Dell Wyse Management Suite Version 4.4

Administrator Guide

May 2024
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 require a license key to use the Standard edition. To generate the standard license key, go to the Wyse Management Suite trials page Wyse Management Suite trials page, and select **Start Free WMS Standard**. You must enter the contact details, email address, and on-premises identifier. An email with the standard license key is sent to the provided email address. The Standard edition is suitable for small and medium businesses. Wyse Management Suite with standard license can have three global administrators. One global administrator is created during the installation and two additional global administrators can be created after the installation.

  NOTE: You must ensure that the on-premises version of Wyse Management Suite is the same as the cloud version while registering your on-premises UUID. If the on-premises version is lower than the cloud version, you cannot use the license key.
- **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 Windows PCs (formerly Wyse Converter for PCs), and Dell Hybrid Client devices. It also offers more advanced features to manage Dell thin clients. For a public cloud deployment, the Pro edition can be managed on noncorporate networks such as home office, third-party partners, mobile thin clients, and so on.

  NOTE: Licenses can be floated between cloud and on-premises 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	Small deployments, single location	Up to 120 thousand devices	Up to 1 million devices
License term	1-year free license subject to registration	Per seat subscription	Per seat subscription
License key	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	√	√ **
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	√	√
Dell thin clients with ThinOS	√	√	√
Wyse thin clients with ThinLinux	√	√	√
Dell 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			

Table 1. Feature matrix for each subscription type (continued)

Features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Localized management console	X	√	√
Alerts, Events, and Audit log using email and mobile application	X	√	√
Enterprise-Grade Reporting	X	√	√

NOTE: **A double asterisk indicates that for cloud edition, API option is not enabled by default. The option is enabled if you have an API license. For more information, see *How to Request API Enablement in Wyse Management Suite Pro* at Dell | Support.

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	√	√

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
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	√	√
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: Dell Technologies recommends upgrading the system to 12 GB RAM as more memory is required to enable secure communication.

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

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

Table 3. Dell thin client solutions feature matrix

Dell thin client solutions 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	√	√	-
Configurable heartbeat and check-in interval	√	√	√
Security			
Secure communication (HTTPS)	√	√	√
802.1x certificate deployment	√	√	√
Secure MQTT	√	√	√
Two-factor authentication	√	√	√
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	√	√

Table 3. Dell thin client solutions feature matrix (continued)

Dell thin client solutions features	Wyse Management Suite Standard	Wyse Management Suite Pro-private cloud	Wyse Management Suite Pro-cloud edition
Configuration			
Dell 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	√	√
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: **A 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: Dell Technologies recommends upgrading the system to 12 GB RAM as more memory is required to enable secure communication.

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

NOTE: ThinOS 9.1.x, Dell Hybrid Client 1.5 and later versions, Wyse Device Agent 14.5.3.11 and later versions support secure MQTT.

New features

IPv6 endpoints and infrastructure routing support

Wyse Management Suite 4.4 enables you to setup on-premises server with IPv6. IPv6 endpoint must connect to an IPv6 address using a DNS hostname. The unmanaged device auto assignment in **Rules** > **Unmanaged Device Auto Assignment** > **Add Rule** > **Add Condition** > **ipv6Prefix** is based on the IPv6 prefix . For example, 2001:1111:2222:3333::/64.

Also, to use subnet-mapping feature, the administrator must provide IPv6 Prefix. For example, 2001:1111:2222:3333::/64.

The following are the known limitations of IPv6 support:

- Remote Shadow P2P is not supported in the IPv6 environment.
- If the WMS environment is switched from IPv4 to IPv6, then you must restart all WMS services.
- If the WMS repository is registered to WMS in IPv4 and later enabled with IPv6, then the administrator must unregister and re-register the repository.

Configure multiple ThinOS firmware for sequential upgrade

The administrator can configure to deploy three ThinOS firmware sequentially from Wyse Management Suite. The new Config UI is enabled for firmware selection in the ThinOS policy. The administrator can define the priority for the deployment of each firmware. The device checks the version and allows only upgrades from the current versions in the sequential order.

ⓘ **NOTE:** This feature is supported from ThinOS firmware version 2405 and Config UI released for this firmware and later versions.

Override device level configuration for select groups

The administrator can decide the priority for a configuration for devices running ThinOS 2405 and later versions having device level exception for a select group. A new checkbox is provided while creating or editing the select group to enable or disable the device level exception to override the select group policy.

When this option is enabled, device level configurations are applied to the device and when the option is disabled select group configurations are applied to the device.

The option is disabled by default and is available only for the parent select group and is not applicable for any other default or custom groups and child select groups.

Appropriate events are generated when you enable or disable the option for the select group.

Remote shadow P2P support

The administrator can remote shadow to a ThinOS 2405 and later versions from the on-premises server. Remote shadow VNC and remote shadow P2P are supported for the on-premises server.

When VNC is enabled, P2P is disabled, and conversely.

The following VNC connection settings can be configured in **Portal Administration** > **Other Settings**:

- **Maximum Concurrent Remote Shadow Connections (1-30): 10**
- **Idle Remote Shadow Session Timeout (1-20 minutes): 20**
- **Maximum Remote Shadow Session Timeout (1-60 minutes):20**
- **No Connection Timeout (1-10 minutes):10**

The option is not available for the public cloud environment.

Standard license renewal

From Wyse Management Suite 4.4, you can renew your standard license from your on-premises environment. A new section with a renewal identifier is displayed in the **Subscription** page in the **Portal Administration** tab for the on-premises environment. This section is enabled before 60 days of expiry.

A new button **Renew WMS Standard** is added in the **Trial** page to renew the standard license keys. The administrator must copy the renewal identifier and enter the details in the **Renew WMS Standard** form in the **Trial** page. A new standard renewal license key is generated with a validity of one year and is sent to the administrator email address.

The administrator must import the license key from **Portal Administration** > **Subscription** > **License**.

If the administrator wants to update the email address, then the updated details must be provided in the renewal form so that the renewal key is delivered to the updated administrator email address.

ⓘ **NOTE:** If the administrator does not provide the correct country or region details, the renewal may fail.

Wave upgrade enhancements

From Wyse Management Suite 4.4, the administrators can schedule a wave policy when a group policy job is active. This feature is similar to scheduling the group policy when a wave job is active. An alert message is displayed where the administrator can cancel or schedule a job.

The wave policy overrides the **Groups and Config** job while both wave and group policies are scheduled simultaneously for a group.

ⓘ **NOTE:** If the wave policy job is scheduled while the group policy job is in-progress, then the wave policy configurations override the group policy configurations.

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:

Prerequisites

Before setting up the thin clients to register to Wyse Management Suite public cloud, ensure that the ports 443 and 1883 are in allow list.

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 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.

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 if you are using thin clients that do not support cloud applications such as Windows Embedded Systems. If the thin client type is ThinOS and Dell Hybrid Client, the remote repository is optional since the client files can be uploaded and hosted in the tenant cloud up to 10 GB. The Dell Hybrid Client ISO files cannot be uploaded to tenant cloud which are more than 1.5 GB. The occupied space from Tenant Cloud can be viewed in **Dashboard** page. Also, the Fully Qualified Domain Name (FQDN) of the server must be registered in DNS so that the thin clients can connect for any package download. For more details on Wyse Management Suite Repository, see Remote repository.

NOTE: Concurrent login of a user is not supported and a user can have only one active session on the web console and on the mobile application. When you try to log in to the server from another browser or try to log in from another system without logging off from the previous session, then

```
Your login attempt was not successful. Reason: User account already logged in
```

error message is displayed. The same error is displayed if you do not log off from the session from a browser. The administrator can select the option **Log me out everywhere else** to log in to the portal forcefully. If the option is selected, the previous login session is invalidated. After you deploy on-premises or public cloud version of Wyse Management Suite , all the active sessions are invalidated. The administrator must relogin to Wyse Management Suite to continue accessing the portal. When the administrator changes the portal administrator role or the username for any other logged in user, then the session of other logged in user gets invalidated. The other administrators must relogin to Wyse Management Suite to continue accessing the portal.

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, Windows Server 2019 Standard or Windows Server 2022. 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			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.

Table 4. Prerequisites (continued)

Description	10,000 devices or less	50,000 devices or less	120,000 devices or less	Wyse Management Suite – Software repository
	● 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.			
Supported browsers	Google Chrome version 97.0.4692.99 and later Mozilla Firefox version 91.5.0 and later Edge browser on Windows—97.0.1072.69 and later (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 cannot install or upgrade Wyse Management Suite 3.3 using any other version of external MongoDB server.

NOTE: From Wyse Management Suite 3.6, the repository installation is supported on Windows 2016 and Windows 2019 virtual machines that are hosted on Azure and Amazon Web Services (AWS). It is not supported on Google Cloud Platform. After you install the repository, the repository URL is displayed as the hostname of the virtual machine. The URL may not be reachable by the end points. To enable the URL to be reachable to the end points, the repository URL must be edited and the DNS name of the virtual machine must be used as the URL before registering to Wyse Management Suite. For example, `uw2-wmstest-vw01.westus2.cloudapp.azure.com` is a sample of the Azure virtual machine DNS address and `ec2-3-141-79-165.us-east-2.compute.amazonaws.com` is a sample of the AWS virtual machine DNS address.

NOTE:

Wyse Management Suite portal cannot be used with Internet Explorer. If the default browser is Internet Explorer and if the Edge browser is installed on the server, when Wyse Management Suite is installed, it is launched in the Edge browser. If any other browser is set as the default browser apart from Internet Explorer, then Wyse Management Suite server portal and repository portal are launched in the same default browser. When you install Wyse Management Suite, the server and repository launches in either the default browser or Edge browser without any certificate error. When the server or repository is upgraded, then certificate error is displayed. The error is also displayed if you use Mozilla Firefox as the default browser.

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.

Two factor authentication improvements

The administrator can request One-Time Password(OTP) eight times after which the administrator is locked for 15 minutes. For wrong OTP attempt or OTP expiry, you can receive the OTP using the **Resend** option. The **Resend** option is enabled every 30 sec and can be performed seven times. After eight resend attempts, the **Resend** option is locked and not displayed in the user interface.

An email is sent to the administrator when the **Resend** option locked and you try to log in again, a message is displayed on the Wyse Management Suite login user interface.

The locked user can be unlocked by another global administrator.

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 a Latitude, OptiPlex, or Precision 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 Latitude, OptiPlex, or Precision 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 and later versions 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 10 IoT Enterprise, Linux, and ThinLinux devices by using Wyse Management Suite.

- **Windows 10 IoT Enterprise 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 the Wyse Device Agent .exe file.

  NOTE: Wyse Device Agent can be installed on the 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.

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 Dell | 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 legacy DHCP option tags.
   > - Using DNS SRV record—see Registering devices by using legacy 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).
4. Configure the thin client using any of the following options:
   - Using the **Groups and Configs** page.
   - Using the **Devices page**.

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.

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

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

The device is registered to Wyse Management Suite.

9. Log in to Wyse Management Suite.
10. Add the device to your desired group (optional).
11. Configure the thin client using any of the following options:
    - Using the **Groups and Configs** page.
    - Using the **Devices page**.

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

3. Add the device to your desired group (optional).
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**.

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

3. Add the device to your desired group (optional).
4. Configure the thin client using any of the following options:
    - Using the **Groups and Configs** page.
    - Using the **Devices page**.

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 .

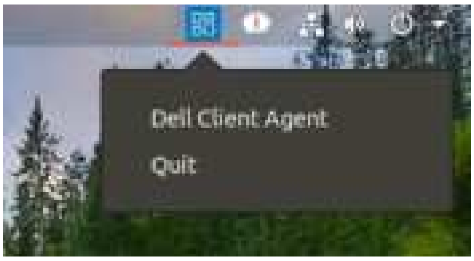


Figure 1. DCA icon

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.

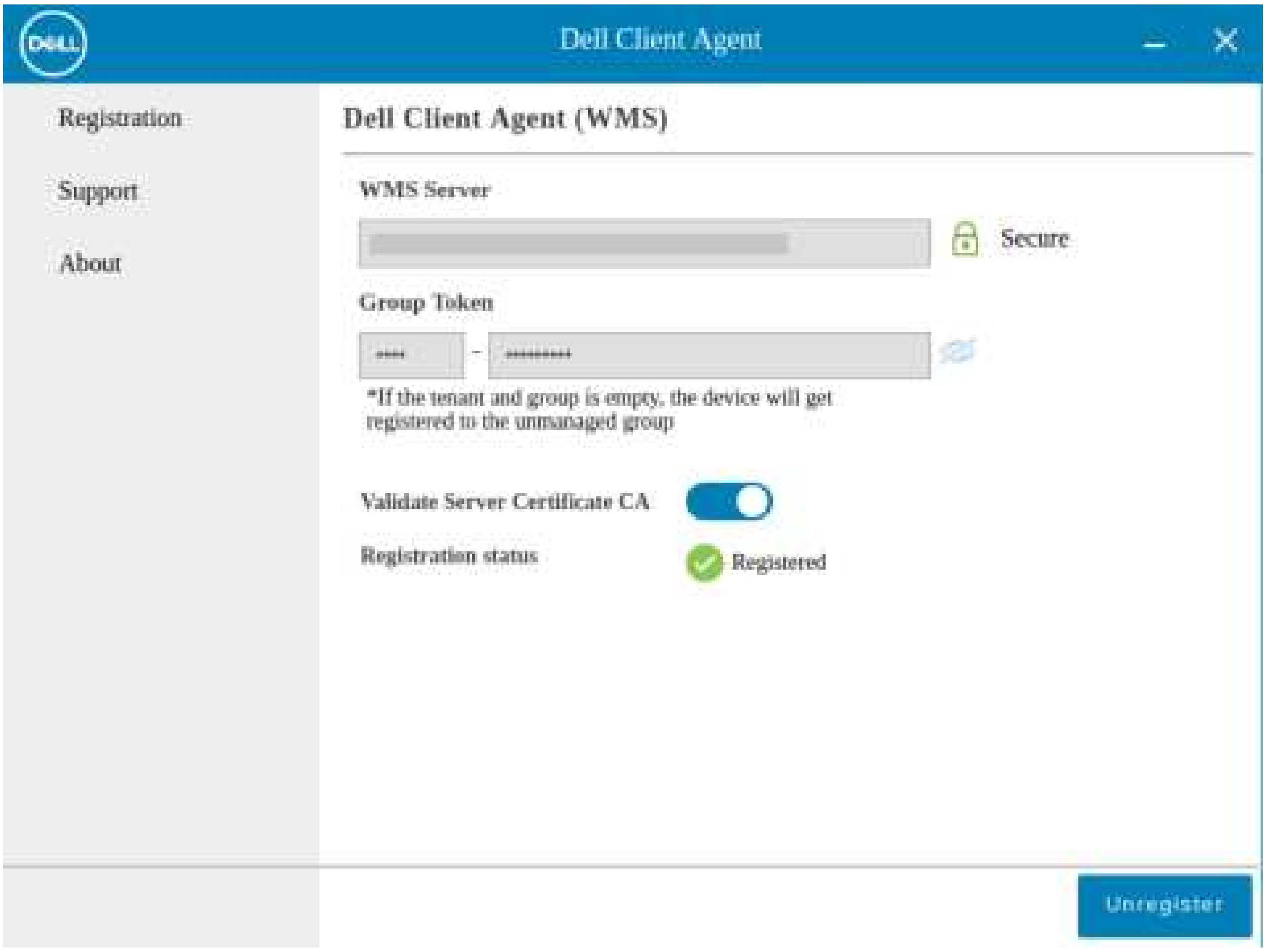
9. Click **Register** to register your hybrid client on the Wyse Management Suite server.

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

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

   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**.



Dell Client Agent (WMS)

WMS Server: [redacted] Secure

Group Token: **** - *********

*If the tenant and group is empty, the device will get registered to the unmanaged group

Validate Server Certificate CA: On

Registration status: ✓ Registered

Figure 2. Dell Client Agent

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

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: To register the device, you should have Ubuntu System Admin privileges and authenticate.

Steps

1. Log in to the Dell Generic Client running Ubuntu operating system.
2. Search for the DCA Enabler user interface in the Ubuntu App menu.
   The **Dell Client Agent - Enabler** window is displayed. You can view the DCA-E agent version in the **Registration** tab.
3. Enter the WMS Server address.
4. Optionally, enter the group token if you are registering to Wyse Management Suite on-premise environment.
   If the group token is empty, the device is registered to the unmanaged group.

5. Enable or disable CA validation based on the public cloud or on-premise and certificate availability on the Generic device.
6. Click **Register**.

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

   - Using DHCP option tags—see Register devices by using legacy DHCP option tags
   - Using DNS SRV record—see Registering devices by using legacy DNS SRV record
   - Using secure DNS SRV record and DHCP option tags—see Register devices using DNS SRV record fields or DHCP scope options

   ⓘ **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.

7. Log in to Wyse Management Suite.
8. Add or move the device to your wanted group (optional).
9. Configure the Generic client using any of the following options:
   - Using the **Groups and Configs** page.
   - Using the **Devices page**.

6

Enhanced Dashboard

The Dashboard user interface is enhanced to display the **Alerts**, **Events**, **Non-Compliance status**, **Jobs**, and **Remote Connections**. You can also view the eMMC health status with the count of devices running ThinOS 2402 and later versions, and the device count with recovery partition changes for Dell Hybrid Client 2403 devices.

The following table describes the categorization of the recovery partition status on the Dashboard:

Table 5. Categorization of the recovery partition status

Status	Description
Major	Any changes that are related to DHC in the recovery partition or if three or more directories are affected in the recovery partition.
Minor	Any other changes.
No change	There are no changes to the recovery partition.
Recovery is not found	Recovery partition is not available in the DHC client.

ⓘ **NOTE:** The **Enable eMMC Disk Lifetime** option must be enabled for the ThinOS devices at the group or device level to view the eMMC status.

The summary of the jobs is enhanced to provide a view of all the jobs and the status of the wave jobs.

The **Events** section is also enhanced to display important events filter from the last 24 hours and the last 7 days in a graphic form.

To switch to the legacy Dashboard,

1. Go to **User Preferences** > **Other Settings**.
2. Select the **Switch to classic dashboard** option, and click **Save**.

This option is displayed for global administrators only.

Topics:

Enhanced Dashboard user interface

The **Dashboard** user interface is enhanced to display the **Alerts**, **Events**, **Non-Compliance status**, **Jobs**, **Remote Connections**, and cloud storage summary in a pie chart form.

The eMMC health status for ThinOS 9.x devices and recovery partition changes for Dell Hybrid Client are added.

The jobs summary is enhanced to provide a view of all the jobs and wave jobs status. The **Events** section is enhanced to display the important events filter along with the last 24 hours and the last 7 days in a graph form.

To switch to the legacy **Dashboard**, go to **User Preferences** > **Other Settings**, select the **Switch to classic dashboard** option, and click **Save**. This option is only available for global administrators.

ⓘ **NOTE:** The Remote Connection data that is displayed on the **Dashboard** is the VDI connection data that is received from the ThinOS device during the check-in. Only the active VDI connection count at the time of check-in is displayed on the **Dashboard**. Any connection that is made and disconnected before check-in time is not displayed on the **Dashboard** or the **Device Telemetry** tab in the **Device Details** page.

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**.
2. In the **Events** section, click **View All Events**.
   The **Events** page is displayed with list of all the events.

View the certificate expiry details

From Wyse Management Suite 4.1, you can view the certificate expiry details for ThinOS 9.x devices on the **Dashboard** page. You can view the details of the certificate that are already expired or going to expire.

Steps

1. Click **Dashboard**.
2. In the **Certificate** section, you can view the expiring and expired certificate details.

   You can also view the certificate expiry details in the **Other Device Alerts** section.

View the vulnerable devices on the Dashboard

You can view the number of vulnerable devices on the **Dashboard**. The **Security Compliance** tab displays the number of vulnerable devices.

Steps

1. Click the **Security Compliance** tab.

   The vulnerable devices with the alert type, device details, and the description of the vulnerability.

2. Optionally, you can click the **Click here to know how to resolve the security alerts** option to understand the process to resolve the vulnerability.

   The device type, security alert, and the resolution are displayed.
3. Click the **here** hyperlink in the **Security Resolution** column to go to the relevant Dell support page where you can download the latest firmware and agent based on the platform type.

View the device status

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

Steps

1. Click **Dashboard**.
2. In the Devices section, 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

Enrollment validation controls the auto-registration of devices and into specific groups.

About this task

You can enable or disable enrollment validation using the following steps:

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**.

Recovery partition status for Dell Hybrid Client

The **Dashboard** displays the Dell Hybrid Cloud device count based on the Recovery partition status.

When you click the count, you are redirected to the **Devices** page and the respective device list is displayed. The Recovery partition status filter is also added in the **Devices** page.

In the **Device Details** page, the **Recovery partition status**, **Impacted file count**, and **Last Hash time** values are displayed under the **System Info** tab.

The following table describes the categorization of the recovery partition status on the Dashboard:

Table 6. Categorization of the recovery partition status

Status	Description
Major	Any changes that are related to DHC in recovery partition or if three or more directories are affected in recovery partition.
Minor	Any other changes
No change	If there are no changes to the recovery partition.
Recovery is not found	Recovery partition is not available in the DHC client.

eMMC status for ThinOS devices

The **Dashboard** is enhanced to display the eMMC status with the device count. You can hover the mouse on the eMMC field on the **Dashboard** to view the device count of the devices with the eMMC status.

When you click the count of the eMMC status, you are redirected to the **Devices** page and the respective device list is displayed. The eMMC status filter is also added in the **Devices** page.

In the **Device Details** page, the **eMMC Life Time** and **eMMC Cache Pre End of Life** values are displayed under **System Info** tab.

ⓘ **NOTE:** **Enable eMMC Disk Lifetime Configuration** must be enabled for the devices from ThinOS 9.x Config user interface on the device group or device level.

ⓘ **NOTE:** If the eMMC status in the server is displayed as **Urgent**, then the administrator should contact Dell support.

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 8.x**
  - **ThinOS 9.x**
- **WinIoT**
  - **WinIoT (WES)**
  - **WinIoT 2.x**
- **Linux**
- **ThinLinux**
- **Wyse Software Thin Client**
- **Edge Gateway**
- **Embedded PC**
- **Dell Hybrid Client**
  - **Dell Hybrid Client 1.x**
  - **Dell Hybrid Client 2.x**
- **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.

Topics:

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 or any parent group.
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 **Enable Device Exception To Override Select Group Policy** if you want the device exception policies to override the select group policies.

   This option is available only for a Parent Select group and is not available for the default device policy group or any custom device policy group.
6. 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.

   These steps are optional.
7. Click **Save**.

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

   To add subgroups 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 groups, and you can register the devices to the 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 subgroups require a client reboot for the 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.

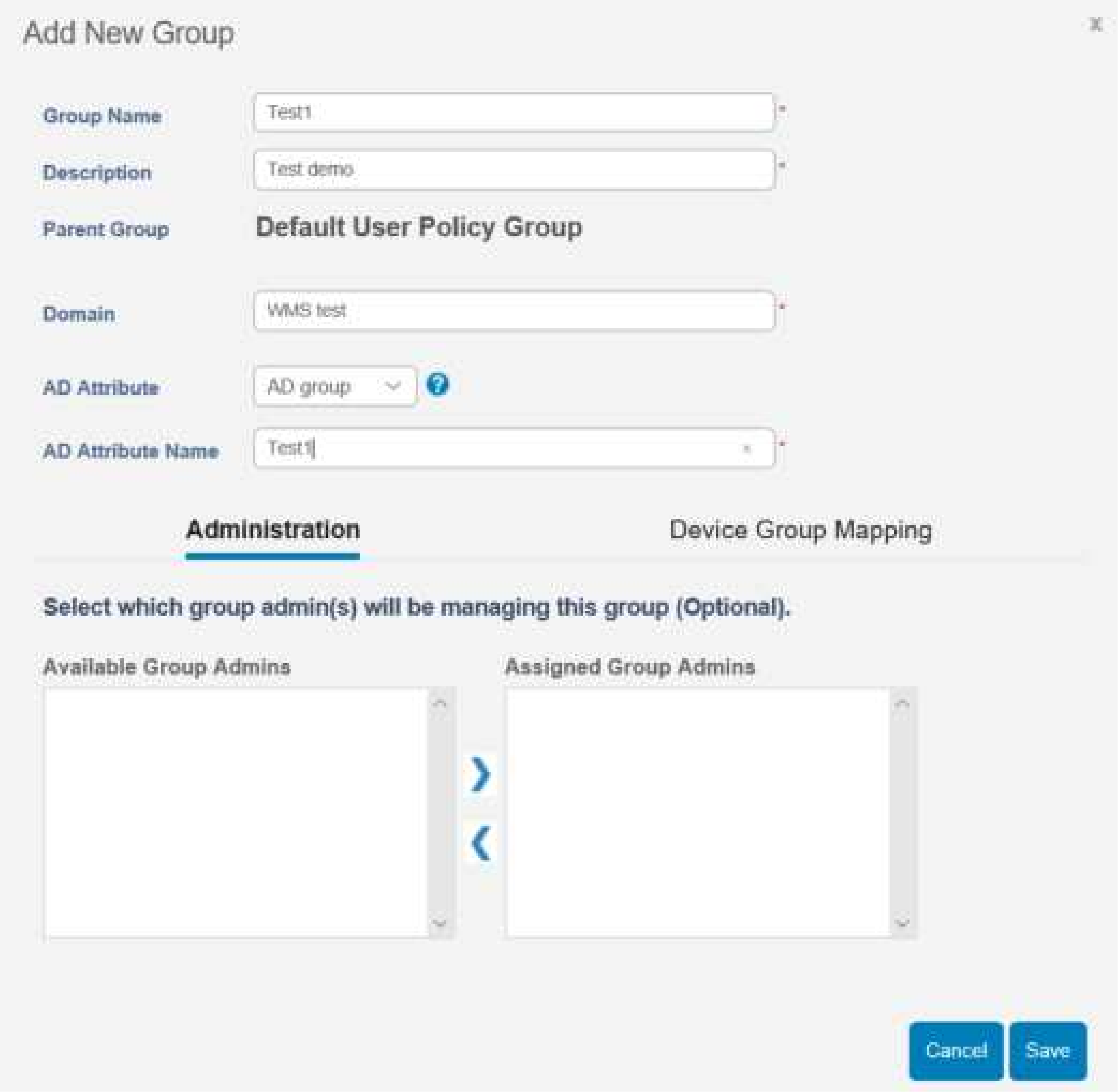
   > ⓘ **NOTE:** When you delete the select group, the devices of removed group cannot be moved to another select group.

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**.



Add New Group

Group Name: Test1 *

Description: Test demo *

Parent Group: Default User Policy Group

Domain: WMS test *

AD Attribute: AD group

AD Attribute Name: Test1 *

Select which group admin(s) will be managing this group (Optional).

Figure 3. 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.

   > **NOTE:** Select Group is not supported in Device Group Mapping.

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 configuration policy

Steps

1. Click **Devices**.
2. Apply the filters to find the specific device.
   The specified device list is displayed.
3. On the **Device Details** page, click **Summary** tab.
   The device summary is displayed.
4. In the **Device Configuration** section, click **Create/Edit Exceptions** to create or edit a device level exception, and configure a particular device policy.

   > **NOTE:** The device level configuration policies do not override the application policies.

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 8.x policy settings

Steps

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **ThinOS 8.x**.
   The **ThinOS 8.x** page is displayed.
4. After configuring the policy settings, click **Save and Publish**.

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.

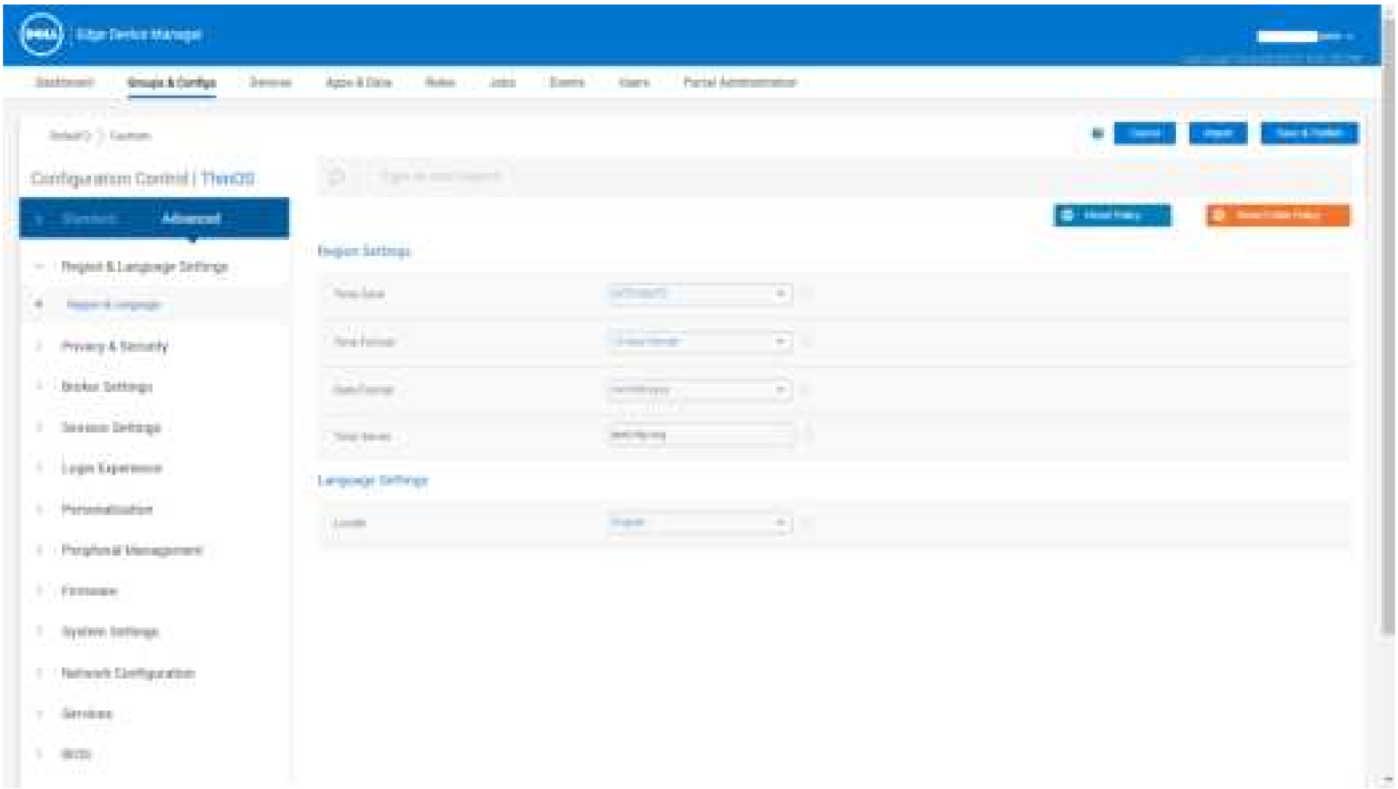


Figure 4. Configuration Control | ThinOS

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 Dell | Support.

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

   ⓘ **NOTE:** The policy configurations with reference files 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 page

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**.
   The application packages are listed in the respective fields.
5. Select the applications and use the slider to install or uninstall the application.
6. Click **Save & Publish**.
   The thin client restarts and the application package is installed or uninstalled.

Sync BIOS admin password for ThinOS 9.x devices from Groups & Configs page

Steps

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 9.x**.
3. The **Configuration Control | ThinOS** window is displayed.
4. Click **Advanced**.
5. In the **BIOS** field, select the platform.
6. In the **Security** section, configure the BIOS Admin password.
7. Click **Save & Publish**.

Upload and push ThinOS 9.x firmware packages using Groups and Configs page

From Wyse Management Suite 4.4, you can define multiple ThinOS firmware images and configure them to be installed in a sequence based on the ThinOS image build number. When multiple firmware builds are defined, you can only upgrade the firmware. The firmware is downgraded only if a single firmware is defined. This feature is supported for ThinOS firmware 2405 and later versions and the ThinOS Config UI package that is released with 2405 version.

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** section, select **OS Firmware Updates**.
5. From the **Firmware Update Logic** drop-down menu, select any of the following options to define when the device should attempt to apply new firmware when defined through the management policy:
   - **Any different firmware**
   - **New firmware only**
6. Select the different firmware that you want to deploy.
7. In the **Priority** field, assign the priority based on which the firmware should be deployed.
8. Click **Save & Publish**.

Edit the Windows 10 Thin Clients legacy policy settings

Steps

1. Click **Groups & Configs**.
   The **Groups & Configs** page is displayed.
2. Click the **Edit Policies** drop-down menu.
3. Click **Win10IoT (WES)**.
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 7. Remote Connections Chromium Browser

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

Configure Azure Virtual Desktop for Windows Embedded Devices

Steps

1. Go to the **Groups & Configs** page, and select a group.

2. From the **Edit Policies** drop-down menu, click **WES**.
3. Click **Azure Virtual Desktop**.
4. Click **Configure this item**.
5. Enter the connection name and server address.
6. Optionally, click **Add Policy** if you want to configure more than one connection.

   ⓘ **NOTE:** You cannot configure two Azure Virtual Desktop connections with the same name.

7. Click **Save & Publish**.

Edit the Win10 IoT 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 **WinIoT 2.x**.
   The **Configuration Control | WinIoT 2.x** window is displayed.
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:** 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 Windows 10 IoT configurations, see *Windows 10 IoT Administrator's Guide and Release notes* at Dell | 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.

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 8. 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

Table 8. Hybrid Client policy settings (continued)

Feature	Sub feature—User policy group	Sub feature—Device policy group
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
		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 Dell | 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 Dell | 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 Hybrid Client 2.x policy settings

Prerequisites

- Create a group with a group token for the devices that 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 **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** 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: 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.

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

   For information about the changes or updates to the Dell Hybrid Client configurations, see *Dell Hybrid Client Administrator's Guide and Release notes* at Dell | Support.

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 9. 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": {
        "F7TQ3P2": {
            "parameters": {
                "TerminalName": {
                    "value": "Test"
                },
                "vmwareAutoConnectList": {
                    "value": "vm9999"
                },
                "DHCPVendorID": {
                    "value": "Gyomu-200"
                },
            "DirectRDPCollection": {
            "values": [
              {
                "sequence": 1700463704675,
                "parameters": {
                  "DirectRDPFullscreen": {
                    "value": "no",
                    "updatedAt": "1700465732777"
                  },
                  "DirectRDPUsername": {
                    "value": "administrator",
                    "updatedAt": "1700463704701"
                  },
                  "DirectRDPAddress": {
                    "value": "192.168.1.119",
                    "updatedAt": "1700463704701"
                  },
                  "DirectRDPDomain": {
                    "value": "thegs.in",
                    "updatedAt": "1700463704701"
                  },
                  "DirectRDPDescription": {
                    "value": "wms",
                    "updatedAt": "1700463704701"
                            }
                        }
                    },
                    {
                        "sequence": 1705450533826,
                        "parameters": {
                            "DirectRDPAddress": {
                                "value": "10.192.64.241:13389",
                                "updatedAt": "1705450533852"
                            },
                            "DirectRDPDomain": {
                                "value": "FUEFUKI",
                                "updatedAt": "1705450533852"
                            },
                            "DirectRDPDescription": {
                                "value": "DST001C",
                                "updatedAt": "1705450533852"
                            }
                        }
                    }
                ]
            }
        }
 }
   }
}
```

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, DNS, subnet, platform, time zone, device tag, IP type or BIOS version.

You can sort the device list based on the following:

- Name
- Device tag
- Compliance
- Platform type
- Operating system type
- Operating system version
- Serial number
- IP address
- Last user details
- Group details
- Last check-in time
- Health
- 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.

Topics:

- 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
- Remote shadowing ThinOS devices from Wyse Management Suite public cloud
- Configure remote shadow connection for Dell Hybrid Client devices
- Shutting down devices
- Tag a device
- Edit or delete device tags
- 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
- Initiate Unified Write Filter servicing mode for Windows Embedded Standard device
- View the missing QFE details
- View the eMMC status of ThinOS devices
- Roll back to the last known configuration for ThinOS devices
- View the telemetry data for ThinOS devices
- View the recovery partition status
- Roll back to the last known good configuration for ThinOS devices
- Telemetry data for all 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 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 must authenticate to open the Dell Client Agent (DCA) window and register the device to Wyse Management Suite.

Steps

1. Log in to Dell Hybrid Client as a guest user. By default, the username is `guest` and there is no password by default for `guest` username.
2. Configure the following options:
    a. On the top bar, click

       (**System Information** icon).

       The **System Information** window is displayed.
    b. In the **Hardware** section, note the serial number of the device. This acts as the default password to launch Dell Client Agent. The password is case-sensitive.
    c. Click the **Show Application** icon on the desktop screen.

       The **Applications Overview** screen is displayed.
    d. Click the **Device Settings** icon.

       The **Device Settings** pane is displayed.
    e. Click **Dell Client Agent**.

       The **Authentication Required** window is displayed.
    f. Enter the serial number of the device and click **Authenticate**.

       Upon successful authentication, the **Dell Client Agent** window is displayed.
3. Click **Registration**.
   The default status is displayed as **Discovery In Progress**.
4. To register manually, click the **Cancel** button.
5. In the **WMS Server** field, enter the URL of the Wyse Management Suite server.
6. 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.

7. 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.
8. Click **Register** to register your hybrid client 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:** Once the device is registered, the password to launch Dell Client Agent will be set to the system password (Grub password).

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

   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**.
9. Log in to Wyse Management Suite.
10. Add the device to your wanted group (optional).
11. Configure the thin client using any of the following options:
    - Using the **Groups and Configs** page.
    - Using the **Devices page**.

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.

   NOTE: If the Wyse Device Agent window is not displayed, you must enter `Dtcwdaui.exe` in the **Windows** search bar.

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.

Register devices using secure DNS record fields or secure DHCP scope options

From Wyse Management Suite 3.5, you can register devices by using secure DNS record fields or DHCP scope options.

About this task

You can register devices with the Wyse Management Suite server if the DNS record fields or DHCP scope options are set using the following values:

- DNS SRV record fields:
  - _WMS_MGMTV2
  - _WMS_GROUPTOKENV2
- DHCP scope options:
  - WMS URL - 201
  - Group Token - 202

Steps

1. Go to **Portal Administration** > **Console Settings** > **WMS Discovery**.
2. Enter the group token.
3. Select the discovery type from the **Discovery Type** drop-down list.
4. Click **Generate Details**.
   The encrypted WMS URL details and the group token is displayed.

   ⓘ **NOTE:** If the Wyse Management Suite certificate is changed, the secure DNS and DHCP code must be recreated to register a new device.

Registering devices by using legacy DHCP option tags

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

Table 10. Registering device by using legacy 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

Table 10. Registering device by using legacy DHCP option tags (continued)

Option Tag	Description
	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.
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 legacy 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 11. 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.

Table 11. Configuring device by using DNS SRV record (continued)

URL/Tag	Description
	ⓘ **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. 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.

Device compliance status

You can view the device compliance details on the **Devices** page. You can hover over the **Compliance** column to view more details about the status.

The following table provides information about the device status:

Table 12. Device status details

Color code	Device status
Red	The device has not sent its heartbeat for more than three attempts (three hours).
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.

The following table provides information about the compliance status:

Table 13. Compliance status details

Color code	Device is using vulnerable hash	Device is having other compliance issue* other than vulnerable hash
Green	No	No
Yellow	Yes	No
Red	No	Yes
Red	Yes	Yes

NOTE: * indicates any of the following compliance issues:

- **Device not checked-in**—Device not checked-in for more than the days defined for **Not Checked In compliance alert** in **Portal Administration** > **Other Settings**.
- **Device using vulnerable hash**—Device using MD5 and SHA1 as hashing algorithm.
- **DHC system password not changed**—Dell Hybrid Client devices for which the system password is not changed.
- **DHC BIOS password not changed**—Dell Hybrid Client devices for which the BIOS password is not changed.

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
   - **Non-Compliant**
     - All Non-Complaint Devices
     - Device not checked-in
     - Device Vulnerable hash
     - DHC System Password not changed

    - DHC BIOS Password not changed
  - **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
   - **Generic Client**
     - Generic 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 **Manufacturer** drop-down list, select the device manufacturer.
7. From the **OS Version** drop-down list, select an operating system version.
8. From the **Agent Version** drop-down list, select an agent version.
9. From the **Subnet/prefix** drop-down list, select a subnet.
10. From the **Timezone** drop-down list, select the time zone.
11. From the **Device Tag** drop-down list, select the device tag.
12. From the **IP Type** drop-down list, select the IP type.
13. From the **BIOS version** drop-down list, select the BIOS version.

View and resolve vulnerabilities in devices

Steps

1. Click Devices.

   The **Devices** page is displayed.
2. From the **Status** drop-down filter, select **Device Vulnerable Hash** in the **Non-Compliant** section.

   The devices with the vulnerability are displayed.
3. Click the device hyperlink.

   In the **Device Details** page, the alert type, device details, and the description of the vulnerability is displayed.
4. Optionally, you can click the **Click here to know how to resolve the security alerts** option to understand the process to resolve the vulnerability.

   The device type, security alert, and the resolution are displayed.
5. Click the **here** hyperlink in the **Security Resolution** column to go to the relevant Dell support page where you can download the latest firmware and agent based on the platform type.

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. Locate the device that you want to view details for and click it.
   The **Device Details** page of the selected device is displayed.

Save the filter in Devices page

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

Steps

1. After specifying the filters, click the **Save** button in the bottom right of the filter pane.
2. Enter the **Name** of the filter.
3. Provide a description for the filter in the **Description** box.
4. Select the check box to set the current filter as the default option.
5. Click **Save Filter**.
   A drop down box allowing you to switch between saved filters is displayed next to the **Save** button.

Clear Unused and Inactive Filters

Steps

1. Click **Devices**.

   The **Devices** page is displayed.
2. Click the **Clear Filters** option.
3. From the **Clear Filter** drop-down list, select any of the following options:
   - **Subnet**
   - **Timezone**
   - **Device Tag**
   - **Platform**
   - **Agent Version**
   - **OS version**
   - **BIOS version**
   - **DNS**
4. Click **Yes**.
   An alert message is displayed.
5. Click **Yes**.
   A job is created to clear the selected filter, and also an event is created.

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. Use search of filters to locate the device.
3. Select the check box next to 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. Use search of filters to locate the device.
3. Select the check box next to 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 the Cloud Management Suite.

Steps

1. Click **Devices**.
   The **Device** page is displayed.
2. Use search of filters to locate the device.
3. Select the check box of the device.
4. Click **Unregister**.
   An **Alert** window is displayed.
5. Select the **Force Unregistration** check box.

   NOTE: Select the **Clean Policies** option if you want to clear the policies applied to the device via CMS.

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.

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.

Soft reset of ThinOS 9.x devices

You can soft reset ThinOS 9.x devices if you do not want to completely reset the device. You can reset the device to clear all configurations except network settings such as DNS, wireless, proxy, and VPN settings, and certificates. The device is not unregistered from when you use the option.

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 **Soft Reset**.
5. Enter a reason for soft reset.
6. Click **Send Command**.

   ⓘ **NOTE:** You can also perform soft reset from the **Device Details** page. You can also schedule the option from the **Jobs** page.

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.

Sync BIOS admin password

You can use the **Sync BIOS admin password** option to update the Device BIOS password in the Wyse Management Suite application. When you deploy a configuration the next time, the password that is entered using this option is used as reference by the device for the current BIOS administrator password. This is required on the device to update the BIOS configurations that are deployed from Wyse Management Suite.

You can perform this action using any of the following options:

- On a single device from the **Devices** page—see Sync BIOS Admin Password from Devices page.
- On a group of devices from the **Jobs** page—see Sync BIOS admin password from Jobs page.
- On ThinOS 9.x devices from the **Groups & Configs** page—see Sync BIOS admin password for ThinOS 9.x devices from Groups & Configs page.

Sync BIOS admin password from Devices page

Steps

1. On the **Devices** page, click the device.
2. From the **More options** drop-down list, select the **Sync BIOS Admin Password** option.
   The **Sync BIOS Admin Password** window is displayed.
3. Enter the password. The password must be a minimum of 4 and a maximum of 32 characters.
4. Optionally, select the **Show Password** check box to view the password.
5. Click **Save**.

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 display parameters

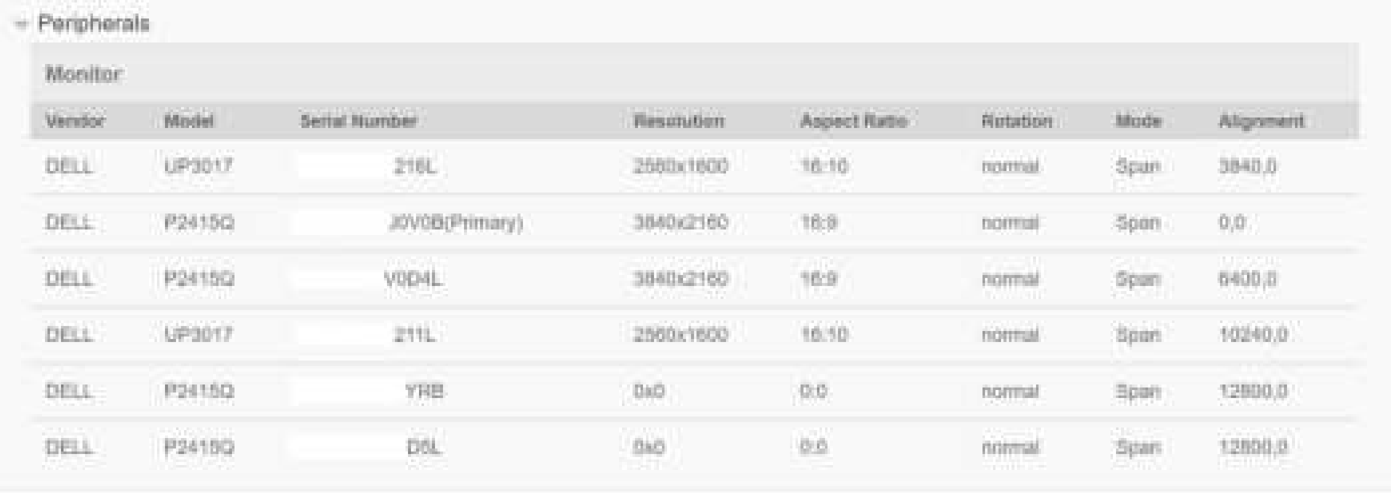
From Wyse Management Suite 3.1, you can view the display setup of the devices running a Windows Embedded and ThinLinux operating system. You can view the vendor name, model number, serial number, resolution, aspect ratio, mode, alignment, and rotation details of the display setup.

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	[redacted] 216L	2560x1600	16:10	normal	Span	3840,0
DELL	P2415Q	[redacted] J0V0B(Primary)	3840x2160	16:9	normal	Span	0,0
DELL	P2415Q	[redacted] V0D4L	3840x2160	16:9	normal	Span	6400,0
DELL	UP3017	[redacted] 211L	2560x1600	16:10	normal	Span	10240,0
DELL	P2415Q	[redacted] YRB	0x0	0:0	normal	Span	12800,0
DELL	P2415Q	[redacted] D6L	0x0	0:0	normal	Span	12800,0

Figure 5. Display parameters

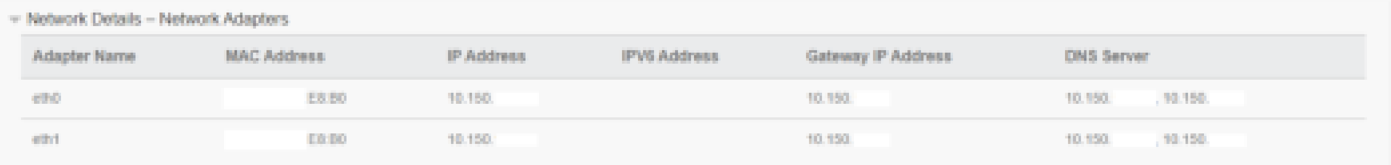
View the virtual NIC details

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.



Network Details – Network Adapters

Adapter Name	MAC Address	IP Address	IPV6 Address	Gateway IP Address	DNS Server
eth0	[redacted] E8:B0	10.150.[redacted]		10.150.[redacted]	10.150.[redacted], 10.150.[redacted]
eth1	[redacted] E8:B0	10.150.[redacted]		10.150.[redacted]	10.150.[redacted], 10.150.[redacted]

Figure 6. 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. You can also view the alerts such as devices not checked in, device expiration details for ThinOS 9.x devices, and so on, in the **Alerts** section.

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** to add a personal note about the device.
   An **Add Note** window is displayed.
4. Type the message in the provided field and click **Save**.
5. Optionally, 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. Optionally, 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. You can view the hardware, operating system, network, peripherals, and BIOS setting details of the selected device. From Wyse Management Suite 4.1, you can view the ethernet speed of registered ThinOS 9.x devices.

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.

Remote shadowing ThinOS devices from Wyse Management Suite public cloud

The administrator can remote shadow ThinOS devices at home and office environment from the Wyse Management Suite public cloud. You can view the complete device desktop and use the keyboard or mouse for remote debugging. The configurations for the remote shadow are defined from the **Groups & Configurations** page.

Steps

1. Click **Devices**.

   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the device.
   The **Device Details** page is displayed.
4. From the **More Action** drop-down menu, click **Remote Shadow (P2P)** .
   An alert window is displayed.
5. In the alert window, select the end user acceptance option to connect to the device remotely after the end user accepts the request.

   If the option is not selected, you can connect directly to the device.
6. Click **Ok**.

   NOTE: If the device is in sleep or shutdown mode, then the remote shadow session cannot be established. In this case, the remote shadow browser closes automatically after two minutes.

   NOTE: A remote shadow session can run for 20 minutes. After 20 minutes, the device is disconnected automatically. You must reestablish the connection with the device. Also, if there is no activity that is done on the device, a remote shadow session disconnects automatically after five minute idle time.

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**.

Edit or delete device tags

You can edit the tag names individually or in bulk. You can also delete the tags associated with the devices.

Steps

1. Click **Devices**.
   The **Devices** page is displayed.
2. Apply the filters to locate the preferred device.
   The preferred device list is displayed.
3. Select one or more devices.
4. From the **More Actions** drop-down list, click **Edit DeviceTag(s)**.
   The **Edit DeviceTag(s)** window is displayed.
5. Select one or more device tags and edit the name as required.
6. Click **Save**.
7. To delete the device tags, select one or more device tags and click **Delete**.

Pulling Windows Embedded Standard or ThinLinux image

Prerequisites

- If you are using Wyse Management Suite 1.3 remote repository, then **Recovery/ Recovery + OS pull** templates 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**

            ⓘ **NOTE:** OS and BIOS options are disabled for the devices with DELL BIOS.
        - When the **Advanced** pull type is selected, a drop-down list for selecting the templates is displayed. Select any template which is available by default.

            ⓘ **NOTE:** You can use the custom templates 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 devices upload Wyse Device Agent logs and Windows Event viewer logs. Linux or ThinLinux devices upload Wyse Device Agent logs and system logs. ThinOS devices upload network trace details and core dump along with configured repositories. You can define the log size for ThinOS devices in **Portal Administration** > **Other Settings**.

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. Click **Send Command**.

   ⓘ **NOTE:** For ThinOS 9.x devices, you can request additional log details by selecting the **Network Trace** or **Core Dump** options.

   ⓘ **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. You can select the **Enable Apply on Check-in Policies after Reimage** if you want to apply the configured standard or advanced policies after the reimage of the device.

   ⓘ **NOTE:** If the **Apply the policy to devices on check in** option is configured, selecting the checkbox applies the policy. Also, if no application policy is configured and the checkbox is selected, no application is installed on the client.
6. 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.

   The CSV file size must not exceed 10 MB.
5. From the **Select a new group for these devices** drop-down list, select the new group for the devices.
6. Click **Save**.
   You can change the group of a maximum of 100 devices at a time.

   ⓘ **NOTE:** From Wyse Management Suite 4.1.1, you can change the group of a maximum of 10,000 devices at a time.

Initiate Unified Write Filter servicing mode for Windows Embedded Standard device

Steps

1. Click the **Devices** tab.

   The **Device** page is displayed.
2. Apply the filters to find the preferred device.
3. Select the check box of the device.
4. Click **Initiate UWF servicing mode**.
   An alert window is displayed.
5. Click **Send Command**.

View the missing QFE 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.
4. Expand the **Operating System Details**.
   The **Missing QFE Updates** information is displayed.

View the eMMC status of ThinOS devices

Steps

1. Go to the **Devices** page, and click a ThinOS device.
2. In the **Device Details** page, click **System Info**.
   You can view the **EMMC Life Time** and **EMMC Cache Pre End Of Life** details.

   If the eMMC status is displayed as **Urgent**, then you must reach out to Dell Support and change the eMMC or motherboard.

Roll back to the last known configuration for ThinOS devices

You can roll back ThinOS devices running version 2402 to the last known good configuration. You can also create a custom administrator with and without this permission to perform a rollback to the last known good configuration.

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 **Rollback To Last Known Good Configuration**.
5. Click **Send Command**.

   ⓘ **NOTE:** After the device rolls back to the last known good configuration, you must suspend the policy update till the administrator makes a new policy change to push the latest policy to the device again.

View the telemetry data for ThinOS devices

You can view the telemetry data such as **Overall Device Health & Alerts**, **Remote Connections**, and **Client Information** of ThinOS devices.

Steps

1. Go to the **Devices** page, and click a ThinOS device.
2. In the **Device Details** page, click **Telemetry**.
   You can view the telemetry data for the device.

View the recovery partition status

Steps

1. Go to the **Devices** page, and click the Dell Hybrid Client device.
2. In the **Device Details** page, click **System Info**.
3. Expand the **Recovery Partition** field to view the status.

   The following table describes the categorization of the recovery partition status:

Table 14. Categorization of the recovery partition status

Status	Description
Major	Any changes that are related to DHC in recovery partition or if three or more directories are affected in recovery partition.
Minor	Any other changes
No change	If there are no changes to the recovery partition.
Recovery is not found	Recovery partition is not available in the DHC client.

Roll back to the last known good configuration for ThinOS devices

Rollback to last known good configuration option is provided in the **Devices**, **Device Details**, and **Jobs** page.

To view the option, go to the **Devices** page, select any of the ThinOS 9.x devices (2402 and later versions) and select the **Rollback to Last Known Good Configuration** option from the **More Action** drop-down list.

The command can be scheduled for a group of devices from the **Jobs** page using the **Schedule Device Commands** option.

After the device rolls back to the last known configuration, the device suspends the policy update till the Wyse Management Suite administrator creates a policy change to push the latest policy to the device again. For more information, see*ThinOS 2402 Administrator's Guide* at Dell | Support.

Telemetry data for all devices

The **Telemetry** tab is added in the **Device details** page for all thin client devices. The **Telemetry** tab displays complete information of device non-compliant reasons, active remote connections information, and the device asset data.

NOTE: The remote connection data is displayed only for ThinOS 9.x devices and is not displayed for other thin clients.

NOTE: The device **Telemetry** tab is not applicable and is not displayed for Teradici and Wyse Software thin clients.

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 types 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 seconds.

ⓘ **NOTE:** From Wyse Management Suite 4.2, you can filter the uploaded files based on the repository.

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/f/p=Fireport`** as install parameters to update BIOS.

    ⓘ **NOTE:** If you are using bitlocker on your Windows system, you can update BIOS using the standard application policy. You must use **`/s/bls/f/p=<BIOS Admin Password>`** 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 or 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 one or more groups.

   NOTE: You can select up to 100 groups for each policy.

8. Select the **Include All Subgroups** check box to apply the policy to sub groups.

   NOTE: When you select multiple groups:

   - **Exceeded maximum number of groups allowed in a policy** message is displayed and the policy creation is blocked when you select more than 100 parent groups or sub-groups.
   - The administrator must select **Include sub-groups** option, if sub-groups must be included in the advanced application policy.
   - The sub-groups selection is not displayed when **Include sub-group** option is selected. However, individual jobs for all parent and sub-groups are created when the policy is scheduled.
   - The policy cannot be scheduled immediately if the total number of applicable devices are more than 25. The administrator must schedule the policy later.

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. If you select this option, only the applications that are associated with the selected operating system type are displayed.
12. From the **Filter Devices** drop-down list, select any of the following options:

    NOTE: This option is applicable for Windows Embedded Standard operating system

    - Select the **Apply On All Devices** if you want to apply the policy to all the devices.
    - Select the **Filter already updated devices** if you do not want the previously deployed applications through Wyse Management Suite to be redeployed.
    - Select the **Filter devices with policy already applied** if you do not want to apply the policy to devices which have already received the same policy.

13. 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.

14. If you want the system to reboot after the application is successfully installed, select **Reboot**.
15. 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, the number of repositories is displayed next to the file name.
16. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Platform Filter**.
17. 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.
18. 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.

19. 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**.

20. 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 clients.
21. 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.

22. Click **Save** to create a policy.
    A message is displayed to enable the administrator to schedule this policy on devices based on group.
23. Select **Yes** to schedule a job on the same page.
24. 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.
25. To create the job, click **Preview** and schedules are displayed on the next page.
26. You can check the status of the job by going to the **Jobs** page.

    For more information about scheduling a job, see Schedule an application policy.

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.

You can also upload the applications using the **Add Package file** option in the **App Inventory** section.

ⓘ **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 **Manufacturer Filter** and **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 **Manufacturer Filter** and **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 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.
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.

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.
    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. 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.

17. 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.
18. 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.
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.

Add Dell Hybrid Client packages to the repository

Steps

1. Log in to Wyse Management Suite using your administrator credentials.
2. In the **Apps & Data** tab, under **App Inventory**, click **Hybrid Client**.
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 the operator account and it is visible to all the tenants. Tenants cannot delete or modify these files.

Add Generic Client packages to the repository

Steps

1. Log in to Wyse Management Suite using your administrator credentials.
2. In the **Apps & Data** tab, under **App Inventory**, click **Generic Client**.
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.

   ⓘ **NOTE:** The DCA-Enabler package can be uploaded from the Generic Client page.

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.

Add Windows Embedded Standard packages to the repository

Steps

1. Log in to Wyse Management Suite using your administrator credentials.
2. In the **Apps & Data** tab, under **App Inventory**, click **Thin Client**.
3. Click **Add WES 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.
5. Select the check box if you want to override an existing file.
6. Click **Upload**.

   ⓘ **NOTE:** If the QFE/KB package size is more than 1 GB, the large packages take up to 60 min to upload.

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

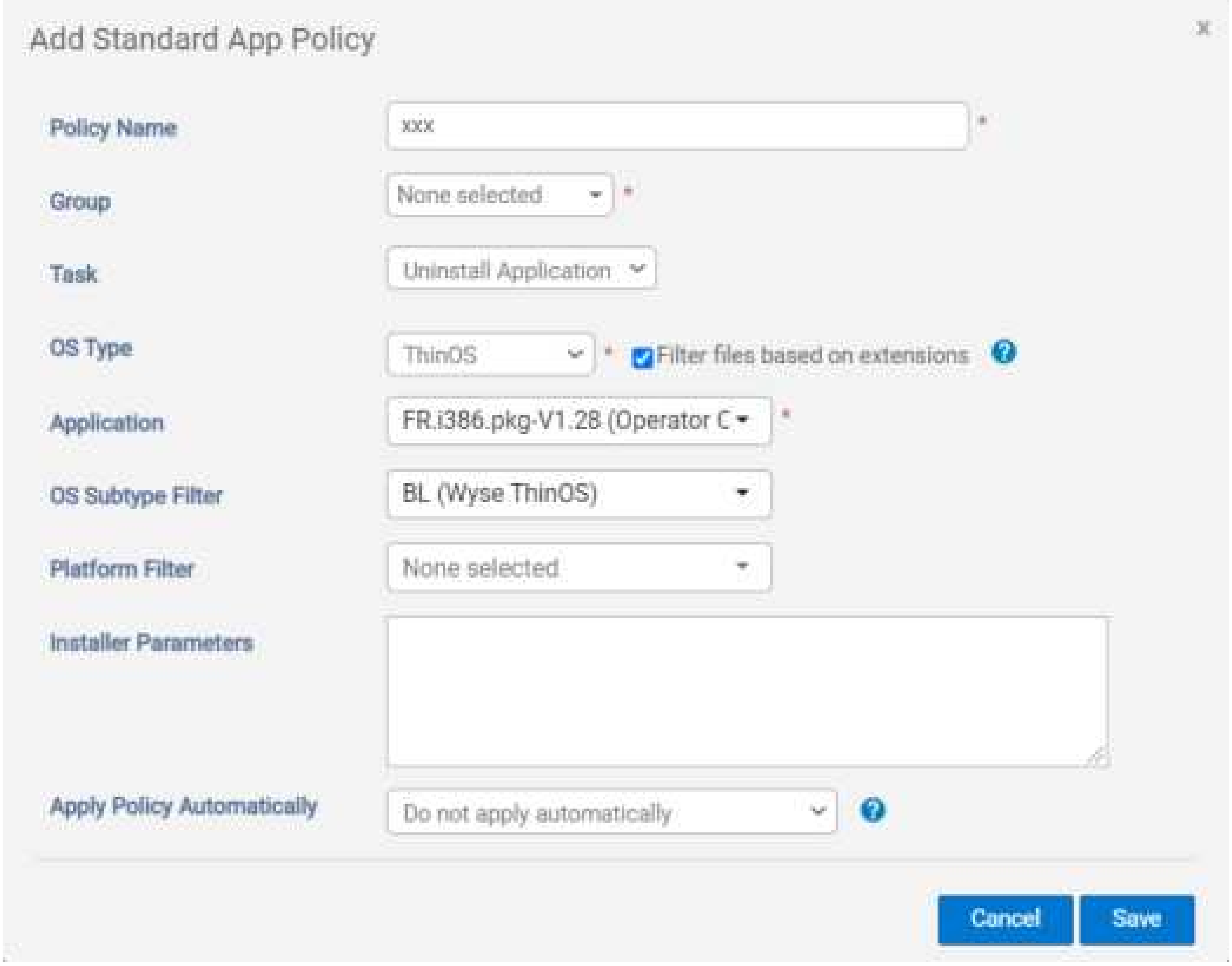
   ⓘ **NOTE:** The file is added to the repository when you select the check box but it is not assigned to any of the groups or devices. To assign the file, create or edit the application policy for the respective group.

Uninstall an application from the client using Wyse Management Suite

Steps

1. Create a policy to remove the package. To create a policy, do the following:
   a. Go to **Apps & Data** > **App Policies** > **Thin Client**.
   b. Click **Add Policy**.

      The **Add Standard App Policy** window is displayed.
   c. Enter the **Policy Name**.
   d. From the **Group** drop-down list, select the group of the device.
   e. From the **Task** drop-down list, select **Uninstall Application**.
   f. From the **Application** drop-down list, select the application that you want to remove.
   g. From the **OS Subtype Filter** and **Platform Filter** drop-down lists, select the filters.



Add Standard App Policy

Policy Name: xxx *

Group: None selected *

Task: Uninstall Application

OS Type: ThinOS * ☑ Filter files based on extensions

Application: FR.i386.pkg-V1.28 (Operator C *

OS Subtype Filter: BL (Wyse ThinOS)

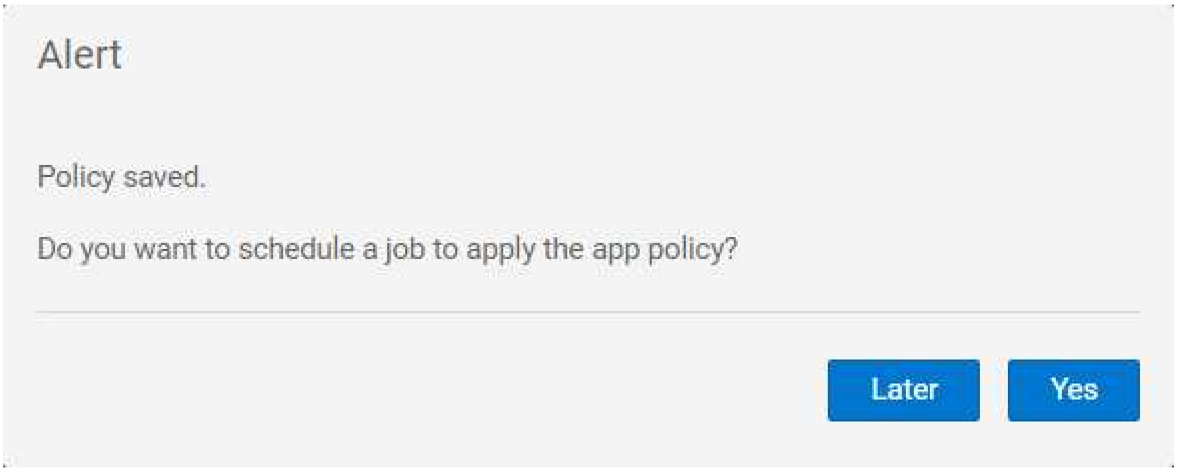
Platform Filter: None selected

Installer Parameters:

Apply Policy Automatically: Do not apply automatically

Figure 7. Add Standard App Policy

h. Click **Save**.
   An **Alert** window is displayed to schedule the app policy.



Alert

Policy saved.

Do you want to schedule a job to apply the app policy?

Figure 8. Alert window

i. Click **Later**.

2. Go to the **Devices** page and select the device from which you want to remove the package.
3. From the **More Actions** drop-down list, select **Schedule App Policy**.

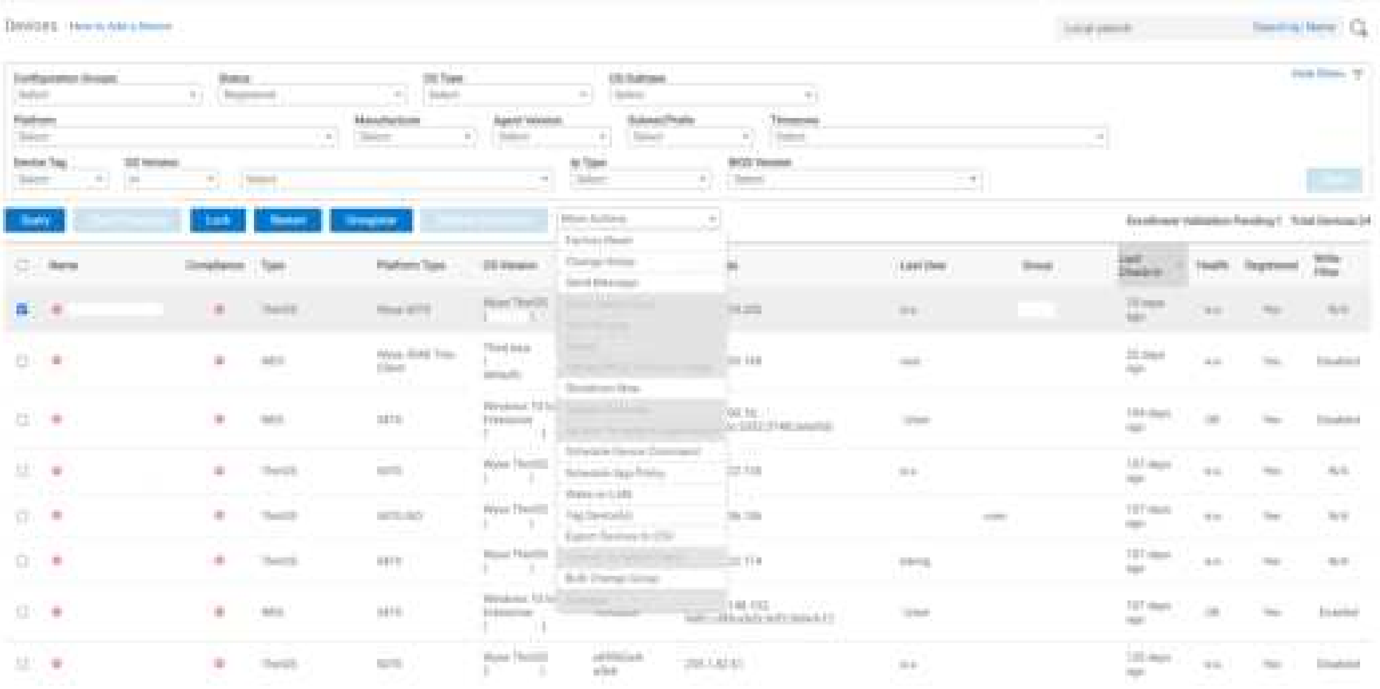


Figure 9. Devices page

The **App Policy Job** window is displayed.

4. From the **Policy** drop-down list, select the policy created to remove the application.
5. From the **Run** drop-down list, select **Immediately**.
6. Click **Preview** and then click **Schedule**.

   The application is removed from the client.

10

Managing waves

The administrator can schedule and deploy ThinOS firmware, BIOS, or application packages in a phased manner. This enables the administrator to test the new firmware, BIOS, or packages on selected devices before deploying to a larger group. You can create a wave with multiple phases for a single group or multiple groups. You can also select the devices based on your requirement using the filters. For example, if there is a group with 500 devices and a new ThinOS firmware must be deployed, the waves upgrade feature can be leveraged to create phases and deploy on firmware on selected 100 devices. This feature is based on Ring Deployment.

You must define a threshold for the success or failure of a phase. The next phase of deployment can be started based on the threshold of the earlier phase.

You can view the status of a wave on the **Dashboard**. The detailed summary of each phase is captured in the **Jobs** page.

This feature is available only in the Pro edition of Wyse Management Suite and is supported for devices running ThinOS 2311 and later versions only.

Topics:

Create a wave

Steps

1. Click **Waves**.
2. Click **Create Wave**.
   The **Waves** page is displayed.
3. In the **Create a Wave** section, do the following:
   - **Wave Name**—Enter the name for the wave.
   - **OS Type**—Select the operating system. ThinOS 9.x is the only supported operating system.
   - **Phase Dependency**—If you select this option, the phase starts when the defined threshold of the previous phase is attained.
   - **Auto merge & publish after completion**—If you select this option, then after completion of the phase you can merge the wave configurations to the main production group after all the phases meet the threshold criteria. An **Alert** window is displayed and if the **Auto merge & publish after completion** option is cleared when you are creating a wave, you can merge and publish the wave manually by going to the **Jobs** tab, selecting the specific wave job, and clicking the **Merge & Publish** button.

     Till the wave configuration is manually merged or rolled back, the devices receive the wave configurations. The wave job reschedule, and wave configuration **Edit** or **Delete** options are blocked. Also, select the **Publish this configuration to other devices in the group** option if you want to push the wave configurations immediately to all the devices in the main or production group.

   NOTE: The administrator must use the **Merge & Publish** option if the auto merge or rollback option is not enabled. Otherwise, the devices part of the wave still receives the wave configuration and the wave cannot be rescheduled.

4. In the **Defined Phases** section, do the following for Phase 1:
   - **Phase Name**—Enter the name for the phase.
   - **Threshold Type**—Set the threshold type to **Success** or **Failure** for the phase.

     If the success or failure percentage reaches the defined threshold percentage, then the next phase starts.

   - **Threshold for next phase to start (%)**—Enter the threshold percentage for the success or failure to be defined for the phase.

- **Select Groups**—Select a group to which the phase must be applied. You can select a parent group, a child group, or a select group.

  ⓘ **NOTE:** If the child group is selected in one of the phases, then the parent group cannot be selected in the next phase. The same rule applies for the select group as well.

  ⓘ **NOTE:** One phase can be tied to a single group.
- **Edit Wave Policies**—After you select the group, click **Edit Wave Policies** to configure the application, BIOS, or Firmware package deployments.
- **View Configuration Summary**—Click the **View Configuration Summary** option to view the summary of the application, BIOS, or Firmware package deployment configurations.
- **Filter Devices**—Configure the **Choose from saved device filters** or **Choose from CSV File** options to filter and select specific devices.
- You can also filter and select the devices from the **Device Tag**, **Platform**, **Hostname**, **Service Tag**, and **IP Address** filters. You can also create a CSV file with ID addresses and import the file to filter the devices.
- **View Targeted Devices**—Click **View Targeted Devices** to view the devices filtered for the phase. You can use the **Targeted Devices**, **Offline Devices**, and **Devices With Pending Jobs** tabs to find the targeted devices.

5. Click **Add a new phase** to configure the next phase and repeat the steps that are defined in Step 4.

   ⓘ **NOTE:** A wave can contain a maximum number of 10 phases.

6. Click **Save** after you configure the required phases.
   The created wave is displayed in the **Wave** page and the number of phases, status of the wave, and the configured **AutoMerge** options are displayed.

   You can then schedule the wave from the **Jobs** page. For information about how to schedule a wave, see Schedule a wave.

   You can also edit and delete the created wave later using the **Edit Wave** and **Delete Wave(s)** options on the **Waves** page.

   ⓘ **NOTE:** Wave configuration can be edited or deleted only when the wave is not scheduled.

Important notes on wave update

- Dell Technologies does not recommend adding new devices to a wave in a running phase. The devices are leveraging the configuration which cannot be altered. If you add any devices during this phase, it might create ambiguity in terms of percentage calculations and overall deployment.

- Offline devices are filtered out during wave deployment when a given phase starts. These devices are listed separately as **Offline Devices** in the **Jobs** page. After the completion of the wave deployment and the configurations are merged to main group configurations, notifications are sent to all the devices again. When the offline devices come back online, they check-in to Wyse Management Suite. The latest configuration which is merged from the wave configuration to the main group configuration is deployed to the devices.
- If the devices of a group are not selected in any of the phase configurations of the wave, they receive only the group configurations.
- Group configurations are not deployed to devices that are selected as part of a wave until the wave schedule is completed.
- When wave configurations are running on a device group, then the group configurations cannot be configured.
- If the wave policy job is scheduled while the group policy job is in-progress, then the wave policy configurations override the group policy configurations.

Improvements to wave upgrade

- **Enhanced View targeted device list in a wave**—The Wyse Management Suite administrator can view the targeted devices, offline devices, and devices with pending jobs while creating a wave using the **View Targeted Devices** button.
- **Support for IP address filter and import CSV with IP address during wave creation**—The Wyse Management Suite administrator can select the IP address of the devices using the **IP Address** filter during wave creation for targeted devices. Alternatively, the administrator can also import CSV with IP address while creating a wave.
- **Wave Phase scheduler**—The Wyse Management Suite administrator can schedule individual phases with different time zones after creating the waves or from the **Jobs** page.
- **Merge and Publish**—The Wyse Management Suite administrator can merge and publish the wave configurations to the main production group anytime irrespective of the wave status—running, completed as error, or completed as success.

- **Wave rollback**—The Wyse Management Suite administrator can rollback the wave configurations so that the devices receive the production group configuration. Rollback can be performed anytime irrespective of the wave status—running, completed as error, or completed as success.

ⓘ **NOTE:** The Wyse Management Suite administrator must perform either **Merge & Publish** or **Rollback** to edit or reschedule a wave. Devices receive the wave configuration till the wave configurations are merged or rolled back and the wave job cannot be rescheduled.

11

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**
- **Failed Check-In**

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. 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**.

Filter unmanaged device auto assignment rule

Steps

1. Click the **Rules** tab.
2. Select the **Unmanaged Device Auto Assignment** option.
3. Filter the rules based on subnet, location, and custom filter.

   The rules are displayed based on the selected filters.

   ⓘ **NOTE:** Group administrator can view and filter only rules that are created by global, custom, and custom group administrator. Viewer and custom viewer do not have permission to go to the **Rules** tab.

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**.

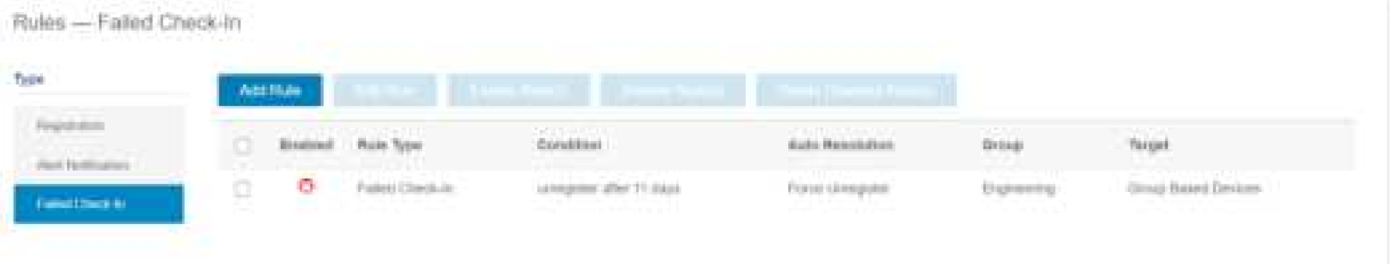
Create rule to auto-unregister a device

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.



Rules — Failed Check-In

Type

Registration

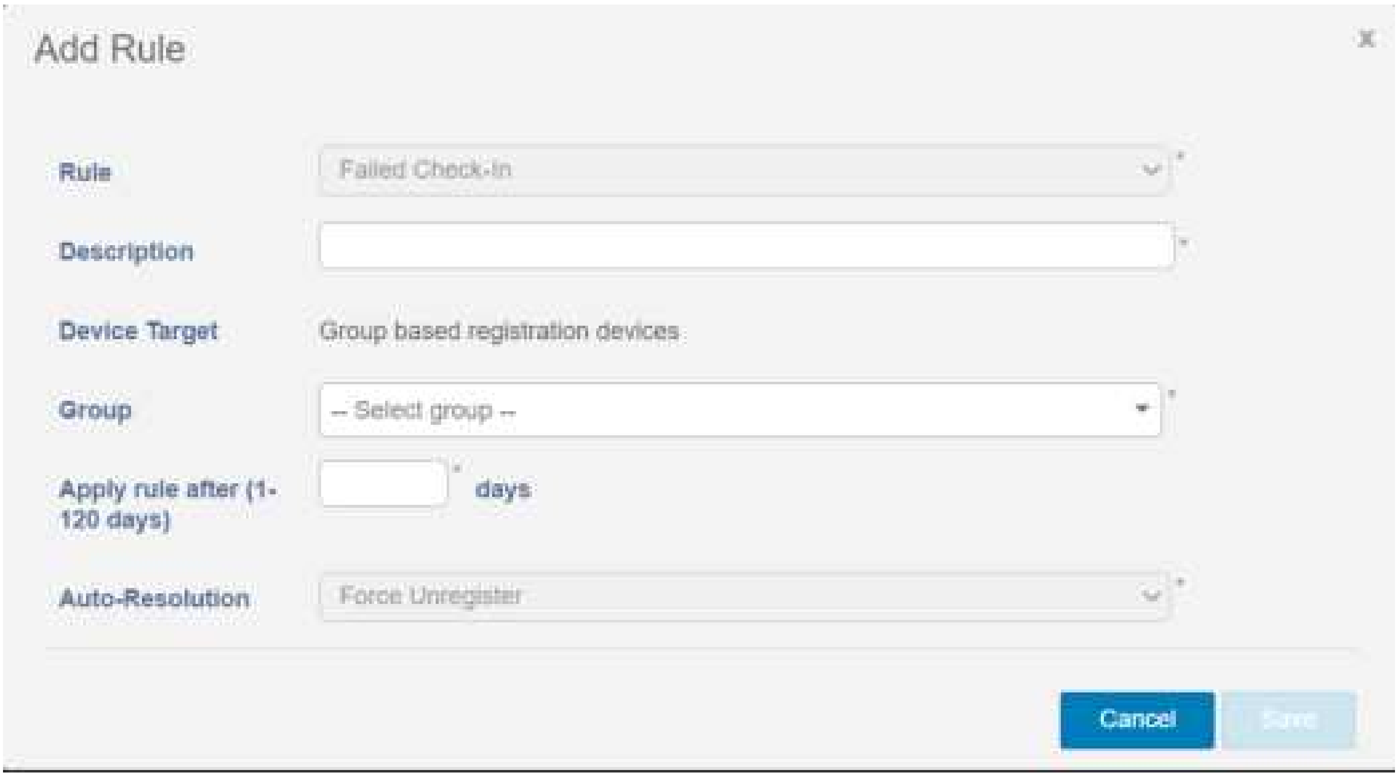
Alert Notification

Failed Check-In

□	Enabled	Rule Type	Condition	Auto Resolution	Group	Target
□	○	Failed Check-In	unregister after 11 days	Force Unregister	Engineering	Group Based Devices

Figure 10. Failed Check-In tab

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



Add Rule

Rule: Failed Check-In

Description:

Device Target: Group based registration devices

Group: -- Select group --

Apply rule after (1-120 days): days

Auto-Resolution: Force Unregister

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.

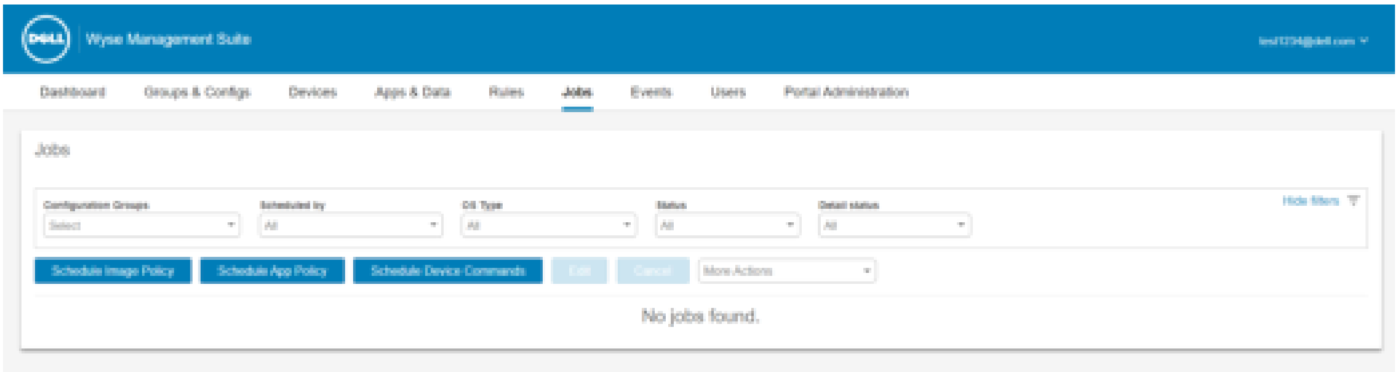
12

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.



Configuration Groups: Select
Scheduled by: All
OS Type: All
Status: All
Detail status: All

No jobs found.

Figure 12. Jobs page

Topics:

Sync BIOS admin password from Jobs page

You can use the **Sync BIOS admin password** option to update the Device BIOS password in the Wyse Management Suite application. When you deploy a configuration the next time, the password entered using this option is used as reference by the device for the current BIOS administrator password. This is required on the device to update the BIOS configurations that are deployed from Wyse Management Suite.

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. Optionally, 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**.

Bulk delete unregistered devices

The administrator can delete unregistered devices by creating a job.

Steps

1. Click **Jobs**.
   The **Jobs** page is displayed.
2. From the **More Actions** drop-down menu, select the **Delete Not Registered Devices** option.
   The **Schedule a Job** window is displayed.
3. Select the group from the drop-down list.
   To delete all the devices, select **Default Device Group** and **Include All Subgroups** check box.
4. Click **Preview** and then click **Schedule**.

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
- Initiate UWF Servicing Mode—Applicable for Windows Embedded Standard devices
- 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 **Run** drop-down list, select any of the options.
5. Select the **Exclude Offline Devices** if you want to exclude the offline devices while creating the job.

You can view the list of excluded offline devices on the **Jobs** page. You can later restart the job for the offline devices from the jobs list.

6. 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.
7. Click the **Preview** option to view the details of the scheduled job.
8. On the next page, click the **Schedule** option to initiate the job.

Schedule a wave

The wave that is created in the **Waves** page can be scheduled.

Steps

1. On the **Jobs** page, click the **Schedule Wave** option.
   The **Wave Job** screen is displayed.
2. From the drop-down list, select a wave.
3. To schedule individual phases, select the **Schedule Phases** option.
4. Enter the job description.
5. Enter the details that are described from Step 6 to 8 for all the phases that are related to the wave.

   ⓘ **NOTE:** If the phase dependency is selected while creating a wave, then the consecutive phases cannot be scheduled before the earlier phases.
6. From the **Run** drop-down list, select any of the options to run the job.
7. Select the **Exclude Offline Devices** option if you want to exclude the offline devices while creating the job. This option is selected by default.
   You can view the list of excluded offline devices on the **Jobs** page. You can later restart the job for the offline devices from the jobs list.
8. Select **Immediately** to schedule the job immediately where a maximum of 25 devices can be handled or select the following details to schedule accordingly:
   - **Time Zone**—Select the time zone from the drop-down list.
   - **Effective**—Enter the starting and ending date.
   - **Start between**—Enter the starting and ending time.
   - **On day(s)**—Select the days of the week.
9. Click the **Preview** option to view the details of the scheduled job.
10. On the next page, click the **Schedule** option to initiate the job.

    To view the summary of the deployment, click the **Download/Install Status** option in the **Details** row on the **Jobs** page. You can view the following details:
    - **Total Number of Devices**
    - **Estimated Downloads & Installations**
    - **Actual Downloads**
    - **Actual Installations**
    - **If the file was BIOS, firmware or application package with the devices list**

Restart a job for offline devices

Steps

1. On the **Jobs** page, select any of the scheduled job.
2. From the **More Actions** drop-down list, select **Restart Job for Offline Devices**.

Schedule a report policy

Steps

1. On the **Jobs** page, click the **Schedule Report** option.
   The **Report Policy Job** screen is displayed.
2. From the drop-down list, select a policy.
3. Enter the job description.
4. From the **Run** drop-down list, select any of the options.
5. 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.
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.

   ⓘ **NOTE:** If a report policy is scheduled, then the administrator cannot edit, delete, or reschedule the policy. The administrator must cancel the scheduled job to modify or reschedule the policy.

13

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.

Topics:

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

Search an 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:
   - 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 **Alert Groups** drop-down menu, select any of the following.
   - Not Checked In
   - App Compliance
   - Device Compliance
   - Other
   - Upcoming Remediation
   - Admin Alerts
   - Security Compliance
6. From the **Alert Category** drop-down menu, select any of the following options:
   - Critical
   - Warning
   - Info

Filter the source of the events

From Wyse Management Suite 4.1, you can filter the events based on the source of the event. The global administrator can view all the events from all the users including system-generated events. The other administrators can view the events that are based on their role and also system-generated events.

Steps

1. Click **Events**.

   The **Events** page is displayed.
2. From the **Source** drop-down menu, select the source of the event that you want to filter. The options are :
   - **Global Administrator**
   - **Group Administrator**
   - **Custom Global Administrator**
   - **Custom Group Administrator**
   - **Viewer**
   - **Custom Viewer**
3. Configure the other filters as required.

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 certificate expiry event details

You can view the event details for certificate expiry on ThinOS 9.x devices. You can filter the events to view the certificate details that have expired and also view the resolved details when the expired certificate is renewed.

Steps

1. Click **Events**.

   The **Events** page is displayed.
2. From the **Event Type** drop-down list, go to **Devices** and select either of the following options:
   - **Certificate Expiration**—View the expired or about to expire certificate details.
   - **Certificate Expiration Resolved**—View the renewed certificate details.

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
   - Last 30 days
   - Custom

Support to clear events in on-premises environment

From Wyse Management Suite 3.8, you can clear events in the on-premises environment. To clear the events, log in to the on-premises environment, go to **Portal Administration** > **Clear History**, select the days beyond which all the events to be cleared and click **Clear Events**. An event is generated to show this action in the **Events** tab.

14

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. You can add only two global administrators if you are using a standard license.
  - 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)

  You can search a specific user in the **Administrators** tab.
- **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.

Topics:

- Deleting end user
- Edit a user profile

Add a new admin profile

Steps

1. Go to the **Users** tab.
2. Click **Administrator(s)**.
3. Click **Add Admin**.

   NOTE: The **Add Admin** option is disabled if you are trying to add more than two global administrators in a standard license setup since only three global administrators are allowed.

   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. From the **Template Name** drop-down list, select a custom role template. This step is optional.
   If you select a template, go to step 8.
7. 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.
8. Click **Save**.

Create a WMS custom role in Wyse Management Suite

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. You must have Pro license to use this feature.

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. Optionally, from the **Select Role Template** drop-down list, select a pre-configured template.

   To create a custom role template, see Create a template for a custom role.
6. Click **Roles**.
   If you select any template in step 5, the options configured from step 7 are pre-configured as per the template. You can still modify the configurations as required.
7. From the **Policy group** drop-down list, select the group that the administrator is assigned.
8. From the **Role** drop-down list, select **Custom WMS Role**.
9. Select **Customer Viewer**, **Custom Group Admin**, or **Custom Global Admin**.

   If you select the **Customer Viewer** option, only the **Device Commands** options can be configured for the user.
10. Under each category, select the appropriate function that the user is allowed to perform.
    From Wyse Management Suite 3.6, you can configure granular privileges for Dell Hybrid Client custom roles. For more information, see Configure granular privileges for Dell Hybrid Client custom roles.
11. Click **Save**.

    The following table provides details about the supported and unsupported permissions that can be assigned to a custom role:

Table 15. Permissions for a custom role

Supported	Not supported
Edit or remove configuration	Bulk Device Exception
Add, edit, and delete groups	Create group admin
Upload reference files	Create global admin
Create device detail exception	Create viewer admin
Create and edit rules	Assign roles to un-assigned administrators
Create and edit application policies	Add subscription (Export and Import license)
Bulk import end users	Change WMS server URL
Manage remote repository	Change MQTT URL
Create and edit reports	Upload Config UI
Edit **Others** page	Configure custom branding
Create and edit active directory on the **Portal Admin** page	

Configure granular privileges for Dell Hybrid Client custom roles

From Wyse Management Suite 3.6, you can provide granular configuration privileges to Dell Hybrid Client custom roles.

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 **Policy group** drop-down list, select the group that the administrator is assigned.
7. From the **Role** drop-down list, select **Custom WMS Role**.
8. Select the **Custom Group Admin** option.
9. From the **Default Device Policy Group** and **Default User Policy Group**, select the groups that the users can configure.
10. In the **Groups & Configs** field, select **Create/Edit Policies**.

    ⓘ **NOTE:** You can configure other options in the **Groups & Configs** field as required.
11. Select the Dell Hybrid Client options that the user can configure.
12. Configure the **Device Commands**, **Apps & Data**, **Rules**, **Users**, and **Admin Portal** options as required.
13. Click **Save**.

Create a template for a custom role

From Wyse Management Suite 3.5, you can create a template for a custom role. You can use the template to update the configurations when you create a WMS custom role.

Steps

1. Go to the **Users** tab.
2. Click **Administrator(s)** or **Unassigned Admins**.
3. Click **Create Role Template**.
   The **Create Custom Role Template** window is displayed.
4. Enter the name for the template and the password.
   You can also select the **Generate random password** option.
5. Go to **Roles** > **Portal Administrator** and from the Role drop-down list, select any of the following options:
   - Global Administrator
   - Viewer
   - Group Administrator
   - Custom WMS Role

   For the custom WMS role, you can further select any of the following options:
   - Custom Viewer—Select the group and the device commands for the custom viewer.
   - Custom Group Admin—Select the group and the options the custom group administrator can configure.
   - Custom Global Admin—Select the options that the custom global administrator can configure.
6. Click **Save**.

   After the template is created, it is not listed on the user interface. The templates are listed in the drop-down list while creating users.

   You can also edit or delete the created template using the **Edit Role Template** or **Delete Role Template** options and by selecting the template from the drop-down list.

Delete a custom role template

A global tenant can delete a custom role template.

Steps

1. Go to the **Users** tab.
2. Click **Administrator(s)** or **Unassigned Admins**.
3. Click **Edit Role Template**.
4. From the **Template name** drop-down list, select the template that you want to delete.
5. Click **Delete**.
   A window is displayed to confirm the deletion of the template.
6. Click **Ok**.

Assign group roles to the created template

Steps

1. Import users from an active directory.
2. Go to the **Users** tab.
3. Click **Group Assignment**.
4. Select the user group.
5. Select the role from the template.
6. Click **Save**.

Assign WMS custom roles to imported AD groups

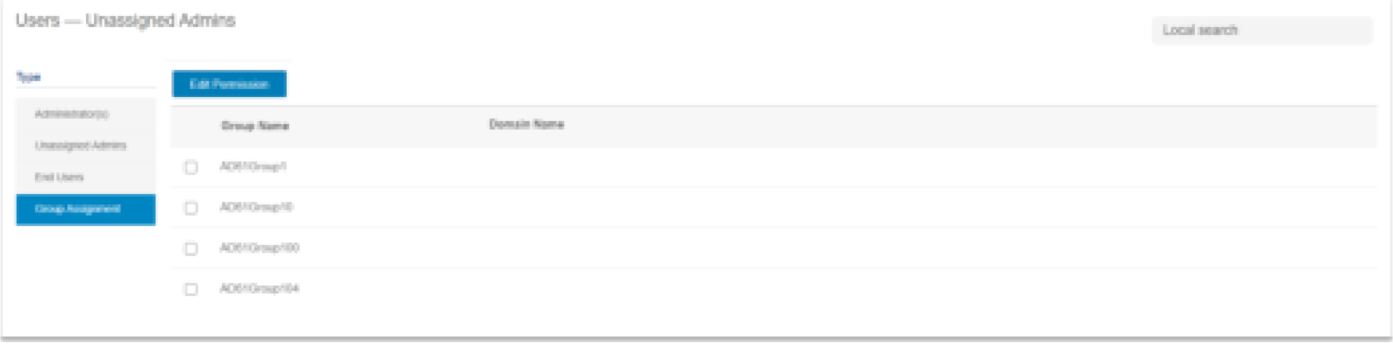
From Wyse Management Suite 3.2, you can assign roles to groups imported from the active directory. The permission assigned to the group is applied to all users of the group.

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**.



Users — Unassigned Admins

Local search

Type

- Administrator(s)
- Unassigned Admins
- End Users
- Group Assignment

Edit Permission

	Group Name	Domain Name
□	AD61Group1	
□	AD61Group10	
□	AD61Group100	
□	AD61Group104	

Figure 13. 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**.
6. Click **Save**.

Activate an administrator profile

You can activate a deactivated profile and provide the necessary roles.

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 the selected administrator from logging in to the console, and removes the 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**.

15

Portal administration

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

Topics:

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`.

      NOTE: Ensure that you do not include the certificate headers in the Federation Metadata XML file. If XML file contains the certificate headers, then the upload of this XML file fails.

   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.

Enable single sign-on using SAML 2.0 for Azure Active Directory users using Ping federate

Steps

1. Log in to Wyse Management Suite.
2. Go to **Portal Administration** > **Active Directory** and click the **ADFS Configuration (SSO using SAML 2.0)** option.
3. Click the **Download WMS xml file** link.
   The xml file is downloaded.

4. Configure the SP connection in the PingFederate administrative console.
   For information about how to configure the SP connection, see *Configuring a SAML application* at Pingidentity | Docs.
5. Configure the required claims and attributes in the Identity Provider section.
   You can get the list of claims and attributes from the Wyse Management Suite user interface.
6. Download the Azure enterprise application federation metadata file.
7. Go to **Portal Administration** > **Active Directory** and click the **ADFS Configuration (SSO using SAML 2.0)** option.
8. In the **Configure Identity Provider** section, click **Update Configuration**.
9. Click **Load XML File** and upload the federation metadata file.
10. Select the **Enable SSO Login using ADFS option**.
11. Click **Save** and go to the same location.
12. Click **Test ADFS Login**.

    NOTE: Ensure that **PARTNER'S ENTITY ID (CONNECTION ID)** and **CONNECTION NAME** are unique before uploading to Wyse Management Suite. It is recommended to use the FQDN.

Enable single sign-on using SAML 2.0 for Azure Active Directory

Steps

1. Log in to Wyse Management Suite.
2. Go to **Portal Administration** > **Active Directory** and click the **ADFS Configuration (SSO using SAML 2.0)** option.
3. Click the **Download WMS xml file** link.
   The xml file is downloaded.
4. Register the enterprise application and enable SAML configuration. Upload the downloaded WMS xml file.
   For information about how to enable single sign-on on Entra ID, see *Enable single sign-on for an enterprise application* at Microsoft | Learn.
5. Configure the required claims and attributes in the Identity Provider section.
   You can get the list of claims and attributes from the Wyse Management Suite user interface.
6. Download the Azure enterprise application federation metadata file.
7. Go to **Portal Administration** > **Active Directory** and click the **ADFS Configuration (SSO using SAML 2.0)** option.
8. In the **Configure Identity Provider** section, click **Update Configuration**.
9. Click **Load XML File** and upload the federation metadata file.
10. Select the **Enable SSO Login using ADFS option**.
11. Click **Save**.

Enable single sign-on using OAuth 2.0 for Azure Active Directory

Steps

1. Register the application in the Microsoft Identity Platform.
   For information about how to register the application, see *Quickstart: Register an application with the Microsoft identity platform* at Microsoft | Learn.
2. Add the following WMS URI as part of application registration:
   - For US cloud—https://us1.wysemanagementsuite.com/ccm-web/azuresso/auth.
   - For EU cloud—https://eu1.wysemanagementsuite.com/ccm-web/azuresso/auth.
3. Log in to Wyse Management Suite.
4. Go to **Portal Administration** > **Active Directory** and click the **ADFS Configuration (SSO using OAuth 2.0)** option.
5. Enter the obtained **Tenant ID**, **Client ID**, and **Secret**.
6. Select the **Enable SSO Login**.
7. Click **Save**.

Import users and groups from Microsoft Entra ID

Steps

1. Register the application in the Microsoft Identity Platform.

   For information about registering the application, see *Quickstart: Register an application with the Microsoft identity platform* at Microsoft | Learn.
2. Add the following Wyse Management Suite URL when you are configuring the application registration details:
   - US cloud—https://us1.wysemanagementsuite.com/ccm-web/admin/portal/azure/processimport
   - EU cloud—https://eu1.wysemanagementsuite.com/ccm-web/admin/portal/azure/processimport
3. Enable the following delegated API permission for the application:
   - Directory.Read.All
   - Domain.Read.All
   - Group.Read.All
   - User.Read.All
   - User.Read
   - GroupMember.Read.All
4. After the registration is complete, log in to Wyse Management Suite.
5. Go to **Portal Administration** > **Active Directory** and click **Users and Groups Import from Microsoft Entra ID (Azure Active Directory and Services)**.
6. Enter the required information in the **Tenant ID**, **Client ID**, and **Secret** fields.
7. Click **Login**.
   You are redirected to the Microsoft authentication page.
8. Enter the authentication details.
   You are redirected to Wyse Management Suite.
9. Click **Show Available Groups** to view the list of available groups from the Azure Directory.
10. Select a group.
    The selected group is moved to the right pane.
11. Optionally, assign roles to users or groups.
12. Click **Import Users** or **Import Groups**.

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

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** .

Configure subnet mapping

Subnet mapping feature can be used when multiple repositories from different subnets are registered to Wyse Management Suite and the administrator wants to deploy application from a particular repository based on the repository capacity or network bandwidth. When subnet mapping is configured, Wyse Management Suite provides the repository URLs based on the subnet map settings to the end points.

Steps

1. Go to **Portal Administration** > **File Repositories**.
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.
6. Select the **Preferred Repository** option to always connect to one repository and not fall back to any other repository till the preferred repository is online.

ⓘ **NOTE:** When the preferred repository is offline, Wyse Device Agent falls back immediately to the next available repository. An attempt to download does not happen for preferred repository when it is offline.

Configure maximum allowed concurrent downloads limitation

The Wyse Management Suite administrator can update the max concurrent download and save and restart tomcat which updates the maximum thread value in the server or the repository tomcat configuration file.

Steps

1. Go to **Portal Administration** > **File Repository**.
2. Select any of the repository and click **Edit**.

   The maximum allowed concurrent file downloads is mentioned.
3. Enter the maximum allowed concurrent downloads limitation in the **Concurrent File Downloads** field.
4. Click **Save Settings**.

   An alert message is displayed.
5. Do any of the following:
   - If you are managing ThinOS devices and updating device packages or firmware through **Groups & Configs**, click **Save and Restart Tomcat**.
   - If you are managing other device types, click **Save**.

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 to 360 minutes. The minimum interval is 5 minutes for private cloud.
- **Checkin interval**—Enter the time. The device sends a full checking signal every 8 to 24 hours.
- **Not Checked In compliance alert**—Enter the number of days before a device triggers a **Not Checked In compliance alert**. The range is 1 to 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 autodiscovered 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 the **EULA Acceptance** page to show the wizard again when uploading the EULA Embedded firmware or packages for ThinOS 9.x.
- **WMS API**—Select this check-box to enable Wyse Management Suite API.
- **Remote Shadow (P2P) Configuration**—Use this option to configure the remote shadow connections for an on-premises environment.

Enable Wyse Management Suite API

Wyse Management Suite server uses a proprietary API to serve requests 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 the Wyse Management Suite server and integrate the server with your custom client such as ServiceNow.

Prerequisites

A 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 Dell Developer Portal .

   > ⓘ **NOTE:** For the cloud edition, the API option is not enabled by default. The option is enabled if you have an API license. For more information, see *How to Request API Enablement in Wyse Management Suite Pro* at Dell | Support.

Enable Wyse Management Suite API through custom port

About this task

If you are using a custom port, you must modify the `catalina.properties` file to enable the Wyse Management Suite API.

Steps

1. Go to `<install directory>\DELL\WMS\Tomcat-9\conf`.
2. Open the `catalina.properties` and add the following properties:
   - **`api.wms.webclient.ccmweb.hostname= <host name ex:wms-ad-131-1`**
   - **`api.wms.webclient.ccmweb.hostport= <port ex:8080>`**
3. Restart the Tomcat service.

   > ⓘ **NOTE:** When the Wyse Management Suite server is upgraded, the administrator must add the hostname and port details again in the `catalina.properties` file.

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.

Steps

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. If you want to troubleshoot the end points, the reports can be shared with the administrator.

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**.

   NOTE: The QFE details of the Windows Embedded devices and details of the installed applications on thin clients are captured in the device report.

   NOTE: If you select the **Type** as **Non-Compliant Devices** and set the delimiter, you can view the reasons for the noncompliance of the devices in the generated report.

ⓘ **NOTE:** From Wyse Management Suite 4.2, the administrator can view the BIOS parameters for ThinOS 9.x devices when you generate a report.

Improvements to report

- **Improvements to device reports**—While generating any devices report (Unmanaged, Online, Offline, Non-Compliant, All Devices), the administrator can select and clear required columns. The column name can be searched in the **Search** window above the **Select All/Deselect All** options.
- **Improvements to event reports**—While generating the event report, the administrator can select the required event types instead of generating a report for all the events.
- **Improvements to the install application reports**—The administrator can generate an installed application report. To generate the report, you must provide an application name in the **Installed App Name** field. The administrator can provide up to 10 application names separated by a comma.

Generate a report on devices with installed and missing QFE

Steps

1. Go to **Portal Administration** > **Reports**
2. Click the **Generate Report** option.

   The **Generate Report** window is displayed.
3. From the **Type** drop-down list, select **QFE**.
4. From the QFE drop-down list, select any of the following options:
   - **Has not installed QFE**—Select this option to generate a report of devices that have not installed the QFE entered in the field. This option is applicable only for Windows Embedded Standard and Wyse Software thin clients.

     ⓘ **NOTE:** You can search up to 10 QFEs separated by a comma.
   - **Has installed QFE**—Select this option to generate a report of devices that have installed the QFE entered in the field. This option is applicable only for Windows Embedded Standard and Wyse Software thin clients.

     ⓘ **NOTE:** You can search up to 10 QFEs separated by a comma.
   - **Missing QFE**—Select this option to generate a report of devices with missing QFE for the group.
5. From the **Groups** drop-down list, select the group.
6. Select the delimiter.
7. Click **Save**.

Create a report policy

You can create a policy for the report generation and schedule the policy.

Steps

1. Go to **Portal Administration** > **Reports**.
2. Click **Report Policy**.
3. Click **Create**.
   The **Create Report Policy** window is displayed.
4. Enter a policy name.
5. From the **Type** drop-down list, select the type of report you want to generate.
6. From the **Group** drop-down list, select the group.
7. Select the delimiter for the report.
8. Click **Save**.
   An **Alert** window is displayed.
9. Select any of the following options:
   - **Later**—If you want to schedule the policy later from the **Jobs** page.
   - **Yes**—If you want to schedule it immediately.

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**.

Clear the running Groups & Configs jobs

From Wyse Management Suite 4.2, the administrator can clear the running **Groups & Configs** jobs for a selected period.

Steps

1. Go to **Portal Administration** > **Clear History**.
2. Select the days beyond which the running jobs should be cleared from the drop-down list.
3. Click **Clear Running Jobs**.
4. Go to the **Jobs** page, select the job and click **Cancel**.

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.x, 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: Dell Technologies recommends upgrading the system to 12 GB RAM as more memory is required to enable secure communication.

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

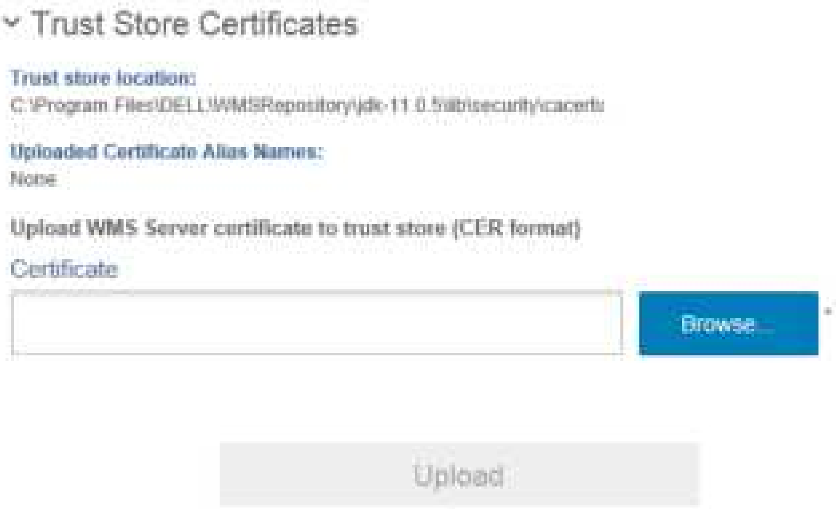
Enable secure LDAP over SSL

Steps

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

   ⓘ **NOTE:** For information about how to create an SSL certificate, see *Enable LDAP over SSL with a third-party certification authority* at Microsoft | Learn.

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



Trust Store Certificates

Trust store location:
C:\Program Files\DELL\WMSRepository\jdk-11.0.5\lib\security\cacerts

Uploaded Certificate Alias Names:
None

Upload WMS Server certificate to trust store (CER format)

Certificate

Figure 14. 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-premises installation, you can import the server certificate and configure secure LDAP by updating the certificate in the OOBE screen.

Next steps

- After the on-premises installation with a single tenant, go to **Portal Administration** > **Setup** to import the public key of the certificate to the trust store. For multitenant 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.

16

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.

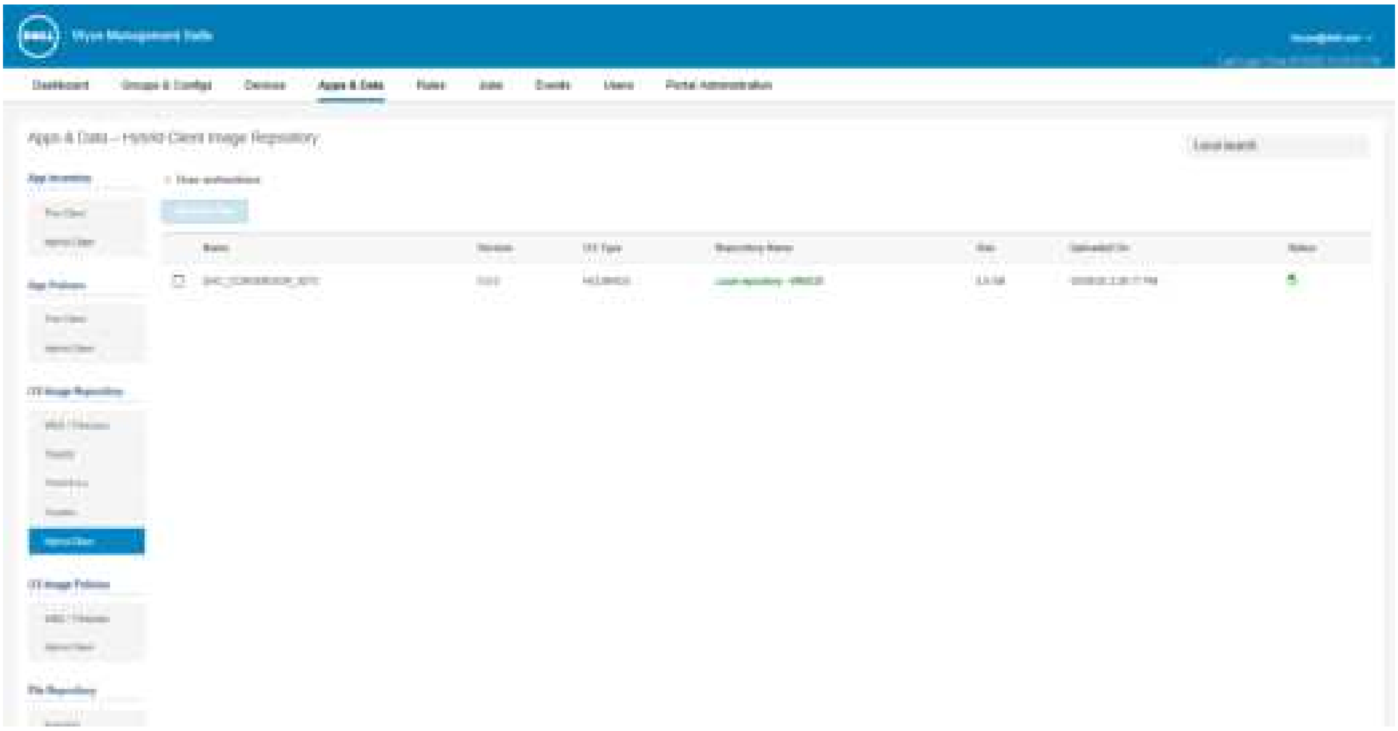


Figure 15. Adding Dell Hybrid Client Images to repository

Creating Hybrid Client Image policies

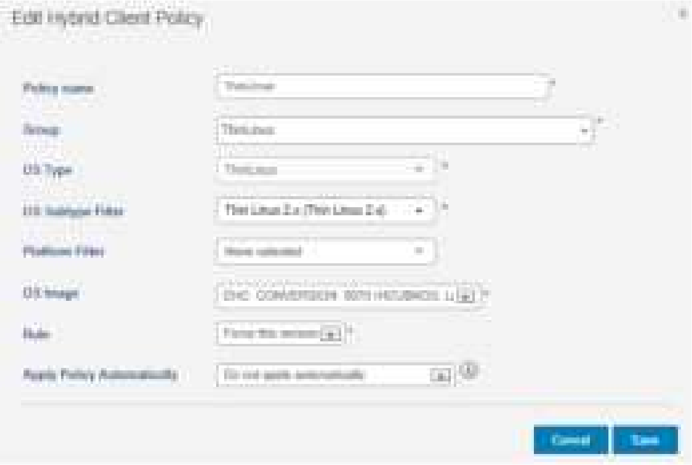
Steps

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**.



Edit Hybrid Client Policy

Policy name	ThinLinux
Group	ThinLinux
OS Type	ThinLinux
OS Subtype Filter	Thin Linux 2.x (Thin Linux 2.x)
Platform Filter	None selected
OS Image	DHC_CONVERSION_5070 HCUBKOS L[illegible]
Rule	Force this version
Apply Policy Automatically	Do not apply automatically

Figure 16. 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.

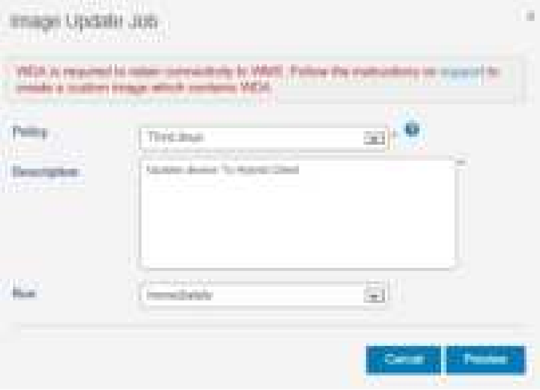


Image Update Job

WDA is required to retain connectivity to WMS. Follow the instructions on support to create a custom image which contains WDA.

Policy	ThinLinux
Description	Update device To Hybrid Client
Run	Immediately

Figure 17. 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 at Dell | 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 the 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 OPERATING SYSTEM-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.

17

Convert Dell Generic Client to ThinOS 9.x

From Wyse Management Suite 3.7, you can convert Dell Generic Client devices to ThinOS devices.

Prerequisites

- If you have a Latitude 3420 device that is running Ubuntu 20.04 operating system, ensure that DCA-Enabler 1.5.0-7 is installed.
- Wyse Management Suite version 3.7 must be used to convert to ThinOS 2205.
- Create a group in Wyse Management Suite with a group token.
- The Latitude 3420 device running Ubuntu 20.04 operating system must be registered to Wyse Management Suite as a generic client.
- If you are converting to ThinOS 2205 on Dell Latitude 3420, ensure that you have connected the device to the external power source using the power adapter.
- Ensure you have downloaded the Ubuntu 20.04 to ThinOS 2205 conversion image.
- Extract the Ubuntu 20.04 to ThinOS 2205 conversion image to get the ThinOS TRT file **DTOS_Ubuntu_Installer_1.0-dtos11-amd64_signed.tar.gz** and ThinOS image **DTOS_9.3.xxxx**.

Steps

1. Go to **Apps & Data** > **App Inventory** > **Generic Client**, and click **Add Package file**.
2. Upload the ThinOS TRT file **DTOS_Ubuntu_Installer_1.0-dtos11-amd64_signed.tar.gz**
3. Go to **Apps & Data** > **OS Image Repository** > **ThinOS 9.x**, and click **Add Firmware file**.
4. Upload the ThinOS image **DTOS_9.3.xxxx**.

   NOTE: You cannot change the image file name.
5. Go to **Apps & Data** > **App Policies** > **Generic Client**, and click **Add Advanced Policy**.
6. Enter the policy name, select the group in which Latitude 3420 has been registered, and select **Generic Client** as **OS type**.
7. Click **Add app**, and select the ThinOS TRT file that was uploaded before from the drop-down menu.
8. Click **Add app** again, and select the ThinOS image file that was uploaded before from the drop-down menu.
9. Click **Save**.

   NOTE: Ensure that the **Apply Policy Automatically** option is set to **Do not apply automatically**.
10. Click **Yes** to schedule a job.
11. Select **Immediately** in the **App Policy Job** window and click **Preview** to get the **Run** option.
12. Click **Schedule**.
    The ThinOS TRT file downloads and installs first followed by the ThinOS image on Latitude 3420. After installation, the device restarts automatically.

    NOTE:

    - Ensure that you have connected the Latitude 3420 device to the external power source using the power adapter.
    - The ThinOS Activation devices license number of Wyse Management Suite must be larger than the Latitude 3420 device number. If it is, you cannot create the Advanced Policy for conversion.
    - After conversion, ThinOS 2205 is in the factory default status. ThinOS 2205 must be registered to Wyse Management Suite manually or using DHCP/DNS discovery.
    - After you register the Latitude 3420 to Wyse Management Suite, the ThinOS activation devices license will be consumed.

18

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.

19

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 16. 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.

20

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.

Wyse Software thin client license

From Wyse Management Suite 3.5, new Wyse Software thin client licenses consume the Thin Client licenses. If the Wyse Software thin client has an existing license, the device is unregistered from Wyse Management Suite after the license expires. You must update the Wyse Software thin client with the new Wyse Device Agent if you want to register to Wyse Management Suite and the Thin Client license is consumed for the device.

ThinOS activation license

From Wyse Management Suite 3.7, you can convert Dell Generic Client devices to ThinOS devices. You need a ThinOS activation license to convert the device.

Each conversion consumes one license. To view the ThinOS activation license details, go to **Portal Administration** > **Subscription** > **License Usage**.

You can click the **View License** option to view the license details such as the service tag and name of the device that consumed the license.

You can also float the licenses from public cloud to on-premise setup. For more information, see How to export public cloud ThinOS activation license to on-premise environment.

How to export public cloud ThinOS activation license to on-premise environment

Prerequisites

You must have ThinOS activation license in public cloud environment.

Steps

1. Log in to Wyse Management Suite public cloud console.
2. Go to **Portal Administration** > **Subscription** > **Export License for Private Cloud**.
3. Enter the number of ThinOS Activation licenses that must be exported to Wyse Management Suite Private Cloud.
   The **On-Prem Identifier** field is displayed.
4. Enter the on-premise identifier to which you want to export the license. To get the on-premise identifier details, go to **Portal Administration** > **Subscription** on the on-premise environment.
5. Click **Export**.

   To view the details of the exported licenses, click **View Exported License Seats**.

You can rename the hostname of the Wyse Management Suite system if the ThinOS activation license is changed. You need to log in to Wyse Management Suite cloud server and rename the respective hostname by entering the new on-premise identifier.

How to retrieve the ThinOS activation license from the on-premise environment

You can retrieve the unused ThinOS activation license that is exported to the on-premise setup back to the public cloud environment.

Prerequisites

You must have unused ThinOS activation license in the on-premise setup.

Steps

1. Log in to Wyse Management Suite on-premise setup.
2. Go to **Portal Administration** > **Account** > **Subscription**.
3. Click **ReIssue Key**.
4. Copy the key.
5. Log in to Wyse Management Suite public cloud console.
6. Go to **Portal Administration** > **Account** > **Subscription** > **Export License for Private Cloud**.
7. Click **ReIssue** and paste the key in the **ReIssue key** field.
8. Click **Proceed ReIssue**.

Migrate on-premise identifier

The administrator can migrate on-premise ID and provide the new identifier along with the public cloud datacenter and tenant credential which returns the ThinOS activation license to the public cloud. You can use the **Migrate On-Premise ID** option to migrate the license.

21

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 Dell | 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 an 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 Dell | 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 an 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 or 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 17. 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

- Upgrade any earlier versions of ThinOS to 8.6_807.
- Upgrade the BIOS on the device to the current version that is mentioned in the ThinOS Release Notes. For more information, see *Dell Wyse ThinOS 8.6 Release Notes* at Dell | Support.
- Add the ThinOS conversion image 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.
- Register the thin client 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.
- Create a group in Wyse Management Suite with a valid group token. Use this group token to register the ThinOS 9.x devices.
- Register your 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, 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: ThinOS 9.1.3129 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.

22 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. The following image describes the architecture of the remote repository:

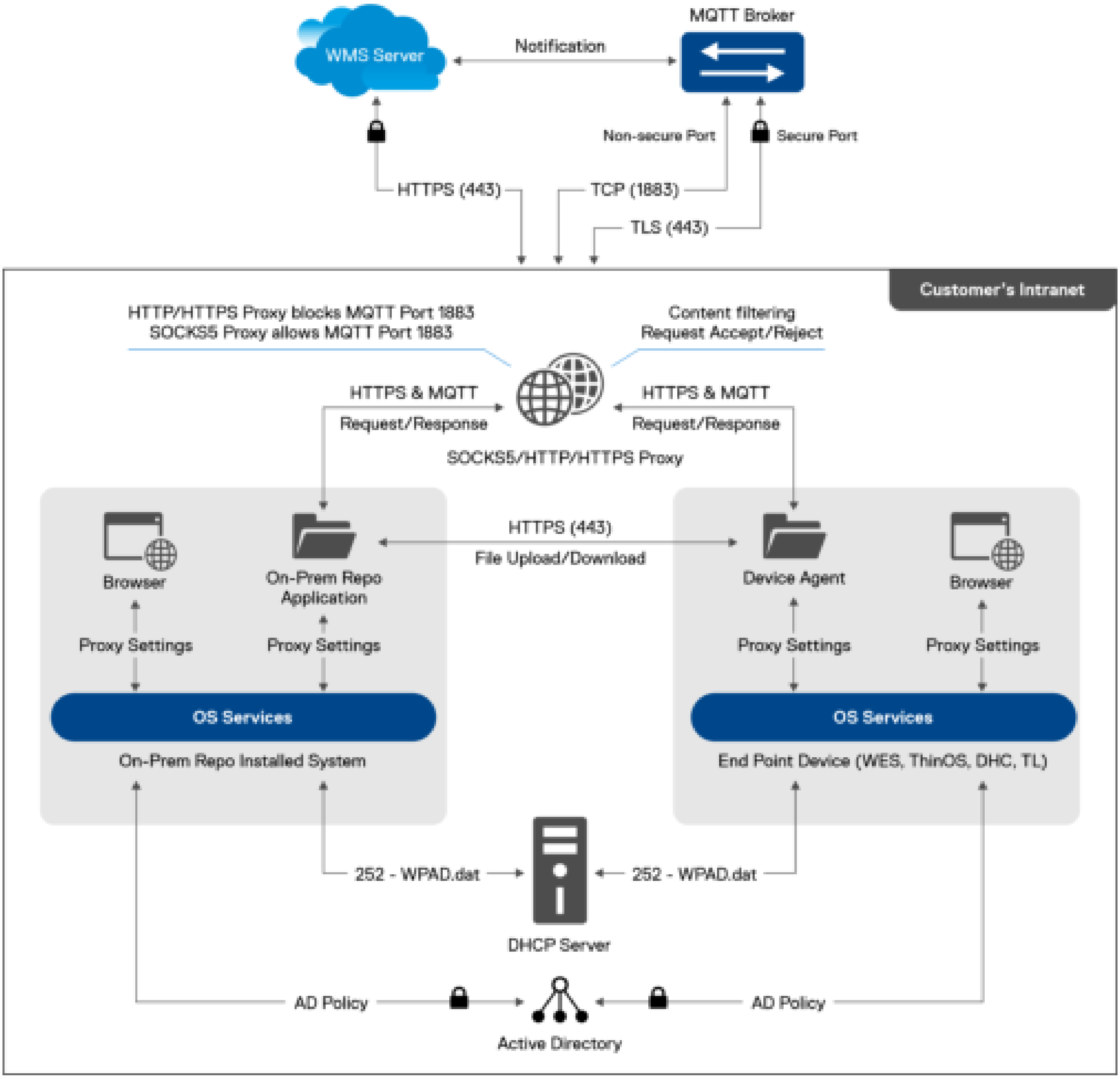


Figure 18. Remote repository architecture

Topics:

- Proxy support for Wyse Management Suite remote repositories
- Install Wyse Management Suite remote repository

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.

Install Wyse Management Suite 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 Server 2016, and Windows Server 2019 Standard and Windows Server 2022
  - Four CPUs
  - 8 GB RAM
  - 40 GB storage space

> **NOTE:** From Wyse Management Suite 3.6, the repository installation is supported on Windows 2016 and Windows 2019 virtual machines that are hosted on Azure and Amazon Web Services (AWS). It is not supported on Google Cloud Platform. After you install the repository, the repository URL is displayed as the hostname of the virtual machine. The URL may not be reachable by the end point. To enable the URL to be reachable to the end points, the repository URL must be edited and the DNS name of the virtual machine must be used as the URL before registering to Wyse Management Suite. For example, `uw2-wmstest-vw01.westus2.cloudapp.azure.com` is a sample of the Azure virtual machine DNS address and `ec2-3-141-79-165.us-east-2.compute.amazonaws.com` is a sample of the AWS virtual machine DNS address.

About this task

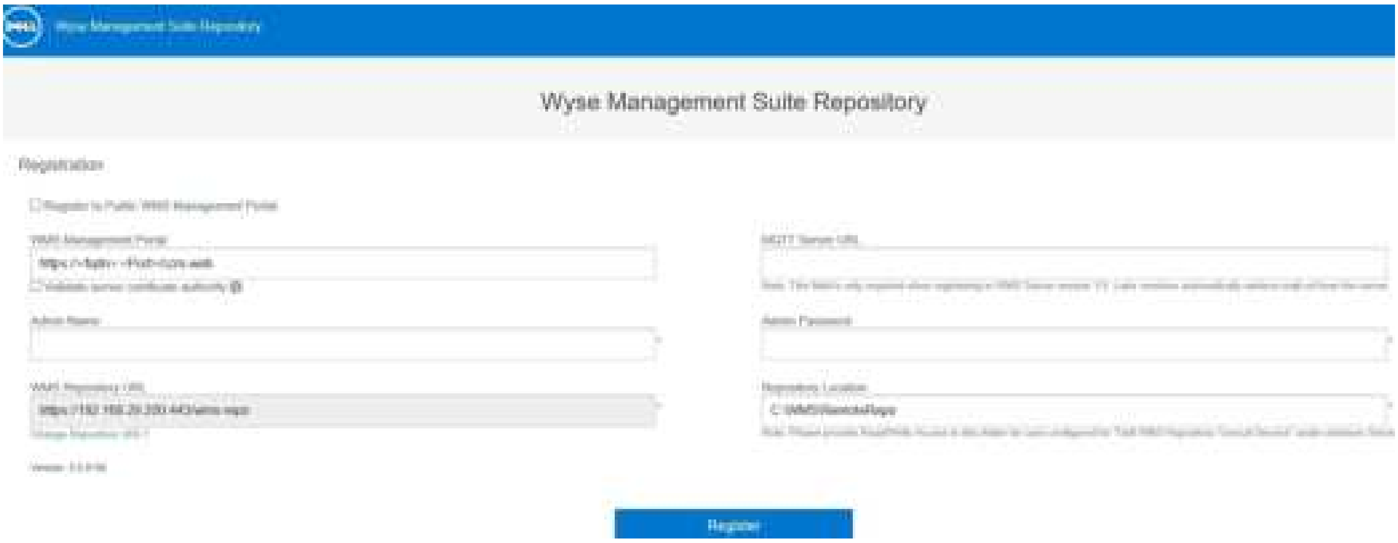
Do the following to install **WMS-Repo** software:

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.

   > **NOTE:** From Wyse Management Suite 4.1, the software vault service is enabled for the repository. You can configure it during the installation of the repository.

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.



Wyse Management Suite Repository

Wyse Management Suite Repository

Registration

□ Register to Public WMS Management Portal

WMS Management Portal

https://<fqdn>:<Port>/ccm-web

□ Validate server certificate authority

Admin Name

WMS Repository URL

https://192.168.29.200:443/wms-repo

Change Repository URL?

Version: 3.5.0-56

MQTT Server URL

[illegible]

Admin Password

Repository Location

C:\WMS\RemoteRepo

[illegible]

Figure 19. Register on a public cloud

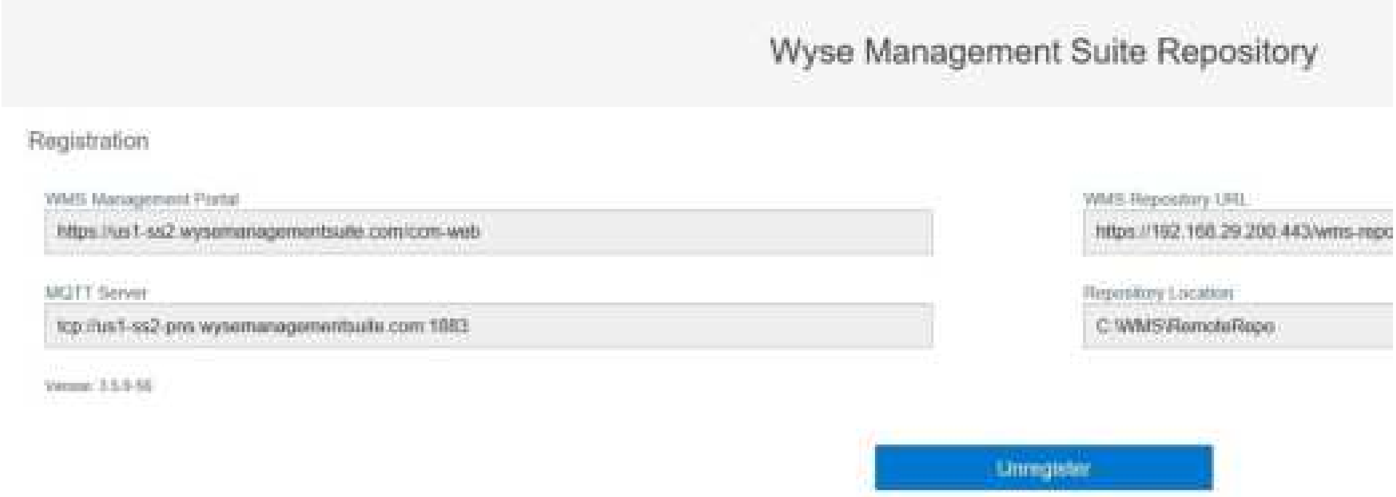
5. Enter the following details:
   a. Wyse Management Suite server URL

      ⓘ **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

   ⓘ **NOTE:** You must provide the read and write access to the folder captured in the **Repository Location** field. The access must be configured for **Dell WMS Repository Tomcat Service** windows service.

6. Click **Register**.
7. If the registration is successful, the **Registration** window is displayed:



Wyse Management Suite Repository

Registration

WMS Management Portal

https://us1-ss2.wysemanagementsuite.com/ccm-web

MQTT Server

tcp://us1-ss2-pns.wysemanagementsuite.com:1883

Version: 3.5.0-56

WMS Repository URL

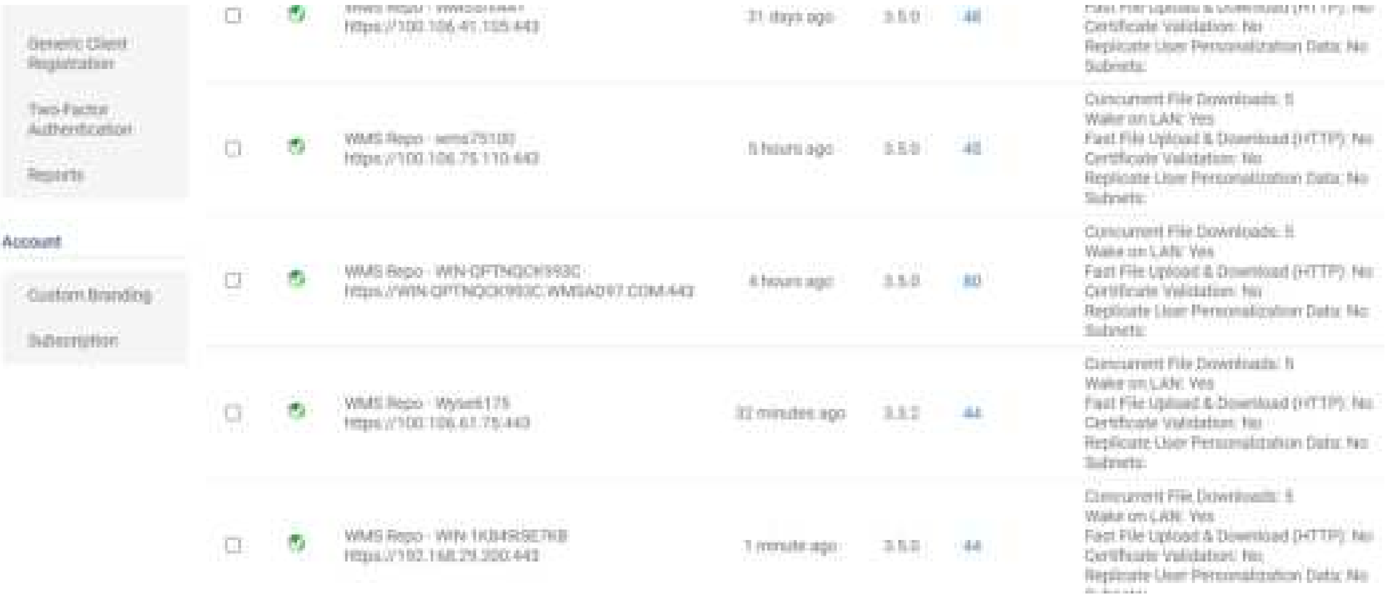
https://192.168.29.200:443/wms-repo

Repository Location

C:\WMS\RemoteRepo

Figure 20. Registration successful

8. The following screen on the Wyse Management Suite portal confirms the successful registration of the remote repository:



Generic Client Registration

Two-Factor Authentication

Reports

Account

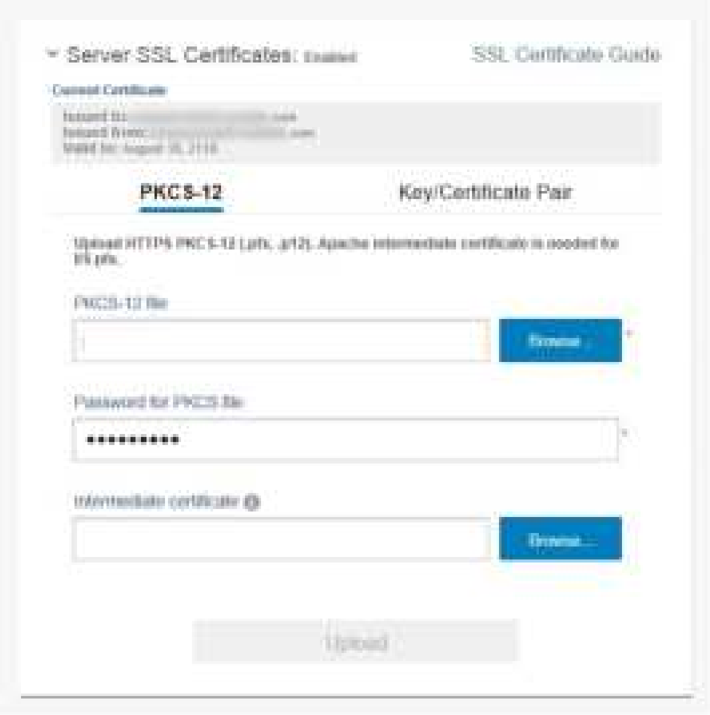
Custom Branding

Subscription

□	●	WMS Repo - [illegible] https://100.106.41.135:443	31 days ago	3.5.0	48	Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
□	●	WMS Repo - wms75100 https://100.106.75.110:443	5 hours ago	3.5.0	45	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
□	●	WMS Repo - WIN-QPTNQCK993C https://WIN-QPTNQCK993C.WMSAD97.COM:443	4 hours ago	3.5.0	80	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
□	●	WMS Repo - Wyse6175 https://100.106.61.75:443	32 minutes ago	3.3.2	44	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No Subnets:
□	●	WMS Repo - WIN-1KB4RSE7KB https://192.168.29.200:443	1 minute ago	3.5.0	44	Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: No

Figure 21. 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.



Server SSL Certificates: Enabled

Current Certificate

Issued to: [redacted].com
Issued from: [redacted].com
Valid to: August 30, 2119

Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is needed for IIS pfx.

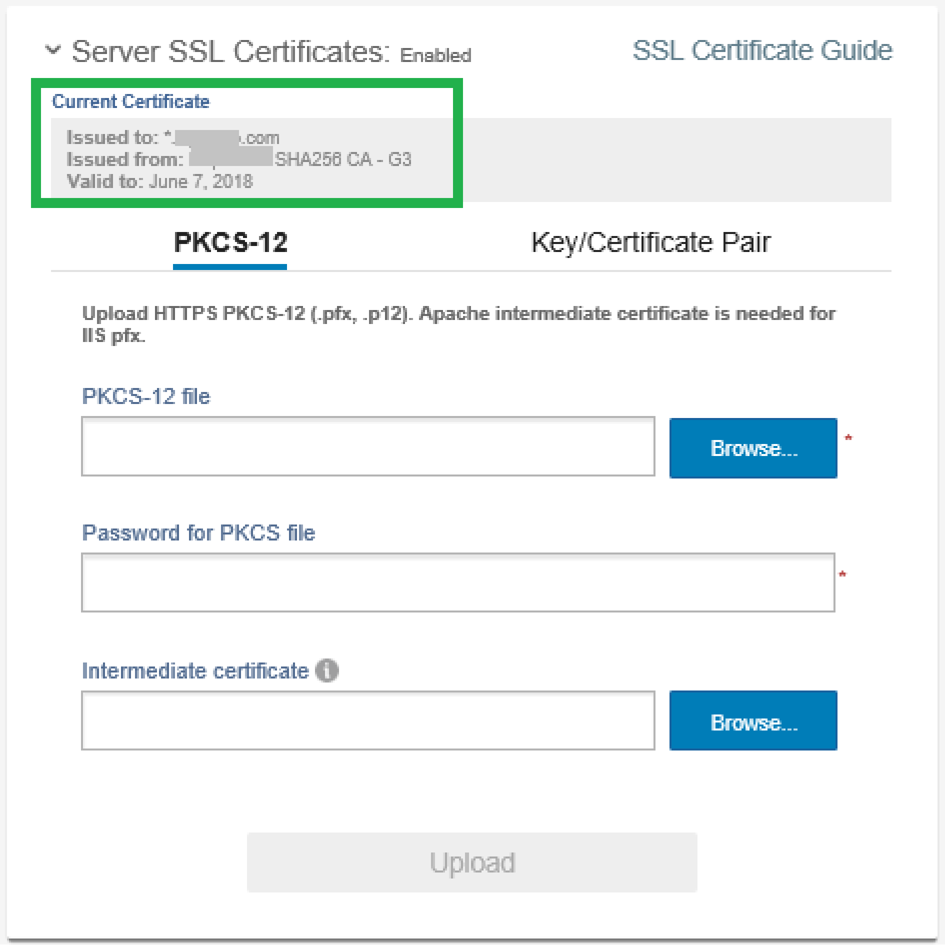
PKCS-12 file

Password for PKCS file: **********

Intermediate certificate

Figure 22. Certificate upload

10. The server restarts, and the uploaded certificate is displayed.



Server SSL Certificates: Enabled

SSL Certificate Guide

Current Certificate

Issued to: *[redacted].com
Issued from: [redacted] SHA256 CA - G3
Valid to: June 7, 2018

Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is needed for IIS pfx.

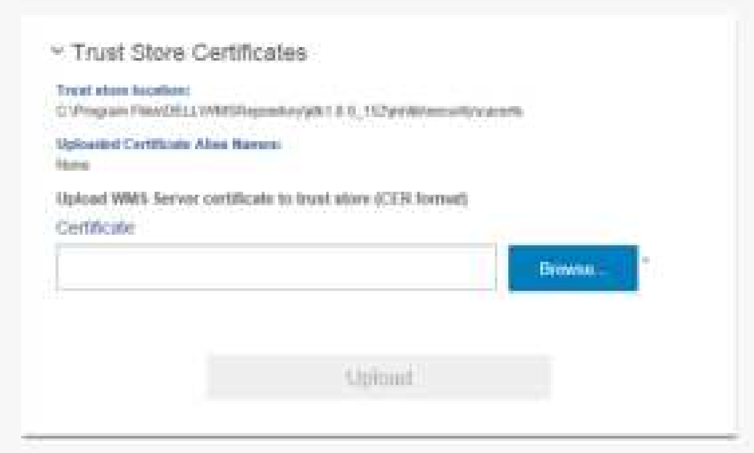
PKCS-12 file

Password for PKCS file

Intermediate certificate

Figure 23. 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.



Trust Store Certificates

Trust store location:
C:\Program Files\DELL\WMSRepository\jdk1.8.0_152\jre\lib\security\cacerts

Uploaded Certificate Alias Names:
None

Upload WMS Server certificate to trust store (CER format)

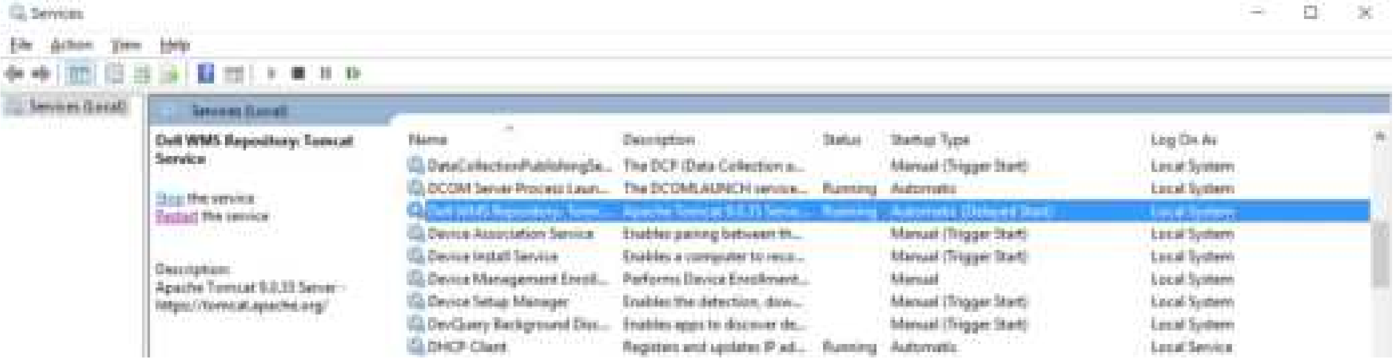
Certificate

Figure 24. Trust store certificates

12. Go 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.

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.



Dell WMS Repository: Tomcat Service

Stop the service
Restart the service

Description:
Apache Tomcat 9.0.33 Server - https://tomcat.apache.org/

Name	Description	Status	Startup Type	Log On As
DataCollectionPublishingSe...	The DCP (Data Collection a...		Manual (Trigger Start)	Local System
DCOM Server Process Laun...	The DCOMLAUNCH service...	Running	Automatic	Local System
Dell WMS Repository: Tom...	Apache Tomcat 9.0.33 Serve...	Running	Automatic (Delayed Start)	Local System
Device Association Service	Enables pairing between th...		Manual (Trigger Start)	Local System
Device Install Service	Enables a computer to reco...		Manual (Trigger Start)	Local System
Device Management Enroll...	Performs Device Enrollment...		Manual	Local System
Device Setup Manager	Enables the detection, dow...		Manual (Trigger Start)	Local System
DevQuery Background Disc...	Enables apps to discover de...		Manual (Trigger Start)	Local System
DHCP Client	Registers and updates IP ad...	Running	Automatic	Local Service

23

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.

24

Software Vault Utility

Software Vault is a service that is used to secure, store, and control access to encryption keys.

To download the SoftwareVaultUtility-1.x.x.exe files, go to the **Drivers & Downloads** page of Wyse Management Suite at Dell | Support. If you are using Wyse Management Suite 3.5 or later versions, you can access the utility using the command prompt. You do not have to install the utility. The utility works with the Windows command line with administrator privileges. The utility is supported with both the default and custom installation of Wyse Management Suite.

Topics:

Export the Software Vault key in a non-High Availability environment

Steps

1. Open a command prompt as an administrator on the server where Wyse Management Suite is installed.
2. Browse to the folder where the utility is copied.
3. Run the .exe file from the command line using the parameters `-mode export -password <password for the zipped file which is created that contains exported keys>`.
   For example, `C:\> softwareVaultUtility-1.x.x.x.exe -mode export -password <PASSWORD>`.

   A password protected .zip file `keys.zip`, with exported keys and checksum file is generated.
4. Extract and use the same password that was used earlier to check the content of the .zip file.

   NOTE: Use WinRAR or 7z to extract the files. The default Windows extractor cannot extract the password-protected files.

   NOTE: After exporting the key, save the keys.zip and checksum file in a secure location and do not rename the files.

   NOTE: If any parameter is missed, entered incorrectly, or if the password is set without the password complexity, an error message is displayed.

Import the Software Vault key in a non-High Availability environment

Steps

1. Copy the utility, keys.zip, and the checksum file to a folder.
2. Run the .exe file from the command line using the parameters `-mode import -password <password for the zipped file which contains exported keys>`.
   For example, `C:\> softwareVaultUtility-1.x.x.x.exe -mode import -password <PASSWORD>`.

   The keys are imported to the destination end point, and the backup.zip file is generated in the same folder. The backup.zip file can be used to rollback the changes.
3. Extract and use the same password that was used to export the keys to check the content of the .zip file.
   The backup.zip file contains the following files:
   - bootstrap.properties

- keys.json
- server.xml
- configuration.properties

4. Restart Memcached (Dell WMS: Memcached) service.
5. Restart Tomcat9 (Dell WMS: Tomcat Service) service.

   ⓘ **NOTE:** The password used to export the key must be used to import the key. Use WinRAR or 7z to extract the files. The default Windows extractor cannot extract the password-protected files.

   ⓘ **NOTE:** Save the backup.zip file in a secure location and do not rename or edit the keys.zip and the checksum file.

   ⓘ **NOTE:** Do not rerun the import command. After the keys.zip file is imported, the file is deleted from the device.

   ⓘ **NOTE:** If the previous WMS Server had a custom Config UI which was not part of WMS installation, then after the WMS services are up and running and the WMS UI is started in the restored server, you must reupload the same version of the Config UI package.

Rollback changes after importing the Software Vault key

To rollback the changes after importing the Software Vault key, run the .exe file from the command line using the parameters **`-mode rollback -password <password for the zipped file which contains exported keys>`**.

For example, **`C:\> softwareVaultUtility-1.0.0.exe -mode rollback -password <PASSWORD>`**.

This action performs a rollback of the previous keys and updates the encrypted database passwords.

ⓘ **NOTE:** The password used to export or import the keys must be used to rollback the changes. After you rollback the key, restart the Tomcat service.

25

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**.

Unable to update the CIFS user from the Wyse Management Suite server

From Wyse Management Suite 3.5, the server is running on a user account with least user privileges. Since there is no local admin privilege, itt is unable to create shared folder for Teradici. To update the CIFS user in future, a shared folder must be created manually and read permission should be given to the CIFS user.

Wyse Management Suite Repository registration fails

Wyse Management Suite Repository registration fails with error **Repository unregistration failed on WMS server** for any of the following reasons:

- **Case 1**— If Wyse Management Suite Repository host Server time is not in sync with UTC time, ensure that the server is configured with proper time in sync with UTC. Dell Technologies recommends that you configure a NTP service such as pool.ntp.org.
- **Case 2**— If Wyse Management Suite Repository host Server has the IPv6 enabled in the active network adapter, go to the Network connections properties, clear the Internet protocol version 6 (TCP/IPv6) and then click **OK**.

Device does not retrieve valid IP address when you perform imaging from Wyse Management Suite with Spanning tree enabled

When you perform an imaging operation from Wyse Management Suite, the device may face an issue to retrieve the valid IP address from a DHCP server in a network where spanning tree protocol is enabled, due to which imaging may fail.

Workaround: You must enable PortFast on all client ports to resolve this issue.

Data not available when you log in to the mobile application

Occasionally, you may not be able to view any data on the mobile application. You must log out and log in to the application again to view the data. When you try to log in to application again, you may receive the message `User already logged in`. You must log out from the previous sessions to log in to the application. To log out from the previous sessions, do the following:

1. Go to the Wyse Management Suite web console.
2. Select the **Log me out everywhere else** option.
3. Log in to Wyse Management Suite.
4. Sign out from the session.

Now you can log in using the mobile application.

Wyse Management Suite application does not start after you change the Hostname

Wyse Management Suite Software Vault stores the sensitive keys inside two files. These files are named with the hostname of the server—one file with the hostname and the other file with the extension `.FCD`.

When the Software Vault service restarts after the hostname change, it tries to read the files with the updated hostname. Since the hostname is changed, Software vault does find these files, and it automatically creates these files with a new hostname.

The newly created files do not have the encryption keys in it which prevents the application from launching because it is unable to decrypt database passwords and other sensitive data.

You can recover the application using any of the following ways:

- Workaround 1
- Workaround 2

After you complete the steps, the application starts.

To ensure all the functions are working, do the following:

- Update the launcher URL
- Update the application and MQTT URLs in MongoDB

Update the launch URL

After changing the hostname, the **Launch WMS** shortcut uses the old URL. Do the following to update the URL:

Steps

1. Go to the Wyse Management Suite installation directory and locate the **WebUI** shortcut.
2. Right-click and select **Properties**.
3. Under the **Web Document** tab, update the URL field with the new hostname.
4. Click **Apply** and then click **OK**.

Use the **Launch WMS** shortcut to launch the application.

Update the application and MQTT URLs in MongoDB

Steps

1. Use a MongoDB user interface application such as Robo 3T and connect to MongoDB.
2. Run the following query: `db.getCollection('bootstrapProperties').find({"name" : { $in: ["mqtt.server.url", "stratus.external.mqtt.url", "stratus.external.preferred.mqtt.url", "stratus.external.secure.mqtt.url", "stratusapp.server.url"]}})`
3. Right-click and edit the document to update the hostname in the value fields.

Workaround 1 to recover the application

Steps

1. Go to `<InstallationPath>\DELL\WMS` and open the SoftwareVault directory.
2. Delete the files with new hostname in the filename.
3. Rename the files with old hostname with new hostname without changing the file extension.
4. Start the Wyse Management Suite Software Vault service.
5. Start the Wyse Management Suite Tomcat service.
6. Wait for the Tomcat service to start and access the application.

Workaround 2 to recover the application

Prerequisites

Software Vault utility is required.

Steps

1. Export the keys using Software Vault utility.
2. Change the hostname and restart the host server.
3. After you restart the server, start the Dell Software Vault service.
4. Import the keys using the Software Vault utility.
5. Start Tomcat service.
6. Wait for the Tomcat service to start and access the application.
   This action transfers the keys to the new files. The application can access the keys from the new files. Use the following commands:
   - To export the key using Software Vault Utility—`softwareVaultUtility-1.0.0.0.exe -mode export -password <PASSWORD>`
   - To import the key using Software Vault Utility— `softwareVaultUtility-1.0.0.0.exe -mode import -password <PASSWORD>`

Wrong credentials provided for Tomcat

When you upgrade Wyse Management from 4.0 or 4.1.1 to 4.2.1, you are prompted to enter the user or service account credentials for Tomcat. If wrong credentials are provided, then the Wyse Management Suite installer displays the **Invalid Credentials** error. The error might also appear if you do not have sufficient permissions. This happens if the user or the user group are not added to the relevant **Allow policy** group or added to the **Deny Policy** group. If the administrator selects **Enable this checkbox to bypass user credential validation**, then the installer proceeds with the upgrade. However, at the end of the installation the installer cannot start the Tomcat service and displays an error. This is because the **Dell WMS: Tomcat Service** is not in a running state.

About this task

To overcome the error, do the following:

Steps

1. Go to **Start** > **Run** and enter `services.msc`.
2. Press **Enter**.
3. Double-click **Dell WMS: Tomcat Service** or right click **Dell WMS: Tomcat Service** and click **Properties**.
4. Go to the **Log On** tab.
5. Click **Browse** and add the correct user account and password.
6. Click **Ok**.
7. Start the service.

Dell Tomcat service does not start after you install System Center Configuration Manager

After installing System Center Configuration Manager (SCCM) , the Dell WMS Tomcat service does not start. When Microsoft System Center Configuration Manager is installed, occasionally another Windows component occupies port 8005. When port 8005 is occupied by any other service or application, the Dell Wyse Management Server Tomcat service fails to start.

Steps

1. Go to **Start** > **Run** and enter `services.msc`.
2. Press **Enter**.
3. Stop the **Dell WMS: Tomcat Service**.
4. Go to `\Tomcat-9\conf` and open the `server.xml` file.
5. Check the server port number.
6. Go to **Start** > **Run** and enter `cmd`.
7. Press **Enter**.
8. In the Command Prompt, enter `netstat -a -o`.
9. Press **Enter**.
10. Locate port 8005 and document the associated PID.
11. Go to **Start** > **Run** and enter `resmon`.
12. Press **Enter**.
13. From the **Resource Monitor**, use the PID number that is documented from Step 8 to check for the service or application which is occupying the port.
14. If an application other than Tomcat is using port 8005, update the Wyse Management Suite server port in `server.xml` to an available port. For example, update the server port to 8006.
15. Go to **Start** > **Run** and enter `services.msc`.
16. Press **Enter**.
17. Stop the **Dell WMS: Tomcat Service**.
18. Launch Wyse Management Suite.

26

Frequently asked questions

Topics:

What happens when devices receive wave configurations and group configurations

You have created a wave with four phases, and each phase has a separate group selection and separate configuration per group. If the wave is in running state and three devices are selected in the phase from one group and the same group receives a group configuration, the deployment is handled as follows:

The selected devices in the wave receive the wave configurations, and then the configurations are merged to group configurations. Later, all devices in that group receive notification again to update configuration—three devices. Devices which have already received the configurations are ignored and the new devices receive the configurations.

Can you add new devices during wave deployment

When deployment waves are in running phase, the devices are leveraging the wave configurations. After the job is completed for a phase, the next phase starts based on the selection criteria for success or failure threshold. If you add devices during this phase, it creates ambiguity in terms of percentage calculations and then overall deployment.

How do you define the success threshold when you configure a wave

The success threshold is defined by the download and installation success.

How does the wave deployment work for offline devices

Devices in an offline state are filtered out during wave deployment when the phase starts. For example, in a group out of 100 devices, if 30 devices are offline, only 70 devices receive the configurations. The 30 devices are listed separately on the **Jobs** page as offline devices.

After the completion of the wave deployment and the configurations are merged to main group configurations, notifications are sent to all the devices again. When the offline devices come back online, they check-in to Wyse Management Suite. The latest configuration which is merged from the wave configuration to the main group configuration is deployed to the devices.

What is the difference between the wave configuration and group configuration

Group configuration is separated from wave configuration. Group configuration is meant for all devices in the group. Wave configuration is meant only for selected devices in wave. Devices that are not selected as part of wave configuration continue to receive group configuration whenever the devices request for configuration.

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.

How to create a domain user

Steps

1. Log in to the AD domain server as an administrator.
2. Go to **Active Directory Users and Computers** > **Users**.
3. Right-click the right window pane and click **New Users**.
4. Enter the username, full name, and password details and click **Save**.
5. Right-click the new user and select **Properties**.
6. Click the **Members of** tab and add the user group details if required.
   By default, the created user is added to the Domain Users group.
7. Clear the **User must change password at next logon** option and select the **User cannot change password and Password never expires** option.
   By default, **User must change password at next logon** option is enabled.

Results

Do the following when you are installing the Wyse Management Suite server or repository:

1. On the Windows server, go to **Local Security Policy** > **Local Policies** > **User Right Assignment**.
2. Right-click **Log on as a service** and select **Properties**.
3. Click **Add User or Group** and add your domain name. For example, domain\users; domain\administrator.
4. Click **Ok**.

How to create a user and assign LogonRight privilege

Steps

1. Log in as an administrator to the Windows server where Wyse Management Suite is going to be installed.
2. Go to **Computer Management** > **Local users and groups** > **Users**.
3. Right-click the right window pane and select **New User**.
4. Enter the username, full name, and password details and click **Save**.
5. Right-click the new user and select **Properties**.
6. Click the **Members of** tab and add the user group details if required.
   By default, the created user is added to the Local Users group.
7. Clear the **User must change password at next logon** option and select the **User cannot change password and Password never expires** option.
   By default, **User must change password at next logon** option is enabled.
8. On the Windows server, go to **Local Security Policy** > **Local Policies** > **User Right Assignment**.
9. Right-click **Log on as a service** and select **Properties**.
10. Click **Add User or Group** and add the user.
11. Click **Ok**.

How to upgrade Wyse Management Suite when MariaDB or MongoDB files are missing

When the MariaDB and MongoDB binary files are not available before you upgrade to version 3.6.1, you cannot upgrade Wyse Management Suite. You must ensure that the MongoDB binaries are present in the MongoDB bin folder. For example, the files should be present in `C:\Program Files\DELL\WMS\MongoDB\bin`. Similarly, the MariaDB files or folder count should be approximately 597 Files and 38 Folders. For example, `C:\Program Files\DELL\WMS\MariaDB`. To address the issue, do the following:

Prerequisites

Download and extract the following MariaDB and MongoDB binaries to a temporary directory based on the version of Wyse Management Suite installed on your system:

Table 18. MariaDB and MongoDB binaries

Wyse Management Suite version	Download link for MariaDB files	Download link for MongoDB files
3.3 and 3.3.1	MariaDB-10.2.35-winx64 zip file	MingoDB-win32-x86_64-2012plus-4.2.12 zip file
3.5, 3.5.1 and 3.5.2	MariaDB-10.2.40-winx64 zip file	MingoDB-win32-x86_64-2012plus-4.2.16 zip file
3.6	MariaDB-10.6.5-winx64 zip file	MongoDB-win32-x86_64-2012plus-4.2.17 zip file

Steps

1. From the extracted MongoDB files, copy the following files to the target directory:
   - Mongo.exe
   - Mongod.exe
   - Mongodump.exe
   - Mongoexport.exe
   - Mongoimport.exe
   - Mongorestore.exe
   - Mongos.exe
2. Copy all the extracted MariaDB files to the target directory.
3. Stop the following Wyse Management Suite services:
   - Dell WMS: Tomcat
   - Dell WMS: MQTT
   - Dell WMS: memcached
   - Dell WMS: MariaDB
   - Dell WMS: MongoDB
   - Dell WMS: Software Vault—applicable for Wyse Management Suite version 3.5 and later
4. Replace the files in `<Install Dir>\MariaDB Folder` and `<Install Dir>\MongoDB\bin` with the extracted files.
5. Restart the Wyse Management Suite services.
6. Upgrade Wyse Management Suite.

How to log in to the mobile application when the "User already logged in" message is received

Concurrent login is not supported in Wyse Management Suite. When you log in to the mobile application and receive the message `User already logged in`, you must log out from the previous sessions. To log out from the previous sessions, do the following:

1. Go to the Wyse Management Suite web console.

2. Select the **Log me out everywhere else** option.
3. Log in to Wyse Management Suite.
4. Sign out from the session.

Now you can log in using the mobile application.

How does the repository fallback function work when the subnets are configured

When there are multiple repositories available and the subnets are configured, WDA gets the list of the available repositories along with the configured subnets to download the application. The selection of the subnet depends on the configuration of **Preferred Repository** option.

- If the **Preferred Repository** option is not selected, the repository with the least subnet difference and highest priority is selected. If the repository is offline, WDA tries to connect to the selected repository again after 15 minutes. If the repository is still offline, the job fails.
- If the **Preferred Repository** option is selected, the preferred repository is used to download the application. If the preferred repository is online, WDA does not fall back to other repositories .

How does the repository fallback function work when the subnets are not configured

When there are multiple repositories available and the subnets are not configured, WDA gets the list of the available repositories from the server. The repository with the least subnet difference is selected for application download. If the administrator has two repositories with the same subnet difference, a test connection is called, and the fastest repository is selected for the download.

If the selected repository is offline, WDA tries to connect to the selected repository again after 15 minutes. If the repository is still offline, WDA falls back to the nearest repository.