username and password.
- There is no user interface to enter the proxy URL as proxy details are read from the underlying operating system.
- The external MQTT with 1883 does not support proxy.
- HTTP proxy is not supported.
- Proxy PAC file through DNS is not supported.

Topics:

Configure proxy server Information using WININET proxy for Windows Embedded Standard WDA

You must configure the domain policy to set the WININET proxy setting at system level for all devices.

Steps

1. Open **Command Prompt** as an administrator.
2. Run the `gpedit.msc` command.
3. Configure the group policy from the domain controller to enable IE-proxy configuration per machine. To configure the policy, go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Proxy settings per-machine** and enable the option.
4. Run `gpupdate/force` in the same command prompt.
5. Open Internet Explorer as an administrator and go to **Connections** > **LAN settings**.
6. Configure the proxy and click **OK**.

Configure proxy server information using DHCP option tag for Windows Embedded Standard WDA and Dell Hybrid Client DCA

Windows Embedded Standard and Dell Hybrid Client powered devices must be configured with DHCP IP. For the DHCP configuration, the DHCP option tag 252 must be configured with the WPAD.pac file.

The following is a sample PAC file (WPAD.dat) content:

```
function FindProxyForURL(url, host)
{
        if (shExpMatch(host, "*wysemanagementsuite.com*"))
{
        return "SOCKS 100.xxx.xxx.xxx:1080";
}
        return "DIRECT";
}
```

The following are the limitations:

- Only Secure MQTT communication supports proxy.
- MQTT port 1833 does not support proxy.

22

Troubleshooting your device

You can view and manage the troubleshooting information using the **Devices** page.

Steps

1. On the **Device Details** page, click **Troubleshooting** tab.
2. Click **Request Screen Shot**.
   You can capture the screenshot of the thin client with or without the client permission. If you select the **Require User Acceptance** check box, then a message is displayed on the client. This option is applicable only for Windows Embedded Standard, Linux, and ThinLinux devices.
3. Click **Request Processes List**, to view the list of the processes running on the thin client.
4. Click **Request Services List**, to view the list of the services running on the thin client.
5. Click **Start Monitoring**, to access the performance metric console.
   On the **Performance metric** console, the following details are displayed:
   - Average CPU last minute
   - Average memory usage last minute

Topics:

Request a log file using Wyse Management Suite

Prerequisites

The device must be enabled to pull the log file.

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.

   NOTE: The ThinOS device uploads the system logs.

View audit logs using Wyse Management Suite

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.
   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.

Device fails to register to Wyse Management Suite when WinHTTP proxy is configured

WDA is a WinHTTP Client and fetches WinHTTP proxy information from the local system.

If you have configured WinHTTP Proxy and the device fails to contact the Wyse Management Suite server, do the following to enable the Proxy Information available at the system level:

- **Case 1**—When the device is added to a domain, enable IE-Proxy Configurations for each user using the Group Policy from the domain. You must configure the Group Policy from domain controller to enable IE-Proxy configurations for each client, and not for each user.

  Go to `Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Make proxy settings per-machine`, and select **Enable**. Also, go to `IE Settings > Internet Options > Connections > LAN Settings` in the Internet Explorer, and enable **Automatically detect settings**.

- **Case 2**—When the device is not added to a domain, go to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings` and create a **32-bit DWORD** called **ProxySettingsPerUser**, and set it to 0. Also, go to `IE Settings > Internet Options > Connections > LAN Settings` in the Internet Explorer, and enable **Automatically detect settings**.

RemoteFX USB redirection Policy does not get applied for USB mass storage devices

Steps

1. Log in to the device as an administrator.
2. Disable the Write Filter.
3. Go to **Run** command and type **`Regedit`**.
4. Go to `HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces`.
5. Add string registry key as **`100`** and set the value as for Mass Storage Device as `{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}` for CD ROM : `{53F56308-B6BF-11D0-94F2-00A0C91EFB8B}`.

   NOTE: Flower brackets are mandatory.

WiFi settings configured from Wyse Management Suite are not persistent across multiple Wyse 5070 thin clients

When you configure a WiFi connection on a Wyse 5070 Thin Client, it connects to a specific wireless network (SSID) without asking for the password. When the same configuration is exported to Wyse Management Suite and deployed to other Wyse 5070 Thin Clients, the configuration is applied and you are prompted to enter a password to connect to the same wireless network. To make the WiFi settings persistent, do the following:

Steps

1. Connect the Wyse 5070 Thin Client to the wireless network.
2. Run `DWirelessProfileEditor.exe` file.
   The **Wireless Profile Password Editor** window is displayed.
3. Browse to the destination path to save the profile as an xml file and click **Save**.
4. Click the **Export WiFi Profiles** button in the **Wireless Profile Password Editor** window.
5. From the **Profiles** drop-down list, select the profile to deploy the configuration.

6. Clear the **Password** field, and enter the password again.
7. Click **Change Password**.

   NOTE: Do not click the **Export WiFi Profiles** button again.

8. Close the **Wireless Profile Password Editor** window.
9. Log in to Wyse Management Suite.
10. Go to **Apps & Data** > **File Repository** > **Inventory**.
11. Click **Add File**.
12. Browse to the xml file.
13. From the **Type** drop-down list, select **Windows Wireless Profile**.
14. Enter the description.
15. Select the **Override existing file** option if you want to overwrite the present configuration.
16. Click **Upload**.
17. Go to **Groups & Configs** > **Edit Profiles** > **WES** > **Network**.
18. Click **Configure this item**.
19. From the **Windows Wireless Profiles** drop-down list, select the uploaded file.
20. Click **Save & Publish**.

23

Frequently asked questions

Topics:

What takes precedence between Wyse Management Suite and ThinOS UI when conflicting settings are enforced?

Any settings that are configured using Wyse Management Suite take precedence over the settings that were configured locally on the ThinOS client or published using the Admin Policy Tool.

The following order defines the priority set for ThinOS configurations:

Wyse Management Suite Policies > **Admin Policy Tool** > **Local ThinOS UI**

How do I use Wyse Management Suite file repository?

Steps

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 the Wyse Management Suite server.
4. To register the repository to the Wyse Management Suite public cloud, enable the **Register to Public WMS Management Portal** option.
5. Click the **Sync Files** option to send the sync file command.
6. Click **Check In** and then click **Send Command** to send the device information command to the device.
7. Click the **Unregister** option to unregister the on-premises service.
8. Click **Edit** to edit the files.
   a. From the drop-down list of **Concurrent File Downloads** option, select the number of files.
   b. Enable or disable **Wake on LAN** option.
   c. Enable or disable **Fast File Upload and Download (HTTP)** option.
      - When HTTP is enabled, the file upload and download occurs over HTTP.
      - When HTTP is not enabled, the file upload and download occurs over HTTPS.
   d. Select the **Certificate Validation** check box to enable the CA validation for a public cloud.

   NOTE:
   - When CA Validation from the Wyse Management Suite server is enabled, the certificate should be present in the client. All the operations, such as, Apps and Data, Image Pull/Push is successful. If the certificate is not present in the client, the Wyse Management Suite server provides one generic audit event message **Failed to Validate**

Certificate Authority under **Events** page. All the operations, such as, Apps and Data, Image Pull/Push is not successful.

- When CA Validation from Wyse Management Suite server is disabled, then the communication from server and client happens in a secure channel without Certificate Signature validation.

e. Add a note in the provided box.
f. Click **Save Settings** .

How do I import users from a .csv file?

Steps

1. Click **Users**.
   The **Users** page is displayed.
2. Select the **Unassigned Admins** option.
3. Click **Bulk Import**.
   The **Bulk Import** window is displayed.
4. Click **Browse** and select the .csv file.
5. Click **Import**.

How do I check the version of Wyse Management Suite

Steps

1. Log in to Wyse Management Suite.
2. Go to **Portal Administration** > **Subscription**.
   The Wyse Management Suite version is displayed in the **Server Information** field.

How to create and configure DHCP option tags

Steps

1. Open the Server Manager.
2. Go to **Tools**, and click **DHCP option**.
3. Go to **FQDN** > **IPv4**, and right-click **IPv4**.
4. Click **Set Predefined Options**.
   The **Predefined Options and Values** window is displayed.
5. From the **Option class** drop-down list, select the **DHCP Standard Option** value.
6. Click **Add**.
   The **Option Type** window is displayed.
7. Configure the required DHCP option tags.
   - To create the 165 Wyse Management Suite server URL option tag, do the following:
     a. Enter the following values, and click **OK**.
        - Name—WMS
        - Data type—String
        - Code—165
        - Description—WMS_Server

     b. Enter the following value, and then click **OK**.

        String—`WMS FQDN`

- To create the 166 MQTT server URL option tag, do the following:
  a. Enter the following values, and click **OK**.
     - Name—MQTT
     - Data type—String
     - Code—166
     - Description—MQTT Server
  b. Enter the following value, and click **OK**.

     String—`MQTT FQDN`

     For example, **`WMSServerName.YourDomain.Com:1883`**
- To create the 167 Wyse Management Suite CA Validation server URL option tag, do the following:
  a. Enter the following values, and click **OK**.
     - Name—CA Validation
     - Data type—String
     - Code—167
     - Description—CA Validation
  b. Enter the following values, and click **OK**.

     String—TRUE or FALSE
- To create the 199 Wyse Management Suite Group Token server URL option tag, do the following:
  a. Enter the following values, and click **OK**.
     - Name—Group Token
     - Data type—String
     - Code—199
     - Description—Group Token
  b. Enter the following values, and click **OK**.

     String—defa-quarantine

NOTE: The options must be either added to the server options of the DHCP server or scope options of the DHCP scope.

How to create and configure DNS SRV records

Steps

1. Open the Server Manager.
2. Go to **Tools**, and click **DNS**.
3. Go to **DNS** > **DNS Server Host Name** > **Forward Lookup Zones** > **Domain** > **_tcp**, and right-click the **_tcp** option.
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:
   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
   b. To create MQTT server record, enter the following values, and then click **ÓK**.
      - Service—_WMS_MQTT
      - Protocol—_tcp
      - Port number—1883

- Host offering this service—FQDN of MQTT server

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

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

How to change the hostname to IP address

About this task

You must change the hostname to IP address when the hostname resolution fails.

Steps

1. Open the DOS prompt in elevated Admin mode.
2. Change the directory to **`C:\Program Files\DELL\WMS\MongoDB\bin`**.
3. Enter the command, **`mongo localhost -username stratus -p --authenticationDatabase admin`**
   Output—MongoDB shell version v4.2.12
4. Enter the password.
   Output—
   - connecting to: mongodb://127.0.0.1:27017/localhost
   - MongoDB server version: 4.2.12
5. Enter : use stratus
   Output—switched to db stratus
6. Enter the command, **`> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, {$set : {'value' : "https://IP:443/ccm-web"}} )`**
   Output—{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7. Enter the command, **`> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})`**
   Output—{ "_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }

How do I image the device using self-signed remote repository

You can perform imaging of Windows Embedded Standard and ThinLinux devices from the local repository of private cloud or from the remote repository of public cloud.

Prerequisites

If the image is deployed from the local repository of private cloud or from the remote repository of public cloud with a self-signed Certificate, the administrator must push the self-signed certificate to the thin clients to perform imaging when the CA Validation is enabled.

Steps

1. Export the self-signed certificate from Internet Explorer or MMC.
2. Upload the certificate to Wyse Management Suite—see Image Policy.

3. Push the certificate to the target clients or groups of clients using the security policy.
   Wait for the **Configuration Policy Job** to complete.
4. Enable CA Validation from local repository of private cloud or from the remote repository of public cloud.
5. Create an image policy and schedule it to the group.